Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 207 (2022) 54–63

Procedia Computer Science

www.elsevier.com/locate/procedia

26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2022)

Cryptographic encoding in modern symmetric and asymmetric encryption

Volodymyr Rudnytskyi [a], Oleksandr Korchenko [b], Nataliia Lada [a], Ruslana Ziubina [b, *]

Lukasz Wieclaw [b], Lukasz Hamera [b]

[a]*Cherkasy State Technological University, 460 Shevchenko bul., Cherkasy, 18-000, Ukraine*
[b]*University of Bielsko-Biala, 2 Willowa st., Bielsko-Biala, 43-300, Poland*

Abstract

In this article, we address the global problem of improving the quality of cryptographic trans-forming information. There were revealed contradictions between the approaches to the development of encryption algorithms for information security systems and encoding algorithms for information protection in computer systems and networks. One of the variants to solve this problem is creation a theory of cryptographic encoding. This work will explain the origins of researching the information encoding processes under the control of cryptographic primitives. The encryption algorithms' synthesis and analysis through the prism of discrete devices synthesis and analysis allow us to consider the cryptographic algorithms' classification issues in a different way, to determine possible directions for developing the new crypto algorithms, and to improve existing crypto algorithms. The correlations between symmetric and asymmetric ciphers are being analyzed. A new approach to the construction of asymmetric stream ciphers is proposed. The methods for increasing the length of the block of information and the length of the key for both new and already known encryption algorithms, as well as options for their implementation, are presented. The given examples of encryption algorithms demonstrate new opportunities for improving the computer cryptography systems and the information security cryptographic systems based on applying the new knowledge being obtained in the process of constructing a cryptographic encoding theory.

Keywords: information security; cryptography; information encoding; the quality of cryptographic algo-rithms; improving the quality of encryption

* Corresponding author. Tel.: +48 33 8279-264; fax: +48 33 8279-264.
E-mail address: rziubina@ath.bielsko.pl

1877-0509
10.1016/j.procs.2022.09.037

1. Introduction

What is the difference between encryption and encoding? In the classical definitions encryption differs from encoding by the fact that the key (password), or an algorithm is unknown, or a key and an algorithm are unknown at encryption [1-3].

In the process of transferring the classified information, three subjects are involved: the sender of the information, the recipient of the information and the attacker wanting to get hold of this information. Let's consider these three subjects' participation in the process of information protection:

• the sender of the information basing on the known to him algorithm and the key provides encrypting information. The question arises, why exactly encrypting information? After all, the sender knows both the key and the algorithm - and this is the process of encoding information. So, from the information sender's position, the process of encrypting information coincides with the process of encoding information;

• the recipient of the information basing on the known to him algorithm and the key provides decrypting information. From the information recipient's position, the process of decrypting information coincides with the process of decoding information;

• a key, or an algorithm is unknown to the attacker, or a key and an algorithm are unknown both to him at the same time. From the attacker's point of view, the information is encrypted, not encoded, and it must be decrypted, not decoded.

The process of encoding information is the process of converting information from one form of representation to another, in order to achieve a set goal. For example, to increase the speed of transferring information, to increase the equipment's service life, to detect and correct errors in the information, to reduce the complexity of devices, etc.

Taking into account the peculiarities of using the algorithms of encoding information in cryptography and the requirements for the results of their implementation, it is advisable to limit the concept of encoding to cryptographic encoding. Cryptographic encoding is in transforming a block of information using randomly selected lookup tables, implemented on the basis of discrete models of encoding [1]. The main task of cryptographic encoding is in randomly generating the models of lookup tables that ensure the implementation of specified requirements for the quality of data block's cryptographic transformation on a certain set of keys.

Main advantages: great variability in the choice of lookup tables. There are lookup tables for one byte, and lookup tables for the -bit block; high generation speed for lookup table's models, which ensure the implementation of the specified requirements for the quality of crypto transformation; high implementation speed of encoding devices' discrete models and their implementation ease.

At present, the main disadvantage of cryptographic encoding is the lack of a complete theory for constructing discrete models of permutation groups that ensure the implementation of the specified requirements for the quality of cryptographic trans-formations, and synthesizing the encoding devices with specified properties on their basis.

It should be noted that the main disadvantage of cryptographic encoding is an advantage at the same time, because in the process of researching the information transformations suitable for use in cryptography, existing approaches are being generalized and new approaches to constructing the computer cryptography systems and the systems of cryptographic information protection are being discovered.

Based on the implementation complexity, it is advisable to divide the systems of cryptographic information protection into the systems of computer cryptography and the systems of cryptographic information protection, because computer cryptography has fewer restrictions on computing resources during its implementation.

