A PRNG based on an improved chaotic map using a self-perturbation mechanism

Merah HOCINE[1], Merah LAHCENE[2], Talbi LARBI[3], Ali-Pacha ADDA[4]

[1] Department of Physics, Higher Normal School, Algeria

[2] Department of Electronics, Faculty of Technology, University Amar Telidji, Algeria

[3] Department of Computer Science and Engineering, University of Quebec, Canada

[4] Coding and Information Security Laboratory, University of Sciences and Technology of Oran, Algeria

merah.hossein2@gmail.com, l.merah@lagh-univ.dz, Larbi.Talbi@uqo.ca, a.alipacha@gmail.com

Abstract: Due to their attractive properties and simplicity, chaotic systems have garnered a lot of attention recently as a source of randomness and unpredictability. In many areas of computer applications, including information security, simulation, gaming etc., their inherent properties, such as sensitivity to the initial conditions, random-like behavior, and unpredictability, are highly desired. The usefulness of such systems as a source of randomness, however, is diminished by the fact that the digital implementation of such systems directly affects their dynamical behavior. This work aims to propose a simple and effective circuit for minimizing the effects of the digitization process on the behavior of chaotic systems and to achieve a strong and secure chaos-based PRNG. The proposed circuit has two main parts. The first is meant to make the digitized chaotic map even more random, and the second is meant to make the cycle-length longer. The proposed circuit has been performed on the logistic chaotic map. The improved map underwent several evaluations using a set of mathematical and statistical tools to affirm the improvement made to it. The simulation results have shown that the improved chaotic map provides better randomness and statistical properties. On the other hand, the designed improved map was synthesized on the Xilinx ZYNQ 7000 Field Programmable Gate Array (FPGA) where it provided better performance with low implementation cost compared with other proposals.

Keywords: Chaotic Maps, Dynamical Degradation, FPGA, PRNG, Cycle-length, Bifurcation.

1. Introduction

Random numbers are useful in a lot of computer applications. A lot of daily applications need the generation of random numbers, such as video games, gambling, cryptography, money transactions, e-payment and secured data exchange. Random numbers are a key part of simulating events in biology, geology, physics, chemistry and other fields. Random Number Generators are classified into two categories: True Random Number Generators (TRNG) and Pseudo Random Number Generators (PRNG). A TRNG is based on many unpredictable physical phenomena that generate noise, such as chemical reactions, machine vibrations, recorded noisy sounds, heat variation, etc. These kinds of random number sources are characterized by their infinite period with high unpredictability and complexity. However, it is not possible to regenerate the same random numbers using a TRNG if needed. Many applications, such as symmetric encryption systems, require this task.

PRNGs are generators that are implemented using finite arithmetic precision machines, whether in software or hardware form. PRNGs are similar to TRNGs, especially when large arithmetic precision is used. They are characterized by their speed and the possibility to regenerate the same sequence when required. In cryptographic applications, PRNGs should provide good statistical properties, be hard to predict, and have undefined periods. Such PRNGs are known as secure PRNGs, and their statistical quality is becoming more important than before. For example, a supercomputer might generate 10^9 random numbers per second and the cryptography algorithm needs 10^{16} random numbers to create a secure channel in very important communications. Thus, small correlations or other weaknesses in the generated sequence could easily lead to a critical leak in several network layers (Hu et al., 2020). A good PRNG should have the following characteristics: 1) a long-period random number sequence; 2) a statistical fit; 3) a high throughput rate; and 4) unpredictability (Li et al., 2011).

https://doi.org/10.33436/v33i2y202304

Recently, there has been a lot of interest in chaotic systems as a source of randomness. The chaotic behaviour of a nonlinear system seems random and has common characteristics of a noise. However, its randomness is purely resulting from a deterministic process (Merah et al., 2015). The defining properties of chaotic dynamics, namely ergodicity, sensitivity to initial conditions and system parameters (Lawande et al., 2005), are in fact the key features toward building robust and secure PRNGs for information security applications.

Recently, many studies have touched on the effects of the digitization process on the dynamical behaviour of chaotic systems. That is, the digital implementation of such systems using finite arithmetic precision leads to significant degradations in their dynamical behaviour (limited cycle-length, worse statistical properties, high density of periodic orbits, etc. (Merah et al., 2021). These degradations are in fact a serious problem that detracts from the importance of chaotic system's usefulness (Merah et al., 2019). Consequently, many recently published studies sought to provide a solution to this issue. The proposed solutions can be briefly classified into 4 main categories: 1) using high computation arithmetic precision (Flores-Vergara et al., 2019); 2) cascading multiple chaotic systems (Zhou et al., 2014b; Zhang et al., 2016; Yuan et al., 2019); 3) perturbing the chaotic system's orbit (Merah et al., 2019; Hu et al., 2014; Liu et al., 2020; Liu et al., 2021); and 4) customized solutions, some of which are a mixture of the first three solutions. Perturbation of the chaotic system's orbit is the more efficient remedy, and it has been supported both by theorists and practitioners in the field.

In this paper, an efficient circuit for improving the statistical properties and cycle-length of digitized chaotic maps while using low arithmetic precision to achieve a chaos-based PRNG is proposed. The proposed circuit was designed with four major issues in mind: statistical properties, cycle-length, hardware implementation cost, and performance. The novelty of this work is that the proposed circuit has an internal mechanism for self-perturbation and requires no external perturbation source. In addition, the perturbation periods are defined randomly, which improves the property of unpredictability. The proposed circuit has been performed on the logistic chaotic map, on which good results have been obtained.

This paper is organized as follows: section 2 reviews related works in this context. In section 3, the proposed circuit is presented in detail, along with a description of each of its sub-blocks. The evaluation of the improved maps using the proposed circuit using some mathematical and statistical tools is the subject of section 4. The hardware-based synthesis results of the improved maps using the ZYNQ 7000 FPGA circuit and the obtained performances are presented in section 5. Section 6 deals with the obtained comparison results of the proposed circuit with other proposals in terms of the statistical properties, complexity, and FPGA-based implementation cost and performance. The paper ends with a conclusion regarding the achieved results and future prospects.

