The Pseudorandom Key Sequences Generator Based on IV-Sets of Quaternary Bent-Sequences

Elena Bakunina [a] and Artem Sokolov [b]

[a] National University "Odessa Law Academy", Fontanska road, 23, Odessa, 65000, Ukraine
[b] Odessa Polytechnic National University, Shevchenko Avenue, 1, Odessa, 65044, Ukraine

Abstract

The development of modern cryptography, steganography, and communication systems with noise-like signals often requires the use of non-binary generators of pseudorandom key sequences. The main requirements for such a cryptographic construct are the compliance of gamma generated by them with the criteria of NIST stochastic tests and the implementation of the concepts of diffusion and confusion with respect to the generated gamma and the cryptographic key. In this paper, we empirically confirm the prospects of combining the advantages of quaternary bent-sequences, which are characterized by the highest nonlinearity value, with the advantages of the linear feedback shift registers, which are characterized by a high stochastic quality of the generated sequences. We present the scheme of a pseudorandom key sequences generator based on binary linear feedback shift registers and the IV-sets of quaternary bent-sequences. It has been established that the presented scheme generates pseudorandom key sequences corresponding to all the NIST stochastic tests, while the maximum values of the nonlinearity of quaternary bent-sequences provide a high level of implementation of the concept of confusion. At the same time, construction of IV-sets of quaternary bent-sequences was found, which provides the best stochastic properties of the generated gamma. The developed generator is characterized by high values of the number of protection levels and the simplicity of the algorithmic implementation. Compared to combining two binary generators of pseudorandom key sequences based on dual sets of binary bent-sequences, 40% fewer linear feedback shift registers are required to ensure the operation of the developed generator. The practical application of the developed generator is justified in systems that require many-valued logic pseudorandom key sequences.

Keywords

Pseudorandom key sequences generator, bent-sequence, many-valued logic.

1. Introduction and statement of the problem

The Pseudorandom Key Sequences Generator (PRKSG) is a very important construct used in modern cryptographic applications as well as in other areas of science and technology: PRKSG is the basis for the functioning of modern stream encryption algorithms, organizing modern efficient modes for block encryption algorithms [1], defining the steganographic path in modern steganographic algorithms, functioning of modern radio communication systems based on Frequency-Hopping Spread Spectrum (FHSS) technology [2], etc.

Today, there are many different layouts for the PRKSG construction: the classical scheme based on Linear Feedback Shift Register (LFSR) with the use of nonlinear elements [3, 4], schemes based on the theory of dynamic chaos [5], cellular automata [6], etc. Regardless of the chosen scheme, the following basic requirements must be applied to PRKSG being developed today: they must be characterized by the high level of stochastic quality (the level of which is measured by the compliance with a generally accepted set of NIST stochastic tests [7]), the ability to generate pseudorandom key

CMIS-2022: The Fifth International Workshop on Computer Modeling and Intelligent Systems, Zaporizhzhia, Ukraine, May 12, 2022
EMAIL: elenabakunina72@gmail.com (E. Bakunina); radiosquid@gmail.com (A. Sokolov)
ORCID: 0000-0002-5700-7321 (E. Bakunina); 0000-0003-0283-7229 (A. Sokolov)

sequences based on a short cryptographic key (at the same time, the PRKSG must provide a high level of implementation of Shannon's concepts of diffusion and confusion [8] between the key element and the generated gamma), the simplicity of the algorithmic implementation, and the high performance of the PRKSG algorithm.

The classical LFSR-based PRKSG layout with a nonlinear element fully fulfills the mentioned requirements, in particular, its modification based on bent-sequences proposed in [9].

The development of the theory of quantum cryptography, as well as the recently proposed cryptographic algorithms based on many-valued logic functions [10], have led to the need to create PRKSG operating on a non-binary alphabet $\overline{A} = \{0,1,...,q-1\}, q \neq 2$. Thus, the scheme of the PRKSG based on LFSR and dual sets of bent-sequences was generalized to operate over the alphabet $\overline{A} = \{0,1,2\}$, which corresponds to the problems of quantum cryptography.

However, the vast majority of information today is stored, processed, and transmitted in binary form, which makes it especially relevant to consider the possibility of constructing PRKSG that would operate over the alphabets $\overline{A} = \{0,1,...,2^k - 1\}$, primarily over the quaternary alphabet $\overline{A} = \{0,1,2,3\}$. The use of the quaternary alphabet fundamentally makes it possible to simplify the PRKSG schemes by generating twice more gamma bits during one cycle, and also increases the possibility of implementing the principles of diffusion and confusion in the PRKSG [8]. The quaternary alphabet also provides a much greater variety of algebraic constructions that can be used to build high-quality PRKSG.

