Method for designing pseudorandom binary sequences generators on Nonlinear Feedback Shift Register (NFSR)

Dr. N.G BARDIS
Department of Automation
Technological Education
Institutes of Halkis
34400 Psahna, Halkis, Evia,
Greece

Dr. A.P. MARKOVSKYY
Department of Computer
Engineering
National Technical
University of Ukraine
37, Peremohy, pr. Kiev
252056, KPI 2003, Ukraine

D.V. ANDRIKOU, MSc
Telecommunications and Computer
Science Engineer
GREECE

Abstract: - This paper presents a new method for designing effective nonlinear pseudorandom bits generator for data security systems. The proposed method allows that design of n-bits Nonlinear Feedback Shift Registers (NFSR), which ensure the repeat cycle of 2^n. In contrast to Linear Feedback Shift Registers (LFSR) the pseudorandom sequences whish are generated by NFSR cannot be predicted if $2 \cdot n$ bits of the sequence are known. A generator, designed by the proposed method ensures the high performance and effectiveness of hardware realization.

Key-Words: - NonLinear Feedback Shift Register (NFSR), pseudorandom binary sequences generators

1 Introduction

The dynamic development of the information integration based on telecommunication and computer networks techniques is closely linked with extending the use of the pseudorandom binary sequences. Such sequences are widely used in CDMA and cosmic telecommunication systems, in digital data transmission channels for error detecting and error correcting, in VLSI embedded self-monitoring devices and in data security systems.

In contemporary situations where the integration of information expands and the increase of productivity of computer systems which can be used to attack data security components the problem of guaranteeing data security is acquiring a great importance.

This problem can be solved by way of perpetually developing data security methods and techniques, including pseudorandom sequence generators. Basically they are an important class of cryptographic algorithms, which are called stream ciphers algorithms. Apart from this, pseudorandom binary sequence generators are widely used to form keys and they are important components of cryptographic protocols and one-way hash functions.

The main sphere of pseudorandom sequence generators is utilized in stream cipher algorithms. This class of algorithms ensures the greatest cryptographic coding rate and is oriented for real-time data security systems. So, the stream cipher algorithms are widely used for cryptographic coding of video and voice telecommunications, telemetry and telecontrol systems.

From this point of view, one of the most important criterions of pseudorandom sequence generator is the effectiveness of bits generation rate.

Another important criterion of pseudorandom sequence generator is the level of crypto-resistance which is characterized by the sample size of sequence forecasting.

Most part from modern pseudorandom binary sequence generators is build with Linear Feedback Shift Registers (LFSR), which ensure a repeat of sequence period of 2^n-1 (n- bits length of shift register) and the effectiveness of hardware implementation. The main disadvantage of LFSR utilization is that the binary sequence generated by the LFSR can easily be forecasted if a sample size of $2 \cdot n$ bits is known (in case the feedback linear function is unknown). Therefore, in real sequence generators it is necessary to use additional nonlinear transformation which increases the complexity and reduces the generation rate [2, 3].

The Nonlinear Feedback Shift Register (NFSR) does not have the above mentioned disadvantage of the LFSR and the utilization of NFSR ensures a significant increase of the crypto - resistance level of pseudorandom bits sequence.

Today there is no mathematical common theory for NFSR design [4,5,6,7]. Thus only one possible way for NFSR practical implementation consists of the development of the particular approaches for the NFSR designing.

2 Basic procedure for nonlinear feedback function designing

The shift register structure is shown in Fig.1, where its state can be describe by a code w which corresponds to a binary vector X_w of the shift register's bits value by such a way as follows:

$$X_w = \{x_1^w, x_2^w, ..., x_{n-1}^w, x_n^w\},$$

$$\forall j \in \{1,...,n\} : x_j^w \in \{0,1\}, w = \sum_{j=1}^{n} x_j^w \cdot 2^{j-1}$$

