1. Introduction

M. J. Mihaljević and H. Imai [8, 9, 11, 12] proposed a general approach for design of randomized stream ciphers based on joint employment of encryption, error-correction coding, and dedicated random (or homophonic) coding. One of the goals of designing such ciphers is to increase the security (without substantial performance reducing) of stream ciphers currently used in wireless communication systems, particularly, in the GSM standard. Another reason is to construct symmetric encryption schemes, whose security can be reduced to the hardness of some known mathematical problem such as the Learning from Parity with Noise (LPN) problem. Recall [see [6], for example] that this problem consists in solving a system of linear Boolean equations with equiprobable random coefficient matrix and the right-hand side corrupted by independent random variables taking values 0 and 1 with probabilities 1−θ and θ, respectively, θ∈(0,1/2). In this case, we say that θ is the noise level in the right-hand side of the given system of linear equations.

In what follows, we focus our attention on the versions of randomized stream ciphers defined in [11, 12] and studied in detail in [10, 11, 13].

Let’s denote by $V_n$ the set of all $n$-dimensional Boolean vectors, by $F_{m×n}$ the set of $m×n$-matrices over the field $F = GF(2)$, and by $F_{m×n}^*$ the group of all invertible matrices of order $m$ over this field.

According to [11, 12], the initial objects for a randomized stream cipher with parameters $l, m, n ∈ N, p ∈ (0, 1/2)$, where $l < m < n$, and a key space $K$ are matrices $G_1 ∈ F_{m×n}, G_2 ∈ F_{msm}^*$, and a keystream generator that produces a sequence $f_0(k), f_1(k), ...$ of $n$-dimensional Boolean vectors determined by a key $k ∈ K$. It is assumed that the functions $f_i : K → V_n, i = 0, 1, ..., p$ can depend on some public parameters, for example, on initialization vectors (IV’s). It is also assumed that $G_1$ is a generator matrix of a binary linear $[n, m]$-code $C_1$ with an efficient decoding algorithm, which is guaranteed to correct errors in the binary symmetric channel with crossover probability $p$.

To encrypt a plaintext $s_0, s_1, ..., s_l$, where $s_i ∈ V_l, i = 0, 1, ..., l$, with a key $k ∈ K$ the sender generates a sequence of independent random vectors $u_0, u_1, v_1, ..., u_l, v_l$, where $u_i$ is uniformly distributed on the set $V_{m−l}$, and $v_i$ is distributed according to Bernoulli’s law with parameters $(n, p)$, and computes the ciphertext $z_0, z_1, ..., z_l$ as follows:

$$z_i = (s_i, u_i)G_2G_1 ⊕ f_i(k) ⊕ v_i, i = 0, 1, ..., l .$$ (1)
The legitimate receiver, knowing $f_i(k)$, can quickly find the message $(s_i, u_t)G_2$ with the efficient decoding algorithm for the code $G_1$, after that he can recover $s_i$ using invertibility of the matrix $G_2$. On the other hand, the adversary in order to find the key $k$ will be forced to deal with a corrupted keystream $f_i(k) \oplus (s_i, u_t)G_2G_1 \oplus v_i$, $i=0, 1, ..., t$.

In [10, 11, 13] different variants of randomized ciphers, as in particular, with the following functions $f_i$:

$$f_i(k) = kS^i, \quad k \in K = V_n,$$

where $S$ is a non-secret $n \times n$ matrix over the field $F$;

$$f_i(k) = \alpha_0 k, \quad k \in K = F_{n \times n},$$

where $\alpha_0, \alpha_1, ..., \alpha_t$ are independent equiprobable random Boolean vectors of size $n$. Note that in the last case, a ciphertext is by definition the sequence $(\alpha_0, z_0), (\alpha_1, z_1), ..., (\alpha_t, z_t)$, where $z_i$ are computed by formula (1). Strictly speaking, randomized encryption schemes of this type do not belong to the class of stream ciphers, and are proposed in [11] in order to generalize and to enhance one of the earlier probabilistic private-key encryption schemes, whose security can be reduced to the hardness of the LPN problem [6].

