Electronic and Cyber Defens
Vol. 13, No.3, 2025 (Serial No. 51) .pp.61-73
ISSN: 2322-4347 , E-ISSN: 2980-8979

Design and Evaluation a new Pseudorandom Number Generator based on Chaotic Maps

Sanaz nazari [1], Abdul Rasool mirghadri [2*]

1 PhD student, Department of Mathematics, Faculty of Basic Sciences, Khwarazmi University, Tehran, Iran. Email: sanaz.nazri@gmail.com

2 Associate Professor Imam Hossein University , Tehran, Iran(*Correspondence: amrghdri@ihu.ac.ir)

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 09 July 2025

Received in revised form: 29 August 2025

Accepted: 14 October 2025

Available online: 23 October 2025

Keywords: Random Number Generator, Quadratic Congruential Generator, Logistic Chaos Map, Pseudorandom Number Generator, NIST Statistical Tests.

GRAPHICAL

In computer science and cyber security, random numbers play a prominent and effective role in some applications such as authentication, secret key generation, game theory, and simulation. Considering the difficult challenges of generating true random numbers, generating pseudorandom numbers is suitable and cost-effective solution. In cryptography schemes, high quality pseudo-random number generators are seriously needed to make password keys. The better the quality of the encryption keys, the stronger and more secure the encryption algorithm will be. It can be said that almost all cryptographic systems are highly dependent on generating high-quality random numbers. In this paper, a new generator for generating pseudorandom numbers is first designed by combining several chaotic maps using $\oplus$ and transition operators. Then, by performing statistical tests of correlation coefficient, goodness of fit, and NIST standard tests, and the evaluation criteria presented in [1], the appropriate quality of the proposed new generator is evaluated for cryptographic applications in terms of independence, data uniformity, and the degree of randomness of the generator output. Finally, it is compared with several other generators.

Cite thisarticle: S. Nazari ,A. R.Mirghadri.," Design and Evaluation a new Pseudorandom Number Generator based on Chaotic Maps," Electronic and Cyber Defens, vol. 13(3), pp. 61-73, 2025. DOI: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.7.6.

Publisher: Imam Hossein University.

«پدافند الکترونیک و سایبری»
سال سیزدهم، شماره ۳،پاییز ۱۴۰۴؛ ص ۷۳-۶۱
شاپا الکترونیکی: ۴۳۴۷-۲۳۲۲ شاپا چاپی: ۸۹۷۹-۲۹۸۰

طراحی و تحلیل یک مولد اعداد شبه تصادفی بر اساس نگاشت‌های آشوبی

ساناز نظری[۱]، عبد الرسول میر قدری[۲*]

[۱] دانشجوی دکتری، دانشکده علوم پایه، دانشگاه خوارزمی، تهران، ایران sanaz.nazri@gmail.com

[۲] دانشیار گروه ریاضی، دانشگاه امام حسین(ع)، تهران، ایران (نویسنده مسئول) amrghdri@ihu.ac.ir

چکیده

در علوم رایانه و امنیت فضای مجازی، اعداد تصادفی در برخی از کاربردها مانند احراز هویت، تولید کلید مخفی، نظریه بازی-ها و شبیه سازی نقشی برجسته و مؤثری دارند. با توجه به چالش های سخت تولید اعداد تصادفی واقعی، تولید اعداد شبه تصادفی راه¬کاری مناسب و مقرون به‌صرفه است. در طرح‌های رمزنگاری برای ساخت کلیدهای رمز نیاز جدی به مولدهای اعداد شبه تصادفی باکیفیت بالا است. هراندازه که کیفیت کلیدهای رمز بهتر باشد، الگوریتم رمزنگاری قوی‌تر و مطمئن‌تر خواهد بود. به‌طورقطع می‌توان گفت که تقریباً همه سامانه‌های رمزنگاری به‌شدت به تولید اعداد تصادفی باکیفیت بالا وابسته هستند. در این مقاله، ابتدا با ترکیب چند نگاشت آشوبی با استفاده از عملگرهای $\oplus$ و انتقال، یک مولد جدید برای تولید اعداد شبه تصادفی طراحی می‌شود. سپس با انجام آزمون‌های آماری ضریب همبستگی، نیکویی برازش و آزمون های استاندارد موسسه NIST، و معیارهای ارزیابی مطرح در [۱]، کیفیت مناسب مولد جدید پیشنهادی، ازنظر استقلال، یکنواختی داده ها و میزان تصادفی بودن خروجی مولد، برای کاربردهای رمزنگاری ارزیابی می شود. درنهایت با چند مولد دیگر مقایسه می‌گردد.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۰۴/۱۸

بازنگری: ۱۴۰۴/۰۶/۰۷

پذیرش: ۱۴۰۴/۰۷/۲۲

ارائه آنلاین: ۱۴۰۴/۰۸/۰۱

کلید واژه ها:

مولد اعداد شبه تصادفی،

نگاشت آشوبی همنهشت درجه‌دو،

نگاشت آشوبی لجستیک،

آزمون‌های آماری NIST

....

استناد: نظری, ساناز, میرقدری, عبدالرسول. (۱۴۰۴). طراحی و ارزیابی یک مولد اعداد شبه تصادفی بر اساس نگاشت های آشوبی. پدافند الکترونیکی و سایبری, ۱۳(۳), ۷۳-۶۱. DORhttps://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.7.6

ناشر: دانشگاه جام امام حسین(ع).

۱- مقدمه

در جهان هستی برخی از پدیده‌های فیزیکی، نتایجی غیرقطعی و غیرقابل‌پیش‌بینی دارند که به پدیده‌های تصادفی معروف‌اند مانند تشعشعات کیهانی، آب‌وهوای فردا، پرتاب سکه، ریختن تاس و غیره. اگر فردی یک تاس را تکان داده و داخل یک سبد بریزد، عددی که مشاهده می‌شود از قبل مشخص نبوده و بر اساس احتمال یکنواخت بوده که به آن عدد تصادفی می‌گویند.

در سال‌های ۱۹۴۰، با ظهور رایانه‌ها، شیوه تولید اعداد تصادفی تغییر کرد. شرکت راند[1] اقدام به ساخت ماشینی کرد که می‌توانست اعداد تصادفی را بر اساس پالس‌های الکترونیکی تولید کند. آن‌ها نتایج اعداد تصادفی تولیدشده را در کتابی با عنوان «یک‌میلیون اعداد تصادفی با انحراف نرمال ۱۰۰ هزار[2]» به چاپ رساندند. این کتاب دوباره در سال ۲۰۰۱ تجدید چاپ شد.

یک رایانه دیگر نیز به نام ارنی[3] در دهه ۵۰ میلادی به تولید اعداد تصادفی پرداخت. از این اعداد به‌منظور قرعه‌کشی و تولید کدهای مربوط به کارت‌های بخت‌آزمایی استفاده می‌شد. به اعداد حاصل از انجام یک رخداد یا آزمایش تصادفی، دنباله اعداد تصادفی و دستگاه تولیدکننده اعداد تصادفی را مولد اعداد تصادفی گویند. مولدها برای اهداف رمزنگاری بایستی امن و مطمئن باشند یعنی ایمن ازنظر رمزنگاری باشند.

مولدهای اعداد تصادفی امن ازنظر رمزنگاری باید دنباله‌ای از اعداد تصادفی را به نحوی تولید کنند که رفتار آماری خوبی داشته و این دنباله‌های تولیدشده نباید قابل پیش‌بینی و دست‌کاری باشند. در طرح‌های رمزنگاری، به دلایل حساسیت امنیتی، کلیدهای رمزنگاری و سایر داده‌های حیاتی باید در داخل ماژول‌های رمزنگاری و به‌ویژه در داخل دستگاه‌های نیمه‌رسانا تولید شوند. اگر ماژول رمزنگاری به‌عنوان یک دستگاه رمزنگاری روی یک تراشه (به‌عنوان‌مثال در کارت‌های هوشمند) پیاده‌سازی شود، بنابراین ما فقط با مولدهایی سروکار داریم که در دستگاه‌های دیجیتال قابل پیاده‌سازی هستند.

۱,۱ اعداد تصادفی و انواع آن

به لحاظ مفهومی می‌توان مولد اعداد تصادفی را دستگاهی دانست که دنباله اعداد را به نحوی تولید می‌کند که ارقام بعدی این دنباله قابل پیش‌بینی نباشند. ممکن است چنین دستگاهی بر مبنای رخدادهای تصادفی فیزیکی یا شیمیایی به تولید اعداد تصادفی بپردازد (مثل رایانه ارنی)، که این مولدها را به‌اختصار HRNG[4] می‌گویند. معمولاً پدیده‌های تصادفی به‌کاررفته در این دستگاه‌ها وابسته به دما، اشعه کاتدی، تشعشعات و شرایط فیزیکی هستند که اعداد تولیدشده توسط چنین دستگاه‌هایی معمولاً به نام TRNG[5] معروف‌اند. ممکن است دستگاه تولید اعداد تصادفی بر اساس روش‌های نرم‌افزاری و الگوریتم‌های شبیه‌سازی عمل کند که این‌گونه ارقام را «اعداد شبه تصادفی[6]» و دستگاه را «مولد اعداد شبه تصادفی یا PRNG[7]» می‌گویند [۲].

