

İNFORMASIYA TEXNOLOGİYALARI

UOT: 621.391.272

DOI: 10.34826/NAA.2022.24.1.006

“STOP AND GO” PRİNSİPİ ƏSASINDA İŞLƏYƏN PSEVDOTƏSADÜFİ ƏDƏD FORMALAŞDIRICISI

Əliyeva İ.N.

Milli Aviasiya Akademiyası

Məqalədə rabitə sistemlərində məlumatların şifrələnməsi zamanı tələb olunan açar ardıcılığının generasiyası üçün “stop and go” prinsipi əsasında işləyən psevdotəsadüfi ədəd formalaşdırıcısının Matlab simulink mühitində modeli reallaşdırılmışdır. Xətti əks rabitəli sürüşmə registri alqoritminin analizi aparılmış, müəyyənləşən çatışmazlıqlar və şifrələmə açarına qoyulan tələblər reallaşdırılan modeldə nəzərə alınmışdır. Tətbiq olunan riyazi alqoritm əsas hissələri olan idarəedici və idarə olunan registrlərin Matlab simulink mühitində modelləri reallaşdırılmışdır. Registrlərin və “stop and go prinsipi” əsasında işləyən psevdotəsadüfi ədəd formalaşdırıcısının çıxışında formalaşan ardıcılıqların bir hissəsinin ossiloqramları, həmçinin onların onluq say sistemində qiymətləri əks olunmuşdur.

Açar sözlər: Xətti əks rabitəli sürüşmə registri, psevdotəsadüfi ədəd formalaşdırıcısı, stop and go prinsipi, açar ardıcılığı, statistik xüsusiyyət, kriptografiya.

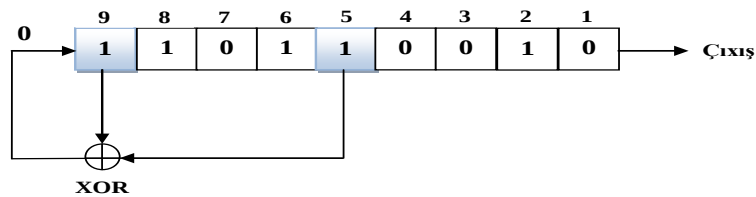
Giriş. Müasir dövrdə ötürülən məlumatların konfidensiallığını daha da artırmaq üçün xüsusi alqoritmlərdən istifadə edilir. Bu alqoritmlər əvvəlcədən müəyyən olunmuş riyazi modelə tabe olduqları üçün nəzəri olaraq statistik təsadüfi olmayan ardıcılıqlar formalaşdırır. Lakin yaxşı statistik xüsusiyyətlərə malik alqoritm seçildiyi halda formalaşan ardıcılıqlar təsadüflük testlərinin bir çoxunu keçə bilər və məlumatların şifrələnməsi zamanı “açar” kimi tətbiq oluna bilər [1]. Belə ardıcılıqlar psevdotəsadüfi ədəd ardıcılıqları adlanır və psevdotəsadüfi ədəd formalaşdırıcısı (PTƏF) vasitəsilə generasiya olunur. PTƏF-in reallaşdırılması üçün xətti konquerent (Linear congruential), ləngimələrlə fibonaççi (Lagged Fibonacci), orta kvadrat (Middle-square) metodları, xətti əks rabitəli sürüşmə registri (Linear feedback shift register) və s. kimi müxtəlif riyazi iş alqoritmləri tətbiq olunur. Müasir elektron hesablama maşını PTƏF-in istənilən iş alqoritmni praktiki olaraq reallaşdırmağa imkan verir [2,3]. Aparılan analizlər nəticəsində [4] müəyyən olunmuşdur ki, xətti konquerent, ləngimələrlə fibonaççi, orta kvadrat metodları əsasında reallaşdırılan PTƏF-in generasiya etdiyi ardıcılıqlar arasında korrelyasiya mövcuddur və çox kiçik perioda malikdirlər.

Kriptografiyada tətbiq olunan PTƏF-a qoyulan cəldlik, yaxşı statistik xüsusiyyətlər, böyük period kimi tələbləri nəzərə alaraq, məqalədə PTƏF-in reallaşdırılması üçün optimal riyazi iş alqoritmni kimi Linear feedback shift register (LFSR) alqoritmindən istifadə olunmuşdur.

