Tabriz Journal of Electrical Engineering (TJEE), vol. 52, no. 3, Autumn 2022 Serial no. 101
DOI: 10.22034/tjee.2022.15745

# Pseudo-random Number Generator Based on Autaptic Izhikevich Neuron Model under Electromagnetic Radiation and Its FPGA Implementation

Mohammad saeed Feali*

Department of Electrical Engineering, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran
E-mail: msaeed.feali@iau.ac.ir
* means corresponding author

**Short Abstract**
The electrical behavior of neurons can be more complex in the presence of autapse. In the presence of an autaptic connection, the Izhikevich neuron model can show a variety of dynamic behaviors, such as chaotic behavior. This paper presents a novel, high speed and robust pseudo random number generator based on the autaptic Izhikevich neuron oscillator and its FPGA implementationThe autaptic Izhikevich neuron model is simulated and .dynamically analyzed. Then, the proposed pseudo-random number generator is modeled and simulated using the Xilinx system generator platform, synthesized using Xilinx Synthesis Tool, and implemented on the XILINX SPARTAN-6 XC6SLX9 FPGA evaluation board. As a post processing implmentation cost of the proposed pseudo- random number generator is lower than similar work, and the proposed generator achieves a maximum frequency of 63.2 MHz. The NIST test suite is used for testing the quality of the generated bit sequences. The NIST test results indicates the high quality of the generated random bit sequence.

**Keywords**
“Izhikevich” ,“Neuron” ,“Autapse” ,“Randon number generator”.

## 1- Short Introduction

Generating random numbers is very important in security systems. In the Pseudo random number generators (PRNGs), the mathematical deterministic algorithms are used for generating random numbers. Pseudorandomness characteristics and the unpredictability make chaos as a good candidate for use in cryptography. The Izhikevich neuron model can represent complex dynamical behavior such as chaos when the effects of the electromagnetic induction and the autaptic connection are considered in the model. In this paper, based on the chaotic dynamics in the improved Izhikevich neuron model, a PRNG is proposed and implemented on XILINX FPGA evaluation board.

## 2- Proposed Work and Methodology

In this paper, based on the chaotic dynamics in the improved Izhikevich neuron model, a pseudo random number generator is proposed. Neuron oscillator, sampling, and post-processing are three modules of the proposwed FPGA-based PRNG. The proposed PRNG is modeled and simulated on Xilinx system generator platform and implemented on XILINX SPARTAN-6 XC6SLX9 FPGA evaluation board. To improve the randomness of the bit sequence, an XOR operation will be performed on the output data as a post-processing step. The FPGA implementation results show that the implementation cost of the proposed PRNG is lower than similar works, and the proposed generator achieves a maximum frequency of 63.2 MHz. The generated random bit sequence has successfully passed NIST 800-22 statistical test.

## 3- Conclusion

A novel, high speed and robust pseudo random number generator based on the autaptic Izhikevich neuron oscillator is presented and implemented on FPGA. The Xilinx system generator platform is used for modeling and simulating the proposed PRNG. Then, the Xilinx system generator model synthesized using Xilinx Synthesis Tool and implemented on the XILINX SPARTAN-6 XC6SLX9 FPGA evaluation board. The implementation results show that the implementation cost of the proposed pseudo-random number generator is lower compared to similar works, and also the proposed generator achieves a maximum frequency of 63.2 MHz and an output rate of bit production up to 18.4 Mbit/s. The p-value results from the NIST test set show the high quality of the generated random bit sequence, so that for most of the test results, the p-value is greater than 0.5.

## 4- References

[۲۵] E. M. Izhikevich, "Simple model of spiking neurons", IEEE Transactions on neural networks, vol. 14, no. 6, pp.1569-1572, 2003.

[۳۲] G. Wang, Y. Wu, F. Xiao, Z. Ye, Y. Jia, "Non-Gaussian noise and autapse-induced inverse stochastic resonance in bistable Izhikevich neural system under electromagnetic induction", Physica A: Statistical Mechanics and its Applications, vol. 598, pp.127274, 2022.

[۳۶] J-L. Danger, S. Guilley, P. Hoogvorst, "High speed true random number generator based on open loop structures in FPGAs", Microelectronics journal, vol. 40, no. 11, pp. 1650-1656, 2009.

# مولد اعداد شبه تصادفی بر اساس مدل نورون ایژیکویچ اتاپسی تحت تابش الکترومغناطیسی و پیاده‌سازی مبتنی بر FPGA

**محمد سعید فعلی**

استادیار، گروه مهندسی برق، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران

**چکیده**

رفتار الکتریکی نورون‌ها در حضور اتاپس می‌تواند پیچیده‌تر باشد. در حضور یک اتصال اتاپسی، مدل نورون ایژیکویچ می‌تواند انواع رفتارهای دینامیکی مانند رفتار آشوبناک را نشان دهد. در این مقاله یک مولد اعداد شبه تصادفی جدید، قوی و با سرعت بالا بر اساس نوسانگر نورون ایژیکویچ اتاپسی و همچنین پیاده‌سازی مبتنی بر FPGA آن ارائه می‌شود. مدل نورون ایژیکویچ اتاپسی شبیه‌سازی شده و به‌صورت دینامیکی تحلیل خواهد شد. سپس، با استفاده از پلتفرم Xilinx system generator مولد اعداد شبه تصادفی پیشنهادی مدل‌سازی و شبیه‌سازی شده، و در ادامه با استفاده از ابزار سنتز Xilinx سنتز شده و درنهایت بر روی برد FPGA از نوع XILINX SPARTAN-6 XC6SLX9 پیاده‌سازی می‌گردد. از تابع XOR به‌عنوان یک عملیات پس از پردازش، برای افزایش میزان تصادفی بودن توالی بیت‌های خروجی استفاده می‌شود. نتایج حاصل از پیاده‌سازی FPGA نشان می‌دهد که هزینه پیاده‌سازی مولد اعداد شبه‌تصادفی پیشنهادی در مقایسه با کارهای مشابه کمتر بوده و همچنین مولد پیشنهادی به حداکثر فرکانس ۶۳/۲ مگاهرتز و نرخ خروجی تولید بیت تا ۱۸/۴ مگابیت بر ثانیه دست می‌یابد. مجموعه تست NIST برای تست میزان تصادفی بودن توالی بیت‌های تولیدشده استفاده می‌شود. نتایج آزمون NIST کیفیت بالای توالی بیت‌های تصادفی تولیدشده را تأیید می‌کند به‌طوری‌که برای اکثر نتایج آزمایش، *p-value* بزرگ‌تر از ۰/۵ است. تولیدکننده اعداد تصادفی پیشنهادی می‌تواند در کاربردهایی نظیر سیستم‌های امنیتی و رمزنگاری مورداستفاده قرار گیرد.

**کلمات کلیدی**

ایژیکویچ، نورون، اتاپس، مولد اعداد تصادفی.