2. Related works

This section reviews some related works in the context, with a focus on proposed schemes aimed at improving the dynamic chaotic behavior of digitized chaotic systems through hardware FPGA-based implementation. The authors in (Kopparthi et al., 2022) have proposed an efficient and simple scheme with the aim of improving the degradation in digital chaos by cascading the chaotic map with a three-stage XORed shift register that perturbs the output of the PWLCM. They further perturb the output of the shift register using a one-stage XOR post-processing. The proposed scheme has been performed on the PieceWise Linear Chaotic Map (PWLCM) and synthesized on the Xilinx ZYNQ-7000 FPGA circuit. The randomness evaluation results and the achieved performance showed clearly the efficacy of the proposed scheme. However, two main drawbacks can be observed in the proposed scheme: The first is that the evaluation was not performed using lower arithmetic precision (less than 32 bits) to confirm strongly its efficacy, and the second is that the cycle-length of the improved chaotic map was not evaluated at all.

The authors in (Kalanadhabhatta et al., 2020) have proposed a perturbation technique that consists of using a PUF (Physical Unclonable Function) to generate a secure seed for the chaotic map. The output of the PUF itself is controlled by the output of the perturbed chaotic map, which is

considered a bidirectional perturbation technique that increases the complexity of the chaotic output state. The authors have evaluated their proposed technique using the logistic map. The improved map has shown good randomness results. In addition, the FPGA-based synthesis results showed that the proposed technique can reach a throughput of 832 Mbits/s. In fact, what can be noted about the proposed technique is that the complexity of the improved map needs more evaluation using some known tools such as the LLE (Largest Lyapunov Exponent), the bifurcation diagrams, the phase space, etc. On the other hand, the authors did not evaluate the cycle-length of the improved map at all; this issue is pivotal in using chaotic maps for constructing secure PRNGs.

The authors in (Garcia-Bosque et al., 2019) have proposed an approach to dynamically changing the control parameters of the digitized chaos by using several values of control parameters instead of a single one. The control parameter γ_i is selected within a defined range according to the sequence k_i , which is chosen randomly as a function of x_i and γ_i . The authors have synthesized the improved chaotic map (the logistic map in their case) using the Virtex 7 FPGA circuit, in which the performance result showed that the achievable frequency is 132 MHz (with an arithmetic precision size of 32 bits). The randomness evaluation results using the NIST statistical test suite showed that the success rate reached 98.9 %. In fact, many drawbacks can be noted for this work; the first is that the efficiency of the proposed approach is not evaluated using low arithmetic precision (less than 32 bits) to confirm its efficacy. The complexity of the improved map needs more evaluation using many well-known tools such as LLE, autocorrelation, bifurcation diagram, SE (Sample Entropy), etc. In addition, the cycle-length of the improved map has not been evaluated at all.

Indeed, numerous works aim to improve the randomness and complexity of digitized chaotic systems in order to create secure PRNGs. It is difficult to review most of them, but what can be noted is that most of them fail to provide an inclusive evaluation to prove the randomness quality deeply. Despite having good ideas, some works did not evaluate the cycle-length of their proposed chaos-based PRNGs, which is critical in information security applications (Barakat et al., 2013; Yu et al., 2013; Thane & Chaudhari, 2018; Alawida et al., 2020; Liu et al., 2020;).

3. The proposed circuit

The logistic chaotic map is improved using the proposed circuit. Mathematically, the logistic map is written:

$$x_n = r.x_n(1-x_n) \tag{1}$$

Where r is the control parameter and $x_n \in [0,1]$, the system (1) exhibit chaos for $r \in [3.8, 4]$.

The basic scheme of the proposed circuit is presented in Figure 1. As seen, the circuit consists of two main parts. The first part consists of a processing block that improves the randomness quality and statistical properties of the chaotic map, while the second part consists of a perturbation block that prevents the chaotic system from entering a cycle (extending the cycle-length).

3.1. The processing block

The processing block receives the chaotic signal x_n of M bits of length and serializes it over the S/P (Parallel to Serial) block. The S_n signal (1 bit of length) is passed through a J-K flip-flop. The J and K inputs take the same value since they are connected to the same signal S_n. The next step consists of XORing the output of the J-K flip-flop with the LSB of the binary sequence x_n (the LSB is obtained using the SLICE block) to enhance the complexity of the final output of the improved chaotic map. We will see later that using the J-K flip-flop in conjunction with the logical operator XOR can disperse the bits of the binary sequence of the chaotic system and generate a new uniformly distributed sequence with good complexity. The output of the XOR gate is passed through the S/P (Serial to Parallel) block to create the modified chaotic signal $x_n^{'}$. The P/S block, the J-K flip flop, and the S/P block are controlled by a clock that is 4 times faster than the input clock.

