Pseudorandom Number Generator Based on Linear Feedback Shift Register Algorithm

I.N. Aliyeva

Azerbaijan National Aviation Academy (Mardakan ave. 30, Baku, AZ1045, Azerbaijan)

For correspondence:
Aliyeva Inci / e-mail: inci777@bk.ru

Abstract

In the article, the analysis of various schemes of pseudorandom number generators is carried out and their main shortcomings are recorded. Taking into account the identified shortcomings, the principle scheme of the pseudo-random number generator based on the linear feedback shift register algorithm is proposed to ensure the confidentiality of transmitted data in communication and control systems. The work algorithms of the control and controlled registers, which are the main parts of the proposed device and are implemented on the basis of PIC16F84A microcontrollers, are shown. At the end of the article, the general view of the device implemented based on the proposed principle scheme is reflected.

Keywords: Linear feedback shift register, pseudorandom number generator, pseudorandom number sequence, statistical property, confidentiality, correlation.

DOI 10.52171/2076-0515_2023_15_03_97_103

Received *25.10.2022*
Revised *15.09.2023*
Accepted *20.09.2023*

For citation:
Aliyeva I.N.
[Pseudorandom Number Generator Based on Linear Feedback Shift Register Algorithm]
Herald of the Azerbaijan Engineering Academy, 2023, vol. 15, no. 3, pp. 97-103 *(in Azerbaijani)*

Xətti əks rabitəli sürüşmə registri alqoritmi əsasında psevdotəsadüfi rəqəm generatoru

İ.N. Əliyeva

Azərbaycan Milli Aviasiya Akademiyası (Mərdəkan pr. 30, Bakı, AZ1045, Azərbaycan)

Yazışma üçün:
Əliyeva İnci / e-mail: inci777@bk.ru

Xülasə

Məqalədə, psevdotəsadüfi rəqəm generatorlarının müxtəlif sxemlərinin analizi aparılmış və onların əsas çatışmazlıqları qeyd olunmuşdur. Müəyyən olunan çatışmazlıqları nəzərə alaraq, rabitə və idarəetmə sistemlərində ötürülən məlumatların məxfiliyinin təmin olunması üçün xətti əks rabitəli sürüşmə registri alqoritmi əsasında psevdotəsadüfi rəqəm generatorunun prinsipial sxemi təklif olunmuşdur. Təklif olunan qurğunun əsas hissələri olan və PİC16F84A mikrokontrollerləri əsasında reallaşdırılan idarəedici və idarə olunan registrlərin iş alqoritmləri göstərilmişdir. Məqalənin sonunda isə təklif olunan prinsipial sxem əsasında reallaşdırılan qurğunun ümumi görünüşü əks olunmuşdur.

Açar sözlər: xətti əks rabitəli sürüşmə registri, psevdotəsadüfi rəqəm generatoru, psevdotəsadüfi rəqəm ardıcıllığı, satistik xüsusiyyət, konfidensiallıq, korrelyasiya.

DOI 10.52171/2076-0515_2023_15_03_97_103

УДК 004.056.5

Генератор псевдослучайных чисел на основе алгоритма регистр сдвига с линейной обратной связью

И.Н. Алиева

Азербайджанская Национальная академия авиации (пр. Мардакян,30, Баку, AZ1045, Азербайджан)

Для переписки:
Алиева Инджи / e-mail: inci777@bk.ru

Аннотация

В статье проведен анализ различных схем генераторов псевдослучайных чисел и отмечены их основные недостатки. С учетом выявленных недостатков предложена принципиальная схема генератора псевдослучайных чисел на основе алгоритма регистр сдвига с линейной обратной связью для обеспечения конфиденциальности передаваемых данных в системах связи и управления. Показаны алгоритмы работы управляющего и управляемого регистров, которые являются основными частями предлагаемого устройства и реализованы на базе микроконтроллеров PIC16F84A. В конце статьи отражен общий вид устройства, реализованного по предложенной принципиальной схеме.

