Study on a new chaotic bitwise dynamical system and its FPGA implementation*

Wang Qian-Xue(王倩雪)[a)†], Yu Si-Min(禹思敏)[a)], C. Guyeux[b)], J. Bahi[b)], and Fang Xiao-Le(方晓乐)[c)]

[a)] College of Automation, Guangdong University of Technology, Guangzhou 510006, China

[b)] Femto-st Institute, University of Franche-Comte, Besancon 25000, France

[c)] Land and Resources Technology Center of Guangdong Province, Guangzhou 510075, China

(Received 2 December 2014; revised manuscript received 9 January 2015; published online 10 April 2015)

In this paper, the structure of a new chaotic bitwise dynamical system (CBDS) is described. Compared to our previous research work, it uses various random bitwise operations instead of only one. The chaotic behavior of CBDS is mathematically proven according to the Devaney's definition, and its statistical properties are verified both for uniformity and by a comprehensive, reputed and stringent battery of tests called TestU01. Furthermore, a systematic methodology developing the parallel computations is proposed for FPGA platform-based realization of this CBDS. Experiments finally validate the proposed systematic methodology.

Keywords: chaos, chaotic bitwise dynamical systems, FPGA implementation

PACS: 05.45.–a **DOI:** 10.1088/1674-1056/24/6/060503

1. Introduction

Current rapid developments of digital technologies and the Internet have led to tremendous convenience in people's work and life. At the same time, new issues appeared such as copyright infringement and information tampering, so that data confidentiality, integrity, and authentication are now difficult to guarantee. Therefore, the need to find new tools to reinforce trust and security through the Internet has become a major concern. Chaotic systems are often proposed to achieve security, due to their properties of sensitivity to initial conditions, topological transitivity, decaying autocorrelation function, and so on.[1,2] Hence the chaotic system has recently emerged as a new research direction to reinforce information security of data sent through the Internet.[3–6]

It is obvious that to consider chaos for information security requires a particularly good statistical profile for the associated system used to achieve security.[7,8] However, until now, almost all studies of chaotic systems applied to information security consider the real domain.[9–11] As all operations in each iteration manipulate real numbers, any Real Domain Chaotic System (RDCS) designed in a computer or a digital device will inevitably lead to dramatic finite precision effects.[12] Furthermore, continuous-time chaotic systems have to be converted to chaotic sequences, leading to rounding errors.[13] Thus each iteration of the discrete dynamical system will bring a tiny error, due to the sensitivity to initial conditions and the approximations resulting from the real numbers to finite precision binary digits conversion. The chaotic system finally experiences a long-term evolution with cumulative effects of these small errors, which often leads to dynamics degradation such as decayed distribution, low linear complexity, short cycle length, and so on.[5] This degradation directly affects the statistical properties of chaotic systems.[14,15] The fundamental reason is that chaotic systems are strongly dependent on their initial conditions: small errors at the beginning of iterations will result in large differences between actual and theoretical chaotic orbits. Finally, test results show that most of the RDCSs cannot meet the statistical requirements of TestU01,[16] which is widely considered as the most comprehensive and stringent battery of tests.

To put it in a nutshell, finite precision affects the dynamics of RDCS. Although many experimental methods have been proposed to solve this problem, their performances cannot be accurately controlled. As these finite precision effects are inevitable, new ways to prevent dynamics degradation of chaotic systems must be investigated, and one of them is the Integer Domain Chaotic System (IDCS).

In 2010, a research team at the University of Franche-Comté, France, proposed a new IDCS designated as CI (Chaotic Iterations) system.[17] This CI system receives one or two random stream(s) as input, and it mixes them with chaotic iterations. This mixture uses only bitwise operations, thus achieving the speed requirement. Furthermore, theoretical analyses show that, these CI systems on integer domains satisfy various mathematical definitions of chaos like the Devaney's one. Since these systems run on finite sets of integer

*Project supported by China Postdoctoral Science Foundation (Grant No. 2014M552175), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, Chinese Education Ministry, the National Natural Science Foundation of China (Grant No. 61172023), and the Specialized Research Foundation of Doctoral Subjects of Chinese Education Ministry (Grant No. 20114420110003).

†Corresponding author. E-mail: wangqianxue@gdut.edu.cn

© 2015 Chinese Physical Society and IOP Publishing Ltd

domains, then the finite precision problem is settled, and the transformation from real numbers to binary sequences is not necessary any more. The CI system is one of the effective solutions for the aforementioned issue that occurs in the RDCS case.

The first collaborative work between French and Chinese teams has consisted in chaotically combining two random inputs in order to construct a first CI system, called PRIM CI in Ref. [18], which has led to better statistical properties for the resultant pseudorandom number generator than each input taken alone. Then MARK CI has been introduced in Ref. [19]: a mark sequence has been applied to avoid wasteful duplication of values, and has resulted in an obvious speed improvement. The LUT (Lookup-Table) CI has then been released and studied in depth in Ref. [20]: this last version of the chaotic combination of two input entropic streams has solved flaws exhibited by the MARK CI version of these IDCSs. The second collaborative work has focused on the design and implementation of IDCS by using only one random source. First chaos generation strategy has finally been realized in Ref. [21], through a sample-hold circuit and a decoder circuit so as to convert the uniform noise signal into a random sequence.