İşin məqsədi məlumatların şifrələnməsi üçün açar generasiya edən “stop and go” prinsipi əsasında işləyən PTƏF-in iş alqoritmni sintezi və onun modelinin Matlab simulink mühitində reallaşdırılmasıdır.

LFSR-in iş alqoritmni. LFSR iki hissədən: sürüşmə registri və yeni bitin qiymətini hesablayan əks rabitə sxemindən (Exclusive or - “XOR” məntiq elementindən) ibarətdir. Sürüşmə registri funksional yaddaş kanallarından ibarət olub, hər bir yaddaş xanasında bir bitin (“0” və ya

“1”) cari zaman anındakı qiymətini yadda saxlayır. Burada yaddaş xanaları rəqəmlərlə nömrələnir, yəni $n = 1, 2, 3, 4, 5, 6, 7, \dots, N$ (n -yaddaş xanasının sıra nömrəsidir) və xanaların sayı registrin uzunluğunu müəyyənləşdirir. Şəkil1-də sürüşmə registrinin uzunluğu 9-a, başlanğıc qiyməti isə “110110010” bərabər olan LFSR-in iş alqoritmi təsvir olunmuşdur. Alqoritmin iş prinsipinə əsasən sürüşmə registrində qeyd olunmuş başlanğıc qiymətin (seed) bitləri (2 və ya daha çox bit) arasında “XOR” məntiq əməliyyatı yerinə yetirilir. Daha sonra registr bir pozisiya sağa sürüşdürülür və alınan yeni bitin qiyməti böyük nömrəli yaddaş xanasında (9N-li yaddaş xanasında) qeyd olunur. Registrin kiçik nömrəli yaddaş xanası (1N-li yaddaş xanası) isə LFSR-in çıxışı funksiyasını yerinə yetirir. Bu proses LFSR-in maksimal periodu əldə olunana qədər davam edir.



Şəkil 1. LFSR-in iş alqoritmi

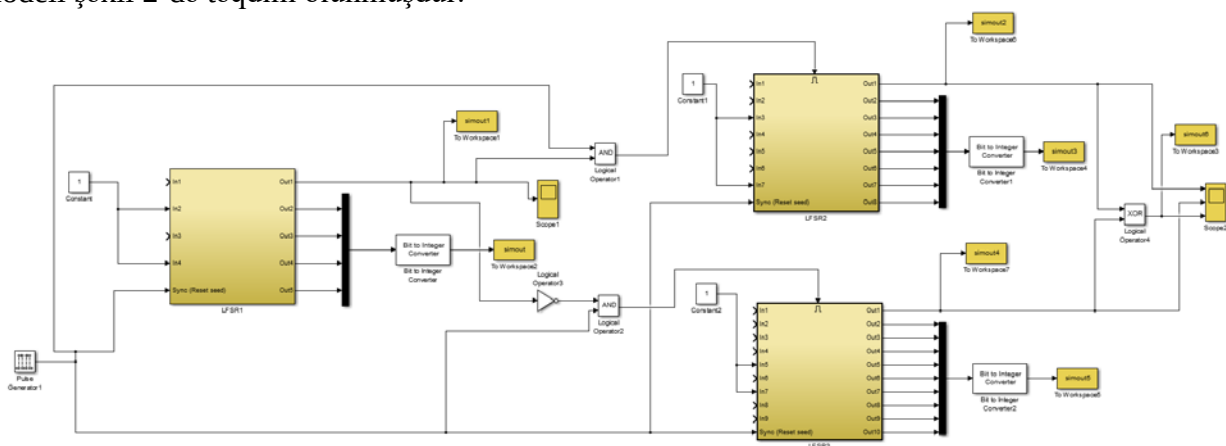
Registrin qadağan olunmuş sıfır vəziyyəti (000...000) nəzərə alınaraq, maksimal period aşağıdakı kimi təyin olunur:

$$T = 2^N - 1, \quad (1)$$

burada, N -registrin uzunluğudur. LFSR alqoritmində sürüşmə registrinin uzunluğu və ilkin başlanğıc qiymət düzgün seçildiyi halda kifayət qədər böyük perioda və cəldliyə malik PTƏF əldə etmək mümkündür [5].

