Multimedia Tools and Applications (2022) 81:39003–39020
https://doi.org/10.1007/s11042-022-13175-6

On the implementation of large period piece-wise linear Arnold cat map

Djeugoue Hermann[1] · Gnyamsi Gaetan Gildas[1] · Jean Sire Armand Eyebe Fouda[1,2] · Wolfram Koepf[2]

Received: 27 April 2021 / Revised: 17 February 2022 / Accepted: 11 April 2022 /
Published online: 26 April 2022

Abstract
This paper presents a piece-wise linear cat map (PWLCM) obtained by perturbing the conventional quantized Arnold cat map (QACM) with a nonlinear term. The effect of the nonlinear term on the dynamics of the QACM is investigated. We show that the eigenvalues, hence the Lyapunov exponents of the PWLCM depend on the initial conditions, which is not the case for the QACM. As a result, the proposed PWLCM is a generalized form of the QACM, whose the period exponentially increases with respect to the precision, thus taking as value 1.09×10^{513} for only 10-bit precision; while that of the corresponding QACM is only 768. The nonlinear term increases the sensitivity of the system to the initial conditions, which contributes to increase its period, hence to enhance its complexity. An electronic implementation of both the QACM and the PWLCM in the case of 4-bit precision using Multisim is presented. The proposed architecture of both the QACM and the PWLCM are implemented using Verilog and prototyped on the Zynq 7020 FPGA board. For 4-bit precision, the FPGA implementation performs 1.072 Gbps throughput at 134 MHz maximum frequency. We verified that experimental and simulation behaviors of the proposed system perfectly match, thus confirming the effectiveness of the proposed electronic circuit for exhibiting the expected dynamics in real-time.

Keywords Dynamical system · Random number · Circuit theory · Digital circuits

1 Introduction

Random number generators are used in cryptography, in games of chance, in all computer algebra systems or other programming languages and in numerical simulations, to cite a

✉ Wolfram Koepf
koepf@mathematik.uni-kassel.de

Jean Sire Armand Eyebe Fouda
efoudajsa@yahoo.fr

[1] Départment de Physique, Université de Yaoundé I, Yaoundé, Cameroun

[2] Institute of Mathematics, University of Kassel, Kassel, Germany

few. In order to achieve fast generation of random numbers, researchers have focused their attention to chaotic systems that can be experimentally implemented [5, 15, 21]. Chaotic systems are sensitive to initial conditions and present mixing properties that are necessary for a good pseudo-random number generator [12]. Since then, various chaotic systems generating a large variety of complex dynamics have been modeled, but they are still suffering from lack of reliable methods for their implementation [3, 24–26, 32]. Some of them are realized with analogue circuits, while many others are more and more implemented using numerical targets like the Field Programmable Gate Array (FPGA) [2, 16, 19, 26–28].

Chaotic systems have been shown efficient and convenient for modern cryptography, although most experimental and commercial systems are using random number generators (RNGs) based on modular algebra operations, as the digitization of chaotic orbits sometimes may reduce the key sensitivity [20, 26]. Such RNGs present the advantage to make modular calculations in a finite field (the Galois field GF(2^n) for example), hence to be easily implemented on hardware with a finite number of basic electronic logic gates without loss of precision. An example is the RNG implemented by the $RAND$ function in the MATLAB software to generate uniformly distributed random numbers. Another example is the Arnold cat map (ACM) which is often used for its ergodic and mixing properties [1, 30]. In practical applications, the original cat map is generalized and discretized in the phase space to obtain the quantized ACM (QACM).

Arnold's cat map is known to be chaotic, area-preserving, ergodic and mixing, and invertible [8, 10, 17]. It has a unique hyperbolic fixed point and the linear transformation defining it is hyperbolic (it presents irrational eigenvalues, one with an absolute value greater than 1 and the other one less than 1). Its quantized version forms short limit cycles whose lengths depend on the modulo value, although it preserves the properties of its continuous analogue [4, 11]. The other properties of this interesting map can be found in the literature [4, 8, 10, 11, 17]. The ACM is used in cryptography, in digital tattoo applications, in watermarking and for random number generation to cite a few [8, 9, 23]. The QACM is particularly used for image scrambling due to its periodic nature [7]. It has been also used for the implementation of public key ciphers [18], but the latter are not secure when dealing with QACM with weak periods [22].

Thus, the period of the QACM is an important parameter when using it in cryptography. It has been shown that the period of the QACM does not exceed $3m$, m being the modulo value. In the case of n-bit precision ($m = 2^n$) which is convenient for digital applications, the period of the QACM is only equal to $3{\cdot}2^{n-2}, n \geq 2$, which is effectively smaller than $3m$. Therefore, for the security level of ciphers including the QACM to be enhanced, its period needs to be increased. In order to overcome such a limitation of the period, the ACM ($n = 0$) is preferred to the QACM in many applications. Some improvements including the increase of the dimension of the map have been proposed. Guoscheng et al. [14] proposed to extend the conventional 2D Arnold's cat map into a 3D map by introducing six control parameters. Although the resulting map allows to increase the key space for data encryption, the authors did not investigate its period distribution, as well as the impact of the introduced control parameters on dynamics of the system. To prevent the degradation of chaotic sequences into periodic ones due to the finite computer precision, they just applied a slight perturbation on the 3D map output without formally investigating its impact. In [33], the authors combined the 2D cat map with an affine cipher to enhance the security level of their proposed cipher. In order to efficiently apply Arnold's cat map to data encryption, it is important to directly investigate and increase its period in the discrete phase space, hence to significantly increase the period of the QACM, even for small data precision.

In this paper, we suggest to introduce a nonlinear perturbation to the linear QACM for its period to increase. In order to preserve the simplicity of the QACM, we consider as nonlinear element another modular algebra based module, such that the final system is a piece-wise linear cat map (PWLCM). We thus investigate the dynamics of the so-called PWLCM and verify that in the case of 4-bit precision, its period is more than 10^{11} times greater than that of the conventional QACM. An equivalent electronic circuit is proposed in the case of 4-bit precision to further confirm the simplicity of the proposed system that can be used for the generation of pseudo-random numbers. Furthermore, an equivalent implementation on Zynq 7020 FPGA board is presented in order to confirm the effectiveness of the proposed architecture.

The rest of the paper is organized as follows: in Section 2 the modeling system is presented, Section 3 is devoted to the results analysis, Section 4 shows the electronic implementation of the PWLCM while in Section 5 some concluding remarks are given.

2 The modeling system

2.1 The conventional quantized Arnold cat map

The Arnold cat map has been widely described and investigated in the literature. The evolution of the 2D system behavior, where the two variables (position and momentum) are completely depending on each other is modeled as follows [17]:

$$\begin{cases} x(t+1) = x(t) + \alpha y(t) \\ y(t+1) = \beta x(t+1) + y(t) \end{cases} \mod m. \tag{1}$$

The system in (1) can be rewritten using matrix representation as

$$\mathbf{x}(t+1) = A\mathbf{x}(t) \mod m \tag{2}$$

where

$$A = \begin{pmatrix} 1 & \alpha \\ \beta & \alpha \cdot \beta + 1 \end{pmatrix},$$

$(\alpha, \beta) \in \mathbb{N}^2_{\geq 1}$, and $\mathbf{x} = (x, y)^T$; $(\cdot)^T$ is the transpose of $(\cdot)$. This discrete time system is continuous in the phase space for $(x, y) \in [0, 1)^2$ and $m = 1$. The QACM is obtained for $(x, y) \in [0, m)^2$ with $m \in \mathbb{N}_{>1}$. It is periodic and its period depends both on m and the parity of α and β. For $\alpha = \beta = 1$ and $m = 2^n$, the period behaves like

$$\Pi_n = 2 \cdot \Pi_{n-1},\ n > 2 \tag{3}$$

with $\Pi_1 = \Pi_2 = 3$ for the minimal period, as shown in [8, 11].