Ключевые слова: регистр сдвига с линейной обратной связью, генератор псевдослучайных чисел, последовательность псевдослучайных чисел, статистическое свойство, конфиденциальность, корреляция.

Giriş

Hal-hazırda, müxtəlif dərəcədə təsadüfliyə malik olan ardıcıllıqlar formalaşdırmaq üçün çoxlu sayda üsul və metodlar mövcuddur. Lakin praktikada bu üsulların əksəriyyəti xassələri təsadüflik tələblərinə cavab verməyən ardıcıllıqlar formalaşdırır. Həmçinin burada hesablama resurslarının məhdudluğu ciddi şəkildə çətinlik törədən problemlərdən biridir. Belə ardıcıllıqlar formalaşdırmaq üçün müxtəlif generatorlardan istifadə olunur [1]. Bunlardan biri statistik xüsusiyyətlərinə görə maksimal dərəcədə ideal təsadüfliyə bənzər ardıcıllıqlar generasiya edən psevdotəsadüfi rəqəm generatorlarıdır (PTRG). Təsadüfi ardıcıllıq generatorlarının xüsusiyyətlərinə və real vaxta yaxın rejimdə işləmək ehtiyacına görə, PTRG-nın hazırlanması və istifadəsi məsələsi çox yüksək aktuallığa malikdir. Hal-hazırda PTRG-ların müxtəlif növləri mövcuddur. Ən geniş tətbiq olunan növləri: xətti konqurent generatorlar; Fibonaççi rəqəm ardıcıllıqları əsasında ləngimələrlə additiv generatorlar; orta kvadrat metodu əsasında işləyən generatorlar; xətti əks rabitəli sürüşmə registri əsasında işləyən generatorlardır. Xətti konqurent generatorlarda tətbiq olunan riyazi modeldə parametrlər düzgün seçilmədiyi halda formalaşan ardıcıllıqlar çox kiçik perioda malik olur. Fibonaççi rəqəm ardıcıllıqları əsasında ləngimələrlə additiv generatorlar vasitəsi ilə əldə olunan ardıcıllıqlar isə böyük perioda malik olsa da, təsadüfi deyildir.

Orta kvadrat metodu əsasında işləyən PTRG-nin əsas çatışmazlığı isə generasiya olunan ardıcıllıqlar arasında korrelyasiyanın mövcud olması və çox kiçik perioda malik olmasıdır. Qeyd edək ki, bu generatorlar vasitəsi ilə formalaşan ardıcıllıqları əvvəlcədən proqnozlaşdırmaq mümkün olduğundan məlumatların şifrlənməsi üçün tələb olunan açar formalaşdırıcısı kimi tətbiq olunmurlar [2].

İşin məqsədi

Ötürülən məlumatların konfidensiallığını təmin edən, həmçinin kifayət qədər böyük perioda, cəldliyə malik üç ədəd xətti əks rabitəli sürüşmə registrindən ibarət PTRG-nin və onun hər üç registri üçün iş alqoritmlərinin reallaşdırılmasıdır.

Məsələnin qoyuluşu

Xətti əks rabitəli sürüşmə registri əsasında PTRG iki sürüşmə registrinin (idarəedici və idarə olunan) biri-biri ilə qeyri-xətti əlaqələndirilməsi prinsipi ilə işləyir [3]. Burada idarəedici registrin çıxışında məntiqi "1" səviyyəsi formalaşan zaman idarə olunan registrin çıxışında psevdotəsadüfi rəqəm ardıcıllığı (PTRA) generasiya olunmağa başlayır. Əgər idarəedici registrin çıxışında məntiqi "0" səviyyəsi formalaşarsa, bu halda idarə olunan registr işə düşmür və heç bir ardıcıllıq generasiya olunmur [4]. Qeyd edək ki, məhz bu səbəbdən yekunda yaranan zaman ləngimələri qurğunun əsas çatışmazlığı hesab olunur [5, 6].