Üç LFSR əsasında “stop and go” prinsipi ilə işləyən PTƏF. “Stop and go” PTƏF iki LFSR-in (LFSR1 və LFSR2) bir-biri ilə qeyri-xətti əlaqələndirilməsi metodu ilə işləyir. Bu generatorun əsas çatışmazlığı ardıcılıqların generasiyası zamanı müəyyən ləngimələrin yaranmasıdır. Qeyd edək ki, bu çatışmazlıq qurğunun reallaşdırılması zamanı üç ədəd LFSR: bir idarəedici LFSR1, iki idarəolunan LFSR2 və LFSR3 tətbiq olunaraq aradan qaldırılmalı bilər. Burada idarəedici registrin (LFSR1) çıxışında formalaşan bitlər ardıcılığı vasitəsi ilə idarə olunan registrlərin (LFSR2 və LFSR3) takt tezliklərinə nəzarət olunur [6].

“Stop and go” prinsipi əsasında işləyən PTƏF-in Matlab simulink mühitində reallaşdırılan modeli şəkil 2-də təqdim olunmuşdur.

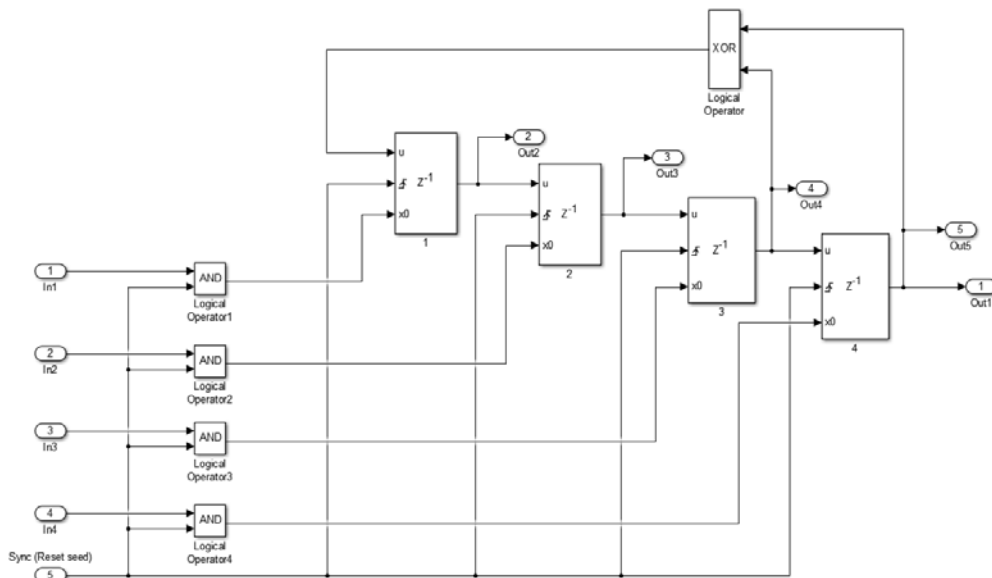


Şəkil 2. “Stop and go” prinsipi əsasında işləyən PTƏF-in Matlab simulink mühitindəki modeli

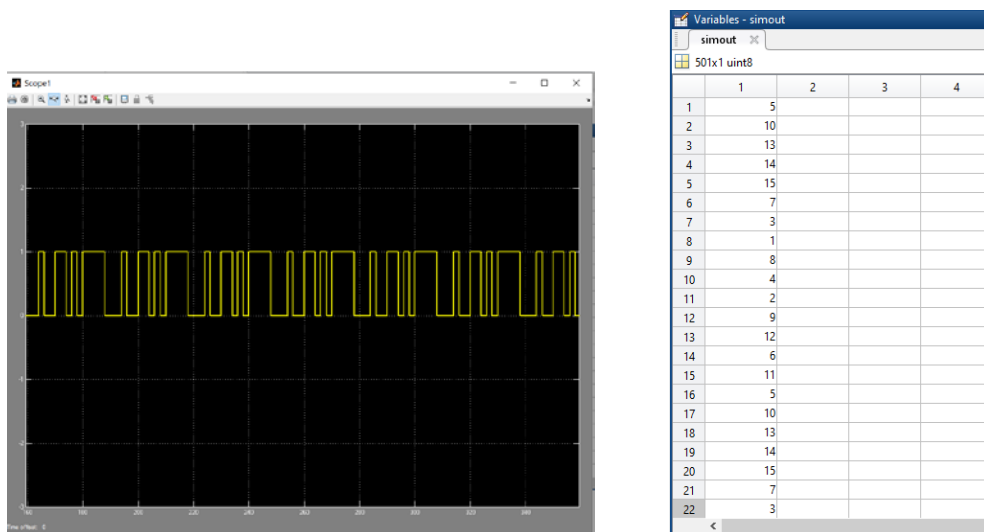
Belə ki, impuls generatorunun (Pulse generator) çıxışında formalaşan takt signalı LFSR1-in sinxroirəsinə (Sync) verilən zaman başlanğıc qiymətə (0101) uyğun olaraq LFSR1-in çıxışında (Out1-də) məntiqi “1” və ya məntiqi “0” generasiya olunmağa başlayır. Əgər LFSR1-in çıxışında məntiqi “1” formalaşarsa, bu halda LFSR2 ilkin verilən başlanğıc qiymətinə (0010001) uyğun olaraq öz vəziyyətini dəyişir, LFSR3 isə əvvəlki çıxış bitini (ilkin takt signalı halında LFSR3-in