نام نویسنده مسئول: دکتر محمد سعید فعلی

ایمیل نویسنده مسئول: msaeed.feali@iau.ac.ir

تاریخ ارسال مقاله: ۱۴۰۱/۰۵/۰۵

تاریخ(های) اصلاح مقاله: ۱۴۰۱/۰۷/۱۵

تاریخ پذیرش مقاله: ۱۴۰۱/۰۸/۲۰

## ۱- مقدمه

با پیشرفت فناوری رایانه، مسئله امنیت اطلاعات اهمیت بیشتری یافته و توجه زیادی به این حوزه شده است . داشتن مقادیر ناشناخته و غیرقابل‌پیش‌بینی در سیستم‌های رمزنگاری بسیار حائز اهمیت است [۳-۱]. تولید اعداد تصادفی در سیستم‌های امنیتی بسیار مهم بوده به‌طوری‌که امنیت سیستم کاملاً به کیفیت اعداد تصادفی تولیدشده وابسته است. اگر کیفیت اعداد تصادفی تولیدشده به‌اندازه کافی خوب نباشد، مهاجمان می‌توانند امنیت سیستم را به خطر بیندازند. اگر طول و دوره دنباله‌های اعداد تصادفی و همچنین مقادیر آنتروپی آن‌ها کافی باشد، اعداد تولیدشده تصادفی و غیرقابل‌پیش‌بینی هستند [۴]. به‌سادگی، اگر مقادیر آینده در دنباله اعداد را نتوان از روی دنباله موجود پیش‌بینی کرد، دنباله اعداد تصادفی است. مولدهای اعداد تصادفی بخش اولیه و مهم سیستم‌های امنیتی هستند. برای کاربردهای رمزنگاری از دو نوع از مولدهای اعداد تصادفی استفاده می‌شود، مولد اعداد تصادفی واقعی[1] و مولد اعداد شبه تصادفی[2]. در مولدهای اعداد تصادفی واقعی از منابع نویز فیزیکی (مانند نویز حرارتی و نویز فوتون) برای تولید اعداد تصادفی استفاده می‌شود. مولد اعداد تصادفی واقعی باید غیرقابل‌پیش‌بینی، غیرقابل تکرار و از نظر آماری بی‌طرف باشد. در مولدهای اعداد شبه تصادفی، از الگوریتم‌های قطعی ریاضی برای تولید توالی‌های به‌ظاهر تصادفی از یک مقدار اولیه به نام دانه[3] استفاده می شود. مولدهای اعداد شبه تصادفی با خواص آماری خوب، تکرارپذیری مناسب و قابلیت بازتولید بالا مطلوب هستند. دشواری حل مسائل ریاضی مربوطه میزان امنیت مولد اعداد شبه تصادفی را تعیین می‌کند. ویژگی‌های تصادفی مناسب اعداد شبه تصادفی منجر به استفاده گسترده از آن‌ها در رمزنگاری و سیستم‌های امنیتی شده است [۶-۵].

ویژگی‌های شبه تصادفی، حساسیت به شرایط اولیه، و غیرقابل‌پیش‌بینی بودن رفتار طولانی‌مدت، آشوب[4] را به‌عنوان کاندیدای مناسبی برای استفاده در رمزنگاری معرفی می‌کند. سیستم‌های آشوبناک در زمینه‌های زیادی مانند شبکه عصبی مصنوعی [۷]، ارتباطات ایمن [۸]، همگام‌سازی [۹] و مولدهای اعداد تصادفی [۱۰] استفاده می‌شوند. ایده استفاده از آشوب برای تولید اعداد تصادفی ایده جدیدی را برای رمزگذاری اطلاعات معرفی می‌کند [۱۲-۱۱]. مولد آشوب یکی از ساختارهای اصلی در مولدهای اعداد تصادفی مبتنی بر آشوب است. بنابراین، به‌منظور افزایش غیرقابل‌پیش‌بینی بودن و تصادفی بودن

[1] True random number generator
[2] Pseudo random number generator
[3] Seed
[4] Chaos

مولدهای اعداد تصادفی، می‌توان از سیستم‌های آشوب هم به‌عنوان دانه [۶ و ۱۳] و هم به‌عنوان منبع تصادفی [۱۵-۱۴] استفاده کرد.

امروزه پیاده‌سازی ساختارهای مشابه مغز انسان جهت تقلید از ویژگی‌های منحصربه‌فرد مغز در انجام محاسبات بسیار موردتوجه دانشمندان قرار گرفته است. اگر مولدهای اعداد تصادفی هم بر مبنای این ساختارها ایجاد شود، آنگاه می‌توان این مولدها را به‌صورت یکپارچه در ساختارهای نورومورفیک استفاده نمود. ازاین‌رو استفاده از رفتار نورون‌ها و شبکه‌های عصبی در تولید اعداد تصادفی موردتوجه قرار گرفته است [۱۶-۱۷]. بر اساس مطالعات نوروفیزیولوژیک، رفتار دینامیکی نورون‌های بیولوژیکی فعالیت مغز انسان را تعیین می‌کند. دینامیک آشوبناک پیچیده و غنی در فعالیت الکتریکی بین نورون‌ها وجود دارد [۱۸]. آشوب در برخی از بیماری‌های عصبی مانند صرع دیده می‌شود [۱۹]. همچنین، سیگنال‌های الکتروانسفالوگرام (EEG) انسان دارای ویژگی‌های آشوبناک است [۲۰].

برای شبیه‌سازی فعالیت نورون‌ها و مطالعه برهمکنش بین نورون‌ها، مدل های نورونی مختلفی توسط محققان طراحی شده است، مانند مدل هوچکین-هاکسلی[۵] [۲۱]، مدل هندمارش-رز[۶] [۲۲]، مدل فیتز هوگ-ناگومو[۷] [۲۴-۲۳]، مدل ایزیکویچ[۸] [۲۵] و غیره. در میان آن‌ها، مدل نورون ایزیکویچ، علاوه بر اینکه ازنظر محاسباتی مقرون‌به‌صرفه است، می‌تواند رفتار اسپایک‌زنی آشوبناک[۹] را به‌خوبی نشان دهد [۲۶]. علاوه بر این، مدل ایزیکویچ می‌تواند متنوع‌ترین رفتار اسپایک‌زنی را در بین مدل‌های دیگر ایجاد کند.

