Hindawi
Discrete Dynamics in Nature and Society
Volume 2019, Article ID 2545123, 10 pages
https://doi.org/10.1155/2019/2545123

Research Article

A Survey on True Random Number Generators Based on Chaos

Fei Yu,[1] **Lixiang Li**,[1] **Qiang Tang**,[1] **Shuo Cai**,[1] **Yun Song**,[1] **and Quan Xu**[2]

[1]*School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China*
[2]*School of Information Science and Engineering, Changzhou University, Changzhou 213164, China*

Correspondence should be addressed to Fei Yu; yufeiyfyf@csust.edu.cn and Yun Song; sonie@126.com

Received 16 April 2019; Accepted 28 July 2019; Published 20 December 2019

Academic Editor: J. R. Torregrosa

With the rapid development of communication technology and the popularization of network, information security has been highly valued by all walks of life. Random numbers are used in many cryptographic protocols, key management, identity authentication, image encryption, and so on. True random numbers (TRNs) have better randomness and unpredictability in encryption and key than pseudorandom numbers (PRNs). Chaos has good features of sensitive dependence on initial conditions, randomness, periodicity, and reproduction. These demands coincide with the rise of TRNs generating approaches in chaos field. This survey paper intends to provide a systematic review of true random number generators (TRNGs) based on chaos. Firstly, the two kinds of popular chaotic systems for generating TRNs based on chaos, including continuous time chaotic system and discrete time chaotic system are introduced. The main approaches and challenges are exposed to help researchers decide which are the ones that best suit their needs and goals. Then, existing methods are reviewed, highlighting their contributions and their significance in the field. We also devote a part of the paper to review TRNGs based on current-mode chaos for this problem. Finally, quantitative results are given for the described methods in which they were evaluated, following up with a discussion of the results. At last, we point out a set of promising future works and draw our own conclusions about the state of the art of TRNGs based on chaos.

1. Introduction

In recent years, with the rapid development of the Internet, the requirements for information security in various fields are getting higher and higher, and the security issues are getting more and more attention [1–5]. In the field of information security, encryption algorithm, and key generation are important factors of encryption system; they must be unpredictable [6–9]. In most cryptographic algorithms, random number is an indispensable element, and random number generator (RNG) has important applications in the field of information security, such as generating parameters of public key cryptosystems (such as ECC, RSA) or image encryption [10–12].

According to the different random sequence generated, random numbers can be divided into two categories, namely pseudo-random numbers (PRNs) and true random numbers (TRNs), as shown in Figure 1. PRNs [13, 14] refer to the extension of one seed into another long output sequence by a determined algorithm, which are generally repeatable, so they are widely used in the field of simulation and testing. Unlike PRNs, TRNs [15, 16] cannot be generated by pure mathematical random algorithms, but only by random physical processes. Compared with PRNs, TRNs not only have good statistical characteristics but also have good unpredictability. They could be used in systems with high security requirements.

The typical TRNG structure can be divided into five modules: (1) analog random signal is obtained from the entropy source; (2) sampling and quantifying the random signal; (3) analog-to-digital conversion of the analog signal to output the random number sequence; (4) the sequence obtained at this time does not necessarily satisfy the uniform distribution, and it needs to be processed; and (5) through random number test suite, as shown in Figure 2.

In true random number generators (TRNGs), there are three main types of entropy sources: thermal noise on resistors and capacitors [17, 18], phase jitter of oscillating signals [19–21], chaos [22–24] and others, as shown in Figure 1. For the TRNGs based on thermal noise, the resistance noise is amplified to a suitable range by an ideal amplifier, and then processed by a comparator to compare the amplified noise voltage with the reference level to obtain a digital random signal [17]. In practice, due to the influence of some nonideal

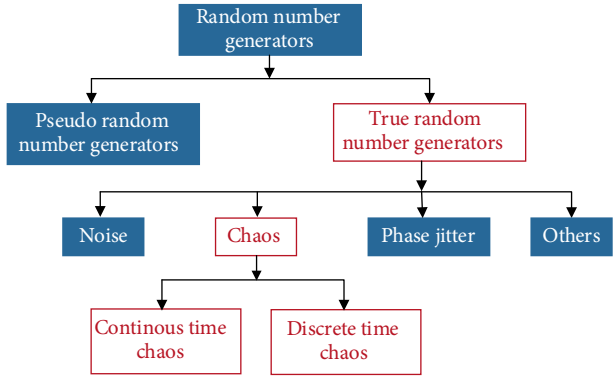

Figure 1: The architecture of random numbers generator.

factors, such as the limited bandwidth of the amplifier, misalignment, periodic noise of the power supply coupled to the system, the randomness of the random number sequence generated by the system will be affected [18]. For the oscillator-based TRNGs, the random source is the phase jitter noise in the ring oscillator in Complementary Metal Oxide Semiconductor (CMOS) circuit [20]. The quality of the random sequence generated by the true random number generator is largely determined by the root mean square (RMS) value of the phase jitter of the low frequency oscillator [21]. But the disadvantage is that it is not suitable for full custom integrated circuit (IC), and the randomness of circuit implementation is low. Compared with the former two methods, the characteristics of chaos, such as nonperiodicity, wide spectrum, unpredictability, and sensitivity to initial conditions [25–28], are in good agreement with the properties of random numbers. Therefore, chaotic theory opens up broad prospects for the design and implementation of TRNGs.

The main contributions of our work are as follows: (1) we provide a broad survey of generating methods that might be useful for TRNGs with chaos; (2) an in-depth and organized review of the most significant methods that use chaos for TRNGs, their origins, and their contributions; (3) we have conducted a comprehensive performance evaluation, which collects quantitative indicators. For example, power, output bit rate, energy and technology, etc.; and (4) a discussion about the above results, and a list of possible future works that may determine the course of upcoming advances, as well as a conclusion summarizing the state of the art of the field.

The remainder of this paper is organized as follows. Firstly, Section 2 describes existing TRNG methods based on chaos, challenges, and benchmarks. It reviews existing methods following two kinds of popular chaotic systems based on their contributions. The TRNGs based on current-mode chaos is described. Other background concepts such as common chaotic model definitions are also reviewed. This section focuses on describing the design techniques and highlights of those methods rather than performing a quantitative evaluation. Then, Section 3 presents a brief discussion on the presented methods based on their quantitative results on the aforementioned TRNGs. In addition, future research directions are also laid out. At last, Section 4 summarizes the paper and draws conclusions about this work and the state of the art of the field.

2. Overview of TRNGs Based on Chaos

Up to date, there are a lot of TRNG structures based on chaos. In this section, we supply a brief introduction about the two most popular and fundamental structures in of TRNG structures based on chaos. Both of them are presented according to a well thought taxonomy of the research completed in the area. We also devote a part of this section to review TRNG based on current-mode chaos for this problem.

