PARADIGMA, No.2, 2025, səh.174-179
https://doi.org/10.30546/30015.2025.2.151

KRİPTOQRAFİK CƏHƏTDƏN GÜCLÜ PSEVDOTƏSADÜFİ NÖMRƏ GENERATORLARI

E.Q. Həsənov, A.E. Məmmmədzadə
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: agil.mammadzada@student.au.edu.az

Xülasə: Tədqiqat psevdo və kvazi-təsadüfi ədədləri analiz edir. Psevdo-təsadüfi ədədlər sürətli və sadədir, kriptoqrafiyada istifadə olunur, lakin təhlükəsizlik post-prosesləşdirmə tələb edir. Kvazi-təsadüfi ədədlər bölgələri optimal əhatə edir, inteqral qiymətləndirmə üçün faydalıdır. Hər iki növ müasir hesablamada və kriptoqrafiyada vacibdir, sistemlərin təhlükəsizliyini və dəqiqliyini artırır.

Açar sözlər: Psevdo-random ədədlər, Kvazi-təsadüfi ədədlər, Kriptoqrafiya, Statistik analiz, Monte Karlo metodu

Giriş

Rəqəmsal sahələrdə, məsələn, informasiya və kommunikasiya texnologiyalarında, kompüter təhlükəsizliyində, riyazi simulyasiyada, nümunə götürmədə, təsadüfi dəyişənlərin yaradılmasında və digər sahələrdə təsadüfi ardıcıllıq generatorlarının istifadəsi çox yayılmışdır. Bu generatorlar telefon rabitəsi siqnallarında və GPS sistemlərində istifadə olunur [7]. Əksər kriptoqrafik protokollar bəzi nöqtələrdə giriş olaraq təsadüfi ədədləri istifadə edir və ya onları axın şifrəsi sistemlərində açar kimi istifadə edir.

Ancaq təsadüfi ardıcıllıqların əldə edilməsi hesablamalı baxımdan sadə bir məsələ deyil. Çünki kompüterlər deterministik, yəni təlimatla idarə olunan maşınlardır, buna görə də "təsadüfi"lik yaradan alqoritmlərin yaradılması çətindir. Əməliyyatlar icra edilərkən təsadüfiymiş kimi görünə bilər, amma onların arxasında müəyyən bir əvvəlcədən təyin olunmuş naxış mövcuddur [1]. Buna görə də, "həqiqətən" təsadüfi məlumatları əldə etmək üçün daxili təsadüfi xüsusiyyətləri olan fiziki hadisələrə müraciət edirik: radioaktiv parçalanma, termal səs-küy, atmosfer hadisələri və s.

Bununla belə fiziki hadisələrdən məlumat əldə etmək nisbətən baha başa gəlir, buna görə də lazım olan təsadüfi ədədlərin tələb olunan miqdarını qısa vaxt ərzində əldə etmək mümkün olmur. Bəzən ya hesablama gücü çox aşağı olduğundan, ya da çox sayda təsadüfi ədədə qısa müddətdə ehtiyac duyulduğu üçün, məsələn, axın şifrələməsi kimi tətbiqlərdə sürətli və hesablama baxımından sadə generatorların yaradılması maraqlı olur [1].

Bu nöqtədə təsadüfi olmaq və ya təsadüf kimi görünmək anlayışını müəyyənləşdirmək vacibdir. Lüğəvi baxımdan təsadüfi olan şey şansa bağlı olandır. Daha rəsmi bir kontekstdə, təsadüfi ədədlərin ardıcıllığının ümumiyyətlə qəbul edilmiş tərifi Marsaqlia tərəfindən verilmişdir: təsadüfi ədədlərin ardıcıllığı, bütün mümkün qiymətlər üzrə vahid paylanmışdır,