1.1. The article structure

The structure of the article is following. In section 2, it was briefly analyzed the history of the cryptographic encoding development. In section 3, an approach to re-searching the cryptographic algorithms was considered. This approach makes it possible to ensure the methodological unity of the crypto algorithms' analysis and classification, and also makes it possible to determine the ways to encryption's further improvement. A generalized analysis of symmetric and asymmetric cryptographic algorithms was carried out. In section 4 it was considered the classification issues of streaming and block crypto algorithms by the transformation quality. The 5th section is devoted to the conflict between the crypto transformation quality and the vulnerability to statistical cryptanalysis. In Section 6 is

devoted to some issues of practical improvement of the modern cryptographic systems' quality. The article ends with generalized conclusions about the presented work and the importance of cryptographic encoding for the development of information security systems.

2. Review of work-related publications

Modern cryptography is increasingly faced with the problems of the need to process huge data amounts in real time and in conditions of limited resources. One of the ways for solving the problem was the creation of the so-called "lightweight cryptography" [4-7]. Achievements in this area can be called the new lightweight cryptographic algorithms' analysis, development and implementation, which developed in parallel with classical crypto algorithms [8-16]. The work devoted to lightweight crypto algorithms is carried out in several directions: optimization of implementations taking into account various constraints or special constructions, in which smaller functions, fewer internal states, simpler rounds, etc. are used [4]. However, it should be noted that almost all developed lightweight ciphers are block ciphers [17]. Another way to solve the problems of low-resource cryptography became the creation and development of cryptographic encoding. The cryptographic encoding was based on the idea of using in cryptographic algorithms the randomly generated logical operations of information's cryptographic transformation that implement randomly selected lookup tables [1,18]. These operations implement both linear and nonlinear transformations of information [19-20]. Within the cryptographic encoding, the influence of redundancy on the complexity of the cryptographic transformation operations' implementation was investigated, re-searching of cryptographic transformations was started, the implementation of which is controlled both by a key sequence and by the information being encrypted [18]. Thus, "the lightweight cryptography" and "cryptographic encoding", although have common goals, achieve them in fundamentally different ways.

3. The approach to the computer cryptography algorithms' analysis, to their classification and determining the ways of further improvement

Some features of generalized encryption algorithms will be represented from the position of cryptographic encoding, and will be demonstrated on examples. It will be considered the operation of a block ciphering conditional system that processes blocks of information by n bits at a time and has a k -bit key. Let's represent the conditional algorithm of operating by the lookup table (Table 1). This substitution table is considered as a truth table of a discrete automaton, which provides encoding of n bits of information depending on a k -bit key.

It should be noted that the given ciphering conditional algorithm represents a linear transformation of information blocks, since for any γ_m $d_i \neq d_j$ if $m, i, j \in \{1, 2, 3, ..., 2^n\}$. Based on this, it can be argued that any block crypto algorithm provides only linear transformation of information blocks. The nonlinearity of the cryptographic transformation will appear when analyzing the encryption results at the level of having been converted information block's parts. A consequence of this statement may be a condition for the crypto algorithm's analyzing correctness: if during the analysis the crypto algorithm turned out to be nonlinear, then the size of the encryption block was determined incorrectly, or another significant error was made during the analysis carrying out.

Table 1. Tabular view of the block ciphering conditional algorithm

A set of keys' variants	A set of data blocks' variants											
	d_1	d_2	d_3	d_4	…	d_{n-1}	d_n	d_{n+1}	…	d_{2^n-2}	d_{2^n-1}	d_{2^n}
γ_1	d_{32}	d_{n-177}	d_{2^n-53}	d_{200}	…	d_{127}	d_{n-68}	d_{228}	…	d_{2^n-56}	d_{189}	d_{2^n-6}
γ_2	d_{108}	d_{n-76}	d_{255}	d_{77}	…	d_{51}	d_{n-8}	d_{168}	…	d_{2^n-41}	d_{2^n-38}	d_{n-209}
γ_3	d_{2^n-10}	d_{n-205}	d_{2^n-22}	d_{2^n-71}	…	d_{21}	d_{n-100}	d_{n-196}	…	d_{101}	d_{n-215}	d_{n-147}
γ_4	d_{n-70}	d_{171}	d_{n-122}	d_{43}	…	d_{89}	d_{40}	d_{2^n-27}	…	d_{48}	d_9	d_{2^n-18}
…	…	…	…	…	…	…	…	…	…	…	…	…
γ_{2^k-1}	d_{n-65}	d_{231}	d_{54}	d_{2^n-11}	…	d_{n-130}	d_{2^n-78}	d_{87}	…	d_{n-170}	d_{n-14}	d_{248}
γ_{2^k}	d_{2^n-13}	d_{n-136}	d_{239}	d_{2^n-31}	…	d_{146}	d_{59}	d_{n-2}	…	d_{n-46}		d_{138}

Table 2. The variant's tabular representation of a given conditional cipher ($n=4,\ k=3$)