2.1. TRNGs Based on Continuous Time Chaotic System. Continuous time chaotic system is a chaotic system based on observation time series, and its state is time-dependent. The mathematical model of continuous time chaotic dynamic system is as follows:

$$\dot{x} = f(x, t), \tag{1}$$

where $x \in R^n$ is the state variable and $f : R^n \times R^n \to R^n$. Common continuous time chaotic systems like Lorenz system [29], Chua's circuit system [30], Jerk system [31], chaotic oscillator [32–34], and many hyperchaotic systems have been proposed [35–37]. Throughout the years, continuous time chaotic systems have been mostly focused on neural network, synchronization, secure communication [38–42], and other fields, especially the design of TRNGs. For that reason, continuous time chaotic circuits are the most abundant ones. In this section, we describe the most popular continuous time chaotic circuits for TRNGs design, considering continuous time chaotic systems that contain any kind of continuous time chaotic circuits representation such as Chua's circuit, Jerk circuit, various chaotic oscillators, and FPGA.

2.1.1. Chua's System. Chua's system is a classical nonlinear electronic circuit, which can show the standard double scroll chaotic dynamic behavior. It was published by Professor Shaotang Cai in 1983. Blaszczyk and Guinee [43] proposed a TRNG which was employed by Chua's circuit and used a simple temperature dependent control resistor in the oscillator circuit and optimal voltage threshold settings. The randomness attributes of the generator were confirmed via PSpice simulation, by the NIST tests for statistical validation. Moqadasi and Ghaznavi-Ghoushchi [44] proposed a TRNG which based on a new Chua's circuit that its negative resistor was a monolithic CMOS based circuit with 12 transistors. This proposed system also consisted of a sample and hold block, an analog to digital converter (ADC) block and a linear feedback shift register (LFSR) block which scrambles generated bit stream and increases randomness, as shown in Figure 3. When the number of LFSR bits changed from 6 to 32, the experiments confirmed that the 6 bits length was optimum for LFSR which was better than previous works.

2.1.2. Jerk System. American scholar Sprott [45] proposed the Jerk system $\dddot{x} = F(\ddot{x}, \dot{x}, x)$, where $\dot{x} = dx/dt$ is the first derivative of position, $\ddot{x} = d^2x/dt^2$ call acceleration,

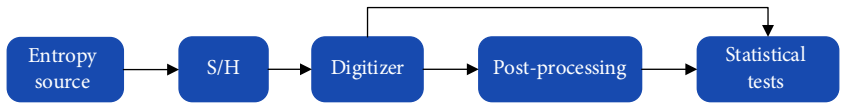

Figure 2: The typical TRNG structure.

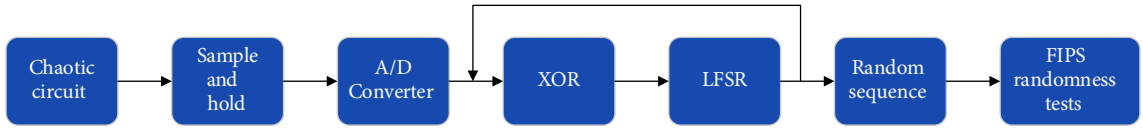

Figure 3: True random number generation from the Chua's circuit core proposed by Moqadasi and Ghaznavi-Ghoushchi.

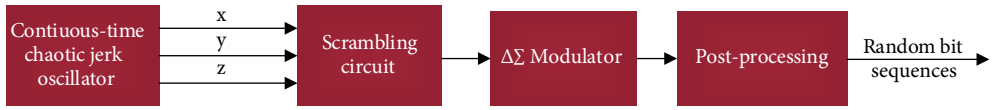

Figure 4: Block diagram of the TRBG with sigma-delta modulation of chaotic jerk signals proposed by Wannaboon et al.

$\dddot{x} = d^3x/dt^3$ call Jerk. Its generalized dimensionless equation of state is:

$$\begin{cases} dx/dt = y, \\ dy/dt = z, \\ dz/dt = -\alpha z - \beta y + f(x), \end{cases} \tag{2}$$

where x, y, z are the state variable, α, β are the system parameters, $f(x)$ is a nonlinear term. In (2), the transformation system of $(x, y, z) \rightarrow (-x, -y, -z)$ can remain unchanged. The system is symmetrical about the origin. Jerk system is characterized by concise equation form and easy circuit realization.

In 2018, Wannaboon et al. [46] presented a fully customized design of TRNG which implemented on a 0.18 μm CMOS technology with unique composition of three major components, chaotic jerk oscillator, $\Delta\sum$ modulator, and simple pre/post-processing. The block diagram of the proposed TRNG is shown in Figure 4. The chaotic Jerk circuit provided chaotic signals with strong robustness and randomness, and exhibited the unique characteristics of smoothly balanced-to-unbalanced alternation of double scroll attractors. In order to improve the resolution of random bit sequence, the continuous time second-order $\Delta\sum$ modulator was introduced as the mixed signal interface without additional clock. The simple structure of shift-registers was implemented as a post-processing process. The bit sequence of the proposed TRNG successfully passed all statistical tests of NIST SP800-22 test suite, and the final output bit rate was 50 Mbps. However, the slight uncertainty of the initial conditions, which is unavoidable in IC implementation, leads to a very large uncertainty after very short time. Because of this, the system behavior can only be predicted for a short time period.

2.1.3. Boolean Chaotic Oscillator. Boolean chaos [47] is a phenomenon in an autonomous network which shows nonrepeating chaotic oscillations, exponential sensitivity to initial conditions, and has a broadband power spectrum. Boolean chaotic oscillator includes Boolean-like state transitions with a fast transition time, and a feedback loop with incommensurate delay inputs. The dynamics of nodes network is described by:

$$x_n(t) = f_n[t, x_1(t - \tau_{n1}), \ldots, x_n(t - \tau_{nm})], \tag{3}$$

where τ_{nm} is the delay time from the nth node to the mth node, $x_n(t)$ is the Boolean logic state at the nth node at time t, and f_n is the logic function for the nth node. Park et al. [48] reported on a TRNG whose randomness derived from a Boolean chaotic oscillator, as shown in Figure 5. Using a CMOS 0.35 μm process, the paper built a CMOS Boolean chaotic oscillator, which consisted of a core chaotic oscillator and a source follower buffer. The generated random bit sequences passed the widely accepted statistical tests used for evaluating cryptographic random number generators.

2.1.4. Jitter Booster Circuit. The nonperiodicity of a chaotic signal implies that the signal has irregular temporal zero crossings as in the case of highly jittered oscillations. The idea of using chaos for enhancing jitter can be an alternative to the multiring oscillator sampling approach. Çiçek and Dündar [49] presented a chaos based integrated jitter booster circuit for multiple oscillator sampling TRNG architecture. The proposed circuit provided an alternative method for enhancing jitter using the chaotic dynamics produced by nonlinear coupling of two ring oscillators, which required fewer components.