hər bir ədəd əvvəlki ədədlərdən müstəqildir. Eyni şəkildə, təsadüfi ədəd generatoru da yuxarıda göstərilən tərifə uyğun olaraq təsadüfi ardıcıllıqlar yaradan sistem olaraq tərif oluna bilər. Lakin, təsadüfi ədədlərin müxtəlif tətbiq sahələri nəzərə alındığında, bu ardıcıllıqların bəzi xüsusiyyətlərə malik olması zəruri olacaqdır. Məsələn, statistikada tətbiqlər üçün tələb olunan şərtlər, kriptoqrafiyada tələb olunanlardan fərqli olacaq, çünki sonuncu halda ardıcıllığın proqnozlaşdırıla bilməməsi, yəni gözlənilməz olması vacibdir. Bu məqalədə, xüsusilə kriptoqrafik tətbiqlərə uyğun olan ədəd generatorlarının təhlilinə fokuslanacağıq [7].

Kriptoqrafik Tətbiqlər və Generatorların Əhəmiyyəti:

Bu işin məqsədi yalnız təsadüfi və psevdotəsadüfi ədədlərin nəzəri aspektlərini təhlil etməklə məhdudlaşmır. Eyni zamanda, kriptoqrafik tətbiqlərdə istifadə olunan generatorların xüsusiyyətləri, onların güvənliyi və səmərəliliyi də ətraflı şəkildə incələnəcəkdir. Kriptoqrafiyada istifadə edilən generatorların əsas xüsusiyyəti, onların kənar müdaxilələrdən və ya hər hansı bir riyazi metoddan istifadə etməklə qabaqcadan proqnozlaşdırıla bilməməsidir. Bu, xüsusən şifrələmə və məlumatın təhlükəsizliyinin təmin edilməsi sahəsində mühüm rol oynayır.

Təsadüfi ədədlərin təsnifatı

Təsadüfi ədədlərin müxtəlif növləri haqqında yaxşı tanınmış təsnifat üç əsas qrup təsadüfi ədəd növü müəyyən edir: "həqiqi" təsadüfi ədədlər, psevdotəsadüfi ədədlər və kvazi-təsadüfi ədədlər [7].

Həqiqi Təsadüfi Ədədlər - Bu ədədlər təxmin edilə bilməyən bir girişlə yaradılır və təsadüfi bir fenomenin entropiyasından istifadə olunur, məsələn, kompüter saatı və ya fotoelektrik dalğalanmalar. Çünki bu ədədlər təxmin edilə bilməzdir və onlardan əvvəl yaradılmış ədədlərin dəyərini bilmək üçün heç bir qayda mövcud deyil, onlar şifrələmə sistemlərində olduqca faydalıdır. Bu növ ədədlərin ardıcıllığının yaradılmasında iki əsas amil rol oynayır:

Təxmin edilə bilməyən resurs (yüksek entropiya ilə): Bu resursdan istifadə edərək təsadüfi ədədlər yaradılır. Resursun entropiyası bir ölçü ilə qiymətləndirilir ki, bu da *min-entropy* adlanır. Min-entropy, ən böyük k ədədini təyin edir ki, bu şərt yerinə yetirilsin:

$$P[X=x] \leq 2^{-k} P[X = x] \leq 2^{-k} P[X=x] \leq 2-k$$

Burada XXX resursu təmsil edir (min-entropy, Shannon entropiyasından daha sərt bir ölçüdür, çünki min-entropy hər zaman Shannon entropiyasından kiçik və ya bərabərdir. Bu amil kritik əhəmiyyət daşıyır, çünki o, mövcud olan entropiyanı müəyyən edir. Bəzi resurslar qərəzli ola bilər, buna görə də onları çıxarmaq və ya post-emal addımı tətbiq etmək lazım gəlir.

“Yığılma” mexanizmi. Bu mexanizm yüksək entropiya resursundan maksimum mümkün entropiyanı yığmağa çalışan bir funksiyadır. İkinci komponentin məqsədi, bütün yüksək entropiyalı resurslarla işləyə biləcək bir mexanizm tapmaqdır. Bəzən bu ardıcıllıqların yaradılmasında algoritmləri gücləndirmək məqsədilə bir post-emal komponenti tətbiq etmək lazım olur. Bu, ya entropiya mənbəyinin və ya mexanizmin qüsurlarını maskalamaq, ya da dəyişikliklər və manipulyasiya hallarında dözümlülük təmin etmək üçün edilir [2].