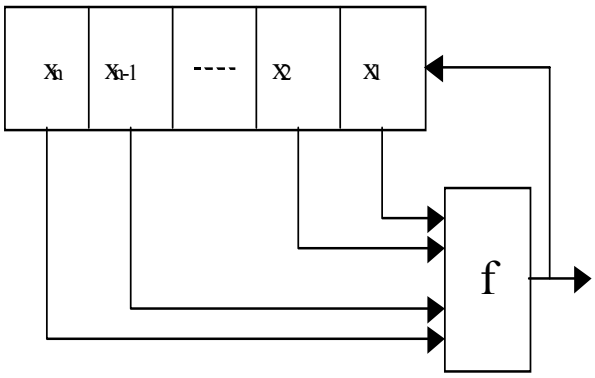

Fig.1

The value of the new code v after the register has been shifted, is defined as follows:

$$X_v = \{f(X_w), x_1^w, ..., x_{n-2}^w, x_{n-1}^w\},$$

$$v = (2 \cdot w) \bmod 2^n$$

$$f(x_1,...,x_{n-1},x_n) = 1 \oplus f(x_1,...,x_{n-1},1 \oplus x_n)$$

Let $f(x_1,x_2,\ldots,x_n)$ be the Boolean feedback function of n-bits length shift register and this function meets the following single-input condition:

$$f(x_1,...,x_{n-1},x_n) = 1 \oplus f(x_1,...,x_{n-1},1 \oplus x_n) \quad (1)$$

If the NFSR feedback function $f(x_1,x_2,\ldots,x_n)$ obeys to condition (1) then every shift register code v have only one previous code w.

The cycle of the NFSR shall be named the set of n-bits codes, which are sequentially formed in the shift register if the feedback function obeys the condition (1). Each of the 2^n possible codes of n-bits entry of the register is called in one round.

Let's have two rounds: A and B. If code $w \in A$, and a symmetric to w code $v=(w+2^{n-1}) \bmod 2^n \in B$, then inverting of the feedback function on these codes $f(X_w)=1 \oplus f(X_w)$, $f(X_v)=1 \oplus f(X_v)$, results in a union or a linear combination of these two rounds.

Proof. Code $w \in A$ and corresponds to binary state register vector $X_W = \{x_1^w, x_2^w, ..., x_n^w\}$. The code e follows the w code in round A: $X_e = \{f(X_w), x_1^w, ..., x_{n-1}^w\}$.

If the feedback function is inverted on code w the next code will be

u: $X_u = \{1 \oplus f(X_w), x_1^w, ..., x_{n-1}^w\}$.

Then code v is symmetric to w: $X_v = \{x_1^w, x_2^w, ..., x_{n-1}^w, 1 \oplus x_n^w\}$. According to (1), $f(X_v)=1 \oplus f(X_w)$. Therefore, the code u follows v in round B. If the feedback function is inverted on the code v the next code will be e: $X_e = \{1 \oplus f(X_w), x_1^w, ..., x_{n-1}^w\}$.

So, if the feedback function is inverted on a symmetric codes $w \in A$ and $v \in B$ after the code w, then we obtains the transfer to code $u \in B$. After that we pass through all the codes of round B consecutively to code v. From this code the transfer to code $e \in A$ is made. In future all code of round A are passed. Therefore, the two rounds A and B are united in a single round (Fig. 2).

The proposed method for designing the nonlinear feedback function which ensures a period of 2^n is found with the basic procedure of uniting rounds which are formed by a feedback rotational function.

The feedback rotational function of n-bits length shift register is equal to high-order bit of current code k:

$$f(X_n) = [\frac{k}{2^{n-1}}] = x_n^k \quad (2)$$

Evidently, the feedback function (2) satisfies condition (1). By using the feedback function (2), the N_R rounds are formed and every round contains codes, which have equal number of ones. Let's denote with R(k), the round containing the code k and with L(A), the number of ones in the rotation round A code. For example, for n=4 and k=6: R(k)={6(0110), 12(1100), 9(1001), 3(0011)}, L(R(k))=2.

