Math-Net.Ru

Общероссийский математический портал

S. V. Smyshlyaev, Об инвариантности свойства совершенной сбалансированности относительно выбора точек съема, *Матем. вopr. криптогр.*, 2014, том 5, выпуск 2, 127–135

DOI: <https://doi.org/10.4213/mvk125>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.197.217.227

26 апреля 2023 г., 14:34:53

On the invariance of perfect balancedness property under the choice of tapping sequence

S. V. Smyshlyaev¹

LLC "CRYPTO-PRO", Moscow

Received 25.09.2013

The property of perfect balancedness of k -valued functions is of primary importance for cryptographic properties of stream ciphers constructed with such functions. The problem of description of the set of perfectly balanced k -valued functions for which the property of perfect balancedness is preserved for any choice of tapping sequence is considered. For the case of 2-valued (Boolean) functions this problem was raised in 1996 by Golić and later addressed and fully solved in 2009 by the author. Recently we obtained some results for the case of k -valued functions. A classification of the known results on this subject (both obtained earlier and new) is provided, open problems and questions are formulated.

Keywords: cryptographic properties of k -valued functions, perfect balancedness, functions without restricts, Golić conjecture.

**Об инвариантности свойства совершенной сбалансированности
относительно выбора точек съема**

С. В. Смышляев

ООО «КРИПТО-ПРО», Москва

Аннотация. Свойство совершенной сбалансированности k -значных функций имеет большое значение для криптографических свойств поточных шифраторов, использующих такие функции. Рассматривается задача описания множества совершенно сбалансированных k -значных функций, остающихся сбалансированными при любом выборе точек съема. Для 2-значных (булевых) функций эта задача была поставлена в 1996 Голичем и полностью решена в 2009 году автором. Недавно нами получены некоторые результаты для k -значных функций. Приводится классификация известных результатов на эту тему (как полученных ранее, так и новых), формулируются нерешенные задачи и вопросы.

Ключевые слова: криптографические свойства k -значных функций, совершенная сбалансированность, функции без ограничений, гипотеза Голича.

¹The work was supported by RFBR (Grant No. 12-01-00680-a).

1 Preliminaries

For each $n \geq 1$, $k \geq 2$ denote by E_k the set $\{0, 1, \dots, k-1\}$, denote by $P_k^{(n)}$ the set of all k -valued functions in n variables: $\{f: E_k^n \rightarrow E_k\}$; $P_k = \bigcup_{n=0}^{\infty} P_k^{(n)}$.

For each $n \geq 1$, $k \geq 2$ denote by $\widetilde{P}_k^{(n)}$ the set of all functions in $P_k^{(n)}$ depending on all variables essentially.

Definition 1.1. A function $f \in P_k^{(n)}$ is permutive in $x_i, i = 1, 2, \dots, n$, if for any $a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in E_k$ the subfunction

$$f_{a_1, a_2, \dots, a_{i-1}, a_{i+1}, \dots, a_n}^{1, 2, \dots, i-1, i+1, \dots, n}(x_i) \equiv f(a_1, a_2, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$$

is a permutation.

For each integer $l \geq 1$ and each function $f \in P_k^{(n)}$ we will also consider the following mapping: $f_l: E_k^{l+n-1} \rightarrow E_k^l$, $f_l(x_1, x_2, \dots, x_{l+n-1}) = (f(x_1, \dots, x_n), \dots, f(x_l, \dots, x_{l+n-1}))$.

The following definition is a natural generalization of the definition of perfect balancedness of a Boolean function proposed by Sumarokov [6].

Definition 1.2. A function $f \in P_k^{(n)}$ is said to be perfectly balanced ($f \in \mathcal{PB}_k^{(n)}$) if $|f_l^{-1}(\mathbf{y})| = k^{n-1}$ for any integer $l \geq 1$ and for any $\mathbf{y} \in E_k^l$.

Definition 1.3. A function $f \in P_k^{(n)}$ has a right barrier of length b , $b \geq 1$, if the relation

$$f_b(x_1, x_2, \dots, x_{n-1}, x'_n, \dots, x'_{b+n-1}) = f_b(x_1, x_2, \dots, x_{n-1}, x''_n, \dots, x''_{b+n-1})$$

implies the equality $x'_n = x''_n$.