Psevdotəsadüfi ədədlər. Psevdotəsadüfi ədədlər müəyyən bir başlanğıc şərti (seed) ilə təyin olunan riyazi bir alqoritm vasitəsilə yaradılır. Bu proses, müəyyən bir ardıcıllığın təkrarlanan və deterministik şəkildə yaranmasını təmin edir. Başlanğıc şərt (seed) müəyyən olunduqdan sonra ardıcıllıq nəzarət edilə bilən və periodik bir şəkildə təkrarlanır. Bu prosesin məqsədi, həqiqi təsadüfi ədədləri təqlid etməkdir.

Bir uyğun formul və yetərincə yaxşı seçilmiş bir başlanğıc şərti ilə, psevdotəsadüfi ədədlər ardıcıllığı əldə edilə bilər ki, bu ardıcıllıq praktik olaraq "həqiqətən təsadüfi" olaraq qəbul edilə bilər [5]. Bunun səbəbi bu ardıcıllığın statistik testlərdən (məsələn, test suite və ya test batareyası) uğurla keçə bilməsidir. Bu testlər ardıcıllığın təsadüfi olma xüsusiyyətini yoxlamaq üçün istifadə olunur və onun təkrar ola bilməyən, müəyyən bir naxışa malik olmadığına əmin olmaq məqsədini güdür.

Tətbiq Sahələri:

Psevdotəsadüfi ədədlər həm statistikada, həm də kriptoqrafiyada geniş istifadə olunur. Statistikada, məsələn, nümunə götürmə və simulyasiya metodlarında bu ədədlərdən istifadə edilir [5]. Kriptoqrafiyada isə şifrələmə və açar idarəetmə sistemlərində güclü və proqnozlaşdırıla bilməyən təsadüfi ədədlər lazım olduğu üçün, psevdotəsadüfi ədədlərin təhlükəsizliyi xüsusilə mühüm rol oynayır.

Psevdotəsadüfi Generatorların İstifadəsi:

Psevdotəsadüfi generatorların yaradılması və istifadəsi, uyğun alqoritmalar və statistik testlərlə təmin olunmuş generatorların seçilməsi tələb edir. Bu generatorlar təkrarlanmayan və proqnozlaşdırıla bilməyən ardıcıllıqlar yaratmağa çalışır. Bu xüsusiyyətlər, məsələn, şifrələmə və digər təhlükəsizlik tətbiqlərində çox vacibdir. Əgər psevdotəsadüfi generator təkrarlanır və ya əvvəlcədən təxmin edilə bilirsə, şifrələmə sisteminin təhlükəsizliyi ciddi şəkildə pozula bilər [7].

Psevdotəsadüfi generatorların əsas üstünlüyü onların sürətindədir; bu generatorlar çox sürətli və hesablama baxımından çox sadədirlər. Buna görə də, böyük miqdarda təsadüfi ədəd tələb olunan tətbiqlərdə (məsələn, şifrələmə sistemlərində), bu tip generatorlar istifadə olunur.

Lakin, təhlükəsizlik tətbiqlərində, ən yaxşı nəticəni əldə etmək üçün, generatorun və seed seçiminin ciddi şəkildə təhlil edilməsi və qiymətləndirilməsi vacibdir.