Thus, every one round has only one minimal code. Obviously, for any rotation round A, except R(0), it's minimal code q=min(A) is odd ($x_1^q = 1$). This means that a nonzero minimal code q of rotational round always can be represented as: $q=2 \cdot d+1$.

The basic procedure of uniting the rotational rounds consists of performing the following sequential actions:

1. The initial value of the current code j is arbitrarily selected such that $0<j<2^n$. The counter h of the codes on which the value of the feedback function has been determined is set to 1: h:=1.
2. Calculate the code $u=(2\cdot j) \bmod 2^n+1$. If the calculated u is minimal in its rotational round, i.e., u=min((R(u)) then the value of the feedback function on code j is determined as the inversion of the rotation
$$f(X_j)=\left\lceil \frac{j}{2^{n-1}} \right\rceil \oplus 1 = x_n^j \oplus 1,$$(where $\lceil x \rceil$ is the smallest integer greater than x), otherwise,
$$f(X_j)=\left\lceil \frac{j}{2^{n-1}} \right\rceil = x_n^j$$
3. Calculate the new current code u:= $(2\cdot j) \bmod 2^n + f(X_j)$. The counter h is incremented: h:=h+1. If $h\le 2^n$ then return to step 2, otherwise – end.

The proposed basic procedure for designing the feedback function which guarantees the maximum period of 2^n for n-bits shift register can be illustrated by the followed example for n=4:

At the beginning we arbitrarily select the code j =8. The process of designing the feedback function is shown in table 1.

Table 1

Code(j)	X_j	h	u=(2·j) mod 16+1	R(u)	$F(X_j)$
0	0000	2	1	{**1**,2,4,8}	1
1	0001	3	3	{**3**,6,9,12}	1
2	0010	13	5	{**5**,10}	1
3	0011	4	7	**7,**14,13,11}	1
4	0100	16	9	{9,3,6,12}	0
5	0101	14	11	{11,7,14,13}	0
6	0110	10	13	{13,11,7,14}	0
7	0111	5	15	{**15**}	1
8	1000	1	1	{**1**,2,4,8}	0
9	1001	12	3	{3,6,12,9}	0
10	1010	15	5	{**5**,10}	0
11	1011	9	7	{7,14,13,11}	0
12	1100	11	9	{9,3,6,12}	1
13	1101	8	11	{11,7,14,13}	1
14	1110	7	13	{13,11,7,14}	1
15	1111	6	15	{**15**}	0

The graph of the feedback codes transformations used in the design of the shift register function is shown in Fig.3.

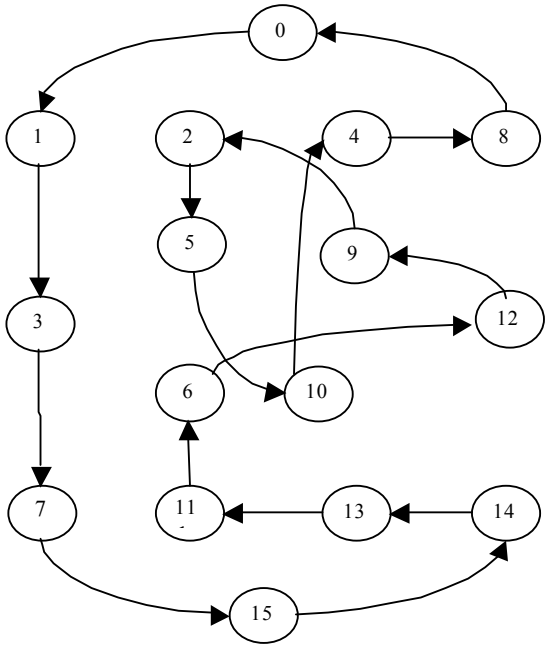

Fig. 3

The feedback rotational function is formed in N_R rounds. The basic procedure ensures the connection of all of them into one.