Steganography is another important application of quaternary PRKSG in view of the peculiarities of the choice of the steganographic path: the ability to select one of the three color components or skip a given pixel from the process of information embedding.

These facts substantiate the tasks of further research on the possibilities of improvement of the classical layout for constructing the PRKSG operating over the quaternary alphabet.

The *purpose* of this paper is to develop a quaternary PRKSG based on IV-sets of bent-sequences.

2. The theoretical foundations for the proposed PRKSG

The classic layout of the PRKSG implies the use of LFSR as the main component.

Definition 1 [11]. An LFSR is a shift register consisting of d memory cells, the value of the input element of which is determined by the value of the function constructed in accordance with the primitive irreducible over the Galois field $GF(2)$ polynomial of degree d.

It is known [10] that the use of LFSR makes it possible to achieve good diffusion, and also provides a sufficiently high stochastic quality of the generated pseudorandom key sequences, which will be shown below in Table 2 on the example of LFSR built on the basis of the primitive irreducible polynomial

$$f(x) = x^{83} + x^{46} + x^{45} + x + 1. \quad (1)$$

The disadvantages of LFSR include the fact that they generate pseudorandom key sequences in accordance with a fairly simple rule defined by a primitive irreducible polynomial.

This does not allow them to provide a sufficiently high level of nonlinearity of the relationship between the elements of the short key and the generated pseudorandom key sequence. In other words, these constructions do not provide a sufficient level of confusion. This circumstance leads to the possibility of launching attacks against such a generator, for example, using the Berlekamp-Massey algorithm.

One of the historical attempts to overcome this shortcoming is the Geffe Generator, which provides a significantly higher level of confusion compared to the direct application of the LFSR through the use of several interconnected LFSR units. However, this level of confusion is also insufficient due to the simplicity of the links between the pooled LFSR units.

In modern PRKSG, this drawback is eliminated by using a non-linear element in conjunction with LFSR, which is often represented by the Boolean function with a high level of nonlinearity. Thus, the block diagram of PRKSG in its classical layout is shown in Fig. 1.

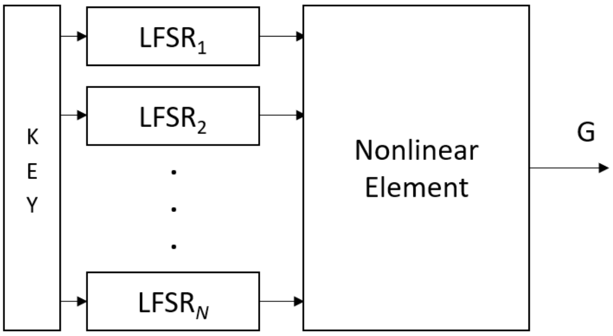

Fig. 1: Block diagram of PRKSG based on LFSR and nonlinear element

The ideal option for nonlinear element is to use such special algebraic constructions as bent-functions (whose truth tables are called as bent-sequences), which have the maximum level of nonlinearity, and, accordingly, provide the highest level of confusion implemented by PRKSG.

In accordance with the definition [9], a binary sequence $B=[b_0,b_1,...,b_i,...,b_{N-1}]$, where $b_i \in \{\pm 1\}$ are coefficients, of even length $N=2^{2m}$, $i=0,1,...,N-1$ is called a bent-sequence if it has uniform absolute values of its Walsh-Hadamard spectrum $W_B(\omega)$, which can be represented in matrix form

$$W_B(\omega)=BA,\ \omega=0,1,...,N-1, \tag{2}$$

where A is the Walsh-Hadamard matrix of order N.

The Walsh-Hadamard matrices are constructed in accordance with the Sylvester construction, which is specified using the following recurrent rule

$$A_{2^k}=\begin{bmatrix} A_{2^{k-1}} & A_{2^{k-1}} \\ A_{2^{k-1}} & -A_{2^{k-1}} \end{bmatrix},\ A_1=1. \tag{3}$$

Despite the successful layout of the block diagram shown in Fig. 1, the practical application of bent-sequences in it is extremely difficult due to bent-sequences imbalance, as a result of which the gamma generated by PRKSG is also unbalanced, and, therefore, does not meet the most basic criteria of stochastic quality.