A set of keys' variants	A set of data blocks' variants										
			d_2		d_3		d_4		⋯	d_{16}	
	0000		0001		0010		0011		…	1111	
	$d_{1.1}$	$d_{1.2}$	$d_{2.1}$	$d_{2.2}$	$d_{3.1}$	$d_{3.2}$	$d_{4.1}$	$d_{4.2}$	⋯	$d_{16.1}$	$d_{16.2}$
	00	00	00	01	00	10	00	11	…	11	11
	d_7		d_5		d_8		d_6		⋯	d_{10}	
γ_1	0110		0100		0111		0101		…	1001	
	$d_{7.1}$	$d_{7.2}$	$d_{5.1}$	$d_{5.2}$	$d_{8.1}$	$d_{8.2}$	$d_{6.1}$	$d_{6.2}$	⋯	$d_{10.1}$	$d_{10.2}$
	01	10	01	00	01	11	01	01	…	10	01
	d_{13}		d_9		d_5		d_1		⋯	d_4	
γ_2	1100		1000		0100		0000		…	0011	
	$d_{13.1}$	$d_{13.2}$	$d_{9.1}$	$d_{9.2}$	$d_{5.1}$	$d_{5.2}$	$d_{1.1}$	$d_{1.2}$	⋯	$d_{4.1}$	$d_{4.2}$
	11	00	10	00	01	00	00	00	…	00	11
…	…	…	…	…	…	…	…	…	…	…	…
	d_{11}		d_3		d_{15}		d_7		⋯	d_6	
γ_8	1010		0010		1110		0110		…	0101	
	$d_{11.1}$	$d_{11.2}$	$d_{3.1}$	$d_{3.2}$	$d_{15.1}$	$d_{15.2}$	$d_{7.1}$	$d_{7.2}$	⋯	$d_{6.1}$	$d_{6.2}$
	10	10	00	10	11	10	01	10	…	01	01

Let's show this on example. Let the data block in block ciphering has a length of 4 bits, and the key has a length of 3 bits. Let's give in a tabular representation (Table 2) the encryption algorithm as one variant of this conditional cipher. The encryption results' analysis for linearity will be made by 2 bits. In the Table 2 the variants of the detected nonlinear transformation of two bit block "00" at different values of the key sequence are highlighted as shaded cells. However, the found non-linearity of this crypto transformation is disappearing when the lookup table is analyzed using 4-bit blocks.

It should be noted some more features of the variant's tabular representation of the given conditional cipher, which have a significant impact on cryptography, but at the same time are quite simple to visualize and do not require complex explanations.

4. The stream and block crypto algorithms' classification by transformation quality

4.1. The block ciphers' classification by strength and its disadvantages

The main characteristic of a cryptosystem is its strength.

Today, the most common block ciphers' classification by strength is the classification based on the length of the information block and the length of the key [22]:

− ultra-high strength - the length of the information block and the length of the key are not less than 512 bits;

− high strength - the length of the information block and the length of the key are not less than 256 bits;

− normal strength - the length of the information block and the length of the key are not less than 128 bits;

− satisfactory strength - the length of the information block is not less than 64 bits and the length of the key is not less than 128 bits.

Thus, the crypto algorithm's strength is determined by the length of the information block and the length of the key, as it can be seen from the classification above. Based on this, the increase of the encryption strength should be based on increasing the length of the information block and the length of the key, or only the length of the information block or the length of the key. It should be noted that this approach allows classifying the block ciphers only, but not stream ciphers, because the block length is equal to one bit in stream ciphers, and as a consequence of the above classification, all of them must have an unsatisfactory level of strength.

4.2. The tabular representation of stream ciphers

The tabular representation of the ciphering conditional algorithm (Figure 1) allows describing block ciphers, and on condition provided that $n=1$ a stream cipher will be described. Therefore, this representation should allow classifying both block and stream ciphers.

If $F_{\gamma_m}(d_i)=z_i$, then exists a mask $M_{\gamma_m,i}$, such that $d_i \oplus M_{\gamma_m,i}=z_i$, so a block cipher may be considered as a stream cipher.

Another stream cipher's interpretation is that the length of the block is equal to the length of the message that is being encrypted.

In this case, the strength will be determined by the length of the message equal to the length of the key, and as a consequence, basing on the given classification, the crypto algorithm's strength will be determined by the length of the encrypted information. Thus, having the information length less than the block length of the block cipher, the block cipher's strength will be greater than that of the stream cipher, and if the length of the message is greater than the block length of the block cipher, the strength of the block cipher will be less than that of the stream cipher. Based on this, the probability of decrypting the short messages will be greater, than the probability of decrypting the large arrays (blocks) of data, which is not true. These examples once again confirm the imperfection of the crypto algorithms' classification based on the length of the key and the length of the information block.

4.3. The quality of cryptographic transforming the information

For symmetric and asymmetric encryption its encryption strength can be determined by the quality of crypto-transforming the information block.