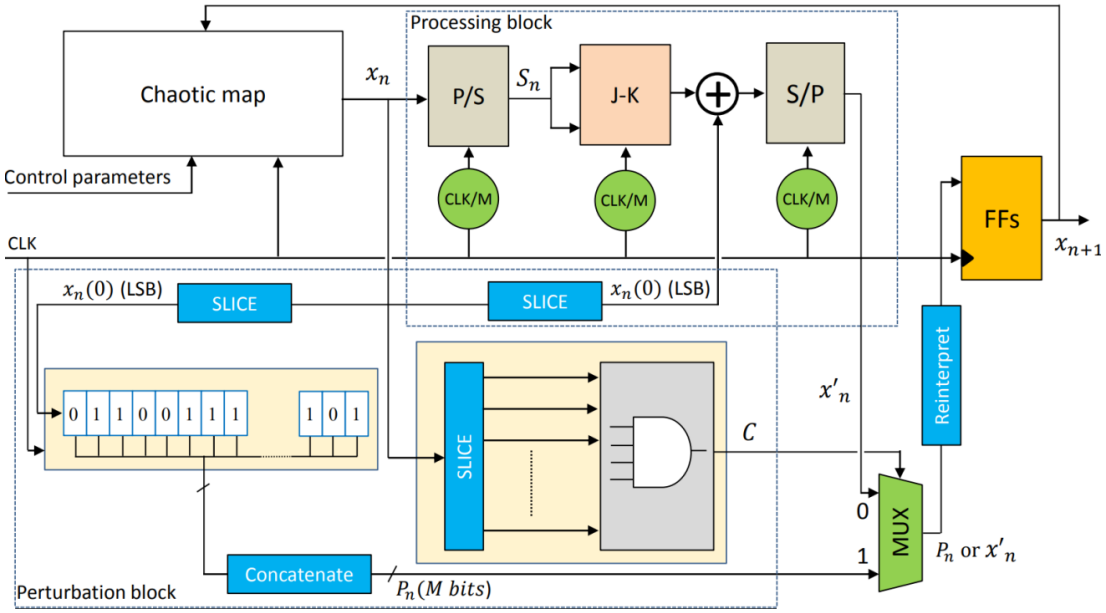

Figure 1. The proposed circuit's basic scheme

3.2. The perturbation block

As stated previously, the perturbation block is responsible for extending the cycle-length of the chaotic map and strengthening the unpredictability feature. The most important features of the proposed perturbation block include the fact that it does not require an external perturbation source and that the perturbation periods are defined at random. This block has two primary parts. The first component is an M-bit shift register, and the second is a controller for defining the perturbation periods. The shift register continuously loads the LSB of the x_n chaotic signal and shifts it to the right at each rising edge of the system clock. The perturbation signal P_n is created by concatenating the contents of each shift register cell.

The perturbation period controller is quite simple. It is made up of the SLICE block, which extracts the odd (or even) bit positions of the chaotic signal x_n. The output of the SLICE block is loaded into an AND logical gate. So, the output of the AND gate gets the logical value "1" only in the case where all its inputs have the value "1". Since the x_n signal is chaotic, having all the AND gate inputs equal to "1" occurs at random. Unknown perturbation periods can strengthen the unpredictability feature of the chaotic map.

The AND gate output controls a multiplexer that delivers either the modified chaotic signal $x_n^{'}$ or the perturbation signal P_n . As a result, the perturbation moments are when the AND gate outputs the value '1' and the signal P_n is fed to the chaotic map instead of $x_n^{'}$. Lastly, the output of the multiplexer goes through the reinterpret block, which changes the binary signal into a U-MQ-1 signal, which is unsigned and has a whole length of M bits and a fractional length of M-1 bits. Thus, the improved logistic chaotic map can be rewritten as follows:

$$x_{n+1} = \begin{cases} x_n = r.x_n(1-x_n) & if\ C=0 \\ x_n = r.P_n(1-P_n) & if\quad C=1 \end{cases} \tag{2}$$

4. Complexity and randomness evaluation

Fixed-point arithmetic precision is used to implement the system. By setting M to 24 bits, a number of statistical and mathematical tools are used to evaluate the improved logistic map. The evaluation results are given in the following sub-sections.

4.1. Phase space analysis

A phase space is a space that represents all conceivable states of a chaotic system. The random behaviour of a given chaotic system is reflected by visiting the maximum of possible values across a specific phase space. The phase space analysis has been performed on both the original and the improved logistic maps. The obtained results are given in Figure 2. It is clear that the output of the original logistic map is confined to a limited range within the entire range [0,1]. However, the improved logistic map's output is dispersed over the entire range [0,1]. The given results clearly affirm the improvement made on the original logistic map.

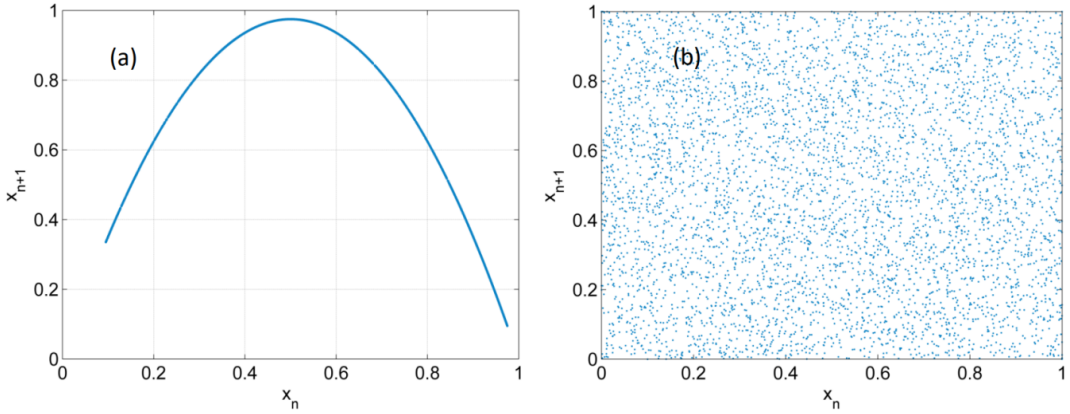

Figure 2. The phase space analysis: (a) The original logistic map and (b) the improved one

4.2. Bifurcation diagram analysis

Depending on the control parameters, a given chaotic system shows different behaviours from stable states, such as fixed points, periodic and quasi-periodic behaviours, to chaotic and unstable states (Merah et al., 2021). Transitions between these behaviours are called bifurcations. This graphical tool can help us evaluate the complexity of the improved map. Figure 3 shows the results of the bifurcation diagrams for both the original logistic map and the improved one. The obtained results show that, in contrast to the original map, the improved logistic map exhibits chaos across the entire control parameter interval [0,4]. This affirms the logistic map improvement made using the proposed circuit.