Another undoubted disadvantage of using binary bent-sequences is their existence only for lengths $N=2^{2m}=4,16,64,256,...$, while binary bent-functions of an odd number of variables do not exist, which limits the scalability of PRKSG schemes.

In [9], for the binary case, a solution to this problem was proposed based on the use of dual sets of maximally nonlinear bent-functions.

This PRKSG scheme showed excellent characteristics both in terms of performance and in terms of the quality of the generated pseudorandom key sequences, which is confirmed by both a set of stochastic tests [12], as shown in [9], and a set of NIST stochastic tests [7]. The number of protection levels of this scheme reaches the value $\Upsilon \approx 2{,}67\cdot 10^{49} \approx 2^{165}$, which exceeds the number of protection levels of the AES-128 block symmetric cipher [13].

This scheme was also modified for the ternary case in [14] using LFSR based on primitive irreducible polynomials over the Galois field $GF(3)$, as well as triple sets of bent-sequences. Despite the absence of specific NIST tests for ternary pseudorandom sequences, the sequences generated by PRKSG [13] fully correspond to the set of tests [12], which suggests their high level of quality.

To construct a quaternary PRKSG, it is proposed to use the complete class of quaternary bent-sequences described in [15] and synthesized in [16]. Let us introduce the definition of the Vilenkin-Chrestenson transform that we will need, as well as the definition of the many-valued logic bent-sequence.

Definition 2 [16]. The coefficients of the Vilenkin-Chrestenson transform of a q-valued logic function is the vector obtained by multiplying its truth table T (represented in the exponential form) by the complex conjugate of the Vilenkin-Chrestenson matrix

$$\Omega_A=T\cdot\overline{V}_{16}. \tag{4}$$

while for the case of 4-functions the Vilenkin-Chrestenson matrix is constructed according to the following recurrent rule

$$V_{4^{k+1}}=\begin{bmatrix} V_k & V_k & V_k & V_k \\ V_k & V_k+1 & V_k+2 & V_k+3 \\ V_k & V_k+2 & V_k & V_k+2 \\ V_k & V_k+3 & V_k+2 & V_k+1 \end{bmatrix}, \tag{5}$$

where "+" is the operation of addition mod4, the matrices V are represented in symbolic form, i.e. the summation is performed with respect to the indices z_i, and

$$V_4=\begin{bmatrix} z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 \end{bmatrix}=\begin{bmatrix} e^{j0} & e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j\frac{\pi}{2}} & e^{j\pi} & e^{j\frac{3\pi}{2}} \\ e^{j0} & e^{j\pi} & e^{j0} & e^{j\pi} \\ e^{j0} & e^{j\frac{3\pi}{2}} & e^{j\pi} & e^{j\frac{\pi}{2}} \end{bmatrix}. \tag{6}$$

Definition 3 [16]. For the Vilenkin-Chrestenson matrix of order $N=q^k$, a bent-sequence $H=[h_0,h_1,...,h_i,...,h_{N-1}]$ is a sequence over the alphabet $h_i\in\left\{e^{j\frac{2\pi}{q}v}\right\}, v=0,1,...,q-1$ if it has a uniform absolute values of the Vilenkin-Chrestenson spectrum, which can be represented in matrix form

$$\left|\Omega_H(\omega)\right|=\left|H\cdot\overline{V}_N\right|=const,\ \omega=0,1,...,N-1, \tag{7}$$

where V_N is the Vilenkin-Chrestenson matrix of order N over the alphabet $h_i\in\left\{e^{j\frac{2\pi}{q}v}\right\}, v=0,1,...,q-1$.

Bent-sequences are very important mathematical objects for cryptographic constructions development, however, their main drawback, which limits their use in cryptography, in particular, in the problems of development of cryptographically secure PRKSG, is their imbalance, the inequality of the number of symbols $0,1,...,q-1$ contained in them, i.e. $K^0\neq K^1\neq...\neq K^{q-1}$. This drawback was solved in [9] and [14] by using dual sets and triple sets of bent-sequences respectively, while the definition of dual sets and triple sets was generalized in [16], resulting in the definition of a *q*-set of bent-sequences which was presented.

Definition 4 [16]. A set of *q* *q*-ary bent-sequences is called a *q*-set if the concatenation of their truth tables is balanced, i.e. it satisfies the relation $K^0=K^1=...=K^{q-1}$.

The research of the complete class of quaternary bent-sequences of length $N=16$ makes it possible to distinguish the following weight structures, which are presented in Table 1 in the following form $\{K^0,K^1,K^2,K^3\}$.