Proof. The connection of rounds is made pair-wise. Let's consider an arbitrarily selected round B, which unite the rounds each containing m ones ($0<m<2^n$). Let's denote the minimal code of this round with $\beta_{min}=\min(B)$. The code β_{min} follows code $\beta\in B$, despite the fact that $\beta \ge 2^{n-1}$ and $\beta_{min}= 2\cdot\beta-2^{n-1}+1$. Evidently, the code $\alpha = \beta-2^{n-1}$ differs from code β by the "ones" in high-order bit. Consequently, code α belongs to another round A: $\alpha\in A$ and all the codes of this round A contain m-1 ones. Thus $\beta_{min}= 2\cdot\alpha+1$ and according to condition (2) of the presented procedure on code α the feedback function value will be equal to one, $F(X_\alpha)=1$, and in such way the next code after α will be the code β_{min}.

According to condition (2) of the presented procedure the value of the feedback function on code β will be inverted with the rotational function. Therefore, after code β, code $\alpha_{next}\in A$, $\alpha_{next} = 2\cdot\alpha$ will be follow. In this way the proposed procedure ensures the connection of rounding pair A and B.

The transition to round B minimal code min(B) is possible from code of round A if L(B)=L(A)+1 with the exception of the situation when L(B)=0. In the last case one code is predecessor to minimal codes of pair-wise rotational rounds. For example, if n=4 and the code 8(1000) is predecessor to minimal code 0(0000) of round {0} then the minimal code 1(0001) is predecessor to rounds {1,2,4,8}.

The minimal code value of every rotational round has one predecessor code from another round. Therefore, the proposed procedure ensures the connection of all rotational rounds into one round.

3 Expansion procedure for nonlinear feedback function designing

Let's consider the above basic procedure of a single valued defined topology of rotational rounds then its connectivity allows obtaining only one nonlinear feedback function at a fixed NFSR length.

Modifying the considered basic procedure can solve the design problem of obtaining more nonlinear feedback functions.

To that end, we suggest beforehand to unite two arbitrarily selected rotational rounds A and B with the conditions L(B)-L(A)=1 and L(A)>0. Apart from this, it is necessary to forbid the foreseen by the basic procedure transition to round B minimal code min(B).

The expansion procedure to unite the rotational rounds consists of performing the following sequential actions:

1. Arbitrarily select code k such, that: $0 < k < 2^n-2$.
2. Arbitrarily select code $b \in R(k)$ with its minimal code belonging in the rotational round R(k): $b \neq \min(R(k))$.
3. Code a is formed as: $a = \left\lfloor \frac{b}{2} \right\rfloor + \xi \cdot 2^{n-1}$, where $\xi \in \{0,1\}$ and $\lfloor x \rfloor$ is the greatest integer but smaller than x. The value of ξ is selected in such a way that $a \notin R(b)$.
4. Define the code d to be the predecessor of the greatest from min(R(a)) and min(R(b)):
$$d = \left\lfloor \frac{\max(\min(R(a), \min(R(b)))}{2} \right\rfloor$$
5. The initial value of current code j is arbitrarily selected such that $0<j<2^n$. The counter h of the codes on which the value of the feedback function has been determined is set to 1: h:=1.
6. If j=a or $j = (a+2^{n-1}) \bmod 2^n$, then $f(X_j) = \left\lceil \frac{j}{2^{n-1}} \right\rceil \oplus 1 = x_n^j \oplus 1$ and go to step 9.
7. If j=d or $j=(d+2^{n-1}) \bmod 2^n$, then $f(X_j) = \left\lceil \frac{j}{2^{n-1}} \right\rceil = x_n^j$ and go to step 9.
8. Calculate $u=(2 \cdot j) \bmod 2^n + 1$. If the calculated u is minimal in its rotational round, i.e. , u=min((R(u)), then the value of the feedback function on code j is determined as the inversion of the rotation $f(X_j) = \left\lceil \frac{j}{2^{n-1}} \right\rceil \oplus 1 = x_n^j \oplus 1$,(where $\lceil x \rceil$ is the smallest integer but greater than x), otherwise, $f(X_j) = \left\lceil \frac{j}{2^{n-1}} \right\rceil = x_n^j$
9. Calculate the new current code $j:= (2 \cdot j) \bmod 2^n + f(X_j)$. The counter h is then incremented by one: $h:=h+1$. If $h \leq 2^n$ then return to step 2, otherwise – end.

