Statistical Properties of Digital Piecewise Linear Chaotic Maps and Their Roles in Cryptography and Pseudo-Random Coding*

Li Shujun[1a], Li Qi[2], Li Wenmin[3], Mou Xuanqin[1b], and Cai Yuanlong[1c]

[1] Institute of Image Processing, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China
[2] Department of Electrical Engineering and Electronics, The University of Liverpool, Brownlow Hill, Liverpool L69 3GJ, UK
[3] Department of Electircal and Electronic Engeering, Imperial College, Exhibition Road, London SW7 2BT, UK

Abstract. The applications of digital chaotic maps in discrete-time chaotic cryptography and pseudo-random coding are widely studied recently. However, the statistical properties of digital chaotic maps are rather different from the continuous ones, which impedes the theoretical analyses of the digital chaotic ciphers and pseudo-random coding. This paper detailedly investigates the statistical properties of a class of digital piecewise linear chaotic map (PLCM), and rigorously proves some useful results. Based on the proved results, we further discuss some notable problems in chaotic cryptography and pseudo-random coding employing digital PLCM-s. Since the analytic methods proposed in this paper can essentially extended to a large number of PLCM-s, they will be valuable for the research on the performance of such maps in chaotic cryptography and pseudo-random coding.

1 Introduction

Chaotic systems have many interesting properties, such as the sensitive dependence on initial conditions and control parameters, ergodicity, mixing and exactness properties, etc. [1]. Most properties can be connected with some requirements in cryptography and pseudo-random coding [2–4]. From 1990s, more and more researchers devote their contributions to a new field – chaotic cryptography; many analog and digital chaotic encryption systems have been proposed [2, 3, 5–9] and analysed [10–12]. As a general method to design chaotic stream ciphers, chaotic pseudo-random coding techniques are commonly used to construct PRBG-s (Pseudo-Random Bits Generators) [5,6,9]. At the same time,

* This paper was published in Cryptography and Coding C Proceedings of the 8th IMA International Conference (IMA-C&C2001, December 17-19, 2001, Cirencester, UK), Lecture Notes in Computer Science, vol. 2260, pp. 205-221, Springer-Verlag, Berlin, 2001.
Shujun Li is the corresponding author, personal web site: `http://www.hooklee.com`.

chaotic pseudo-random coding techniques have also developed separately in other areas, such as electronics, communications [13–15] and computer physics [16].

As we know, piecewise linear chaotic maps (PLCM) are the simplest kind of chaotic maps from the viewpoint of realization. What's more, they have uniform invariant density and good correlation functions [17], which is very useful for cryptography and pseudo-random coding [18]. In fact, many researchers have used them to realize chaotic ciphers and PRBG-s [6–9, 14].

It seems that chaotic systems are perfect as a new rich source of cryptography and pseudo-random coding. Unfortunately, when chaotic systems are realized in finite computing precision, their digital dynamical properties will be far different from the continuous ones. Some severe problems will arise, such as short cycle length, non-ideal distribution and correlation functions, etc. Assume the finite precision is L (bits) and fixed-point arithmetic is adopted, it is the following reasons to cause such degradation: 1) All values represented with finite precision are binary rational decimals formulated as $a/2^L (a = 0 \sim 2^L - 1)$. Since the Lebesgue measure of all the decimals is zero, they cannot represent the right dynamical behaviors of the chaotic systems defined on a real interval with positive measure; 2) There are only 2^L digital values to represent the chaotic orbits, so the cycle length of the orbits will not be larger than 2^L, generally it will be much smaller than 2^L; 3) The quantization errors, which are introduced into the iterations of chaotic systems, will make the chaotic orbits depart from the theoretical ones with uncontrolled manners (it is impossible to know the exact errors).

Some researchers have noticed the degradation of digital chaotic systems [9–11, 13, 19, 20], and several remedies have been suggested: using higher finite precision [11,19], the perturbation-based algorithm [9,20], and cascading multiple chaotic systems [13]. Because it is difficult to measure the statistical properties of digital chaotic maps theoretically, experiments are generally used as the analytic tools to estimate the performance of the above remedies. However, sometimes experiments are not enough to tell us the right things about digital chaotic systems. The theoretical tools for digital chaotic systems are needed.

2 Outline of Our Works

In this paper, we strictly prove some interesting statistical properties about a class of digital PLCM with finite computing precision. Based on our proved results, we can explain some statistical degradation of digital PLCM-s theoretically. Such degradation will cause the chaotic ciphers insecure, and cause chaotic pseudo-random sequences unbalanced. Furthermore, we discuss the performance of the three proposed remedies, and point out none of them can essentially improve such degradation. But the perturbation-based algorithm is still useful in practice, since it can be carefully used to enhance the performance of digital chaotic ciphers and pseudo-random coding.

For other digital chaotic maps, we have not yet obtained exact corresponding results. But our proof techniques may probably be extended to many other digital chaotic maps conceptually. If one chaotic map contains a control parameter that

is proportional to uniformly distributed final output, the digital chaotic map may be weak from the viewpoint of this control parameter. In the future, we will try to find more delicate results.

This paper is organised as follows. In Sect. 3, we firstly introduce some preliminary knowledge. In the following Sect. 4, we focus on the mathematically rigorous proofs of the interesting properties of digital PLCM-s. Since the whole proof is rather lengthy, it is divided into several parts. Based on the proved properties, we explain what they mean in chaotic cryptography and pseudo-random coding in Sect. 5. A brief conclusion is given in the last section.

3 Preliminary Knowledge

3.1 Piecewise Linear Chaotic Map (PLCM)

Generally, given a real interval $X = [\alpha, \beta] \subset \mathbb{R}$, a piecewise linear chaotic map $F : X \to X$ is a multi-segmental map: $i = 1 \sim m, F(x)|C_i = F_i(x) = a_i x + b_i$, where $\{C_i\}_{i=1}^m$ is a partition of X, which satisfies $\bigcup_{i=1}^m C_i = X$ and $C_i \cap C_j = \varnothing, \forall i \neq j$. Each element of the partition is mapped to X by F_i: $\forall i = 1 \sim m, F_i : C_i \to X$. Such a map has the following statistical properties on its definition interval X: 1) it is chaotic, its Lyapunov exponent λ satisfies $0 < \lambda < \ln m$; 2) it is exact, mixing and ergodic, and has uniform invariant density function $f(x) = 1/(\beta - \alpha)$; 3) the correlation $\tau(n) = \frac{1}{\sigma^2} \lim\limits_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{x})(x_{i+n} - \bar{x})$ will go to zero as $n \to \infty$, where $\bar{x}, \sigma$ are the mean value and the variance of x respectively; especially, if some conditions are satisfied, $\tau(n) = \delta(n)$ [1, 17].

As we know [1], the uniform invariant density function means that uniform input will generate uniform output, and that the chaotic orbit from almost every initial condition will lead to the same uniform distribution $f(x) = 1/(\beta - \alpha)$. But such a fact is not true for a digital chaotic map, this paper will point out that uniform digital input cannot generate uniform digital output for all control parameters. Such a fact will subsequently cause serious dynamical degradation when the maps are iterated again and again. Because it is inconvenient to analyse chaotic maps with uncertain formulas, in this paper, we focus our attention on the following specific PLCM used in [8]:

$$F(x,p) = \begin{cases} x/p, & x \in [0,p) \\ (x-p)/(1/2-p), & x \in [p,1/2] \\ F(1-x,p), & x \in [1/2,1] \end{cases}, \tag{1}$$

where p is the control parameter, which satisfies $0 < p < 1/2$.

