A Low Power Circuit Design for Chaos-Key Based Data Encryption

NGOC NGUYEN1, LOAN PHAM-NGUYEN2, (Member, IEEE), MINH B. NGUYEN2, AND GEORGES KADDOUM1, (Member, IEEE)

1Department of Electrical Engineering, École de Technologie Supérieure (ÉTS), Université du Québec, Montréal, H3C1K3, Canada
2School of Electronics and Telecommunications, Hanoi University of Science and Technology, Hanoi 100000, Vietnam

Corresponding author: Ngoc Nguyen (ngoc.nguyen-thi-thu.1@ens.etsmtl.ca)

This work was supported in part by Richard J. Marceau Chair.

ABSTRACT Dynamic and non-linear systems have been used to generate random bits in high-security applications for decades. In this perspective, due to their stochastic characteristic, chaotic systems have been emerging as the natural choice for the generation of random bits. This paper presents the design and the implementation of a chaos-based true random number generator and a chaos-key based data encryption scheme for secure communications. The mathematical expression of the dynamic system is presented and analyzed to evaluate the possibility of chaos occurrence. Then, the chaotic system is realized at the circuit level using 130 nm CMOS technology to generate random bit sequences, which are utilized in data encryption. Chaotic signal outputs of the chaos-based random number generator circuit are sampled at a maximum frequency of 50 MHz, enabling a high throughput of random bits. The core of the chaotic circuit consumes 630 µW in static mode and a maximum of 660 µW in running mode. The chaos-based one-time pad encryption scheme using the chaos-key generator shows the advantages of using this random number generator in secure communications. In this context, the data secrecy is compared to the advanced encryption standard AES128. Moreover, the design is simulated in different working conditions such as voltage supply and temperature variations, where it is shown that the random bit output benefits from a high entropy per bit and passes the standard statistical test suite (NIST) for cryptographic applications.

INDEX TERMS Chaos, random key, security, CMOS, true random number generator, one-time pad encryption, image encryption, and NIST.

I. INTRODUCTION

Random number generators are critical components that are responsible of generating public keys, private keys, and other kinds of random numbers that are utilized in cryptographic applications and data security [1]–[5]. The explosive growth of Internet-of-Things (IoTs) devices places new challenges on random number generators including energy efficiency, hardware security, and flexibility. Nowadays, true random number generators, taking advantage of the nonlinear and dynamic characteristics of chaotic systems, are attracting substantial research interest [6]–[10]. A chaotic system, which is represented by a deterministic expression, is nonlinear and dynamic [6]. Therefore, it is not sensitive to the system’s noise, such as voltage and temperature variations. Despite being deterministic, chaotic systems have been emerging as the natural choice for random bit generators in high-security applications, due to their sensitivity to initial conditions and irregular motion in the phase space. Therefore, at a certain point of observation, the chaotic system behaves as a random-like process [10]. Chaotic systems used in generating random bits are categorized into discrete and continuous systems. The discrete chaotic maps, in which the next state is calculated depending on some previous states and is represented by a map $x_{k+1} = M(x_k)$, include logistic maps, piece-wise affine Markov maps, Renyi maps. Whereas continuous chaotic systems, in which the next state is an integration of the previous states, are regulated by a set of differential equations $X' = F(X)$. Some well-known continuous chaotic systems are Lorenz’s equations, Chua’s circuit, and Rossler’s oscillators. Both discrete chaotic maps and continuous chaotic systems can be digitized to produce pseudo-random numbers. The “pseudo” term refers to random number generators which use deterministic algorithms where the data is represented by a digital word [11]–[13]. Whereas true random number generators
are generated from physical entropy sources such as thermal noise, jitter noise, or analog implemented chaotic systems. Although chaotic systems have deterministic expressions, they are considered as true random number generators if the chaotic system is implemented in analog circuit design. Many chaos-based true random number generators have been designed in the state-of-the-art [14]–[19]. Due to quantization errors in the digital domain, the dynamic characteristics of chaotic pseudo-random number generators are limited. Therefore, we focus on the design of a true random number generator based on a chaotic system in the analog circuit. Many true chaos-based RNGs are induced from linear circuits due to their simplified implementation. Among the numerous approaches used to implement linear chaotic maps, Markov chaotic maps are widely used in very-large-scale integration designs for their low implementation cost. Some transforms of Markov chaotic maps such as N-Bernoulli maps, tent maps, zigzag maps, and piecewise affine Markov maps (PWAM) have been utilized to generate random bit sequences [20]–[24]. However, in cryptographic applications, linear methods are not recommended for generating random keys. Ngoc et al. proposed an analog circuit to implement a nonlinear logistic map based on fuzzy modeling [25]. However, the accuracy of nonlinear modeling maps depends on experience and is limited by circuit parameters. Although many continuous chaotic systems have been developed and verified by mathematics, due to their high power consumption, low-frequency operation, and low capability of operating at low voltage levels, only a few of them were designed in a highly integrated circuit. Most of them use off-the-shelf electronic devices which are power-hungry circuits [26]–[28]. Chua’s circuit is a well-known implementation of a continuous chaotic system in integrated circuits [29]–[31]. Moreover, implementations in integrated circuit using external components including inductors, and capacitors which occupy a large area have been conducted in [32], [33]. The research in [34] presented a fully CMOS circuit design for random bit generator using Jerk equations. The circuit was implemented in 180nm CMOS technology. However, the system analysis is not fully addressed and the large capacitors limit the internal oscillator frequency which reduces the random signal throughput.