əvvəlki çıxış biti “0” hesab olunur) yenidən təkrarlayır. Əgər LFSR1-in çıxışında məntiqi “0” formalaşarsa, bu halda isə əksinə LFSR2 əvvəlki biti (ilkin takt signalı halında LFSR2-in əvvəlki çıxış biti “0” hesab olunur) təkrarlayır, LFSR3 isə ilkin verilən başlanğıc qiymətinə (000010100) uyğun olaraq öz vəziyyətini dəyişir və yeni ardıcılıq generasiya edir. Yəni, burada LFSR1-in kiçik nömrəli yaddaş xanasında yerləşən biti (çıkış biti) periodik olaraq LFSR2 və LFSR3 üçün icazə signalı funksiyasını yerinə yetirir. Sonda hər dəfə LFSR2 və LFSR3-in çıxışında formalaşan bitlər arasında XOR məntiq əməliyyatı yerinə yetirilir və məlumatın şifrənməsi üçün tələb olunan açar ardıcılığı əldə olunur. Bu proses “stop and go” prinsipi əsasında işləyən PTƏF-in maksimal periodu əldə olunana qədər davam edir.

LFSR1 idarəedici registrin uzunluğu $L_1 = 4$ seçilmişdir, (1) ifadəsini nəzərə alsaq, uyğun olaraq əldə olunan maksimal period $T_1 = 15$ - ə bərabərdir. LFSR1-də maksimal period əldə etmək üçün XOR əməliyyatı hər dəfə 3-cü və 4-cü bitlər arasında yerinə yetirilmişdir. Şəkil 3-də LFSR1 idarəedici registrin Matlab simulink mühitindəki modeli, şəkil 4-də isə LFSR1-in çıxışında formalaşan ardıcılığın ossiloqramı (scope1) və onun onluq say sistemində (simout) qiymətləri əks olunmuşdur.