2.1.5. Coupled Chaotic Oscillator. Coupled chaotic oscillators are very suitable for monolithic implementation and capable of operating at very high frequencies when appropriate design considerations and experience are exercised. In [50], two integrated continuous-time chaotic oscillators based on cross-coupled $-g_m$ oscillators were presented and their application

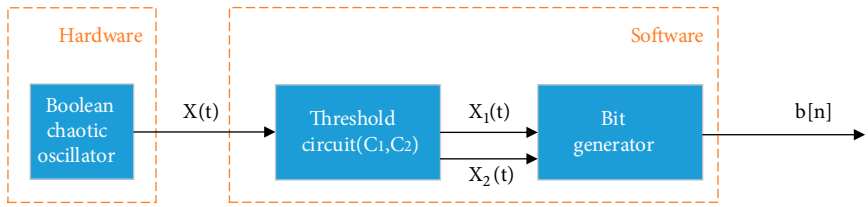

Figure 5: Schematic diagram of random number generation using CMOS Boolean chaotic oscillator.

to random bit generation was described. In [51], a TRNG design was proposed which employed a dual coupled oscillator architecture. This structure improved the output throughput and solved the external interference problems. The frequency of a slower clock modulated the chaotic oscillator output signal, and with the rising edge of the chaotic modulation clock, a faster clock was sampled. The proposed design fulfilled the tests used in both the FIPS-140-2 and the NIST-800-22 random number test suites.

2.1.6. FPGA-Based. Considering technologies mentioned above, the highest performance could be obtained from IC-based chaotic generators. However, IC-based implementations do not promise a flexible use. In addition, the cost of prototyping and testing such systems will be high. FPGA chips are able to run concurrently and have relatively flexible architecture. The cost of design and test cycles of FPGA chips is particularly low [52]. Because of its high-speed and high-quality random generation, FPGA has become a popular platform for implementing random generators or complete cryptographic schemes. Koyuncu and Ozcerit [53] modeled Sundarapandian-Pehlivan chaotic system and simulated in three distinct platforms to show the advantages of FPGA-based chaotic oscillator with respect to alternative solutions. The chaotic system was modeled by the Runge-Kutta (RK4) in hardware description language (VHDL) and the model was synthesized and tested on Xilinx Virtex-6 FPGA chip, the block diagram of an FPGA based TRNG designed is illustrated in Figure 6. The designed chaotic oscillator was tested by TRNG and the maximum operating frequency was 293 MHz with a speed of 58.76 Mbit/s. Akgul et al. [54] used the 3D chaotic system without equilibrium points as the source of entropy built the chaotic system model with FPGA, then designed and implemented the chaotic oscillator with VHDL and RK-4 algorithm, and finally chose the most complex bits of binary numbers to generate random numbers.

2.2. TRNGs Based on Discrete Time Chaotic System. Discrete time chaotic systems also exist widely in the field of nonlinear science, such as physics, biology, and chemistry [55], especially in the generation of TRNs. One-dimensional discrete time nonlinear dynamical systems are defined as follows:

$$x_{k+1} = \tau(x_k), \tag{4}$$

where $x_k, k = 0, 1, 2, \cdots$, are state. And τ is a mapping that mapping the current state x_k to the next state x_{k+1}. If we start with an initial x_0 value and apply τ repeatedly, we get a sequence $\{x_k, k = 0, 1, 2, \cdots\}$. This sequence is called a trajectory of the discrete time dynamic system. Classical discrete time chaotic systems include logistic mapping, tent mapping, Bernoulli mapping, and so on. FPGAs can be used to implement discrete time systems as well, but as far as the author knows, there are few literatures about the realization of TRNGs based on discrete time chaotic systems by using FPGA, so there is no detailed introduction here.

2.2.1. Logistic Mapping. A very simple but widely studied dynamical system is logistic mapping, which originates from the insect population model. Its definition has many forms: (1) $x_{k+1} = \mu x_k (1 - x_k)$, when $3.5699456 \cdots \leq \mu \leq 4$, logistic mapping works in chaotic state; (2) $x_{k+1} = 1 - \gamma x_k^2$, when $\gamma \in (1.5437, 2)$, logistic mapping works in chaotic state; (3) $x_{k+1} = \mu x_k - x_k^2$, when $\mu \in (3.5699, 4)$, logistic mapping works in chaotic state. It can be seen that logistic mapping is actually a first-order equation, which requires initialization conditions and control parameters. Therefore, it is easy to implement in hardware, and people often use this mapping to design TRNGs.

In 2015, Avaroğlu et al. [56] used logistic map in post-processing to ensure that numbers generated by RO-based TRNG were of high quality. In order to observe the influences of the logistic map, four different scenarios considering RO-based TRNG structure were studied. [57] proposed a TRNGs with graphics processing units as the source of entropy, unpredictable behavior of which was managed by computing logistic maps, and high throughput achieved 447.83 Mbit/s. Tuncer [58] applied the random challenges from the logistic map to physical unclonable functions based on ring oscillator (RO-PUF) to generate random numbers in real time in FPGA, which prevented the PUF from being attacked (cracked) and improved the randomness of the random numbers. Because the value distribution of logistic mapping points is too centralized and blank bands appear in other regions, the uniform distribution characteristics of the mapping points are poor, so that logistic mapping needs post-processing (Von Neumann corrector [59], XOR correctors [60], one-way hash function [61], etc.) to achieve uniform distribution. At the same time, logistic mapping reduces the speed of generating random numbers and has a higher tolerance for the performance of the FPGA.

2.2.2. Tent Mapping. Tent mapping is a piecewise linear one-dimensional mapping with uniform probability density function (PDF), power spectral density (PSD). And the iteration speed of tent mapping is faster than that of Logistic mapping. Angulo et al. [62] constructed a discrete chaotic