The proposed modified procedure for designing of the feedback function which guarantees the maximum period of 2^n for the n-bits shift register can be illustrated by the followed example for n=4:

According to step 1 we arbitrarily selected code k : 0<k<15. For example, k=12.

The rotational round R(12)={12(1100), 9(1001), 3(0011), 6(0110)}, then according to step 2 arbitrarily we select $b \in R(k)$, $b \neq \min(R(k))=3$. Let b=9.

Code a is formed as: $a=4+\xi \cdot 8$. If $\xi=0$, then $a=4 \notin R(k)$. Thus, a=4.

The rotational round R(12)={12,9,3,6} and R(4)={4,8,1,2}, correspondently the min(R(b))=3 and the min(R(a))=1. According to step 4 the code d is defined as:

$$d = \left\lfloor \frac{\max(3,1)}{2} \right\rfloor = 1 \cdot$$

Thus, a=4 and $a+2^{n-1}=12$, d=1 and $d+2^{n-1}=9$.

Let at the beginning of the procedure j = 0. Since $j \neq a = 4$, $j \neq a+2^{n-1} = 12$, $j \neq d = 1$, $j \neq d+2^{n-1} = 9$, then according to step 8 we calculate $u=2 \cdot 0+1=1$; R(u)={1,2,4,8} and u=min(R(u)), therefore f(0000) = 1 and next j=1.

Since j=d=1, then according to step 7, $f(X_1)=f(0001)=0$. The next j is defined as $j=2 \cdot 1+0 = 2$.

Table 2 has illustrated the consistency of designing the feedback functions in the sequel.

The graph of the shift register designed using the codes of the feedback nonlinear function transformations is shown in Fig.4.

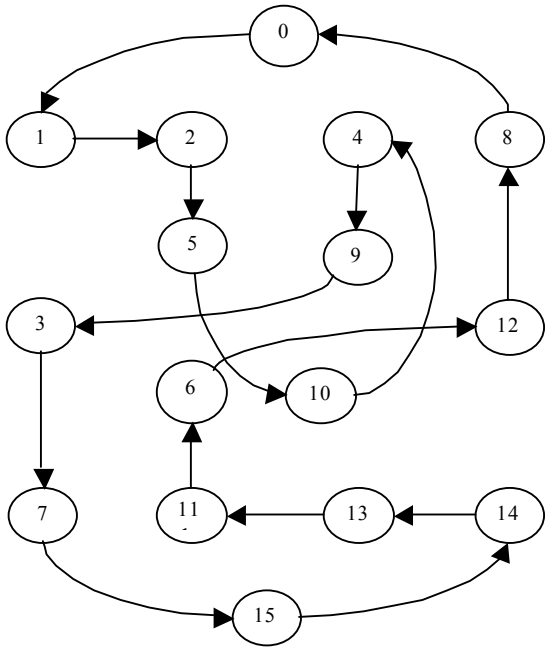

Fig.4

Table 2

j	X_j	h	Equality of j to a, d,$a+2^{n-1}$, $d+2^{n-1}$	u=(2·j +1) mod 16	R(u)	F
0	0000	1		1	{**1**,2,4,8}	1
1	0001	2	j = d		-	0
2	0010	3		5	{**5**,10}	1
3	0011	8		7	{**7**,14,13,11}	1
4	0100	6	j = a		-	1
5	0101	4		11	{**7**,14,13,11}	0
6	0110	14		13	{7,14,13,11}	0
7	0111	9		15	{15}	1
8	1000	16		1	{**1**,2,4,8}	0
9	1001	7	j = d+8		-	1
10	1010	5		5	{5,10}	0
11	1011	13		7	{**7**,14,13,11}	0
12	1100	15	j = a+8		-	0
13	1101	12		11	{7,14,13,11}	1
14	1110	11		13	{7,14,13,11}	1
15	1111	10		15	{15}	0

The number N_f of the NFSR nonlinear feedback function transformations which can be designed by using the proposed method for different shift register n bits length is represented in Table 3.