In this paper, a new chaotic bitwise dynamical system (CBDS) is proposed, whose dynamics of chaos are still preserved in digital computers. Its obvious speed improvement makes it a good candidate when developing new approaches in some fields regarding information security like digital watermarking, because it uses multiple random bitwise operations instead of only one like in Ref. [21]. Then, its proof of chaos according to the Devaney's definition is presented in this paper. After having introduced the theoretical framework of this study, we will give a comparison based on the uniformity of the sequence and on statistical tests. We will then focus on the Field Programmable Gate Array (FPGA) implementation of this CBDS, with the presentation of both theoretical background and practical details. Some specific components like ring oscillator,[22] D flip–flop, iterate function circuit, DAC (digital to analog converter) have been applied to design the FPGA. The main feature of this kind of CBDS circuit is that it takes advantage of parallel computations in FPGA.

The remainder of this research work is organized as follows. The improved version of CBDS is given in Section 2, while its proof of chaos is provided in Section 3. The uniformity and statistical property of this novel version will be evaluated in Sections 4 and 5. FPGA implementation of CBDS are detailed in the next section. This article ends with a conclusion section in which the contributions are summarized (Section 7).

2. Improvements of CBDS

In this section, we first introduce the basic concept of RDCSs and IDCSs.

Let $N \in 1,2,...$ be a positive integer, $B = \{0,1\}$ denotes the set of Boolean numbers with its usual algebraic structure, while B^N is the set of binary vectors of size N.

Definition 1 Let $f : \mathbb{R} \to \mathbb{R}$ be a function, and x^n and x^{n-1} be two real numbers, which are represented as infinite numbers of bits in their binary decomposition:

$$\begin{cases} x^{n-1} = (x_{i_1}x_{i_2}\ldots x_{i_M}.x_{j_1}x_{j_2}\ldots x_{j_N}\ldots)_2, \\ x^n = (x_{k_1}x_{k_2}\ldots x_{k_L}.x_{l_1}x_{l_2}\ldots x_{l_P}\ldots)_2, \end{cases} \tag{1}$$

where each element is a Boolean, while $x_{i_1}x_{i_2}\ldots x_{i_M}$ and $x_{j_1}x_{j_2}\ldots x_{j_N}$ are respectively the integral and fractional parts for x_{n-1}. Similarly, $x_{k_1}x_{k_2}\ldots x_{k_L}$ and $x_{l_1}x_{l_2}\ldots x_{l_P}$ are respectively the integral and fractional parts for x_n. The so-called iterative equation in RDCSs is defined by

$$\begin{aligned} &x^{n-1} = (x_{i_1}x_{i_2}\ldots x_{i_M}.x_{j_1}x_{j_2}\ldots x_{j_N}\ldots)_2 \to x^n = f(x^{n-1}) = \\ &(f(x^{n-1})_{i_1}f(x^{n-1})_{i_2}\ldots f(x^{n-1})_{i_M}\cdot f(x^{n-1})_{j_1}f(x^{n-1})_{j_2}\ldots \\ &f(x^{n-1})_{j_N}\ldots)_2, \end{aligned} \tag{2}$$

where $f(x^{n-1})_i$ and $f(x^{n-1})_j$ are the i-th and j-th components of $f(x^{n-1})$ for the integral and fractional parts respectively. In other words, at each iteration, all the binary components of these real numbers are iterated.

Consider now a system with a finite number of N elements (or cells) $x = (x_{N-1}x_{N-2}\ldots x_0)$, so that each element has a Boolean state: $x_{N-1}, x_{N-2}, \ldots, x_0 \in B$. Having N Boolean values for these cells leads to the definition of a particular state of the system $x = (x_{N-1}, x_{N-2}, \ldots, x_0) \in B^N$. A one-sided infinite sequence of integers bounded by $N-1$ is called a strategy: $\forall n \in \mathbb{N}, s^n \in \{0,1,2,\ldots,N-1\}$.

Definition 2 (Ref. [21]) Let $f : B^N \to B^N$ be a function, $x^0 = (x^0_{N-1}, x^0_{N-2}, \ldots, x^0_0) \in B^N$ be the initial condition, while $x^{n-1} = (x^{n-1}_{N-1}, x^{n-1}_{N-2}, \ldots, x^{n-1}_0) \in B^N$ and $x^n = (x^n_{N-1}, x^n_{N-2}, \ldots, x^n_0) \in B^N$ denote the $(n-1)$-th and n-th iterations respectively. The so-called iterative equation in IDCSs is defined by

$$\begin{aligned} x^n_i &= \begin{cases} x^{n-1}_i, & \text{if } i \neq s^n, \\ (f(x^{n-1}))_i, & \text{if } i = s^n, \end{cases} \\ \to x^n &= (x^{n-1}_{N-1}, x^{n-1}_{N-2}, \ldots, x^{n-1}_{s^n+1}, f(x^{n-1})_{s^n}, x^{n-1}_{s^n-1}, \ldots, x^{n-1}_0), \end{aligned} \tag{3}$$

where $i = 0,1,2,\ldots,N-1$, $n = 1,2,\ldots$, and $f(x^{n-1})_{s^n}$ is the s^n-th component of $f(x^{n-1})$. In other words, at the n-th iteration, only the s^n-th element is iterated.

The major difference between CBDS and the basic IDCSs published in Ref. [21] is that w^n is a subset ($w^n \subset \{1,2,\ldots,N\}$) instead of a single integer ($s^n \in \{1,2,\ldots,N\}$).