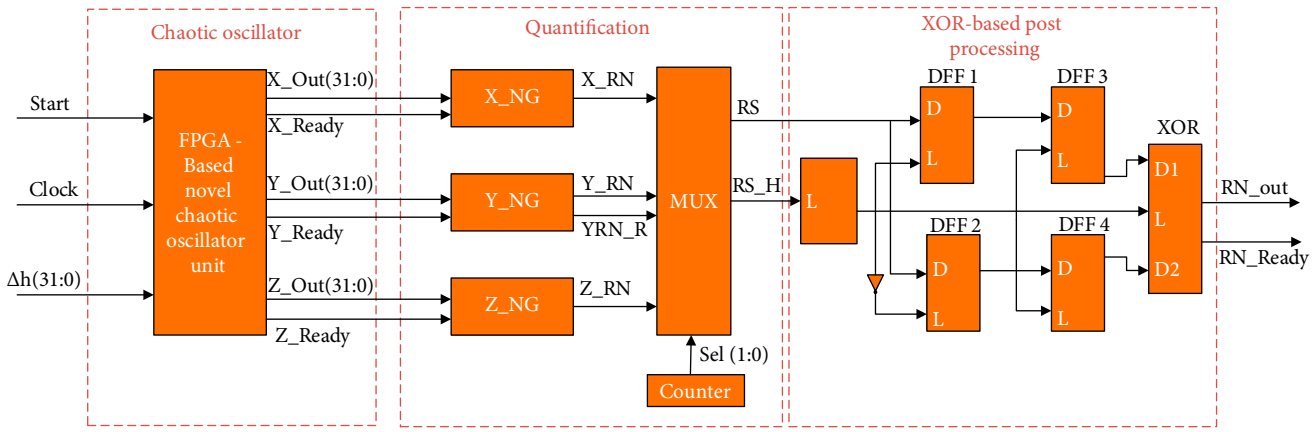

Figure 6: Block diagram of FPGA-based chaotic TRNG.

oscillator with tent mapping, buffer and clock generator, and then generated random numbers by 8 bit LFSR corrector. A low power real random number generator based on discrete-time chaos was designed and implemented using standard CMOS AMS 0.35 μm process. Cicek et al. [63] used a one-dimensional discrete-time skew tent map as the entropy source to design TRNGs. A practical information measurement method was used to determine the maximum allowable parameter range, and a current mode skew tent circuit was designed to verify the method. Teh and Samsudin [64] proposed a new AEAD (authenticated encryption with associated data) scheme that was implemented with true random number generators based on the chaotic tent map. However, there were small periodic and unstable periodic points in the tent iteration sequence, it would degrade the random performance and reduce the security.

2.2.3. Bernoulli Mapping. Bernoulli mapping is a linear mapping consisting of two piecewise linear parts, which are separated by discontinuous points and are often used in random number generators. In 2014, Cicek et al. [65] proposed a dual entropy core TRNG architecture, by using Bernoulli mapping as the entropy source, and using FPGA to successfully design and implement the proposed architecture. Compared with the single entropy core, this architecture has a wide range of control parameter values, and the stochastic performance is better. However, the single Lyapunov index and limited entropy of bernoulli mapping leads to higher cost. In 2019, Hsueh and Chen [66] proposed an ultra-low voltage chaos-based true random number generator for IoT applications. The authors used folded Bernoulli mapping to generate random numbers. In the switched-capacitor chaotic circuits, bulk-driven amplifiers were used to alleviate gate leakage issue, two-stage comparators were used to increase voltage headroom.

2.2.4. Piece-Wise Affine Markov (PWAM) Mapping. PWAM mapping is piecewise one-dimensional Markov mapping which has infinite folding property with uniform distribution in finite intervals to enhance robustness in simulation implementation. The state interval $[-1, 1]$ of an exact extensible mapping $M : [-1, 1]|\rightarrow [-1, 1]$ is divided into n sub-intervals $X_i, i = 1, 2, \cdots, n$. For any interval X_i and X_j, or $M(X_i) \cap X_j = \emptyset$ or $X_i \subset (X_j)$, then the mapping M is also called the PWAM mapping of the piecewise interval. Milos and Pavol [67] proposed PWAM mapping to the switched capacitor based hybrid signal PSoC devices to reduce the impact of circuit imperfections on the quality of random bit streams. Pareschi et al. [68] proposed two methods of rearranging a pipelined ADC to generate random bit stream using discrete chaotic circuit as entropy source. The two methods were compared with the traditional methods. The CMOS technology of 0.35 μm and 0.18 μm were used to realize the two methods, respectively. PWAM mapping is better than traditional mappings in security, randomness, and other aspects, but its equations and implementation are more complex than traditional mappings.

2.2.5. Discrete Time Chaotic Oscillator. Discrete time chaotic oscillator is one of the most interesting topics of research and the designing of the circuit been extensively studied for many decades. A common structure of discrete time chaotic oscillator is shown in Figure 7. It can be seen that this chaotic oscillator consisted of three parts of circuit, a nonlinear circuit to represents the chaotic map, two sample-and-hold circuits (S/H) to track and store the signals as a memory and the buffer to carry signals to the next stage implemented by a two-stage operational amplifier (op-amp). Dhanuskodi et al. [69] had proposed a TRNG based on chaotic ring oscillator. In order to pass the statistical test, XOR was used to post-process the random number generated by the chaotic ring oscillator. The output bitstream of TRNG implemented in 45 nm CMOS process was tested by NIST test suite and it passed 11 tests with throughput of 127 MB/s. Jiteurtragool et al. [70] proposed a TRNG for discrete time chaotic oscillator based on 0.18 μm CMOS technology. A chaotic oscillator was designed by using three transistor mapping circuits and approximating V-shaped mapping as a chaotic nonlinear function. In order to improve the randomness of the output signal, the double oscillator and XOR were used to sample the random signal generated by the chaotic oscillator. The random number generated by the processing technology

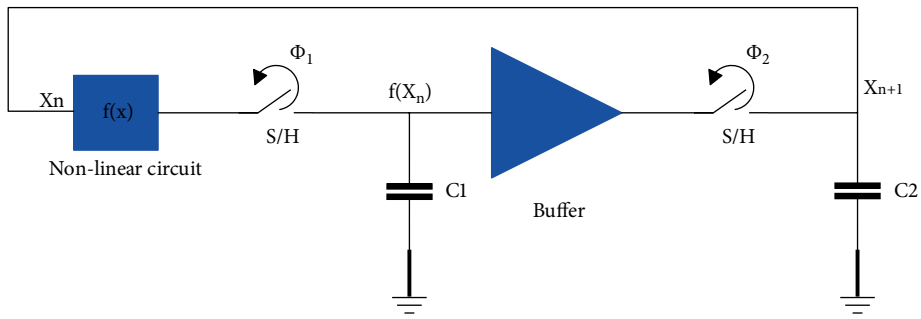

Figure 7: A common structure of discrete-time chaotic oscillator.

was evenly distributed, and the final output bit rate was 23 MB/s.

2.3. TRNGS Based on Current-Mode Chaos. One of the main drawbacks of chaotic RNG integrated circuits is the robustness of the system. Chaotic nonlinear finite difference equation (FDE) is very sensitive to the coefficients of the equation [71]. Therefore, the circuit for realizing chaotic FDE must be very precise and have narrower boundaries than other analog applications. Small variations in coefficients can also be attributed to external effects, such as power supply voltage, temperature, and process variations [72].