۲,۱ کاربردهای اعداد تصادفی

مولدهای اعداد تصادفی (RNG) کاربردهای زیادی دارند. به‌عنوان نمونه: بازی‌های سرگرمی، که در آن قرعه‌کشی‌ها و ماشین‌های قمار بر اساس استفاده از اعداد تصادفی هستند، بازی‌های ویدیویی اعداد تصادفی را برای تأثیرگذاری بر ابتکارات هوشی[8] یا برای تغییر دادن بازی، موسیقی و ترکیب گرافیکی با آمیختن محتوا بابیت‌های تصادفی به کار می‌برند، مدل‌های پیچیده علمی و مالی که از اعداد تصادفی برای شبیه‌سازی استفاده می‌کنند. برنامه‌های کاربردی هوش مصنوعی که به داده‌های تصادفی برای تعیین صحت طبقه‌بندی یا رفتار شبکه عصبی نیاز دارند، تولیدکنندگان نرم‌افزار از داده‌های تصادفی برای آزمایش برنامه‌ها و الگوریتم‌ها برای شناسایی باگ‌ها، حل معادلات، رمزنگاری، امضای دیجیتال، احراز هویت در پروتکل‌های ارتباطی و غیره استفاده می‌کنند.

تا قبل از به‌کارگیری اعداد تصادفی در اینترنت، محیط مرورگرها امن نبود تا اینکه در سال ۱۹۹۵ پروتکل SSL و روش‌های رمزنگاری اطلاعات در اینترنت توسط الگوریتم پیشرفته PRNG معرفی شد. در بیشتر CPUهای رایانه‌های دهه ۹۰ میلادی، دستورالعملی برای تولید اعداد تصادفی وجود نداشت و با الگوریتم‌هایی که بر مبنای بذر (Seed) کار می‌کردند اعداد شبه تصادفی تولید می‌شد. به همین علت سرورهای وب Netscape از ترکیب ID و زمان استفاده کاربر، برای تولید بذر استفاده می‌کردند. در این میان فیلیپ بیکر[9] به‌عنوان یک دانشمند علوم رایانه کشف کرد که یک هکر می‌تواند به‌عنوان یک مهاجم، با استفاده از حدس‌های مختلف برای مقدار بذر و محاسبات ساده، به رمزهای رایانه‌ها دسترسی پیدا کند.

[1] RAND
[2] A Million Random Digits with 100000 Normal Deviates
[3] ERNIE
[4] Hardware Random Number Generators
[5] True Random Number Generators
[6] Pseudo-Random Numbers
[7] Pseudo-Random Number Generators
[8] Intelligence heuristics
[9] Phillip Hallam-Baker

در سال ۱۹۹۹، شرکت اینتل یک مدار الکترونیکی تولید اعداد تصادفی بر روی سرور i810 خود قرارداد. این مدار بر اساس تغییرات دما، به تولید اعداد تصادفی واقعی می‌پرداخت. متأسفانه دستگاه‌ها و روش‌های تولید اعداد تصادفی واقعی (TRNG) نسبت به روش‌های شبه تصادفی (PRNG) کند تر و پرهزینه‌تر هستند به همین دلیل الگوریتم‌های تولید اعداد شبه تصادفی از محبوبیت بیشتری (البته با دقت کمتری) نسبت به روش‌های واقعی برخوردارند.

در سال ۲۰۱۲ شرکت اینتل بر مبنای همان روشی که در i810 ارائه داده بود، دو دستورالعمل RDRAND و RDSEED را به‌عنوان روش TRNG معرفی کرد که با نرخ ۵۰۰ مگابایت در ثانیه اعداد تصادفی را تولید می‌کند. امروزه دستگاه‌های تولید اعداد تصادفی واقعی(TRNG) به‌صورت سخت‌افزارهای متن‌باز نیز قابل‌دستیابی هستند. ریدوبلر[1] یکی ازاین‌گونه برنامه‌ها است که کد آن در GitHub(±) قابل‌دسترس است .

هدف این پژوهش، طراحی و ارزیابی یک مولد اعداد شبه-تصادفی بر اساس نگاشت‌های آشوبی است. ساختار مابقی مقاله بدین شرح است که در بخش دوم مفاهیم اساسی و کارهای مرتبط معرفی می‌شوند. در بخش سوم یک مولد جدید برای تولید اعداد شبه تصادفی طراحی و پیشنهاد می‌گردد. در بخش چهارم مولد پیشنهادی از جهات آماری توسط آزمون‌های استاندارد تحلیل می‌شود. در بخش پنجم مولد پیشنهادی با چند مولد دیگر ازنقطه‌نظر تصادفی بودن مقایسه می‌شوند. درنهایت نتیجه گیری موضوع در بخش ششم ارائه می‌شود.

۲. مفاهیم اساسی و کارهای مرتبط

ازلحاظ مبانی نظری، در اصل یک مولّد اعداد شبه تصادفی، الگوریتمی است که دنباله‌ای از اعداد را به نحوی تولید می‌کند که خروجی خیلی نزدیک به تصادفی داشته باشند. درواقع دنباله‌ی تولیدشده توسط مولد شبه تصادفی، تصادفی واقعی نبوده و تقریباً" تصادفی است. تعریف دقیق مولد شبه تصادفی به‌صورت زیر بیان می‌شود.

تعریف ۲-۱. یک مولد شبه تصادفی عبارت است از یک الگوریتم زمان چندجمله‌ای قطعی G که در دو شرط زیر صدق کند:

الف) گسترش: تابعی مثل $L:N\rightarrow N$ موجود باشد که برای هر $n\in N$، $L(n)>n$ و برای هر $S\in\{0,1\}^*$ داشته باشیم $|G(S)|=L(|S|)$ یعنی برای هر $S\in\{0,1\}^*$ با طول $|S|$ مولد یک‌رشته دودویی $G(S)$ با طول $L(|S|)$ تولید کند.

ب) شبه تصادفی بودن: گردایه $\{G(U_n)\}_{n\in N}$ شبه تصادفی به این معنی است که برای هر الگوریتم زمان چندجمله‌ای احتمالی A و برای هر چندجمله‌ای مثبت p و برای همه nهای به‌قدر کافی بزرگ داشته باشیم:

$$|Pr(A(G(U_n),1^n)=1)-Pr(A(G(U_{L(n)}),1^n)=1)|<\frac{1}{p(n)} \quad (۱)$$

بسیاری از برنامه‌های امنیتی مبتنی بر مولد اعداد شبه تصادفی است. اعداد باینری تصادفی یک قسمت اساسی در بسیاری از الگوریتم‌های امنیت شبکه است. به‌عنوان‌مثال ، سامانه‌های رمزنگاری رایج به یک کلید پویا طولانی نیاز دارند که باید از یک کلید مخفی کوتاه تولید شود و دارای رفتار تصادفی باشد. ورودی‌های تصادفی یا شبه تصادفی در بسیاری از پروتکل‌ها که نیاز به تولید کلیددارند، یک الزام مهم هستند. مولد اعداد شبه تصادفی، یک الگوریتم قطعی است که دنباله‌ای از بیت‌ها تولید می‌کند که رفتار دنباله اعداد واقعاً تصادفی را شبیه‌سازی می‌کند.

مولدهای اعداد تصادفی به سه دسته کلی زیر تقسیم می‌شوند:

الف) مولدهای اعداد تصادفی واقعی یا به‌اختصار TRNG's

ب) مولدهای اعداد شبه تصادفی یا به‌اختصار PRNG's

ج) مولدهای اعداد تصادفی گوسی یا به‌اختصار QRNG's[2]

مولدهای PRNG (دنباله‌های با ویژگی اختلاف زیاد) با توجه به مقدار اولیه‌ای(بذر) که به آن‌ها داده می‌شود، اعدادی شبه تصادفی تولید می‌کنند. پس همیشه می‌توان با تغییر مقدار اولیه دنباله‌ای متفاوت از اعداد قبلی تولید کرد و با دانستن آن مقدار اولیه آن دنباله را مجدد بازتولید نمود. هدف این مولدها، تولید اعداد با سرعت زیاد و پیچیدگی زمانی مناسب است به‌طوری‌که پراکندگی مناسبی هم داشته باشند.

(دنباله‌های با ویژگی اختلاف کم)، همواره QRNGاما مولدهای دنباله‌ای ثابت از اعداد تولید می‌کنند که برای راحتی می‌توان یک‌بار این اعداد را تولید کرده و برای همیشه از آن‌ها در محاسبات استفاده کرد. هدف این مولدها، تولید اعدادی با پراکندگی زیاد است تا کل فضای حالت را پوشش دهند. این‌ها به نحوی طراحی می‌شوند که از یکنواختی بالایی در فضای چندبعدی برخوردار باشند، اما برخلاف اعداد شبه تصادفی ازنظر آماری مستقل نیستند.

[1] REDOUBLER

[2] Quasi-Random Number Generators

دنباله‌های با ویژگی اختلاف زیاد از جهات مختلف نسبت به دنباله‌های با ویژگی اختلاف کم برتری دارند، مهم‌ترین مزیت استفاده از این دنباله‌ها علاوه بر پراکندگی زیاد و فرضیات یکنواخت آماری اعداد تولیدشده، پیچیدگی زمانی مناسب آن است [۳].