Definition 3 In the so-called CBDS, the iterative equation is defined as follows:

$$\begin{aligned} x^n_i &= \begin{cases} x^{n-1}_i, & \text{if } i \notin w^n, \\ (f(x^{n-1}))_i, & \text{if } i \in w^n, \end{cases} \to \\ x^n &= (x^{n-1}_{N-1}, x^{n-1}_{N-2}, \ldots, x^{n-1}_{w^n_1+1}, f(x^{n-1})_{w^n_1}, x^{n-1}_{w^n_1-1}, \ldots, \end{aligned} \tag{4}$$

$$x^{n-1}_{w^n_2+1}, f(x^{n-1})_{w^n_2}, x^{n-1}_{w^n_2-1}, \ldots, f(x^{n-1})_{w^n_3}, \ldots, x^{n-1}_0),$$

where $i = 0,1,2,\ldots,N-1$, $n = 1,2,\ldots$, and $\forall n, w^n$ is a set, which can be represented by a one-sided infinite sequence of integers bounded by $N-1$ as $w = w^1, w^2, \ldots, w^n, \ldots = w^1_1, w^1_2, \ldots, w^1_{|w^1|}, w^2_1, w^2_2, \ldots, w^2_{|w^2|}, \ldots, w^n_1, w^n_2, \ldots, w^n_{|w^3|}, \ldots : \forall i \in \mathbb{N}$ and $j \in \{1,2,\ldots N\}$, $w^i_j \in \{0,1,2,\ldots,N-1\}$. Let us remark that $|\cdot|$ means the size of the set and w is also named a chaotic strategy. In other words, at the n-th iteration, only the elements whose id is contained into the set w^n are iterated.[23]

The subset w^n can be expressed as an integer p^n having N bits: the k-th digit in the binary decomposition of p^n is 1 if and only if k belongs to w^n (the other digits are set to 0). That is, the size of the set w^n is the number of 1's in the binary decomposition of p^n while the elements in the set w^n are the positions of these 1's. The state x^n of the system, for its part, is similarly represented as an integer y^n having N bits. Therefore, the iterative equation is as follows:

$$y^n = (y^{n-1} \wedge \neg p^n) \vee (f(y^{n-1}) \wedge p^n), \tag{5}$$

where $\wedge$ is the logical conjunction, $\vee$ is the disjunction, and $\neg$ is the negation. This formula means that the k-th component of state y^n (a binary digit) is updated by $(f(y^{n-1}))_k$ if and only if the k-th digit in the binary decomposition of p^n is 1. Remark that in our previous research works the iterate function f has often been the vectorial negation,[21] given by

$$f(y^{n-1}) = \neg y^{n-1}. \tag{6}$$

With such a choice, a more specific formula can be obtained

$$F_f(p,y) = (y \wedge \neg p) \vee (\neg y \wedge p) = y \oplus p. \tag{7}$$

Let $E = (p,y)$ be a couple constituted by a chaotic strategy and a binary digit, consider the phase space:

$$\varepsilon = (0,1,2,\ldots,N-1)^{\mathbb{N}} \times (0,1,2,\ldots,N-1) \tag{8}$$

and the map defined on ε with $E = (p,y) \in \varepsilon$:

$$G_f(E) = G_f((p,y)) = (\sigma(p), F_f(i(p),y)), \tag{9}$$

where $i(p) = p^1$ and $\sigma^k(p) = \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{k}(p), k = 1,2\ldots$ is the result of shifting k integers in the one-sided infinite sequence $p = (p^1 p^2 \ldots p^n \ldots)$ to the left:

$$\sigma^k(p) = p^{k+1} p^{k+2} \ldots p^n \ldots, \ (k = 1,2,\ldots). \tag{10}$$

Then the iterative equation proposed in Definition 3 can be rewritten as follows:

$$E^0 \in \varepsilon \text{ and } \forall k \in \mathbb{N}, \ E^{k+1} = G_f(E^k). \tag{11}$$

To study the Devaney's chaos property, a distance between two points (p,y) and $(\hat{p},\hat{y})$ of ε must be defined. Let us introduce

$$d((p,y),(\hat{p},\hat{y})) = d_p(p,\hat{p}) + d_y(y,\hat{y}), \tag{12}$$

where $p = p^1 p^2 p^3 \ldots p^n \ldots$ and $\hat{p} = \hat{p}^1 \hat{p}^2 \hat{p}^3 \ldots \hat{p}^n \ldots$ are one-sided infinite sequences of integers, while y and $\hat{y}$ are binary digits of N bits. More precisely, the distance between p and $\hat{p}$ is

$$d_p(p,\hat{p}) = \sum_{k=1}^{\infty} \frac{p^k \oplus \hat{p}^k}{2^{Nk}} \in [0,1], \tag{13}$$

where $p^k \oplus \hat{p}^k$ is for the symmetric difference. Finally, following the 1-norm distance, the distance between y and $\hat{y}$ is

$$d_y(y,\hat{y}) = H(y^k \oplus \hat{y}^k). \tag{14}$$

Remark that where $H(X)$ is the hamming weight of X and d is defined as the sum of two other distances. Before investigating the chaotic properties of CBDS, the following lemma is first introduced.

Lemma 1 Let the $p = p^1 p^2 p^3 \ldots p^n \ldots$ and the $\hat{p} = \hat{p}^1 \hat{p}^2 \hat{p}^3 \ldots \hat{p}^n \ldots$, where $p^k, \hat{p}^k \in \{0,1,2,\ldots,N-1\}$ for $k = 1,2,\ldots$. If $p^i = \hat{p}^i$ for $i = 1,2,\ldots,n$, then $d(p,\hat{p}) \leq 1/2^{Nn}$. Conversely, if $d(p,\hat{p}) \leq 1/2^{Nn}$, then $p^i = \hat{p}^i$ for $i = 1,2,\ldots,n$.