Let $q_1,\ q_2, q_3, \dots, q_b$ be the minimum permissible values of the quality indicators for cryptographic transforming the information block, which are determined by the methods $Q_1(d_i, F_{\gamma_v}(d_i))$, $Q_2(d_i, F_{\gamma_v}(d_i))$, $Q_3(d_i, F_{\gamma_v}(d_i))$,…, $Q_b(d_i, F_{\gamma_v}(d_i))$ where $i \in \{1, 2, 3, ..., 2^n\}$, $v \in \{1, 2, 3, ..., 2^k\}$. If $Q_1(d_i, F_{\gamma_v}(d_i)) \geq q_1$; $Q_2(d_i, F_{\gamma_v}(d_i)) \geq q_2$; $Q_3(d_i, F_{\gamma_v}(d_i)) \geq q_3$; …; $Q_b(d_i, F_{\gamma_v}(d_i)) \geq q_b$, then it can be argued that $Q(d_i, F_{\gamma_v}(d_i)) \geq q$ and the crypto algorithm *meets the specified requirements* for the quality of the data block crypto-transformation on a given set of keys. Having $Q(d_i, F_{\gamma_v}(d_i))[<\geq]q$ the crypto algorithm will *partially meet the requirements* for the crypto transformation quality, and having $Q(d_i, F_{\gamma_v}(d_i)) < q$ *will not meet the specified requirements*. For the results of evaluating the set of values q a sign $[<\geq]$ was used that shows that the set simultaneously contains indicators for the cryptographic transformation quality that are not less than the minimum acceptable values, as well as quality indicators that are less than the minimum acceptable values.

If the crypto algorithm, given in the Table 1 is qualitative, then the result of crypto transforming the i-th block of information is always in the i-th column of the table, in any other case, at this stage of the study, we will assume that the algorithm does not meet, or partially meets the specified requirements for the crypto-transformation quality.

4.4. The stream and block ciphers' quality

The quality of transforming the information block by the crypto algorithm given in Table 1 will be defined as $q = f(d_i, F_{\gamma_v}(d_i))$, where $F_{\gamma_v}(d_i) = (A, \gamma_v, d_{i.1}, d_{i.2}, .., d_{i.n})$ and will depend on the algorithm of crypto transformation (A), the key (γ_v), and all bits of the information block ($d_{i.1}, d_{i.2}, .., d_{i.n}$), which will be encrypted. The transformation quality depends on many factors in block encryption, and none of them is able to ensure the guaranteed achievement of the set result.

If it is implemented the streaming encryption based on the Table 1, then the transformation quality of the i-th bit of information will be determined as $q_i = f(d_i, \gamma_v(i))$ depended on i -th bit of information and i -th bit of a pseudo-random sequence derived based on the sweep of the key. In streaming encryption, in contrast to the block encryption, the crypto algorithm's quality depends only on the quality of pseudo-random sequence, which, in the process of the modulo addition, with the same quality, is guaranteed to change information.

5. Overcoming the conflict between the indicators' increase of crypto-transformation quality and the vulnerability to statistical analysis

5.1. Causes of appearance of the conflict

Despite the high quality of the cryptographic transforming the block of information, the given ciphering conditional algorithm cannot be effectively applied in promising systems of computer cryptography. Why? Open information analysis makes it possible to identify statistical dependences in it, which in turn will ensure the presence of similar dependences in closed output information. This is due to the fact that the ciphering conditional algorithm (Table 1) implements one lookup table, and statistical data can be collected from the one lookup table.

One of the simplest ways for partially counteracting the statistical (linear) cryptanalysis of block ciphering results is to increase the data block.

Increasing the data block length leads to complicating the statistical analysis of encrypted information, since it needs a significant increase in the required data amount, and also leads to an exponential increase in the necessary computing resources for the analysis itself.

It should be noted that an increase in the encryption quality requires an increase in the number of quality indicators for the cryptographic transformation of the information block, which in turn, as a rule, leads to decreasing the number of variants for converting the information block. Decreasing the number of conversion variants is due to increasing the restrictions on the results of converting an information block, due to increasing the number of quality indicators. In addition, decreasing the number of variants for conversing a block of information leads to deterioration in the statistical characteristics of the results of encrypting information if they are considered as a pseudo-random sequence.

5.2. The ways for overcoming the conflict

The crypto algorithm given in the lookup table can be considered as a cryptosystems' group with completely identical properties. The cryptosystems of this group will differ only in the complexity of practical implementation.

Let’s consider two ways for constructing this group of algorithms:

- developing the similar algorithms which will provide permutation of rows in the lookup table;
- applying a well-known proven algorithm with additional transformation of keys.

Using any of the above options will allow getting up to $2^k!$ lookup tables with the similar cryptographic properties, where k is bitness of the key. In practice, both options for constructing a group of crypto algorithms will be reduced to key numbering, for example, based on their XOR ciphering.

To enable the ability of the conditional crypto algorithm’s practical application, it is necessary to modify the lookup table to encrypt each next block of incoming information. To do this, by analogy with streaming encryption, it will be applied additional XOR ciphering.

The main effect of additional XOR ciphering on the cryptographic strength and on the length of the key is manifested through the lookup tables’ modification (Table 1) by the rows and /or columns permutation at each step of encryption and decryption. Also, an additional XOR ciphering can additionally change the tabular representation of the block ciphering conditional algorithm by expanding the variants' set of the keys (the number of table’s rows).