Məsələnin həlli

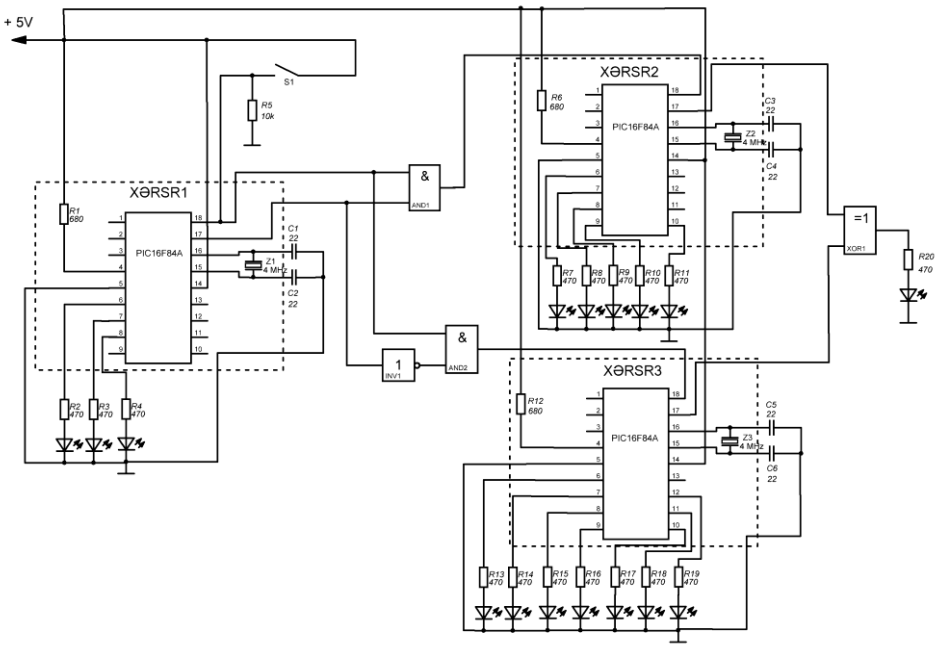
Qeyd olunan çatışmazlığı aradan qaldırmaq üçün üç ədəd xətti əks rabitəli sürüşmə registri (idarəedici-XƏRSR1 və idarə olunan-XƏRSR2, XƏRSR3 registrlər) əsasında PTRG-nin prinsipial sxemi şəkil 1-də əks olunmuşdur. Burada həm idarəedici həm də idarə olunan registrlər PİC16F84A mikrokontrollerləri üzərində yığılmışdır.

Qurğunun iş prinsipinə əsasən PİC16F84A mikrokontrollerinin (MK) 18-ci pininə (RA1 portuna) bağlanmış açar qapanan zaman burada formalaşan məntiqi "1" səviyyəsi həm idarəedici (XƏRSR1) registri işə sa-

lır, həm də hər iki "VƏ" (AND1 və AND2) məntiq elementlərinin girişlərinə verilir. Beləliklə, məntiqi "1" səviyyəsinin təsirindən sonra idarəedici (XƏRSR1) registrin çıxışında yəni, 17-ci pində (RA0 portunda) generasiya olunan ardıcıllıq "VƏ" (AND1) məntiq elementinin digər girişinə verilir. Nəticədə, "VƏ" (AND1) məntiq elementinin çıxışında əldə olunan məntiqi "0" və ya "1" səviyyəsi idarə olunan (XƏRSR2) registrin 18-ci pininə (RA1 portuna) verilir. Həmçinin, burada idarəedici registrin (XƏRSR1) RA0 portunda generasiya olunan ardıcıllıq eyni zamanda "YOX" (İNV1) məntiq elementinin girişinə verilir, invers olunur və "VƏ" (AND2) məntiq elementinin digər girişinə verilir. "VƏ" (AND2) məntiq elementinin çıxışında əldə olunan məntiqi "0" və ya "1" səviyyəsi idarə olunan (XƏRSR3) registrin RA1 portuna verilir. Qeyd edək ki, burada idarə olunan registrlərdən hansının girişinə (RA1 portuna) məntiqi "1" səviyyəsi verilərsə, həmin registr öz vəziyyətini dəyişir və yeni psevdotəsadüfi rəqəm generasiya edir.