Table 3

N	N_f	n	N_f	n	N_f
4	6	8	186	12	3394
5	18	9	394	13	6930
6	38	10	810	14	14022
7	90	11	1764	15	28386

4 Conclusions

The suggested method for pseudorandom binary sequence generators based on the nonlinear feedback shift register design ensures the increase of the effectiveness of an important class of cryptographic algorithms such as the stream cipher.

The utilization of the NFSR instead of the LFSR registers in stream cipher allows a significant improved level of stream cipher crypto-resistance. At the same time the NFSR, designed by the suggested method ensures the maximum value of a repeat period of 2^n as well as simplicity in the hardware implementations.

The number of nonlinear feedback function which can be obtained by the suggested method is significantly larger in comparison to the number of prime polynomials. For example, if n=15, the suggested method allows to built 28386 different NFSR schemes. For the same value n=15, only 1800 different LFSR schemes are existing. This fact is very important for the cryptographic applications of pseudorandom bit sequence generators.

Compared to other known methods [2,3,4,5,6,7], the suggested NFSR design approach is much more simple and effective from the technological point of view (implementation and algorithmically). Another significant advantage of the suggested method in comparison to known ones [2,3,4,5,6,7] is the larger number of NFSR schemes that may be designed at a fixed length of shift register. The stated method is implemented in the form of an existing program written in C++.

References:

[1] Key E.L. An analysis of the structures and complexity of nonlinear binary sequence generators. *IEEE Trans.Infor*. IT-22 ,1976 pp. 732-736.

[2]Rueppel R.A. Analysis and Design of Stream Cipher.LNCS-431,*Springer-Verlag*,:1986 -182 p.

[3] N.G.Bardis**,** A.Polymenopoulos, E.G.Bardis, A.P.Markovskyy, D.V.Andrikou, "An approach to determine the complexity of random and pseudo random binary sequences", *WSES, TRANSACTIONS on COMMUNICATIONS*, Issue 1, Volume 1, ISSN 1109-2742, 2002, pp: 37 – 42.

[4] Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. *Ed.John Wiley.*: 1996 - 758 p.

[5] A.Menezes, P.Van Oorschot and S.Vanstone, "Handbook of Applied Cryptography,"*CRC Press,* 1996.

[6] Pieprzyk, Hardjono, Seberry, Fundamentals of Computer Security, *Springer Verlag*, 2003

[7] Βασίλειος Κάτος, Γεώργιος Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ISBN 960-8065-40-2, 2003

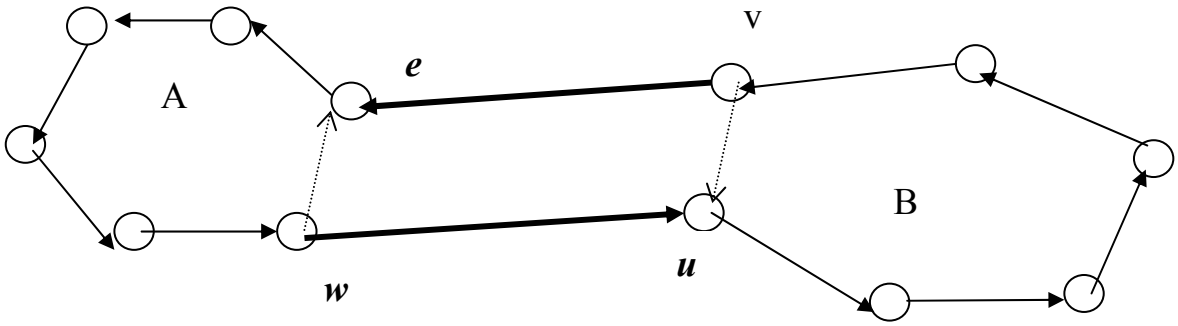

Fig. 2