Şəkil 3. LFSR1 idarəedici registrin Matlab simulink mühitindəki modeli

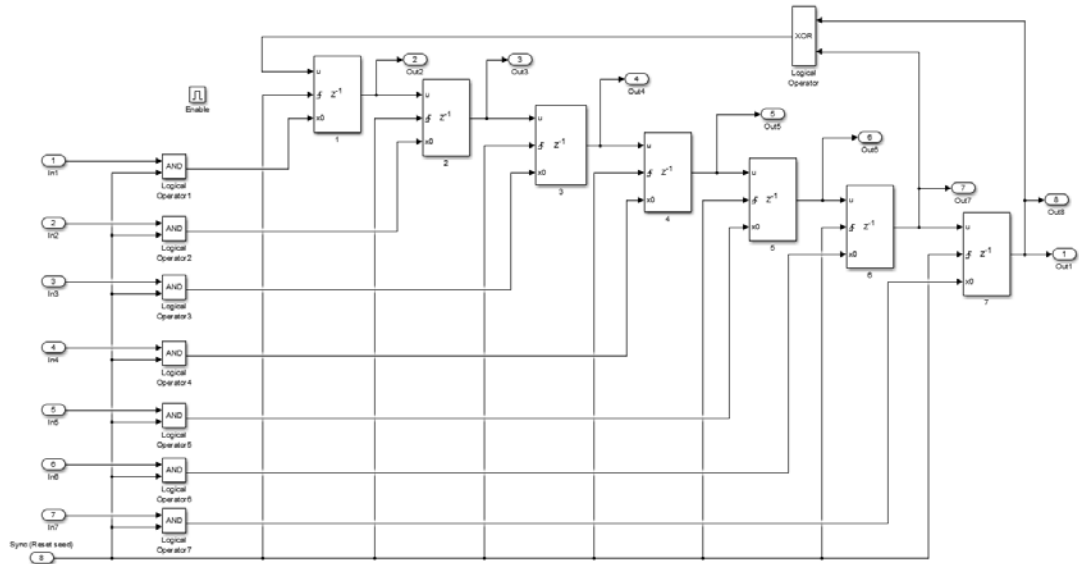


(a)

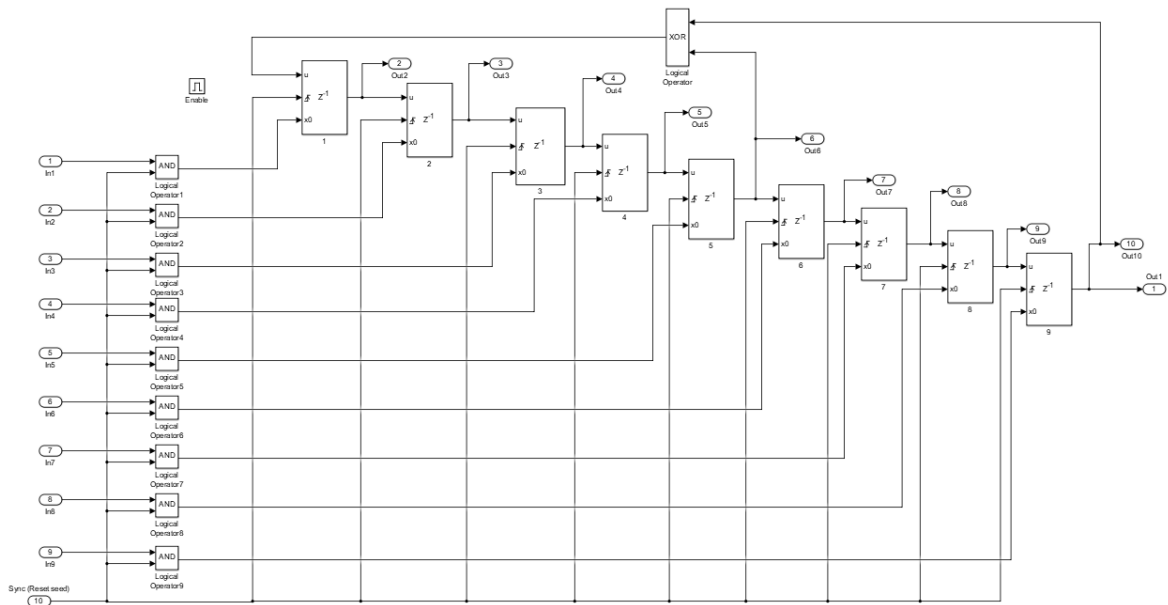
(b)

Şəkil 4. LFSR1-in çıxışında formalaşan ardıcılıq: (a) ossiloqram; (b) onluq say sistemində

İdarə olunan registrlərin LFSR2, LFSR3 uzunluqları L_2 və L_3 seçilən zaman isə mütləq qarşılıqlı sadə ədədlər olmasına diqqət yetirilməlidir, yəni $\text{ƏBOB}(L_2, L_3) = 1$ [6]. Beləliklə, LFSR2-in uzunluğu $L_2 = 7$, LFSR3-in uzunluğu isə $L_3 = 9$ seçilmişdir. (1) ifadəsini nəzərə alsaq, LFSR2-in maksimal periodu $T_2 = 127$, LFSR3-in maksimal periodu isə $T_3 = 511$ -ə bərabərdir. Şəkil 5 (a) və (b)-də LFSR2, LFSR3-in Matlab simulink mühitində reallaşdırılan modelləri göstərilmişdir. Reallaşdırılan modelə əsasən maksimal period əldə etmək üçün LFSR2-də XOR əməliyyatı hər dəfə 6-cı və 7-ci bitlər arasında, LFSR3-də isə 5-ci və 9-cu bitlər arasında yerinə yetirilmişdir.