Table 1

Weight structures of quaternary bent-sequences of length $N=16$

Weight structure	J	Weight structure	J	Weight structure	J	Weight structure	J
{10,0,6,0}	192	{4,6,0,6}	2112	{8,2,4,2}	6336	{3,3,7,3}	10240
{0,10,0,6}	192	{6,4,6,0}	2112	{2,8,2,4}	6336	{3,3,3,7}	10240
{6,0,10,0}	192	{1,5,5,5}	6144	{4,2,8,2}	6336	{2,4,6,4}	25152
{0,6,0,10}	192	{5,1,5,5}	6144	{2,4,2,8}	6336	{4,2,4,6}	25152
{0,6,4,6}	2112	{5,5,1,5}	6144	{7,3,3,3}	10240	{6,4,2,4}	25152
{6,0,6,4}	2112	{5,5,5,1}	6144	{3,7,3,3}	10240	{4,6,4,2}	25152

Based on the data presented in Table 1, as well as on the Definition 4, it is fundamentally possible to construct 3948 IV-sets, which can be formed on the basis of a complete class of quaternary bent-sequences of length $N = 16$. As the experiments show, the best stochastic quality of the generated pseudorandom key sequences is provided with the following choice of their structure

$$[H \quad (H+1)\bmod 4 \quad (H+2)\bmod 4 \quad (H+3)\bmod 4], \qquad (8)$$

where H is one of the quaternary bent-sequences of length $N = 16$, the cardinality of the complete class of which is $J = 200704$.

Note that theoretically, as a LFSR, it is possible to use registers based on primitive irreducible polynomials over the extended field $GF(2^2)$. A method for synthesizing such a primitive irreducible polynomials over extended fields is presented in [17]. Based on this method, for example, we can construct following polynomial

$$f(x) = x^{10} + x^9 + 3x^8 + 3x^7 + 2x^6 + x^4 + 3x^3 + x^2 + 2, \qquad (9)$$

on the basis of which the LFSR scheme shown in Fig. 2 can be built.

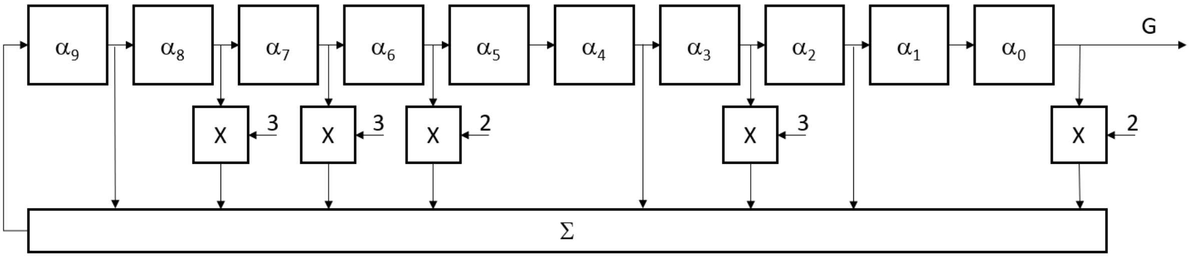

Fig. 2: LFSR scheme based on primitive irreducible polynomial (9)

Note that the operations of multiplication and summation in the LFSR scheme shown in Fig. 2 are performed in the extended Galois field $GF(2^2)$, which arithmetic is determined by a single irreducible polynomial over the Galois field $GF(2)$ of second degree $f(x) = x^2 + x + 1$ in accordance with the following tables

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 0 & 3 & 2 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 \end{array}, \quad \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 3 & 1 \\ 3 & 0 & 3 & 1 & 2 \end{array}. \qquad (10)$$

However, the results of the performed research which are presented in Table 2 show that LFSR constructed using extended fields show significantly worse stochastic performance compared to LFSR constructed using prime Galois fields. This circumstance does not allow them to be applied in the developed quaternary PRKSG. In our opinion, a good solution is to use binary LFSR with their subsequent multiplexing to ensure that arguments are supplied to the input of the IV-set of bent-sequences, as well as the choice of a specific quaternary bent-sequence from the IV-set is performed.