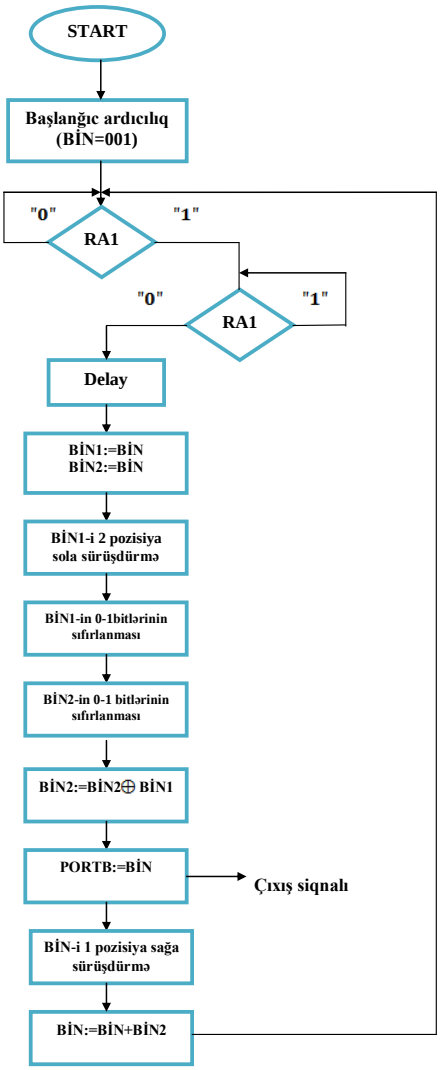
Əgər idarə olunan registrin girişinə məntiqi "0" səviyyəsi verilərsə həmin registr əvvəlki rəqəmi yenidən təkrarlayır. Aydındır ki, burada idarəedici (XƏRSR1) registrin çıxışında formalaşan PTRA idarə olunan registrlərin (XƏRSR2 və XƏRSR3) takt tezliklərini müəyyən edir. Bu proses maksimal period əldə olunana qədər periodik olaraq davam edir və hər dəfə idarəedici registrlərin çıxışında formalaşan ardıcıllıqlar arasında "XOR" məntiq əməliyyatı yerinə yetirilir, yəni, yeni PTRA generasiya olunur.

Burada (şək.1) idarəedici (XƏRSR1) registrin uzunluğunun L_1=3-ə, idarə olunan registrlərin (XƏRSR2 və XƏRSR3) uzunluqlarının isə uyğun olaraq, L_2=5 və L_3=7-ə bərabər olduğunu qurğunun maksimal periodunun [7-9] ifadəsində nəzərə alsaq, reallaşdırılan qurğunun maksimal periodu T_{max}=31496-a bərabərdir.