In order to facilitate the descriptions and proofs of the statistical properties in Sect. 4, we give some definitions in Sect. 3.2 and related results in Sect. 3.3.

3.2 Preliminary Definitions

Definition 1. *A discrete set* $S_n = \left\{ a \,\middle|\, a = \sum_{i=1}^n a_i \cdot 2^{-i}, a_i \in \{0,1\} \right\}$ *is called a* ***digital set*** *with* ***resolution*** n; $\forall i < j$, S_i *is called the* ***digital subset*** *with*

resolution *i of* S_j*. Specially, define* $S_0 = \{0\}, S_\infty = [0,1)$*, then we have* $\{0\} = S_0 \subset S_1 \subset \ldots \subset S_i \subset \ldots \subset S_\infty = [0,1)$*.*

Definition 2. *Define* $V_i = S_i - S_{i-1} (i \geq 1)$ *and* $V_0 = S_0$*.* $V_i (0 \leq i \leq n)$ *is called the* ***digital layer*** *with* ***resolution*** *i;* $\forall p \in V_i$*, i is called the* ***resolution*** *of p. The partition of* S_n*,* $\{V_i\}_{i=0}^n$*, is called the* ***complete multi-resolution decomposition*** *of* S_n*;* $\{V_i\}_{i=0}^\infty$ *is called the* ***complete multi-resolution decomposition*** *of* $S_\infty = [0,1)$*. For* S_n*, its resolution n is also called* ***decomposition level****,* $\bigcup_{i=0}^n V_i = S_n$*, and* $\forall i \neq j, V_i \cap V_j = \varnothing$*.*

Definition 3. $\forall n > m$*,* $D_{n,m} = S_n - S_m$ *is called the* ***digital difference set*** *of the two digital sets with parameters n and m.* $\{V_i\}_{i=m}^n = \{S_i - S_{i-1}\}_{i=m}^n$ *is called the* ***complete multi-resolution decomposition*** *of* $D_{n,m}$*,* $n - m + 1$ *is called the* ***decomposition level****.*

Definition 4. *A function* $G : \mathbb{R} \to \mathbb{Z}$ *is called an* ***approximate transformation function (ATF)****, if* $\forall x \in \mathbb{R}$*,* $|G(x) - x| < 1$*. Three basic ATF-s are: 1)* $\lfloor x \rfloor$ *– the maximal integer not greater than x; 2)* $\lceil x \rceil$ *– the minimal integer not less than x; 3)* $\mathrm{round}(x)$ *– the rounded integer of x.* $\forall x \in \mathbb{R}$*, define its* ***decimal part*** $x - \lfloor x \rfloor$ *as function* $\mathbf{dec}(\boldsymbol{x})$*. The above* ***three*** *ATF-s have the following useful properties (please note* ***not all*** *ATF-s):*

$$\textit{ATF Property 1}: \forall m \in \mathbb{Z}, G(x+m) = G(x) + m; \tag{2}$$

$$\textit{ATF Property 2}: a < x < b \Rightarrow \lfloor x \rfloor \leq G(x) \leq \lceil x \rceil. \tag{3}$$

The proofs of the two properties are rather simple, we omit them here.

Definition 5. *A function* $G_n : S_\infty \to S_n$ *is called a* ***digital approximate transformation function (DATF)*** *with* ***resolution*** *n, if* $\forall x \in S_\infty = [0,1)$*,* $|G_n(x) - x| < 1/2^n$*. The following three DATF-s are concerned in this paper (they are also the most frequently adopted DATF-s in digital computing algorithms): 1)* $\mathrm{floor}_n(x) = \lfloor x \cdot 2^n \rfloor / 2^n$*; 2)* $\mathrm{ceil}_n(x) = \lceil x \cdot 2^n \rceil / 2^n$*; 3)* $\mathrm{round}_n(x) = \mathrm{round}(x \cdot 2^n)/2^n$*.*[4] *The above* ***three*** *DATF-s have the following useful properties (please note* ***not all*** *DATF-s):*

$$\textit{DATF Property 1}: \forall m \in \mathbb{Z}, G_n(x + m/2^n) = G_n(x) + m/2^n; \tag{4}$$

$$\textit{DATF Property 2}: a < x < b \Rightarrow \mathrm{floor}_n(a) \leq G_n(x) \leq \mathrm{ceil}_n(b). \tag{5}$$

The two properties are easily derived from the ATF Property 1–2.

3.3 Preliminary Lemmas about the Three Basic ATF-s

For the three basic ATF-s – $\lfloor \cdot \rfloor$, $\lceil \cdot \rceil$ and $\mathrm{round}(\cdot)$, we have two fundamental lemmas and one corollary, which will be useful in the proofs of the theorems in the next section.

[4] Consider $1 \notin S_\infty$, without loss of generality, define $\mathrm{ceil}_n(x) = 0$ if $\lceil x \cdot 2^n \rceil = 2^n$, and define $\mathrm{round}_n(x) = 0$ if $\mathrm{round}(x \cdot 2^n) = 2^n$. Such redefinitions will not essentially influence the following results since $\mathrm{dec}(1) = 0$.

Lemma 1. *$\forall n \in \mathbb{Z}^+, a \geq 0$, the following three facts are true:*

1. $n \cdot \lfloor a \rfloor \leq \lfloor n \cdot a \rfloor \leq n \cdot \lfloor a \rfloor + (n-1)$, *and* $n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor$ *when and only when* $\mathrm{dec}(a) \in \left[0, \frac{1}{n}\right)$;
2. $n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$, *and* $n \cdot \lceil a \rceil - (n-1) = \lceil n \cdot a \rceil$ *when and only when* $\mathrm{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$;
3. $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor \leq \mathrm{round}(n \cdot a) \leq n \cdot \mathrm{round}(a) + \lfloor n/2 \rfloor$, *and* $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor = \mathrm{round}(n \cdot a)$ *when and only when* $\mathrm{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$.

The proof of this lemma is given in Appendix A.

Corollary 1. *$\forall n \in \mathbb{Z}^+, a \geq 0$, we have the following results:*

1. $\lfloor n \cdot a \rfloor \equiv 0 \pmod{n}$ *when and only when* $\mathrm{dec}(a) \in \left[0, \frac{1}{n}\right)$;
2. $\lceil n \cdot a \rceil \equiv 0 \pmod{n}$ *when and only when* $\mathrm{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$;
3. $\mathrm{round}(n \cdot a) \equiv 0 \pmod{n}$ *when and only when* $\mathrm{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$.

Proof. This corollary can be derived directly from the above lemma.

Lemma 2. *$\forall j, N, N' \in \mathbb{Z}^+$, and N, N' are odd integers satisfying $2^j | (N + N')$, we have $\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = (N + N')/2^j - 1$.*

The proof of this lemma is given in Appendix B.

4 Statistical Properties of Digital PLCM

Give a one-dimensional chaotic map $F(x, p) : I \to I$, where $I = S_\infty = [0, 1)$. When the finite precision is n, its digital version can be expressed by $F_n(x, p) = G_n \circ F(x, p) : S_n \to S_n$, where $G_n(\cdot)$ is a DATF, $\mathrm{floor}_n(\cdot)$, $\mathrm{ceil}_n(\cdot)$ or $\mathrm{round}_n(\cdot)$. Denote the corresponding ATF of $G_n(\cdot)$ as $G_0(\cdot)$.