مولدهایی مانند میان مربعی، میان ضربی، مضرب ثابت که به جهت معایب عمده‌ای که در آن‌ها وجود دارد، تقریباً منسوخ‌شده تلقی می‌شوند و همنهشتی جمعی و خطی و ضربی و مولد همنهشتی مرکب، همنهشتی درجه ۲ و همنهشتی درجه ۳ و مولد همنهشتی معکوس و ثبات‌های انتقال پس‌خور غیرخطی، ثبات‌های انتقال پس‌خور خطی و توابع آشوب گون از نوع PRNG و هم‌چنین مولدهایی مانند هالتون، فائور و سوبول از نوع QRNG می‌باشند.

۱,۲ مولد همنهشتی

روش‌های متعدد و مختلفی جهت تولید اعداد تصادفی وجود دارد که طی سالیان متمادی مورداستفاده قرار می‌گرفته است. از بین تمامی روش‌های ارائه‌شده، مولدهای همنهشتی برای تولید اعداد تصادفی بیش از سایر روش‌ها بکار رفته است. دنباله حاصل از مولد هم نشت خطی(LCG[1]) یکی از دنباله‌های با ویژگی اختلاف زیاد است، که توسط تابعی بازگشتی با مقدار اولیه‌ای خاص، اعداد تصادفی مناسبی را در زمان قابل‌قبول تولید می‌کند. مولد همنهشت خطی به‌صورت زیر تعریف می‌شود:

$$x_{i+1} = ax_i + b \mod m \qquad (۲)$$

به‌عنوان‌مثال یکی از مولدهای همنهشتی که مدت طولانی استفاده می‌شد عبارت است از [۴].

$$X_{i+1} = 19031X_i + 9298X_{i-1} \mod 65536 \qquad (۳)$$

اما مولد همنهشتی دیگری که ادعاشده تمامی آزمون‌های آماری را با موفقیت گذرانده است دنباله ذیل است [۵].

$$X_{i+1} = 107374182 + 104104480X_{i-4} \mod 2^{31} - 1 \qquad (۴)$$

برای معرفی مولد همنهشت درجه‌دو، فرض کنید $r \geq 1$ عدد صحیح باشد و مقادیر $p_1, p_2, \dots, p_r$ اعداد اول متمایز با شرط $p_i \geq 3$ و $\omega_1, \dots, \omega_r$ اعداد صحیح مثبت با شرط $\omega_i \geq 2$ باشند. به علاوه قرار دهید

$m = {p_1}^{\omega_1} \cdot \dots \cdot {p_r}^{\omega_r}$. سپس یک دنباله همنهشت درجه دوم $(z_n)_{n\geq 0}$ با عناصر $Z_m = \{0,1, \dots, m-1\} > \mathrm{m}$ اعداد صحیح بزرگ‌تر مساوی یک) و با انتخاب مقدار اولیه دلخواه z_0 و رابطه زیر تولید می‌شود.

$$z_{n+1} \equiv az_n^2 + bz_n + c \quad n \geq 0 \mod m \qquad (۵)$$

پارامترهای $a, b, c, z_0 \in Z_m$، که در آن $a \equiv 0 \pmod{p_i}$ و $b \equiv 1 \pmod{p_i}$

$c \not\equiv 0 \pmod{p_i}$ برای $1 \leq i \leq r$ و همچنین اگر m مضرب ۴ باشد آنگاه

$a \equiv b - 1 \pmod 4$ و اگر m مضرب ۹ باشد در این صورت $ac \not\equiv 3 \pmod 9$. دقیقاً برای انتخاب پارامترهای دنباله $(z_n)_{n\geq 0}$ حداکثر طول دوره ممکن m هست (اما توجه داشته باشید که اگر m مضرب ۹ باشد شرط $b \equiv 1 \pmod 9$ غیرضروری هست). در ادامه، همیشه فرض خواهد شد که این شرایط صادق هستند. دنباله $(x_n)_{n\geq 0}$ از اعداد شبه تصادفی همنهشتی درجه‌دو به‌صورت زیر تعریف می‌شود: $x_n = \frac{z_n}{m} \in [0,1)$ برای $n \geq 0$ [۶].

۲,۲ نگاشت‌های آشوبی

در نظریه آشوب نگاشت‌هایی که به شرایط اولیه بسیار حساس بوده و رفتاری گذرا داشته باشند را نگاشت آشوبی نامند که تعریف دقیق آن عبارت است از:

تعریف ۲-۲. نگاشت f در مجموعه فشرده S را آشوبی گوییم اگر و تنها اگر

الف) f به شرایط اولیه حساس است. یعنی برای هر شرط اولیه x و همسایگی U آن وجود دارد $\varepsilon > 0, y \in U$ و $n \in Z^+$، به‌طوری‌که $|f^n(x) - f^n(y)| > \varepsilon$، و

ب) f گذراست. یعنی برای هر مجموعه باز $\mathrm{U, V} \in \mathrm{S}$، وجود دارد $k \in Z^+$، داریم $f^k(U) \cap V \neq \emptyset$.

نظریه آشوب یکی از زمینه‌های جذاب تحقیقات ریاضی است که با سامانه‌های غیرخطی، قطعی و پویا سروکار دارد. در بسیاری از حوزه‌های مختلف مانند فیزیک، روباتیک، زیست‌شناسی، امور مالی و رمزنگاری کاربرد دارد. مهم‌ترین خصوصیات آشوب وابستگی زیاد به شرایط اولیه و تغییر پارامترها، ارگودیسیتی و رفتار شبه تصادفی است. این ویژگی‌ها، محققان را به سمت توسعه سامانه‌های ارتباطی امن آشوبی ترغیب می‌کند.

در رمزنگاری، از آشوب در زمینه‌های مختلف تولید کلید رمزگذاری، تولید دنباله‌های شبه تصادفی، توابع چکیده‌سازی، رمزنگاری تصویر و رمزنگاری متن، پروتکل‌های احراز اصالت و توافق کلید استفاده می‌شود.

[1] Linear Congruential Generator

نگاشت‌های آشوبی همان توابع ریاضی هستند که یک الگوی بسیار دلخواه بر اساس مقدار اولیه ایجاد می‌کنند. تولید اعداد شبه تصادفی مبتنی برنگاشت آشوبی را می‌توان در رمزگذاری چندرسانه‌ای، پویانمایی بازی‌های ویدئویی، بازاریابی دیجیتال، شبیه‌سازی سامانه‌های آشوب، سامانه‌های موشکی آشوب و سایر برنامه‌ها مورداستفاده قرارداد [۷] .

مولدهای شبه تصادفی از اهمیت ویژه‌ای در رمزنگاری به‌خصوص برای تولید دنباله کلید اجرایی در الگوریتم‌های رمز برخوردارند. سرعت تولید و پراکندگی زیاد از ویژگی‌های موردعلاقه دانشمندان در تولید اعداد شبه تصادفی است که با کشف پدیده آشوب و معادلات حاکم بر آن وارد مرحله جدیدی گشته است. در حقیقت ورود معادلات آشوب در مولدهای شبه تصادفی باعث به وجود آمدن حساسیت بسیار زیاد مولدها به مقدارهای اولیه شده است.

در سال‌های اخیر با ورود توابع آشوب به ساختار مولدهای تصادفی شاهد رشد چشمگیری در توسعه سامانه‌های تصادفی هستیم. اولین بار در سال ۱۹۸۹، ماتئوس [۱] اولین کسی بود که استفاده از نگاشت‌های آشوبی زمان- گسسته را برای اهداف رمزنگاری پیشنهاد کرد. در این روش یک نگاشت تک‌بعدی آشوبی با محدوده مشخص از شرایط اولیه و پارامترهای کنترلی برای تولید دنباله شبه تصادفی اعداد به‌منظور رمزگذاری و رمزگشایی پیام‌ها به‌کارگیری شد [۸]. پس‌ازآن در هابوتسو [۲] و همکاران یک سیستم رمزنگاری مبتنی برنگاشت آشوبی قطعه-ای– خطی تنت پیشنهاد دادند. در این طرح از نگاشت تنت به‌عنوان کلید محرمانه برای رمزنگاری و رمزگشایی پیام استفاده‌شده است [۹].