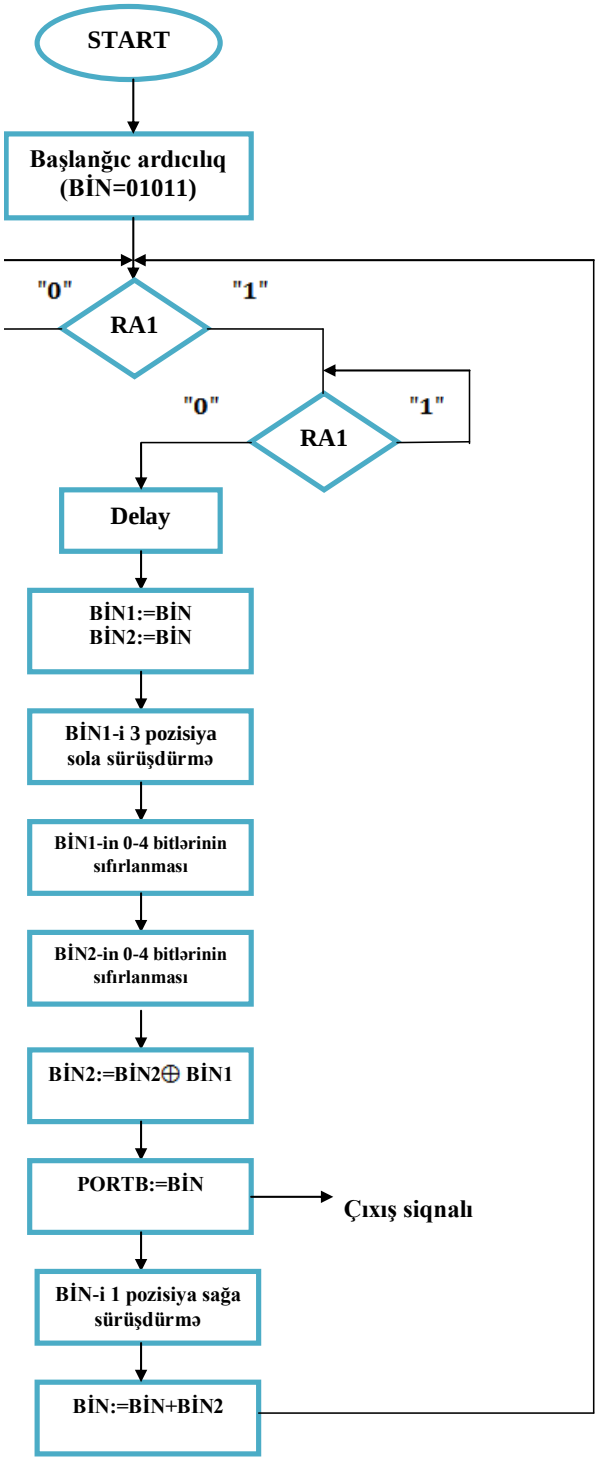
Şəkil 1 – Üç ədəd xətti əks rabitəli sürüşmə registri əsasında PTRG-nin prinsipial sxemi
Figure 1 – The principle scheme of PTRG based on three numbers of linear feedback shift registers

PTRG-nın PİC16F84A mikrokontrolleri əsasında reallaşdırılan idarəedici registrinin iş alqoritmi şəkil 2-də əks olunmuşdur.