(a)



(b)

Şəkil 5. İdarə olunan registrlərin Matlab simulink mühitində modeli: (a) LFSR2; (b) LFSR3

Şəkil 6 (a) və (b)-də LFSR2, LFSR3-in çıxışında (simout3 və simout5) formalaşan ardıcılıqların bir hissəsinin onluq say sistemində qiymətləri əks olunmuşdur.

Qeyd edək ki, ilkin takt signalı verilən zaman (şəkil 2) LFSR1-in çıxışında “5” rəqəmi (şəkil 4 (b)), yəni ikilik say sistemində “0101” ardıcılığı generasiya olunur. Aydındır ki, burada kiçik nömrəli yaddaş xanasında yerləşən çıxış biti məntiqi “1”-ə bərabərdir. Bu halda sxemə əsasən LFSR2-in girişinə məntiqi “1” verilir və çıxışında (Out1) “17” rəqəmi (“0010001” ardıcılığı) (şəkil 6 (a)) generasiya olunur. LFSR3-də isə əvvəldə inkar-“NOT” məntiq elementi yerləşdiyi üçün məntiqi “1” məntiqi “0”-a çevrilir, daha sonra LFSR3 -in girişinə verilir. İlkin takt signalı halında LFSR3-nin əvvəlki çıxış bitini “0” hesab olunduğu üçün çıxışda “0” rəqəmi (“000000000” ardıcılığı) (şəkil 6 (b)) generasiya olunur. Növbəti dəfə LFSR1-in çıxışında “10” rəqəmi (şəkil 4 (b)), yəni ikilik say sistemində “1010” ardıcılığı generasiya olunur.

	1	2	3	4
1	17			
2	17			
3	72			
4	72			
5	36			
6	18			
7	73			
8	100			
9	100			
10	100			
11	100			
12	50			
13	50			
14	50			
15	89			
16	108			
17	108			
18	54			
19	54			
20	91			
21	45			
22	86			

(a)

	1	2	3	4
1	0			
2	20			
3	20			
4	266			
5	266			
6	266			
7	266			
8	266			
9	133			
10	322			
11	161			
12	161			
13	336			
14	424			
15	424			
16	424			
17	212			
18	212			
19	362			
20	362			
21	362			
22	362			

(b)

Şəkil 6. İdarə olunan registrlərin çıxışında formalaşan ardıcılıqların bir hissəsinin onluq say sistemində qiymətləri: (a) LFSR2; (b) LFSR3

Burada kiçik nömrəli yaddaş xanasında yerləşən çıxış bitini məntiqi “0”-a bərabərdir. Bu halda LFSR2-in girişinə məntiqi “0” verilir və LFSR2 əvvəlki çıxış bitini “17” rəqəmini (“0010001” ardıcılığı) (şəkil 6 (a)) yenidən təkrarlayır. LFSR3-də isə əvvəldə inkar-“NOT” məntiq elementi yerləşdiyi üçün məntiqi “0” məntiqi “1”-ə çevrilir, daha sonra LFSR3 -in girişinə verilir. Beləliklə, LFSR3-in çıxışında (Out1) “20” rəqəmi (“000010100”) (şəkil 6 (b)) generasiya olunur. Periodik olaraq, LFSR1-in çıxışında formalaşan ardıcılığın (şəkil 4 (b)) kiçik nömrəli yaddaş xanasında yerləşən bitləri vasitəsi ilə LFSR2 və LFSR3 idarə olunur. Sxemin sonuncu mərhələsində hər dəfə idarə olunan registrlərin LFSR2 və LFSR3-in çıxışında formalaşan bitlər arasında XOR məntiq əməliyyatı yerinə yetirilir və açar yəni, psevdotəsadüfi ədəd ardıcılığı generasiya olunur.