6. Improving the quality of modern cryptographic systems

It is used several rounds of encryption for increasing the resistance to statistical cryptanalysis in most of the existing crypto algorithms. Let’s consider re-encryption of the information block using the example of the block ciphering conditional algorithm shown in the Table 1

If $F_{\gamma_p}(F_{\gamma_v}(d)) = F_{\gamma_h}(d)$, under the condition that $p, v, h \in \{1, 2, 3, ..., 2^k\}$, it can be argued that given in the Table 1 ciphering algorithm is a group of transformations on a given set of keys. Since the given crypto algorithm is a group of transformations, according to Shannon's theorem [21], it does not provide an increase in cryptographic strength when re-encrypted. In order to bypass this Shannon's limitation and to increase the cryptographic strength, it is necessary to achieve increasing the number of keys during the re-encryption process, or to increase the length of the information block that is being encrypted. It is possible to achieve an increase in the field of the keys only in some

cases considered earlier, but this requires a change in the encryption algorithm. The cryptographic strength is possible to be increased by using of another crypto algorithm when re-encrypted.

Let's consider one of the variants for improving any encryption algorithm that will provide the cryptographic strength increasing by increasing the length of the key and the length of the information block.

To assess the advantages and disadvantages of the proposed approach, in comparison with multi-round encryption, the following notation will be introduced:

If the algorithm has q rounds of encryption, then it will be described as:

$$F_{\gamma}(d) = F_{q\gamma_q}(F_{(q-1)\gamma_{(q-1)}}(...(F_{3\gamma_3}(F_{2\gamma_2}(F_{1\gamma_1}(d))))...))$$

where $F_{i\gamma_i}(d_{i-1})$ – is the i-th round of encryption on the i - th round key.

The encryption time ($t_{ш}$) will be determined as the sum of time amounts spent on all encryption rounds ($t_{шр}$): $t_{ш} = q \cdot t_{шр}$.

In general, q rounds of decryption will be described as:

$$F'_{\gamma}(d) = F'_{1\gamma_1 q\gamma_q}(F'_{2\gamma_2}(F'_{3\gamma_3}(...(F'_{(q-1)\gamma_{(q-1)}}(F'_{q\gamma_q}(d)))...)))$$

The decryption time will be determined as the sum of time amounts spent on all decryption rounds: $t'_{ш} = q \cdot t'_{шр}$. It should be noted that the multi-round encryption does not allow parallelizing the encryption and decryption of the information block by the round.

Let the modulo two addition operation be the basis for improving the multi-round algorithms of block ciphering. This operation is often used to improve the quality of the resulting pseudo-random sequence of several, by their bitwise modulo addition.

However, the bitwise addition of the encryption results by several keys, for example, keys m and n cannot be used to improve the conversion quality, since the encryption result cannot be recovered. This is due to the fact that the encryption result will not always depend on the input data being encrypted.

The modulo addition is possible to be used for improving the quality of encryption only in the conditions of encrypted blocks displacement before addition. For example, if $F_{\gamma_m}(d_i) = (M_{\gamma_m,i} \oplus d_i) = z_i$ is the result of encrypting the i-th block of information by an arbitrary crypto algorithm on the m-th key, obtained on the basis of addition with the transformation mask, and $F_{\gamma_n}(d_j) = (M_{\gamma_n,j} \oplus d_j) = z_j$ is the result of encrypting the j-th block of information by an arbitrary crypto algorithm on the n-th key, obtained on the basis of addition with the transformation mask, then:

$$F_{\gamma_m}(d_i) \oplus F_{\gamma_n}(d_j) = (M_{\gamma_m,i} \oplus d_i) \oplus (M_{\gamma_n,j} \oplus d_j) = (M_{\gamma_m,i} \oplus M_{\gamma_n,j}) \oplus (d_i \oplus d_j).$$

Please note that the encryption result will depend on the value of two blocks being encrypted and two keys that define the transformation masks. Consequently, this approach allows increasing the length of information blocks that need to be analyzed when breaking a cryptosystem.

To decrypt the modulo addition results of the encrypted blocks, it is to be known $F_{\gamma_m}(d_i)$ or $F_{\gamma_n}(d_j)$.

If d_j is unknown, then it should be known $F_{\gamma_m}(d_i)$, consequently $d_j = F'_{\gamma_n}(z_j \oplus F_{\gamma_m}(d_i))$. If d_i is unknown, then it should be known $F_{\gamma_n}(d_j)$, consequently $d_i = F'_{\gamma_m}(z_i \oplus F_{\gamma_n}(d_j))$.

Let us apply the considered modulo two addition with the encryption blocks offset to improve any crypto algorithm for ensuring an increase in cryptographic strength by increasing the length of the key and the length of the information block.

Let's consider by an example the improved information encryption and decryption when using two keys. The variants of the turn-based implementing the combination of the information encryption and decryption results, based on two keys, are given in the Table 3. This encryption improvement is applicable to increase the cryptographic strength of both symmetric and asymmetric crypto transformations.