Based on the condition of implementation simplicity of the described encryption scheme, it was proposed in [10] to set up the matrices $G_1$ and $G_2$ as follows:

$$G_1 = \begin{pmatrix} I_{m-l} & 0 & A_l \\ 0 & I_l & A_2 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 0 & I_l \\ I_{m-l} & B \end{pmatrix}$$

(4)

where $A_l \in F_{(m-l) \times (n-m)}$, $A_2 \in F_{l \times (n-m)}$, $B \in F_{(m-l) \times l}$, and $I_l$, $I_{m-l}$ are identity matrices of specified size. In this case the transform

$$s \mapsto (s, u)G_2G_1 = (u, s \oplus uB, sA_2 \oplus u(A_l \oplus BA_2)),$$

$$s \in V_l, \quad u \in V_{m-l},$$

(5)

used in (1) describes well-known combined random coding scheme for the wiretap channel proposed in fact in the fundamental paper [15] and extensively studied later (see [1, 14] for a comprehensive survey). Security evaluation of randomized ciphers specified by (1), both from information-theoretic and computational points of view, was performed in [10, 11, 13]. In [11], the authors claim that under condition (3) the secret key recovery of the proposed encryption scheme in the chosen plaintext attacking (CPA) scenario is as hard as solving the LPN problem with the noise level $1/2 \cdot (1 - (1 - 2p)^{m-l/2})$. Note that in the proof of this result an ad hoc assumption about the matrix $G_2G_1$ is used; but, this assumption is not mentioned in the main part of the paper (see Proof of Theorem 2 in [11]).

In [10], the authors show that under conditions (1), (2), (4) the recovery of secret key in CPA scenario is reduced to the solving a system of linear Boolean equations corrupted by noise, where the noise level is at least $p_w = 1/2 \cdot (1 - (1 - 2p)^{m-l})$ and $w$ depends somehow on the matrices $G_1, G_2$. In the same time, let us remark that condition $\text{rank}(G') \geq w + 1$ given in [10] (together with other conditions; see [10], p. 11) doesn’t guarantee that the noise level in the right-hand side of obtained linear equations is lower bounded by $p_w$ (this can be stated directly by analyzing an example given in [10], p. 15). Thus, the question about real computational security of ciphers proposed in [11, 12] is in fact open and requires further research.

**Contribution of this Paper.** We investigate the security of arbitrary ciphers specified by (1) and (4) in various attacking scenarios and show that it can be considerably less than it is claimed in [10 - 12]. In particular, we show that under condition (2) the complexity of the secret key recovery of the considered stream cipher in CPA scenario is upper bounded by the complexity of solving a system of linear Boolean equations corrupted by noise with the noise level $p_w$, where $w + 1$ coincide with the dual distance of a code, determined by the matrices $G_1$ and $G_2$. Note that the specified system of equations has very dedicated form and can be solved considerably faster than the LPN problem with the same parameters. (Let us emphasize that this is not holds for the ciphers specified by (1) and (3). However, also in this case the noise level in the right-hand side of the obtained system of linear equations can be considerably less than the value $1/2 \cdot (1 - (1 - 2p)^{m-l/2})$ reported in [11]).

In contrast to the approach for security evaluation used in [10, 11], our technique is significantly simpler and allows us to find out the code-theoretic sense of parameters that determine the security of the considered ciphers. It follows from our results that to construct reasonably secure randomized encryption schemes, the matrices $G_1$ and $G_2$ should be very carefully selected, what seems a non-trivial problem. In concluding part of the paper we propose another possible solution (based
on nonlinear random coding) for design of randomized stream cipher with enhanced security.

2. Preliminaries

In what follows, standard concepts and terminology from coding theory are used (see [4, 7] for more details). For a linear code $C \subseteq V_n$ the dual code, $C^\perp$, and the dual distance, $d(C^\perp)$, of $C$ are defined as follows:

$$C^\perp = \{ y \in V_n \mid \forall x \in C : xy^T = 0 \},$$
$$d(C^\perp) = \min \{ wt(x) : x \in C^\perp \setminus \{0\} \},$$

where $wt(x)$ is the Hamming weight of a vector $x \in V_n$.

Let's consider an arbitrary cipher specified by (1), where matrices $G_1$ and $G_2$ are defined by (4). As above, let's denote by $C_1$ the linear code generated by the rows of the matrix $G_1$.

Set $C_0 = \{ (0, u)G_2G_1 : u \in V_{m-1} \}$. It is clear that $C_0$ is an $[n, m-1]$-sub-code of the code $C_1$. We denote by $d_0^\perp$ and $d_1^\perp$ the dual distances of the codes $C_0$ and $C_1$, respectively. Note that the relation $C_0 \subseteq C_1$ implies the inequality

$$d_0^\perp \leq d_1^\perp. \quad (6)$$

Finally, for any $w = 0, 1, \ldots$ let's denote $p_w = 1/2 \cdot (1 - (1 - 2p)^w)$.