Assume P_j denotes the probability of the lowest j bits of $F_n(x, p)$ are all zeros, i.e., the probability of $F_n(x, p)$ belongs to S_{n-j}: $P_j = P\{F_n(x, p) \in S_{n-j}\}$. For the map denoted by (1)[5], $\forall p \in V_i \subset S_i \subseteq S_n (2 \leq i \leq n)$, we can deduce some interesting results about $P_j (1 \leq j \leq n)$, which are rather different from the expected ones based on the perfect continuous statistical properties of the map. Moreover, the results can be essentially extended to all digital PLCM-s described in Sect. 3.1.

Because the whole proof is rather lengthy, we divide it into several parts: firstly a fundamental lemma, then the results about $P_j (i \leq j \leq n)$ and the ones about $P_j (1 \leq j < i)$, finally two comprehensive theorems.

[5] Because $1 \notin S_\infty$, redefine $F_n(1/2, p) = 0$. Consider $F^2(1/2, p) = 0$ and $\mathrm{dec}(1) = 0$, such redefinition will not essentially influence the following results.

4.1 A Fundamental Lemma

Firstly, we introduce Lemma 3, which gives some useful results about the highest $n-i$ bits and the lowest i bits of $F_n(x,p)$. This lemma is the fundamental of the following proofs. At the same time, this lemma reflects some facts about the local linearity of the PLCM-s, which makes the obtained results in this paper conceptually available for other PLCM-s.

Lemma 3. *$\forall p \in D_{i,0} = S_i - \{0\}(1 \le i \le n), x \in S_n$. Assume $p = N_p/2^i, x = N_x/2^n$, where N_p, N_x are integers satisfying $1 \le N_p \le 2^i - 1$ and $0 \le N_x \le 2^n - 1$. we have the following three results:*

1. $G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}$, (6)
2. $\text{floor}_{n-i}(G_n(x/p)) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$, (7)
3. $G_n(x/p) \bmod \dfrac{1}{2^{n-i}} = \dfrac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}$. (8)

Proof. Because $x/p = \dfrac{N_x/2^n}{N_p/2^i} = \dfrac{N_x/N_p}{2^{n-i}} = \dfrac{\lfloor N_x/N_p \rfloor + (N_x \bmod N_p)/N_p}{2^{n-i}}$, we have $G_n(x/p) = \dfrac{G_0(2^i \cdot \lfloor N_x/N_p \rfloor + 2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}$. From *ATF Property 1*, we can rewrite $G_n(x/p)$ as follows

$$G_n(x/p) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n} \ . \tag{9}$$

Let us discuss the above equation under the following two conditions:

a) When $N_x \bmod N_p = 0$: $G_n(x/p) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + 0 \in S_{n-i}$;

b) When $N_x \bmod N_p = k \neq 0$: Obviously $1 \le k \le N_p - 1$. Considering $p < 1$, we have $2^i/N_p > 1$, then $1 < 2^i \cdot (N_x \bmod N_p)/N_p < 2^i - 1$. Thus, from *ATF Property 2*, $1 \le G_0(2^i \cdot (N_x \bmod N_p)/N_p) \le 2^i - 1$. Therefore,

$$\frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{1}{2^n} \le G_n(x,p) \le \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{2^i - 1}{2^n} \Rightarrow G_n(x,p) \notin S_{n-i}. \tag{10}$$

From a) and b), we can deduce $G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}$.

At the same time, when $N_x \bmod N_p = 0$, $\text{floor}_{n-i}(G_n(x/p)) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$; when $N_x \bmod N_p = k \neq 0$, $\text{floor}_{n-i}(G_n(x/p)) \ge \dfrac{\lfloor \lfloor N_x/N_p \rfloor + 1/2^i \rfloor}{2^{n-i}} = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$ and $\text{floor}_{n-i}(G_n(x/p)) \le \dfrac{\lfloor \lfloor N_x/N_p \rfloor + (2^i - 1)/2^i \rfloor}{2^{n-i}} = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$, so finally we can get $\text{floor}_{n-i}(G_n(x/p)) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$.

From the above result and (9), the following result is true:

$$G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n} \ .$$

The proof is complete.

4.2 Results about $P_j(i \le j \le n)$

Theorem 1. *Assume random variable x distributes uniformly in S_n, for the digital PLCM (1), $\forall p \in D_{i,1}(2 \le i \le n)$[6], we have: $P_i = 4/2^i$.*

Proof. Assume $p = N_p/2^i, x = N_x/2^n$, where N_p, N_x are integers that satisfy $1 \le N_p \le 2^i - 1$ and $0 \le N_x \le 2^n - 1$. Because x distributes uniformly in S_n, N_x will distribute uniformly in integer set $[0, 2^n - 1]$. Since the chaotic map is defined piecewisely, we consider it on different segments:

a) $x \in [0, p) \Rightarrow N_x \in [0, 2^{n-i} \cdot N_p - 1]$: $F_n(x, p) = G_n(x/p)$, from Lemma 3, we know $F_n(x, p) \in S_{n-i}$ when and only when $N_x \equiv 0 \pmod{N_p}$. Because N_x distributes uniformly in $[0, 2^n - 1]$, the probability of $F_n(x, p) \in S_{n-i}$ will be $2^{n-i}/(2^{n-i} \cdot N_p) = 1/N_p$. That is to say, $P_i|x \in [0, p) = 1/N_p$.

b) $x \in [p, 1/2)$: Assume $x' = x - p, p' = 1/2 - p$, we have $F_n(x, p) = x'/p'$, where $x' \in [0, p')$. Similarly to a), define $p' = N'_p/2^i, x' = N'_x/2^n$, we will get $P_i|x \in [p, 1/2) = P_i|x' \in [0, p') = 1/N'_p$.

c) $x \in [1/2, 1)$: Consider the map is even symmetric to $x = 1/2$, we can easily get the following two results: $P_i|x \in (1/2, 1 - p] = 1/N'_p$ and $P_i|x \in ((1 - p, 1) \cup \{1/2\}) = 1/N_p$. Here please note that $1 \notin S_n$ and $1/2$ takes its position that is symmetrical to 0, which will not make any difference to P_i.

From a) – c) and the total probability rule, we can deduce:

$$\begin{aligned} P_i &= P(x \in [0, p)) \cdot P_i|x \in [0, p) + P(x \in [p, 1/2)) \cdot P_i|x \in [p, 1/2) \\ &\quad + P(x \in (1/2, 1 - p]) \cdot P_i|x \in (1/2, 1 - p] \\ &\quad + P(x \in ((1 - p, 1) \cup \{1/2\})) \cdot P_i|x \in ((1 - p, 1) \cup \{1/2\}) \\ &= p \cdot \frac{1}{N_p} + p' \cdot \frac{1}{N'_p} + p' \cdot \frac{1}{N'_p} + p \cdot \frac{1}{N_p} = \frac{1}{2^i} + \frac{1}{2^i} + \frac{1}{2^i} + \frac{1}{2^i} = \frac{4}{2^i} \ . \end{aligned}$$

The proof is complete.