2.2 The piece-wise linear cat map

In order to increase the period of the QACM, we introduce a nonlinear perturbation term to the conventional QACM. The modified system is written as

$$\mathbf{x}(t+1) = A\mathbf{x}(t) + \mathbf{x}_c(t) \mod m, \tag{4}$$

where

$$\mathbf{x}_c(t) = \begin{pmatrix} \sum_{i=1}^{M} \Big(a_i + y(t)\Big) \bmod c_i \\ \sum_{j=1}^{N} \Big(b_j + x(t+1)\Big) \bmod d_j \end{pmatrix} \tag{5}$$

with $(i, j) \in \mathbb{N}^2$, c_i and d_j two natural numbers such that $0 \leq c_i < m + a_i$ and $0 \leq d_j < m + b_j$, $0 \leq a_i, b_j < m$ if $(c_i, d_j) = (0, 0)$; $0 \leq a_i < c_i$ if $c_i \neq 0$ and, $0 \leq b_j < d_j$ if $d_j \neq 0$. Let us consider $\mathbf{x}_c(t) = \Big(x_c(t), y_c(t)\Big)^T$ with

$$x_c(t) = \sum_{i=1}^{M} x_{c,i}(t), \tag{6}$$

$$y_c(t) = \sum_{j=1}^{N} y_{c,j}(t). \tag{7}$$

and

$$x_{c,i}(t) = \Big(a_i + y(t)\Big) \bmod c_i, \tag{8}$$

$$y_{c,j}(t) = \Big(b_j + x(t+1)\Big) \bmod d_j, \tag{9}$$

Equations (8)-(9) can be written as piece-wise linear functions such that:

$$x_{c,i}(t) = \begin{cases} a_i + y(t), & \text{if } a_i + y(t) < c_i; \\ a_i + y(t) - q_i c_i, & \text{otherwise,} \end{cases} \tag{10}$$

where $q_i = \lfloor \frac{a_i + y(t)}{c_i} \rfloor$; and

$$y_{c,j}(t) = \begin{cases} b_j + x(t+1), & \text{if } b_j + x(t+1) < d_j; \\ b_j + x(t+1) - q_j d_j, & \text{otherwise,} \end{cases} \tag{11}$$

$q_j = \lfloor \frac{b_j + x(t+1)}{d_j} \rfloor$. By developing the whole set of equations, we obtain the PWLCM defined as:

$$\mathbf{x}(t+1) = B\mathbf{x}(t) + C(t) \mod m \tag{12}$$

where

$$B = \begin{pmatrix} 1 & \alpha' \\ \beta' & \alpha'\beta' + 1 \end{pmatrix}, \tag{13}$$

with $\alpha' = M + \alpha$, $\beta' = N + \beta$ and,

$$C(t) = \begin{pmatrix} \sum_{i=1}^{M} \Big(a_i - q_i c_i \cdot u\Big(a_i + y(t) - c_i\Big)\Big) \\ \beta' \sum_{i=1}^{M} \Big(a_i - q_i c_i \cdot u\Big(a_i + y(t) - c_i\Big)\Big) + \sum_{j=1}^{N} \Big(b_j - q_j d_j \cdot u\Big(b_j + x(t+1) - d_j\Big)\Big) \end{pmatrix}. \tag{14}$$

$u(t)$ is the Heaviside function defined as

$$u(t) = \begin{cases} 0, & \text{if } t < 0; \\ 1, & \text{otherwise.} \end{cases} \tag{15}$$

The PWLCM thus obtained presents a conservative linear term $B\mathbf{x}(\mathbf{t})$ ($\det(B) = 1$) that exhibits the same behavior as a QACM, and a nonlinear term $C(t)$ that contributes to

increase the period of the linear term by modifying its trajectory for a given initial condition. a_i and b_j, c_i and d_j are defined as perturbation parameters.

2.3 Stability analysis of the PWLCM

In this section, we investigate the stability of the PWLCM. While considering the system in (12), we deduce the following Jacobian matrix:

$$J = \begin{pmatrix} 1 & \alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right) \\ \beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right) & 1 + \left(\alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right)\right)\left(\beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right)\right) \end{pmatrix} \tag{16}$$

where $\tau_x^j = d_j - b_j$ and $\tau_y^i = c_i - a_i$. Indeed, $q_i = 1$ when $\delta\left(y(t) - \tau_y^i\right) = 1$ and $q_j = 1$ when $\delta\left(x(t+1) - \tau_x^j\right) = 1$. From the above Jacobian matrix we deduce the eigenvalues

$$\Lambda_1(t) = 1 + \tfrac{1}{2}\left(\alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right)\right)\left(\beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right)\right) \left(1 + \sqrt{1 + \frac{4}{\left(\alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right)\right)\left(\beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right)\right)}}\right) \tag{17}$$

and

$$\Lambda_2(t) = 1 + \tfrac{1}{2}\left(\alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right)\right)\left(\beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right)\right) \left(1 - \sqrt{1 + \frac{4}{\left(\alpha' - \sum_{i=1}^{M} c_i \delta\left(y(t) - \tau_y^i\right)\right)\left(\beta' - \sum_{j=1}^{N} d_j \delta\left(x(t+1) - \tau_x^j\right)\right)}}\right) \tag{18}$$

The determinant of J is equal to 1, which implies that the sum of the Lyapunov exponents $\lambda_1(t)$ and $\lambda_2(t)$ is equal to 0, hence $\Lambda_1(t) \geq 1$ and $0 \leq \Lambda_2(t) \leq 1$. The PWLCM is thus a conservative system as the generating ACM, independently to the choice of the parameters a_i, b_i, c_i and d_i. Depending on the choice of these parameters, it can be difficult to determine the steady states of the system, whenever they exist. For $a_i = b_j = 0, \forall i,\ j$, $(x = 0, y = 0)$ is the single steady state of the system. Given that $\Lambda_{1,2} > 0$, all the existing steady states of the PWLCM are unstable.

2.4 The reverse PWLCM

The generalized inverse PWLCM is obtained by determining $x(t)$ and $y(t)$ from (4) as:

$$\begin{cases} x(t) = x(t+1) - y(t) - \sum_{i=1}^{M}(y(t) + a_i) \bmod c_i \\ y(t) = x(t+1) - y(t+1) - \sum_{j=1}^{N}(x(t+1) + b_j) \bmod d_j. \end{cases} \bmod 2^n \tag{19}$$

Given that $x(t+1)$ and y(t+1) are the initial condition for the reverse system, $x(t)$ and $y(t)$ are the iterates that are obtained from the initial conditions. By reversing the time evolution, (19) can be rewritten as:

$$\begin{cases} y(t+1) = x(t) - y(t) - \sum_{j=1}^{N}(x(t)+b_j) \bmod d_j \\ x(t+1) = x(t) - y(t+1) - \sum_{i=1}^{M}(y(t+1)+a_i) \bmod c_i. \end{cases} \bmod 2^n \qquad (20)$$

Equation (20) is the reverse PWLCM.