در ادامه توسعه مولدهای اعداد تصادفی مبتنی بر توابع آشوبی، استوجانوسکی [۳] و همکاران یک مولد شبه تصادفی ارائه نمودند که دنباله اعداد تصادفی را بر اساس سیگنال‌های آشوبی گسسته تولید می‌کرد [۱۰، ۱۱]. همچنین کوکارف [۴] و ژاکیموسکی [۵] امکانات متفاوتی از آشوب را برای تولید اعداد تصادفی ارائه کردند آن‌ها نوعی مولد شبه تصادفی آشوبی را ارائه کردند که امنیت آن به مسئله نظریه اعداد وابسته نبوده و در مقابل، امنیت آن به تعداد زیادی شاخه معکوس نگاشت آشوبی مورداستفاده در الگوریتم، وابسته است [۱۲]. مولدی بر اساس الگوریتم آشوب گونه تکه‌ای‌خطی توسط فو [۶] ساخته شد که در یک مسیر واحد، سامانه‌های آشوب گونه به هم متصل می‌شدند و نشان داده شد، با داشتن عملکرد مناسبی از این سامانه‌ها دنباله بسیار مناسبی از اعداد تصادفی تولید می‌شوند، که دارای دوره تناوب بلند و سرعت تولید بالا است [۱۳]. در سال ۲۰۰۵ یک ایده جدید از مولدهای تصادفی آشوب گونه بر اساس نگاشت مکانی-زمانی یک‌طرفه متشکل از نگاشت لجستیک توسط لیو [۷] مطرح شد که بر اساس مدل اصلاح‌شده سامانه‌های قبلی بود [۱۴]. پس‌ازآن یک مولد اعداد تصادفی آشوبی توسط وانگ [۸] و همکاران طراحی شد که بر اساس یک مدار آنالوگ بود [۱۵]. همچنین وانگ تولید اعداد تصادفی را بر اساس نگاشت z-logistic ارائه کرد به‌طوری‌که دنباله بیت‌های تصادفی بر اساس یک مدار آشوب گونه با دقت محاسباتی محدود تولید می‌شوند [۱۶]. ارگون [۹] و همکارانش نشان دادند که می‌توان دنباله تصادفی واقعی بیت‌ها را توسط یک نوسان‌ساز آشوبی غیر خودکار تولید کرد. آن‌ها یک مولد اعداد تصادفی واقعی دیجیتال بر اساس سامانه‌های زوج- آشوب (CCS-PRBG) پیشنهاد کردند و ویژگی‌های رمزنگاری موردمطالعه قرار گرفت. بیت‌های دنباله کلید خروجی CCS-PRBG، مستقل و هم توزیع(i.i.d) بوده و دنباله خروجی تصادفی است آن‌ها دنباله بیتی را از نگاشت استروبوسکوپیک پوانکاره [۱۰] که یک مدار الکترونیکی آشوب غیر خودکار است تولید کردند که دنباله‌های بیتی خروجی مدار آشوبی، بسته آزمون‌های FIPS-140-2 و بسته آزمون‌های NIST را گذراندند [۱۷]. در سال ۲۰۰۹ یک مولد اعداد تصادفی حقیقی بر اساس حرکت موشواره توسط هیو [۱۱] ارائه شد که قادر بود ۲۵۶ بیت تصادفی را با سرعتی خوب تولید کند [۱۸].

اخیراً، فیرات آرتوگر [۱۲] و همکارش، یک PRBG بر اساس سیستم آشوب چن با ابعاد بالا و ترکیبی از سه مختصات مسیر آشوب پیشنهاد کردند که نمای لیاپانوف بالایی داشت و آزمون‌های NIST و همبستگی را به‌خوبی گذرانده بود و فضای کلید کافی نیز دارد [۱۹]. فرانسوا و همکاران، یک الگوریتم شامل یک تابع آشوب را برای تولید دنباله‌های شبه تصادفی چندگانه توسعه داد. این الگوریتم از جایگشت‌هایی استفاده می‌کند که موقعیت‌های آن‌ها توسط یک تابع آشوب همنهشت خطی محاسبه و نمایه‌سازی می‌شوند. همچنین ونبو ژائو [۱۳] و همکارش یک مولد اعداد تصادفی بر اساس نگاشت لجستیک اصلاح‌شده ارائه داد که در رمزنگاری گفتار کاربرد دارد [۲۰].

[1] Matthews
[2] Habutsu
[3] Stojanovski
[4] Kocarev
[5] Jakimoski
[6] Fu
[7] Liu
[8] Wang
[9] Ergun
[10] Poincare
[11] Hu
[12] Firat Artuger
[13] Wenbo Zhao.

موسیس[1] و همکاران یک فن آشوب سازی پیشنهاد دادند که از آن می‌توان برای افزایش پیچیدگی هر نگاشت یک‌بعدی با افزودن عملگر باقی‌مانده و اصلاح پارامترهای نگاشت لجستیک به آن استفاده کرد [۲۱]. با استفاده از توابع آشوبی در رمزنگاری امکان تولید کلیدهایی با اندازه طولانی همراه با الگوریتمی ساده، سریع و ایمن فراهم‌شده است، همچنین با توجه به فضای بزرگ کلید در توابع آشوب این روش در برابر حملاتی چون حمله جستجوی فراگیر[2] نیز بسیار مقاوم است . آشوب به هر زبانی که ترجمه شود مفهوم آن دلالت بر رفتاری حساس به شرایط اولیه، تصادفی و غیرقابل‌پیش‌بینی دارد. در حقیقت بار معنایی این لغت دربرگیرنده به‌هم‌ریختگی ناخواسته و اغتشاش است. بااین‌حال در دنیای دانشمندان، این رفتار غیرقابل‌پیش‌بینی به‌هیچ‌وجه ناخواسته و بی‌دلیل نیست.

در ادامه تعدادی از نگاشت‌های آشوبی معروف را که می‌توان از آن‌ها برای تولید اعداد شبه تصادفی مطلوب استفاده نمود به‌اختصار معرفی می‌کنیم.

نگاشت لجستیک یک تابع آشوبی بسیار ساده است که تاکنون در حوزه نظری علوم کامپیوتر به‌عنوان مولدی ابتدایی برای تولید اعداد تصادفی مدنظر بوده است .

نگاشت لجستیک باوجود قدیمی بودن به دلیل سادگی فرمول و درعین‌حال رفتاری آشوب گونه در بازه‌ای خاص از پارمترهای آن هنوز هم به‌عنوان یک مولد اعداد شبه تصادفی مطرح است. اما درعین‌حال ارائه مولدهای جدید که بسیار قوی‌تر هستند به نحوی سبب کم‌رنگ‌تر شدن جایگاه نگاشت لجستیک درزمینهٔ تولید اعداد تصادفی شده است.

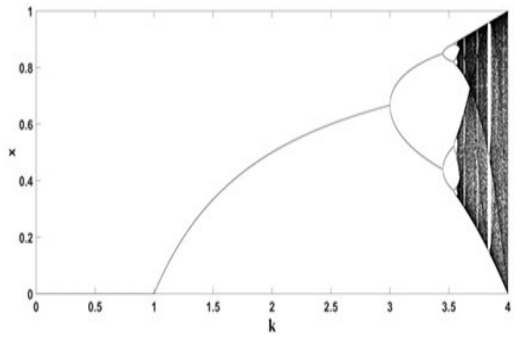
رابطه تابع لجستیک که در معادله زیر نشان داده‌شده است یک مدل از سامانه‌های دینامیک غیرخطی است که اغلب برای نشان دادن رشد بیولوژیکی جمعیت به کار می‌رود. در سال ۱۹۷۶مشخص شد که این مدل به‌ظاهر ساده دارای سیستم دینامیکی پیچیده‌ای است. امروزه الگوریتم لجستیک در زمینه‌های مختلفی ازنظریِ آشوب مانند آشوب در رمزنگاری، رشد بسیار زیادی داشته است. ضابطه تابع آشوبی لجستیک در حالت گسسته به‌صورت زیر است:

$$x_{n+1} = f(x_n) = ax_n(1 - x_n) \qquad (6)$$

x_0ام، n برای اندازه‌گیری جمعیت در نسل $x_n \in [0,1]$که نرخ رشد و عددی ثابت در محدوده aجمعیت اولیه و $a \in [3.5, 4]$.می‌باشند

[1] Mosis
[2] Brute force attack

نگاشت لجستیک یک نگاشت تک پارامتری هست که برای a=4، نمودار انشعاب و نمای لیاپانوف در زیر نشان داده‌شده است. نمودار دوشاخه‌ای برای شناسایی سریع مقادیر پارامتر کنترل که خروجی مناسب را برای یک برنامه خاص از نگاشت آشوب تولید می‌کند، بسیار مفید است.

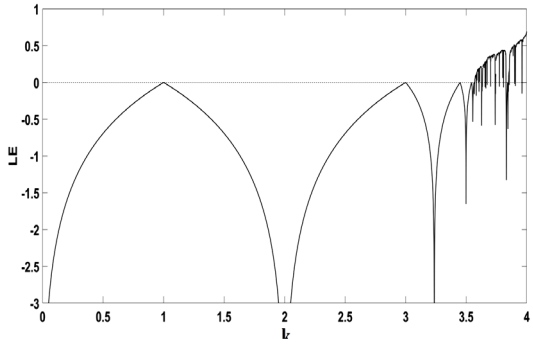


شکل (۱): نمودار دوشاخه‌ای نگاشت لجستیک [۲۱].

نمای لیاپانوف یک ابزار بسیار قوی برای شناسایی آشوب است. نمای لیاپانوف را می‌توان به‌عنوان نرخ متوسط واگرایی یا همگرایی نمایی مسیرهای بسیار نزدیک در فضای فاز تعریف کرد. هر سامانه‌ای که حداقل یک LE[3] مثبت داشته باشد به‌عنوان یک سیستم آشوب تعریف می‌شود و زمانی که دینامیک آن غیرقابل‌پیش‌بینی می‌شود، اندازه آن را در مقیاس زمانی منعکس می‌کند. LE برای یک نگاشت آشوب را می‌توان با استفاده از فرمول زیر محاسبه کرد:

$$\lambda = \frac{1}{n}\sum_{i=0}^{n-1} ln\left|\frac{dx_{n+1}}{dx_n}\right| \qquad (7)$$

بر اساس شکل، می‌توان دید که نمای لیاپانوف در نگاشت لجستیک زمانی که $k > 3.57$ بیشتر از ۰ است. در همین حال، برخی از نقاط کمتر از ۰ هست زمانی که $k\epsilon[3.57,3.9]$. اکثراً نماهای لیاپانوف مثبت می‌شوند وقتی $k\epsilon[3.9,4]$. بنابراین، نگاشت لجستیک رفتار آشوب پایدارتری دارد که .$k\epsilon[3.9,4]$ مشاهده می‌شود که بالاترین مقدار LE حدود ۰,۷ است.