To reduce the probability of encryption errors' propagation, at the w-th algorithm's step, a length limitation of the resulting encryption block is implemented. In this and subsequent examples, when limiting the resulting information block, the keys' renumbering will not be considered. In the improved block cipher, in addition to the encryption block, it is necessary to select the resulting encryption block. In this example, encryption based on two keys is carried out by n bits at a time, and the resulting encryption block will be $w \cdot n$ bits long, and exactly this block length determines the complexity of cryptanalysis and the cryptosystem's strength.

Table 3. The algorithms of encryption and decryption when applying two keys

The conversion steps	Encryption If $F_\gamma(d)=z$ then	Decryption If $F'_\gamma(z)=d$ then
1	$z_1=F_{\gamma_1}(d_1)$	$d_1=F'_{\gamma_1}(z_1)$;
2	$z_2=F_{\gamma_1}(d_2)\oplus F_{\gamma_2}(d_1)$	$d_2=F'_{\gamma_1}(z_2\oplus F_{\gamma_2}(d_1))$
3	$z_3=F_{\gamma_1}(d_3)\oplus F_{\gamma_2}(d_2)$	$d_3=F'_{\gamma_1}(z_3\oplus F_{\gamma_2}(d_2))$
4	$z_4=F_{\gamma_1}(d_4)\oplus F_{\gamma_2}(d_3)$	$d_4=F'_{\gamma_1}(z_4\oplus F_{\gamma_2}(d_3))$
…	……	……
w	$z_w=F_{\gamma_1}(d_w)\oplus F_{\gamma_2}(d_{w-1})$	$d_w=F'_{\gamma_1}(z_w\oplus F_{\gamma_2}(d_{w-1}))$
w+1	$z_{w+1}=F_{\gamma_1}(d_{w+1})$	$d_{w+1}=F'_{\gamma_1}(z_{w+1})$
w+2	$z_{w+2}=F_{\gamma_1}(d_{w+2})\oplus F_{\gamma_2}(d_{w+1})$	$d_{w+2}=F'_{\gamma_1}(z_{w+2}\oplus F_{\gamma_2}(d_{w+1}))$
w+3	$z_{w+3}=F_{\gamma_1}(d_{w+3})\oplus F_{\gamma_2}(d_{w+2})$	$d_{w+3}=F'_{\gamma_1}(z_{w+3}\oplus F_{\gamma_2}(d_{w+2}))$
…	……	……

As it can be seen from the given examples (Table 3), to implement the algorithms of encryption and decryption, one must have both keys. Based on this, the length of the resulting key will be doubled.

By analogy, let's consider the encryption and decryption of information when using q keys. The variants of the turn-based implementing the combination of the information encryption and decryption results, based on applying q keys, are given in the Table 4.

The symmetry of encryption algorithms, which are presented in Table 4 depends on the symmetry of the used crypto-transformations or crypto systems.

The length of the resulting encryption block is a multiple of the length of the one-round algorithm's encryption block and is determined by the specified merges amount of intermediate encryption results into the final encryption result. In this case, w blocks by n bits each are combined, and the resulting encryption block will be $w\cdot n$ bits long.

Based on this, it can be argued that the transition from the encryption rounds to encryption stages, based on the use of several keys, provides increasing the length of the resulting encryption block and the length of the key. The length of the key will increase in proportion to the encryption stages' number. The statement's correctness about the increase of the resulting key's length is based on the resulting algorithm output from the group of algorithms providing the stages of encryption implementation. For different encryption stages, different crypto algorithms can be used with the same or multiple encryption block lengths.

Table 4. The algorithms of encryption and decryption when applying q keys

Steps	Encryption If $F_\gamma(d)=z$ then	Decryption If $F'_\gamma(z)=d$ then
1	$z_1=F_{\gamma_1}(d_1)$	$d_1=F'_{\gamma_1}(z_1)$;
2	$z_2=F_{\gamma_1}(d_2)\oplus F_{\gamma_2}(d_1)$	$d_2=F'_{\gamma_1}(z_2\oplus F_{\gamma_2}(d_1))$
3	$z_3=F_{\gamma_1}(d_3)\oplus F_{\gamma_2}(d_2)\oplus F_{\gamma_3}(d_1)$	$d_3=F'_{\gamma_1}(z_3\oplus F_{\gamma_2}(d_2)\oplus F_{\gamma_3}(d_1))$
…	……	……
q	$z_q=F_{\gamma_1}(d_q)\oplus F_{\gamma_2}(d_{q-1})\oplus\ldots\oplus F_{\gamma_q}(d_1)$	$d_q=F'_{\gamma_1}(z_q\oplus F_{\gamma_2}(d_{q-1})\oplus\ldots\oplus F_{\gamma_q}(d_1))$
q+1	$z_{q+1}=F_{\gamma_1}(d_{q+1})\oplus F_{\gamma_2}(d_q)\oplus\ldots\oplus F_{\gamma_q}(d_2)$	$d_{q+1}=F'_{\gamma_1}(z_{q+1}\oplus F_{\gamma_2}(d_q)\oplus\ldots\oplus F_{\gamma_q}(d_2))$
q+2	$z_{q+2}=F_{\gamma_1}(d_{q+2})\oplus F_{\gamma_2}(d_{q+1})\oplus\ldots\oplus F_{\gamma_q}(d_3)$	$d_{q+2}=F'_{\gamma_1}(z_{q+2}\oplus F_{\gamma_2}(d_{q+1})\oplus\ldots\oplus F_{\gamma_q}(d_3))$
…	……	……
w	$z_w=F_{\gamma_1}(d_w)\oplus F_{\gamma_2}(d_{w-1})\oplus\ldots\oplus F_{\gamma_q}(d_{w-q})$	$d_w=F'_{\gamma_1}(z_w\oplus F_{\gamma_2}(d_{w-1})\oplus\ldots\oplus F_{\gamma_q}(d_{w-q}))$
w+1	$z_{w+1}=F_{\gamma_1}(d_{w+1})$	$d_{w+1}=F'_{\gamma_1}(z_{w+1})$
w+2	$z_{w+2}=F_{\gamma_1}(d_{w+2})\oplus F_{\gamma_2}(d_{w+1})$	$d_{w+2}=F'_{\gamma_1}(z_{w+2}\oplus F_{\gamma_2}(d_{w+1}))$