This work presents a low power circuit design for a chaotic system that fills the gap between theoretical analysis and implementation of chaotic systems for the generation of random bit sequences. A novel 3D continuous chaotic system is proposed with mathematical analysis. The chaotic circuit is implemented in 130nm CMOS technology with a supply voltage of 1.2V which significantly reduces the power consumption. Moreover, post-processing is implemented to eliminate the bias effect and provide ready-to-use random bits. Therefore, according to the evaluation methodology of random number generators proposed by the German Federal Office for Information Security (AIS-20/31), the proposed random bit generator falls into the PTG.3 class, which can be used in cryptography [35]. As an application, chaos-based one-time pad cryptography is developed using the proposed chaotic-key generator. In one-time pad (OTP) cryptography, the security relies on the randomness of the keys [36], [37]. The OTP cryptosystem based on the XOR operation uses chaos-based random bit sequences as the OTP codebook. The contributions of this paper include:

1) The design of a novel 3D continuous chaotic system which is rich of dynamic characteristics.
2) The implementation of a chaos-based true random number generator in 130nm CMOS technology providing ready-to-use random bits.
3) The application of an one-time pad cryptography for image encryption/decryption based on the chaos-key generator.

The rest of this paper is organized as follows. To assess the system’s robustness, Section II presents the mathematical analysis of the chaotic system. Section III details the circuit design using 130 nm CMOS technology to be used in integrated devices. The randomness performance is evaluated in Section IV. The OTP image encryption based on chaos-key generation is presented in Section V. Finally, Section VI concludes the paper.

II. PROPOSED 3D CONTINUOUS CHAOTIC SYSTEM

This section presents the 3D continuous chaotic system in mathematical expressions. The system dynamics and chaotic complexity are analyzed using Lyapunov spectrums, bifurcation diagrams, wavelet analysis, and stability evaluation.

A. CONTINUOUS CHAOTIC SYSTEM

The proposed 3D dynamic system is expressed in the canonical form $X' = F(X)$, $X = x_1, x_2, x_3 \in \mathbb{R}^3$, with

$$
\begin{align*}
    x'_1 &= -(x_3 - x_2) \\
    x'_2 &= -x_3 \\ 
    x'_3 &= -a \times (x_1 - x_2 + x_3) + f(x_1)
\end{align*}
$$

where $f(x_1) = b_1 \times \tanh(b_2 \times x_1 - b_3)$ is a non-linear function. The following subsections present the mathematical analysis in terms of chaotic and dynamic characteristics by evaluating the Lyapunov exponents and Kaplan-York dimension. Moreover, the stability analysis of equilibrium points is also an important aspect that we address in this section.

B. MATHEMATICAL ANALYSIS

In this part, we present the dynamic characteristics of the dynamic system mentioned above. Based on mathematical analysis, we can evaluate if a dynamic system has a chaotic characteristic and how strong it is. The dynamic system was simulated in MATLAB using the $4^{th}$-order Runge-Kutta integration algorithm with a step size of $10^{-4}$. The Lyapunov exponents of a differential system are defined as:

$$
L_i = \lim_{t \to \infty} \frac{1}{t} \log \frac{\|x_i(t)\|}{\|x_i(0)\|}.
$$

For $a = 0.3$, $b_1 = 0.1$, $b_2 = 80$, and $b_3 = 0.7$, the Lyapunov exponents of the differential system are: $L_1 = 0.0841$, $L_2 = -1.0410$, $L_3 = 0.0592$. Since $L_1 > 0$ and $L_2 < 0$, the system is chaotic.
Table 1 compares the Lyapunov exponents of the proposed 3D chaotic system to previous studies. As evidenced in the table, the proposed 3D chaotic system has the highest Lyapunov dimension which indicates highly dynamic complexity.

| Chaotic system | $L_1$  | $L_2$  | $L_3$  | $D_L$  |
|---------------|-------|-------|-------|-------|
| [39]          | 0.5698| 0     | -4.2189| 2.1347|
| [27]          | 0.1704| 0     | -2.5921| 2.0657|
| [40]          | 0.2263| 0     | -1.2263| 2.1845|
| [41]          | 0.2332| 0     | -11.3944| 2.0221|
| This work     | 0.0841| 0     | -0.3844| 2.2188|

C. STABILITY OF EQUILIBRIUM POINTS

The stability evaluation of the equilibrium is an important step in practical designs supporting the choice of system parameters. The Jacobian matrix of the chaotic system is calculated to evaluate the stability of equilibrium points.