مطالعات نشان می‌دهد که القای الکترومغناطیسی[۱۰] و همچنین اتصال اتاپسی[۱۱] اثرات قابل‌توجهی بر رفتار دینامیکی نورون‌ها دارند [۲۸-۲۷]. در نورون‌های بیولوژیکی، تبادل یون‌های باردار در سراسر غشاء و تغییر توزیع غلظت یون‌های باردار نورون باعث ایجاد یک میدان الکترومغناطیسی متغیر با زمان در نورون می‌شود. در مدل‌سازی رفتاری نورون، شار مغناطیسی برای توصیف این اثر میدان الکترومغناطیسی مورداستفاده قرار می‌گیرد که پتانسیل غشا را از طریق یک ممریستور تنظیم می‌کند. [۲۹]. این جریان مغناطیسی القایی می‌تواند دینامیک نورون را تنظیم کند. عامل دیگری که بر رفتار دینامیکی نورون‌ها تأثیر می‌گذارد، اتاپس[۱۲] است. مشخص شده است که رفتار الکتریکی نورون‌ها در حضور اتاپس پیچیده‌تر است [۳۰]. اتصال اتاپسی که یک نورون را از طریق یک حلقه بسته به خود متصل می‌کند، ازنظر ریاضی با یک عبارت فیدبک با تأخیر زمانی مدل‌سازی می‌شود [۳۱]. مدل نورون ایزیکویچ می‌تواند رفتار دینامیکی پیچیده‌ای مانند آشوب را زمانی که اثرات القای الکترومغناطیسی و اتصال اتاپسی در مدل در نظر گرفته شود، نشان دهد [۳۲].

Nobukawa و همکاران ویژگی‌های آشوبناک مدل نورونی ایزیکویچ را ارزیابی کردند [۳۳]. دو حالت آشوبناک متمایز مانند حالت آشوبناک متناوب و حالت آشوبناک با حرکت عمدتاً آشفته در این مطالعه کشف شده‌اند. Tamura و همکاران ساختار دوشاخگی[۱۳] مدل نورون ایزیکویچ و مناطق پارامتری آشفته در صفحه پارامتر را مشخص کردند [۳۴]. بر اساس این مطالعه، مدل ایزیکویچ پاسخ آشوبناکی را برای برخی از مقادیر پارامترها نشان می‌دهد.

در این مقاله، بر اساس دینامیک آشوبناک در مدل نورون ایزیکویچ بهبود یافته، یک مولد اعداد شبه تصادفی پیشنهاد شده است. مولد اعداد شبه تصادفی پیشنهادی بر روی پلت فرم Xilinx system generator مدل‌سازی و شبیه‌سازی شده و بر روی برد FPGA از نوع XILINX SPARTAN-6 XC6SLX9 پیاده سازی شده است. برای بهبود تصادفی بودن توالی بیت تولیدی، یک عملیات XOR بر روی داده‌های خروجی به‌عنوان یک مرحله پس از پردازش انجام می شود. میزان تصادفی بودن توالی بیت تصادفی تولیدشده توسط آزمون آماری NIST 800-22 ارزیابی می‌گردد. بقیه بخش‌های مقاله به شرح زیر ارائه شده است. در بخش دوم، مدل نورون ایزیکویچ اتاپسی ارائه، تحلیل و گسسته‌سازی شده است. بخش ۳ ساختار مولد اعداد شبه تصادفی و جزئیات پیاده‌سازی FPGA را ارائه می‌دهد. در بخش ۴، تحلیل تصادفی بودن توالی تصادفی تولیدشده ارائه شده است.

## ۲- مدل نورون ایزیکویچ اتاپسی و تحلیل دینامیکی آن

مدل نورون ایزیکویچ یک مدل فشرده است که تقریباً تمام رفتارهای اسپایک‌زنی نورون‌ها را بازتولید می‌کند. تنوع پاسخ دینامیکی ارائه‌شده توسط مدل ایزیکویچ بیشتر از سایر مدل‌های عصبی است [۲۶]. با در نظر گرفتن اثرات القای الکترومغناطیسی و اتصال اتاپسی، مدل نورونی بهبود یافته ایزیکویچ به‌صورت زیر بیان می‌شود:

$$\begin{aligned} \upsilon' &= 0.04\upsilon^2 + 5\upsilon + 140 - u + I_{syn} - \kappa_1\rho(\varphi)\upsilon + I_{aut} \\ u' &= a(b\upsilon - u) \\ \varphi' &= \kappa_2\upsilon - \kappa_3\varphi \end{aligned} \qquad (۱)$$

$$\text{اگر} \quad \upsilon \geq 30 \quad \text{آنگاه} \quad \left.\begin{matrix} \upsilon \leftarrow c \\ u \leftarrow u + d \end{matrix}\right\}$$

که در آن $\upsilon$ و $u$ به ترتیب متغیر پتانسیل و متغیر بازیابی هستند. پتانسیل $\upsilon$ و زمان $t$ به ترتیب با واحدهای [mV] و [ms] اندازه‌گیری می‌شوند. هنگامی که $\upsilon \geq 30$ mV مدل آتش می‌کند، و سپس $\upsilon$ روی $c$ و $u$ روی $u+d$ تنظیم می‌شوند. پارامترهای $a$ و $b$ به ترتیب مقیاس زمانی و حساسیت $u$ هستند. $I_{syn}$ جریان سیناپسی ورودی را نشان می‌دهد. متغیر $\varphi$ شار مغناطیسی را نشان می‌دهد. $\rho(\varphi) = dq/d\varphi$ رسانایی ممریستور کنترل‌شده با شار است، که در آن $q(\varphi)$ شار بار در سراسر ممریستور است. $\rho(\varphi) = \alpha\varphi^2 + \beta\varphi + \gamma$، که در آن $\alpha$، $\beta$ و $\gamma$ ثابت‌ها هستند، $\beta = 0.5$ و $\gamma = 0.5$. $\rho(\varphi)$ رابطه بین پتانسیل غشا و شار مغناطیسی را توصیف می‌کند. عبارت $\kappa_1\rho(\varphi)\upsilon$ جریان مغناطیسی القایی اضافه‌شده به سمت راست معادله پتانسیل را تعیین می‌کند. برهمکنش بین پتانسیل غشا و شار مغناطیسی توسط متغیرهای $\kappa_1$، $\kappa_2$ و $\kappa_3$ تنظیم می‌شود. $I_{aut}$ جریان اتاپسی است که توسط رابطه زیر وصف می‌شود [۳۵]:

$$I_{aut} = g(\upsilon(t-\tau) - \upsilon(t)) \qquad (۲)$$

که در آن پارامترهای $g$ و $\tau$ به ترتیب رسانایی اتاپسی و تأخیر زمانی در اتاپس هستند. شکل ۱ نمودار دوشاخگی $u$ برحسب محرک‌های ورودی DC ($I_{syn}$) را برای هر دو حالت با و بدون اتصال اتاپسی نشان می‌دهد. پارامترهای سیستم به‌صورت $a$=۰/۰۲، $b$=۰/۲، $c$=-۶۵، $d$=۱/۵، $\alpha$=۰/۰۱، $\kappa_1$=۰/۰۱، $\kappa_2$=۰/۵، $\kappa_3$=۰/۵، و مقادیر اولیه به‌صورت [-۲۰، -۲۰، -۲۰] انتخاب شده‌اند. بدون اتصال اتاپسی، پدیده دوشاخگی دیده نمی‌شود. اما هنگامی‌که اتصال اتاپسی در مدل در نظر گرفته می‌شود ($g$=۰/۵ و $\tau$=۲ ms)، با تغییر جریان ورودی، چندین پدیده دوشاخگی در محدوده دیده می‌شود. در این حالت می‌توان رفتار آشوبناک را برای $I_{syn}$ بین مقادیر ۸ تا ۱۰ مشاهده کرد.