Proof If $p^i = \hat{p}^i$ for $i = 1,2,\ldots,n$, then

$$\begin{aligned} d(p,\hat{p}) &= \sum_{i=1}^{n} \frac{p^i \oplus \hat{p}^i}{2^{Ni}} + \sum_{i=n+1}^{\infty} \frac{p^i \oplus \hat{p}^i}{2^{Ni}} \\ &= \sum_{i=n+1}^{\infty} \frac{p^i \oplus \hat{p}^i}{2^{Ni}} \\ &\leq \sum_{i=n+1}^{\infty} \frac{2^N - 1}{2^{Ni}} \\ &= (2^N - 1) \times \frac{\frac{1}{2^{Nn+N}}}{1 - \frac{1}{2^N}} \\ &\leq \frac{1}{2^{Nn}}. \end{aligned} \tag{15}$$

Conversely, and due to the definition of the proposed distance: for any $m \leq n$, if $p^m \neq \hat{p}^m$, then $d(p,\hat{p}) \geq 1/2^{Nn}$. The contraposition is the desired result: if $d(p,\hat{p}) \leq 1/2^{Nn}$, then $p^1 = \hat{p}^1$.

3. Proof of chaos for CBDS

In this section, the chaotic behavior of CBDS is proven according to the Devaney's definition recalled below.

Definition 4 (Devaney's definition of chaos[24]) Let $f : \mathscr{X} \to \mathscr{X}$ be a continuous function on the metrical space $(\mathscr{X},d)$. The dynamical system $x^0 \in \mathscr{X}, x^{n+1} = f(x^n)$ is said to be chaotic if

D4-a its periodic points are dense in $\mathscr{X}$;

D4-b it is transitive: for any nonempty open sets U_A and U_B in $(\mathscr{X},d)$, there is always $k_0 > 0$ such that $G_f^{n_0}(U_A) \cap U_B \neq \varnothing$;

D4-c it has sensitive dependence on initial conditions.

The meaning of these properties are detailed thereafter.

Theorem 1 (Banks[25]) If a dynamical system is transitive and has dense periodic points, then it has sensitive dependence on initial conditions.

Thus, to prove that we are in the framework of Devaney's topological chaos, we have to check the regularity and transitivity conditions.

3.1. Dense periodic points

Theorem 2 The periodic points of G_f are dense in ε.

Proof Let $(\tilde{p},\tilde{y}) \in \varepsilon$, and $\varepsilon > 0$. We are looking for a periodic point $(\tilde{p},\tilde{y}) \in \varepsilon$ that satisfies $d((\tilde{p},\tilde{y}),(\hat{p},\hat{y})) < \varepsilon$,

P1 The general form of $(\hat{p},\hat{y})$ is

$$(\hat{p},\hat{y}) = ((\hat{p}^1\hat{p}^2\dots\hat{p}^{k_0}\dots\hat{p}^n\dots),\hat{y}) \in \varepsilon. \tag{16}$$

As ε can be strictly lesser than 1, we must choose $\tilde{y} = \hat{y}$, because if $\tilde{y} \neq \hat{y}$, then $d_y(\tilde{y},\hat{y}) \geqslant 1$, and so $d((\hat{p},\hat{y}),(\tilde{p},\tilde{y})) > 1$.

P2 Let us define

$$k_0 = \text{floor}\left(\frac{-log_2(\varepsilon)}{N}\right) + 1$$

according to the previous Lemma 1, and let us consider that the first k_0 elements of $\hat{p}$ and $\tilde{p}$ are the same. For $\forall\varepsilon < 1$, an integer k_0 can always be found to satisfy the relation $d(\hat{p},\tilde{p}) < 2^{-Nk_0} < \varepsilon$.

P3 If after k_0-th iteration, we have

$$\tilde{y} = G_f^{k_0}((\tilde{p},\tilde{y}))_2 = \hat{y}, \tag{17}$$

then a cycle point $(\tilde{p},\tilde{y}) = ((p^1p^2\dots p^{k_0}p^1p^2\dots p^{k_0}\dots),\tilde{y}) \in \varepsilon$ is found that satisfies

$$(\tilde{p},\tilde{y}) = G_f^{k_0}((\tilde{p},\tilde{y})) \tag{18}$$

making

$$d((\tilde{p},\tilde{y}),(\hat{p},\hat{y})) = d_p(\tilde{p},\hat{p}) + d_y(\tilde{y},\hat{y}) = d_p(\tilde{p},\hat{p}) < \varepsilon \tag{19}$$

true.

P4 Suppose that, after the k_0-th iteration, we have

$$\hat{y} \neq \tilde{y} = G_f^{k_0}((\tilde{p},\tilde{y}))_2. \tag{20}$$

To obtain that, after another iteration, the following condition is met

$$\hat{y} = \tilde{y} = G_f^{k_0+1}((\tilde{p},\tilde{y}))_2,$$

we must set: $p^{k_0+1} = G_f^{k_0}((\tilde{p},\tilde{y}))_2 \oplus \hat{y}$. Then, within range ε of the point $(\hat{p},\hat{y})$, one can find the following periodic point

$$\begin{aligned}(\tilde{p},\tilde{y}) &= ((p^1p^2\dots p^{k_0}p^{k_0+1}\dots p^1p^2\dots p^{k_0}p^{k_0+1}\dots),\tilde{y}) \\ &= G_f^{k_0+1}(\tilde{p},\tilde{y})\end{aligned} \tag{21}$$

making

$$d((\tilde{p},\tilde{y}),(\hat{p},\hat{y})) = d_p(\tilde{p},\hat{p}) + d_y(\tilde{y},\hat{y}) = d_p(\tilde{p},\hat{p}) < \varepsilon \tag{22}$$

true.

In summary, the periodic points of G_f are dense in ε.

3.2. Transitive property

Theorem 3 G_f is a transitive map on ε.