In the same way as in the case $k = 2$ ([3]) for arbitrary integer $k \geq 2$ it may be proven that existence of a barrier implies perfect balancedness in P_k .

Statement 1.4 ([5]). *If a function $f \in P_k^{(n)}$ has a barrier, then it is perfectly balanced.*

Statement 1.5 ([5]). *A function $f \in P_k^{(n)}$ has a right barrier of length 1 iff it is permutive in the last variable.*

Statement 1.6 ([5]). *If a function $f \in P_k^{(n)}$ has a right barrier of length b , then for any integer $n' \geq \max\{0, b - n + 1\}$ and any function $f' \in P_k^{(n'+n-b)}$ the function $g(x_1, \dots, x_{n'+n}) \equiv f'(x_1, \dots, x_{n'+n-b}) + f(x_{n'+1}, \dots, x_{n'+n})$ is perfectly balanced.*

2 Golić property

Definition 2.1. For any integer $n \geq 1$, function $f \in P_k^{(n)}$ and tuple $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n)$, where $\gamma_i \geq 1$ for $i = 1, 2, \dots, n$, $\gamma_i \neq \gamma_j$ for $i \neq j$, by f^γ we will denote a k -valued function $f(x_{\gamma_1}, x_{\gamma_2}, \dots, x_{\gamma_n})$.

We will say that a function $f \in \mathcal{PB}_k^{(n)}$ preserves perfect balancedness under the choice of generalized tapping sequence if for any $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n)$, where $\gamma_i \neq \gamma_j$ when $i \neq j$, the function f^γ is perfectly balanced.

Obviously, any function of algebraic degree 1 is perfectly balanced and preserves perfect balancedness under the choice of generalized tapping sequence.

Jovan Golić [1] in 1996 had considered (in the case $k = 2$) a property, important for synthesis of filter generators, that is stronger than perfect balancedness but weaker than perfect balancedness with invariance under the choice of generalized tapping sequence.

Definition 2.2. A function $f \in \mathcal{PB}_k^{(n)}$ is strongly perfectly balanced if inclusion of any number of fictive variables preserves perfect balancedness.

In fact, a function is strongly perfectly balanced if and only if it is perfectly balanced and preserves perfect balancedness property under the choice of tapping sequence (not generalized tapping sequence: the relation $\gamma(i+1) > \gamma(i)$ must hold for any $i = 1, 2, \dots, n-1$).

It is easy to show that permutiveness of a function either in the first or in the last essential variable is sufficient for strong perfect balancedness. In [1] Golić conjectured that it is also necessary for strong perfect balancedness — this conjecture later, beginning with the paper of Dichtl [2], was named Golić Conjecture.

Conjecture 2.3 ([1]). *For $k = 2$ strong perfect balancedness of a k -valued function implies its permutiveness (i. e. linearity in the case of $k = 2$) either in the first or in the last essential variable.*

A statement that indirectly confirmed correctness of Golić Conjecture was first obtained in 2008 in [3]. In the paper [4] in 2012 the Golić Conjecture was fully proven.

Theorem 2.4 ([3, 4]). *A function $f \in P_2$ is strongly perfect balanced iff it is permutive either in the first or in the last essential variable.*

The following corollary is easily proven.

Corollary 2.5. *A function $f \in P_2$ is perfectly balanced and preserves perfect balancedness under the choice of generalized tapping sequence iff it is non-constant and permutive (linear) in any essential variable (i. e. $\deg(f) = 1$).*

Proof. It is completely evident that if a function f is permutive (linear) in any essential variable and it is not constant, then for any γ function f^γ is also linear in any essential variable and thus is linear in the first essential variable that induces that f^γ is perfectly balanced.

It is evident that for $k = 2$ and any $n \geq 2$ any function $f \in P_k^{(n)}$ that is not permutive in some essential variable is not permutive in at least two of them, x_i and x_j , $i < j$. Then it is sufficient to construct a tuple $\gamma' = (i, 1, 2, \dots, i-1, i+1, \dots, j-1, j+1, \dots, n-1, n, j)$ and see that $f^{\gamma'}$ is non-permutive in the first and in the last essential variables. Thus, using Theorem 2.4 it is possible to construct $\gamma'' = (t_1, t_2, \dots, t_n)$ such that $f^{\gamma''}$ is not perfectly balanced. Thus for

$$\gamma = (t_i, t_1, t_2, \dots, t_{i-1}, t_{i+1}, \dots, t_{j-1}, t_{j+1}, \dots, t_{n-1}, t_n, t_j)$$

the function f^γ is not perfectly balanced. $\square$

Thus it is known that it is impossible (under alphabet $\{0, 1\}$): 1) to construct a filter with a filtering function that is nonlinear in the first and the last essential variable and preserves pure randomness of the input sequence for any choice of tapping sequence and 2) to construct a filter with a nonlinear filtering function, preserving pure randomness of the input sequence for any choice of generalized tapping sequence.