\[
J = \begin{bmatrix}
0 & -1 & 1 \\
0 & 0 & -1 \\
A & a & -a
\end{bmatrix},
\]

where $A = -a + b_1b_2(1 - \tanh^2(b_2x - b_3))$. The eigenvalues of the Jacobian matrix satisfy the condition:

\[
J - \lambda I = 0 \leftrightarrow \lambda^3 + a\lambda^2 + (a + A)\lambda - A = 0.
\]
The chaotic system has equilibrium at \( E = [x_1, 0, 0] \), in which \( x_1 \) satisfies:

\[
-ax_1 + b_1 \tanh(b_2 x_1 - b_3)) = 0, \\
\leftrightarrow \tanh(b_2 x_1 - b_3) = \frac{ax_1}{b_1}.
\]

(7)

For a small perturbation from the fixed points \( X(t) = X(0) + \Delta X \). If \( \Delta x \approx e^{\lambda t} \), the characteristic polynomial equation is derived as in equation (6). According to the Routh-Hurwitz criterion, the real parts of the roots of (6) are negative if and only if \( A < 0 \), and \( a(a + A) + A > 0 \). The system at the equilibrium set \( E \) must be unstable, thereby the chaotic phenomenon is enabled. The parameters must satisfy one of the following conditions:

\[
-a + b_1 b_2 (1 - \left(\frac{ax_1}{b_1}\right)^2) > 0, \\
\lambda^2 + (a + 1)(-a + b_1 b_2 (1 - \left(\frac{ax_1}{b_1}\right)^2) < 0.
\]

(8)

From (7), we determined that the equilibrium of the system is at \( E = [0.03167, 0, 0] \). Therefore, the first condition in (8) is satisfied. In other words, we prove that the proposed chaotic system has an unstable and saddle focus equilibrium which enables chaotic characteristics. Overall, the above presented chaotic system has non-periodicity in which the data space is limited in the range \([-0.5 - 0.5]\) as shown in Fig. 3. This enables the deployment of the proposed chaotic system using CMOS devices with a supply voltage of 1.2V. In this context, the common voltage is set to 0.6V.

### III. CIRCUIT IMPLEMENTATION

In this section, we present the chaotic circuit design for the above differential chaos and the post-processing circuit using a 130 nm CMOS technology.

#### A. CHAOTIC CIRCUIT DESIGN

The main components of continuous chaotic systems are integrators. In this section, we present the Gm-C integrator circuit design and the non-linear function based on operation amplifier. The chaotic system is formalulated using Kirchhoff’s law, and the results reveal the following system of Ordinary Differential Equations (ODEs):

\[
\begin{align*}
    v_x' &= -\frac{g_m}{C_x} v_x + \frac{g_m}{C_x} v_z \\
    v_y' &= -\frac{g_m}{C_y} v_y \\
    v_z' &= -\frac{g_m}{C_z} v_x + \frac{g_m}{C_z} v_y - \frac{g_m}{C_z} f(v_x) + \frac{f(v_z)}{C_z},
\end{align*}
\]

(9)

where \( C_x, C_y, C_z \) are integrating capacitors with \( C_z = C_y \), and \( f(v_x) \) is the nonlinear \( \tanh(x) \) function. The circuit realization in (9) is normalized by the time constant \( \tau = \frac{C}{g_m} \), then it is undimensioned by an arbitrary voltage \( V_r \) as:

\[
\begin{bmatrix}
    \partial V_x \\
    \partial V_y \\
    \partial V_z
\end{bmatrix} = 
\begin{bmatrix}
    \frac{\partial V_x}{V_r} \\
    \frac{\partial V_y}{V_r} \\
    \frac{\partial V_z}{V_r}
\end{bmatrix}
\]

(10)

The integrator is implemented using an inverted-based Gm-C integrator as depicted in Fig. 4. The relationship between the output current \( i_o \) and the input voltage \( v_i \) follows:

\[
\begin{align*}
    i_o &= -g_m v_i, \\
    i_o &= \frac{1}{\tau} \frac{\partial V_i}{\partial t} = -g_m v_i, \\
    \frac{\partial V_o}{\partial t} &= \frac{-g_m}{C} v_i.
\end{align*}
\]

(11)

The transconductance gain \( g_m \) is comprised of a pair of nMOS and pMOS devices. The total transconductance gain is calculated as:

\[
g_m = \mu_n C_{ox} \frac{W_n}{L_n}(V_{GSn} - V_{THn}) + \mu_p C_{ox} \frac{W_p}{L_p}(V_{GSp} - V_{THp}).
\]

(12)

The nonlinear function \( i_{out} = f(v_x) \) is a hyperbolic tangent function. The circuit implementation of the non-linear function \( f(v_x) \) using a differential amplifier is shown in Fig. 5. The saturated drain current \( I_{sat} \) of a mosfet device is exponential to the gate and source voltages as:

\[
I_{sat} = I_D e^{(V_G - V_S)}.
\]

(13)

Assuming that a differential input pair is saturated, the voltage-to-current transfer characteristic \( i_{out} = i_{D1} - i_{D2} \).
\( i_{D2} = f(v_x) \), is proportional to the difference between two drain currents as follow:

\[
\begin{align*}
\text{i}_{\text{out}} & = i_{D1} - i_{D2} = I_{SS} \frac{e^{v_x} - e^{v_T}}{e^{v_x} + e^{v_T}} \\
& = I_{SS} \tanh \left( \frac{\kappa (v_x - V_T)}{2} \right). 
\end{align*}
\] (14)