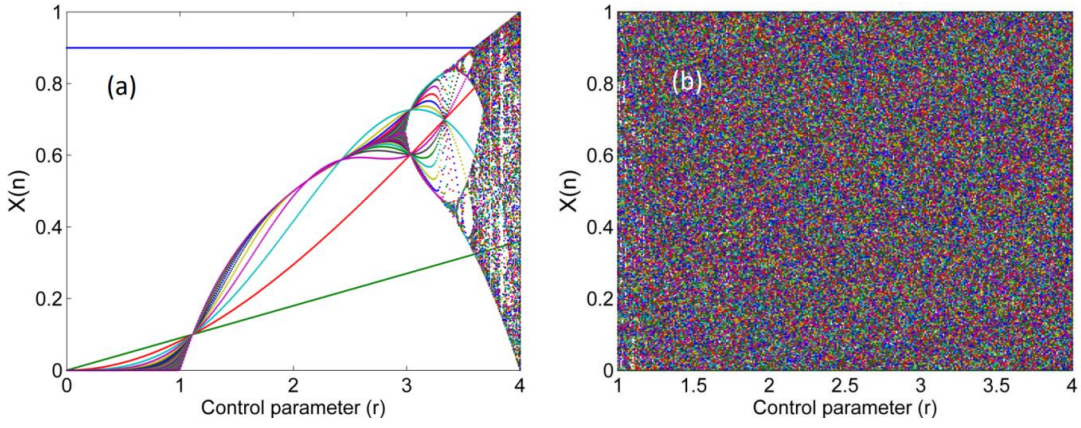

Figure 3. The bifurcation diagrams analysis: (a) The original logistic map and (b) the improved logistic map

4.3. The Largest Lyapunov Exponent analysis

The Largest Lyapunov Exponent *LLE* is a different metric that more accurately characterizes the chaotic behaviour (sensitivity to the initial conditions). It measures the evolution of an extremely tiny difference between two initial conditions.

A chaotic map with a positive *LE* would have completely divergent trajectories as time evolves, whereas a larger *LE* value characterizes the high unpredictability and sensitivity. For 1D maps, the *LE* can be calculated as follow:

$$LE = \lim_{k\to\infty} \frac{1}{k}\sum_{n=1}^{k} \ln|f'(x_n)| \tag{3}$$

The *LLE* analysis has been performed on both the original and the improved logistic maps as a function of the control parameter *r*. The obtained results are presented in Figure 4. As it can be seen, the *LLE* results for the improved map are all positive across the entire interval of *r*, in contrast to the original map, where the *LLE* has negative values across the entire interval of *r* except for $r \in [3.8, 4]$. On the other hand, the *LLE* approaches the value of *1.49* for the improved map, whereas the best case for the original map is *LLE=0.7*. The obtained results affirm the improvement made on the logistic map using the proposed circuit.

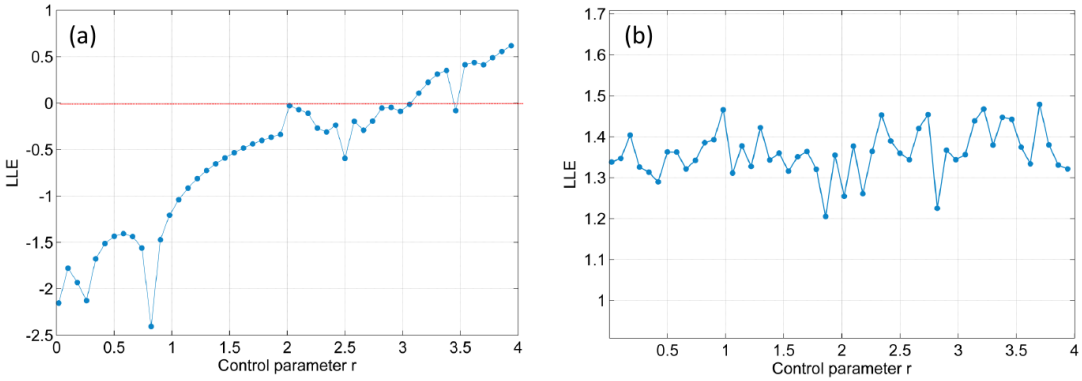

Figure 4. The Largest Lyapunov exponent analysis:
(a) The original logistic map and (b) the improved logistic map

4.4. Sample entropy analysis

Another metric that is used to characterize the complexity and unpredictability of a given time series is the *SampEn* (Sample Entropy). The objective of *SampEn* is to estimate the randomness of a series of data without any previous knowledge about the source generating the dataset (Delgado-Bonal et al., 2019). *SampEn* with high values indicates high complexity and unpredictability of the evaluated signal, while low values indicate its regularity and predictability.

The *SampEn* analysis is performed on both the original and improved logistic maps for a sequence of length of 10^6 and as a function of a set of control parameters *r*. In Figure 5, it is evident that the *SampEn* has the higher values (around 2.1) for the improved map throughout the entire interval of *r*, whereas for the original map, the *SampEn* is very low (around 0) and increases for $r > 3.2$ to reach the best-case value of 0.69. It can be concluded that the obtained results affirm the improvement made on the logistic map using the proposed circuit.

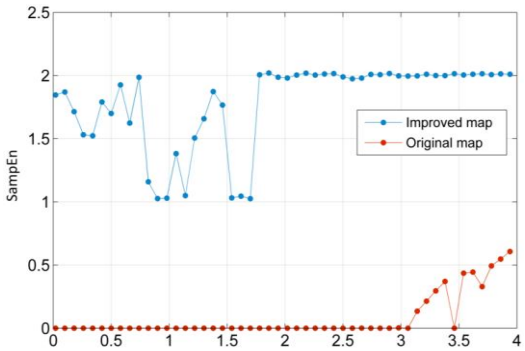

Figure 5. The Sample Entropy analysis

4.5. Permutation entropy analysis

The Permutation Entropy (*PE*) can also be used to evaluate the complexity of dynamical systems. It is based on the idea of capturing the order of values in a time series and getting the probability distribution of the ordinal patterns. The *PE* is characterized by its conceptual clarity and computational speed, and it offers numerous benefits. More details about the *PE* can be found in (Henry, 2018). The closer the *PE* is to 1, the more random the signal is and vice-versa.