The interesting question is: is it possible to construct such filters for alphabet of larger cardinality, particularly, in the case of alphabet of cardinality of the power of 2, $k = 2^m$, $m \geq 2$, e. g. in the case of block-oriented filters with block length equal to m with Boolean mapping $E_2^{n-m} \rightarrow E_2^m$.

Let us formulate Golić Property (denoted by “Golić Condition” in [5]) and Strong Golić Property for the case of arbitrary $k \geq 2$.

Golić Property. Strong perfect balancedness in P_k is equivalent to permutiveness in either the first or the last essential variable.

Strong Golić Property. Perfect balancedness with invariance of perfect balancedness property under the choice of generalized tapping sequence is equivalent to permutiveness in every essential variable (assuming there is at least one essential variable).

It is proven that Golić Property and Strong Golić Property are correct in P_2 . Consider the following generalizations of Golić Conjecture, connecting correctness of Golić Property and Strong Golić Property in P_k with primality of k .

Conjecture 2.6. *Golić Property holds for P_k iff k is prime.*

Conjecture 2.7. *Strong Golić Property holds for P_k iff k is prime.*

If Golić Property holds for some k , then Strong Golić Property also holds for the same k , since if a function is not permutive in certain essential variable, then this variable may be set to be the last essential variable with corresponding generalized tapping sequence, and then correctness of Golić Property will guarantee existence of tapping sequence that will make the obtained function (that, in turn, may be obtained by applying some generalized tapping sequence to the initial function) to be not perfectly balanced.

3 Prime k

First we assume that k is prime.

Theorem 3.1 ([5]). *Let k be prime and let function $f \in P_k^{(n)}$ have right barrier of length 2. Then f does not depend on the last variable and is permutive in the last but one.*

Corollary 3.2 ([5]). *For any prime k Golić Property does not get broken on functions with barrier of length 2.*

Theorem 4.3 and Corollary 3.2 induce the following criterion.

Corollary 3.3 ([5]). *Golić Property does not get broken on functions with barrier of length 2 in P_k iff k is prime.*

Theorem 3.4 ([5]). *For $k \in \{2, 3, 5, 7\}$ all perfectly balanced functions in $P_k^{(2)}$ are permutative either in the first or in the last variable.*

Corollary 3.5 ([5]). *For $k \in \{2, 3, 5, 7\}$ Golić Property does not get broken on functions in $P_k^{(2)}$.*

Since for $P_k^{(2)}$ Golić Property is equivalent to Strong Golić Property, the following statement holds.

Corollary 3.6. *For $k \in \{2, 3, 5, 7\}$ Strong Golić Property does not get broken on functions in $P_k^{(2)}$.*

4 Composite k

Now assume that k is composite. Consider a representation $k = pq$, where $p, q \in \{2, 3, \dots, k-1\}$, p and q are not necessarily prime numbers.

Theorem 4.1 ([5]). *For any composite k there exists a function $f \in \mathcal{PB}_k^{(2)}$ that is essential in both variables and that is non-permutative in both of them.*

Corollary 4.2 ([5]). *If k is composite, then Golić Property does not hold in P_k .*

Theorem 4.3 ([5]). *For any composite k there exists a function $f \in P_k^{(2)}$ with right barrier of length 2, that is non-permutative in both variables and depends on both variables essentially.*

Theorem 4.4 ([5]). *For any composite k and any $n \geq 2$ there exists a strongly perfectly balanced function $f \in P_k^{(n)}$ that have n essential variables and is non-permutative both in the first and in the last variable.*

Corollary 4.5. *If k is composite, then Golić Property does not hold in $\widetilde{P}_k^{(n)}$ for any $n \geq 2$.*