3. PRKSG scheme and its characteristics

Based on the above theoretical information, we present a quaternary PRKSG scheme based on a IV-set of quaternary bent-sequences. The following primitive irreducible polynomials are used for constructing LFSR (in accordance with the results of [9], in order to maximize the period of the generated pseudorandom key sequences, the degrees of primitive irreducible polynomials are chosen as coprime)

$$\begin{aligned}
&\mathrm{LFSR}_1 : f_1(x) = x^{23} + x^{17} + x^{11} + x^5 + 1;\\
&\mathrm{LFSR}_2 : f_2(x) = x^{29} + x^{20} + x^{16} + x^{11} + x^8 + x^4 + x^3 + x^2 + 1;\\
&\mathrm{LFSR}_3 : f_3(x) = x^{31} + x^{21} + x^{12} + x^3 + x^2 + x + 1;\\
&\mathrm{LFSR}_4 : f_4(x) = x^{19} + x^9 + x^8 + x^5 + 1;\\
&\mathrm{LFSR}_5 : f_5(x) = x^{17} + x^{16} + x^3 + x + 1;\\
&\mathrm{LFSR}_6 : f_6(x) = x^{37} + x^{28} + x^{18} + x^9 + 1,
\end{aligned} \tag{11}$$

and also, the IV-set of quaternary bent-sequences is chosen in accordance with condition (8)

$$\begin{aligned}
&H_1 = \{0331132333230113\};\\
&H_2 = \{1002203000301220\};\\
&H_3 = \{2113310111012331\};\\
&H_4 = \{3220021222123002\}.
\end{aligned} \tag{12}$$

In Fig. 3, we present the scheme of the developed PRKSG based on the IV-set of quaternary bent-sequences (12) and LFSR constructed in accordance with primitive irreducible polynomials (11).

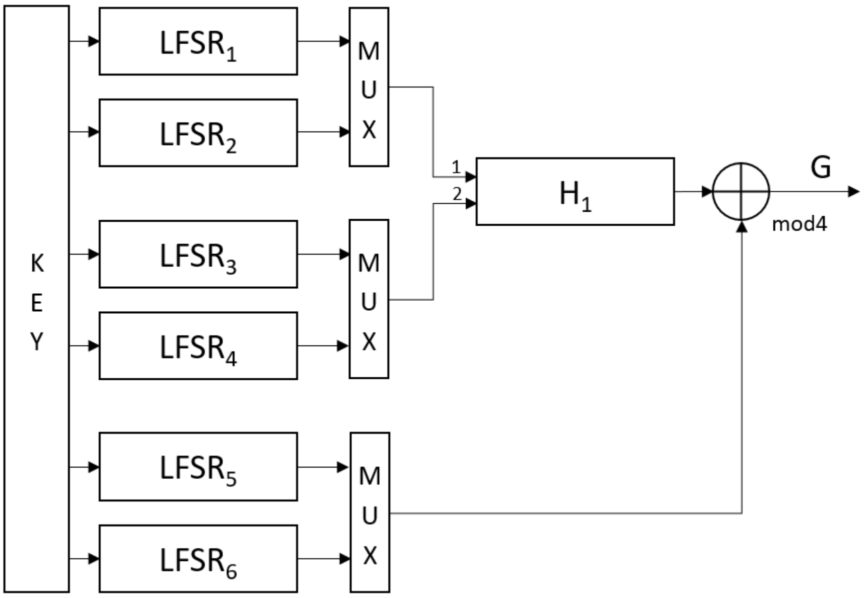

Fig. 3: Scheme of the proposed PRKSG based on IV-sets of bent-sequences (12)

Note that in view of the formation of a IV-set of quaternary bent-sequences in accordance with rule (8), in contrast to the PRKSG schemes presented in [9] and [14], there is no need to store the entire IV-set, as well as implement a selection block, which can be replaced by a summation device, which greatly simplifies the technical implementation of PRKSG and saves required for its implementation memory cells.

Thus, the values of quaternary bent-functions H_2, H_3, H_4 can be formed by adding a constant $1, 2$ or 3 to the original bent-function H_1, respectively. At the same time, the simultaneous operation of LFSR_5 and LFSR_6 allows choosing these values with equal probabilities, which leads to ensuring the equiprobable choice of one of the quaternary bent-sequences from the IV-set at each iteration of the PRKSG operation.

Let us note the features of the operation of the proposed PRKSG scheme based on IV-sets of quaternary bent-sequences. Binary registers LFSR_1 and LFSR_2 generate pseudorandom sequences, which are subsequently multiplexed into quaternary sequences that determine the first input variable of the bent-function (equivalent to corresponding bent-sequence). Similarly, the binary registers

LFSR_2 and LFSR_3 define the second input variable of the quaternary bent-function (equivalent to corresponding bent-sequence).