The current bias \( I_{SS} \) was designed to be resilient against process-voltage-temperature (PVT) variations based on the research in [43]. Here we match the parameters in the first equation and the circuit parameters as:

\[
a = \frac{C_x}{C_z}; \quad b_1 = \frac{I_{SS} C_x}{g_m C_z}; \quad b_2 = \frac{\kappa}{2}; \quad b_3 = \frac{\kappa}{2} V_T. \quad (15)
\]

The whole circuit design of the chaotic system is elaborated in Fig. 6. The integrating capacitors set to \( C_x = 1.2pF \), \( C_y = 1.2pF \), and \( C_z = 4pF \). The transconductance \( g_m \) in (12) is \( 240 \ \mu S \), and the current source for \( \text{tanh}(.)I_{SS} = 80\mu A \). The circuit design of continuous chaotic systems has a great impact on the intrinsic oscillator frequency. Low-frequency chaotic oscillators limit the final random bit throughput. In our chaotic circuit design, the optimization and tradeoff between circuit parameters including transconductance and capacitors are carefully taken into account. The intrinsic oscillator frequency is \( f = \frac{g_m}{2\pi C} = 31.8 \) MHz, which is indeed a very high frequency with respect to other discrete or integrated solutions.

Continuous chaotic systems implemented using off-the-shelf devices are power-hungry circuits that, due to the large values of passive components, limit the oscillator frequency in the “KHz” range. In [44], the authors used inductor \( L = 10mH \) and capacitor \( C = 10nF \) in the chaotic circuit, where the maximum oscillator frequency is 830 kHz and the sampling frequency is 19 MHz. In the full CMOS
implementation of a continuous chaotic system presented in [18], the chaotic signal is post-processed at a frequency of 50 MHz, but the oscillator frequency is undeclared and is expected to be much lower than in this work due to the large capacitors used (between 10nF and 20 nF, instead of 1.2pF).

Trajectories of the chaotic outputs of the chaotic system are shown in Fig. 7 with control voltage $V_T = 0.7$. The attractor of the chaotic system is observed and compatible with the simulation results. The layout diagram of the chaotic circuit is shown in Fig. 9. Continuous chaotic systems have high dynamic characteristics (compared to chaotic maps and chaotic iterations) due to higher dimensional signals and multiple parameters. However, they are also associated to more complicated circuit designs, especially when the existing physical noises can degrade the dynamic characteristics if the chaotic system is too sensitive to its parameters. Our continuous chaotic system is shown to be robust since the dynamic characteristics are preserved with existence of circuit noise and device mismatch.

**B. POST-PROCESSING CIRCUIT DESIGN**

1) **COMPARATOR**

The comparator includes a preamplifier (PREAMP) and a latch circuit (LATCH). The main function of the preamplifier is to provide sufficient gain to overcome the offset of the subsequent comparator without introducing significant offset of its own. The comparator is designed to work at a frequency of 50MHz; the aperture time is 10 ns with a 50%-duty cycle clock. Random offsets due to transistor mismatches, which may be introduced to the second-stage of the comparator (LATCH circuit), will be eliminated by the following post-processing. Therefore, the comparator circuit does not require a highly critical design. Transistor sizes are chosen properly to reduce mismatch and satisfy the gain requirement. The PREAMP circuit, shown in Fig. 10, uses an output reset

![FIGURE 7. 2D trajectories with initial state of $V = [0.62, 0.61, 0.6]$.](image1)

![FIGURE 8. Chaotic signal waveform outputs.](image2)

![FIGURE 9. Layout diagram of the chaotic circuit design without padding.](image3)
TABLE 2. Summary of comparison with previous designs.

| Entropy source   | This work* | JSSC’17 [47]** | NEWCAS’18 [23]* | Chaos’18 [34]* | Other TRNGs     |
|------------------|------------|----------------|-----------------|----------------|----------------|
| Technology       | CT-Chaos   | DT-Chaos       | 65nm CMOS       | 65nm CMOS      | Jitter acc. Meta & jitter |
| Supply voltage [V]| 1.2        | 0.6            | 2.5             | 1.8            | 1.2            |
| Throughput [MHz] | 50         | 0.27           | 3               | 80             | 9.9            |
| Power [mW]       | 0.78       | 0.000082       | 0.15            | 1.32           | 0.418          |
| Energy Efficiency [pJ/b] | 15.6   | 0.3            | 33.33           | 26.4           | 23.71          |

(*) post-layout simulation results, (**) measurement results.

FIGURE 10. Comparator circuit design.

FIGURE 11. SHIFT-XOR based post processing circuit.

switch (M5), to prevent regeneration during the comparing phase. When the clock signal CLK is at a low level, the dioded-connected PMOS transistors M3 and M4 generate the output. The offset of PREAMP is amplified with a high gain. Meanwhile, when CLK is at a high level, the output of PREAMP is fed into an edge-triggered latch (LATCH) that also amplifies its inputs.