3. Main Results

Ciphertext-Only Attacks. Let us consider the system of equations (1) and suppose that adversary can access only the ciphertext $z_0, z_1, \ldots, z_t$. First of all, observe that, in order to recover plaintext symbols, the adversary is not required to have full information about the secret key.

**Statement 1.** Let $H$ be an arbitrary parity-check matrix of the code $C_0$; then for any $i = 0, 1, \ldots$ and $k \in K$ the adversary can recover (in real time) the vector $s_i$ from the known values $z_i$ and $\phi_i(k) = f_i(k)H^T$.

**Proof.** Let $a \in V_n$ be an arbitrary vector such that $\phi(k) = aH^T$. Then $g = a \oplus f_i(k) \in C_0$, and by (1), we have $z_i \oplus a = (s, u)G_2G_1 \oplus g \oplus v_i$, where the vector $(s, u)G_2G_1 \oplus g$ is a codeword in $C_1$. Hence, the adversary can recover this codeword as well as the vector $v_i$ by applying efficient decoding algorithm for $C_1$ to corrupted codeword $z_i \oplus a$.

Now, knowing $v_i$, the adversary can find the vector $(z_i \oplus a \oplus v_i)H^T = (s, u)G_2G_1H^T \oplus gH^T = (s, u)G_2G_1H^T$.

Let's denote by $G'_1$ and $G''_1$ submatrices contained in the first $m-1$ and in the last $l$ rows of the matrix $G_1$, respectively. Using (4), we get

$$(s, u)G_2G_1 = (u, s_i \oplus uB)G'_1 = uG'_1 \oplus (s_i \oplus uB)G''_1.$$  

Since $H$ is a parity-check matrix of the code $C_0 = \{ uG'_1 \oplus uB : u \in V_{m-1} \}$, we have $G'_1H^T = BG''_1H^T$. Thus

$$G'_1H^T = sG''_1H^T.$$  

So, the adversary can find $s_i$ from the known vector $(s, u)G_2G_1H^T$ by solving the system of linear equations $xG''_1H^T = sG''_1H^T$ with respect to the unknown $x \in V_t$.

Let us remark that this system has a unique solution (equal to $s_i$). Indeed, in the converse case there exists a non-zero vector $x \in V_t$ such that $xG''_1H^T = 0$. But then $xG'_1 \in C_0$, and, hence, there exists $u \in V_{m-1}$ such that $xG''_1 = uG'_1 \oplus uB$. Therefore $u = 0$, $uB \perp x = 0$ since rows of the matrix $G_i$ are linearly independent (see (4)). Thus, $x = 0$ that contradicts the above assumption.

As a result, we obtain the following algorithm for the recovery of $s_i$ from the known values $z_i$ and $\phi_i(k) = f_i(k)H^T$.

1. Find (by Gaussian elimination, for example) an arbitrary vector $a \in V_n$ such that $\phi(k) = aH^T$.
2. Recover the vector $v_i$ by applying efficient decoding algorithm for the code $C_1$ to corrupted codeword $z_i \oplus a$.
3. Recover $s_i$ as a unique solution $x \in V_t$ of the system of linear equations $xG''_1H^T = (z_i \oplus a \oplus v_i)H^T$.

The statement is proved.

Now, let us show that key recovery in the ciphertext-only attacking scenario can be reduced to solving a system of linear Boolean equations corrupted by noise with the noise level equal to $p_{d_{i-1}}$.

**Statement 2.** Under condition (1) the complexity of recovering the secret key in the ciphertext-only attacking scenario is upper bounded by the complexity of solving the following system of linear equations corrupted by noise:

$$z_ih^T = f_i(k)h^T \oplus \xi_i, \quad i = 0, 1, \ldots, t,$$

where $h \in C_1^\perp$ is an arbitrary codeword of weight $d_1^\perp$, $\xi_0, \xi_2, \ldots, \xi_t$ are independent random variables with the distribution law $\mathcal{B}(p_{d_{i-1}})$ for $i = 0, 1, \ldots, t$.  