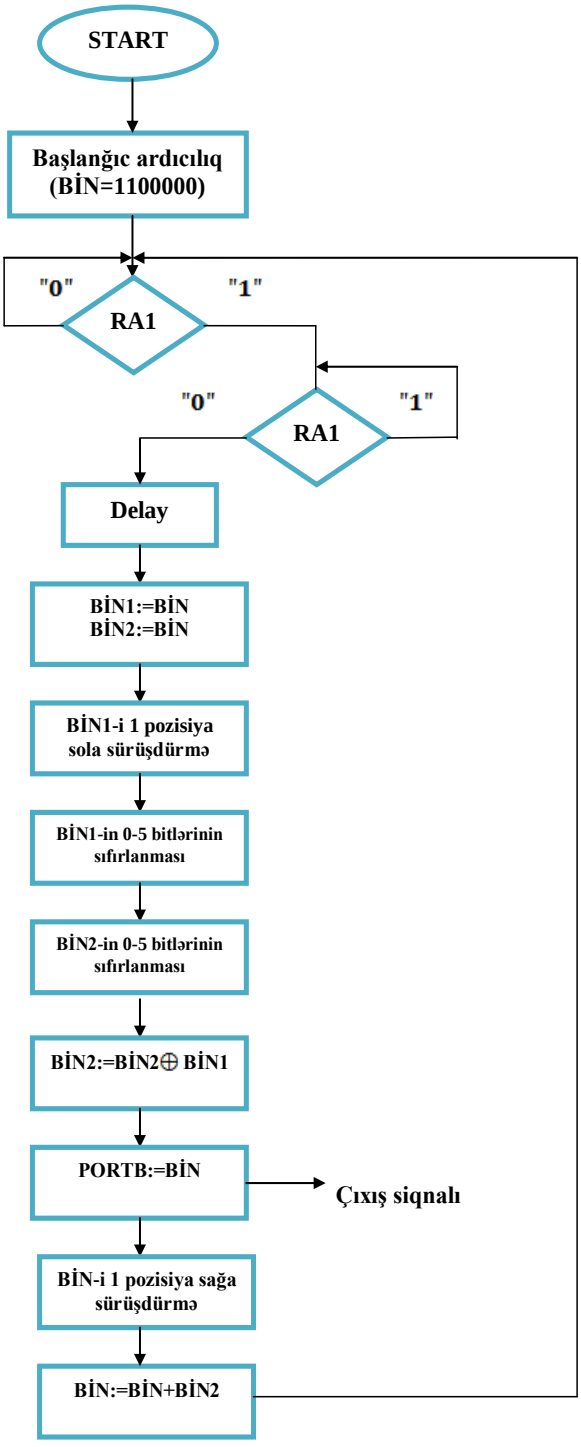


Şəkil 2 – İdarəedici registrin (XƏRSR1) iş alqoritmi
Figure 2 – Working algorithm of the control register (LFSR1)

Alqoritmin iş prinsipi belədir: İlkin olaraq proqrama ikilik başlanğıc rəqəm (BİN) daxil edilir və idarəedici registrin RA1 portu proqram tərəfindən periodik olaraq yoxlanılır. Əgər RA1 portunda məntiqi "1" səviyyəsi formalaşarsa, bu halda daxil olunan ardıcıllığın 0-cı və 2-ci xanalarında yerləşən bitlər arasında "XOR" məntiq əməliyyatı yerinə yetirilir və yeni bitin qiyməti hesablanır. Daha sonra sürüşmə registri bir pozisiya sağa sürüşdürülür və yeni bitin qiyməti həmin pozisiyaya qeyd olunur.



Şəkil 3 – İdarə olunan registrin (XƏRSR2) iş alqoritmi
Figure 3 – Working algorithm of the managed register (LFSR2)



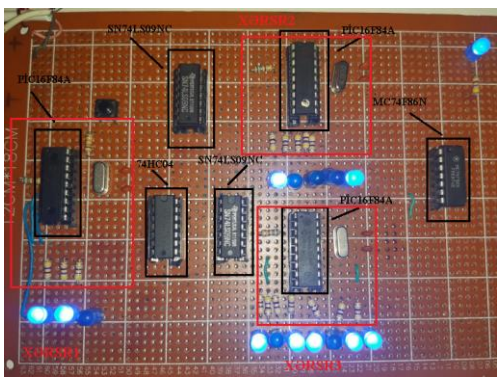
Şəkil 4 – İdarə olunan registrin (XƏRSR3) iş alqoritmi
Figure 4 – Working algorithm of the managed register (LFSR3)

Beləliklə, hər dəfə generasiya olunan yeni bit həm çıxışa yəni, PORTB-ə ötürülür, həm də sürüşmə registrində qeyd olunur və bu proses maksimal period əldə olunana qədər periodik olaraq davam edir.

PTRG-nın PİC16F84A mikrokontrolleri əsasında reallaşdırılan idarə olunan registrlərin iş alqoritmləri isə şəkil 3 və şəkil 4-də-də əks olunmuşdur.

İdarə olunan registrlərin (XƏRSR2 və XƏRSR3) iş alqoritmləri idarəedici registrdə (XƏRSR1) olduğu kimidir. Burada XƏRSR2-də daxil olunan ardıcıllığın 0-cı və 3-cü xanalarında yerləşən bitlər arasında, XƏRSR3-də isə daxil olunan ardıcıllığın 5-ci və 6-cı xanalarında yerləşən bitlər arasında "XOR" məntiq əməliyyatı yerinə yetirilir və yeni bitin qiyməti hesablanır. Daha sonra sürüşmə registri bir pozisiya sağa sürüşdürülür və yeni bitin qiyməti həmin pozisiyaya qeyd olunur. Beləliklə, hər dəfə generasiya olunan yeni bit həm çıxışa yəni, PORTB-ə ötürülür, həm də sürüşmə registrində qeyd olunur və bu proses maksimal period əldə olunana qədər periodik olaraq davam edir.