2) SHIFT-XOR BASED POST-PROCESSING CIRCUIT

The circuit design is based on shift and exclusive-OR operations, in which the eliminated bits are re-used by the feedback. Therefore, the bit-rate between input and output is preserved. This post-processing is composed of four shift registers [45], [46]. The working principle is to evaluate the incoming bits from comparators and reuse these bits by XORing them with the same bit-stream after a few step shifting. In this context, we use 8-bit length registers. The circuit design for a one-bit shift register uses a positive-edge trigger dynamic flip-flop while 8-bit shift registers are composed of eight one-bit shifters. The circuit design is shown in Fig. 11.

IV. RANDOMNESS EVALUATION

The following section presents the system’s performance in terms of power consumption and randomness evaluation including signal entropy, signal correlation, and random-test suite. The chaotic circuit consumes 630µW in static mode and a maximum of 660µW in running mode. The comparator consumes 120µW at a 50MHz sampling frequency. Therefore, the low-power circuit design achieves an energy efficiency of 15.6 pJ/b for random binary outputs. The proposed system’s performance is compared to other previous designs in Table 2. The comparison indicates that our proposed design benefits from a low power consumption with high throughput compared to other chaos-based RNGs using different continuous chaotic systems or discrete time chaotic maps in [25], [34]. Although the design in [47] consumes less power, the data rate is limited at “KHz”. Besides, we compare our work with previous generators using physical noises [17], [48]. The work in [17], which uses metastability and jitter noise to generate random bits, has the highest throughput. However, it consumes much more power than our design. Thus, the proposed system design is more suitable for applications that require a relatively high throughput (Mbps) and low power.

To evaluate the randomness, Shannon’s entropy of the output bitstream is calculated as follows:

\[ H(X) = - \sum_{i=0}^{N-1} p_i \log_2 p_i \]  

(16)

where \( p_i \) is the probability of a given symbol and \( N \) is the number of symbols. The ideal entropy of a binary bitstream is unity. The entropy test for 600 sets of 60Kb length binary sequences is illustrated in Fig. 12. It is observed that the entropy of all the sets is near unity, and 98% of the samples
have an entropy higher than 0.9998, which indicates a highly random performance. Moreover, the design was evaluated in different working conditions such as power supply and temperature variations. As illustrated in Fig. 13, the average random bit entropy does not show significant changes with power variation at different corners in Monte Carlo simulations.

The correlation, which measures the similarity between two time-serial sequences, is another important standard function to evaluate the randomness. The correlation is calculated as:

$$r_{y_1y_2}(k) = \frac{c_{y_1y_2}(k)}{s_{y_1}s_{y_2}}; \quad k = 0, \pm 1, \pm 2, \ldots$$     (17)

where $c_{y_1y_2}$ denotes the cross-covariance of the time series $y_1,t$ and $y_2,t$, which is calculated as:

$$c_{y_1y_2}(k) = \begin{cases} \frac{1}{T} \sum_{t=1}^{T-k} (y_{1,t} - \bar{y_1})(y_{2,t+k} - \bar{y_2}); & k = 1, 2, \ldots \\ \frac{1}{T} \sum_{t=1}^{T+k} (y_{2,t} - \bar{y_2})(y_{1,t-k} - \bar{y_1}); & k = -1, -2, \ldots \end{cases}$$     (18)

where $s_{y_1}$ and $s_{y_2}$ are standard deviations of the series $\sqrt{c_{y_1y_1}(0)}$ and $\sqrt{c_{y_2y_2}(0)}$, respectively, and $k$ is the number of lags (time delays). Likewise, the auto-correlation measures the similarity between the time series and its k-lags delay.

Fig. 14 shows the auto-correlation and cross-correlation measurements of the proposed output bitstreams. The average similarity is of 0.13% which demonstrates the uncorrelated relationship between two different time series and the non-periodic random outputs. Moreover, the ready-to-use random bits after the data post-processing must satisfy the randomness criteria, measured by statistical tests, to determine that the proposed chaotic system can be used as a random source. The highly-acceptable statistical test suite NIST sp800-22, with numerical tests developed by the National Institute of Standards and Technology, is utilized to evaluate the randomness of binary sequences. This statistical test works under a tentative assumption of randomness ($H_0$). The output of each test (the P-value) is computed by comparing features of the stream to those of an effectively random stream. Tests are designed in a way that, if $H_0$ is true, the P-value is a uniformly distributed random variable in the interval [0, 1]; conversely, if $H_0$ is false, P-values collapse to zero. When a single sequence is available, the test interpretation is achieved by comparing the achieved P-value with a small but non-zero threshold value (a typical considered value is 0.01). The sequence is considered random if the P-value is larger than the threshold value, and non-random when smaller. When multiple sequences are available from the same generator, it is also possible to compute all the associated P-values and check the uniformity ($\chi^2$) of their distribution which is known as the second-level test [49].