330
Let \( h \in C_1 \) such that \((s, u) G_s G_h h^T = 0 \) for any \( s \in V_r, u \in V_{m-1} \). Thus, by (1), \( z_i h^T = f_i(k) h^T \oplus v_i h^T \). Since the coordinates of random vector \( v_i \) are independent and take values 0 and 1 with probabilities 1 - \( p \) and \( p \), respectively, we have for any \( i \)
\[
P(v_i h^T = 1) = 1 - P(v_i h^T = 1) = p \text{wt}(v_i) \tag{8}
\]
(see Lemma 9.49 in [4], for example). This completes the proof.

Note that in some cases, the secret key \( k \) can be uniquely recovered from the system (7) in time substantially smaller than the complexity of solving the LPN problem with the same number of unknowns and noise level defined by (8). For example, for the functions \( f_i \) of the form (2) the complexity of solving the system (7) depends essentially on algebraic properties of the sequence \( S' h^T, i = 0, 1, ..., t \). In particular, when a large collection of low-weight parity-check equations for this sequence is available, the specified system of equations can be efficiently solved by applying well-known algorithms used in fast correlation attacks (see [5], for example).

**Chosen-Plaintext / Chosen-IV Attacks.** Now, let us consider the attack described in [10, 11], where it is supposed that the adversary can encrypt the same message \( s_i = 0 \) with an (unknown) key getting the messages \( z_i \) of the form (1), \( i = 0, 1, ..., t \). It is clear that the considerations stated above for the ciphertext-only attacking scenario are applicable in this case as well, with the only difference that instead of the code \( C_1 \) its subcode \( C_0 \) should be considered. In particular, the following statement holds.

**Statement 3.** Under conditions (1), (2) the complexity of recovering the secret key in CPA scenario is upper bounded by the complexity of solving the following system of linear equations corrupted by noise:
\[
z_i h^T = k(S^i h^T) \oplus \xi_i, i = 0, 1, ..., t, \tag{9}
\]
where \( h \in C_0^1 \) is an arbitrary codeword of weight \( d_0^1 \), \( \xi_0, \xi_2, ..., \xi_t \) are independent random variables with the distribution law
\[
P(\xi = 1) = 1 - P(\xi = 0) = p_{d_0^{1-1}}, i = 0, 1, ..., t.
\]

Let us remark that in [10], in order to recover the secret key in CPA scenario a system of linear equations corrupted by noise is formed as well. This system differs from (9) and has a more complicated form. Moreover, the noise level in the right-hand side of this system is not less (but, can be greater) than \( p_{d_0^{1-1}} \).

In the case when the adversary has access to the encryption device and can choose (on his own) public parameters (for example, initialization vectors) determining the functions \( f_i \), he can mount a more powerful attack by encrypting (for some fixed \( i \)) the same message \( s_i = 0 \) under the same IV. Note that such multiple encryptions don’t give additional information about the key if an ordinary (non-randomized) cipher is used. But, for the cipher specified by (1) the adversary can derive the following equations:
\[
z^{(j)} = (u^{(j)}, v^{(j)}) G_2 G_1 \oplus f_i(k) + v^{(j)}, j = 0, 1, ..., \tag{10}
\]
where the unknown value \( f_i(k) \) is fixed, and \( u^{(0)}, v^{(0)}, u^{(1)}, v^{(1)}, ... \) are independent random vectors distributed as follows:
\[
P(u^{(j)} = u) = 2^{-j(m - i)}, P(v^{(j)} = v) = p^{\text{wt}(v)}(1 - p)^{n - \text{wt}(v)},
\]
\( u \in V_{m-i}, v \in V_n \).

Using standard technique it is not hard to prove the following statement.

**Statement 4.** Let \( H \) be an arbitrary parity-check matrix of the code \( C_o, d(H) = \max_{1 \leq i < n} \text{wt}(H_i) \), where \( H \), is the \( r \)-th row of the matrix \( H \). Then for any \( i = 0, 1, ..., k \in K \), and \( \delta \in (0,1) \) the adversary can recover the value \( f_i(k) = f_i(k) H^T \) with probability at least \( 1 - \delta \) in \( O(n \log t) \) bit operations from \( t = \left \lfloor \frac{1}{2} \cdot (1 - 2p)^{-2d(H)} \ln(\delta^{-1}(n - m + 1)) \right \rfloor \) arbitrary equations of the system (10).