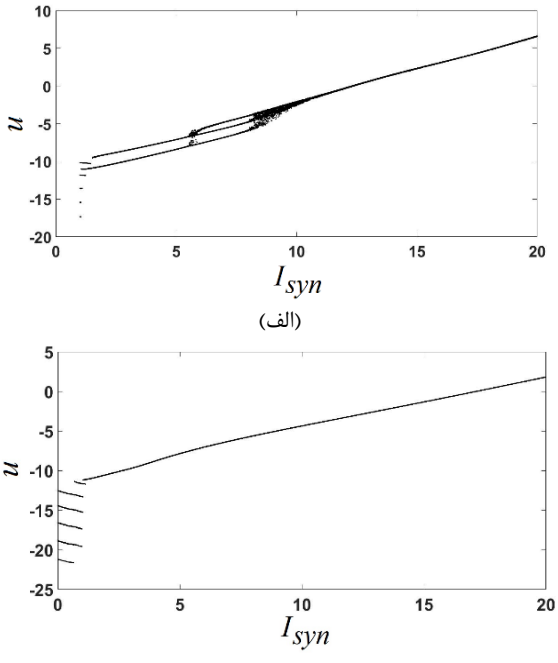
[۵] Hodgkin-Huxley
[۶] Hindmarsh-Rose
[۷] FitzHugh-Nagumo
[۸] Izhikevich
[۹] Chaotic spiking

[۱۰] Electromagnetic induction
[۱۱] Autaptic connection
[۱۲] Autapse
[۱۳] Bifurcation structure

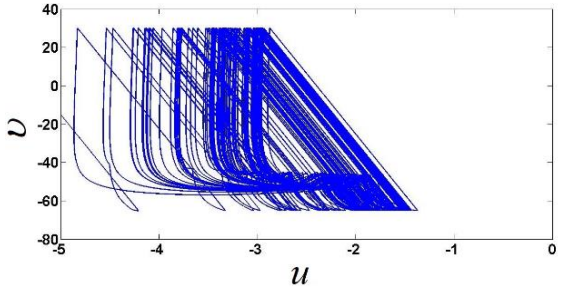
شکل ۲ مسیر نمودار فاز مدل اتاپسی را برای $I_{syn}$ = ۹ نشان می‌دهد. نمودار فاز یک جاذب آشوبناک تک پیچک را نشان می‌دهد. با توجه به این شکل مشخص است که با گذشت زمان مسیر نمودار فاز $u-v$ مدام در حال تغییر بدون قائده است که این نشان‌دهنده آشوبناک بودن تغییرات متغیرهای $u$ و $v$ در زمان است.

## ۳- طراحی مولد اعداد شبه تصادفی پیشنهادی و پیاده‌سازی FPGA

مولدهای اعداد تصادفی بلوک‌های اساسی در سیستم‌های رمزنگاری هستند. اجرای سخت‌افزاری این بلوک‌ها به دو صورت دیجیتال و آنالوگ انجام می‌شود. در پیاده‌سازی آنالوگ معمولاً از فناوری CMOS استفاده می‌شود. اما اجرای آنالوگ پرهزینه است و به‌اندازه کافی انعطاف‌پذیر نیست. پیاده‌سازی دیجیتالی مولدهای اعداد تصادفی مزایای زیادی نسبت به اجرای آنالوگ دارد [۳۶]. ساختارهای مختلفی برای اجرای دیجیتال مولدهای اعداد تصادفی مبتنی بر آشوب وجود دارد، مانند آرایه گیتی با قابلیت پیکربندی مجدد[۱۴] (FPGA) [۳۷-۳۸] و پردازشگر سیگنال دیجیتال (DSP) [۳۹]. در ساختارهای مبتنی بر DSP، عملیات پیچیده ریاضی یکی پس از دیگری انجام می‌شود (پردازش متوالی) که زمان اجرا را بسیار طولانی می‌کند. اما ساختارهای FPGA انعطاف‌پذیر هستند و عملیات را به‌صورت موازی اجرا می‌کنند. درنتیجه، هزینه‌های پیاده‌سازی و همچنین زمان اجرا در ساختارهای مبتنی بر FPGA کمتر است.



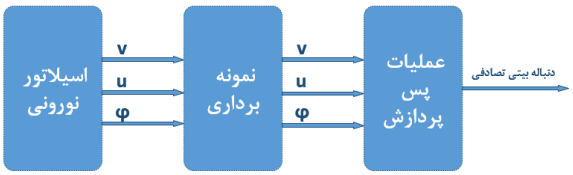

**شکل ۱- نمودار دوشاخگی $u$ برحسب $I_{syn}$: (الف) با در نظر گرفتن اتصال اتاپسی (ب) بدون در نظر گرفتن اتصال اتاپسی**




**شکل ۲- شبیه‌سازی مسیر نمودار فاز مدل نورونی اتاپسی**

مقالات مختلفی در مورد پیاده‌سازی سخت‌افزاری مولد اعداد تصادفی ارائه شده است. zhang و همکاران پیاده‌سازی DSP یک مولد اعداد شبه تصادفی مبتنی بر مدل نورونی هندمارش-رز با در نظر گرفتن اثر القای الکترومغناطیسی ارائه کردند. خواص مناسب دینامیکی این مدل باعث تولید اعداد تصادفی باکیفیت مناسب شده است [۱۶]. Yu و همکاران یک مولد اعداد شبه تصادفی مبتنی بر نوسان‌ساز آشوب شبکه عصبی هاپفیلد تحت القای الکترومغناطیسی ارائه کردند [۱۷]. کیفیت خروجی آشوب در مدل پیشنهادی با توجه به تحلیل دینامیکی مدل مناسب ارزیابی شده است. پیاده‌سازی FPGA این مولد نشان داد با اعمال عملیات پس‌پردازش مبتنی بر XOR کیفیت اعداد تصادفی تولیدی مطلوب می باشد. در مقاله [۴۰] یک مولد اعداد شبه تصادفی بر مبنای سیستم آشوبناک ممریستوری پنج بعدی ارائه و به کمک FPGA پیاده‌سازی شده است. نتایج نشان داد که سیستم ممریستوری پنج بعدی رفتار دینامیکی پیچیده‌ای را ارائه می‌دهدکه برای استفاده در مولدهای اعداد شبه‌تصادفی بسیار مناسب است. نتایج تست اعداد شبه‌تصادفی تولیدی در پیاده‌سازی FPGA نشان داد که کیفیت اعداد تصادفی تولیدی با سرعت ۱۵/۳۷ مگابیت بر ثانیه مناسب است. در مقاله [۴۱] بر مبنای سیستم آشوبناک ممریستوری چهاربعدی یک مولد اعداد شبه تصادفی ارائه و بر بستر FPGA پیاده‌سازی شده است. به‌منظور افزایش نرخ و کیفیت تولید اعداد تصادفی، مولد پیشنهادی علاوه بر سیستم ممریستوری پیشنهادی از منبع دیگر آنتروپی یعنی نقشه برنولی[۱۵] نیز استفاده می‌کند. نتایج حاصل از تست NIST نشان داد که اعداد باینری تولیدی خصوصیات تصادفی مناسبی دارند. نرخ تولید اعداد تصادفی ۶۲/۵ مگابیت بر ثانیه گزارش شده است.

