On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision

Shujun Li [a,*], Xuanqin Mou [a], Yuanlong Cai [a], Zhen Ji [b] and Jihong Zhang [b]

[a] *School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China*

[b] *College of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, P. R. China*

Abstract

H. Zhou et al. have proposed a chaotic encryption scheme, which is based on a kind of computerized piecewise linear chaotic map (PWLCM) realized in finite computing precision. In this paper, we point out that Zhou's encryption scheme is not secure enough from strict cryptographic viewpoint. The reason lies in the dynamical degradation of the computerized piecewise linear chaotic map employed by H. Zhou et al. The dynamical degradation of the computerized chaos induces many weak keys to cause large information leaking of the plaintext. In addition, we also discuss three simple countermeasures to enhance the security of Zhou's cryptosystem, but none of them can essentially enhance the security.

PACS: 05.45.Vx/Pq

Key words: Chaotic encryption system, Computerized chaos, Piecewise linear chaotic map (PWLCM), Cryptanalysis

1 Introduction

As we know, chaotic systems have many interesting features, such as the sensitivity to the initial condition and control parameter, ergodicity and mix-

⋆ This paper has been published in *Computer Physics Communications*, 153(1):52-58, 2003.

* Corresponding author: Shujun Li (`http://www.hooklee.com`).

ing property [1–3], which have tight relationships with the requirements of pseudo-random coding and cryptography [4,5]. For example, the sensitivity to the initial condition and the mixing property can be connected with confusion and diffusion property of a good cryptosystem [6]. Thus, it is a natural idea to use chaos as a new source to construct new encryption systems.

From 1989, together with the use of analog chaotic systems in the design of secure communication systems [7], applications of computerized (also called digital [8] or discrete-time discrete-value [9]) chaotic systems in cryptography have attracted more and more attention [5, 10–24]. It has been known that many chaotic encryption systems are not secure enough [21, 25–30], especially the early-proposed analog chaotic secure communication approaches [26, 29]. For surveys of the state-of-the-art of chaotic cryptography, please see [5, 7, 9, 20, 31, 32].

In 1996, U. Feldmann et al. proposed a general model for secure chaotic communications, which is called inverse system approach [33]. Soon H. Zhou et al. pointed out some defects of inverse system approach, which make the encryption system not secure from strict cryptographic viewpoint [17]. As a resolution, H. Zhou et al. suggested an enhanced chaotic encryption model of inverse system approach [17,18]. Different from the Feldmann's model, Zhou's enhanced model is based on a kind of computerized piecewise linear chaotic map (PWLCM) realized in finite computing precision.

In this paper, we point out that Zhou's chaotic cryptosystem is either not secure enough from strict cryptographic viewpoint. The reason lies in the dynamical degradation of the computerized PWLCM employed in [17,18]. Such dynamical degradation destroys the uniform distribution of the key-stream generated from the chaotic iterations of the PWLCM, and introduces many weak keys that cause large information leaking. In addition, three simple countermeasures are also discussed to enhance the security of Zhou's cryptosystem, but it is found that none of them can essentially enhance its security. To estimate the security of chaotic cryptosystems, further studies are wanted.

2 Zhou's chaotic encryption scheme

Zhou's scheme is based on a computerized one-dimensional PWLCM realized with finite computing precision [17, 18]. The PWLCM can be denoted by the

following equation (see also Fig. 1):

$$T(x(t),p)=\begin{cases} x(t)/p & 0\le x(t)<p \\ (x(t)-p)/(\frac{1}{2}-p) & p\le x(t)<\frac{1}{2} \\ T(1-x(t),p) & \frac{1}{2}\le x(t)\le 1 \end{cases}, \tag{1}$$

where p is the control parameter and $0<p<\frac{1}{2}$.

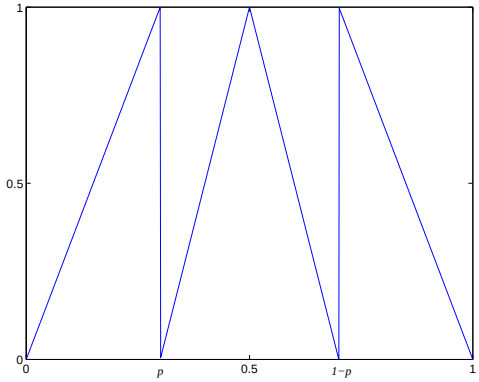


Fig. 1. The PWLCM used by H. Zhou et al. in [17, 18]