The results of the *PE* analysis on both the original and improved maps are shown in Figure 6. It seems clear that the improved map gives the best results over the entire control parameter interval. The *PE* has always been very close to 1 (the best-case scenario for the *PE* is *0.99999804*), whereas the best-case for the original map is *PE = 0.85093339*. Consequently, it can be stated that the proposed circuit significantly improved the randomness of the original map.

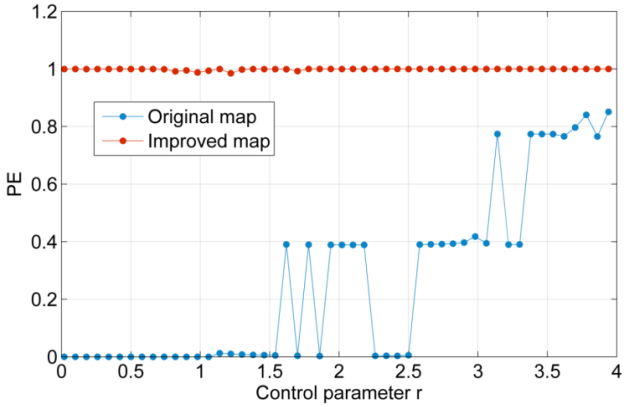

Figure 6. The Permutation Entropy analysis

4.6. Autocorrelation and cycle-length analysis

This section's goal is to evaluate the complexity of the improved map's output by identifying repeated patterns within the chaotic sequence. Thus, a time series is deemed random if its samples are not correlated (there are no repeated or similar samples). The autocorrelation function is an effective mathematical tool for this purpose. A low correlation value between samples indicates the chaotic generator's unpredictability level. In fact, the autocorrelation can also be used to determine the cycle-length of the chaotic generator. A peak on the autocorrelation graph shows that the system has entered a cycle.

The autocorrelation analysis has been done for a sequence of 10^5 samples on the original map and a sequence of 10^8 samples on the improved map. Figure 7 shows the results that were found. It is evident from Figure 7 (a) that the original map quickly enters a cycle with high correlation between samples, despite using 32-bit arithmetic precision. In this case, it's clear that the original logistic map is deterministic and far from chaotic.

In contrast, the improved map provides better results. The map's output in this case does not show any repeated patterns over 10^8 samples using 24 bits of arithmetic precision. On the other hand, Figure 7 (b) shows a very low correlation between samples (correlation coefficients $\in[-2.83\times10^{-3}, 3.34\times10^{-3}]$). This reflects the high level of randomness of the signal.

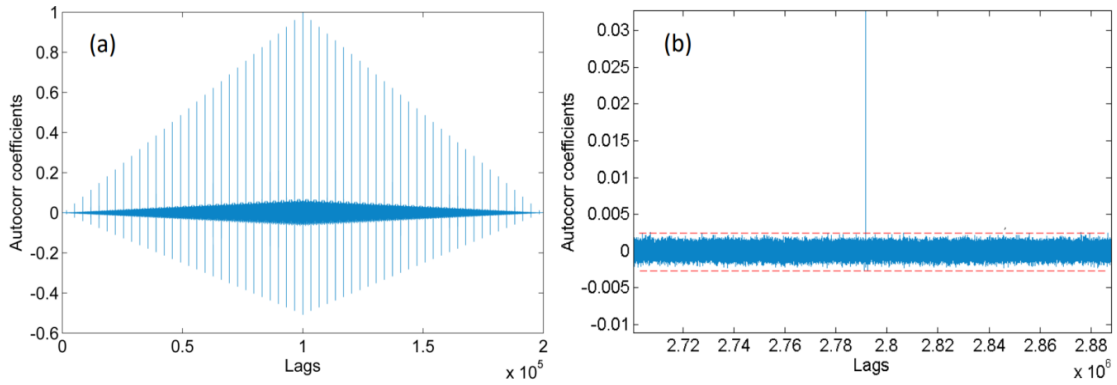

Figure 7. Autocorrelation function analysis: (a) The original logistic map and (b) the improved logistic map

The results of the obtained cycle-length for the original and the improved maps versus arithmetic precision size are given in Table 1. The simulation is done using a 10700KF Intel CPU (Turbo Boost Technology 2.0 Frequency of 5 GHz) with 64 Gb of DDR4 SRAM. We remark that the original logistic map falls quickly into a cycle, and the best case of the cycle-length is 38388 using 32 bits of arithmetic precision. Contrary, in the case of the improved map and for an arithmetic precision of 12 bit the cycle-length is 3633053, which is 55 times longer than the original map using 32 bits of arithmetic precision. On the other hand, we can't define how long the cycle is for the improved map over a sequence of length of 10^9, even using low arithmetic precision (16 bits). Therefore, we can say that the results we got are very good and that the logistic map has been satisfactorily improved.

Table1. Obtained cycle-length versus precision size

Chaotic map	Precision (bits)	Cycle-length
The original map	12	55
	16	179
	24	3389
	32	38388
The improved map	12	3633053
	16	Undefined
	24	Undefined
	32	Undefined

4.7. NIST statistical test suite

The Statistical Test Suite developed by NIST (Bassham et al., 2010) is an excellent and exhaustive document looking at various aspects of randomness in a long sequence of bits. It is a very important tool to understand randomness not only of the PRNGs but also of the crypto ciphers (Zaman et al., 2012). The NIST test suite is a set of 15 tests. For each test, a p_{value} (level of significance) is computed and the success condition of each test should be $p_{value} \geq 0.01$. The improved logistic map is subjected to NIST tests with randomly selected control parameters, using an arithmetic precision of 24 bits. The obtained results are shown in Table 2, where all tests were passed successfully in all cases except one, for $r = 0.2$, where two of the 15 tests failed. In fact, the original logistic map underwent the NIST tests, choosing the best case $r = 3.9$, and the success rate was 21.50%. The improved map has a 99.21% overall success rate. This is a much better result than what we got with the original map. Hence, the given results strongly confirm the improvement made on the original logistic map using the proposed circuit.