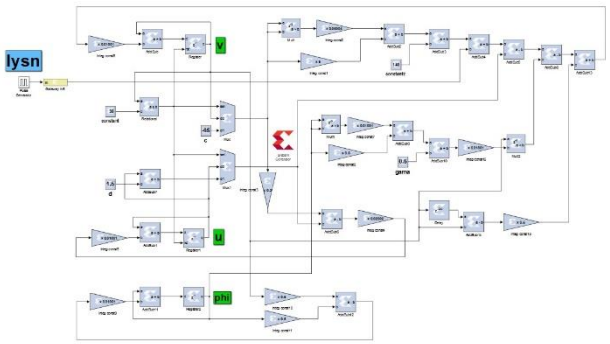
FPGA ها به طور گسترده در امنیت اطلاعات، صنعت، اینترنت اشیا، خودرو، شبکه‌های عصبی مصنوعی، پردازش تصویر و سیستم‌های آشوبناک استفاده می‌شوند [۴۲-۴۶]. بنابراین، در اینجا مولد اعداد شبه تصادفی پیشنهادی روی FPGA پیاده‌سازی می‌شود که در آن از مدل نورون ایزیکویچ اتاپسی برای تولید آشوب (منبع آنتروپی) استفاده می‌گردد.



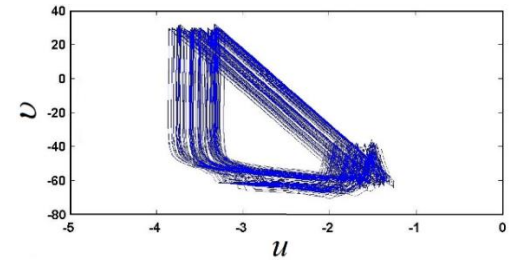

**شکل ۳- بلوک دیاگرام مولد اعداد شبه تصادفی پیشنهادی**

[۱۴] Field Programmable Gate Array

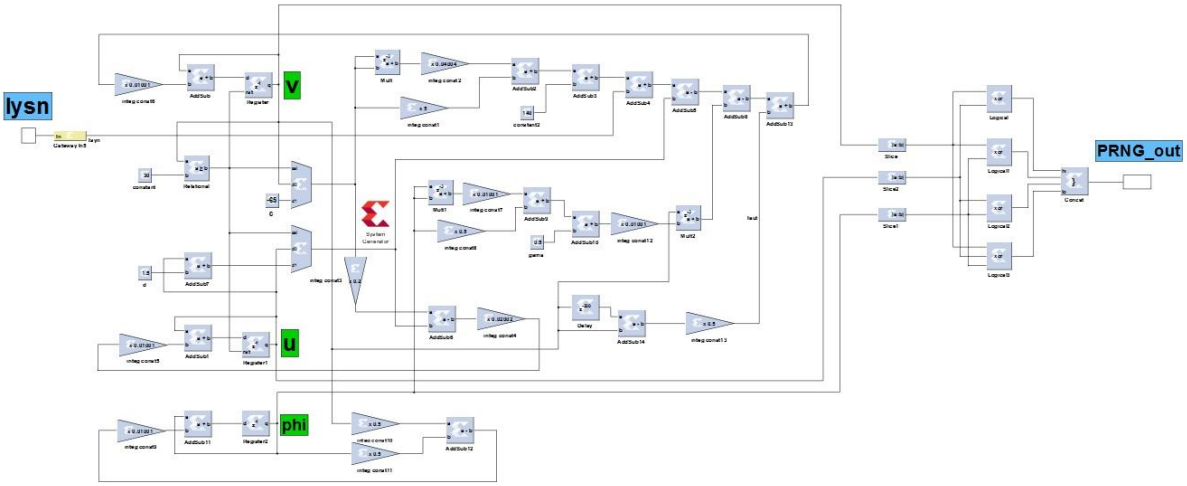
[۱۵] Bernoulli map



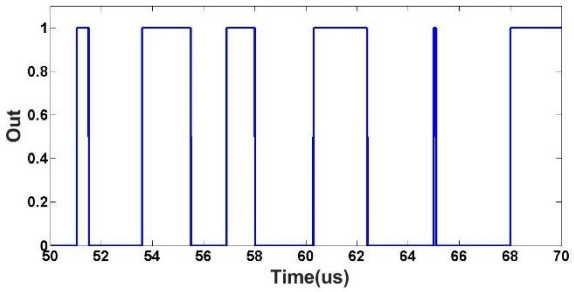

**شکل ۴- پیاده‌سازی دیجیتالی نوسان‌ساز نورونی پیشنهادی با استفاده از ابزار generator system Xilinx**




**شکل ۵- شبیه‌سازی مسیر نمودار فاز نوسان‌ساز نورونی پیاده‌سازی شده با بلوک‌های Xilinx Generator System**




**شکل ۶- معماری دیجیتال مولد اعداد شبه تصادفی پیشنهادی پیاده‌سازی شده با بلوک‌های Xilinx System Generator**




**شکل ۷- نتایج شبیه‌سازی خروجی مولد اعداد شبه تصادفی پیشنهادی پیاده‌سازی شده با بلوک‌های** Generator System Xilinx

### ۳-۱- پیاده‌سازی FPGA

بلوک دیاگرام مولد اعداد شبه تصادفی پیشنهادی در شکل ۳ نشان داده شده است. ماژول‌های نوسان‌ساز نورون، نمونه‌برداری و پس‌پردازش سه ماژول تشکیل‌دهنده مولد اعداد شبه‌تصادفی پیشنهادی مبتنی بر FPGA هستند. از روش اویلر برای مدل‌سازی دیجیتالی نوسان‌ساز نورونی مبتنی بر FPGA استفاده می‌شود. تعداد بیت‌های واحدهای سخت‌افزاری باید به‌گونه‌ای انتخاب شود که از صحت و دقت محاسبات اطمینان حاصل شود. با توجه به محدوده اعداد در معادلات مورد بررسی، تعداد بیت ساختار سخت‌افزاری ۳۲ بیتی (۲۰ بیت برای بخش صحیح و ۱۲ بیت برای بخش کسری) در نظر گرفته شده است. در ماژول نمونه‌برداری فقط ۱۶ بیت (بین ۰ و ۱۵ ) از سیگنال‌های ۳۲ بیتی نوسانگر نورونی برای نمونه‌برداری انتخاب می‌شوند. در ماژول پس پردازش، دو و سه سیگنال ۱۶ بیتی به طور همزمان توسط تابع XOR پردازش می‌شوند به‌طوری‌که مولد اعداد شبه تصادفی اعداد تصادفی ۶۴ بیتی را در هر دوره تکرار تولید می‌کند.