FIGURE 13. Average entropy with multiple corners in Monte Carlo simulations: (a) TT($-20^\circ$C, VDD = 1.2V) (b) TT($60^\circ$C, VDD = 1.3V) (c) TT($60^\circ$C, VDD = 1.1V) (d) SS($60^\circ$C, VDD = 1.2V) (e) SF($60^\circ$C, VDD = 1.2V) (f) FS($60^\circ$C, VDD = 1.2V).
Eighty streams of 1-Mb length are directly used for the sub-tests in NIST including overlapping test, Maurer’s universal statistical test, linear complexity test, serial test, run excursion test, and random excursion variant test which require at least 1-Mb length data. The other tests including the mono-bit test, frequency test within a block, run test, the longest run of one in a block, binary matrix rank test, approximate entropy test, and cumulative sums test use 500 streams of 160-Kbit length. The results of the NIST test are presented in Table 3. All the tests are passed with a reasonable proportion. The minimum pass rate for the first ten tests is 488 for a sample size of 500 bitstreams. The minimum pass rate for the last five tests is 76/80. Moreover, the random bit streams passed the second-level tests of randomness.

V. CHAOS-BASED ONE-TIME PAD CRYPTO SYSTEM
In this section, we present an OTP image encryption application using chaos-key generation. Security and encryption performance analysis are performed to demonstrate the advantages of using chaos-key in data encryption.
simplest and least expensive in terms of device resource (uses an XOR operations between the plain image pixel values and generated random bits) [50]. This application is presented as a proof of concept that the ready-to-use random bits generated from the proposed chaos-based generator can be used directly for secure communications. In this context, the OTP cryptography can use a very-long generated chaos-based random key, which is securely sent to the receiver, for multiple messages until the length of key is reached. The initial conditions and control voltage used to generate chaotic signals define the key space. Different initial conditions and control voltages generate different codebooks for the encryption process. In this context, we assume that the key is securely sent to the receiver over a secure channel which with no transmission errors.

A. STATISTICAL ANALYSIS

1) HISTOGRAM ANALYSIS

The Advanced Encryption Standard (AES) and chaos-key based OTP cryptography were implemented using MATLAB on an 8th-generation Intel core i7 and 8G RAM computer. Fig. 16 provides comparison between AES and the proposed algorithm using chaos-key generation for image encryption. As described in these figures, the encrypted images using the AES algorithm and the proposed encryption scheme have a flat histogram. The chaos-key based algorithm finished within 13s. The encryption time excludes the key generation. For AES encryption, the keys are static and stored in the memory. The proposed chaos-key generation has a throughput of 50Mbps, therefore, it takes approximately 0.042s to generate 262144 8-bit chaotic numbers for the sample color image size of \([W \times H] = 512 \times 512\), which is insignificant compared to the encryption time.

2) IMAGE ENTROPY, UACI AND NPCR EVALUATION

Entropy is a statistical measure of randomness that can be used to characterize the texture of an image. In image encryption, the entropy is used to evaluate the randomness of encrypted image pixel values. The entropy test results, shown in Table 4, indicate that the encrypted images have good randomness pixel values. To test the influence of an one-pixel change on the whole image encrypted using the proposed chaos-based algorithm, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). Let the grey-scale value of the pixel at grid \((i, j)\) be denoted as \(C_1(i, j)\) in the plain image and \(C_2(i, j)\) in the encrypted image, the NPCP is defined as follows:

\[
NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100%.
\]

\[
D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{if } C_1(i,j) = C_2(i,j) \end{cases}
\]  

(19)

The UACI, which measures the average intensity of differences between the plain image and the encrypted image, is defined as follows.

\[
UACI = \frac{\sum_{i,j} \| C_1(i,j) - C_2(i,j) \|}{(W \times H) \times 255} \times 100%.
\]

(20)

Table 4 shows the NPCR and UACI test results for image encryption with different image sizes.

3) CORRELATION TEST

The correlation tests of two horizontally adjacent pixels, two vertically adjacent pixels, and two diagonally adjacent pixels in the plain image and encrypted image using the chaos-key generator are presented in Fig.17. According to the correlation coefficients listed in Table. 5, it can be inferred that the adjacent pixels in the encrypted image are uncorrelated.

B. KEY SPACE

Data security should have a big enough keyspace to withstand brute-force attacks. In chaos-key generation, the size of the chaotic system and its parameters define the keyspace. In this application, each parameter has \(2^{32}\) different values. The 3D continuous chaotic system has a key length of \(2^{90}\) because it has a different value set \((V_{i0}, V_{i0}, V_{i0})\) for initialization. Moreover, the system parameter \(V_T\) is also controlled by a 32-bit key length. In total, the chaotic system has a keyspace of \(2^{128}\).

C. KEY SENSITIVITY

The different generated chaos-keys with different sets of input \((V_{i0}, V_{i0}, V_{i0}, V_T)\) are evaluated. The chaos-key \(k_1\) is generated by the input set \((0.615, 0.6, 0.6, 0.7)\) and the chaos-key \(k_2\) is generated by the input set \((0.61500001, 0.6, 0.6, 0.7)\). Chaos-key \(k_1\) is used to encrypt the original image. Fig. 18 shows the image decryption with correct chaos-key \(k_1\) and image decryption using wrong chaos-key \(k_2\). A tiny change in the input set caused a huge difference in the decryption results. Therefore, the proposed scheme with chaos-key generation has a high sensitivity to secret keys in the encryption and decryption process.
VI. CONCLUSION

We have presented a novel continuous chaotic system implementation in highly integrated analog circuit design and its engineering application to image encryption. The chaotic dynamics were analyzed and studied. The circuit realization in 130 nm CMOS technology enables our design to be used in constrained devices. The generated random numbers passed all the statistical tests of the NIST testsuite at a throughput of 50Mbps. Moreover, an image encryption scheme using the chaos-key generator was presented. The encryption and decryption performances of the chaos-key based image encryption scheme were compared to the standard AES128 algorithm in terms of data secrecy and accomplishing time. In the future, the chaotic system implementation could be integrated into a microprocessor as a standalone cryptographic processor. Moreover, power and speed optimization will be attempted to increase system performance.