Təklif olunan qurğunun ümumi görünüşü şəkil 5-də təsvir olunmuşdur.



Şəkil 5 – Üç ədəd xətti əks rabitəli sürüşmə registri əsasında PTRG-nin ümumi görünüşü
Figure 5 – General view of PTRG based on three linear feedback shift registers

Burada XƏRSR1, XƏRSR2, XƏRSR3 registrlərinin və reallaşdırılan qurğunun çıxışında (MC74F86N-XOR məntiq elementinin çıxışı) əldə olunan ardıcıllıqları vizual olaraq görmək üçün işıq diodlarından istifadə olunmuşdur.

Nəticə

Üç ədəd xətti əks rabitəli sürüşmə registri əsasında reallaşdırılan psevdotəsadüfi rəqəm generatoru kifayət qədər böyük cəldliyə və perioda malikdir. Burada həm idarəedici həm də idarə olunan registrlərin uzunluqlarını daha böyük seçərək generasiya olunan ardıcıllıqların periodunu daha da artırmaq mümkündür. Həmçinin daha böyük takt tezliyinə malik mikrokontrollerdən istifadə edərək qurğunun cəldliyini daha çox artırmaq olar. Qeyd edək ki, qurğu reallaşdırılan zaman "zaman ləngiməsi" kimi çatışmazlıq aradan qaldırıldığı üçün real vaxta yaxın rejimdə işləməyə imkan verir və ötürülən məlumatların konfidensiallığının təmin olunması üçün ən optimal vasitələrdən biri kimi tətbiq oluna bilər.

Burada idarəedici və idarə olunan registrlərinin başlanğıc qiymətlərini təsadüfi seçərək formalaşan ardıcıllıqların kriptodayanıqlılığını və statistik xüsusiyyətlərini mükəmməlləşdirə bilərik.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Akhmetov B.A., Korchenko A.G., Sidenko V.P., Dreis Yu.A., Seilova N.A.** Applied cryptology. Almaty, 2015. - 496 p. *(in English)*
2. **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. *(in English)*
3. **Kanso A.A.** Modified clock-controlled alternating step generator. Computer Communications 32, *Elsevier,* pp. 787799, 2009. *(in English)*
4. **Əliyeva İ.N.** Stop and go prinsipi əsasında işləyən psevdotəsadüfi ədəd formalaşdırıcısı. *Milli Aviasiya Akademiyasının Elmi məcmuələri.* Bakı. 2022. №1, s. 29-36 *(in Azerbaijan)*
5. **Englund H. and Johansson T.** A new distinguisher for clock controlled stream ciphers. In H. Gilbert and H. Handschuh, editors, Fast Software Encryption - FSE 2005, volume 3557 of Lecture Notes in Computer Science, *Springer-Verlag,* 2005. Pp. 181–195. *(in English)*
6. **Khazaei S., Fisher S., Meier W.** Reduced complexity attacks on the alternating step generator. Proceedings of SAC'07, , Berlin, Heidelberg, *Springer-Verlag,* pp. 1-16, 2007. *(in English)*
7. **Ndaw A., Djiby S., Sanghar.** Construction of Maximum Period Linear Feedback Shift Registers (LFSR) (Primitive Polynomials and Linear Recurring RelationsBritish Journal of Mathematics & Computer Science 11(4): 1-24, 2015, Article no.BJMCS.19442 ISSN: 2231-0851, p. 24*(in English)*
8. **Golic J., Menicocci R.** Correlation analysis of the Alternating Step Generator. Design, Codes and Cryptography, 31, pp. 51-74, *Kluwer Academic Publishers,* 2004. *(in English)*
9. **Rzaev H.N., Gasanov R.A.** Analiz protokolov bezopasnosti i dostovernosti v perspektivnyh sistemah predostavleniya uslug svyazi. *Vestnik Azerbajdzhanskoj Inzhenernoj Akademii*, 2016, T. 8, №4, s. 83-98 *(in Russian).*