Many chaotic circuits are implemented in switched capacitor voltage-mode. Contrary to current-mode, voltage-mode circuits require large capacitors and high gain amplifiers, which consume both power and area [73]. In addition, in sub-100 nm technology, the leakage current of the capacitor is larger, and its capacitance value has higher dispersion, which reduces the robustness of voltage mode design [74–77]. In recent years, the realization of chaotic oscillation circuits by current mode devices has become a new research direction, such as current followers (CF) [78], second-generation current conveyor (CCII) [79], current controlled current conveyor (CCCII) [80], current-feedback operational amplifier (CFOA) [81], Operational Transconductance Amplifier (OTA) [82] and unity-gain cells (UGCs) [83], etc. Katz et al. [84] proposed a robust TRNG based on a differential current-mode chaos which was implemented on 90 nm CMOS-SOI technology. The differential design also showed excellent robustness to power supply voltage, temperature and process changes. In order to verify that the circuit could be used as a white noise generator, according to the suggestion of Federal Information Processing Standard (FIPS), the simulation results were tested and verified on hardware.

3. Discussion

In the previous section we reviewed the existing TRNGs based on chaos from a literary and qualitative point of view, i.e., Figure 8 shows a graph of the reviewed methods for the TRNGs based on chaos. In this Section we are going to discuss the merits and demerits of TRNGs based on chaos.

Discrete time chaos has long been used in TRNG, but recent studies have shown that continuous time oscillators can also be used in TRNG. The application of discrete time chaos is well known, but there are few experimental reports on integrated circuits, most of them use FPGA to realize TRNGs. Continuous time chaos is easy to integrate, but it needs to be discretized before sampling. TRNG based on discrete time chaos dynamically controls the evolution and bit generation speed by adjusting the clock signal. Table 1 summarizes the implementation methods of chaos-based TRNGs in recent years.

According to the random bit rate requirement of output per second, it can be defined as:

$$\text{Bit Rate} = \frac{\text{Power Dissipation (mW)}}{E_b \text{ (nJ/bit)}}. \tag{5}$$

As can be seen from Table 1, by comparing the output bit rates of all continuous time chaotic oscillators, it can be seen that the speed of Boolean chaotic oscillator in [48] is much higher than that of other TRNGs based on continuous time chaotic oscillators. Meanwhile, the power of Boolean chaotic oscillator in [48] is much larger than that in [47]. Because of the low frequency and narrow bandwidth of chaos, TRNG is based on the traditional chaotic oscillator as the source of entropy, such as Chua's circuit [44], Jerk circuit [46], no-equilibrium chaotic system [54], etc. By comparing the output bit rates of all TRNGs based on discrete time chaos, we can see that the speed of [57] is much faster than that of other chaotic output bits, because it is realized by CPU. In addition, [67] provides higher throughput than most designs in lower regions, reaching 127 Mbit/s. In [69], besides the inherent chaos, the oscillator also collects physical noise, and uses the combination of two light sources to improve the output speed of the oscillator. Compared with the TRNG's area of the same CMOS process, under 0.35 μm CMOS process in [48], [62] and [69], the largest area is [69]. The reason is that the authors used eight-stage pipeline ADC and two-stage pipeline ADC to design circuits. ADC is often used to design chaotic maps to generate random numbers, speed is better, but it takes up a large area.

4. Conclusion and Future Work

To identify the state-of-the-art in the area of TRN and to find out what we know about TRNGs based on chaos, we conducted and presented in this article a systematic literature mapping. The purpose of this article is to help readers

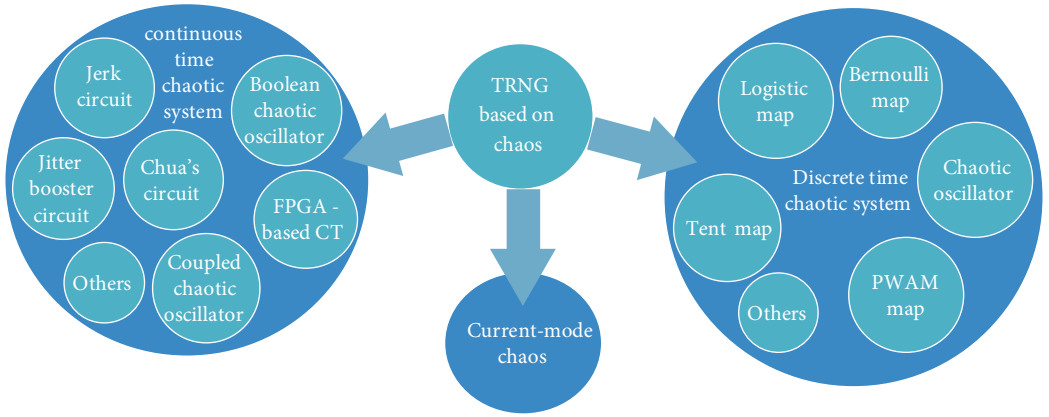

Figure 8: A graph of the reviewed methods for the TRNGs based on chaos.

Table 1: Summary of TRNGs methods based on chaos.

Classification	Author and reference	Area (mm^2)	Power (mW)	Out bit rate (speed) (Mbit/s)	Energy (PJ/bit)	Post processing	Test suite	Technology
Chua's system	Moqadasi [44]	N/A	N/A	2.02	N/A	6 bit LFSR	FIPS 140-1	0.18 μm CMOS
Jerk system	Wannaboon [46]	0.037689	1.32	50	26.4	Von Neumann	NIST SP800-22 and TestU01	0.18 μm CMOS
Boolean chaotic oscillator	Park [48]	0.057	26.1	300	87	XOR	NIST	0.35 μm CMOS
Coupled chaotic oscillator	Ozoguz [51]	N/A	N/A	2	N/A	Von Neumann	FIPS 140-1 and NIST	0.35 μm CMOS
FPGA-based	Akgul [54]	N/A	N/A	4.59	N/A	XOR	FIPS 140-1 and NIST SP800-22	FPGA
Logistic mapping	Avaroglu [56]	N/A	N/A	20	N/A	RO and inverter number	NIST SP800-22 and TestU01	FPGA
Logistic mapping	Teh [57]	N/A	N/A	447.83	N/A	XOR and32-bit addition	NIST SP 800-22	CPU
Tent mapping	Angulo [62]	0.07	0.15	0.25	800	8 bit LFSR	NIST	0.35 μm CMOS
Bernoulli mapping	Cicek [65]	N/A	125	1.5	83300	N/A	NIST SP800-22	FPGA
PWAM mapping	Pareschi [68]	0.752	29	40	0.725	N/A	NIST SP800-22	0.35 μm CMOS
Discrete-timechaotic oscillator	Dhanuskodi [69]	93.1	1.0967	127	8	XOR	NIST	0.45 μm CMOS
Current-modechaos	Katz [80]	0.02	0.8	25	32	N/A	FIPS 140-2	0.09 μm CMOS

(including practitioners and researchers) conduct the most comprehensive survey in the field of TRNG based on chaos. In the end, the research results are discussed, which provides useful insights for future research directions and open issues in this field. From this study, we can draw a general conclusion that TRNGs based on chaos has obtained many successful cases, but it is still an open problem, and its solution will prove very useful for wide application.