REFERENCES

[1] K. Lee, S.-Y. Lee, C. Seo, and K. Yim, “TRNG (True random number Generator) method using visible spectrum for secure communication on 5G network,” IEEE Access, vol. 6, pp. 12838–12847, 2018.
[2] A. Giakoumis, C. K. Volos, J. M. Murucbile, L. del Carmen Gomez-Pavon, I. N. Stouboulos, and I. M. Kyprianidis, “Text encryption device based on a chaotic random bit generator,” in Proc. IEEE 9th Latin Amer. Symp. Circuits Syst. (LASCAS), Feb. 2018, pp. 1–5.
[3] Ü. Çavuşoğlu, S. Panahi, A. Akgül, S. Jafari, and S. Kačar, “A new chaotic system with hidden attractor and its engineering applications: Analog circuit realization and image encryption,” Anal. Integr. Circuits Signal Process., vol. 98, no. 1, pp. 85–99, Jan. 2019.
[4] B. Li, X. Liao, and Y. Jiang, “A novel image encryption scheme based on improved random number generator and its implementation,” Nonlinear Dyn., vol. 95, no. 3, pp. 1781–1805, Feb. 2019.
[5] B. K. Park, H. Park, Y.-S. Kim, J.-S. Kang, Y. Yeom, C. Ye, S. Moon, and S.-W. Han, “Practical true random number generator using CMOS image sensor dark noise,” IEEE Access, vol. 7, pp. 91407–91413, 2019.
[6] K. Demir and S. Ergun, “Analytical modeling of continuous-time chaos based random number generators,” in Proc. New Genes. CAS (NGCAS), Nov. 2018, pp. 106–109.
[7] R. Tchinga, T. Nguazon, P. H. Louodop Fotso, and J. A. C. Gallas, “Chaos in a single op-amp-based jerk circuit: Experiments and simulations,” IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 63, no. 3, pp. 239–243, Mar. 2016.
[8] D. A. Prousalis, C. K. Volos, I. N. Stouboulos, and I. M. Kyprianidis, “A hyperjerk memristive system with infinite equilibrium points,” in Proc. AIP Conf., Sep. 2017, vol. 1872, no. 1, p. 020024.
[9] S. Ergun, “Vulnerability analysis of a chaos-based random number generator,” in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2018, pp. 3331–3334.

[10] L. Gong, J. Zhang, H. Liu, L. Sang, and Y. Wang, “True random number generators using electrical noise,” IEEE Access, vol. 7, pp. 125796–125805, 2019.

[11] K. Cho and T. Miyano, “Design and test of pseudorandom number generator using a star network of lorentz oscillators,” Int. J. Bifurcation Chaos, vol. 27, no. 12, Nov. 2017, Art. no. 1750184.

[12] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, “A novel pseudorandom number generator based on pseudorandomly enhanced logmap,” Nonlinear Dyn., vol. 87, no. 1, pp. 407–425, Jan. 2017.

[13] A. A. Rezk, A. H. Madian, A. G. Radwan, and A. M. Soliman, “Multiplierless chaotic pseudo random number generators,” AEU-Int. J. Electron. Commun., vol. 113, Jan. 2020, Art. no. 152947.

[14] R. Modeste Nguimdo, R. Tchitnga, and P. Woafo, “Dynamics of coupled simplest chaotic two-component electronic circuits and its potential application to random bit generation.” Chaos: Interdiscip. J. Nonlinear Sci., vol. 23, no. 4, Dec. 2013, Art. no. 043112.

[15] J.-C. Hsieh and V.-H.-C. Chen, “An ultra-low voltage chaos-based true random number generator for IoT applications,” Microelectron. J., vol. 87, pp. 55–64, May 2019.

[16] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and J.-C. Hsueh and V.-H.-C. Chen, “An ultra-low voltage chaos-based true random number generator,” Proc. 26th Int. Conf. Field Programm. Log. Appl. (FPL), Aug. 2016, pp. 1–10.

[17] T. Miyano and K. Cho, “Chaos-based one-time pad cryptography,” in Proc. Int. Symp. Inf. Theory Appl. (ISITA), 2016, pp. 156–160.

[18] A. Vázquez-Medina, “Digital noise generator design using inverted 1D tent signal processing and chaos,” Int. J. Bifurcation Chaos, vol. 26, no. 12, pp. 1364–1370, Dec. 2015.

[19] A. Ergun and S. Ozoguz, “A truly random number generator based on a pseudorandomly enhanced logistic map,” Chaos: Interdiscip. J. Nonlinear Sci., vol. 29, no. 05, May 2019, Art. no. 152947.