Table 2. NIST statistical test suite results

Statistical test	r=0.2	r=0.8	r=1.2	r=2.3	r=3.2	r=3.5	r=3.9	Success rate
	p_{value}	p_{value}	p_{value}	p_{value}	p_{value}	p_{value}	p_{value}	
Frequency	0,0180	0,9680	0,1300	0,6935	0,7964	0,9394	0,6213	100%
Block Frequency	0,0516	0,4729	0,4328	0,6546	0,4322	0,2903	0,5918	100%
Runs	0,9707	0,3211	0,4021	0,0690	0,0141	0,6016	0,0213	100%
Longest run of ones	0,9463	0,9642	0,3749	0,2318	0,7639	0,9543	0,8770	100%
Binary matrix rank	0,7858	0,5201	0,5787	0,3566	0,8469	0,7296	0,5055	100%
DFT	0,0948	0,9268	0,7411	0,7273	0,2053	0,1925	0,3833	100%
Non Overlapping	0,8373	0,9313	0,9106	0,9211	0,9900	0,9853	0,7608	100%
Overlapping	0,1546	0,9977	0,2464	0,9849	0,9032	0,4558	0,3906	100%
Universal	0,0293	0,3171	0,8121	0,2605	0,9751	0,6049	0,4502	100%
Linear complexity	0,4771	0,3489	0,3664	0,2826	0,9247	0,9856	0,7332	100%
Serial	0,1720	0,5578	0,2875	0,4885	0,7980	0,3632	0,8038	100%
Approximate Entropy	0,0307	0,6655	0,8581	0,8526	0,**630**6	0,8962	0,476**5**	100%
Cum Sums Forward	0,0193	0,9184	0,1035	0,7589	0,9237	0,8444	0,7985	100%
Cum Sums	0,0263	0,8898	0,1534	0,4186	0,7495	0,7765	0,6246	100%
Random Excursions	Failed	0,9404	0,6914	0,8189	0,9910	0,607**1**	0,8539	**85**.**71**%
Random Excursions var	Failed	0,9624	0,8167	0,3190	0,0462	0,1698	0,9645	**85**.**71**%

5. FPGA - based hardware implementation

The proposed circuit was designed and synthesized using XSG (Xilinx System Generator) and ISE (Integrated Synthesis Environment) design suite tools targeting the Xilinx ZYNQ-7000 FPGA. The XSG lets us design and simulate the system in Simulink, and then we can export the design as an ISE project that includes all the VHDL files that were made. We can choose between using the FPGA fabric or DSP (digital signal processing) slices to implement the two multiplication blocks. The ZYNQ- 7000 FPGA series contains 220 DSP48E1 slices. Each of them contains a 25×18 two's-complement multiplier, a 48-bit accumulator, and a power-saving pre-adder, in addition to other components. These embedded DSP slices are characterized by their high performance compared with FPGA fabric (Xilinx, 2018).

The exported project is then synthesized, mapped, placed, and routed under the ISE tool. A complete report detailing the hardware resource consumption and achievable performance using the ZYNQ-7000 FPGA is then generated.

Table 3 summarizes the generated report for the designed circuit that was built with an arithmetic precision size of 24 bits. There are two examples of implementation. The first uses the FPGA fabric to implement multipliers, whereas the second uses DSP48E1 slices. In the case of using DSP48E1 slices, the timing report covers 8580 paths, 0 nets, and 871 connections. The minimum period statistic $T_{min} = 5.977ns$ ($F_{max} = 167.308\ MHz$) assumes all single-cycle delays, such as logic component delays, routing delays, setup path delays, and so on. The system delivers 24 bits per one clock cycle, so the achievable throughput is $F_{max} \times 24\ bits = 4.015\ Gbps$.

Table 3. NIST statistical test suite results

		FPGA fabric		DSP48E1	
Resources	Available	Used	Usage	Used	Usage
LUTs	53200	1425	2.67 %	170	0.32 %
Registers	106400	1430	1.34 %	215	0.20 %
DSP48E1	220	0	0 %	**4**	1.81 %
Frequency		122.941 MHz		167.308 MHz	
Throughput		2.950 Gbps		4.15 Gbps	

6. The proposed circuit vs other proposals

This section aims to give an overall comparison between the proposed PRNG and other recently pro- posed chaos-based PRNGs. The comparison includes the statistical evaluation results, the cycle-length, the hardware implementation cost, and the achievable performance.

What can be concluded from Table 4 is that the proposed PRNG based on the improved logistic map provides better results in terms of FPGA-based hardware performance, has the lowest implementation cost, and has better randomness properties. On the other hand, the improved logistic map has been evaluated carefully using different mathematical and statistical tools. On the other hand, the cycle-length is an important issue that has been overlooked by the other proposals; in our case, the cycle-length has been greatly extended, and it cannot be detected, at least using our available computing platform. The proposed chaos-based PRNG reaches a throughput of 4.015 *Gbps* with a lower implementation cost compared to the other proposals. Our design uses only 0.32% of the available registers, 0.20% of the available LUTs, and 1.80% of the available DSP slices in terms of hardware resources.