By classifying the entire body of knowledge, this survey paper "mapped" the body of knowledge on TRNGs based on chaos. We systematically classified a large set of 85 papers and investigated several review structures under three groups. The first group investigated the contribution as well as the TRNGs based on continuous time chaotic systems. The second group investigated the mappings for TRNGs based on discrete time chaotic systems. The third group investigated the TRNGs based on current-mode chaos.

In recent years, it has been proved that continuous time chaotic systems can be used in the design of TRNGs. Because the number of positive Lyapunov exponents of entropy sources is limited, so hyperchaotic systems used in TRNGs is one of the important development directions in the future. It can be seen that PRNGs based on discrete-time chaos have developed from one-dimensional to two-dimensional and multi-dimensional, so the design of TRNGs using multi-dimensional discrete-time chaotic map is also the future research direction.

The current-mode devices have good frequency gain characteristics and the bandwidth of these kind of devices are almost independent of gain, so there are no need to weigh the gain and bandwidth in the design circuit, which can improve the working frequency of the circuit. Therefore, using current mode devices to realize TRNGs have gradually become a new research direction.

Recently, a TRBG based on a memristive chaotic circuit was proposed in [85]. The proposed TRBG structure used a memristive canonical Chua's oscillator and a logistic mapping as the entropy source, while the XOR function was used for post-processing. It can be seen that TRBGs based on memristive chaotic system and multi-entropy sources will be an important development direction in the future.

As future work, we are committed to improving the out bit rate, randomness and development cost of TRNG solutions and applications. There are three very important research groups, many of which are under development based on chaos of current mode devices or memristive chaotic system or multi-entropy sources, like combination of continuous-time chaotic system and discrete-time chaotic system. We are currently analysing how to study different solutions and other suggestions in these approaches.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China under Grants 61504013, 61772087, 61702052 and 61801054, and by the Natural Science Foundation of Hunan Province under Grants 2019JJ50648 and 2016jj2005, and by the Scientific Research Fund of Hunan Provincial Education Department under grants 18B162 and 18A137 and by the National Key Research and Development Project under Grant 2018YFE0111200.

References

[1] L. Zhou, F. Tan, and F. Yu, "A robust synchronization-based chaotic secure communication scheme with double-layered and multiple hybrid networks," *IEEE Systems Journal*, pp. 1–12, 2019.

[2] K. Gu, W. Jia, G. Wang, and S. Wen, "Efficient and secure attribute-based signature for monotone predicates," *Acta Informatica*, vol. 54, no. 5, pp. 521–541, 2017.

[3] Z. Xia, Z. Fang, F. Zou, J. Wang, and A. K. Sangaiah, "Research on defensive strategy of real-time price attack based on multiperson zero-determinant," *Security and Communication Networks*, vol. 2019, Article ID 6956072, 13 pages, 2019.

[4] K. Gu, N. Wu, B. Yin, and W. Jia, "Secure data query framework for cloud and fog computing," *IEEE Transactions on Network and Service Management*, 2019.

[5] K. Gu, Y. Wang, and S. Wen, "Traceable Threshold Proxy Signature," *Journal of Information Science and Engineering*, vol. 33, pp. 63–79, 2017.

[6] S. He, W. Zeng, K. Xie, H. Yang, M. Lai, and X. Su, "PPNC: privacy preserving scheme for random linear network coding in smart grid," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 3, pp. 1510–1533, 2017.

[7] K. Gu, N. Wu, B. Yin, and W. Jia, "Secure data sequence query framework based on multiple fogs," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[8] K. Gu, K. Wang, and L. Yang, "Traceable attribute-based signature," *Journal of Information Security and Applications*, vol. 49, pp. 1–13, 2019.

[9] K. Gu, X. Dong, and L. Wang, "Efficient traceable ring signature scheme without pairings," *Advances in Mathematics of Communications,* 2019.

[10] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, p. 1950115, 2019.

[11] M. Long, F. Peng, and H. Y. Li, "Separable reversible data hiding and encryption for HEVC video," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 171–182, 2018.

[12] F. Peng, X. W. Zhu, and M. Long, "An ROI. privacy protection scheme for H.264 video based on FMO and chaos," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 10, pp. 1688–1699, 2013.

[13] F. Yu, L. Li, B. He et al., "Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map," *IEEE Access*, 2019.

[14] A. A. Rezk, A. H. Madian, A. G. Radwan, and A. M. Soliman, "Reconfigurable chaotic pseudo random number generator based on FPGA," *AEU-International Journal of Electronics and Communications*, vol. 98, pp. 174–180, 2019.

[15] R. S. Hasan, S. K. Tawfeeq, N. Q. Mohammed, and A. I. Khaleel, "A true random number generator based on the photon arrival time registered in a coincidence window between two single-photon counting modules," *Chinese Journal of Physics*, vol. 56, no. 1, pp. 385–391, 2018.

[16] M. M. Abutaleb, "A novel true random number generator based on QCA nanocomputing," *Nano Communication Networks*, vol. 17, pp. 14–20, 2018.

[17] E. Kim, M. Lee, and J.-J. Kim, "8.2 8 Mb/s 28 Mb/mJ robust true-random-number generator in 65 nm CMOS based on differential ring oscillator with feedback resistors," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 144–145, IEEE, San Francisco, CA, USA, 2017.

[18] M. Drutarovsky and P. Galajda, "A robust chaos-based true random number generator embedded in reconfigurable switched-capacitor hardware," in *17th International Conference Radioelektronika*, pp. 1–6, IEEE, Brno, Czech Republic, 2007.

[19] E. Bejar, J. Saldana, E. Raygada, and C. Silva, "On the jitter-to-fast-clock-period ratio in oscillator-based true random number generators," in *24th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, pp. 243–246, IEEE, Batumi, Georgia, 2017.

[20] Y. Yang, G. Bai, and H. Chen, "A 200Mbps random number generator with jitter-amplified oscillator," in *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pp. 1–5, IEEE, Hefei, China, 2014.

[21] T. Amaki, M. Hashimoto, and O. Takao, "Jitter amplifier for oscillator-based true random number generator," in *16th Asia and South Pacific Design Automation Conference (ASP-DAC 2011)*, pp. 81–82, IEEE, Yokohama, Japan, 2011.

[22] X. Li, G. Zhang, and Y. Liao, "Chaos-based true random number generator using image," in *2011 International Conference on Computer Science and Service System (CSSS)*, pp. 2145–2147, IEEE, Nanjing, China, 2011.