شکل (۲): نمودار نمای لیاپانوف نگاشت لجستیک [۲۱].

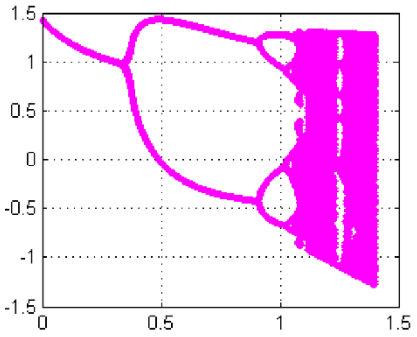
[3] Lyapunov exponent

نگاشت هنون برای اولین بار در سال ۱۹۷۶ توسط مایکل هنون معرفی شد که وی با ساده کردن بخش پوانکاره مدل لورنز به این فرمول رسید. نگاشت هنون، یک سیستم دینامیکی زمان گسسته است. این نگاشت یکی از پرکاربردترین سامانه‌های دینامیکی با رفتارهای آشوب گون به شمار می‌آید به‌طوری‌که بیشترین مطالعات در زمینه نگاشت‌های آشوب گون در مورد آن صورت پذیرفته است. معادله این نگاشت به‌صورت زیر است:

$$x_{n+1} = ax_n^2 - bx_{n-1} + 1 \qquad (۸)$$

فرمول این نگاشت وابسته به دو پارامتر a و b است که معمولاً مقادیر a=1.4 , b=0.3 در نظر گرفته می‌شود. به ازای این مقدار پارامترهای ذکرشده، نگاشت هنون رفتار آشوب‌گونه‌ای از خود نشان می‌دهد و البته به ازای مقادیر دیگری از این پارامترها هم ممکن است بازهم رفتار آشوب گونه از خود نشان دهد. اگر در نگاشت هنون برای ضرایب a و b شرط $a = \frac{3}{4}(1-b)^2$ برقرار باشد پدیده دوشاخه‌ای شدن رخ می‌دهد [۲۲-۲۳].

در شکل زیر نمودار دوشاخه‌ای شدن نگاشت هنون را مشاهده می‌کنید.

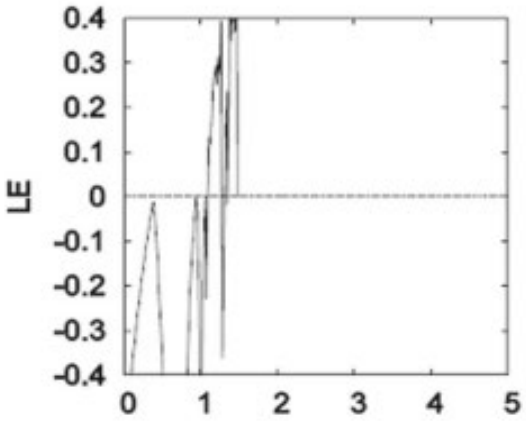


شکل (۳): نمودار دوشاخه‌ای شدن نگاشت هنون [۲۳].

برای نگاشت آشوب هنون نمی‌توان یک عبارت تحلیلی برای LE وابسته به a با استفاده از فرمول بالا به دست آورد. در شکل زیر مقدار تقریبی LE با 10^6 نمونه برای هر متغیر مستقل a با استفاده از نرم‌افزار TISEAN نشان داده‌شده است. انتظار می‌رود که یک سیستم آشوب غیرقابل‌پیش‌بینی‌تر می‌شود زمانی که مقدار LE مثبت آن افزایش می‌یابد.

از دیگر نگاشت‌های آشوبی می‌توان به نگاشت تنت(خیمه)، چبی‌شف، استاندارد، گربه(آرنولد)، نعل اسب[۱]، کوبیک[۲]، سینوسی[۳]، دایره[۴] و برنولی و گاوس[۵] و نگاشت لجستیک اصلاح‌شده [۱۸-۲۳] اشاره کرد. پس از تجزیه‌وتحلیل دقیق تمام ادبیات اخیر، ما دریافتیم که کمترین ضریب همبستگی ۰,۰۰۰۰۶ بود که توسط نگاشت آشوب ایکدا به دست آمد. بالاترین آنتروپی ۷/۵۹۹۹۹۹ بیت بر بایت با استفاده از نگاشت آشوب کوانتومی بود. کمترین زمان اجرای مشاهده‌شده ۲۳/. ثانیه با نگاشت آشوب زاسلاوسکی[۶] و بالاترین سرعت داده ۱۵,۳۶۷ مگابیت بر ثانیه با استفاده از نگاشت هاپیر آشوب بود [۲۱].

[1] Horseshoe map
[2] cubic
[3] sine
[4] circle
[5] Gauss map



شکل (۴): . نمودار نمای لیاپانوف نگاشت هنون [۲۳].

از دیگر نگاشت‌های آشوبی می‌توان به نگاشت تنت(خیمه)، چبی شف، استاندارد، گربه(آرنولد)، نعل اسب[۷]، کوبیک[۸]، سینوسی[۹]، دایره[۱۰] و برنولی و گاوس[۱۱] و نگاشت لجستیک اصلاح‌شده [۱۸-۲۰] اشاره کرد. پس از تجزیه‌وتحلیل دقیق تمام ادبیات اخیر، ما دریافتیم که کمترین ضریب همبستگی ۰,۰۰۰۰۶ بود که توسط نگاشت آشوب ایکدا به دست آمد. بالاترین آنتروپی ۷/۵۹۹۹۹۹ بیت بر بایت با استفاده از نگاشت آشوب کوانتومی بود. کمترین زمان اجرای مشاهده‌شده ۲۳/. ثانیه با نگاشت آشوب زاسلاوسکی[۱۲] و بالاترین سرعت داده ۱۵,۳۶۷ مگابیت بر ثانیه با استفاده از نگاشت هاپیر آشوب بود [۲۱].

در بخش بعد با ترکیب نگاشت‌های آشوبی به طراحی یک مولد جدید برای تولید دنباله اعداد تصادفی(مولد اعداد شبه تصادفی) برای کاربردهای رمزنگاری پرداخته و با آزمون‌های آماری، تصادفی بودن خروجی آن‌ها را تحلیل و ارزیابی خواهیم کرد.

۳. طراحی مولد جدید

چون به‌طور ذاتی باید خروجی مولدهای اعداد تصادفی طوری باشند که ارقام بعدی بر اساس خروجی‌های قبلی نا همبسته و غیرقابل‌پیش‌بینی باشند، لذا دنباله تولیدشده توسط هر PRNG

[6] Zaslavesky
[7] Horseshoe map
[8] cubic
[9] sine
[10] circle
[11] Gauss map
[12] Zaslavesky

باید ویژگی‌های زیر را داشته باشد: (۱) دنباله خروجی PRNG دارای رفتار آماری بسیار خوبی باشد. (۲) برای هر مقدار اولیه، دنباله خروجی PRNG دارای دوره تناوب کوتاه‌تر از قبلی نباشد. (۳) مقادیر متوالی دنباله دارای همبستگی خیلی ضعیف باشند.

مولد همنهشت درجه دوم $x_{i+1} = ax_i^2 + c \ mod\ p$ که p یک عدد اول و a و c اعداد صحیح در مد p می‌باشند. با دادن مقادیر مناسب به ضرایب و پارامترهای تابع همنهشتی درجه دوم می‌توان خواص آماری خروجی‌های آن را به‌طور قابل‌توجهی بهبود داد. در این معادلات، مقادیر a, c, p اعداد حقیقی‌اند و می‌توانند به‌صورت بهینه انتخاب شوند.

به‌عنوان نمونه می‌توان با انتخاب مقادیر $a = 2^{15} - 2^{10}$ و $c = 2^{31} - 1$، که بسیار هم مؤثر و کارا بوده دوره تناوب آن را افزایش داد، ولی بااین‌حال این مولد به‌تنهایی برای کاربردهای رمزنگاری و بالأخص به‌کارگیری در الگوریتم‌های رمز جریانی مناسب نیستند، زیرا دوره تناوب دنباله خروجی در این مولدها به‌اندازه کافی طولانی نیست و با احتمال زیادی دنباله اعداد تولیدشده به تکرار می‌رسد. برای غلبه بر این مشکل، یک تابع مولد که مبتنی بر ترکیب توابع همنهشتی درجه‌دو و توابع آشوبی است، پیشنهاد می‌شود. در دنباله خروجی این تابع مولد، هرگاه به یک مقدار تولیدشده تکراری رسیدیم آنگاه به‌جای به‌کارگیری آن عدد تکراری، از طریق تابع دیگری که می‌تواند یک نگاشت آشوبی باشد، یک عدد متفاوت جدید تولید کرده و تولید دنباله اعداد را با آن مقدار جدید غیرتکراری ادامه می‌دهیم. با این کار هیچ‌گاه در دنباله، تکرار نخواهیم داشت و به‌نوعی طول دوره تناوب دنباله خروجی را به شکل فوق‌العاده‌ای افزایش داده‌ایم. برای تولید این عدد غیرتکراری می‌توان از توابع مختلفی استفاده کرد. یکی از توابع مناسب نگاشت آشوبی لجستیک است که خواص آن در قضیه زیر آمده است [۲۲-۲۴].