The chief chaotic cryptosystem based on Zhou's scheme is as follows:

$$\begin{aligned} &\text{Encryption: } y(t)=[u(t)+T^m\left(y(t-1),p\right)] \pmod 1, \\ &\text{Decryption: } u(t)=[y(t)-T^m\left(y(t-1),p\right)] \pmod 1, \end{aligned} \tag{2}$$

where $u(t)$ is the plaintext, $y(t)$ is the ciphertext and p is the secret key. As H. Zhou et al. stated, the chaotic map (1) should be realized with L-bit finite precision. The finite precision $L<m$ is needed to avoid recovery of the secret key p from plaintext/ciphertext pairs. It is claimed that such an enhanced chaotic encryption scheme can avoid the defects of chaotic cryptosystems based on the original inverse system approach and therefore provide higher security. But we will point out that such a statement is not "entirely" true, because of the dynamical degradation of the computerized PWLCM.

3 Dynamical degradation of computerized chaotic systems

From the work of [34], we know that the PWLCM (1) has uniform invariant density function and δ-like correlation. In addition, it can be easily realized by both hardware and software, since its iterations only involve divisions and additions. It seems that this PWLCM (1) is rather good to construct chaotic cryptosystems [6]. However, it has been found that the dynamical properties

of chaotic systems will decay badly when they are realized with finite computing precision [3,8,27,35–37]. The related problems include short-cycle-length, degraded distribution and correlation of the computerized chaotic orbits, etc. Such problems have not been carefully considered by H. Zhou et al. in [17,18].

In the following, following the analytic idea used in [8], let us see how the dynamical degradation occurs for computerized chaotic systems. Consider a one-dimensional chaotic system $T : X \to X$ defined on $X = [0, 1)$, such as the PWLCM (1). When such a chaotic system is realized with L-bit finite precision, the chaotic iterations will be confined in the following discrete set

$$S_L = \left\{ x \left| x = \sum_{i=1}^{L} a_i 2^{-i}, a_i \in \{0, 1\} \right. \right\} \subset [0, 1), \tag{3}$$

whose size is 2^L. Thus, the computerized (digital) chaotic system $T_L(\cdot) : S_L \to S_L$ can be denoted as a composite function of $D_L(\cdot)$ and $T(\cdot)$:

$$T_L(x) = D_L\left(T\left(x, p\right)\right) = D_L \circ T(x, p), \tag{4}$$

where $D_L : [0, 1) \to S_L$ is a function that transforms a real number to a discrete element in S_L. Generally speaking, for most computer algorithms, D_L is one of the following three functions [1]: $\text{floor}_L(x) = \left\lfloor x \cdot 2^L \right\rfloor / 2^L$, $\text{round}_L(x) = \text{round}\left(x \cdot 2^L\right) / 2^L$ and $\text{ceil}_L(x) = \left\lceil x \cdot 2^L \right\rceil / 2^L$.

For the computerized chaotic map T_L, there are two crucial problems about the dynamical degradation: 1) The control parameters, initial conditions and chaotic orbits can only be represented and stored as elements in S_L. Hence, each chaotic orbit will lead to a fixed point or a n-length cycle finally [38], where $n < 2^L$ is absolutely right and $n \ll 2^L$ almost everywhere. The diagram of computerized chaotic iterations is given in Fig. 2, where $l + n \ll 2^L$ is satisfied for almost every chaotic orbit. Numeric simulations have found that the maximal length of the computerized chaotic orbits is $O(2^{\varepsilon L})$, where $0 < \varepsilon < 1$ (and $1/\varepsilon \gg 1$ is right for many chaotic systems [39]). 2) $D_L(\cdot)$ will introduce small quantization errors to perturb the real-valued chaotic orbits to the discretized ones in S_L. Since the chaotic systems are very sensitive to small errors of initial conditions, the dynamical properties of the computerized orbits will be far different from the ones of real-valued orbits [3].

Generally speaking, it is very difficult to exactly analyze the dynamical properties of computerized chaotic maps. Fortunately, with the help of statistical experiments, we still can make qualitative analyses. In addition, for the

[1] In [8], D_L is called a *digital approximate transformation function (DATF)*. In [3, Chapter 5], $T_L(\cdot)$ is considered as a 2^{-L}-discretized (perturbed) chaotic map, and D_L is called an *operator of* 2^{-L}*-discretization*. This paper uses the concept of [8].