Proof Consider two nonempty open sets U_A and U_B, and $(p_A,y_A) \in U_A$, $(p_B,y_B) \in U_B$. U_A and U_B are open, and we take place in a metric space, so there exist real numbers $r_A > 0$ and $r_B > 0$ such that the open ball $\mathscr{B}_A$ of center (p_A,y_A) and radius r_A is inside U_A (resp. the open ball $\mathscr{B}_B$ of center (p_B,y_B) and radius r_B is into U_B). Without loss of generality, we can suppose that $r_A < 1$.

P-a We introduce the following notations:

$$(p_A,y_A) = ((p_A^1p_A^2\dots p_A^{n_0}\dots p_A^n\dots),y_A) \in U_A \in \varepsilon$$

and

$$(p_B,y_B) = ((p_B^1p_B^2\dots p_B^n\dots),y_B) \in U_B \in \varepsilon.$$

P-b Let $(\tilde{p},\tilde{y}) \in U_A$. If $\tilde{y} \neq y_A$, then $d_y(\tilde{y},y_A) \geqslant 1$, and so $d((p_A,y_A),(\tilde{p},\tilde{y})) > 1$. Consequently, if $(\tilde{p},\tilde{y}) \in \mathscr{B}_A$, then $d((p_A,y_A),(\tilde{p},\tilde{y})) < 1$, and so $\tilde{y} = y_A$.

P-c If we demand that the k_0 first elements of $\tilde{p}$ are equal to those from p_A, then we obtain $d(p_A,\tilde{p}) < 2^{-Nk_0}$. For the given r_A, an integer k_0 (that is, a sequence $\tilde{p}$) can always be found to achieve $d(p_A,\tilde{p}) < 2^{-Nk_0} < r_A$.

P-d If after k_0 iterations, the following condition is satisfied

$$G_f^{k_0}((p_A,p_A))_2 = y_B, \tag{23}$$

then $n_0 = k_0$ and $(\tilde{p},\tilde{y}) = ((p_A^1p_A^2\dots p_A^{n_0}p_B^1p_B^2\dots p_B^n\dots),y_A) \in U_A$ has been found that satisfies:

$$G_f^{n_0}(\tilde{p},\tilde{y}) = (p_B,y_B) \in G_f^{n_0}(U_A) \cap U_B \tag{24}$$

making

$$G_f^{n_0}(U_A) \cap U_B \neq \varnothing \tag{25}$$

true.

P-e If after the k_0-th iteration, $G_f^{k_0}((p_A,y_A))_2 \neq y_B$, then, define now $p^{k_0+1} = G_f^{k_0}((p_A,y_A))_2 \oplus y_B$, so the point $(\tilde{p},\tilde{y}) = ((p_A^1p_A^2\dots p_A^{n_0}p_B^1p_B^2\dots p_B^n\dots),y_A) \in U_A$ satisfies $G_f^{n_0}(\tilde{p},\tilde{y}) = (p_B,y_B) \in G_f^{n_0}(U_A) \cap U_B$ with $n_0 = k_0 + 1$, making the claim

$$G_f^{n_0}(U_A) \cap U_B \neq \varnothing \tag{26}$$

true.

In summary, (G_f,ε) is transitive.

Because of dense periodic points and transitivity, and according to Definition 1 and Theorem 1, we can conclude that CBDS is chaotic in the sense of Devaney.

4. Uniformity

Definition 5 (Uniform probability index) Let α be a random variable with a Bernoulli distribution. So

$$Y = \frac{\min\{P(\alpha=0), P(\alpha=1)\}}{\max\{P(\alpha=0), P(\alpha=1)\}}, \quad Y \in (0,1]$$

is called the uniform probability index of α.

The uniform probability index Y characterizes the uniformity of the binary sequence. In particular, if $Y=1$, then α is distributed evenly. The larger Y, the more uniform for α.

Theorem 4 Let α be a sequence of random variables having a Bernoulli distribution and β^n being a sequence of random variables defined by: β^0 is a random variable with a Bernoulli distribution, and $\forall n, \beta^{n+1} = \beta^n \oplus \alpha^n$. Then the uniformity of β is better than the one of α, in the sense that $\forall n, Y_{\beta^n} \geq Y_{\alpha^n}$.

Proof Let $P(\beta^0=0)=b$ and $P(\alpha^0=0)=a$.

P-i Let us prove that the statement holds when $n=1$

$$\begin{aligned} P(\beta^1=0) &= P(\alpha^0=0,\beta^0=0)+P(\alpha^0=1,\beta^0=1) \\ &= P(\alpha^0=0)P(\beta^0=0)+P(\alpha^0=1)P(\beta^0=1) \\ &= ab+(1-a)(1-b) \\ &= a+(1-b)(1-2a), \end{aligned} \tag{27}$$

$$\begin{aligned} P(\beta^1=1) &= P(\alpha^0=0,\beta^0=1)+P(\alpha^0=1,\beta^0=0) \\ &= a(1-b)+(1-a)b \\ &= a+b(1-2a). \end{aligned} \tag{28}$$

When $a \leq 1/2$ then $1-a \geq 1/2$, so we get

$$a \leq a+(1+b)(1-2a) = 1-a-(1-2a)b \leq 1-a, \tag{29}$$

$$a \leq a+b(1-2a) = 1-a-(1-2a)(1-b) \leq 1-a. \tag{30}$$

Conversely, when $a \geq 1/2$ then $1-a \leq 1/2$, and the above two inequalities still hold, while the equality holds if and only if $a=1/2$. Taking these two cases into account, we have:

$$\begin{aligned} \min(a,1-a) &\leq \min(P\{b=0\},P\{b=1\}) \\ &\leq \max(P\{b=0\},P\{b=1\}) \\ &\leq \max(a,1-a). \end{aligned} \tag{31}$$

These inequalities combined with Definition 5 leads to $1 \geq Y_{\beta^n} \geq Y_{\alpha^n}$, and the base case is obtained.