قضیه ۳,۱- تابع آشوبی لجستیک نسبت به مقدار اولیه حساسیت زیادی دارد، نمای لیاپانوف آن مثبت بوده و نمودار آن دوشاخه‌ای است.

اثبات: بنا به تعریف ۲,۲ در خصوص نگاشت آشوبی، لذا تابع آشوبی لجستیک نسبت به تغییرات کوچک مقادیر اولیه حساسیت زیادی دارد. از طرفی با توجه به نمودار تابع لجستیک به ازای مقادیر مختلف $k = 4$ و (شکل ۲-۱)، مشاهده می‌شود که شکل دوشاخه‌ای است. با محاسبه نمای لیاپانوف از فرمول زیر

$$\lambda = \frac{1}{n}\sum_{i=0}^{n-1} ln \left|\frac{dx_{n+1}}{dx_n}\right|$$

دیده می‌شود که برای مقادیر $k > 3.57$ نمای لیاپانوف مثبت است.

یک دنباله دودویی را می‌توان با استفاده از رابطه زیر تولید کرد:

$$b_{n+1} = \begin{cases} 0 & if \quad x_{n+1} < q \\ 1 & if \quad x_{n+1} \geq q \end{cases} \qquad (۱۰)$$

که x_{n+1} با الگوریتم بالا محاسبه می‌شود. به‌طورمعمول مقدار آستانه q، ۰/۵ است. دنباله تولیدشده «شبه تصادفی» گفته می‌شود زیرا می‌توان همان دنباله را دقیقاً با استفاده از همان شرایط اولیه بازتولید کرد.

۳-۱ الگوریتم مولد جدید

با توجه به خواص و رفتار توابع آشوبی و مطالب بیان‌شده در بالا، برای تشدید رفتار آشوب گون و حساسیت بیشتر نسبت به شرایط اولیه به‌منظور افزایش طول دوره تناوب و میزان تصادفی بودن و کاهش میزان همبستگی و عدم تکرار الگوهای خاص قابل حدس در خروجی مولدها، ما توابع آشوبی لجستیک و گاوس را با نگاشت درجه‌دو توسط عملگرهای انتقال، xor و الحاق باهم ترکیب کرده و یک مولد جدید برای تولید اعداد شبه تصادفی طراحی و پیشنهاد می‌دهیم. مراحل الگوریتم مولد جدید به‌صورت زیر است:

۱- ابتدا اعداد دلخواه $x_0 \in [0,1]$ ، $y_0 \in [0,2]$ و $z_0 \in [4.7,17]$ را انتخاب کرده و با توجه به مقادیر ثابت a ، b، cو d توابع آشوبی زیر را مقداردهی کرده و n بار محاسبه می‌کنیم.

$$x_i = ax_{i-1}(1 - x_{i-1}),\ 3.5 \leq a \leq 4, 0 \leq x_n \leq 1, y_i = by_{i-1}^2 - cy_{i-1} - 1,$$

$$0 \leq b \leq 1, -1 \leq c \leq 1, z_i = \exp(-z_{i-1}^2) + d, -1 \leq d \leq 1, i = 1, 2, .., n$$

۲- مقادیر به‌دست‌آمده $\{(X_n, Y_n, Z_n) = (x_i, y_i, z_i): i = 0, 1, 2, \dots, n\}$ را به مبنای ۲ تبدیل و به‌اندازه دلخواه R_1، R_2 و R_3 به صورت

$$F_n = X_n \ggg R_1, G_n = Y_n \lll R_2, H_n = Z_n \ggg R_3$$

انتقال می‌دهیم.

۳- مقادیر مرحله ۲ را با عملگر $\oplus$ و انتقال به راست $\ggg$ ترکیب می‌کنیم:

$$O = \{(F_n \oplus Z_n || G_n \oplus X_n || H_n \oplus Y_n) \ggg R_4\}$$

که R_4 یک عدد دلخواه فرد است.

۴- خروجی مولد دنباله دودویی O است.

این الگوریتم به زبان پایتون کد نویسی شده و خروجی‌های آن مورد تحلیل و ارزیابی قرارگرفته است. لازم به ذکر است که مرتبه

پیچیدگی محاسباتی الگوریتم برابر $O(km + n^2)$ است که n تعداد بیت ورودی، m تعداد اعمال ریاضی و k تعداد مراحل اجرایی الگوریتم است.

۴. تحلیل و ارزیابی آماری مولد جدید

برای تحلیل میزان تصادفی بودن، استقلال و یکنواختی این دنباله، به ترتیب از معیار آنتروپی، آزمون‌های استاندارد NIST، آزمون‌های معروف آماری ضریب همبستگی و نیکویی برازش خی دو (χ^2)(هیستوگرام) استفاده‌شده است. این نتایج، کیفیت آماری و تصادفی بودن خروجی مولد جدید را تأیید می‌کند و همچنین معیارهای ارزیابی آمده در مقاله [۱] نیز این نتیجه را تائید می‌کند.

۱,۴ معیار آنتروپی

معیار آنتروپی یک دنباله دودویی مشخصه مهمی برای میزان تصادفی بودن و غیرقابل‌پیش‌بینی بودن آن دنباله است.

مقدار آنتروپی را می‌توان با استفاده از فرمول زیر تعیین کرد:

$$H(B) = -\sum_{i=0}^{n} p_i \log_2 p_i \qquad (۱۱)$$

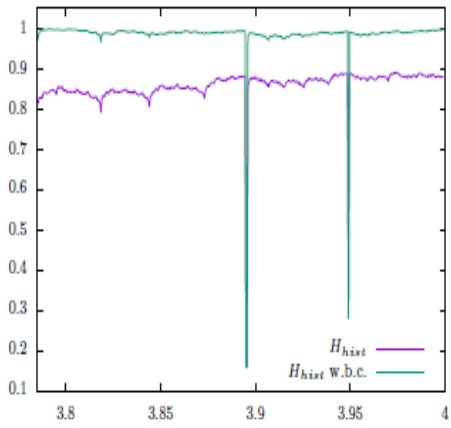
که در آن B دنباله‌ای بیتی با ارقام {۰،۱} و با توزیع احتمال $\{p_1, p_2, \dots, p_n\}$ است.

آنتروپی مولد جدید با دو روش به‌صورت زیر محاسبه می‌شود:

الف) روش اول بدین‌صورت است که یک دنباله طولانی یک‌میلیون بیتی تولید کرده و سپس هیستوگرام آن را محاسبه و رسم می‌شود، وقوع زیر دنباله‌های کوچکی از دو، سه یا چند نماد دودویی با طول ۱۰ محاسبه می‌شود. زیر دنباله‌هایی به طول ۱۶ از مجموع یک‌میلیون بیت برای محاسبه آن هیستوگرام‌ها استفاده شد. هیستوگرام‌ها احتمالات برآورد شده را برای محاسبه معادله بالا تشکیل می‌دهند. آنتروپی‌های تقریبی محاسبه‌شده به آنتروپی واقعی همگرا می‌شود زیرا تعداد دنباله‌های گرفته‌شده به سمت بی‌نهایت است.

ب) روش دوم از الگوریتم وزن دهی درخت متن (CTW[1]) استفاده می‌کند. اندازه‌گیری‌های انجام‌شده توسط این الگوریتم با طرح‌های فشرده‌سازی بی‌اتلاف[2] مرتبط است. آنتروپی عملکرد قوی‌ترین فشرده‌سازی بدون تلفات را محدود می‌کند، که می‌تواند در تئوری با استفاده از مجموعه معمولی یا در عمل با استفاده از طرح‌های هافمن، لمپل‌زیو یا کدگذاری حسابی محقق شود.

سپس، عملکرد الگوریتم‌های فشرده‌سازی داده‌های موجود اغلب به‌عنوان یک تخمین تقریبی از آنتروپی یک بلوک داده استفاده می‌شود. مطالعه در سال ۲۰۰۸ توسط گائو و همکارانش نتیجه داد که روش CTW مؤثرترین روش برای اندازه‌گیری آنتروپی است، با دقیق‌ترین و قابل‌اعتمادترین نتایج بابیت‌های بسیار کمتر، اما زمان محاسبات بیشتری را نیز می‌طلبد. برای تمام دنباله‌های خروجی با $x_0 = 0.2$ آنتروپی با دو روش CTW و هیستوگرام محاسبه‌شده است. برای روش CTW از دنباله‌های ۵۰۰۰ بیتی و روش هیستوگرام از دنباله‌های یک‌میلیون بیتی استفاده‌شده است. نتایج مقادیر آنتروپی هر دو روش در شکل (۵) در زیر نشان داده‌شده است که هر دو روش اندازه‌گیری ازلحاظ مقادیر آنتروپی باهم تطابق خوبی دارند.