3 Results and discussion

In this section, we investigate the dynamics of the PWLCM period and largest Lyapunov exponent with respect to the system control parameters and initial conditions. For a given precision, the period of the PWLCM is equivalent to the least common multiple (lcm) of the individual periods of the set of initial conditions [6, 13, 27, 29, 31]. Indeed, each possible initial condition of the phase space generates its own dynamics whose period is determined. The number of initial conditions is directly related to the precision n. For $n = 1$ for example, there are four possible initial conditions that are $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$.

3.1 Sensitivity to initial conditions

3.1.1 Sensitivity of the period

We evaluate the period of the system for various precisions $n = 2$ to $n = 8$. Table 1 illustrates the matrix $T(x_0, y_0)$ of individual periods for the different initial conditions of the PWLCM in the case of $n = 2$. We set for this example $\alpha = \beta = 1$, $M = N = 2$, $c_1 = 0$, $c_2 = 3$, $d_1 = 3$, $d_2 = 5$, $a_1 = 1$, $a_2 = 1$, $b_1 = 0$ and $b_2 = 2$. The period of the PWLCM in that case is equal to $\Pi = \text{lcm}(\{T(x_0, y_0)\}) = 105$, $0 \leq x_0, y_0 \leq 2^n - 1$; while the corresponding period for the QACM is 3. In order to estimate the impact of the nonlinear term on the QACM, we evaluated the period of the QACM described by matrix B, instead of matrix A. We obtained as period $\Pi_B = 3$ while $\Pi_A = 3$. It appears that by adding the modulus terms, the system described by T_A is both linearly and nonlinearly modified, thus leading to a new QACM that is perturbed by the nonlinear term $C(t)$. The linear modification leads to the conventional QACM, whereas the nonlinear modification leads to a completely different system with a large period that does not necessarily respect the relation in (3).

Table 1 also shows that the system above described presents a single steady state that is ($x_0 = 2$, $y_0 = 3$). While evaluating the impact of the perturbation on the QACM, we observed that for some combinations of parameters a_i, b_i c_i and d_i, the PWLCM may present or not multiple steady states. For $\alpha = \beta = 1$, $M = N = 2$, $c_1 = c_2 = 0$,

Table 1 Matrix of the individual period of different initial conditions of the PWLCM for $n = 2, \alpha = \beta = 1, M = N = 2, c_1 = 0, c_2 = 3, d_1 = 3, d_2 = 5, a_1 = 1, a_2 = 1, b_1 = 0$ and $b_2 = 2$

$x_0 \backslash y_0$	0	1	2	3
0	7	5	7	5
1	7	3	5	7
2	7	3	5	1
3	3	5	7	7

Table 2 Matrix of the individual largest Lyapunov exponent of different initial conditions of the PWLCM for $n = 2$, $\alpha = \beta = 1$, $M = N = 2$, $c_1 = 0$, $c_2 = 3$, $d_1 = 3$, $d_2 = 5$, $a_1 = 1$, $a_2 = 1$, $b_1 = 0$ and $b_2 = 2$; $\lambda_0(3, 3) = 2.3895$

$x_0 \backslash y_0$	0	1	2	3
0	1.6777	1.2718	1.6778	1.2719
1	1.6778	2.4554	1.2721	1.6778
2	1.6778	2.4554	1.2720	2.3895
3	2.4554	1.2719	1.6777	1.6777

$d_1 = d_2 = 0$, $a_1 = 0$, $a_2 = 0$ and $b_1 = b_2 = 0$ for example, there is a single steady state, that is ($x_0 = 0$, $y_0 = 1$) while the period of the system is $\Pi = 3$. By just changing the value of c_2 as $c_2 = 3$, the system now presents two steady states that are ($x_0 = 0$, $y_0 = 1$) and ($x_0 = 0$, $y_0 = 2$) and a period $\Pi = 20$.

3.1.2 Sensitivity of the Lyapunov exponent

We also evaluate the Lyapunov exponents of the above system for each initial condition with the above three parameter settings and compare them to the largest Lyapunov exponent of the corresponding QACM, that is

$$\lambda_0(\alpha', \beta') = \log\left(1 + \frac{1}{2}\alpha'\beta' + \frac{1}{2}\sqrt{\alpha'^2\beta'^2 + 4\alpha'\beta'}\right) \tag{21}$$

We considered 20 000 iterations of the PWLCM to evaluate the Lyapunov exponents.

For the first parameter setting, Table 2 shows the corresponding largest Lyapunov exponents of the PWLCM that are to be compared to $\lambda_0(3, 3) = 2.3895$. It appears from this table that setting $c_i \neq 0$ and $d_j \neq 0$ contributes to reduce the Lyapunov exponent, while it contributes to increase the period of the system.

The second parameter setting leads to Table 3, with values that are to be compared to $\lambda_0(3, 3) = 2.3895$. We can confirm that the Lyapunov exponent does not depend on a_i and b_i in the case $c_i = d_j = 0$.

The third parameter setting leads to Table 4, with values that are also to be compared to $\lambda_0(3, 3) = 2.3895$. This table as compared to Table 3 shows that setting $c_i \neq 0$ or $d_j \neq 0$ reduces the value of the Lyapunov exponent, while increasing the period of the PWLCM.

The combination of the observations made from these three tables implies that there is no direct relationship between the Lyapunov exponent and the period of the system. Furthermore, a large Lyapunov exponent in that case does not induce a high complexity of the PWLCM, as it corresponds to the smallest period. However, we observe that the period of the system increases with the diversity or variability of the Lyapunov exponent. Indeed, a high sensitivity of the Lyapunov exponent to the initial conditions contributes to increase the period of the system. Figure 1 shows the behavior of the Lyapunov exponent in the case of $n = 4$ for the above three parameter settings. In the first case (setting 1), there are

Table 3 Matrix of the individual largest Lyapunov exponent of different initial conditions of the PWLCM for $n = 2$, $\alpha = \beta = 1$, $M = N = 2$, $c_1 = c_2 = 0$, $d_1 = d_2 = 0$, $a_1 = 0$, $a_2 = 1$, $b_1 = b_2 = 0$; $\lambda_0(3, 3) = 2.3895$

$x_0 \backslash y_0$	0	1	2	3
0	2.3895	2.3895	2.3895	2.3895
1	2.3895	2.3895	2.3895	2.3895
2	2.3895	2.3895	2.3895	2.3895
3	2.3895	2.3895	2.3895	2.3895

Table 4 Matrix of the individual largest Lyapunov exponent of different initial conditions of the PWLCM for $n = 2, \alpha = \beta = 1$, $M = N = 2, c_1 = 0, c_2 = 3$, $d_1 = d_2 = 0, a_1 = 0, a_2 = 1$, $b_1 = b_2 = 0$; $\lambda_0(3, 3) = 2.3895$

$x_0 \backslash y_0$	0	1	2	3
0	2.3895	2.3895	0.0006	2.3895
1	1.8542	1.8542	1.8543	2.3895
2	1.8542	1.8542	1.8543	1.8542
3	2.3895	1.8542	1.8543	1.8542

187 distinct values of λ, five distinct period values ($T = \{1, 4, 5, 8, 233\}$), and the corresponding period of the PWLCM is $T_1 = 9320$; in the second case, a single value of λ and four distinct period values ($T = \{1, 3, 6, 12\}$) are obtained, thus leading to $T_2 = 12$; while in the third case (setting 3), there are 63 distinct values of λ and 9 distinct periods ($T = \{1, 2, 4, 8, 10, 12, 14, 18, 40\}$), which corresponds to $T_3 = 2520$. We can observe that in the case of a single Lyapunov exponent, the largest period value is a multiple of the other values, which contributes to reduce the period of the whole system.