[23] S. Ergun, "Lessons learnt from the cryptanalysis of a chaos based random number generator," in *IEEE EUROCON 2017–17th International Conference on Smart Technologies*, pp. 197–200, IEEE, Ohrid, Macedonia, 2017.

[24] M. Kim, U. Ha, Y. Lee, K. Lee, and H.-J. Yoo, "A 82nW chaotic-map true random number generator based on sub-ranging SAR ADC," in *42nd European Solid-State Circuits Conference*, pp. 157–160, IEEE, Lausanne, Switzerland, 2016.

[25] F. Yu, L. Gao, K. Gu, B. Yin, Q. Wan, and Z. Zhou, "A fully qualified four-wing four-dimensional autonomous chaotic system and its synchronization," *Optik*, vol. 131, pp. 79–88, 2017.

[26] J. Jin and L. V. Zhao, "Low voltage low power fully integrated chaos generator," *Journal of Circuits, Systems and Computers*, vol. 27, no. 10, p. 1850155, 2018.

[27] L. Zhou, C. Wang, and L. Zhou, "A novel no-equilibrium hyperchaotic multi-wing system via introducing memristor," *International Journal of Circuit Theory and Applications*, vol. 46, no. 1, pp. 84–98, 2018.

[28] L. Zhou, C. Wang, X. Zhang, and W. Yao, "Various attractors, coexisting attractors and antimonotonicity in a simple fourth-order memristive twin-T oscillator," *International Journal of Bifurcation and Chaos*, vol. 28, no. 4, p. 1850050, 2018.

[29] B. Munmuangsaen and B. Srisuchinwong, "A hidden chaotic attractor in the classical Lorenz system," *Chaos, Solitons & Fractals*, vol. 107, pp. 61–66, 2018.

[30] J. Yang and L. Zhao, "Bifurcation analysis and chaos control of the modified Chua's circuit system," *Chaos, Solitons & Fractals*, vol. 77, pp. 332–339, 2015.

[31] C. Wang, H. Xia, and L. Zhou, "A memristive hyperchaotic multiscroll jerk system with controllable scroll numbers," *International Journal of Bifurcation and Chaos*, vol. 27, no. 6, p. 1750091, 2017.

[32] J. Jin, "Programmable multi-direction fully integrated chaotic oscillator," *Microelectronics Journal*, vol. 75, pp. 27–34, 2018.

[33] F. Yu, P. Li, K. Gu, and B. Yin, "Research progress of multi-scroll chaotic oscillators based on current-mode devices," *Optik*, vol. 127, pp. 5486–5490, 2016.

[34] X. Zhang, C. Wang, W. Yao, and H. Lin, "Chaotic system with bondorbital attractors," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2159–2174, 2019.

[35] J. Jin and L. Cui, "Fully integrated memristor and its application on the scroll-controllable hyperchaotic system," *Complexity*, vol. 2019, Article ID 4106398, 8 pages, 2019.

[36] X. Zhang and C. Wang, "Multiscroll hyperchaotic system with hidden attractors and its circuit implementation," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, p. 1950117, 2019.

[37] F. Yu, L. Liu, B. He, et al., "Analysis and FPGA realization of a novel 5D hyperchaotic four-wing memristive system, active control synchronization, and secure communication application," *Complexity*, vol. 2019, Article ID 4047957, 18 pages, 2019.

[38] F. Yu, L. Liu, L. Xiao, K. Li, and S. Cai, "A robust and fixed-time zeroing neural dynamics for computing time-variant nonlinear equation using a novel nonlinear activation function," *Neurocomputing*, vol. 350, pp. 108–116, 2019.

[39] Y. Huang, Y. Wang, H. Chen, and S. Zhang, "Shape synchronization control for three-dimensional chaotic systems," *Chaos, Solitons & Fractals*, vol. 87, pp. 136–145, 2016.

[40] L. Zhou, F. Tan, F. Yu, and W. Liu, "Cluster synchronization of two-layer nonlinearly coupled multiplex networks with multi-links and time-delays," *Neurocomputing*, vol. 359, pp. 264–275, 2019.

[41] W. Yao, C. Wang, and J. Cao, "Hybrid multisynchronization of coupled multistable memristive neural networks with time delays," *Neurocomputing*, vol. 363, pp. 281–294, 2019.

[42] F. Yu and C. Wang, "Secure communication based on a four-wing chaotic system subject to disturbance inputs," *Optik*, vol. 125, no. 20, pp. 5920–5925, 2014.

[43] M. Blaszczyk and R. A. Guinee, "A true random binary sequence generator based on chaotic circuit," in *IET Irish Signals and Systems Conference (ISSC 2008)*, pp. 294–299, IET, Galway, Ireland, 2008.

[44] H. Moqadasi and M. B. Ghaznavi-Ghoushchi, "A new Chua's circuit with monolithic Chua's diode and its use for efficient true random number generation in CMOS 180 nm," *Analog Integrated Circuits and Signal Processing*, vol. 82, no. 3, pp. 719–731, 2015.

[45] J. C. Sprott, "Simple chaotic systems and circuits," *American Association of Physics Teachers*, vol. 68, pp. 758–763, 2000.

[46] C. Wannaboon, M. Tachibana, and W. San-Um, "A 0.18- CMOS high-data-rate true random bit generator through modulation of chaotic jerk circuit signals," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 6, p. 063126, 2018.

[47] R. Zhang, H. L. D. de S.Cavalcante, Z. Gao et al., "Boolean chaos," *Physical Review E*, vol. 80, no. 4, p. 045202, 2009.

[48] M. Park, J. C. Rodgers, and D. P. Lathrop, "True random number generation using CMOS Boolean chaotic oscillator," *Microelectronics Journal*, vol. 46, no. 12, pp. 1364–1370, 2015.

[49] İ. Çiçek and G. Dündar, "A chaos based integrated jitter booster circuit for true random number generators," in *2013 European Conference on Circuit Theory and Design (ECCTD)*, pp. 1–4, IEEE, Dresden, Germany, 2013.

[50] S. Ozoguz, A. S. Elwakil, and S. Ergun, "Cross-coupled chaotic oscillators and application to random bit generation," *IEE Proceedings-Circuits, Devices and Systems*, vol. 153, no. 5, pp. 506–510, 2006.

[51] S. Ergun and S. Ozoguz, "Truly random number generators based on non-autonomous continuous-time chaos," *International Journal of Circuit Theory and Applications*, vol. 38, no. 1, pp. 1–24, 2010.

[52] J.-L. Zhang, W.-Z. Wang, X.-W. Wang, and Z.-H. Xia, "Enhancing security of FPGA-based embedded systems with combinational logic binding," *Journal of Computer Science and Technology*, vol. 32, no. 2, pp. 329–339, 2017.