معماری دیجیتالی نوسان‌ساز نورونی با استفاده از ابزار system Xilinx generator در محیط سیمولینک نرم‌افزار MATLAB پیاده‌سازی و در شکل ۴ نشان داده شده است. شکل ۵ نتیجه شبیه‌سازی، مسیر نمودار فاز برای ۹= $I_{syn}$ را برای نوسان‌ساز نورونی پیاده‌سازی شده با بلوک‌های system Xilinx generator را نشان می‌دهد . همان‌طور که مشخص است، این نتایج تقریباً با نتایج در شکل ۲ مطابقت دارد.

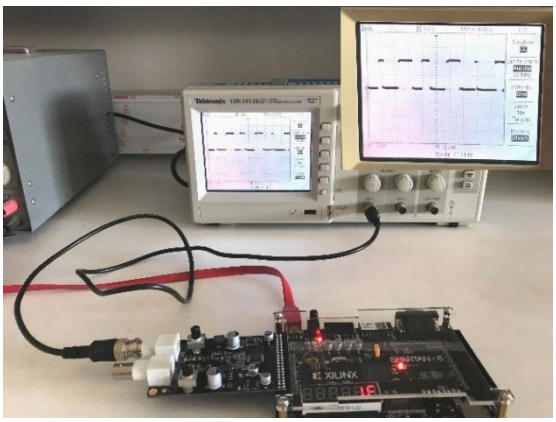
**جدول ۱- هزینه پیاده‌سازی مولد اعداد شبه تصادفی پیشنهادی**

| منابع مصرفی | مولد پیشنهادی | [۴۱] | [۴۰] | [۴۷] |
|---|---|---|---|---|
| Slice registers | ۵۷۴ (٪۵) | ۲۷۳۷۱ | ۲۶۰۵۶ | ۹۴۸ |
| Slice LUTs | (٪۲۷) ۱۵۸۴ | ۲۴۸۳۶ | ۲۰۵۱۷ | ۲۹۴ |
| Number of bonded IOBs | ۸۱ (٪۵۰) | ۳۴ | ۲۰ | ۱۲۹ |
| حداکثر فرکانس کاری(MHz) | ۶۳/۲ | ۱۳۵ | ۱۳۸ | ۳۹۳ |
| نرخ بیت خروجی (Mb/s) | ۱۸/۴ | ۶۲/۵ | ۱۵/۳۷ | --- |
| توان مصرفی (mW) | ۱۰۷ | --- | --- | ۱۱۷ |

شکل ۶ معماری دیجیتال مولد اعداد شبه تصادفی پیشنهادی را نشان می‌دهد که با استفاده از مجموعه بلوک‌های Xilinx در Xilinx System Generator در MATLAB طراحی و اجرا شده است. نتایج شبیه‌سازی خروجی مولد اعداد شبه تصادفی پیشنهادی در شکل ۷ نشان داده شده است. معماری دیجیتالی مولد اعداد شبه تصادفی با ابزار سنتز Xilinx سنتز شده و بر روی تراشه XILINX SPARTAN-۶ XC۶SLX۹ پیاده‌سازی شده است. جدول ۱ هزینه پیاده‌سازی مولد اعداد شبه تصادفی پیشنهادی را نشان می‌دهد.

همان‌گونه که از نتایج مشخص است هزینه پیاده‌سازی سخت‌افزاری مولد پیشنهادی در مقایسه با کارهای مشابه کمتر بوده و فرکانس کاری قابل قبولی را ارائه می‌دهد. همچنین توان دینامیکی و کل توان مصرفی مولد به ترتیب ۷۶ و ۱۰۷ میلی‌وات است که نشان‌دهنده کم‌مصرف بودن ساختار پیشنهادی است. علت پایین بودن توان مصرفی در مولد پیشنهادی کمتر بودن هزینه پیاده‌سازی سخت‌افزاری مولد پیشنهادی در مقایسه با کارهای مشابه و همچنین کمتر بودن فرکانس کاری آن است.

با توجه به تصویر اسیلوسکوپ از دنباله بیتی تصادفی تولیدشده توسط مولد اعداد شبه تصادفی پیشنهادی در شکل ۸ نشان داده شده است. مشاهده می‌شود که نتایج به‌دست‌آمده از پیاده‌سازی سخت‌افزاری و شبیه‌سازی (شکل ۷) بسیار سازگار هستند. فرکانس کاری می‌تواند تا ۶۳/۲ مگاهرتز باشد و نرخ خروجی تولید بیت در مولد اعداد شبه تصادفی پیشنهادی می‌تواند تا ۱۸/۴ مگابیت بر ثانیه افزایش پیدا کند.



**شکل ۸- پیاده‌سازی مولد اعداد شبه تصادفی پیشنهادی و تصویر اسیلوسکوپ از دنباله بیتی تصادفی تولیدشده**

**جدول ۲- نتایج آزمون NIST**

| ردیف | آزمون | p-value | Result |
|---|---|---|---|
| ۱ | Frequency (monobit) | 0.58 | Pass |
| ۲ | Block Frequency | 0.63 | Pass |
| ۳ | Runs | 0.73 | Pass |
| ۴ | longest run of ones | 0.53 | Pass |
| ۵ | Binary matrix rank test | 0.37 | Pass |
| ۶ | Discrete Fourier transform | 0.52 | Pass |
| ۷ | Non-overlapping template | 0.73 | Pass |
| ۸ | Overlapping template matching | 0.47 | Pass |
| ۹ | Maurers universal statistical | 0.56 | Pass |
| ۱۰ | Linear complexity | 0.35 | Pass |
| ۱۱ | Serial test | 0.81 | Pass |
| ۱۲ | Approximate entropy | 0.86 | Pass |
| ۱۳ | Cumulative sums (Forward) | 0.91 | Pass |
| ۱۴ | Random excursions | 0.36 | Pass |