P-ii Suppose that the statement holds for a given n. Redefine a and b such that $P(\beta^n=0)=b$ while $P(\alpha^n=0)=a$. Then

$$\begin{aligned} P(\beta^n=0) &= P(\alpha^n=0,\beta^n=0)+P(\alpha^n=1,\beta^n=1) \\ &= a+(1-b)(1-2a), \end{aligned} \tag{32}$$

$$\begin{aligned} P(\beta^n=1) &= P(\alpha^n=0,\beta^n=1)+P(\alpha^n=1,\beta^n=0) \\ &= a+b(1-2a). \end{aligned} \tag{33}$$

The same canvas of proof as for the base case leads to the fact that the same statement holds for $n+1$, which concludes the proof.

Corollary 1 Let p^n be a sequence of random independent variables of integers having N bits, y^0 be an integer random variable, and (y^n) a sequence of random variables defined by $y^{n+1} = y^n \oplus p^n$. Then the binary sequence represented by y^n is more uniform than the one represented by p^n.

This corollary is an obvious consequence of the aforementioned theorem.

In order to evaluate this conclusion, density histograms have been computed. In these experiments, the length of p^n and y^n is $N=4$ bits, while a large number of sampled values are simulated (10^5 samples). Figure 1(a) shows that, as expected, the histogram is not uniformly distributed in all areas for p^n when $P(p^n=0)=0.6$ and $P(p^n=1)=0.4$. It can however be observed that a uniform histogram is obtained for y^n, and we have $P(y=0) \approx P(y=1) \approx 0.5$ for CBDS, see Fig. 1(b). This first evaluation of the uniformity in CBDS is systematically verified using numerous tests presented in the next section.

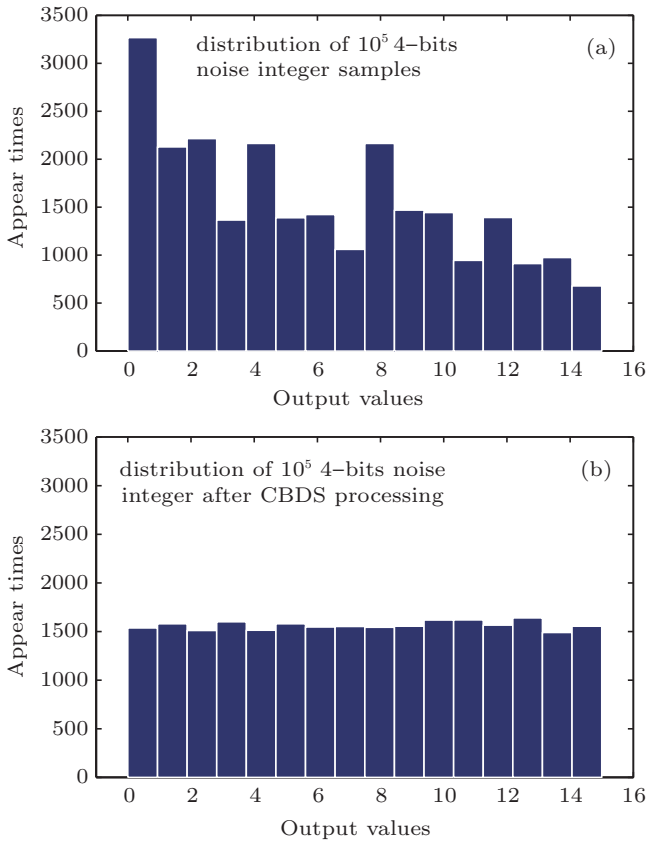


Fig. 1. (color online) The density histograms of p^n (a) and y^n in CBDS (b).

5. TestU01 statistical test results

There are many approaches to analyze the safety performance of chaotic systems used in information security, depending on which aspect sounds important. These approaches

encompass speed, cryptographical security, or statistical profile evaluation. This paper is a prerequisite for numerous applications, it is quite quick and simple to evaluate through reputed batteries of tests. Furthermore it does not need to consider the internal structure of the chaotic system, which explains why using such batteries becomes an internationally accepted analytical tool for PRNGs.

Various statistical tests are available in the literature that test a given sequence for some level of computational indistinguishability with a truly random stream. Major test suites for random sequences are TestU01, the NIST suite,[26] and the DieHARD one.[27] DieHARD suite, which implements many classical tests, has revealed over time some drawbacks and limitations. The National Institute of Standards and Technologies (NIST) in the United States, for its part, has implemented a suite (16 tests) for testing random sequences. It is geared mainly for the test and certification of random sequences used in cryptographic applications. Finally, TestU01 is extremely diverse in implementing classical tests, cryptographic tests, new tests proposed in the literature, and original ones. In fact, it encompasses most of the other test suites. The proposed CBDS has been evaluated using TestU01 for its statistical randomness.

Table 1 lists seven batteries of tests in the TestU01 package. "Standard" parameter in this table refers to the built-in parameters of the battery. TestU01 suite implements 518 tests and reports p-values. If a p-value is within [0.001, 0.999], the associated test is a success. A p-value lying outside this boundary means that its test has failed. The intention of CBDS is to enhance the effects of chaotic and random behaviors, to improve the statistical properties relative to p^n. This CBDS may utilize any reasonable random sequence as p^n. For demonstration purposes, ISAAC are adopted here. The y^n with this input can pass all of the performed tests.

Table 1. TestU01 statistical test.