Proof. Consider a function $g \in P_k^{(2)}$ with right barrier of length 2, that is non-permutative in the last variable and depends on the last variable essentially. Existence of such functions is proven in Theorem 4.3. If $n = 2$, the statement follows immediately. Let $n \geq 3$, $k = pq$, $p > 1$, $q > 1$. Consider a function $f(x_1, x_2, \dots, x_n) = (x_1 \bmod p) + (x_2 \bmod p) + \dots + (x_{n-2} \bmod p) + g(x_{n-1}, x_n) \bmod k$. Obviously, f depends essentially on all variables and is non-permutative in each of them. Since g has right barrier of length 2, thus f also has

right barrier of length 2 and thus $f \in \mathcal{PB}_k^{(n)}$. For any tuple $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n)$, where $\gamma_i > \gamma_j$ for $i > j$, the function f^γ may be represented as

$$f^\gamma(x_1, x_2, \dots, x_{\gamma_n}) = h(x_1, x_2, \dots, x_{\gamma_{n-1}-1}) + g(x_{\gamma_{n-1}}, x_{\gamma_n}),$$

where $h \in \mathcal{P}_k^{(\gamma_{n-1}-1)}$. Since $g(x_1, x_2)$ has right barrier of length 2, thus $g'(x_1, x_2, \dots, x_{\gamma_n-\gamma_{n-1}+1}) \equiv g(x_1, x_{\gamma_n-\gamma_{n-1}+1})$ has right barrier of length $\gamma_n - \gamma_{n-1} + 1$ and this f^γ has right barrier of length $\gamma_n - \gamma_{n-1} + 1$ and thus $f^\gamma \in \mathcal{PB}_k^{(\gamma_n)}$.

Thus for any $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_n)$, where $\gamma_i > \gamma_j$ for $i > j$, the function f^γ is perfectly balanced, that means that f is strongly perfectly balanced. Since f is in $\tilde{\mathcal{P}}_k^{(n)}$ and is not permutive in any variable, Golíc Property does not hold in $\tilde{\mathcal{P}}_k^{(n)}$. $\square$

Now consider the question on the existence for any $n \geq 2$ and any composite k of a function in $\tilde{\mathcal{P}}_k^{(n)}$ which is perfectly balanced with invariance of perfect balancedness property under the choice of generalized tapping sequence. I. e., does Strong Golíc Property hold in $\mathcal{P}_k$ for any composite k ? And in $\tilde{\mathcal{P}}_k^{(n)}$ for any $n \geq 2$ and any composite k ?

The answer for the first of these questions is positive and can be derived from Theorem 4.1.

Corollary 4.6. *If k is composite, then Strong Golíc Property does not hold in $\mathcal{P}_k$.*

Proof. For any composite k consider a function $f \in \mathcal{PB}_k^{(2)}$, that is essential in both variables and that is non-permutive in both of them. Existence of such a function is guaranteed by Theorem 4.1. For any tuple $\gamma = (\gamma_1, \gamma_2)$, where $\gamma_1 \neq \gamma_2$, $N = \max\{\gamma_1, \gamma_2\}$ consider a function $f^\gamma(x_1, \dots, x_N) \equiv f(x_{\gamma_1}, x_{\gamma_2})$. Obviously, this function is perfectly balanced iff the function f is. Thus $f^\gamma \in \mathcal{PB}_k^{(N)}$ for any γ , f is not permutive in any variable and depends on both variables essentially. $\square$

Moreover, it is possible to prove that Strong Golíc Property does not hold in $\tilde{\mathcal{P}}_k^{(3)}$.

Theorem 4.7. *If k is composite, then Strong Golíc Property does not hold in $\tilde{\mathcal{P}}_k^{(3)}$.*

Proof. Let $k = pq$, $p > 1$, $q > 1$. Consider the following function from $\mathcal{P}_k^{(3)}$:

$$g(x, y, z) = \left((x \bmod p) \cdot q + \left\lfloor \frac{y}{p} \right\rfloor + (z \bmod p) \cdot q \right) \bmod k.$$

It is obvious that this function depends essentially on all variables and is not permutive in any of them.