Such an observation also implies a high sensitivity of the period to the precision n. Indeed, for a parameter setting with a high sensitivity of the Lyapunov exponent to the initial conditions, the diversity of the Lyapunov exponent values increases with n, as the number of initial conditions itself increases. While setting $n = 5$ for the above parameter settings, the periods become respectively $T_1 = 1.51 \cdot 10^{15}$, $T_2 = 24$ and $T_3 = 1.02 \cdot 10^{10}$. As shown in Fig. 2, the values of the largest Lyapunov exponent are within the same range (1.4, 2.5), but the number of distinct values has significantly increased, 450 for the first parameter setting

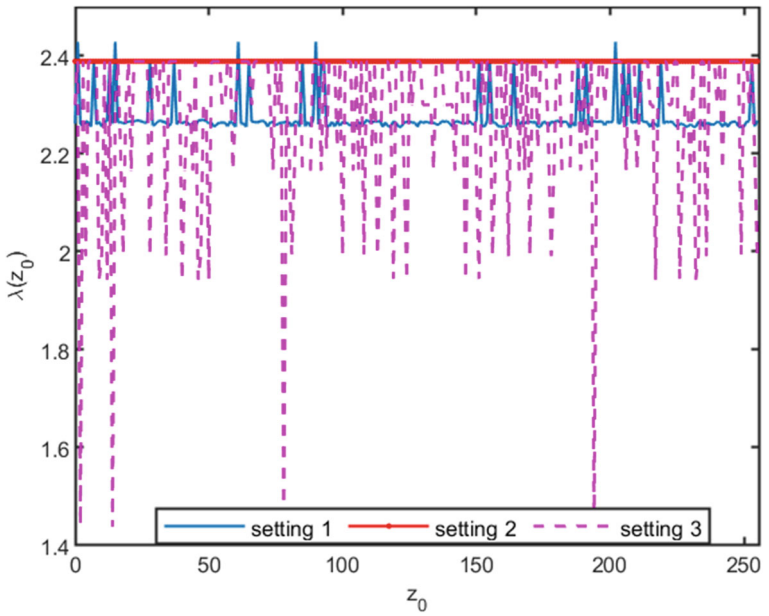

Fig. 1 Behavior of the Lyapunov exponent $\lambda(z_0)$ with respect to the initial condition $z_0 = 2^n x_0 + y_0$, for $n = 4$ and a_i, b_i, c_i and d_i set as in Table 2 (setting 1), Table 3 (setting 2) and Table 4 (setting 3). The corresponding periods are respectively $T_1 = 9320$, $T_2 = 12$ and $T_3 = 2520$.The Lyapunov exponents were evaluated after 1000 iterations of the PWLCM

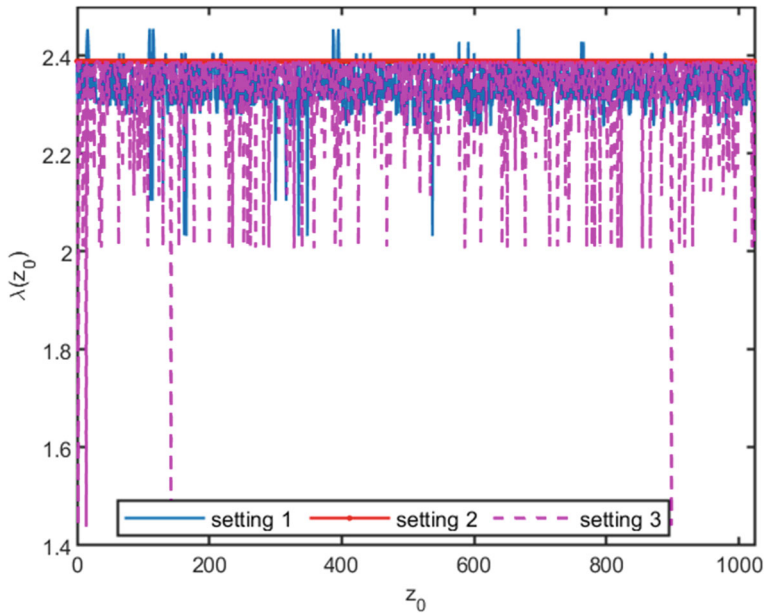

Fig. 2 Behavior of the Lyapunov exponent $\lambda(z_0)$ with respect to the initial condition $z_0 = 2^n x_0 + y_0$, for $n = 5$ and a_i, b_i, c_i and d_i set as in Table 2 (setting 1), Table 3 (setting 2) and Table 4 (setting 3). The corresponding periods are respectively $T_1 = 1.51 \cdot 10^{15}$, $T_2 = 24$ and $T_3 = 1.02 \cdot 10^{10}$. The Lyapunov exponents were evaluated after 1000 iterations of the PWLCM

(setting 1), and 163 for the third one (setting 3). There is no change for the second parameter setting as the corresponding Jacobian matrix does not depend on the initial conditions.

3.2 Sensitivity to control parameters a_i and b_i

For the analysis of the impact of a_i and b_i, we first set $M = N = 1$ and $n = 3$, $\alpha = \beta = 1$, $c_1 = 3$, $d_1 = 5$. The corresponding periods are summarized in Table 5 from where we can appreciate the sensitivity of the system to the parameters a_i and b_j. These periods are to be compared to $\Pi_A = 6$ that is the period of the equivalent QACM.

3.3 Sensitivity on control parameters c_i and d_i

Table 6 shows the dependence of the PWLCM period on the perturbation parameters c_1 and d_1, for $n = 2$, $M = N = 1$, $\alpha = \beta = 1$, $a_1 = 1$ and $b_1 = 3$. It appears from this table that the maximum period is obtained for $(c_1, d_1) = (1, 6)$. This table shows that large periods can be achieved even with a small number of bits ($n = 2$ for example), which is not possible

Table 5 Dependence of the PWLCM period Π_{PWLCM} on a_i and b_i for $n = 3$, $M = N = 1$, $\alpha = \beta = 1$, $c_1 = 3$, $d_1 = 5$ and different values of (a_1, b_1)

$a_1 \backslash b_1$	0	1	2	3	4
0	504	108	60	252	48
1	62	456	72	120	462
2	350	429	252	13566	12558

Table 6 Dependence of the PWLCM Π_{PWLCM} period on c_i and d_i for $n = 2$, $\alpha' = \beta' = 2$, $a_1 = 1$, $b_1 = 3$ and different values of (c_1, d_1)

$c_1 \backslash d_1$	0	1	2	3	4	5	6
0	2	4	4	16	2	6	4
1	4	3	12	70	4	105	12
2	4	12	6	16	4	14	8
3	6	28	14	8	6	36	14
4	2	4	4	16	2	6	4

with the conventional QACM. Indeed, the period depends on the choice of the parameters a_i, b_i, c_i and d_i.