Theorem 2. *Assume random variable x distributes uniformly in S_n, for the digital PLCM (1), $\forall p \in D_{i,1}(2 \le i \le n)$, $\mathrm{floor}_{n-i}(F_n(x, p))$[7] distributes uniformly in S_{n-i}.*

Proof. Similarly to the proof of Theorem 1, assume $p = N_p/2^i, x = N_x/2^n$, we separately consider the map on different segments:

a) $x \in [0, p) \Rightarrow N_x \in [0, 2^{n-i} \cdot N_p - 1]$: $F_n(x, p) = G_n(x/p)$, from Lemma 3, we have $\mathrm{floor}_{n-i}(F_n(x, p)) = \lfloor N_x/N_p \rfloor / 2^{n-i}$. Because x distributes uniformly in S_n, N_x distributes uniformly in $[0, 2^{n-i} \cdot N_p - 1]$. Thus $\lfloor N_x/N_p \rfloor$ distributes uniformly in $[0, 2^{n-i} - 1]$, i.e., $\mathrm{floor}_{n-i}(F_n(x, p))$ distributes uniformly in S_{n-i} when $x \in [0, p)$.

[6] Please note p should also satisfy $0 < p < 1/2$ for the map (1). But such a fact will not essentially influence the theorems proved in this paper, we omit this requirement of p. This note is also available for the following theorems.

[7] The highest $n - i$ bits of $F_n(x, p)$.

b) $x \in [p, 1/2)$: Assume $x' = x - p, p' = 1/2 - p$, we have $F_n(x,p) = x'/p'$, where $x' \in [0, p')$. Similarly to a), we can prove $\text{floor}_{n-i}(F_n(x,p))$ distributes uniformly in S_{n-i} when $x \in [p, 1/2)$.

c) $x \in [1/2, 1)$: Because the map is even symmetrical to $x = 1/2$, it can be easily deduced that $\text{floor}_{n-i}(F_n(x,p))$ distributes uniformly in S_{n-i} when $x \in [1/2, 1)$.

From a) – c), we know it is true that $\text{floor}_{n-i}(F_n(x,p))$ distributes uniformly in S_{n-i}. The proof is complete.

Theorem 3. *Assume random variable x distributes uniformly in S_n, for the digital PLCM (1), $\forall p \in D_{i,1}(2 \le i \le n)$ and $i \le j \le n$, $P_j = 4/2^j$ holds.*

Proof. Let us discuss the different conditions when $j = i$ and $j > i$.

a) $j = i$: From Theorem 1, $P_j = 4/2^i = 4/2^j$;

b) $i < j \le n$: Assume $b_m (m = 1 \sim n)$ represents the m^{th} bit (from the lowest bit to the highest one) of $F_n(x,p)$, $P_j = P\left\{ F_n(x,p) \in S_{n-i} \wedge b_j \cdots b_{i+1} = \overbrace{0 \cdots 0}^{j-i} \right\}$. Recall the proof of Theorem 2, when $F_n(x,p) \in S_{n-i}$ (i.e., $N_x \bmod N_p = 0$), $\lfloor N_x/N_p \rfloor$ (the highest $n-i$ bits of $F_n(x,p)$) still distributes uniformly in $[0, 2^{n-i} - 1]$. So we can get $P_j = P\{F_n(x,p) \in S_i\} \cdot \frac{1}{2^{j-i}} = \frac{4}{2^i} \cdot \frac{1}{2^{j-i}} = \frac{4}{2^j}$.

From a) and b), we have: $i \le j \le n \Rightarrow P_j = 4/2^j$. The proof is complete.

4.3 Results about $P_j (1 \le j < i)$

Firstly, we introduce Lemma 4 and Corollary 2, which will be used to facilitate the proof of Theorem 4.

Lemma 4. *Assume n is an odd integer, random integer variable K distributes uniformly in $\mathbb{Z}_n = [0, n-1]$, the following fact is true: $K' = f(K) = (2^i \cdot K) \bmod n$ distributes uniformly in $\mathbb{Z}_n$, i.e., $\forall k \in [0, n-1], P\{K' = k\} = 1/n$.*

Proof. As we know, $(\mathbb{Z}_n, +)$ is a finite cyclic group of degree n, and a is its generator when and only when $\gcd(a, n) = 1$, where "+" is defined as "$(a + b) \bmod n$" (see Theorem 2 on page 60 of [21]). Therefore, $a = 2^i \bmod n$ is one generator of $\mathbb{Z}_n$ since $\gcd(a, n) = \gcd(2^i, n) = 1$. Consider $K' = (2^i \cdot K) \bmod n = (a \cdot K) \bmod n$, we can see $f : \mathbb{Z}_n \to \mathbb{Z}_n$ is a bijection. Then we will immediately deduce: $K' = f(K)$ distributes uniformly in $\mathbb{Z}_n$ because K distributes uniformly in $\mathbb{Z}_n$. That is to say, $\forall k \in [0, n-1], P\{K' = k\} = 1/n$. The proof is complete.

Corollary 2. *Assume n is an odd integer, random integer variable K distributes uniformly in $\mathbb{Z}_n = [0, n-1]$. Then $\text{dec}(2^i \cdot K/n)$ distributes uniformly in $S = \{x | x = k/n, k \in \mathbb{Z}_n\}$.*

Proof. This corollary is the straightforward result of the above lemma.

Theorem 4. *Assume random variable x distributes uniformly in S_n, for the digital PLCM (1), $\forall p \in V_i (2 \le i \le n)$[8] and $1 \le j \le i-1$, we have:*

$$P_j = \left\{ \begin{array}{c} 1/2^j + 2/2^i \\ 1/2^j, 1 \le j \le i-2 \\ 4/2^i, \quad j = i-1 \end{array} \right\}, \begin{array}{l} \\ G_n(\cdot) = \text{floor}_n(\cdot) \text{ or } \text{ceil}_n(\cdot) \\ G_n(\cdot) = \text{round}_n(\cdot) \end{array} .$$

Proof. $p = N_p/2^i, x = N_x/2^n$, where N_p, N_x are integers that satisfy $1 \le N_p \le 2^i - 1$ and $0 \le N_x \le 2^n - 1$. Because x distributes uniformly in S_n, N_x will distribute uniformly in integer set $[0, 2^n - 1]$. Let us consider the digital map on different segments:

a) $x \in [0, p) \Rightarrow N_x \in [0, 2^{n-i} \cdot N_p - 1]$: $F_n(x, p) = G_n(x/p)$, from Lemma 3, we know the lowest i bits of $F_n(x, p)$ are determined by $G_0(2^i \cdot (N_x \bmod N_p)/N_p)$. Then we can deduce $F_n(x, p) \in S_{n-j} \Leftrightarrow G_0(2^i \cdot (N_x \bmod N_p)/N_p) \equiv 0 \bmod 2^j$. Define $\hat{N} = N_x \bmod N_p$, which distributes uniformly in $[0, N_p - 1]$ because of the uniform distribution of N_x. Define $a = (2^{i-j} \cdot \hat{N})/N_p$, we can re-write $G_0(2^i \cdot (N_x \bmod N_p)/N_p)$ as $G_0(2^j \cdot a)$. From Corollary 1, we can get:

$$G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \Leftrightarrow \text{dec}(a) \in \left\{ \begin{array}{ll} \left[0, \frac{1}{2^j}\right) & , G_0(\cdot) = \lfloor \cdot \rfloor \\ \left(1 - \frac{1}{2^j}, 1\right) \bigcup \{0\} & , G_0(\cdot) = \lceil \cdot \rceil \\ \left[0, \frac{1}{2^{j+1}}\right) \bigcup \left[1 - \frac{1}{2^{j+1}}, 1\right) & , G_0(\cdot) = \text{round}(\cdot) \end{array} \right. . \tag{11}$$