$w+3$	$z_{w+3} = F_{\gamma_1}(d_{w+3}) \oplus F_{\gamma_2}(d_{w+2}) \oplus F_{\gamma_3}(d_{w+1})$	$d_{w+3} = F^{/}_{\gamma_1}(z_{w+3} \oplus F_{\gamma_2}(d_{w+2}) \oplus F_{\gamma_3}(d_{w+1}))$
…	……	……

Let's define the time q of staged encryption and decryption of a n-bit block of information. The block length of n bits was chosen for the correct comparison of the conversion time compared to a q-round encryption.

Let's consider a sequential implementation of the encryption. The encryption time will be determined as $t_{ш} = q \cdot t_{шр} + (q-1) \cdot t_{\oplus}$ where $t_{\oplus}$ – is implementation time of the modulo two addition operation. With the sequential implementation of decryption, the transformation will be determined as $t^{/}_{ш} = t^{/}_{шр} + (q-1) \cdot (t_{шр} + t_{\oplus})$. As it can be seen from the given expressions, the multi-round encryption and decryption time practically matches the multi-stage encryption and decryption time, since $t_{шр} = t^{/}_{шр}$, $t_{шр} >> t_{\oplus}$. It can be seen from the given examples that combining the encryption stages based on the use of several keys allows parallelizing the encryption and decryption processes: $t_{ш} = t_{шр} + (q-1) \cdot t_{\oplus}$; $t^{/}_{ш} = t^{/}_{шр} + t_{шр} + (q-1) \cdot t_{\oplus}$. Based on this, it can be argued that the use of the pipeline-parallel structure of the algorithms' hardware implementation makes it possible to reduce the time of multi-stage encryption practically to the time of one encryption round implementation, and the decryption time to the time of two rounds implementation: the encryption round and the decryption round.

The considered multi-stage encryption algorithms' modification can be implemented based on the use of multi-operand operations of cryptographic encoding instead of modulo addition. The use of these operations will provide combinatorial increasing the variability in the procedure of the encrypted blocks' resulting combination

The given options for modifying multi-key encryption algorithms implement methods of multi-stage information transformation and eliminate the disadvantages of multi-round encryption. They provide an increase in the encryption block, in the length of the key sequence and in the strength of the crypto transformation. These examples demonstrate new opportunities for improving computer cryptography systems and cryptographic systems of information security. The above results are based on new knowledge gained in the process of constructing a theory of cryptographic encoding.

7. Conclusions

Cryptographic encoding is one of the new promising areas of cryptology, which has not received sufficient attention. For the research, a conditional algorithm of block ciphering by the lookup table was presented. This table is considered as a truth table of a discrete automaton, which provides the information encoding, depending on the key. It is shown that with the correct definition of the encryption block, the cryptographic algorithm will be linear. As a result of studying the operations' symmetry of cryptographic transformation and the block cryptographic algorithms, the interdependencies between symmetric and asymmetric transformations of information have been established. It is proposed to extend the algorithms' classification by the symmetry additionally depending on the ratio of symmetric and asymmetric keys, on the ratio of symmetric and asymmetric transformations, on the complexity of the keys' transformation. It is shown that practical implementation is an essential factor in most cases in defining an asymmetric cryptographic transformation as an algorithm with a public or private key. The use of cryptographic encoding operations in stream ciphering allows creating symmetric and asymmetric ciphers, in which the length of the pseudo-random sequence may not coincide with the length of the information being converted. Based on the tabular presentation of stream ciphers, the possibility of constructing the asymmetric stream ciphers is considered. It is considered a proposal for the classification of stream and block ciphers by the quality of cryptographic transformation. The reasons for the occurrence and ways of overcoming the conflict between the increase in the quality indicators of cryptographic transformation and the vulnerability to statistical analysis are considered. The analysis of the key length is carried out and the possibilities of its increase are considered. The issues of improving the quality of modern symmetric and asymmetric cryptosystems are considered. The presented results of applying the cryptographic encoding make it possible to overcome the limitations associated with an increase of the encryption block, a long key sequence and encryption strength. New previously unknown results obtained during the study of cryptographic encoding are very important for the improvement and development of both computer cryptography systems and cryptographic systems of information security.