The proposed PWLCM is conservative and depending on the parameter setting, it can be linear or nonlinear. As it includes all the properties of the QACM, it can be seen as a generalized form of the QACM that can exhibit large periods. The worst parameter setting of the PWLCM corresponds to a QACM. For the PWLCM to generate dynamics with large periods, its Jacobian matrix should depend on the initial conditions. We suggest a particular parameter setting depending on the parity of n that generates large periods such that:

$$c_i(\text{resp.}d_i) = \begin{cases} n+2, & \text{if } n = 2p+1; \\ 2^{n+1} - (n+1), & \text{if } n = 2p. \end{cases}, \; p \in \mathbb{N}_{\geq 1}, \tag{22}$$

and

$$a_i(\text{resp.}b_i) = \begin{cases} p, & \text{if } n = 2p+1; \\ 2^{n+1} - (2^n + 1), & \text{if } n = 2p. \end{cases}, \; p \in \mathbb{N}_{\geq 1}. \tag{23}$$

We verified that the case $c_i = 0$ or $d_i = 0$ corresponds to the forced QACM in which the steady state (0,0) is modified and depends on a_i and b_i and the case $c_i = 1$ or $d_i = 1$ corresponds to the conventional QACM. The period of the system is large when only one dimension is perturbed with $d_i = 1$ and c_i as in (22), or $c_i = 1$ and d_i as in (22). In such a case, the Lyapunov exponent of the PWLCM is sensitive to the initial condition as it is the case for many chaotic systems. It can therefore generate rich and complex dynamics. An example periodic image shuffling using both 8-bit QACM and 8-bit PWLCM is shown in Fig. 3. The period of the QACM in that case is 192, while that of the PWLCM, with $a_1 = 0$, $a_2 = 0$, $c_1 = 0$, $c_2 = 11$ and $d_1 = d_2 = 1$, is 4.28×10^{114}. Applying the reverse system to the shuffled image with the same number of iterations allows to obtain the original image without needs of running the shuffling process on the whole period of the system.

In order to compare the mixing property of the PWLCM and QACM, we applied the NIST800-22 statistical test to a periodic $2^{13} \times 2^{13}$ image shuffled with both systems. The periodic image is obtained by repeating sequences of 8-bit encoded integers ranged from 0 to 255. Such a data set can be divided into 50 bitstreams of 10^6 length each. The NIST test was applied to the shuffled images, after 50 iterations. The PWLCM parameters were set as $a_1 = 0$, $a_2 = 0$, $c_1 = 0$, $c_2 = 11$ and $d_1 = d_2 = 1$, and the number of bits was $n = 13$ for both systems. The corresponding results are shown in Table 7, from where it appears that the PWLCM shuffled image is passing NIST test, whereas the QACM image is failing. The PWLCM thus better mixes the pixels of the image than the QACM, hence is suitable for image shuffling.

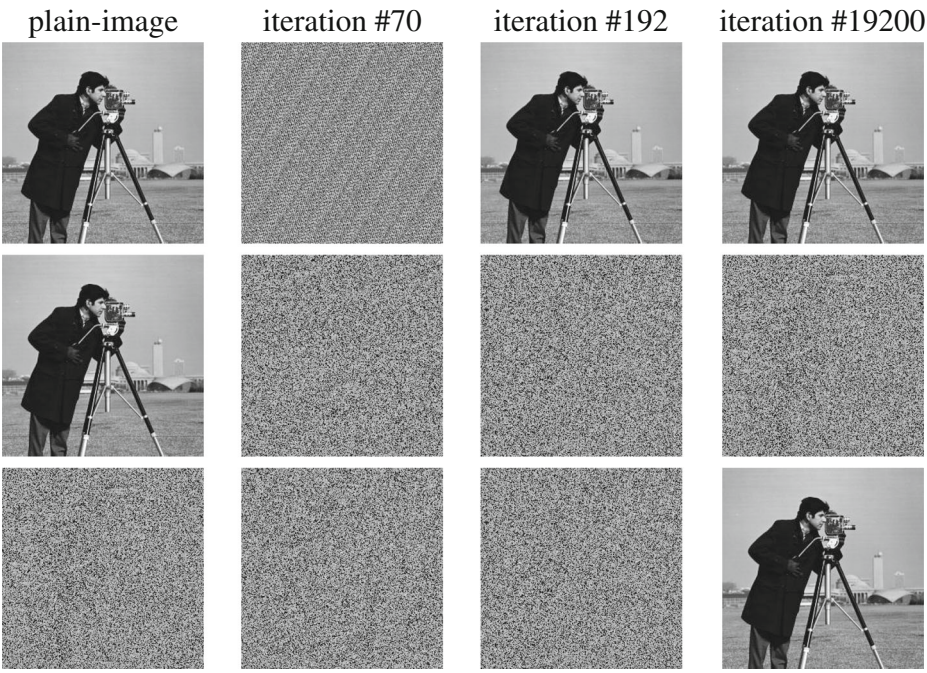

Fig. 3 Image shuffling using the QACM and PWLCM Transformation. The first line shows the results of the QACM, the second line depicts the PWLCM results, while the third line shows the reverse image obtained from the reverse PWLCM

Table 7 NIST 800-22 test results:

Sub-Tests	QACM		PWLCM	
	P-value	Proportion	P-value	Proportion
Frequency	0.0	7/50	0.3505	50/50
Block frequency	0.0	0/50	0.6993	49/50
Cumulative sums (forward)	0.0	0/50	0.3191	50/50
Cumulative sums (reverse)	0.0	0/50	0.1538	50/50
Runs	0.0	5/50	0.6163	49/50
Longest run	0.0	0/50	0.5749	49/50
Rank	0.0	0/50	0.1223	49/50
FFT	0.0	0/50	0.1719	48/50
Non overlapping	0.0	0/50	0.9114	50/50
Overlapping	0.0	0/50	0.6579	49/50
Universal	0.0	0/50	0.3191	50/50
Approximate entropy	0.0	0/50	0.4190	49/50
Random excursions	0.0	0/36	0.3505	36/36
Random excursions variant	0.0	0/36	0.8044	36/36
Serial	0.0	0/50	0.6163	50/50
Linear complexity	0.0	0/50	0.5749	50/50

4 Hardware implementation

In this section, we propose 2-dimensional (2D) electronic implementations of the conventional QACM and the proposed PWLCM. The implementation circuit includes exclusively basic electronic logic circuits such as adders, multiplexers, D-type flip-flops, and basic logic gates (AND, NOR, NAND, NOT, ...). We propose a hardware architecture which is simulated on both Multisim and Vivado HLx, and implemented on a Zynq 7020 FPGA board to confirm the effectiveness of the proposed architecture. The Multisim synthesis allows to optimize the FPGA architecture.

4.1 Multisim architecture

We first designed the circuit corresponding to the conventional 2-dimensional (2D) QACM with $\alpha = \beta = 1$. For such a circuit, we considered two stages, the one computing $x(t+1)$ and the one computing $y(t+1)$. Given that $y(t+1)$ depends on $x(t+1)$, we considered a delay time of half the clock period to sequentially determine $x(t+1)$, then $y(t+1)$. The corresponding electronic architecture is shown in Fig. 4.

Components U1 and U4 are multiplexers (74157N) that are used to set initial conditions x_0 and y_0, respectively. The SET input allows to load initial conditions when $SET = 1$. Once initial conditions have been set, the circuit starts oscillating ($SET = 0$), that is computing $x(t+1)$ on the leading edge of the clock pulse and $y(t+1)$ on the trailing edge of the clock signal. U3 and U6 are D-type flip-flops (74ALS273) that allow the circuit to sequentially change the output value as a clock pulse occurs (time increment). U2 and U5 are 4-bit adders (74283N) that are used to implement (1).