From Corollary 2 (please note $p \in \boldsymbol{V_i}$ ensures N_p is an odd integer), we know

$$\text{dec}(a) = k/N_p (k = 0 \sim N_p - 1) \text{with uniform probability.} \tag{12}$$

Based on (11) and (12), we can deduce:

$$k \in \left\{ \begin{array}{ll} \left[0, \frac{N_p}{2^j}\right) & , G_0(\cdot) = \lfloor \cdot \rfloor \\ \left(N_p - \frac{N_p}{2^j}, N_p\right) \bigcup \{0\} & , G_0(\cdot) = \lceil \cdot \rceil \\ \left[0, \frac{N_p}{2^{j+1}}\right) \bigcup \left[N_p - \frac{N_p}{2^{j+1}}, N_p\right) & , G_0(\cdot) = \text{round}(\cdot) \end{array} \right. . \tag{13}$$

Consider k is an integer, we can get the probability

$$P\left\{G_0(2^j \cdot a) \equiv 0 \pmod{2^j}\right\} = \left\{ \begin{array}{ll} \frac{\lfloor N_p/2^j \rfloor + 1}{N_p} & , \quad G_0(\cdot) = \lfloor \cdot \rfloor \text{ or } \lceil \cdot \rceil \\ \frac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_0(\cdot) = \text{round}(\cdot) \end{array} \right. . \tag{14}$$

[8] Please note the condition $p \in \boldsymbol{V_i}$, **NOT** $p \in \boldsymbol{D_{i,1}}$ in Theorem 1–3.

b) $x \in [p, 1/2)$: Assume $x' = x - p, p' = 1/2 - p$, we have $F_n(x,p) = x'/p'$, where $x' \in [0, p')$. Similarly to a), define $p' = N'_p/2^i, x' = N'_x/2^n$, we will get

$$P\left\{G_0(2^j \cdot a') \equiv 0 \pmod{2^j}\right\} = \begin{cases} \dfrac{\lfloor N'_p/2^j \rfloor + 1}{N'_p}, & G_0(\cdot) = \lfloor \cdot \rfloor \text{ or } \lceil \cdot \rceil \\ \dfrac{2 \cdot \lfloor N'_p/2^{j+1} \rfloor + 1}{N'_p}, & G_0(\cdot) = \text{round}(\cdot) \end{cases}, \tag{15}$$

where $a' = (2^{i-j} \cdot \hat{N}')/N'_p, \hat{N}' = N'_x \bmod N'_p$.

From (14) and (15), we can get the conditional probability $P_j|x \in [0, 1/2)$. Consider the map is even symmetrical to $x = 1/2$, the final probability will be $P_j = 2 \cdot (P_j|x \in [0, 1/2))$. In the following, we separately consider the condition of $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$ and $G_n(\cdot) = \text{round}_n(\cdot)$:

i) $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$, i.e., $G_0(\cdot) = \lfloor \cdot \rfloor$ or $\lceil \cdot \rceil$: $p + p' = 1/2 \Rightarrow N_p + N'_p = 2^{i-1} \Rightarrow 2^j | (N_p + N'_p)$, from Lemma 2, we can deduce:

$$\begin{aligned} P_j =& 2\left(p \cdot \frac{\lfloor N_p/2^j \rfloor + 1}{N_p} + p' \cdot \frac{\lfloor N'_p/2^j \rfloor + 1}{N'_p}\right) \\ =& 2\left(\frac{\lfloor N_p/2^j \rfloor + \lfloor N'_p/2^j \rfloor + 2}{2^i}\right) = \frac{2^{i-j-1} - 1 + 2}{2^{i-1}} = \frac{1}{2^j} + \frac{2}{2^i}. \end{aligned} \tag{16}$$

ii) $G_n(\cdot) = \text{round}_n(\cdot)$, i.e., $G_0(\cdot) = \text{round}(\cdot)$: When $j < i - 1$, $N_p + N'_p = 2^{i-1} \Rightarrow 2^{j+1} | (N_p + N'_p)$, from Lemma 2, we can get:

$$\begin{aligned} P_j =& 2\left(p \cdot \frac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p} + p' \cdot \frac{2 \cdot \lfloor N'_p/2^{j+1} \rfloor + 1}{N'_p}\right) \\ =& 2\left(\frac{2\left(\lfloor N_p/2^{j+1} \rfloor + \lfloor N'_p/2^{j+1} \rfloor\right) + 2}{2^i}\right) = \frac{2\left(2^{i-j-2} - 1\right) + 2}{2^{i-1}} = \frac{1}{2^j}. \end{aligned} \tag{17}$$

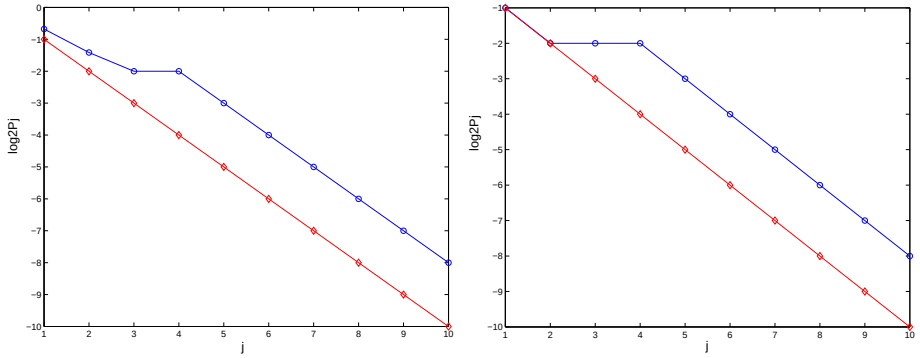
When $j = i - 1$, $N_p + N'_p = 2^{i-1} \Rightarrow 2^{j+1} \nmid (N_p + N'_p)(j + 1 = i > i - 1)$, Lemma 2 cannot be used, but we can calculate the probability P_j by directly observing (14) and (15): $N_p < 2^i, N'_p < 2^i$, so $N_p/2^{j+1} < 1 \Rightarrow \lfloor N_p/2^{j+1} \rfloor = 0, N'_p/2^{j+1} < 1 \Rightarrow \lfloor N'_p/2^{j+1} \rfloor = 0$, then we have

$$P_j = 2\left(p \cdot \frac{2 \cdot 0 + 1}{N_p} + p' \cdot \frac{2 \cdot 0 + 1}{N'_p}\right) = 2 \cdot \frac{2}{2^i} = \frac{4}{2^i}. \tag{18}$$

From (16) – (18),we can directly get the final result. The proof is complete.

4.4 Comprehensive Results about $P_j(1 \le j \le n)$

In the above subsections, we have separately proved the results about $P_j(i \le j \le n)$ and $P_j(1 \le j < i)$ for any $p \in V_i \subset S_i \subseteq S_n(2 \le i \le n)$. To make the above "rough-and-tumble" results tidier, we rearrange them into two new theorems, which are easier to be understood and to be used in practice.