Table 4. Performance and complexity comparison of the proposed design other proposals, (-) denotes this point has not been addressed, (*) information not given

Ref	Chaotic system	Precision (bits)	FPGA series	Hardware resources			Max frequency (MHz)
				LUTs	Reg	DSP	
(Kopparthi et al., 2022)	PWLCM	32	ZYNQ-7000	4215	578	0	81
(Kalanadhabhatta et al., 2020)	Logistic map	32	XC7VX330T	631	662	-	52
(Garcia-Bosque et al., 2019)	Logistic map Four-Wing Memristive	32	Virtex 7	510	120	13	132
(Yu et al., 2019)		32	ZYNQ-XC7Z020	24836	27371	-	135.04
(Thane et al., 2018)	PWLCM	-	Virtex II	310	119	-	373.218
Our work	Logistic map	24	ZYNQ-XC7Z020	170	215	4	167.308

Ref	Throughput Gbps	Cycle-length	LLE	SampEn/PE	NIST success rate (%)
(Kopparthi et al., 2022)	1.296	-	-	-	93.93
(Kalanadhabhatta et al., 2020)	0.832	-	-	-	99.13
(Garcia-Bosque et al., 2019)	0.132	-	-	-	98.90
(Yu et al., 2019)	-	-	-	-	98.70
(Thane et al., 2018)	-	-	-	-	*
Our work	4.015	Undefined	1.49027	2.1389480 0.9999980	99.21

7. Conclusion

In this paper, a trustworthy and secure PRNG based on an improved chaotic map was proposed. The primary component of the proposed PRNG is the proposed circuit, which is tasked with mitigating the dynamical degradation caused by the digitization process. The proposed circuit is novel in that it has an internal mechanism for self-perturbation and does not require an external perturbation source. It also has an efficient component to improve the statistical properties of the digitized chaotic map and performs the perturbation at random and unpredictable periods. The proposed circuit has been applied to the chaotic logistic map. In contrast to many other works, the enhancements made to the chaotic map have been thoroughly evaluated. Even using low arithmetic

precision (24 bits), good results have been obtained compared to other proposals in terms of complexity, cycle-length, and performance. The FPGA-based hardware synthesis results showed good results given by the proposed chaos-based PRNG. The proposed design offers better performance (a throughput of 4.015 Gbps) at a lower implementation cost (the implementation requires no more than 0.32% of the available registers, 0.20% of the available LUTs, and 1.80% of the available DSP slices). The future work will be focused on integrating the proposed chaos-based PRNG into a real-time application of information security. Given its simplicity, the proposed chaos-based PRNG will be useful in securing resource-constrained wireless networks.

REFERENCES

Alawida, M., Samsudin, A. & Teh, J. S. (2020) Enhanced digital chaotic maps based on bit reversal with applications in random bit generators. *Information sciences*. 512, 1155–1169. doi:10.1016/j.ins.2019.10.055.

Barakat, M. L. (2013) Generalized hardware post-processing technique for chaos-based pseudorandom number generators. *ETRI journal.* 35(3), 448–458. doi:10.4218/etrij.13.0112.0677.

Delgado-Bonal, A. & Marshak, A. (2019) Approximate Entropy and Sample Entropy: A comprehensive tutorial. *Entropy* (Basel, Switzerland). 21(6), 541. doi:10.3390/e21060541.

Flores-Vergara, A. et al. (2019) Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. *Nonlinear dynamics*. 96(1), 497–516. doi:10.1007/s11071-019-04802-3.

Garcia-Bosque, M. et al. (2019) Chaos-based bitwise dynamical pseudorandom number generator on FPGA. *IEEE Transactions on Instrumentation and Measurement*. 68(1), pp. 291–293. doi:10.1109/tim.2018.2877859.

Henry, M. (2018) Permutation Entropy. *Aptech*. https://www.aptech.com/blog/permutation-entropy [Accessed: 12th May 2022].

Hu, H., Deng, Y. & Liu, L. (2014) Counteracting the dynamical degradation of digital chaos via hybrid control. *Communications in nonlinear science & numerical simulation.* 19(6), 1970–1984. doi:10.1016/j.cnsns.2013.10.031.

Hu, Z. et al. (2020) High-speed and secure PRNG for cryptographic applications. *International Journal of Computer Network and Information Security.* 12(3), 1–10. doi:10.5815/ijcnis.2020.03.01.

Kalanadhabhatta, S. et al. (2020) PUF-based secure chaotic random number generator design methodology. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. 28(7), pp.1740–1744. doi:10.1109/tvlsi.2020.2979269.

Kopparthi, V. R. et al. (2022) Hardware architecture of a digital piecewise linear chaotic map with perturbation for pseudorandom number generation. *AEU-International Journal of Electronics and Communications*, 147(3), 154138. doi:10.1016/j.aeue.2022.154138.

Lawande, Q. V. & Dhodapkar, S. (2005) Chaos based cryptography: A new approach to secure communications.https://www.semanticscholar.org/paper/a25208ca01cca852b01b5e7177255a76b222a1ab [Accessed: 10th November 2022].

Li, C.-Y. et al. (2012) Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. 20 (2), pp.385–389. doi:10.1109/tvlsi.2010.2103332.

Liu, B., Xiang, H. & Liu, L. (2020) Reducing the dynamical degradation of digital chaotic maps with time-delay linear feedback and parameter perturbation. *Mathematical Problems in Engineering.* 2020, 1–12. doi:10.1155/2020/4926937.

Liu, J. et al. (2020) A hardware pseudo-random number generator using stochastic computing and logistic map. *Micromachines*. 12(1), 31. doi:10.3390/mi12010031.

Liu, L., Xiang, H. & Li, X. (2021) A novel perturbation method to reduce the dynamical degradation of digital chaotic maps. *Nonlinear dynamics.* 103(1), 1099–1115. doi:10.1007/s11071-020-06113-4.

Merah, L. et al. (2018) New and efficient method for extending cycle length of digital chaotic systems. *Iranian Journal of Science and Technology Transactions of Electrical Engineering*. 43(09), 259–268. doi:10.1007/s40998-018-0122-0.

Merah, L. et al. (2021) Real-time implementation of a chaos based cryptosystem on low-cost hardware. *Iranian Journal of Science and Technology Transactions of Electrical Engineering*. 45(4), 1127–1150. doi:10.1007/s40998-021-00433-w.