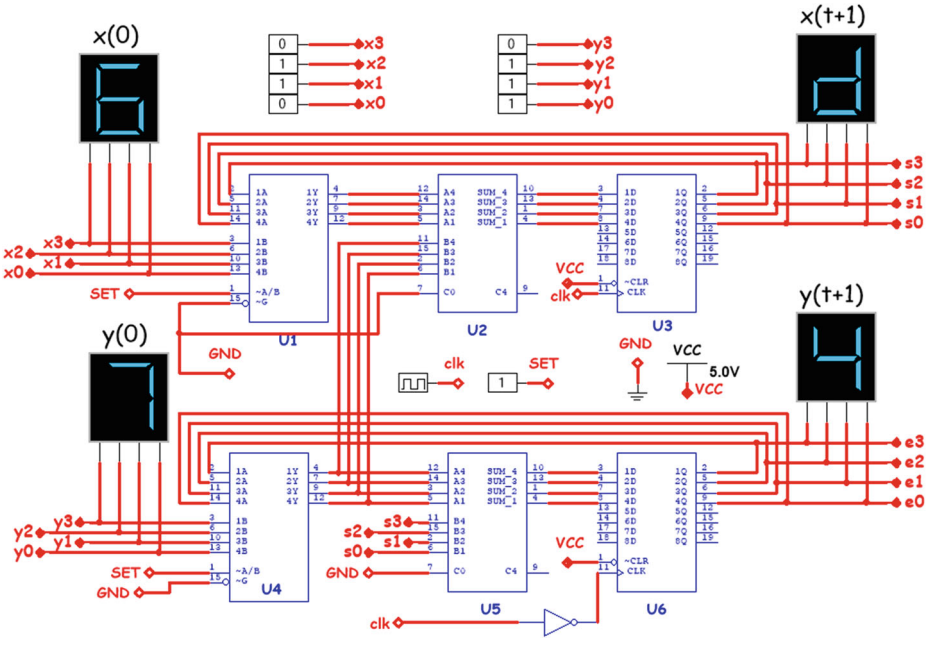

Fig. 4 Circuit of the conventional 2D QACM for $\alpha = \beta = 1$, $n = 4$. Values are displayed in hexadecimal representation

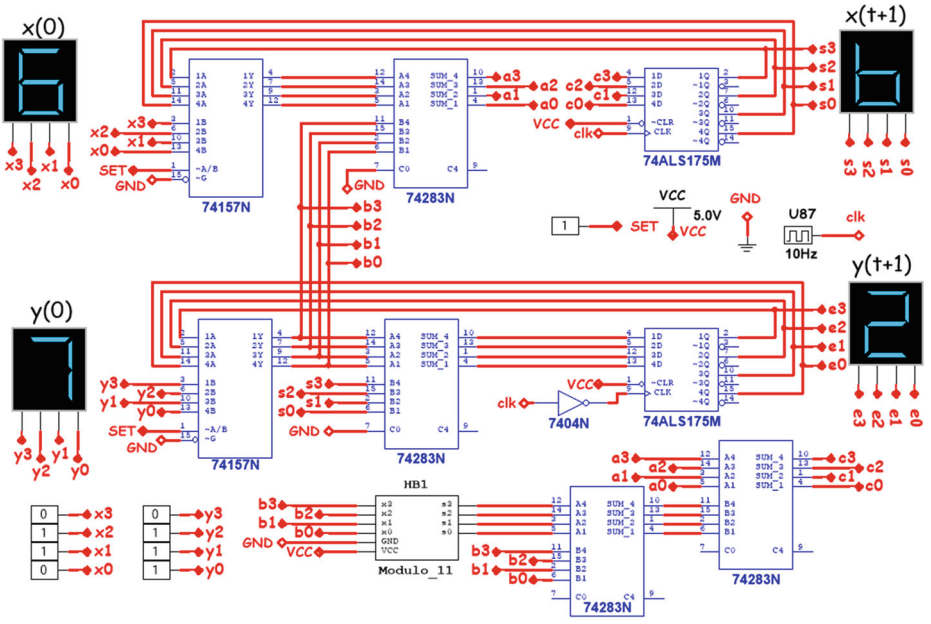

Fig. 5 Electronic implementation of 4-bit PWLCM with $\alpha' = 3$, $\beta' = 1$, $c_1 = 0$, $c_2 = 11$ and, $a_1 = a_2 = 0$. Values are displayed in hexadecimal representation

Now considering the perturbation term, we propose the schematic of the PWLCM whose equation is

$$\begin{cases} x(t+1) = x(t) + y(t) + \Big(a_1 + y(t)\Big) \mod c_1 + \Big(a_2 + y(t)\Big) \mod c_2 \\ y(t+1) = x(t+1) + y(t) \end{cases} \mod 2^n. \tag{24}$$

The circuit in Fig. 5 implements such a system for $\alpha' = 3$, $\beta' = 1$, $c_1 = 0$, $c_2 = 11$, $a_1 = a_2 = 0$ and, $n = 4$. The circuit implementing modulo 11 is shown in Fig. 6. The

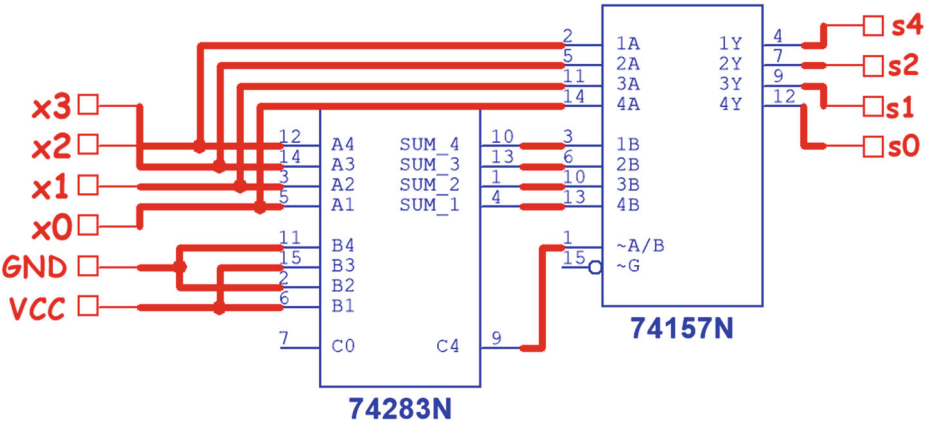

Fig. 6 Electronic implementation of modulo 11 (Modulo_11 module), 4-bit precision

Table 8 Dependence of the period Π on the precision n

n	Π_{QACM}	Π_{PWLCM}
2	3	6
3	6	6
4	12	4.81×10^{12}
5	24	1.06×10^{15}
6	48	1.03×10^{37}
7	96	5.49×10^{53}
8	192	4.28×10^{114}
9	384	1.96×10^{260}
10	768	1.09×10^{513}

period of the above PWLCM is $T = 4.8135 \times 10^{12}$, while that of the corresponding QACM is only $T = 12$. The period gain for this example is therefore $\gamma = 4^{11}$. We simulated this circuit using MULTISIM software as well as PROTEUS/ISIS software and verified that the dynamics of the electronic system perfectly matches with the MATLAB simulation. Based on the low complexity of the electronic circuit and the period gain brought by the insertion of the nonlinear term into the QACM, we concluded that the proposed system can be efficiently included in a pseudo-random number generator.