(a) $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$ (b) $G_n(\cdot) = \text{round}_n(\cdot)$

Fig. 1. $P_j (1 \le j \le n)$ when $p = 3/16 \in V_4 \subset S_4$, where the finite precision $n = 10$ (The line marked with diamond signs denotes the probability under digital uniform distribution $1/2^j$, and the other line denotes the probability P_j)

Theorem 5. *Assume random variable x distributes uniformly in S_n, $\forall p \in V_i (2 \le i \le n)$, the following results are true for the digital PLCM (1):*

1. When $G_n(\cdot) = \text{round}_n(\cdot)$, $P_j = \begin{cases} 4/2^j, & i \le j \le n \\ 4/2^i, & j = i-1 \\ 1/2^j, & 1 \le j \le i-2 \end{cases}$;
2. When $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$, $P_j = \begin{cases} 4/2^j, & i \le j \le n \\ 1/2^j + 2/2^i, & 1 \le j \le i-1 \end{cases}$;
3. $\forall k \in [0, 2^{n-i} - 1], P\left\{\text{floor}_{n-i}(F_n(x,p)) = k/2^{n-i}\right\} = 1/2^{n-i}$.

Proof. the first two parts are the combinations of Theorem 3 and 4, the last part is just equivalent to Theorem 2.

Remark 1. If x distributes uniformly in the digital set S_n, $F_n(x,p)$ does not distribute uniformly in S_n (but its highest n-i bits does in S_{n-i}, $\forall p \in S_i$), since $P_j = 1/2^j$ if $F_n(x,p)$ distributes uniformly in S_n. To understand what Theorem 5 really means, see Fig. 1 for more visual details.

Remark 2. Note there is an absolutely weak control parameter $p = 1/4 \in V_2 \subset S_2$, which satisfies $P_2 = 4/2^2 = 1$. That is to say, the lowest 2 bits of $F_n(x,p)$ will always be zeros. In addition, $\forall x_0 \in V_i (2 \le i \le n)$, after at most $\lceil i/2 \rceil$ iterations, the chaotic orbit will converge at zero: $\forall m \ge \lceil i/2 \rceil, F^m(x_0) = 0$.

Theorem 6. *Assume random variable x distributes uniformly in S_n, and $P_i = P\{F_n(x,p) \in S_{n-i}\}$. The following results are true for the digital PLCM (1):*

1. $\forall p \in D_{i,1} = S_i - S_1 = \bigcup_{k=2}^{i} V_i$, $P_i = 4/2^i$;
2. $\forall p \in V_{i+1}$, $P_i = 4/2^{i+1}$;

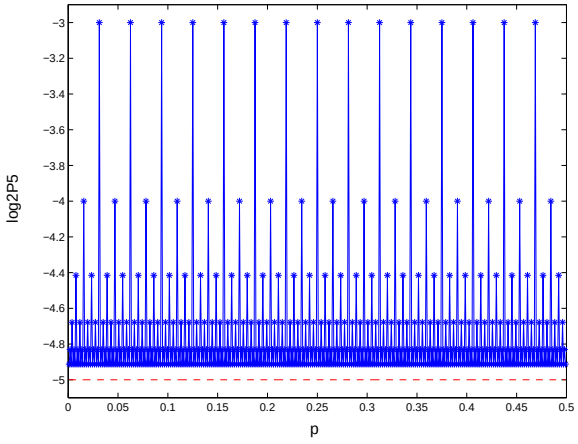


Fig. 2. $P_5 = P\{F_n(x,p) \in S_{n-5}\}$ with respect to p, where $n = 10, G_n(\cdot) = \text{floor}_n(\cdot)$ (The dashed line denotes 2^{-5}, the ideal probability under digital uniform distribution)

3. $\forall p \in V_j (j \geq i+2)$, $P_i = \begin{cases} 1/2^i & , G_n(\cdot) = \text{round}_n(\cdot) \\ 1/2^i + 2/2^j & , G_n(\cdot) = \text{floor}_n(\cdot) \text{ or } \text{ceil}_n(\cdot) \end{cases}$.

Proof. This theorem is an equivalent form of Theorem 5.

Remark 3. Theorem 6 tells us: for the control parameters p with different resolution (i.e., in different digital layers of $D_{n,1}$), rather large difference exists in the generated chaotic orbits. Hence, from the observation of $P_1 \sim P_n$, one can get the resolution of the control parameter p. In Fig. 2, we give the experimental result of P_5 with respect to p when $n = 10$ and $G_n(\cdot) = \text{floor}_n(\cdot)$, which entirely coincides with Theorem 6.

4.5 Extension to Other Digital PLCM-s

Although the above results are based on the specific PLCM denoted by (1), they can be essentially extended to all PLCM-s described in Sect. 3.1, of course the exact results will be different for different maps. From the proofs of theorems in above sub-sections, we can see that the statistical degradation occurs because of the piecewise linearity (Lemma 3 and 4) and the essential properties of the three ATF-s (Lemma 1 and 2). Employing Lemma 1–4 and Corollary 1–2 on other PLCM-s[9], we can easily obtain results corresponding to Theorem 5 and 6. For example, we can get the results about the following chaotic map:

$$F(x,p) = \begin{cases} x/p & , x \in [0,p) \\ (1-x)/(1-p) & , x \in [p,1] \end{cases}, \tag{19}$$

[9] Any PLCM defined on interval $[\alpha, \beta]$ can be re-scaled to its topologically conjugated PLCM defined on $[0,1]$ with a linear function $h(x) = (x-\alpha)/(\beta-\alpha)$.

where p satisfies $0 < p < 1$. This map is one of the simplest PLCM-s, and generally called **tent map**.

Theorem 5′. *Assume random variable x distributes uniformly in S_n, $\forall p \in V_i (1 \le i \le n)$, the following results are true for digital tent map:*

1. When $G_n(\cdot) = \mathrm{round}_n(\cdot)$, $P_j = \begin{cases} 2/2^j & , \quad i \le j \le n \\ 2/2^i & , \quad j = i-1 \\ 1/2^{j-1}, & 1 \le j \le i-2 \end{cases}$;
2. When $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ or $\mathrm{ceil}_n(\cdot)$, $P_j = \begin{cases} 2/2^j & , \quad i \le j \le n \\ 1/2^j + 1/2^i, & 1 \le j \le i-1 \end{cases}$;
3. $\forall k \in [0, 2^{n-i} - 1], P\{\mathrm{floor}_{n-i}(F_n(x,p)) = k/2^{n-i}\} = 1/2^{n-i}$.

Experiments show the results absolutely right. Of course there is the corresponding Theorem 6′, we omit it here since it is just another form of Theorem 5′.

5 The Roles of Digital PLCM-s in Cryptography and Pseudo-Random Coding

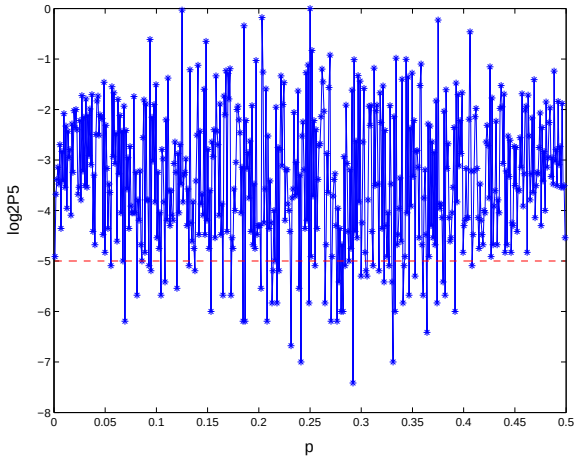


Fig. 3. $P_5' = P\{F_n^{32}(x,p) \in S_{n-5}\}$ with respect to p, where $n = 10, G_n(\cdot) = \mathrm{floor}_n(\cdot)$ (P_5' is the probability after 32 chaotic iterations of the digital PLCM (1), the dashed line denotes 2^{-5}, the ideal probability under digital uniform distribution)

From *remark 1*, we can know that a uniformly distributed digital signal will lead to non-uniform distribution after iterations of a digital PLCM. Such non-uniformity will become more and more severe as the iterations go, see Fig. 3 for some intuitional view (compare it with Fig. 2, the probability at most control parameters increases, and the probability at $p = 1/16$ even reaches to 1). We

can use the probability P_i to denote the degree of such non-uniformity: for a fixed control parameter, the larger P_i is, the larger the degradation will be. In *remark 2*, $p = 1/4 \in V_2$ corresponds to the most serious degradation, so it is the weakest control parameter. The less weak control parameters are ones in V_3; then those in V_4, V_5, $\cdots$.