The registers LFSR_5 and LFSR_6 after the multiplexer generate one of the values from the set $\{0,1,2,3\}$, which determines the choice (with help of summation) of quaternary bent-sequence from the IV-set. Next, the corresponding value of the quaternary bent-function (equivalent to corresponding bent-sequence) is calculated, which is the output value of the PRKSG at a current cycle of operation.

The number of protection levels of the developed PRKSG is determined both by the number of possible initial states of the LFSR and by the number of bent-sequences in the complete class. In our case, when using primitive irreducible polynomials (11), as well as the complete class of quaternary bent-sequences [16], the number of protection levels of the developed PRKSG is defined as

$$\mathrm{Y} = (2^{23}-1)(2^{29}-1)(2^{31}-1)(2^{19}-1)(2^{17}-1)(2^{37}-1)\cdot 200704 \approx 2^{173,6}, \tag{13}$$

which exceeds the number of protection levels of the AES-128 block symmetric cipher.

At the same time, we note that in order to obtain a quaternary PRKSG based on a combination of two binary PRKSG units based on dual sets of bent-sequences [9], we would have to use 10 LFSR items, which is 40% more than in the proposed scheme. Thus, the use of IV-sets of quaternary bent-sequences makes it possible to simplify the algorithmic implementation of PRKSG in the applications where quaternary pseudorandom key sequences are required.

We note an important property of the proposed PRKSG scheme: it is easily scalable and makes it possible, if necessary, to easily increase the number of protection levels by using quaternary IV-sets of bent-sequences of greater length.

For example, consider the possibility of using quaternary bent-sequences of length $N = 64$. We take as a basis one of the quaternary bent-sequences of given length $N = 64$

$$H_1 = [3333301203213131000001231032020233333012032131312222230132102020], \tag{14}$$

on the basis of which, considering the construction (8), we obtain the IV-set

$$\begin{aligned}
H_1 &= \{3333301203213131000001231032020233333012032131312222230132102020\};\\
H_2 &= \{0000012310320202111112302103131300000123103202023333301203213131\};\\
H_3 &= \{1111123021031313222223013210202011111230210313130000012310320202\};\\
H_4 &= \{2222230132102020333330120321313122222301321020201111123021031313\}.
\end{aligned} \tag{15}$$

In view of the fact that each of the bent-sequences (15) is the equivalent of the corresponding bent-function of three variables, to construct the corresponding PRKSG we need another two LFSR to ensure the presence of an input signal for each of the variable of equivalent bent-function, as well as two LFSR for ensuring the selection of the bent-sequence from the IV-set.

Thus, in addition to the primitive irreducible polynomials (11), we choose two additional primitive irreducible polynomials

$$\begin{aligned}
&\mathrm{LFSR}_7 : f_7(x) = x^{41} + x^3 + 1;\\
&\mathrm{LFSR}_8 : f_8(x) = x^{43} + x^6 + x^4 + x^3 + 1.
\end{aligned} \tag{16}$$

On Fig. 4 we present a PRKSG scheme operating using eight LFSR and a IV-set of quaternary bent-sequences (15) of length $N = 64$.