## ۴- تجزیه‌وتحلیل تصادفی بودن اعداد خروجی

در مولدهای اعداد تصادفی، ارزیابی تصادفی بودن اعداد تولیدشده بسیار مهم است. این اعداد باید ارزیابی شوند تا مشخص شود آیا اعداد تولیدشده می‌توانند در برنامه‌های رمزنگاری استفاده شوند یا خیر. روش‌های استاتیک مختلفی برای آزمایش تصادفی بودن توالی بیت‌ها وجود دارد، مانند NIST 800-22 ، AIS31، Diehard و TestU01. مجموعه تست NIST یکی از محبوب‌ترین و معتبرترین ابزارهایی است که به طور گسترده برای آزمایش توالی‌های آشفته استفاده می شود [۴۸] . مجموعه تست NIST دارای ۱۶ تست است و می‌توان از آن برای توالی‌های بیتی با اندازه بزرگ استفاده کرد. دو پارامتر مهم مورداستفاده در آزمون عبارت‌اند از اندازه‌گیری تصادفی‌بودن ( *value-p* ) و سطح معنی‌داری ($\alpha$). توسط NIST توالی‌های بیتی گرفته شده از مولدهای اعداد شبه تصادفی پیشنهادی با استفاده از ۱۰۰۰ توالی نمونه (۱ مگابیت) آزمایش می‌شوند. سطح معنی‌داری در NIST 800-22 روی ۰/۰۱ تنظیم شده است. در این آزمایش، هر دنباله باینری تولیدشده (۱ مگابیت داده ) به ۱۰۰ گروه تقسیم می‌شود، که هر گروه شامل ۱۰۰۰۰ بیت است. اگر مقدار $p$ به‌دست‌آمده از هر آزمون بزرگ‌تر از سطح معنی‌داری باشد (در اینجا، ۰،۰۱)، این نشان می‌دهد که دنباله بیت تولیدشده دارای ویژگی‌های آماری خوبی است و آزمون موفق در نظر گرفته می‌شود. جدول ۲ نتایج آزمون را نشان می‌دهد. نتایج نشان می‌دهد که تمام نتایج آزمون موفقیت‌آمیز بوده‌اند ( $value - p \leq$ ۰،۰۱ )، بنابراین تمام دنباله‌های عددی به‌دست‌آمده تصادفی در نظر گرفته می‌شوند. در جدول ۲، برای ۱۰ نتیجه آزمایش، value-p بزرگ‌تر از ۰/۵ است، که این نشان‌دهنده کیفیت بالای اعداد تصادفی تولیدشده است.

## ۵- نتیجه‌گیری

یک مولد اعداد شبه تصادفی جدید، با سرعت بالا و قوی بر اساس نوسان‌ساز نورونی ایزیکویچ اتاپسی ارائه و بر روی تراشه FPGA پیاده‌سازی شده است. پلتفرم Xilinx generator system برای مدل‌سازی و شبیه‌سازی مولد اعداد شبه تصادفی پیشنهادی استفاده شد. سپس، مدل مبتنی بر Xilinx generator system با استفاده از ابزار سنتز Xilinx سنتز شد و بر روی برد FPGA از نوع XILINX SPARTAN-6 XC6SLX9 پیاده‌سازی شد. نتایج پیاده‌سازی نشان می‌دهد که هزینه پیاده‌سازی مولد اعداد شبه‌تصادفی پیشنهادی نسبت به کارهای مشابه کمتر بوده و همچنین مولد پیشنهادی به حداکثر فرکانس ۶۳/۲ مگاهرتز و نرخ خروجی تولید بیت تا ۱۸/۴ مگابیت بر ثانیه دست می‌یابد. نتایج *p-value* از مجموعه تست NIST کیفیت بالای توالی بیت‌های تصادفی تولیدشده را نشان می‌دهد، به‌طوری‌که برای اکثر نتایج آزمایش، *p-value* بزرگ‌تر از ۰/۵ است.

## مراجع


[1] K. Gu, N. Wu, B. Yin, W. Jia, "Secure data sequence query framework based on multiple fogs", IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1883-1900, 2019.

[۲] ل.صادقی خرمی، ع. صفوی، "طراحی رویتگر امن با ورودی ناشناخته با استفاده از رمزنگاری"، مجله مهندسی برق دانشگاه تبریز، دوره ۵۰، شماره ۲، صفحه ۷۵۷-۷۶۴ ، سال ۱۳۹۹.

[3] K. Gu, X. Dong, L. Wang, "Efficient traceable ring signature scheme without pairings", Advances in Mathematics of Communications, vol. 14, no. 2, pp. 207, 2020.

[4] F. Yu, S. Qian, X. Chen, Y. Huang, S. Cai, J. Jin, S. Du, "Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map", Complexity 2021, 2021.

[5] M. Itoh, "Spread spectrum communication via chaos", International Journal of Bifurcation and Chaos, vol. 9, no. 01, pp.155-213, 1999.

[6] Y. Wang, Z. Liu, J. Ma, H. He, "A pseudorandom number generator based on piecewise logistic map", Nonlinear Dynamics, vol. 83, no. 4, pp. 2373-2391, 2016.

[7] C. Wang, L. Xiong, J. Sun, W. Yao, "Memristor-based neural networks with weight simultaneous perturbation training", Nonlinear Dynamics, vol. 95, no. 4, pp. 2893-2906, 2019.

[8] L. Zhou, F. Tan, F. Yu, "A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks", IEEE Systems Journal, vol. 14, no. 2, pp. 2508-2519, 2019.

[9] Y. Huang, Y. Wang, Y. Zhang, "Shape synchronization of drive-response for a class of two-dimensional chaotic systems via continuous controllers", Nonlinear Dynamics, vol. 78, no. 4, pp. 2331-2340, 2014.

[10] Cicek, Ihsan, Ali Emre Pusane, and Gunhan Dundar. "A new dual entropy core true random number generator." Analog Integrated Circuits and Signal Processing 81, no. 1 (2014): 61-70.

[11] M. Bucolo, R. Caponetto, L. Fortuna, M. Frasca, A. Rizzo, "Does chaos work better than noise?", IEEE Circuits and Systems Magazine, vol. 2, no. 3, pp.4-19, 2002.

[12] H. Hu, L. Liu, N. Ding, "Pseudorandom sequence generator based on the Chen chaotic system", Computer Physics Communications. Vol. 184, no. 3, pp. 765-768, 2013.

[13] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map", Nonlinear Dynamics, vol. 87, no. 1, pp. 407-425, 2017.

[14] A. Akhshani, A. Akhavan, A. Mobaraki, S-C. Lim, Z. Hassan, "Pseudo random number generator based on quantum chaotic map", Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 1, pp. 101-111, 2014.

[15] E. Avaroğlu, I. Koyuncu, A. Bedri Özer, M. Türk, "Hybrid pseudo-random number generator for cryptographic systems", Nonlinear Dynamics, vol. 82, no. 1, pp. 239-248, 2015.

[16] S. Zhang, J. Zheng, X. Wang, Z. Zeng, "Multi-scroll hidden attractor in memristive HR neuron model under electromagnetic radiation and its applications", Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 31, no. 1, pp. 011101, 2021.

[17] F. Yu, Z. Zhang, H. Shen, Y. Huang, S. Cai, J. Jin, S. Du, "Design and FPGA implementation of a pseudo-random number generator based on a Hopfield neural network under electromagnetic radiation", Frontiers in Physics, pp. 302, 2021.