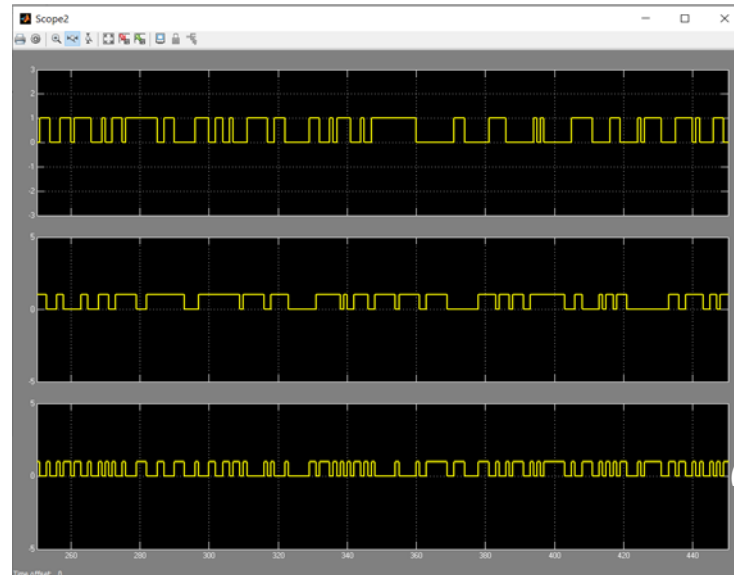
Şəkil 7 (a) və (b)-də LFSR2, LFSR3-in, (c)-də isə “stop and go” prinsipi əsasında işləyən PTƏF-in çıxışında formalaşan ardıcılıqların bir hissəsinin ossiloqramları (scope2) əks olunmuşdur.

Beləliklə, bu proses takt signalının davam etmə müddətindən asılı olaraq maksimal period əldə olunana qədər davam edir. “Stop and go” prinsipi əsasında işləyən PTƏF-in maksimal periodu [6] aşağıdakı ifadə ilə təyin olunur:

$$T = 2^{L_1}(2^{L_2} - 1)(2^{L_3} - 1) \quad (2)$$

LFSR1, LFSR2 və LFSR3-in seçilən uzunluqlarını ($L_1 = 4, L_2 = 7, L_3 = 9$) (2) ifadəsində nəzərə alsaq, bu halda “stop and go” prinsipi əsasında işləyən PTƏF-in maksimal periodu:

$$T = 2^4 \cdot (2^7 - 1) \cdot (2^9 - 1) = 1\,038\,352$$



Şəkil 7. Formalaşan ardıcılıqların ossiloqramları: (a) LFSR2-in çıxışı; (b) LFSR3-in çıxışı; (c) “stop and go” prinsipi əsasında işləyən PTƏF-in çıxışı

Şəkil 8-də maksimal periodu $T=1038352$ -a bərabər olan “stop and go” prinsipi əsasında işləyən PTƏF-in çıxışında formalaşan psevdotəsadüfi ədəd ardıcılığının bir hissəsi (simout6) əks olunmuşdur.

Variables - simout6				
simout6				
	1	2	3	4
1	1			
2	1			
3	0			
4	0			
5	0			
6	0			
7	1			
8	0			
9	1			
10	0			
11	1			
12	1			
13	0			
14	0			
15	1			
16	0			
17	0			
18	0			
19	0			
20	1			
21	1			
22	0			

Şəkil 8. “Stop and go” prinsipi əsasında işləyən PTƏF-in çıxışında formalaşan psevdotəsadüfi ədəd ardıcılığının bir hissəsi

Nəticə. Matlab simulink proqram paketində reallaşdırılan “stop and go” prinsipi əsasında işləyən psevdotəsadüfi ədəd formalaşdırıcısı çox böyük perioda və cəldliyə malik olduğu üçün radorabitə sistemində ötürülən böyük məlumat paketlərinin (massivlərinin) şifrənməsi zamanı ən optimal vasitə kimi tətbiq oluna bilər. Burada idarəedici və idarə olunan registrlərin uzunluqlarını daha böyük seçərək kifayət qədər böyük period əldə etmək olar. Eyni zamanda, seçilən uzunluqdan asılı olaraq registrlərin daxilində xətti əks rəbitələrin sayını artırmaqla formalaşan ardıcılıqların daha mürəkkəb olmasını təmin etmək mümkündür. Bu isə növbəti şifrəlmə açarının əvvəlcədən proqnozlaşdırılmasını kifayət qədər çətinləşdirərək tətbiq olunduğu sistemin kriptohücumlara qarşı dayanıqlılığını daha da artırmağa bilər. Həmçinin, burada ilkin başlanğıc qiymətləri hər dəfə təsadüfi olaraq dəyişərək formalaşdırılan ardıcılıqların statistik xüsusiyyətlərini daha da mükəmməlləşdirmək olar.