[53] I. Koyuncu and A. T. Ozcerit, "The design and realization of a new high speed FPGA-based chaotic true random number generator," *Computers & Electrical Engineering*, vol. 58, pp. 203–214, 2017.

[54] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, and A. Istanbullu, "Chaos-based engineering applications with a 3D chaotic system without equilibrium points," *Nonlinear Dynamics*, vol. 84, no. 2, pp. 481–495, 2016.

[55] H. S. Steven, *Nonlinear Dynamics and Chaos-with Applications to Physics, Biology, Chemistry, and Engineering*, CRC Press, 2nd edition, 2014.

[56] E. Avaroğlu, T. Tuncer, A. B. Özer, B. Ergen, and M. Türk, "A novel chaos-based post-processing for TRNG," *Nonlinear Dynamics*, vol. 81, no. 1-2, pp. 189–199, 2015.

[57] J. S. Teh, A. Samsudin, M. Al-Mazrooie, and A. Akhavan, "GPUs and chaos: a new true random number generator," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1913–1922, 2015.

[58] T. Tuncer, "The implementation of chaos-based PUF designs in field programmable gate array," *Nonlinear Dynamics*, vol. 86, no. 2, pp. 975–986, 2016.

[59] B. S. Vikram and P. B. Wayne, "Entropy extraction in metastability-based TRNG," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 135–140, IEEE, Anaheim, CA, USA, 2010.

[60] B. S. Vikram and P. B. Wayne, "Entropy and energy bounds for metastability based TRNG with lightweight post-processing," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, pp. 1785–1793, 2015.

[61] Y. F. Wang, "Research and design of true random number generator [Master Dissertation]," *Zhejiang University*, 2010.

[62] J. A. A. Angulo, E. Kussener, H. Barthelemy, and B. Duval, "Discrete chaos-based random number generator," in *2014 IEEE Faible Tension Faible Consommation (FTFC)*, pp. 1–4, IEEE, Monaco, 2014.

[63] I. Cicek, A. E. Pusane, and G. Dundar, "A novel design method for discrete time chaos based true random number generators," *Integration,* vol. 47, no. 1, pp. 38–47, 2014.

[64] J. S. Teh and A. Samsudin, "A chaos-based authenticated cipher with associated data," *Security and Communication Networks*, vol. 2017, Article ID 9040518, 15 pages, 2017.

[65] I. Cicek, A. E. Pusane, and G. Dundar, "A new dual entropy core true random number generator," *Analog Integrated Circuits and Signal Processing*, vol. 81, no. 1, pp. 61–70, 2014.

[66] J. C. Hsueh and V. H. C. Chen, "An ultra-low voltage chaos-based true random number generator for IoT applications," *Microelectronics Journal*, vol. 87, pp. 55–64, 2019.

[67] D. Milos and G. Pavol, "Chaos-based true random number generator embedded in a mixed-signal reconfigurable hardware," *Journal of Electrical Engineering*, vol. 57, pp. 218–225, 2006.

[68] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 12, pp. 3124–3137, 2010.

[69] S. N. Dhanuskodi, A. Vijayakumar, and S. Kundu, "A chaotic ring oscillator based random number generator," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 160–165, IEEE, Arlington, VA, USA, 2014.

[70] N. Jiteurtragool, C. Wannaboon, and T. Masayoshi, "True Random Number Generator based on compact chaotic oscillator," in *2015 15th International Symposium on Communications and Information Technologies (ISCIT)*, pp. 315–318, IEEE, Nara, Japan, 2015.

[71] C. S. Jog, A. Manish, and N. Arup, "The time finite element as a robust general scheme for solving nonlinear dynamic equations including chaotic systems," *Applied Mathematics and Computation*, vol. 279, pp. 43–61, 2016.

[72] A. E. Rania and A. B. Ehab, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons & Fractals*, vol. 118, pp. 134–144, 2019.

[73] J. Jin and C. Wang, "Single CDTA-based current-mode quadrature oscillator," *AEU-International Journal of Electronics and Communications*, vol. 66, no. 11, pp. 933–936, 2012.

[74] F. Yu, Q. Tang, W. Wang, and H. Wu, "A 2.7 GHz low-phase-noise LC-QVCO using the gate-modulated coupling technique," *Wireless Personal Communications*, vol. 86, no. 2, pp. 671–681, 2016.

[75] F. Yu, "A low-voltage and low-power 3-GHz CMOS LC VCO for S-band wireless applications," *Wireless Personal Communications*, vol. 78, no. 2, pp. 905–914, 2014.

[76] F. Yu, L. Gao, L. Liu, S. Qian, S. Cai, and Y. Song, "A 1 V, 0.53 ns, 59 μW current comparator using standard 0.18 μm CMOS technology," *Wireless Personal Communications*, 2019.

[77] Q. Wan, J. Dong, H. Zhou, and F. Yu, "A very low power quadrature VCO with modified current-reuse and back-gate coupling topology," *Journal of Circuits, Systems and Computers*, vol. 26, no. 11, p. 1750184, 2017.

[78] C. Sanchez-Lopez, "A 1.7 MHz Chua's circuit using VMs and CF+s," *Revista Mexicana de Física*, vol. 58, no. 1, pp. 86–93, 2012.

[79] Y. Lin, C. Wang, and L. Zhou, "Generation and implementation of grid multiscroll hyperchaotic attractors using CCII+," *Optik*, vol. 127, no. 5, pp. 2902–2906, 2016.

[80] X. Zhang and C. Wang, "A novel multi-attractor period multi-scroll chaotic integrated circuit based on CMOS wide adjustable CCCII," *IEEE Access*, vol. 7, pp. 16336–16350, 2019.

[81] R. Trejo-Guerra, E. Tlelo-Cuautle, V. H. Carbajal-Gómez, and G. Rodriguez-Gómez, "A survey on the integrated design of chaotic oscillator," *Applied Mathematics and Computation*, vol. 219, no. 10, pp. 5113–5122, 2013.

[82] G. Gandhi and T. Roska, "MOS-integrable circuitry for multi-scroll chaotic grid realization: a SPICE-assisted proof," *International Journal of Circuit Theory and Applications*, vol. 37, no. 3, pp. 473–483, 2009.

[83] C. Sánchez-López, A. Castro-Hernández, and A. Pérez-Trejo, "Experimental verification of the Chua's circuit designed with UGCs," *IEICE Electronics Express*, vol. 5, no. 17, pp. 657–661, 2008.

[84] O. Katz, D. A. Ramon, and I. A. Wagner, "A robust random number generator based on a differential current-mode chaos," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 16, no. 12, pp. 1677–1686, 2008.

[85] B. Karakaya, A. Gülten, and M. Frasca, "A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA implementation," *Chaos, Solitons & Fractals*, vol. 119, pp. 143–149, 2019.