We analyzed its period for $2 \leq n \leq 10$ and compared it with that of the corresponding QACM. The overall results obtained are summarized in Table 8, from where we can confirm the efficiency of the nonlinear element for increasing the QACM period, thus giving an exponential growth of the period with respect to the precision n. Cases $n = 2$ and $n = 3$ correspond to the QACM with $\alpha = 3$ and $\beta = 1$, as $c_2 > 2^n$, while the periods of the cases $4 \leq n \leq 10$ are evaluated using the Maple software to avoid calculation errors in Matlab. An example of distribution of the orbit periods $T(x_0, y_0)$ with respect to the initial condition (x_0, y_0) for the case $n = 8$ is shown in Fig. 7. One can observe that there are some initial

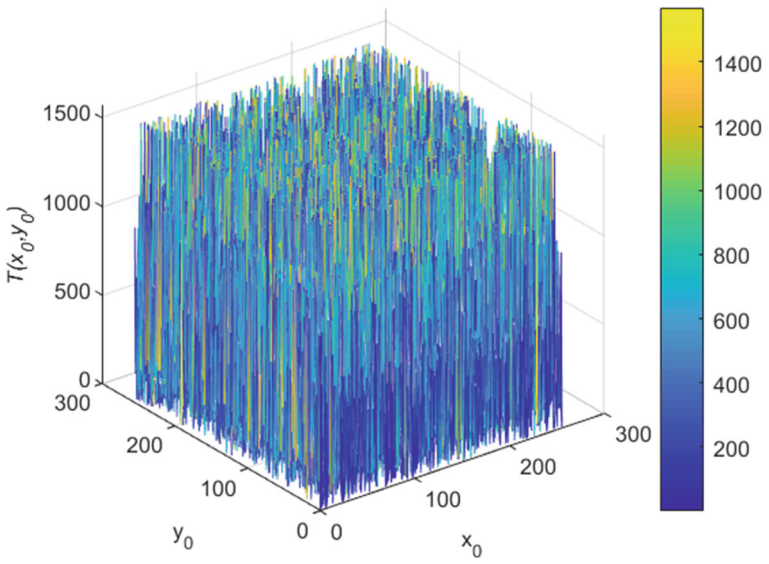

Fig. 7 Distribution of the PWLCM orbit period $T(x_0, y_0)$ with respect to the initial condition (x_0, y_0), case of $n = 8$. The other parameters are set as $\alpha' = 3$, $\beta' = 1$, $c_1 = 0$, $c_2 = 11$ and $a_1 = a_2 = 0$

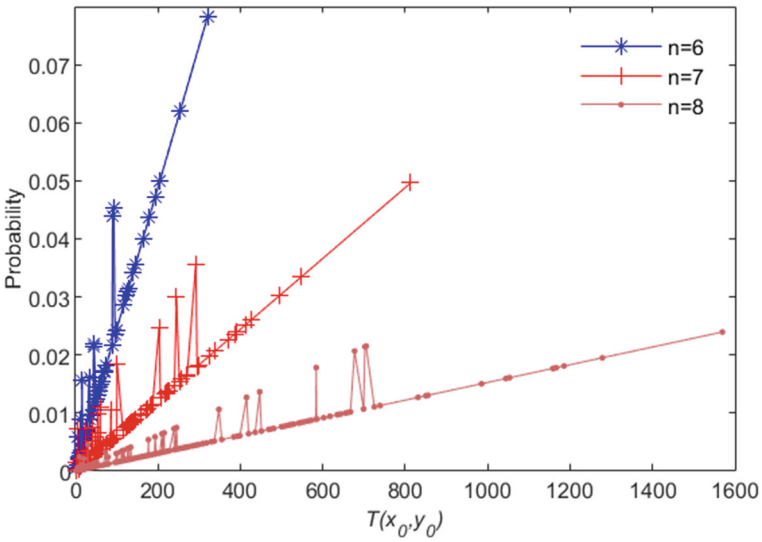

Fig. 8 Probability distribution of $T(x_0, y_0)$ of the PWLCM for $n = 6$, $n = 7$ and, $n = 8$; with $\alpha' = 3$, $\beta' = 1$, $c_1 = 0$, $c_2 = 11$ and $a_1 = a_2 = 0$

conditions for which the period is greater than the upper limit of the orbit periods of the QACM, that is $\pi = 2^n$. Figure 8 shows the probability distribution of $T(x_0, y_0)$ for $n = 6$, 7 and 8. It appears from this figure that the frequency or probability increases with the period: the highest probability corresponds to the largest period $T(x_0, y_0)$. Such a result is interesting as our goal is to obtain large periods for all the nontrivial points of the PWLCM.

4.2 FPGA implementation

In order to confirm the effectiveness of the above architecture simulated with the Multisim software, we used Vivado and implemented the system on Zynq 7020 FPGA board. The schematic of the implemented system is shown in Fig. 9, with $\alpha' = 3$, $\beta' = 1$, $c_1 = 0$,

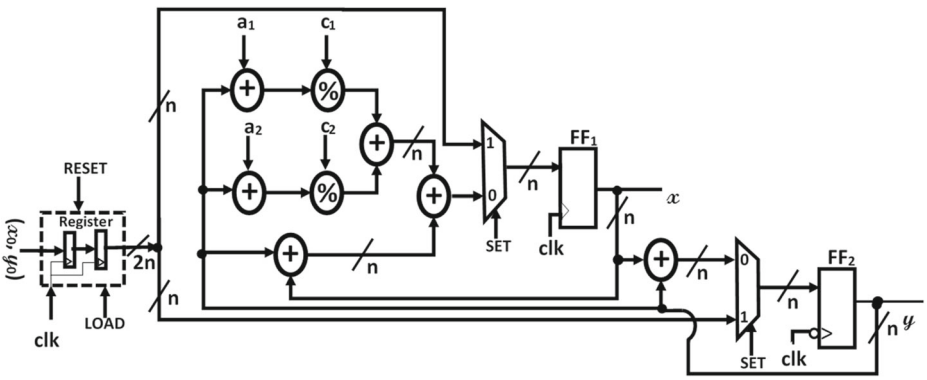

Fig. 9 Generalized FPGA implementation of n-bit PWLCM. The "LOAD" command allows to set x_0 and y_0 as initial conditions in the $2n$-bit register; "RESET" allows to clear the $2n$-bit register; and the "SET" command allows to load the initial conditions to n-bit registers FF_1 and FF_2, therefore to start the system

Table 9 Hardware resource utilization of the 4-bit PWLCM architecture

	Vivado HLx
Data format	Unsigned integer
Technology	Zynq 7020
LUT	16
FF	12
Fmax (MHz)	134
Throughput(Gbps)	1.072

$c_2 = 11$, $a_1 = a_2 = 0$ and, $n = 4$. The resource utilisation as well as the throughput of the proposed architecture are given in Table 9. From this table we observe that the implementation of the PWLCM does not require any DSP module, but exclusively basic modules such as look-up tables (LUT) and flip-flops (FF). We verified that the outputs of the FPGA and Multisim architectures perfectly match, thus confirming the effectiveness of the proposed architectures of the QACM and the PWLCM. For 4-bit precision, the FPGA implementation performs 1.072 Gbps throughput at 134 MHz maximum frequency. Such a high throughput shows that the proposed system can be easily combined with other basic gates such XOR gates or linear feedback shift registers (LSFR) for a real-time generation of pseudo-random numbers.