Psevdotəsadüfi ədədlərin Təhlükəsizliyi və Post-Emal Texnikaları:

Psevdotəsadüfi ədədlərin təhlükəsizliyi, onların şifrələmə sistemlərində istifadəsi üçün əsas şərtdir. Güclü və proqnozlaşdırıla bilməyən psevdotəsadüfi generatorlar yalnız təsadüfi olma xüsusiyyətinə deyil, həm də müdaxiləyə qarşı dözümlü olmalıdır. Psevdotəsadüfi generatorlar üçün post-emal metodlarının tətbiqi, onların xüsusiyyətlərini gücləndirə və zəifliklərini aradan qaldıra bilər. Məsələn, kriptoqrafik hash funksiyaları, Von Neumann düzəldiciləri və digər çıxarış funksiyaları psevdotəsadüfi ədədlərin keyfiyyətini artırmaq və onları daha güclü etmək üçün istifadə edilə bilər.

Bu post-emal texnikaları, xüsusən kriptoqrafik tətbiqlərdə, çox vacibdir, çünki hər hansı bir zəiflik və ya naxışın varlığı, sistemin təhlükəsizliyini ciddi şəkildə təhdid edə bilər. Post-emal tətbiq edilərkən, ardıcıllığın statistik xüsusiyyətlərinin pozulmaması və generatorun təkrarlanmaması təmin edilməlidir.

Kvazi-Təsadüfi Ədədlər (Low-Discrepancy Points)

Kvazi-təsadüfi ədədlər, digər adı ilə "aşağı uyğunsuzluq nöqtələri", təsadüfi ədədlərdən fərqli olaraq, təsadüfi olmağı hədəfləməyən, lakin statistik xüsusiyyətləri ilə təsadüfi ardıcıllıqlara oxşayan bir sıra nöqtələrdən ibarətdir. Bu ədədlər ardıcıllığı, uyğun olan regionu ən optimal şəkildə örtmək məqsədini güdür. Bu, o deməkdir ki, kvazi-təsadüfi ardıcıllıqlar bir sıra nöqtələrdən ibarətdir və bu nöqtələr müəyyən bir ölçüdə yerləşdirilmişdir, belə ki, bu nöqtələr uyğun paylanma şərtlərini təmin edir.

Kvazi-təsadüfi ardıcıllıqlar təsadüfi ədədlər deyil, lakin bu nöqtələr müəyyən bir inteqralın ədədi qiymətləndirilməsi üçün istifadə olunduqda, onların statistik xüsusiyyətləri təsadüfi ardıcıllıqlarla müqayisə edilə bilər [6]. Kvazi-təsadüfi ardıcıllıqların məqsədi, müvafiq məkanın mümkün olan hər hissəsini mümkün qədər bərabər şəkildə əhatə etməkdir, bu da onları əsasən nömrələrin deyil, nöqtələrin ardıcıllığı kimi müəyyən edir.

Bu nöqtələrin paylanması müəyyən bir **ekvidistribusiya (eşit paylanma)** kriteriyasını təmin edir və onların əsas tətbiqi inteqralların ədədi qiymətləndirilməsidir. Məsələn, Monte-Karlo metodlarında təsadüfi nöqtələrdən istifadə olunsa da, kvazi-təsadüfi nöqtələr daha sürətli və daha dəqiq nəticələr verə bilər. Kvazi-təsadüfi ədədlər, nümunə götürmə prosesində daha optimal bir yanaşma təmin edərək, inteqralın daha az sayda nöqtə ilə düzgün qiymətləndirilməsini təmin edir [6].

Nəticə

Bu məqalədə psevdotəsadüfi və kvazi-təsadüfi ədədlərin yaradılması, xüsusiyyətləri və müxtəlif tətbiq sahələrindəki istifadəsi təhlil edilmişdir. Psevdotəsadüfi ədədlər müəyyən bir başlanğıc şərtindən (seed) asılı olaraq periodik şəkildə yaradılır və bu ardıcıllıqlar müəyyən statistik testlərdən keçərək praktik olaraq təsadüfi ədədlər kimi qəbul edilə bilər. Kriptoqrafiya və statistik analiz sahələrində geniş istifadə olunan bu generatorlar, xüsusilə sürət və hesablama sadəliyi ilə önə çıxır. Lakin bu generatorların zəifliklər, xüsusən kriptoqrafik tətbiqlərdə ciddi təhlükəsizlik riskləri yarada bilər. Buna görə də bu generatorların təhlükəsizliyini təmin etmək üçün müvafiq post-emal texnikalarının tətbiqi əhəmiyyətlidir.