[20] J. Lü, G. Chen, and D. Cheng, “A new chaotic system and beyond: The generalized lorentz-like system,” Int. J. Bifurcation Chaos, vol. 14, no. 05, pp. 1507–1537, May 2004.

[21] R. Benítez, V. J. Bolós, and M. E. Ramírez, “A wavelet-based tool for studying non-periodicity,” Comput. Math. with Appl., vol. 60, no. 3, pp. 634–641, Aug. 2010.

[22] D. Wang, X. L. Tan, and P. K. Chan, “A 65-nm CMOS constant current source with reduced PVT variation,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 4, pp. 1373–1385, Apr. 2017.

[23] S. Ergun and S. Ozoguz, “A truly random number generator based on a continuous-time chaotic oscillator for applications in cryptography,” in Computer and Information Sciences, vol. 3733. Berlin, Germany: Springer, 1979, pp. 240–247.

[24] V. Roccia, B. Yang, W. Dehaene, and I. Verbauwhede, “Iterating von Neumann’s post-processing under hardware constraints,” in Proc. IEEE Int. Symp. Hardware Oriented Secure Trust (HOST), May 2016, pp. 37–42.

[25] F. Pareschi, R. Rovatti, and G. Setti, “Simple and effective post-processing stage for random stream generated by a chaos-based RNG,” in Proc. Int. Symp. Nonlinear Theory Appl. (NOLTA), 2006, p. 5.

[26] M. Kim, U. Ha, K. J. Lee, Y. Lee, and H.-J. Yoo, “A 62-nW chaotic map true random number generator based on a sub-ranging SAR ADC,” IEEE J. Solid-State Circuits, vol. 52, no. 7, pp. 1953–1965, Jul. 2017.

[27] E. Kim, M. Lee, and J.-I. Kim, “8Mb/s 28MHz/1 robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors,” in IEEE ESSC Dig. Tech. Papers, Feb. 2017, pp. 144–145.

[28] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, USA, Special Publication 800-22, Tech. Rep. 800-22 Rev 1a, Apr. 2010.

[29] X. Wang, Y. Wang, X. Zhu, and C. Luo, “A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level,” Opt. Lasers Eng., vol. 125, Feb. 2020, Art. no. 105851. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0143816619302143
NGOC NGUYEN received the Engineering’s degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 2010, and the M.S. degree in electrical engineering from the Ulsan National Institute of Science and Technology, Ulsan, South Korea, in 2014. She is currently pursuing the Ph.D. degree with the École de Technologie Supérieure (ÉTS), Université du Québec, Montréal, QC, Canada. Her research interests include chaos theory, communication system, hardware security in analog, and digital circuit design. She has awarded the Faculty for the Future scholarship from the Schlumberger Foundation in 2018, 2019, and 2020.

LOAN PHAM-NGUYEN (Member, IEEE) graduated from Ecole Centrale de Lyon, France, in 2005. She received the M.Sc. degree in microelectronics from University Joseph Fourier, in 2006, and the Ph.D. degree in microelectronics from the Grenoble Institute of Technology (INPG), France, in 2009. Her Ph.D., funded by STMicroelectronics (industry fund), focused on the fabrication and electrical characterization of advanced Fully Depleted SOI MOSFETs. Since 2010, she has been leading a research group in Analog IC design, HUST, Vietnam, where she is currently a Lecturer and a Researcher with the School of Electronics and Telecommunications. She is author or coauthor of about ten journals and more than 30 international conference papers. Her research focuses on power management for biomedical applications, wearable devices, and LED drivers. Actually, her group has 20 bachelor’s degree students, three master’s degree students working closely with Professors from KAIST, South Korea, UC San Diego, USA, and Telecom-ParisTech, France, for collaborative projects.

MINH B. NGUYEN received the bachelor’s degree in electronic and telecommunication engineering from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 2019. He is currently pursuing the M.S. degree with the Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research interest focus on integrated circuit designs.

GEORGES KADDOUM (Member, IEEE) received the bachelor’s degree in electrical engineering from the École Nationale Supérieure de Techniques Avancées (ENSTA Bretagne), Brest, France, the M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne (ENSTB), Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences (INSA), University of Toulouse, Toulouse, France, in 2009. In 2014, he was awarded the ÉTS Research Chair in physical-layer security for wireless networks. Since 2010, he has been a Scientific Consultant in the field of space and wireless telecommunications for several USA and Canadian companies. He is currently an Associate Professor and the Tier 2 Canada Research Chair with the École de Technologie Supérieure (ÉTS), Université du Québec, Montréal, Canada. He has published more than 200 journals and conference papers and has two pending patents. His recent research activities cover mobile communication systems, modulations, security, and space communications and navigation. He received the best papers awards at the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications (WIMOB), with three coauthors, and at the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), with four coauthors. Moreover, he received the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award for the year 2015, 2017, and 2019. In addition, he received the Research Excellence Award of the Université du Québec, in 2018. In 2019, he received the Research Excellence Award from the ÉTS in recognition of his outstanding research outcomes. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and the IEEE COMMUNICATIONS LETTERS.