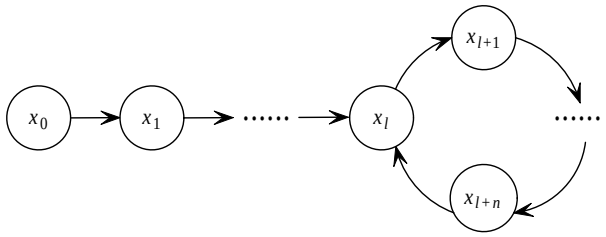


Fig. 2. Computerized chaotic iterations with finite precision

PWLCM (1) used by H. Zhou et al., there exist some useful theoretical results proved in [8], which can be used to qualitatively explain the problems of Zhou's encryption scheme. In the following section, we will point out some facts about the dynamical degradation of the computerized PWLCM (1), and analyze its negative influence on the security of Zhou's encryption scheme (2).

4 Dynamical degradation of the PWLCM (1) and problems with Zhou's encryption scheme

Firstly, let us give a simple example to show how the dynamical degradation of the PWLCM (1) makes Zhou's cryptosystem (2) insecure. Without loss of generality, assume $D_L(\cdot) = \text{floor}_L(\cdot)$, and the finite precision is $L = 8$. When $p = 3/8$, $y(t-1) = 1/16$, we can easily calculate that $T_L^9(y(t-1), p) = 0$. Since $m \geq L + 1 = 9$, $T_L^m(y(t-1), p) = T_L^9(y(t-1), p) = 0$. Hence,

$$y(t) = \lfloor u(t) + T_L^m\left(y(t-1), p\right) \rfloor \pmod 1 = u(t). \tag{5}$$

That is to say, the plaintext $u(t)$ is directly output without encryption by Zhou's cryptosystem. Further experiments show that $y(t) = u(t)$ holds for 114 values in total 256 values of $y(t-1) \in S_L$. Such a possibility of information leaking ($114/256 \approx 44.5\%$) will make the ciphertext-only attack and known-plaintext attack feasible. Thus, we can see $p = 3/8$ is a very weak key. Such a serious problem is induced by the dynamical degradation of the computerized PWLCM (1), considering $Pr[T^m(x, p) = 0] = 0$ for the real-valued version of the chaotic map (1) since its invariant density function is $f(x) = 1$ [34].

Then let us investigate how many weak keys there are in Zhou's encryption scheme under L-bit finite precision. Rigorously, for a secret key p, if the probability of $y(t) = u(t)$ is larger than 2^{-L}, it can be regarded as a weak key. The larger the probability is, the weaker the key will be. To measure the weakness level of a given key p, define the *weak factor* $\alpha(L, m, p)$ as follows:

$$\alpha(L, m, p) = Pr\left[T_L^m\left(y(t-1), p\right) = 0\right] \Big/ 2^{-L}. \tag{6}$$

Here, $\alpha(L, m, p) > 1$ indicates p is a weak key; and the larger $\alpha(L, m, p)$ is, the

weaker the key will be. In addition, when $T_L^m(y(t-1),p)$ distributes uniformly in S_L, $\alpha(L,m,p)=1$ (i.e., $Pr\left[T_L^m(y(t-1),p)=0\right]=2^{-L}$), so $\alpha\left(L,m\right)$ also can partially reflect the non-uniformity of the distribution of $T_L^m(y(t-1),p)$ in S_L. From (6), we can easily get $m_1>m_2 \Rightarrow \alpha\left(L,m_1\right) \geq \alpha\left(L,m_2\right)$, and then we can derive that $\alpha(L,L+1,p)$ is the lower bound of $\alpha(L,m,p)$ for all values of m. Thus, in the following context, we assume $m=L+1$ to make the experiments (in fact, $m=L+1$ is also the optimal value of Zhou's cryptosystem since larger m implies more heavy computation).

When $L=8$ and $D_L(\cdot)$ is respectively $\mathrm{floor}_L(\cdot)$, $\mathrm{ceil}_L(\cdot)$ and $\mathrm{round}_L(\cdot)$, Fig. 3 gives the value of $\log_2(\alpha(L,L+1,p))$ with respect to the secret key p. From the experimental data, we can find the following facts:
Fact 1) $\alpha(L,L+1,p)>1$ almost everywhere, and many keys are rather weak since $\alpha(L,L+1,p)\gg 1$.
Fact 2) The weakest key is $p=1/4$, which makes $\alpha(L,L+1,p)=2^8$ so that $Pr[y(t)=u(t)]=1$ (cipher disappears!).
Fact 3) The number of weak keys when $D_L(\cdot)=\mathrm{round}_L(\cdot)$ is less than the number when $D_L(\cdot)=\mathrm{floor}_L(\cdot)$ and $D_L(\cdot)=\mathrm{ceil}_L(\cdot)$, so $\mathrm{round}_L(\cdot)$ can provide better security than $\mathrm{floor}_L(\cdot)$ and $\mathrm{ceil}_L(\cdot)$.