شکل (۵): نمودار آنتروپی دنباله‌های تولیدشده

۲,۴ آزمون‌های استاندارد NIST

مولد جدید طراحی‌شده با زبان پایتون برنامه‌نویسی و با رایانه شخصی اینتل ۵ هسته‌ای CPU@3.40 GHZ با حافظه جانبی (RAM) ۸ گیگابایتی با نرخ تولید حدود ۱۵,۳۶۵۷ مگابیت بر ثانیه اجراشده و دنباله‌های خروجی یک‌میلیون بیتی آن با مجموعه آزمون‌های آماری استاندارد NIST ارزیابی‌شده است. مجموعه آزمون‌های NIST یک بسته آماری برای ارزیابی میزان تصادفی بودن دنباله بیت‌ها است که شامل ۱۵ آزمون است. اگر دنباله اعداد از تمام ۱۵ آزمون با موفقیت عبور کند، در حد انتظار تصادفی است. برای هر آزمون، عددی بین صفر و یک به نام p- مقدار از دنباله دودویی محاسبه می‌شود، اگر p- مقدار محاسبه‌شده از آستانه از پیش تعیین‌شده α (خطای رد) بزرگ‌تر باشد، آنگاه تصادفی بودن دنباله را با احتمال $1 - \alpha$ پذیرفته و دنباله با موفقیت آزمون را می‌گذراند و در غیر این صورت، آزمون رد می‌شود.

سطح معنی‌داری هر آزمون دربسته NIST مقدار α=0.01 در نظر گرفته‌شده است، یعنی اگر از ۱۰۰ نمونه مورد آزمایش حدود

[1] Context tree weighting
[2] Lossless compression

۹۹ نمونه دارای رفتار تصادفی خوب باشند آزمون‌ها تائید می‌شوند. مقدار $p \geq 0.01$ به این معنی است که دنباله با اطمینان ۰/۹۹ تصادفی است. ما در آزمایش خود ۲۰۰۰ دنباله دودویی مختلف با طول یک‌میلیون بیت تولید کرده‌ایم. نسبت قبولی هر آزمون از مجموعه NIST و مقادیر p مربوط به هر دنباله برای تمام ۱۵ آزمون مجموعه NIST محاسبه‌شده‌اند. از نتایج جدول زیر به این نتیجه می‌رسیم که دنباله‌های دودویی تولیدشده توسط مولد پیشنهادی دارای ویژگی‌های آماری خوبی بوده و تمام آزمون‌ها را با موفقیت گذرانده‌اند.

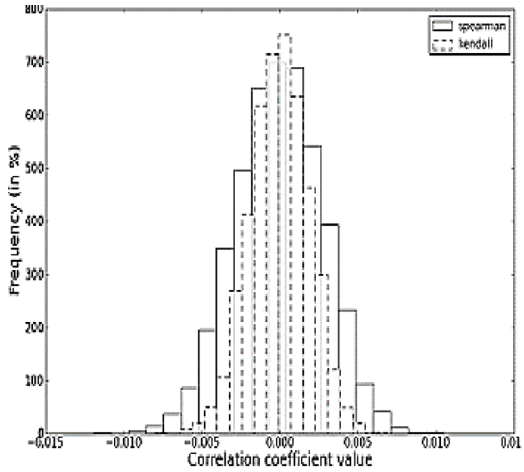
جدول (۱): نتایج بررسی آزمون‌های NIST

نام آزمون	مقدار p -	نتیجه
آزمون فراوانی	۰/۹۱۱۴۶۵	قبول
آزمون فراوانی درون بلوک	۰/۵۸۲۳۴۱	قبول
آزمون ردیف	۰/۸۴۵۶۳۹	قبول
طولانی‌ترین ردیف داخل بلوک	۰/۷۸۵۴۲۳	قبول
آزمون رتبه ماتریس باینری	۰/۹۱۲۳۵۶	قبول
آزمون تبدیل فوریه گسسته	۰/۴۸۷۹۵۶	قبول
انطباق الگوی غیرهمپوشان	۰/۷۴۹۴۹۶	قبول
انطباق الگوی همپوشان	۰/۷۴۸۵۹۶	قبول
آزمون ماورر	۰/۷۱۲۳۵۶	قبول
آزمون پیچیدگی خطی	۰/۲۱۲۱۳۶	قبول
آزمون سریال	۰/۶۴۱۵۹۸	قبول
آزمون آنتروپی تقریبی	۰/۸۱۲۵۶۹	قبول
آزمون مجموع‌های تجمعی	۰/۵۱۱۲۴۵	قبول
آزمون گشت‌های تصادفی	۰/۶۰۲۶۱۱	قبول
آزمون گشت‌های تصادفی گوناگون	۰/۵۲۲۳۷۱	قبول

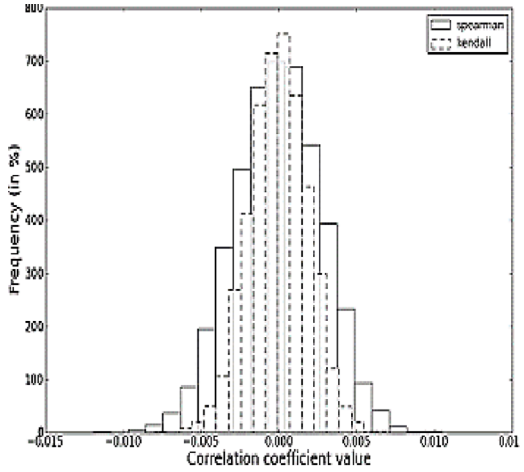
۲,۴ آزمون همبستگی

با توجه به این حقیقت که بایستی دنباله‌های خروجی یک مولد اعداد شبه تصادفی مستقل از هم باشند، از شاخص ضریب همبستگی به‌عنوان معیار مناسبی می‌توان استفاده نمود. ضرایب همبستگی پیرسون، اسپیرمن و کندال در این رابطه رواج گسترده‌ای دارند.

در این قسمت برای تحلیل آماری نمونه‌های تصادفی تولیدشده با مولد پیشنهادی، ضرایب همبستگی بین آن‌ها محاسبه‌شده و نتایج مورد تحلیل و بررسی قرار می‌گیرند. تعداد ۱۱۰ دنباله ۱۰۰۰۰۰۰ بیتی مورد مقایسه قرار گرفتند و ضریب همبستگی بین عناصر دنباله محاسبه و نتایج فراوانی آن‌ها در شکل‌های زیر نشان داده‌شده است. همان‌طور که مشاهده می‌کنید این ضرایب در بازه [۰,۰۱, ۰,۰۱-] قرار می‌گیرند که نشان می‌دهد دنباله‌های تولیدشده توسط مولد پیشنهادی نا همبسته هستند. درواقع هرچقدر این بازه به صفر نزدیک‌تر باشد دنباله‌های تولیدشده دارای همبستگی کمتری نسبت به یکدیگر بوده و درواقع بهتر می‌باشند. دقت شود که تعداد ۵۹۹۵ همه ترکیبات دوتایی دنباله‌های نمونه تصادفی است.



شکل (۶). هیستوگرام ضرایب همبستگی پیرسون و اسپیرمن برای ۵۹۹۵ دنباله دلخواه



شکل (۷). هیستوگرام ضرایب همبستگی کندال و اسپیرمن برای ۵۹۹۵ دنباله دلخواه

به‌طورکلی ضریب همبستگی برای تعیین اندازه میزان وابستگی و روابط آماری معنی‌دار بین مشاهدات دو یا چند متغیر تصادفی استفاده می‌شود. برای دو دنباله داده، ضریب همبستگی به‌صورت زیر تعریف می‌شود:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (۱۲)$$

که

$$cov(x,y) = \frac{1}{M}\sum_{i=1}^{M}(x_i - E(x))(y_i - E(y)) \qquad (۱۳)$$

و در آن x و y مقادیر عددی دو دنباله اعداد می‌باشند و

$$E(x)=\frac{1}{M}\sum_{i=1}^{M}x_i \ , \ D(x) \ =\frac{1}{M}\sum_{i=1}^{M}(x_i-E(x))^2 \qquad (۱۴)$$

در این آزمون هر چه مقدار r به صفر نزدیک‌تر باشد می‌گوییم اعداد خروجی مولد بیشتر نا همبسته هستند و هر چه به ۱ و ۱- نزدیک‌تر باشند می‌گوییم اعداد تولیدشده همبستگی بیشتری دارند [۲۵].

۳,۴ آزمون نیکویی برازش

با توجه به ساختار و ویژگی‌های رفتاری مولدهای اعداد تصادفی، دنباله‌های خروجی مولدها نباید دارای الگوی خاص و تکراری و قابل حدس باشند و نیز هیستوگرام فراوانی بیت‌های دنباله نباید باهم اختلاف بارزی داشته باشند و این شرایط زمانی محقق می‌شود که توزیع فراوانی ارقام دنباله خروجی هم‌شانس بوده و از توزیع احتمال یکنواخت تبعیت کنند. در استنباط آماری، آزمون نیکویی برازش خی دو از مشهورترین آزمون‌های آماری برای آزمودن فرض یکنواخت بودن توزیع داده‌ها است که در سال ۱۹۹۰ توسط پیرسن معرفی شد. فرض آماری به‌صورت زیر است:

فرض H_0: توزیع داده‌های نمونه با توزیع موردنظر تطابق دارد (توزیع داده‌ها یکنواخت هستند).