**Proof.** It follows from (10) that for any \( r = 1, 2, ..., n - m + 1 \) the following equalities hold:
\[
z^{(j)} H_r^T = f_i(k) H_r^T \oplus \xi_{j,r}, j = 0, 1, ..., \tag{11}
\]
where \( \xi_{j,r} \) are independent random variables distributed as follows:
\[
P(\xi_{j,r} = 1) = 1 - P(\xi_{j,r} = 0) = 1/2 \cdot (1 - 2p)^{\text{wt}(H_r)} \tag{12}, j = 0, 1, ... .
\]

Suppose that to recover the value \( f_i(k) H_r^T \) the majority rule is used, i.e., \( f_i(k) H_r^T \) is set in 0 if
\[
\sum_{j=1}^{n} z^{(j)} H_r^T < \frac{t}{2}.
\]
Then using the Chernoff bound we can estimate the error probability as follows:
\[
P \left( \sum_{j=1}^{n} z^{(j)} \geq \frac{t}{2} \right) = P \left( 1 - \sum_{j=1}^{n} z^{(j)} \cdot (1 - 2p)^{\text{wt}(H_r)} \right) \leq \exp(-2(1 - 2p)^{\text{wt}(H_r)}) \leq \exp(-2(1 - 2p)^{2d(H)}).
\]

331
Thus, the probability of the event that all values \( f_i(k)H_i^T \), \( r=1, 2, ..., n-m+1 \), are correct recovered is lower bounded by

\[
1-(n-m+1)\exp[-2r(1-2p)^{2d(H)}] \geq 1-\delta,
\]

where the last inequality follows from the definition of \( t \). Finally, it is clear that the bit time complexity of recovering all values \( f_i(k)H_i^T \), \( r=1, 2, ..., n-m+1 \), with the majority rule is upper bounded by \( O(nt\log t) \). This completes the proof.

Note that chosen IV attacks are not considered in [9, 10, 12], but they should be taken into account in security analysis of randomized encryption schemes based on real keystream generators used in ordinary stream ciphers.

4. Conclusion. The computational security of randomized stream ciphers specified by (1) significantly depends on the choice of matrices \( G_1 \), \( G_2 \), and functions \( f_i \), which are determined by the employed keystream generator, and can be much less than it is claimed in [10 – 12]. In particular, some of specified ciphers are vulnerable even to ciphertext-only attacks.

The influence of the keystream generator is demonstrated through the fact that systems of linear equations with corruptions formed to recover the key can have very dedicated form and can be solved considerably faster than the LPN problem with the same number of unknowns and noise level. The last parameter depends on the dual distance of the code \( C_2 \), whose appropriate choice (for a fixed code \( C_1 \)), taking into account (6), seems a non-trivial problem. (Emphasize that the design criteria for the matrix \( G_2 \) formulated in [10], pp. 11 and 15, do not guarantee the claimed level of security).

From our point of view, to increase the security of the considered stream ciphers it is desirable to refuse from error-correction coding at all and use an encryption scheme of the following form:

\[
z_i = (u_i, s_i \oplus \phi(u_i))P \ast f_i(k), \quad i = 0, 1, ..., (11)
\]

where \( z_i, u_i, s_i, f_i(k) \) have the same sense as above, \( n = m \), \( P \) is a permutation matrix (for example, defined by a rotation by certain number of bits), \( \ast \) is a commutative group operation on the set \( V_m \), and \( \phi: V_{m-1} \to V_1 \) is a mapping “with good cryptographic properties” such as those used in modern block ciphers. For example, we can set \( a \ast b = (a+b) \mod 2^m \), where arbitrary vectors \( a, b \in V_m \) are identified with the corresponded numbers in the set \( \{0, 1, ..., 2^m-1\} \), \( m = 2^l \), and \( \phi(x) = x^{2^{l-2}} \).

Note that in [2, 3] a similar approach for design of randomized block ciphers with provable security against some known cryptographic attacks was proposed. Another possible approach is to use a keyless hash function (such as Keccak) as the function \( \phi \). Taking into account the fact that practically secure hash function simulates a random mapping (in our case from \( V_{m-1} \) to \( V_1 \)) sufficiently well, the last variant looks more preferable with regard to providing adequate security of the randomized cipher. The computational security of the stream ciphers specified by (11) is a subject of future research.

REFERENCES


криптоаналізу на основі методики криптостійкості широкого класу рандомізованих поточних шифрів може бути значно менше, ніж у випадку слідовального шифрування, і, відповідно, специфічного випадкового кодування. Показано, що стійкість уточнених кодувальних параметрів, визначених вище, може збільшитись зі збільшенням розміру парадигми шифрування.