Consider a tuple $\gamma = (\gamma_1, \gamma_2, \gamma_3)$, where $\gamma_1 \neq \gamma_2$, $\gamma_1 \neq \gamma_3$, $\gamma_2 \neq \gamma_3$; $N = \max\{\gamma_1, \gamma_2, \gamma_3\}$. Then the function $g^\gamma(x_1, x_2, \dots, x_N)$ may have one of the following three forms (since $g(x, y, z) \equiv g(z, y, x)$):

$$1. \left(\left\lfloor \frac{x_{t_1}}{p} \right\rfloor + (x_{t_2} \bmod p) \cdot q + (x_{t_3} \bmod p) \cdot q \right) \bmod k;$$

$$2. \left((x_{t_1} \bmod p) \cdot q + \left\lfloor \frac{x_{t_2}}{p} \right\rfloor + (x_{t_3} \bmod p) \cdot q \right) \bmod k;$$

$$3. \left((x_{t_1} \bmod p) \cdot q + (x_{t_2} \bmod p) \cdot q + \left\lfloor \frac{x_{t_3}}{p} \right\rfloor \right) \bmod k;$$

where $t_1 < t_2 < t_3$, $\{t_1, t_2, t_3\} = \{\gamma_1, \gamma_2, \gamma_3\}$.

Prove that g^γ has left barrier of length t_2 in case 1, g^γ has right barrier of length $t_3 - t_2 + 1$ in case 3, g^γ has left barrier of length t_2 and right barrier of length $t_3 - t_2 + 1$ in case 2.

Obviously, to prove this it is sufficient to prove two facts:

$$1. f'(x_1, x_2, x_3) = \left((x_1 \bmod p) \cdot q + (x_2 \bmod p) \cdot q + \left\lfloor \frac{x_3}{p} \right\rfloor \right) \bmod k \text{ has right barrier of length 2;}$$

$$2. f''(x_1, x_2, x_3) = \left((x_1 \bmod p) \cdot q + \left\lfloor \frac{x_2}{p} \right\rfloor + (x_3 \bmod p) \cdot q \right) \bmod k \text{ has right barrier of length 2.}$$

To prove that f', f'' have right barriers of length 2, it is sufficient to prove that the following systems do not have any solutions:

$$\begin{cases} f'(x, u, y_1) = f'(x, u, z_1), \\ f'(u, y_1, y_2) = f'(u, z_1, z_2), \\ y_1 \neq z_1; \end{cases} \quad (1)$$

$$\begin{cases} f''(x, u, y_1) = f''(x, u, z_1), \\ f''(u, y_1, y_2) = f''(u, z_1, z_2), \\ y_1 \neq z_1. \end{cases} \quad (2)$$

It is easy to see that for the system (1) the following equivalences hold:

$$\begin{aligned} & \begin{cases} \left((x \bmod p) \cdot q + (u \bmod p) \cdot q + \left\lfloor \frac{y_1}{p} \right\rfloor \right) \bmod k = \\ = \left((x \bmod p) \cdot q + (u \bmod p) \cdot q + \left\lfloor \frac{z_1}{p} \right\rfloor \right) \bmod k, \\ \left((u \bmod p) \cdot q + (y_1 \bmod p) \cdot q + \left\lfloor \frac{y_2}{p} \right\rfloor \right) \bmod k = \\ = \left((u \bmod p) \cdot q + (z_1 \bmod p) \cdot q + \left\lfloor \frac{z_2}{p} \right\rfloor \right) \bmod k, \\ y_1 \neq z_1, \end{cases} \iff \\ & \iff \begin{cases} \left\lfloor \frac{y_1}{p} \right\rfloor \bmod k = \left\lfloor \frac{z_1}{p} \right\rfloor \bmod k, \\ (((y_1 - z_1) \bmod p) \cdot q) \bmod k = \left(\left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \right) \bmod k, \\ y_1 \neq z_1. \end{cases} \quad (3) \end{aligned}$$

The first relation of this system implies inequality $|y_1 - z_1| \leq p - 1$. Since $y_1 \neq z_1$, it follows that

$$(y_1 - z_1) \bmod p \geq 1. \quad (4)$$

Using (4) we obtain from (3) the following:

$$\begin{cases} \left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \bmod k \geq q, \\ \left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \bmod k \leq (p-1) \cdot q. \end{cases} \quad (5)$$

From the other hand, for any $z \in E_k$ relation $0 \leq \left\lfloor \frac{z}{p} \right\rfloor \leq q - 1$ holds, thus $\left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \bmod k = 0$ or $1 \leq \left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \bmod k \leq q - 1$ or $k - 1 \geq \left\lfloor \frac{z_2}{p} \right\rfloor - \left\lfloor \frac{y_2}{p} \right\rfloor \bmod k \geq k - (q - 1) = (p - 1) \cdot q + 1$ holds. Hence in any case conditions of the system (5) are not satisfied, thus the system (3) and the system (1) do not have solutions. Thus f' has right barrier of length 2.