ƏDƏBİYYAT

1. Шпітяк Я.І., Аметов А.Ю., Григоренко А.К., Задорожний П.А., Фоменко А.І., Козелкова О.С. Системи управління, навігації та зв'язку. Джерела та опис сучасних генераторів псевдовипадкових чисел, Державний університет телекомунікацій, Київ. 2014, випуск 2(30) ISSN 2073-7394 Ахметов Б. А., Корченко А. Г., Сиденко В. П., Дрейс Ю. А., Сейлова Н. А. Прикладная криптология: Алматы 2015. - 496 с.
2. Иванов М. А., Ковалев А. В., Мацук Н. А., Чугунков И. В. Методы и средства защиты информации в компьютерных системах и сетях, 2009. – 602 с.
3. Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А. Методы генерации и тестирования случайных последовательностей – СПб: Университет ИТМО, 2019. – 70 с.
4. Ndaw A., Djiby S., Sanghar. Construction of Maximum Period Linear Feedback Shift Registers (LFSR) (Primitive Polynomials and Linear Recurring Relations British Journal of Mathematics & Computer Science 11(4): 1-24, 2015, Article no.BJMCS.19442 ISSN: 2231-0851. - P 24
5. Wicik R., Rachwalik T. Modified Alternating Step Generators. Military Communication Institute Warszawska 22A, 05-130 Zegrze, Poland {r.wicik, t.rachwalik}@wil.waw.pl/- P 8

REFERENCES

1. Shpityak Ya.I., Ametov A.Yu., Grigorenko A.K., Zadorozhny P.A., Fomenko A.I., Kozelkova E.S. Management systems, navigation and communication. Sources and description of modern pseudo-random number generators, State University of Telecommunications, Kiev. 2014, Issue 2(30) ISSN 2073-7394
2. Akhmetov B. A., Korchenko A. G., Sidenko V. P., Dreis Yu. A., Seilova N. A. Applied cryptology: Almaty 2015. - 496 p.
3. Ivanov M.A., Kovalev A.V., Matsuk N.A., Chugunkov I.V. Methods and means of information protection in computer systems and networks, 2009. - 602 p.
4. Budko M.B., Budko M.Yu., Girik A.V., Grozov V.A. Methods for generating and testing random sequences - St. Petersburg: ITMO University, 2019. - 70 p.
5. Ndaw A., Djiby S., Sanghar. Construction of Maximum Period Linear Feedback Shift Registers (LFSR) (Primitive Polynomials and Linear Recurring Relations British Journal of Mathematics & Computer Science 11(4): 1-24, 2015, Article no.BJMCS.19442 ISSN: 2231-0851. - P 24
6. Wicik R., Rachwalik T. Modified Alternating Step Generators. Military Communication Institute Warszawska 22A, 05-130 Zegrze, Poland {r.wicik, t.rachwalik}@wil.waw.pl/- P 8

**PSEUDO-RANDOM RANDOM NUMBER GENERATOR BASED ON
"THE STOP AND GO" PRINCIPLE**

Aliyeva İ.N.

National Aviation Academy

The article researches a model of a pseudo-random number generator for the generation of the key sequence required when encrypting data in communication systems based on the "stop and go" principle in the Matlab simulink environment. The analysis of the linear feedback shift register algorithm was carried out, the identified shortcomings and the requirements for the encryption key were taken into account in the implemented model. Models of control and managed registers, which are the main parts of the applied mathematical algorithm, were implemented in the Matlab simulink environment. The oscillograms of some of the sequences formed by the registers and the pseudo-random number generator based on the "stop and go principle", as well as their values in the decimal number system are reflected.

Keywords: *Linear feedback shift register, pseudorandom number generator, stop and go principle, key sequence, statistical feature, cryptography.*

Rəyçi: *t.f.d., dos. F.H. Dadaşov*

Müəllif haqqında məlumat

Soyadı, adı, atasının adı	İş yeri	Vəzifəsi, elmi dərəcəsi, elmi adı	Əlaqə
Əliyeva İnci Namiq qızı	Milli Aviasiya Akademiyası	Radioelektronika kafedrasının müəllimi	inci777@bk.ru mob: (+994) 55 419 45 64