5.1 Performance of the Three Remedies to Digital PLCM-s

In Sect. 1, we have mentioned three remedies proposed by other researchers. In this subsection, we discuss whether they will work well to improve the degradation of digital PLCM-s.

Apparently, cascading multiple digital chaotic maps cannot essentially improve the weaknesses, since multiple cascading PLCM-s are just equivalent to a new PLCM with more segments.

Using higher precision cannot change the weaknesses of any fixed control parameter either. For example, for the map (1), $p = 1/4$ will always be absolutely weak for any finite precision, and $\forall p \in V_i$ will always be same weak for any finite precision $n \geq i$. But higher precision will introduce more stronger digital layers[10] and then improve the overall weakness, which makes the condition better.

Now assume the perturbation-based algorithm is used to improve the degradation of digital PLCM-s. We find there exists a "strange" paradox: assume the chaotic orbit $\{x(m)\}_{m=1}^{\infty}$ is improved to obey nearly uniform by perturbation, according to Theorem 5 and 6, the chaotic sub-orbit $\{x(m)\}_{m=2}^{\infty}$ will not obey uniform distribution because $\{x(m)\}_{m=2}^{\infty} = \{F_n(x(m), p)\}_{m=1}^{\infty}$; thus $\{x(m)\}_{m=1}^{\infty}$ will not either. What does such a fact mean? It implies the non-uniformity revealed by the above theorems is the lower bound of the degradation of digital chaotic orbits. In other words, the perturbation-based algorithm cannot **essentially** improve the degradation to a better condition than the one depicted in Theorem 5 and 6. However, as we will point out in the next subsection, the perturbation-based algorithm is still useful to enhance the digital chaotic ciphers and pseudo-random coding with careful considerations.

5.2 Notes on Chaotic Ciphers and Pseudo-Random Coding

If the digital PLCM-s are directly used in chaotic ciphers and the control parameter are used as the secret key (as most chaotic ciphers do), the cryptographic properties of the ciphers will not be perfect, and many weak keys will arise (see Fig. 3), because of the severe degradation induced by the digital chaotic iterations.

To escape from such a bad condition and enhance the security, we suggest using the perturbation-based algorithm as follows: the perturbation is **secretly** exerted and the chaotic orbit is output **after** perturbation (See Fig. 4). It is based on the following fact: if $\{x(m)\}_{m=1}^{\infty}$ can be observed by one intruder, he

[10] When finite precision increases from n to n', $n' - n$ stronger digital layers $V_{n'-n+1} \sim V_{n'}$ will be added, although n old digital layers $V_1 \sim V_n$ remain.

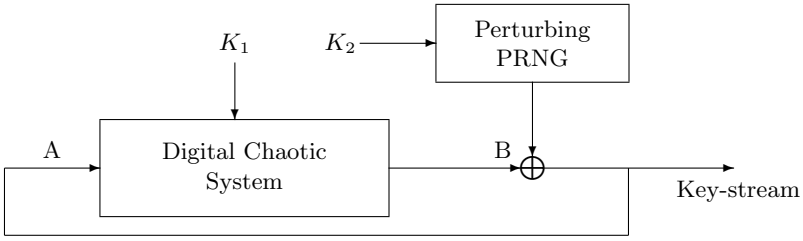


Fig. 4. Digital chaotic cipher with secretly exerted perturbation
(The perturbation should be secretly exerted at position B not A)

will probably judge the resolution i of the right key through the probabilities $P_j(j = 1 \sim n)$ (see Theorem 6 and *Remark 3*), and then search the key only in the digital layer V_i that is smaller than the whole key space (the smaller i is, the faster the search will be and the weaker the key). If the perturbation is exerted secretly at point B, one intruder can only observe perturbed $\{x(m)\}_{m=1}^{\infty}$ not $\{x(m)\}_{m=1}^{\infty}$ itself, then it is relatively more difficult for him to get information about K_1 without knowing K_2. But it is obvious that K_1 will still be weak if K_2 is broken, and vice versa. It means the final key entropy will be smaller than the sum of the two sub ones: $H(K) = H((K_1, K_2)) < H(K_1) + H(K_2)$.

If the digital PLCM-s are used to generate pseudo-random bits, the generated binary sequences may be unbalanced since the chaotic orbits are not uniform. For example, if the map denoted by (1) with $p = 1/4$ is selected and the lowest 2 bits of chaotic orbit are used to generate pseudo-random bits, we can see they will be $000\cdots$. Fortunately, from Theorem 2, we can use the highest n-i bits to construct desired pseudo-random bits. Here please note (approximately) uniform distribution of chaotic input is required. The perturbation-based algorithm will be useful for such a task.

6 Conclusion

We have rigorously proved some statistical properties of digital piecewise linear chaotic maps (PLCM) and explained their roles in chaotic cryptography and pseudo-random coding. Our works will be useful for the design and performance analyses of chaotic ciphers with theoretical security and PRBG-s with really good statistical properties.

For other chaotic maps, our results cannot straightforward be extended. But the proofs made in this paper depend on some essentially properties of ATF-s (Lemma 1 and 2) and the following fact: on every monotonic segment of digital chaotic maps, one control parameter is proportional to the uniformly distributed final output (Lemma 3 and 4). Consider the uniform final output is always desired for cryptography and pseudo-random coding, the proofs may be available for other digital chaotic maps that can be used in the two areas. In the future, we will try to find results concerning more generic digital chaotic maps.

Acknowledgement

The authors wish to thank Dr. Di Shuang-liang at Xi'an Jiaotong University for his valuable suggestions, and Miss Han Lu at Xi'an Foreign Language University for her help in the preparation of the final paper.

Appendix A: The proof of Lemma 1

Proof. We prove the three sub-lemmas separately:

1. Because $a = \lfloor a \rfloor + \mathrm{dec}(a)$, $n \cdot a = n \cdot \lfloor a \rfloor + n \cdot \mathrm{dec}(a)$. Considering $0 \leq \mathrm{dec}(a) < 1$, $0 \leq n \cdot \mathrm{dec}(a) < n \Rightarrow 0 \leq \lfloor n \cdot \mathrm{dec}(a) \rfloor \leq n-1$. From the definition of $\lfloor \cdot \rfloor$, we can get $\lfloor n \cdot a \rfloor = \lfloor n \cdot (\lfloor a \rfloor + \mathrm{dec}(a)) \rfloor = n \cdot \lfloor a \rfloor + \lfloor n \cdot \mathrm{dec}(a) \rfloor \Rightarrow n \cdot \lfloor a \rfloor \leq \lfloor n \cdot a \rfloor \leq n \cdot \lfloor a \rfloor + (n-1)$, where $n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor \Leftrightarrow \lfloor n \cdot \mathrm{dec}(a) \rfloor = 0$, that is to say, $0 \leq n \cdot \mathrm{dec}(a) < 1 \Leftrightarrow \mathrm{dec}(a) \in \left[0, \frac{1}{n}\right)$.