5 Conclusion

We presented in this paper the PWLCM obtained from a QACM that is nonlinearly perturbed. Depending on the parameter setting, the PWLCM exhibits large periods as compared to the equivalent QACM. The increase of the period enhance the complexity of the PWLCM, thereby is more suitable for image shuffling than the QACM. We evaluated the dependence of the period of the proposed system on the control parameters involved by the perturbing nonlinear term and observed that the worst parameter setting corresponds to a QACM. The PWLCM thus appears to be a generalized form of the QACM in which the sensitivity to the initial conditions has been improved for generating rich and complex dynamics. We showed that the Lyapunov exponent of the PWLCM is sensitive to the initial condition as it is the case for many chaotic systems, which justifies the large periods obtained. We noticed that the period of the PWLCM does not depend on the value of the largest Lyapunov exponent, but on its variability: a large Lyapunov exponent does not imply a large period, but a constant Lyapunov exponent implies a weak period. We also proposed an electronic implementation of both the QACM and the PWLCM. The two circuits are nearly identical, whatever confirms that introducing the perturbation term does not significantly modify the complexity of the QACM, despite the high period gain obtained. The effectiveness of the proposed architecture was confirmed by implementing the system on a Zynq 7020 FPGA board. Both the resource utilisation and the throughput of 1.072 Gbps at a maximum frequency of 134 MHz attest that the PWLCM can be easily combined with other basic gates to design a complete PRNG. The analysis of the model electronically implemented shows that the period exponentially increases with the precision n. In prospect, we intend to apply the PWLCM to data encryption in order to take advantage of its large periods, and to investigate its dynamics in the continuous phase space.

Acknowledgements This work was supported by the Alexander von Humboldt Foundation under Ref 3.4-CMR/1133622.

We thank all the reviewers for their valuable comments that allowed us to improve the content of this paper.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Arnold V, Avez A (1968) Ergodic problems of classical mechanics. New York:Benjamin
2. Bakiri M, Guyeux C, Couchot J-F, Marangio L, Galatolo S (2018) A hardware and secure pseudo-random generator for constrained devices. IEEE Trans Industr Inform IEEE T Ind Inform 14:3754–3765
3. Bakiri M, Couchot J-F, Guyeux C (2018) CIPRNG: A VLSI family of chaotic iterations post-processings for $\mathbb{F}_2$ -linear pseudorandom number generation based on zynq mpsoc. IEEE Trans Circuits Syst I Regul Pap 65:1628–1641
4. Bao J, Yang Q (2012) Period of the discrete Arnold cat map and general cat map. Nonlinear Dyn 70:1365–1375
5. Bonilla LL, Alvaro M, Carretero M (2016) Chaos-based true random number generators. M J Math Industry 7:1–17
6. Chen C, Ma H, aand HC, Meng Y, Ding Q (2015) FPGA Implementation of a UPT chaotic signal generator for image encryption. Pacific Science Review A: Natural Science and Engineering 17:97–102
7. Chen G, Mao Y, Chui C (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 21:749–761
8. Chen F, Wong K-W, Liao X, Xiang T (2012) Period distribution of generalized discrete Arnold cat map for $n = p^e$. IEEE Trans Inf Theory 58:445–452
9. Chen F, Wong K-W, Liao X, Xiang T (2013) Period distribution of generalized discrete Arnold cat map for $n = 2^e$. IEEE Trans Information Theory 59:3249–3255
10. Chen F, Wong K-W, Liao X, Xiang T (2014) Period distribution of generalized discrete Arnold cat map. Theor Comput Sci 552:13–25
11. Dyson FF, Falk H (1992) Period of a discrete cat mapping. Am Math Mon 99:603–614
12. Eckmann J-P, Ruelle D (1985) Ergodic theory of chaos. Rev Mod Phys 57:617–656
13. Fouda JSAE, Sabat S, multiplierless hyperchaotic system using coupled Duffing oscillators A (2015) Commun nonlinear sci. Numer Simulat 20:24–31
14. Gu G, Ling J (2014) A fast image encryption method by using chaotic 3d cat maps. Optik 125:4700–4705
15. Hu J, Gao JB, Tung WW (2009) The analysis of observed chaotic data in physical systems. Chaos 19:028506
16. Kalanadhabhatta S, Kumar D, Anumandla KK, Reddy SA, Acharyya A (2020) Puf-based secure chaotic random number generator design methodology. IEEE Trans Very Large Scale Integr (VLSI) Syst 28:1740–1744
17. Keating JP, Mezzadri F (2000) Pseudo-symmetries of Anosov map and spectral statistics. Nonlinearity 13:747–775
18. Kocarev L, Sterjev M, Fekete A, Vattay G (2004) Public-key encryption with chaos, chaos: Interdisciplinary. J Nonlinear Sci 14:1078–1082
19. Kumar Panda A, Chandra Ray K (2020) A coupled variable input LCG method and its VLSI architecture for pseudorandom bit generation. IEEE Trans Instrum Meas 69:1011–1019
20. Li C, Lin D, Feng B, Hao F (2018) Cryptanalysis of a chaotic image encryption algorithm based on information entropy. IEEE Access 6:75834–75842

21. Li W, Reidler I, Aviad Y, Huang Y, Song H, Zhang Y, Rosenbluth M, Kanter I (2013) Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices. Phys Rev Lett 111:044102
22. Li C, Tan K, Feng B, Lu J (2017) The graph structure of the generalized discrete Arnold's cat map, arXiv:1712.07905, pp 1–15
23. Lou D, Sung C (2004) A steganographic scheme for secure communications based on the chaos and euler theorem. IEEE Trans Multimedia 6:501–509
24. Merah L, Lorenz P, Adda A-P (2021) A new and efficient scheme for improving the digitized chaotic systems from dynamical degradation. IEEE Access 9:88997–89008
25. Öztürk I, Kiliç R (2015) A novel method for producing pseudorandom numbers from differential equation-based chaotic systems. Nonlinear Dyn 80:1147–1157
26. Öztürk I, Kiliç R (2021) Utilizing true periodic orbits in chaos-based cryptography. Nonlinear Dyn 103:2805–2818
27. Rameshbabu R, Karthikeyan R, Balamurali R, Prasina A (2015) FPGA Implementation of adaptive complete synchronization methodology for novel chaotic systems, Middle-East. J Sci Res 23:36–44
28. Rezk AA, Madian AH, Radwan AG, Soliman AM (2020) Multiplierless chaotic pseudo random number generators. AEU-International Journal of Electronics and Communications 113:152947
29. Shah DK, Chaurasiya RB, Vyawahare VA, Pichhode K, Patil MD (2017) FPGA Implementation of fractional-order chaotic systems. Int J Electron Commun (AEU) 78:245–257
30. Souza CEC, Shavez DPB, Pimentel C (2018) One-dimensional nonlinear model for producing chaos. IEEE Transactions on Circuits and Systems I: Regular Papers 65:235–246
31. Wang D, Xu W, Xu J, Gu X, yang G (2019) Resonance responses in a two-degree-of-freedom viscoelastic oscillator under randomly disordered periodic excitations. Commun Nonlinear Sci Numer Simulat 68:302–318
32. Wang Y, Liu Z, Zhang LY, Pareschi F, Setti G, Chen G (2021) From chaos to pseudorandomness: A case study on the 2-d coupled map lattice. IEEE Trans Cybern, pp 1–11
33. Zhua H, Zhao C, Zhang X, Yang L (2014) An image encryption scheme using generalized Arnold map and affine cipher. Optik 125:6672–6677