Ключові слова: симетрична криптографія, рандомізоване шифровання, поточний шифр, слідова криптографія.

ПРО ОБЧИСЛЮВАЛЬНУ СТІЙКОСТЬ РАНДОМІЗОВАНЬ ФОТОЧОВ НИ ПОТОЧНИХ ШИФРІВ, ЗАПРОПОЗОВАНИХ МІХАСЛАЕВИЧЕМ ТА ІМАІ

В даній статті проводиться аналіз вичислювальної стійкості широкого класу рандомізованих поточних шифрів, постурованих на основі обчислювального процесу шифрування, що включає в себе спеціальні випадкові рандомізовані параметри. Показано, що стійкість таких шифрів може бути значно меншою, ніж у випадку вичислювальних шифрів, з урахуванням наявності спеціальних випадкових кодувань. Показано, що
стійкість зазначених шифрів може бути значно менше, ніж стверджують їх розробники. На відміну від підходу до аналізу стійкості, що використовується у попередніх роботах, запропоновано більш прості аналітичні методи, які дозволяють з'ясувати теоретико-кодовий сенс параметрів, що визначають обчислювальну стійкість цих шифрів. Запропоновано один із можливих альтернативних способів (на основі неелінійного випадкового кодування) побудови рандомізованих потокових шифрів із підвищеною стійкістю.

Ключові слова: симетрична криптографія, рандомізоване шифрування, потоковий шифр, випадкове кодування, відвідний канал, задача LPN, кореляційна атака.

Олексійчук Антон Миколайович, доктор технічних наук, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».

Алексейчук Антон Николаевич, доктор технічних наук, професор Інститута спеціальної связи и защиты информации НТУУ «КПІ».

Гришаков Сергій Володимирович, здобувач Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».

Гришаков Сергей Владимирович, соискатель Института специальной связи и защиты информации НТУУ «КПИ».

УДК 004.056.2:004.421.5

МЕТОД ФОРМИРОВАНИЯ ИМИТОВСТАВКИ НА ОСНОВЕ ПЕРЕСТАНОВОК

Эмиль Фауре, Валерий Швыдкий, Валентина Щерба

Для построения защищенных телекоммуникационных систем актуальной является задача контроля целостности передаваемых сообщений, который обеспечивается за счет использования процедуры имитозащиты данных. С учетом роста производительности вычислительных средств, а также совершенствования методов взлома систем защиты информации, в том числе защиты от навязывания ложных данных, возрастает требования к стойкости методов и средств имитозащиты. В работе разработана и представлена структурная схема устройства формирования случайной последовательности перестановок. На основе принципов построения данного устройства предложен метод формирования имитовставки и устройство, его реализующее. Сущность метода заключается в том, что в качестве имитовставки используется выбранная в некотором порядке часть символов перестановки большой размерности. Указанная перестановка формируется из последовательности символов сообщений, преобразованных в факториальную систему счисления. Скрытая закон формирования имитовставки используется сменяемым ключом преобразования. Определена стойкость перестановки и сформированной из нее имитовставки при попытке взлома ключа методом "грубой силы".

Ключевые слова: генератор перестановок, имитозащита, имитовставка, факториальная система счисления, преобразование факториального числа в перестановку, ключ преобразования.

Введение. Непрерывное совершенствование средств вычислительной техники, их эффективное применение для взлома систем защиты информации приводит к непрерывному процессу совершенствования методов и средств защиты, включающих средства и методы имитозащиты [2]. Естественным ответом на непрерывный рост производительности ЭВМ, используемых для взлома систем защиты информации, является требование столь же быстрого роста крипто- и имитостойкости систем защиты. Это обстоятельство обуславливает актуальность разработки новых методов и средств имитозащиты данных с повышенной стойкостью.

Выделение нерешенных задач. Несмотря на несомненные успехи в области разработки технологий повышения стойкости имитозащиты, любые работы, проводимые в этом направлении, представляют значительный интерес. В частности, представляют интерес работы, связанные с разработкой и исследованием новых методов и средств синтеза (случайных) последовательностей перестановок, упрощения алгоритмов их формирования (уменьшение числа и сложности операций, уменьшение объема требуемой памяти и т.п.), в том числе на основе использования факториальной системы счисления [1, 3, 4]. Использование факториальной системы счисления предусматривает представление каж-