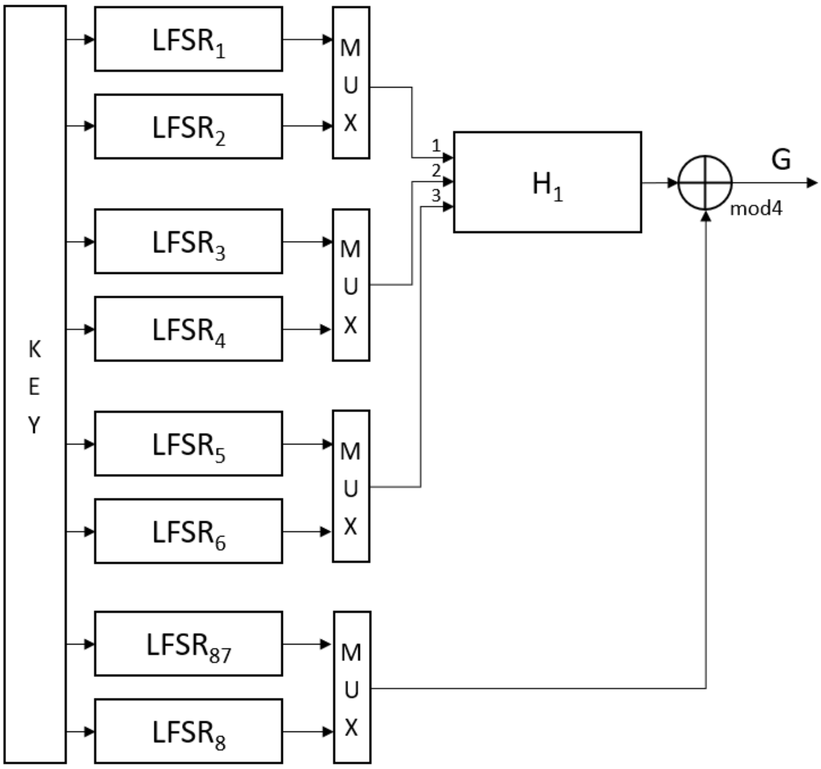

Fig. 4: Scheme of the proposed PRKSG based on IV-sets of bent-sequences (15)

The number of protection levels of the developed PRKSG is determined by the number of possible initial states of the eight LFSR included in it. In the case of using primitive irreducible polynomials (11) and (16), we obtain the following value

$$\begin{gathered} \mathrm{Y} = (2^{23}-1)(2^{29}-1)(2^{31}-1)(2^{19}-1)(2^{17}-1)(2^{37}-1)\times \\ \times(2^{41}-1)(2^{43}-1)(2^{47}-1) \approx 2^{287}. \end{gathered} \tag{17}$$

The obtained value of the number of protection levels exceeds the value of the number of protection levels of the AES-256 cryptographic algorithm.

Note that, to date, there are practically no methods for synthesizing complete classes of quaternary bent-sequences of length $N > 16$ represented in the literature, which leads to the decrease in the total value of protection levels number for developed PRKSG shown in Fig. 4. This circumstance naturally poses the practical problem of developing such a methods in order to increase the number of protection levels for PRKSG based on IV-sets of quaternary bent-sequences.

In Table 2, we present the results of the NIST stochastic tests of the developed PRKSG, its structural elements as well as some known analogues.

Table 2

Results of the NIST stochastic tests

No.	Test	LFSR based on (1)		LFSR based on (9)		PRKSG [10]		Developed PRKSG (Fig. 3)		Developed PRKSG (Fig. 4)	
		P-value	Pass rate	P-value	Pass rate	P-value	Pass rate	P-value	Pass rate	P-value	Pass rate
1	Monobit test	0.51	✓	0.86	✓	0.30	✓	0.09	✓	0.18	✓
2	Frequency within block test	0.74	✓	0.73	✓	0.99	✓	0.47	✓	0.06	✓
3	Runs test	0.72	✓	0.85	✓	0.11	✓	0.40	✓	0.72	✓
4	Longest run ones in a block test	0.14	✓	0.80	✓	0.04	✓	0.75	✓	0.19	✓

5	Binary matrix rank test	0.76	✓	0	✗	0.08	✓	0.87	✓	0.78	✓
6	DFT test	0.84	✓	0	✗	0.79	✓	0.34	✓	0.68	✓
7	Non overlapping template matching test	0.99	✓	0.97	✓	1	✓	1	✓	1	✓
8	Overlapping template matching test	0.01	✓	0.98	✓	0.26	✓	0.89	✓	0.08	✓
9	Maurers universal test	0.8	✓	0.01	✓	0.16	✓	0.40	✓	0.23	✓
10	Linear complexity test	0.16	✓	0	✗	0.83	✓	0.24	✓	0.93	✓
11	Serial test	0.9	✓	0.99	✓	0.18	✓	0.04	✓	0.81	✓
12	Approximate entropy test	0.9	✓	0.99	✓	0.18	✓	0.04	✓	0.81	✓
13	Cumulative sums test	0.49	✓	0.99	✓	0.18	✓	0.06	✓	0.16	✓
14	Random excursion test	0.33	✓	0.04	✓	0.16	✓	0.17	✓	0.04	✓
15	Random excursion variant test	0.42	✓	0	✗	0.29	✓	0.07	✓	0.03	✓

The analysis of the data presented in Table 2 leads to the conclusion that the proposed PRKSG based on IV-sets of quaternary bent-sequences of length $N = 16$, as well as quaternary bent-sequences of length $N = 64$ has a high level of stochastic quality and fully complies with all the NIST stochastic tests.

The NIST test results presented in Table 2, as well as the obvious simplicity of the technical implementation of the proposed PRKSG structure, allow us to recommend to use both developed PRKSG variants (Fig. 3 and Fig. 4) for practical use.