Battery	Parameters	Applied tests	ISAAC	CBDS
Rabbit	32×10^9 bits	40	Pass	Pass
Alphabit	32×10^9 bits	17	Pass	Pass
Pseudo DieHARD	Standard	126	Pass	Pass
FIPS_140_2	Standard	16	Pass	Pass
Small crush	Standard	15	Pass	Pass
Crush	Standard	144	Pass	Pass
Big crush	Standard	160	Pass	Pass

6. FPGA-based realization of CBDS

The design principle of CBDS is described and verified in this section.

The CBDS construction starts with the noise source design, which has been developed using ring oscillators. A ring oscillator is a device composed of an odd number of NOT gates as shown in Fig. 2, whose output oscillates between two voltage levels, representing true and false. As it is depicted, the output of the last inverter is fed back into the first one. Because a single inverter computes the logical NOT of its input, it can be deduced that the last output of a chain of an odd number of inverters is the logical NOT of the first input. This final output is asserted a finite amount of time after the first input is asserted, and thus, the feedback of this last output to the first input causes oscillation.

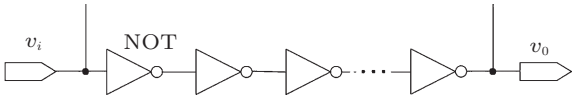


Fig. 2. The ring oscillator circuit schematic (with an odd number of NOT gates).

A multiple ring-based design was developed with several ring oscillators with different ring lengths. Here we use three rings, each with the long length gates. The three rings (as shown in Fig. 2) are XORed together to generate the output signal, as described in Fig. 3, where ring3:r31, ring3:r32, and ring3:r33 are the three long ring oscillators. The ring lengths for several ring oscillators were chosen in the range of relatively prime.[28]

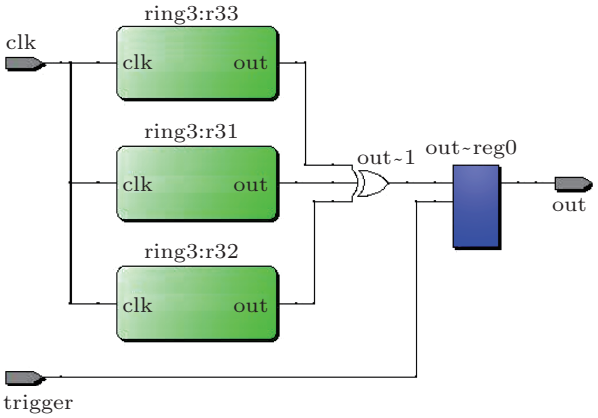


Fig. 3. (color online) A multiple ring-based design in FPGA.

The ring oscillator output once XORed is sampled using the D flip–flop as shown in Fig. 3, the 'trigger' input has to be carried out from lower or similar frequencies of the 'clk', this can cause more metastability effects in the D flip–flop, which can cause more metastability effects in the D flip–flop, which reduces the mutual coupling effects. The output has later to be subjected to post processing, that is, to chaotic iterations.

Each multiple ring oscillator outputs one component of state p^n (a binary digit). For our experiments, we have decided that p^n will be constituted by four binary digits, which means that $N = 4$. The iterative equation is $y^n = y^{n-1} \oplus p^n$ as shown in Fig. 4. Two D flip–flops are used to store state information: init[3...0] is for y^0 while out[3...0] reg0 stores y^{n-1}.

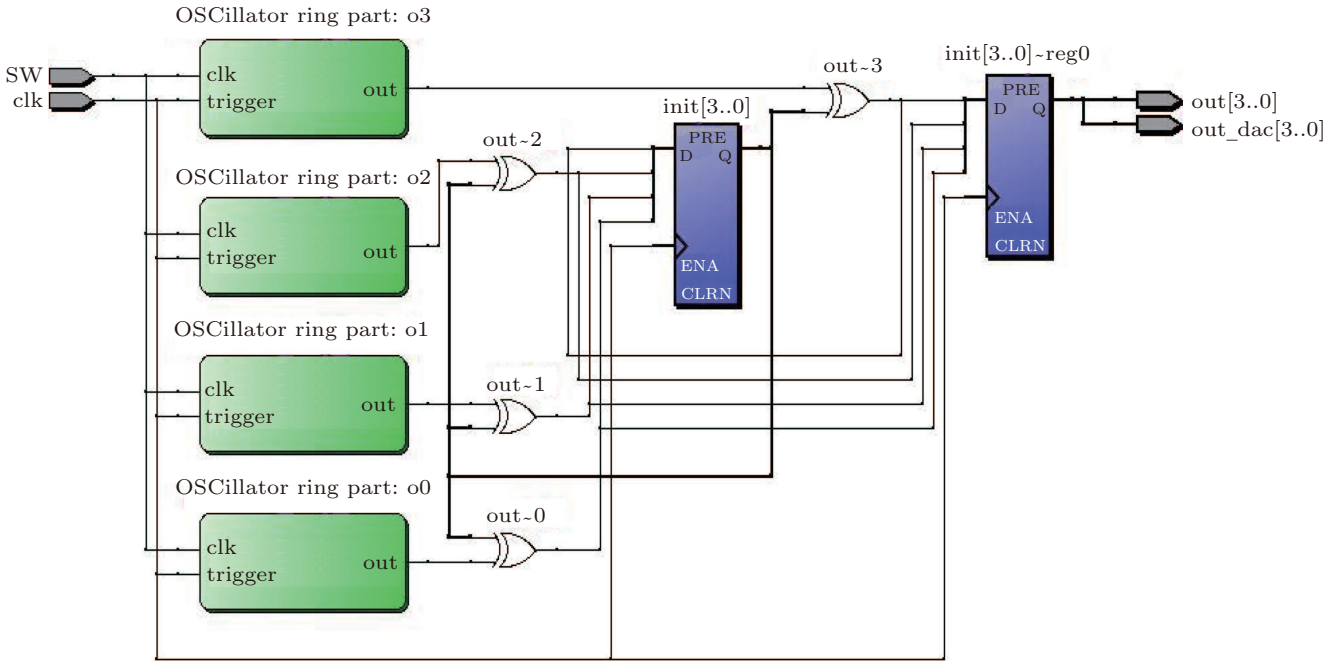


Fig. 4. (color online) The iteration function design in FPGA.