[18] H. Lin, C. Wang, W. Yao, Y. Tan, "Chaotic dynamics in a neural network with different types of external stimuli", Communications in Nonlinear Science and Numerical Simulation, vol.90, pp. 105390, 2020.

[19] P. Kwan, J. Brodie, "Early identification of refractory epilepsy", New England Journal of Medicine, vol. 342, no. 5. Pp. 314-319, 2000.

[20] A.L. Goldberger, D.R. Rigney, B.J. West, "Chaos and fractals in human physiology", Scientific American, vol. 262, no. 2, pp. 42-49, 1990.

[21] A.L. Hodgkin, A.F. Huxley, "A quantitative description of membrane current and its application to conduction and excitation in nerve", The Journal of physiology, vol. 117, no. 4, pp. 500, 1952.

[22] J.L. Hindmarsh, R.M. Rose, "A model of neuronal bursting using three coupled first order differential equations", Proceedings of the Royal society of London. Series B. Biological sciences, vol. 221, no. 1222, 87-102, 1984.

[23] R. FitzHugh, "Impulses and physiological states in theoretical models of nerve membrane", Biophysical journal, vol. 1, no. 6, pp. 445-466, 1961.

[24] J. Nagumo, , S. Arimoto, S. Yoshizawa, "An active pulse transmission line simulating nerve axon", Proceedings of the IRE, vol. 50, no. 10, pp.2061-2070, 1962.

[25] E. M. Izhikevich, "Simple model of spiking neurons", IEEE Transactions on neural networks, vol. 14, no. 6, pp.1569-1572, 2003.

[26] E. M. Izhikevich, "Which model to use for cortical spiking neurons?", IEEE transactions on neural networks, vol. 15, no. 5, pp. 1063-1070, 2004.

[27] H. Wang, J. Ma, Y. Chen, Y. Chen, "Effect of an autapse on the firing pattern transition in a bursting neuron", Communications in Nonlinear Science and Numerical Simulation, vol.19, no. 9, pp. 3242-3254, 2014.

[28] Y. Xu, H. Ying, Y. Jia, J. Ma, T. Hayat, "Autaptic regulation of electrical activities in neuron under electromagnetic induction", Scientific Reports, vol. 7, no. 1, pp.1-12, 2017.

[29] M. Lv, C. Wang, G. Ren, J. Ma, X. Song, "Model of electrical activity in a neuron under magnetic flow effect", Nonlinear Dynamics, vol. 85, no. 3, pp.1479-1490, 2016.

[30] D. Guo, S. Wu, M. Chen, M. Perc, Y. Zhang, J. Ma, Y. Cui, P. Xu, Y. Xia, D. Yao, "Regulation of irregular neuronal firing by autaptic transmission", Scientific reports, vol. 6, no. 1, pp.1-14, 2016.

[31] J. M. Bekkers, "Synaptic transmission: functional autapses in the cortex", Current Biology, vol. 13, no. 11, pp. R433-R435, 2003.

[32] G. Wang, Y. Wu, F. Xiao, Z. Ye, Y. Jia, "Non-Gaussian noise and autapse-induced inverse stochastic resonance in bistable Izhikevich neural system under electromagnetic induction", Physica A: Statistical Mechanics and its Applications, vol. 598, pp.127274, 2022.

[33] S. Nobukawa, H. Nishimura, T. Yamanishi, J. Liu, "Analysis of chaotic resonance in Izhikevich neuron model", PloS one, vol. 10, no. 9, pp. e0138919, 2015.

[34] A. Tamura, T. Ueta, S. Tsuji, "Bifurcation analysis of Izhikevich neuron model." Dynamics of continuous, discrete and impulsive systems, Series A: mathematical analysis, vol. 16, no. 6, pp. 759-775, 2009.

[35] Y. Li, G. Schmid, P. Hänggi, L. Schimansky-Geier, "Spontaneous spiking in an autaptic Hodgkin-Huxley setup", Physical Review E, vol. 82, no. 6, pp. 061907, 2010.

[36] J-L. Danger, S. Guilley, P. Hoogvorst, "High speed true random number generator based on open loop structures in FPGAs", Microelectronics journal, vol. 40, no. 11, pp. 1650-1656, 2009.

[37] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA", IEEE Transactions on Instrumentation and Measurement, vol. 68, no. 1, pp. 291-293, 2018.

[38] I. Koyuncu, M. Tuna, I. Pehlivan, C. Bülent Fidan, M. Alçın, "Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator", Analog Integrated Circuits and Signal Processing, vol. 102, no. 2, pp. 445-456, 2020.

[39] V. Guglielmi, P. Pinel, D. Fournier-Prunaret, A. Taha, "Chaos-based cryptosystem on DSP", Chaos, Solitons & Fractals, vol. 42, no. 4, pp. 2135-2144, 2009.

[40] F. Yu, L. Li, B. He, L. Liu, S. Qian, Z. Zhang, H. Shen, S. Cai, Y. Li, "Pseudorandom number generator based on a 5D hyperchaotic four-wing memristive system and its FPGA implementation", The European Physical Journal Special Topics, vol. 230, no. 7, pp. 1763-1772, 2021.

[41] F. Yu, L. Li, B. He, L. Liu, S. Qian, Y. Huang, S. Cai, "Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map", IEEE Access, vol. 7, pp. 181884-181898, 2019.

[۴۲] پ. دری، ع. قیاسیان، ح. سعیدی، "طراحی و پیاده‌سازی رمزنگار AES در بستر FPGA برای خطوط پرسرعت"، مجله مهندسی برق دانشگاه تبریز، دوره ۴۶، شماره ۱، صفحه ۱۵۳-۱۶۷، سال ۱۳۹۵.

[43] C. A. Lúa, S. D. Gennaro, A. N. Guzman, S. Ortega-Cisneros, J. R. Domínguez, "Digital implementation via FPGA of controllers for active control of ground vehicles", IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2253-2264, 2019.

[44] L. D. Medus, T. Iakymchuk, J. Vicente Frances-Villora, M. Bataller-Mompeán, A. Rosado-Muñoz. "A novel systolic parallel hardware architecture for the FPGA acceleration of feedforward neural networks", IEEE Access, vol. 7, pp. 76084-76103, 2019.

[45] M. Meribout, I. M. Saied, E. Al Hosani, "A new FPGA-based terahertz imaging device for multiphase flow metering", IEEE Transactions on Terahertz Science and Technology, vol. 8, no. 4, pp. 418-426, 2018.

[46] M, Tuna, M. Alçın, I. Koyuncu, C. B. Fidan, I. Pehlivan, "High speed FPGA-based chaotic oscillator design", Microprocessors and Microsystems, vol. 66, pp. 72-80, 2019.

[47] E.A. Hagras, M. Saber, "Low power and high-speed FPGA implementation for 4D memristor chaotic system for image encryption", Multimedia Tools and Applications, vol. 79, no. 31, pp. 23203-23222, 2020.

[48] A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D.Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22 (revised May 15." (2002).