Kvazi-təsadüfi ədədlər, digər tərəfdən, təsadüfi ədədlərlə oxşar statistik xüsusiyyətlərə malik olmaqla yanaşı, mümkün olan regionu daha optimal şəkildə əhatə edir. Bu nöqtələr, inteqral qiymətləndirmə və nümunə götürmə metodlarında xüsusilə faydalıdır, çünki onlar daha az sayda nöqtə ilə daha dəqiq nəticələr təmin edir. Kvazi-təsadüfi generatorlar, yüksək ölçülü inteqral hesablamalarında Monte Carlo metodlarına effektiv alternativlər təqdim edir.

Bu araşdırma göstərdi ki, təsadüfi ədədlər və onların müxtəlif növləri müasir hesablama və kriptoqrafiya sahələrində kritik rol oynayır. Psevdotəsadüfi və kvazi-təsadüfi ədədlərin düzgün seçilməsi və tətbiqi, daha təhlükəsiz və daha dəqiq sistemlərin qurulmasına imkan verir. Gələcək tədqiqatlar, xüsusilə yeni alqoritmaların və post-emal texnikalarının inkişafına yönəlməli, bu generatorların gücünü və etibarlılığını daha da artırmalıdır.

Ədəbiyyat siyahısı

1. Chen, I.T.; Tsai, J.M.; Tzeng, J. Audio random number generator and its application. In Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, China, 10–13 July 2011; Volume 4, pp. 1678–1683.
2. Dhaou, I.B.; Skhiri, H.; Tenhunen, H. Study and Implementation of a Secure Random Number Generator for DSRC Devices. In Proceedings of the 2017 9th IEEE-GCC Conference and Exhibition (GCCCE), Manama, Bahrain, 8–11 May 2017; pp. 1–9.
3. Nguyen-Duc, A.; Viet Do, M.; Quan, L.; Nguyen Khac, K.; Nguyen Quang, A. On the adoption of static analysis for software security assessment-A case study of an open-source e-government project. Comput. Secur.2021, 111, 102470.
4. Choi, J. Physical Layer Security for Channel-Aware Random Access with Opportunistic Jamming. IEEE Trans. Inf. Forensics Secur.2017, 12, 2699–2711.

5. Tang, J.; Jiao, L.; Zeng, K.; Wen, H.; Qin, K.Y. Physical Layer Secure MIMO Communications Against Eavesdroppers with Arbitrary Number of Antennas. *IEEE Trans. Inf. Forensics Secur.***2021**, *16*, 466–481.
6. Gedam, S.; Beaudet, S. Monte Carlo simulation using Excel(R) spreadsheet for predicting reliability of a complex system. In Proceedings of the Annual Reliability and Maintainability Symposium, 2000 Proceedings, International Symposium on Product Quality and Integrity (Cat. No.00CH37055), Los Angeles, CA, USA, 24–27 January 2000; pp. 188–193.
7. Gergely, A.M.; Crainicu, B. A succinct survey on (Pseudo)-random number generators from a cryptographic perspective. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017; Volume 42, pp. 1–6.

CRYPTOGRAPHICALLY STRONG PSEUDORANDO NUMBER GENERATORS

E.G.Hasanov, A.E.Mammadzade
Azerbaijan University, Jeyhun Hajibeyli, 71, Baku, Azerbaijan

Abstract. This study analyzes pseudo-random and quasi-random numbers. Pseudo-random numbers are fast and simple, used in cryptography, but require post-processing for security. Quasi-random numbers optimally cover regions and are useful for integral estimation. Both types are crucial in modern computing and cryptography, enhancing system security and accuracy.

Keywords: Pseudo-random numbers, Quasi-random numbers, Cryptography, Statistical analysis, Monte Carlo methods