The experimental observations of CBDS are finally shown in Fig. 5. Then a 10^8-bits long CBDS sequence is generated and passes the NIST statistical test suite.

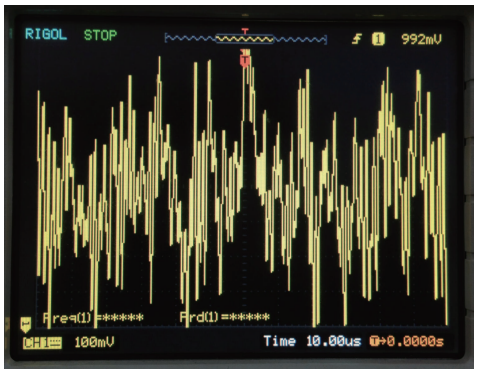


Fig. 5. (color online) The experimental observations of CBDS.

7. Conclusions

In order to solve degradation of chaotic dynamical properties by finite precision effects in traditional RDCS, the structure of a new CBDS, which uses random bitwise operations instead of only one, has been described. Its proof of chaos according to the Devaney's definition has been provided too. A comparison based on the uniformity of the outputs and on statistical tests has verified the good statistical profile of the generator. Finally, the performances of the corresponding FPGA-based implementation have been evaluated, confirming the feasibility and applicability of CBDS. These considerations enable us to claim that this CBDS offers a sufficient speed and level of security for a whole range of applications where secure generators are required as cryptography and data hiding.

References

[1] Nguyen V H, Park W, Kim N and Song H J 2014 *Chin. Phys. B* **23** 058201
[2] Shen C W, Yu S M, Lü J H and Chen G R 2014 *IEEE Trans. Circuits Syst. I* **61** 2380
[3] Yan S L 2014 *Chin. Phys. B* **23** 090503
[4] Dachselt F and Schwarz W 2001 *IEEE Trans. Circuits Syst. I* **48** 1498
[5] Li S J, Chen G R and Mou X Q 2005 *Int. J. Bifur. Chaos* **15** 3119
[6] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, Garcia-Ojalvo J, Mirasso C R, Pesquera L and Shore K A 2005 *Nature* **438** 343
[7] Ai X X, Sun K H, He S B and Wang H H 2014 *Acta Phys. Sin.* **63** 120511 (in Chinese)
[8] Shen C W, Yu S M, Lü J H and Chen G R 2014 *IEEE Trans. Circuits Syst. I* **61** 854
[9] Zhang C, Yu Y, Han X J and Bi Q S 2012 *Chin. Phys. B* **21** 100501
[10] Wang F L 2010 *Chin. Phys. B* **19** 090505
[11] Qi G Y and Sandra B M 2014 *Chin. Phys. B* **23** 050507
[12] Schuster H G and Just W 2006 *Deterministic Chaos: An Introduction* (Weinheim: John Wiley & Sons) p. 7
[13] Stability M, Zourntos T and Johns D A 2002 *IEEE Trans. Circuits Syst. I* **49** 41
[14] Li S, Mou X, Cai Y, Ji Z and Zhang J 2003 *Comput. Phys. Commun.* **153** 52
[15] Liu S B, Sun J, Xu Z Q and Liu J S 2009 *Chin. Phys. B* **18** 5219
[16] Simard R and Montréal U D 2007 *ACM T. Math. Software* **33** 22
[17] Bahi J and Guyeux C 2013 *Discrete Dynamical Systems and Chaotic Machines: Theory and Applications*, Chapman and Hall/CRC, June, 2013
[18] Bahi J, Couchot J F, Guyeux C and Wang Q X 2011 *IEEE International Conference on Evolving Internet*, June 19–24, 2011, Luxembourg, pp. 52–57
[19] Bahi H, Fang X L, Guyeux C and Wang Q X 2014 *J. Netw. Comput. Appl.* **37** 282
[20] Bahi J, Fang X, Guyeux C and Wang Q X 2011 *International Journal on Advances in Security* **4** 118
[21] Wang Q X, Yu S M, Guyeux C, Bahi J and Fang X L 2014 *Int. J. Bifur. Chaos* **24** 1450128

[22] Hajimiri A and Lee T 1998 *IEEE J. Solid-ST Circ.*, **33** 179
[23] Couturier R and Guyeux C 2013 *Designing Scientific Applications on GPUs* (Besancon: CRC) p. 441
[24] Devaney R L 1989 *An Introduction to Chaotic Dynamical Systems*, 2nd edn. (Redwood: Addison-Wesley) p. 48
[25] Banks J, Brooks J, Cairns G and Stacey P 1992 *Am. Math. Monthly* **99** 332
[26] Rukhin A, Soto J, Nechvatal J, Barker E, Leigh S, Levenson M, Banks D, Heckert A, Dray J, Vo S, Rukhin A, Soto J, Smid M, Leigh S, Vangel M and Iii L E B "A *statistical test suite for random and pseudorandom number generators for cryptographic application*" [date of the citation: Sept. 21, 2014] http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf [May 15, 2001]
[27] Marsaglia G 1995 "Diehard battery of tests of randomness", Florida State University" [date of the citation: Sept. 21, 2014] http://stat.fsu.edu/pub/diehard [1995]
[28] Sunar B, Martin W J and Stinson D R 2007 *IEEE T. Comput.* **56** 109