Merah, L., Ali-Pacha, A. & Hadj-Said, N. (2015) Real-time cryptosystem based on synchronized chaotic systems. *Nonlinear dynamics*. 82(1–2), 877–890. doi:10.1007/s11071-015-2202-2.

Merah, L., Lorenz, P. & Adda, A.-P. (2021) A new and efficient scheme for improving the digitized chaotic systems from dynamical degradation. *IEEE access: practical innovations, open solutions.* 9, pp. 88997–89008. doi: 10.1109/access.2021.3089913.

Rukhin, A. et al. (2010) A statistical test suite for random and pseudorandom number generators for. *Acm.org*. https://dl.acm.org/doi/pdf/10.5555/2206233 [Accessed: 16th May 2022].

Thane, A. & Chaudhari, R. (2018) Hardware design and implementation of pseudorandom number generator using piecewise linear chaotic map. *2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018, Bangalore, India, September 19-22, 2018.* IEEE, 2018.

User Guide (2018) 7 Series DSP48E1 Slice. *Bdtic.com.* http://www.bdtic.com/download/XILINX/UG479.pdf [Accessed: 10th April 2022].

Yu, F. et al. (2019) Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map. *IEEE access: practical innovations, open solutions*. 7, pp. 181884–181898. doi:10.1109/access.2019.2956573.

Yuan, F. et al. (2019) A cascading method for constructing new discrete chaotic systems with better randomness. *Chaos* (Woodbury, N.Y.). 29(5), 053120. doi:10.1063/1.5094936.

Zaman, J. K. M., Sadique, Uz & Ghosh, R. (2012) A review study of NIST Statistical Test Suite: Development of an indigenous computer package. doi:10.48550/ARXIV.1208.5740.

Zhang, T. et al. (2016) A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci-Lucas transform. *Mathematical Problems in Engineering*, 2016, 1–15. doi:10.1155/2016/7683687.

Zhou, Y. et al. (2015) Cascade chaotic system with applications. *IEEE Transactions on Cybernetics*. 45(9), pp. 2001–2012. doi:10.1109/TCYB.2014.2363168.

Merah HOCINE obtained his engineering degree in Electronics (Communication) from Amar Telidji University of Laghouat – Algeria in 2009 and a magister degree also from Ferhet Abbess University in Setif, Algeria in 2012. He got his Ph.D. from Amar Telidji University of Laghouat – Algeria in 2019. Due to his efforts, he benefited from an exceptional national program scholarship from the Algerian government (2018-2020) to Canada, immediately after this training he worked as a head of the Physics department at the level of ENS Laghouat, Algeria. Currently, he is an associate professor at the École Normale Supérieure of Laghouat – Algeria. He is mainly interested in research fields like: performance analysis of multicarrier modulation, communication systems, networks and multi-carrier waveforms. He is also concerned with certain aspects such as: channel coding, signal processing, PAPR reduction, information security and channel estimation.

Merah LAHCENE received an engineering degree in Electronics (Instrumentation) from the University Amar Telidji of Laghouat, Algeria, in 2004, and the M.Sc. and Ph.D. degrees in telecommunication systems from the University of Science and Technology of Oran, Algeria, in 2010 and 2016, respectively. From 2006 to 2008, he worked as an Instrumentation Engineer with the National Company SONATRACH, where he acquired good experience in the maintenance of gas turbines. He is currently a Lecturer with the Department of Electronics, University Amar Telidji of Laghouat. He has several published works in these contexts. He joined several research laboratories, such as the Advanced Microsystems Engineering Laboratory, University of Quebec, Ottawa, ON, Canada, the Coding and Information Security Laboratory, University of Science and Technology of Oran, Algeria, and the Signals and Systems Laboratory, University Amar Telidji of Laghouat, Algeria. His research interests include information security, chaos-based secure information, random number generators, and signal processing on reconfigurable hardware.

Talbi LARBI (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering from Laval University, Quebec, QC, Canada, in 1989 and 1994, respectively. He completed a postdoctoral fellowship with INRS-Telecommunications, Montreal, QC, within the Personal Communications Research Group, from 1994 to 1995, where he led projects supported by

Bell Canada. From 1995 to 1998, he was an Assistant Professor with the Electronics Engineering Department, at Riyadh College of Technology, Saudi Arabia. From 1998 to 1999, he was an Invited Professor with the Electrical and Computer Engineering Department, at Laval University. Since 1999, he has been a Professor with the Department of Computer Science and Engineering, University of Quebec, Outaouais/Ottawa region, Canada, where he is M.Sc. Program Chair in sciences and information technologies. He has authored or co-authored more than 170 journal articles and conference papers. His research interests include the experimental characterization and modelling of UHF/EHF indoor radio propagation channels and the design of antennas and microwave circuits for wireless communication systems. Currently, he is actively involved in major projects related to the deployment of wireless technologies in underground mines, mainly experimental characterization of underground mine channels using MIMO antennas at 60 GHz, the design of microwave and RF components using SIW techniques and metamaterials, and antenna arrays for wireless applications. He is a member of Ordre des Ingénieurs du Québec.

Ali-Pacha ADDA was born in Algeria. He received the engineering degree in telecommunications from the Institute of Telecommunication of Oran, Algeria, in 1986, the University degree in mathematics and the Magister degree in signal processing from the University of Oran I, Algeria, in 1986 and November 1993, respectively, and the Ph.D. degree in safety data from the University of Sciences and Technology of Oran, in 2004. From 1986 to 1988, he worked with the Telecommunications Administration (PTT Oran) in the position of Head of Telephone Traffic for a period of two years. He is currently a Professor (Teacher/Researcher) with the Electronics Department, University of Sciences and Technology of Oran (USTO). He is also the Head of the Laboratory of Coding and Security of Information (LACOSI Laboratory). His research interests include coding, cryptography and security, and digital signal processing using reconfigurable hardware.