4. Conclusion

We note the main results of the research:

1. It has been established that the construction of quaternary PRKSG is possible on the basis of binary LFSR, as well as IV-sets of quaternary bent-sequences. At the same time, the configuration of the IV-set was found, which provides the best stochastic properties of the gamma generated by the PRKSG.
2. The scheme of the PRKSG is proposed which is based on binary LFSR and IV-set of quaternary bent-sequences. The proposed PRKSG provides a high level of stochastic properties of the generated sequences and the number of protection levels that can be easily scaled. For the case of use of the complete class of quaternary bent-sequences of length $N = 16$, the number of protection levels reaches the value $\mathrm{Y} \approx 2^{209,65}$, while in the case of using bent-sequences of length $N = 64$, the number of protection levels reaches the value $\mathrm{Y} \approx 2^{287}$, which exceeds the number of protection levels of the AES-256 cryptographic algorithm. Developed PRKSG also requires 40% smaller number of LFSR for generation of quaternary pseudorandom key sequences compared to combining of two PRKSG, based on dual sets of bent-sequences.
3. The presented PRKSG is of interest from the point of view of practical application where quaternary pseudorandom key sequences are needed, for example stream encryption algorithms operating based on many-valued logic principles, communication systems based on the FHSS technology, steganographic algorithms with the possibility of pseudorandom selection of a steganographic path.

Considering the above material, an important direction for further research is the development of methods for the synthesis of complete classes of quaternary bent-sequences, which will expand the variety of possible structures of the developed PRKSG, as well as increase the number of its protection levels value.

Another possible direction for further development of the proposed PRKSG is its modification in order to use larger values of base q.

5. References

1. G. Megala, S. Prabu, P. Swarnalatha, R. Venkatesan, Analysis on Cryptographic Design Techniques of Stream Ciphers and Attacks, in: P. Swarnalatha, S. Prabu (Ed.), Blockchain Technologies for Sustainable Development in Smart Cities, IGI Global, US, 2022, pp. 19–33. doi: 10.1007/978-3-540-40974-8_6.
2. M. Hasan, J. M. Thakur, P. Podder, Design and implementation of FHSS and DSSS for secure data transmission, International Journal of signal processing systems (2015) 144–149. doi: 10.12720/ijsps.4.2.144-149.
3. I. V. Agafonova, Cryptographic properties of nonlinear Boolean functions, in: Proceeding of the Seminar on discrete harmonic analysis and geometric modeling, Saint-Petersburg, 2007, pp. 1–24.
4. B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 2015.
5. O. Datcu, C. Macovei, R. Hobincu, Chaos based cryptographic pseudorandom number generator template with dynamic state change, Applied sciences (2020) 451. doi: 10.3390/app10020451.
6. E. Goncu, A. Kocdogan, M. E. Yalcin, A high speed true random number generator with cellular automata with random memory, in: Proceedings of the IEEE international symposium on circuits and systems (ISCAS), Florence, 2018, pp. 1730017. doi: iscas.2018.8351127.
7. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000.
8. C. E. Shannon, A Mathematical Theory of Cryptography, Bell System Technical Memo, USA, 1945.
9. M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov, The key sequences generator based on bent functions dual couples, Proceedings of Odessa Polytechnic University (2013) 150–156.
10. A. Sokolov, N. Kazakova, L. Kuzmenko, M. Mahomedova, Prerequisites for developing a methodology for estimating and increasing cryptographic strength based on many-valued logic functions, in: Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, 2021, pp. 107–116.
11. M. I. Mazurkov, Broadband radio systems, Odessa: Science and Technology, 2010.
12. M. A. Ivanov, I. V. Chugunkov, Theory, application and evaluation of the quality of generators of pseudorandom sequences, Moscow, KUDITS-OBRAZ, 2003.
13. FIPS 197. Advanced encryption standard, 2001. URL: http://csrc.nist.gov/publications/
14. A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov, Pseudorandom key sequence generator based on triple sets of bent-functions, Problems of Physics, Mathematics and Technics (2016) 85–91.
15. K. Schmidt, Quaternary Constant-Amplitude Codes for Multicode CDMA, IEEE transactions on information theory (2009) 1824–1832. doi: 10.1109/tit.2009.2013041.
16. A. V. Sokolov, Properties of the full class of quaternary bent-functions of two variables, Journal of discrete mathematical sciences and cryptography (2021): 1–14. doi: 10.1080/09720529.2021.1884380.
17. M. I. Mazurkov, Ye. A. Konopaka, The families of linear recurrent sequences based on full sets of Galois' isomorphic fields, Radioelectronics and Communications Systems (2005) 42–47.