Absence of solutions of the system (2) is proven absolutely analogously.

Thus function g^γ has left barrier of length t_2 or right barrier of length $t_3 - t_2 + 1$ or both of them. Hence it is perfectly balanced.

Thus there exists a function in three essential variables that is not permutive in any of them and is perfectly balanced with invariance of perfect balancedness property under the choice of generalized tapping sequence.

Hence Strong Golić Property does not hold in $\tilde{P}_k^{(3)}$ for any composite k . □

Example 4.8. For $k = 4$ one can obtain the following function in $\tilde{P}_k^{(3)}$ that is not permutive in any essential variable and is perfectly balanced with invariance of perfect balancedness property under the choice of generalized tapping sequence (vector of values for lexicographically ordered inputs).

$$(0, 2, 0, 2, 0, 2, 0, 2, 1, 3, 1, 3, 1, 3, 1, 3, 2, 0, 2, 0, 2, 0, 2, 0, 3, 1, 3, 1, 3, 1, 3, 1, \\ 2, 0, 2, 0, 2, 0, 2, 0, 2, 1, 3, 1, 3, 1, 3, 1, 3, 2, 0, 2, 0, 2, 0, 2, 0, 3, 1, 3, 1, 3, 1, 3, 1).$$

5 Conclusion

Thus it is proven that Golić Property:

1. gets broken on functions in $P_k^{(2)}$ for any composite k (Corollary 4.2) and does not get broken on functions in $P_k^{(2)}$ when k is equal to one of the four least prime numbers (Corollary 3.5);

2. gets broken on functions in P_k with barrier of length 2 for any composite k (Theorem 4.3) and does not get broken on functions in P_k with barrier of length 2 for any prime k (Corollary 3.3);
3. gets broken on functions in $\tilde{P}_k^{(n)}$ (k -valued functions that depend on all n variables) for any composite k (Corollary 4.5);
4. does not get broken in P_2 ($[4]$).

It is proven that Strong Golić Property:

1. gets broken on functions in $P_k^{(2)}$ for any composite k (Corollary 4.6) and does not get broken on functions in $P_k^{(2)}$ when k is equal to one of the four least prime numbers (Corollary 3.6);
2. gets broken on functions in $\tilde{P}_k^{(3)}$ for any composite k (Theorem 4.7);
3. does not get broken in P_2 ($[4]$).

Thus, Conjecture 2.6 and Conjecture 2.7 are completely proven in the part of necessity of k to be prime for correctness of Golić Property in P_k . Moreover, a number of statements is proven that indirectly confirm correctness of Conjecture 2.6 in the part of sufficiency.

References

- [1] *Golić J. Dj.* On the security of nonlinear filter generators // LNCS. — 1996. — V. 1039. — P. 173–188.
- [2] *Dichtl M.* On nonlinear filter generators // LNCS. — 1997. — V. 1267. — P. 103–106.
- [3] *Logachev O. A., Salnikov A. A., Smyshlyaev S. V., Yashchenko V. V.* Perfectly balanced functions in symbolic dynamics // Proc. NATO ARW, Veliko Tarnovo, Bulgaria, 6–9 October 2008. — 2009. — P. 222–233.
- [4] *Smyshlyaev S. V.* Perfectly balanced Boolean functions and Golić Conjecture // J. Cryptology. — 2012. — V. 25. No 3. — P. 464–483.
- [5] *Smyshlyaev S. V.* Perfectly balanced k -valued functions and Golić Condition // Discrete Mathematics and Applications. — 2013. — V. 23. No 1. — P. 75–89.
- [6] *Sumarov S. N.* Functions of defect zero and invertibility of one class of finite-memory encoders // Obozrenie prom. i prikl. mat. — 1994. — V. 1. No 1. — P. 33–55. (in Russian).