References

[1] Rudnitsky V, Pivneva S, Babenko V, Mironets I, et al. Cryptographic coding: methods and means of implementation: monograph. Togliatti. State University; 2013. (in Russian)

[2] Communication Theory Information Theory Cryptography. Claude E Shannon [Internet]. IEEE; 2009.

[3] Schneier B. Applied Cryptography, Second Edition. John Wiley & Sons, Inc.; 2015.

[4] Avoine G, Hernandez-Castro J, editors. Security of Ubiquitous Computing Systems. Springer International Publishing; 2021.

[5] Biryukov A, Perrin L. Symmetrically and Asymmetrically Hard Cryptography. Lecture Notes in Computer Science [Internet]. Springer International Publishing; 2017;417–45.

[6] Hatzivasilis G, Fysarakis K, Papaefstathiou I, Manifavas C. A review of lightweight block ciphers. Journal of Cryptographic Engineering [Internet]. *Springer Science and Business Media LLC*; 2017 Apr 12;**8**(**2**):141–84.

[7] Manifavas C, Hatzivasilis G, Fysarakis K, Papaefstathiou Y. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks* [Internet]. Wiley; 2015 Dec 21;**9**(**10**):1226–46.

[8] Matsui M. New block encryption algorithm MISTY. Lecture Notes in Computer Science [Internet]. Springer Berlin Heidelberg; 1997;54–68.

[9] Karakoç F, Demirci H, Harmancı AE. ITUbee: A Software Oriented Lightweight Block Cipher. Lightweight Cryptography for Security and Privacy [Internet]. Springer Berlin Heidelberg; 2013;16–27.

[10] Knudsen L, Leander G, Poschmann A, Robshaw MJB. PRINTcipher: A Block Cipher for IC-Printing. Lecture Notes in Computer Science [Internet]. Springer Berlin Heidelberg; 2010;16–32.

[11] Shirai T, Shibutani K, Akishita T, Moriai S, Iwata T. The 128-Bit Blockcipher CLEFIA (Extended Abstract). Lecture Notes in Computer Science [Internet]. Springer Berlin Heidelberg; 2007;181–95.

[12] De Cannière C, Dunkelman O, Knežević M. KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. Cryptographic Hardware and Embedded Systems - CHES 2009 [Internet]. Springer Berlin Heidelberg; 2009;272–88.

[13] Journault A, Standaert F-X, Varici K. Improving the security and efficiency of block ciphers based on LS-designs. Designs, Codes and Cryptography [Internet]. *Springer Science and Business Media LLC*; 2016 Mar 9;**82**(**1-2**):495–509.

[14] Rivest RL. The RC5 encryption algorithm. Lecture Notes in Computer Science [Internet]. Springer Berlin Heidelberg; 1995;86–96.

[15] Guo J, Peyrin T, Poschmann A, Robshaw M. The LED Block Cipher. Lecture Notes in Computer Science [Internet]. Springer Berlin Heidelberg; 2011;326–41.

[16] Berger TP, Francq J, Minier M, Thomas G. Extended Generalized Feistel Networks Using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput. *IEEE Transactions on Computers* [Internet]. Institute of Electrical and Electronics Engineers (IEEE); 2016 Jul 1;**65**(**7**):2074–89.

[17] McKay KA, Bassham L, Turan MS, Mouha N. Report on lightweight cryptography. National Institute of Standards and Technology; 2017 Mar.

[18] Rudnitsky V, Milchevich V, Babenko V, Melnik R, Rudnitsky S, Melnik O. Cryptographic coding: methods and means of implementation (part 2): a monograph. Generous Estate Plus; Kharkov; 2014. (in Ukrainian)

[19] Babenko V, Pivneva S, Melnik O, Melnik R. Parallel implementation of nonlinear extended matrix cryptographic transformation. *Vector of science of Togliatti State University.* Togliatti; TSU; 2014; **3** (**29**):17-19. (in Russian)

[20] Sysoienko S, Myronets I, Babenko V. Practical Implementation Effectiveness of the Speed Increasing Method of Group Matrix Cryptographic Transformation. Proceedingsof the Second International Workshop on Computer Modelingand Intelligent Systems (CMIS-2019), Zaporizhzhia, Ukraine, April 15-19, 2019.CEUR Workshop Proceedings 2353, CEUR-WS.org2019: 402–412. (In Ukrainian).

[21] Kuznetsov O, Ol'yinikov R, Gorbenko Y, others: A framework for the requirements, the generation and analysis of promising symmetric cryptocurrencies on the basis of block ciphers. *Visn. National University "Lviv Polytechnic*; 2014Vol. **806**:124-140. (in Ukrainian)

[22] Jancarczyk D, Rudnytskyi V, Breus R, Pustovit M, Veselska O, Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits. 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) [Internet]. IEEE; 2020 Sep 17; 247-254.