2. i) When $\mathrm{dec}(a) = 0$: $\lceil n \cdot a \rceil = n \cdot a = n \cdot \lceil a \rceil$; ii) When $\mathrm{dec}(a) \in (0,1)$: Assume $\mathrm{dec}'(a) = 1 - \mathrm{dec}(a) \in (0,1)$, then $a = \lceil a \rceil - \mathrm{dec}'(a)$, then $n \cdot a = n \cdot \lceil a \rceil - n \cdot \mathrm{dec}'(a)$. Considering $0 < n \cdot \mathrm{dec}'(a) < n$, $n \cdot \lceil a \rceil - n < n \cdot a = n \cdot \lceil a \rceil - n \cdot \mathrm{dec}'(a) < n \cdot \lceil a \rceil$. From the definition of $\lceil \cdot \rceil$, we can get $n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$, where $n \cdot \lceil a \rceil = \lceil n \cdot a \rceil \Leftrightarrow n \cdot \mathrm{dec}'(a) \in (0,1)$, then $\mathrm{dec}(a) \in (1 - \frac{1}{n}, 1)$. As a whole, we have $n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$, and $n \cdot \lceil a \rceil = \lceil n \cdot a \rceil$ when and only when $\mathrm{dec}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$.

3. From the definition of $\mathrm{round}(\cdot)$, we have $\mathrm{round}(a) - 1/2 \leq a \leq \mathrm{round}(a) + 1/2$. Thus $n \cdot \mathrm{round}(a) - n/2 \leq n \cdot a < n \cdot \mathrm{round}(a) + n/2$. i) When n is an even integer, it is obvious that $n \cdot \mathrm{round}(a) - n/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + n/2$. ii) When n is an odd integer, $n \cdot \mathrm{round}(a) - n/2 + 1/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + n/2 - 1/2$, that is to say, $n \cdot \mathrm{round}(a) - (n-1)/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + (n-1)/2$. As a whole, we can deduce: $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor \leq \mathrm{round}(n \cdot a) \leq n \cdot \mathrm{round}(a) + \lfloor n/2 \rfloor$, where $n \cdot \mathrm{round}(a) = \mathrm{round}(n \cdot a) \Leftrightarrow n \cdot \mathrm{round}(a) - 1/2 \leq n \cdot a < n \cdot \mathrm{round}(a) + 1/2$, that is to say, $\mathrm{dec}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$.

The proof is complete.

Appendix B: The proof of Lemma 2

Proof. Because $a = \lfloor a \rfloor + \mathrm{dec}(a)$, $\left\lfloor N/2^j \right\rfloor + \left\lfloor N'/2^j \right\rfloor = \left(N/2^j - \mathrm{dec}(N/2^j)\right) + \left(N'/2^j - \mathrm{dec}(N'/2^j)\right)$. Assume $N = n_1 \cdot 2^j + n_2, N' = n_1' \cdot 2^j + n_2'$ and $N + N' = 2^k (k \geq j)$, we have $\mathrm{dec}(N/2^j) = (N \bmod n)/2^j = n_2/2^j, \mathrm{dec}(N'/2^j) = (N' \bmod n)/2^j = n_2'/2^j$. Since N, N' are odd integers, we can get $n_2 > 0, n_2' > 0$. From $2^j | (N+N')$, it is obvious that $n_2 + n_2' = 2^j \Rightarrow \mathrm{dec}(N/2^j) + \mathrm{dec}(N'/2^j) = 1$, thus $\left\lfloor N/2^j \right\rfloor + \left\lfloor N'/2^j \right\rfloor = (N+N')/2^j - 1$. The proof is complete.

References

1. Andrzej Lasota and Michael C. Mackey. *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics*. Springer-Verlag, New York, second edition, 1997.

2. Ljupčo Kocarev, Goce Jakimoski, Toni Stojanovski, and Ulrich Parlitz. From chaotic maps to encryption schemes. In *Proc. IEEE Int. Symposium Circuits and Systems 1998*, volume 4, pages 514–517. IEEE, 1998.
3. Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurcation and Chaos*, 8(6):1259–1284, 1998.
4. R. Brown and L. O. Chua. Clarifying chaos: Examples and counterexamples. *Int. J. Bifurcation and Chaos*, 6(2):219–249, 1996.
5. R. Matthews. On the derivation of a 'chaotic' encryption algorithm. *Cryptologia*, XIII(1):29–42, 1989.
6. Zhou Hong and Ling Xieting. Generating chaotic secure sequences with desired statistical properties and high security. *Int. J. Bifurcation and Chaos*, 7(1):205–213, 1997.
7. T. Habutsu, Y. Nishio, I. Sasase, and S. Mori. A secret key cryptosystem by iterating a chaotic map. In *Advances in Cryptology - EuroCrypt'91*, Lecture Notes in Computer Science 0547, pages 127–140, Berlin, 1991. Spinger-Verlag.
8. Hong Zhou and Xie-Ting Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits and Systems I*, 44(3):268–271, 1997.
9. Sang Tao, Wang Ruili, and Yan Yixun. Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34(9):873–874, 1998.
10. D. D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, XIII(3):243–250, 1989.
11. D. D. Wheeler and R. Matthews. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, XV(2):140–151, 1991.
12. E. Biham. Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91. In *Advances in Cryptology - EuroCrypt'91*, Lecture Notes in Computer Science 0547, pages 532–534, Berlin, 1991. Spinger-Verlag.
13. Ghobad Heidari-Bateni and Clare D. McGillem. A chaotic direct-sequence spread-spectrum communication system. *IEEE Trans. Communications*, 42(2/3/4):1524–1527, 1994.
14. Shin'ichi Oishi and Hajime Inoue. Pseudo-random number generators and chaos. *Trans. IECE Japan*, E 65(9):534–541, 1982.
15. Tohru Kohda and Akio Tsuneda. Statistics of chaotic binary sequences. *IEEE Trans. Information Theory*, 43(1):104–112, 1997.
16. Jorge A. González and Ramiro Pino. A random number generator based on unpredictable chaotic functions. *Computer Physics Communications*, 120:109–114, 1999.
17. A. Baranovsky and D. Daems. Design of one-dimensional chaotic maps with prescribed statistical properties. *Int. J. Bifurcation and Chaos*, 5(6):1585–1598, 1995.
18. Bruce Schneier. *Applied Cryptography – Protocols, algorithms, and souce code in C*. John Wiley & Sons, Inc., New York, second edition, 1996.
19. Julian Palmore and Charles Herring. Computer arithmetic, chaos and fractals. *Physica D*, D 42:99–110, 1990.
20. Zhou Hong and Ling Xieting. Realizing finite precision chaotic systems via perturbation of m-sequences. *Acta Eletronica Sinica*(In Chinese), 25(7):95–97, 1997.
21. Hu Guanhua. *Applied Modern Algebra*. Tsinghua University Press, Beijing, China, second edition, 1999.
22. Pan Chengdong and Pan Chengbiao. *Concise Number Theory*. Beijing University Press, Beijing, China, 1998.
23. The Committee of *Modern Applied Mathematics Handbook*. *Modern Applied Mathematics Handbook – vol. Probability Theory and Stochastic Process*. Tsinghua University Press, Beijing, China, 2000.