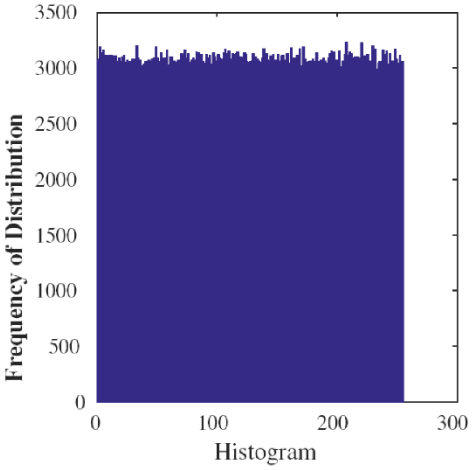
فرض H_1: توزیع داده‌های نمونه با توزیع موردنظر تطابق ندارد. اگر داده‌های تولیدشده را به k گروه مختلف تقسیم کنیم آنگاه توزیع نمونه‌ای متغیرهای تصادفی با $k\text{-}1$ درجه آزادی با رابطه زیر محاسبه می‌شود:

$$\chi^2=\sum_{i=1}^{k}\frac{(O_i-E_i)^2}{E_i} \qquad (15)$$

که O_i تعداد مشاهدات هر دسته و E_i تعداد مشاهدات مورد انتظار (مطابق یا توزیع یکنواخت) در هر دسته است.

اگر $\chi^2_{\text{محاسبه شده}} > \chi^2_{(1-\alpha,k-1)}$ (α سطح معنی‌داری آزمون فرض است که اغلب مقدار ۰/۰۵ یا ۰/۰۱ را در نظر می‌گیرند) در این صورت فرض H_0 رد می‌شود.

برای بررسی اینکه «آیا داده‌های خروجی مولدهای اعداد شبه تصادفی دارای توزیع یکنواخت هستند یا خیر؟» از آزمون نیکویی برازش خی دو استفاده‌شده است. ابتدا ۱۰۰۰و۱۰۰۰۰و۲۰۰۰۰ و۵۰۰۰۰ عدد توسط مولد پیشنهادی تولید و سپس آزمون خی دوروی داده‌ها اجرا گردید. نتایج حاصل از آزمون، یکنواختی در حد مطلوب دنباله تولیدی توسط مولد پیشنهادی را به‌خوبی نمایش می‌دهد. با توجه به نمودارهای هیستوگرام که نحوه توزیع داده‌ها را نشان می‌دهد می‌توان به‌طور شهودی درک کرد که داده‌ها تا چه اندازه‌ای هم‌شانس و مطابق توزیع یکنواخت پخش‌شده‌اند (شکل (۸) را ببینید).



شکل (۸). هیستوگرام داده‌های نمونه

۵. مقایسه مولد پیشنهادی با چند مولد دیگر

برای بررسی میزان تصادفی بودن، استقلال و یکنواختی دنباله‌های تولیدشده توسط مولد پیشنهادی و مولدهای Standard C ,MT19937 ,PHP-MT ,CCCBG ,CI ,CCS ,TCLM ,LCG، تعداد ۱۰۰۰، ۱۰۰۰۰، ۲۰۰۰۰ و ۵۰۰۰۰ عدد توسط مولدها تولیدشده و سپس به ترتیب آزمون‌های NIST و ضریب همبستگی و نیکویی برازش را روی آن‌ها اجرا کردیم که نتایج به‌دست‌آمده در جدول ۲ در زیر نمایش داده‌شده است. نتایج ارائه‌شده نشان می‌دهد که مولد پیشنهادی در مقایسه با سایر مولدها از وضعیت خیلی خوبی برخوردار هست.

جدول (۲): نتایج مقایسه مولد جدید با چند مولد دیگر

نام مولد	آزمون همبستگی	آزمون‌های NIST	آزمون نیکویی برازش
مولد جدید	قبول	قبول	قبول
Standard C LCG	قبول	قبول	رد
MT 19937	رد	قبول	رد
PHP-MT	قبول	قبول	رد
CCCBG	رد	قبول	قبول
TCLM	قبول	قبول	رد
CCS	رد	قبول	رد
CI	قبول	قبول	رد

۶. نتیجه‌گیری

در این مقاله با استفاده از ترکیب تابع آشوبی لجستیک، تابع مولد همنهشتی درجه‌دو و نگاشت گوسی و استفاده از عملگر انتقال و xor یک مولد جدید برای تولید اعداد شبه تصادفی طراحی گردید. سپس خروجی آن با عمل الحاق و انتقال به راست مخلوط شد . با این عمل ترکیب، شاخص‌های طول دوره تناوب، میزان استقلال و یکنواختی داده‌های خروجی مولد پیشنهادی به نحو مطلوبی بهبود یافت. این بهبودها توسط آزمون‌های همبستگی، نیکویی برازش و نمودارهای هیستوگرام به‌خوبی نشان داده شد. همچنین با کمک نتایج آزمون‌های استاندارد NIST نشان داده شد که دنباله‌های خروجی این مولد دارای رفتار آماری مطلوب و تصادفی داشته که با توزیع احتمال یکنواخت مطابقت دارند. همچنین میزان کیفیت مولد پیشنهادی با چندین مولد شناخته‌شده مقایسه گردید که نتایج این مقایسه، کیفیت مطلوب و قابل‌قبول مولد جدید را تائید می‌کند.

۷. مراجع

[1] Gaeini A., Mirghadri A., Jandaghi G., “A General Evaluation Pattern for Pseudo Random Number Generators”, Trends in Applied Sciences Research, 10 (5), 2015, pp 231-244.

[2] Padányi V., Herendi T., “A study on comparison of pseudorandom number generator”, International Journal of Mathematics and Computer in Engineering, 1(1) , 2023, pp 25 – 44.

[3] Hasted J., “Pseudo-random generators under uniform assumptions”, In 22nd ACM Symposium on Theory of Computing, 1880.

[4] Michael Pidd, “Computer Simulation in Management Science”, 4th Edition, John Wiley & Sons, (1998).

[5] L'Ecuyer P., "Uniform Random Number Generation, Annuls of Operations Research", Vol. 23 (1994).

[6] Gomez D., Gutierrez J., Ibeas A., "Cryptanalysis of the Quadratic Generator", Progress in Cryptology – INDOCRYPT, 2005, pp 118–129.

[7] Moysis L., Kafetzis I., Baptista S., Volos C., "Chaotification of One-Dimensional Maps Based on Remainder Operator Addition", Mathematics, 10, 2801, 2022.

[8] Matthews, R.A.J., “On the Derivation of a “Chaotic” Encryption Algorithm”. Cryptologia, Vol. 13, Issue 1, 1989, pp. 29-42. http://dx.doi.org/10.1080/0161-118991863745

[9] Habutsu H., Y. Nishio, I. Sasase and S. Mori, “A Secret Key Cryptosystem by Iterating a Chaotic Map”. Advances in Cryptology, Proceedings of EuroCrypt91,Vol .547,pp.127-140,1991.

[10] Stojanovski T., Kocarev L., "Chaos-based random number generators – part 1: practical realization", IEEE Transactions on circuits and systems I: Fundamental Theory and applications, vol. 48 (2001) 281-288.

[11] Stojanovski T., Pihl J., Kocarev L., "Chaos-based random number generators – part 2: Practical realization", IEEE Transactions on circuits and systems I: Fundamental Theory and applications, vol. 48 (2001) 382-385.

[12] Kocarev L., and Jakimoski G., "Pseudorandom bits generated by chaotic maps", IEEE Transactions on circuits and systems I: Fundamental Theory and applications, 50 (2003) 123-126.

[13] Fu S. M., Chen Z. Y., and Zhou Y. A., "Chaos-based random number generators", Computer research and development, 41 (2004) 749-754.

[14] Liu J., "Design of chaotic random sequence and its application", Computer Engineering, 31 (2005) 150-152.

[15] Wang Y., Shen H., Yan X., "Design of a chaotic random number generator", Chinese Journal of Semiconductors, 26 (2005) 2433-2439.

[16] Wang L., Wang F.P., Wang Z.J., "Novel chaos based pseudorandom number generator", Acta Physical Sinica, 55 (2006) 3964-3968.

[17] Ergun S., and Ozoguz S., "Truly random number generators based on a non-autonomous chaotic oscillator", AEU-International J. Electronics & Communications, 62 (2007) 235-242.

[18] Hu Y., Liao X., Wong K.W., and Zhou Q., "A true random number generator based on mouse movement and chaotic cryptography", Chaos solitons and fractals, 40 (2009) 2286-2293.

[19] Firat Artuger, Fatih Ozkaynak, “A new chaotic system and its practical applications in substitution box and random number generator”, Multimedia Tools and Applications, 04 April 2024.

[20] Wenbo Zhao, and Caochuan Ma, "Modification of intertwining logestic map and anovel Pseudo-Random Number Generator", Symmetry, Vol. 16, Issue 2, 31 January 2024, 169. https://doi.org/10.3390/sym16020169

[21] Moysis L., Tutueva A., Volos C., Butusov D., Munoz-Pacheco J., Nistazakis H., "A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation", 12 (2020) 829.

[22] Huang X., Liu L., Li X., Yu M., Wu Z., “A New Pseudorandom Bit Generator Based on Mixing Three-Dimensional Chen Chaotic System with a Chaotic Tactics”, 6567198, Complexity (2019).

[23] Adhikari S., Karforma S., "A novel audio encryption method using Henon –Tent chaotic pseudo random number sequence", Vol. 13(4) (2021) pp1463–1471.

[24] Rasika B. Naik and Udayprakash Singh, “A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption”, Annals of Data Science, 18 January 2022.

[25] Gaeini A., Mirghadri A., Jandaghi G., “Design and analysis of a new efficient Pseudo Random Number Generators for Cryptography”, Ph.D Thesis, Imam Hussein University, 2014 (In Persian).