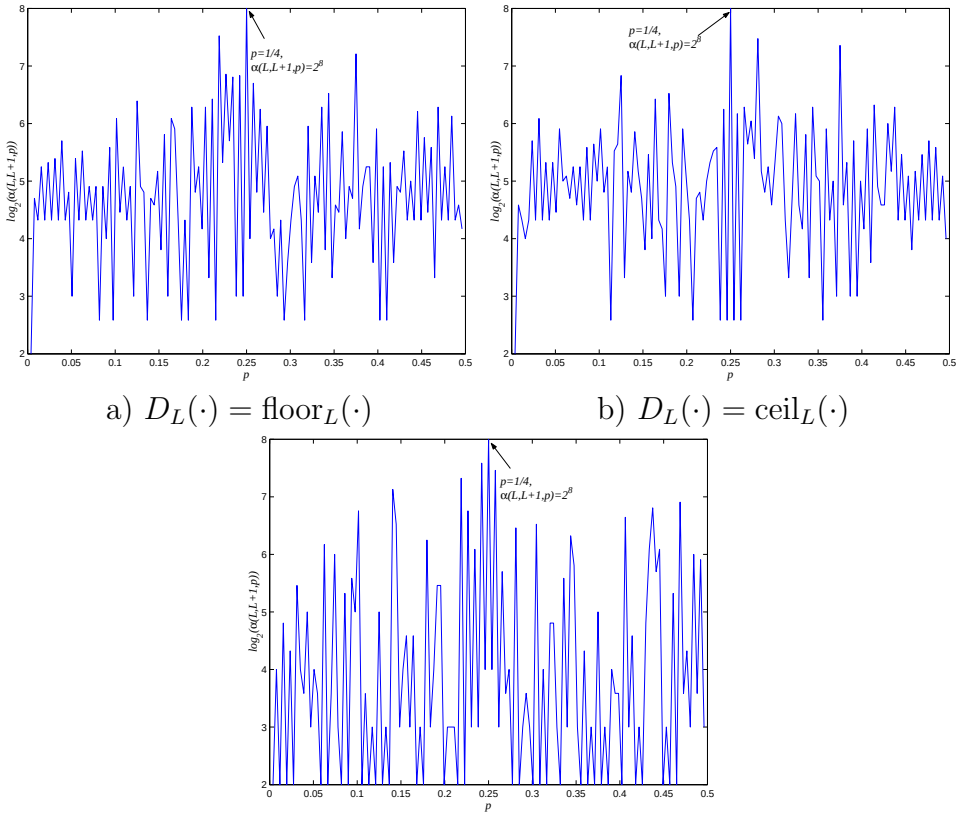
The last fact is natural since $\mathrm{round}_L(\cdot)$ can introduce smaller quantization errors than $\mathrm{floor}_L(\cdot)$ and $\mathrm{ceil}_L(\cdot)$. Apparently, the existence of many weak keys implies that Zhou's chaotic cryptosystem (2) is not secure enough from strict cryptographic viewpoint.

With the theoretical results proved in [8], the above experiments about $\alpha(L,L+1,p)$ can be qualitatively explained. In [8], aiming at the same chaotic map (1), we rigorously studied the relationship between the control parameter p and the probability $P_i=Pr[T_L(x,p)\in S_{L-i}]$ $(i=1\sim L)$. It is obvious that $\alpha(L,1,p)=P_L/2^{-L}$ (assume $S_0=\{0\}$ [8]). As a result, we get the following interesting theorem (define $V_0=S_0, V_i=S_i-S_{i-1}$ [8]):

Theorem 1 (Theorem 6 in [8]) *Assume a random variable x distributes uniformly in S_L, and $P_i=Pr[T_L(x,p)\in S_{L-i}]$. The following results are true for the digital PWLCM (1) $T_L(x,p)$:*

(1) $\forall p\in D_{i,1}=S_i-S_1=\bigcup_{k=2}^{i}V_i$, $P_i=4/2^i$;
(2) $\forall p\in V_{i+1}$, $P_i=4/2^{i+1}$;
(3) $\forall p\in V_j(j\geq i+2)$, $P_i=\begin{cases} 1/2^i & , G_n(\cdot)=\mathrm{round}_n(\cdot) \\ 1/2^i+2/2^j & , G_n(\cdot)=\mathrm{floor}_n(\cdot) \text{ or } \mathrm{ceil}_n(\cdot) \end{cases}$.

This theorem shows that the dynamical degradation of the computerized PWLCM (1) can be measured by the *resolution* of the control parameter p, where the *resolution* is defined as follows [8]: if $p\in V_i$, then its resolution is i (in fact, the resolution is determined by the position of the least significant bit



a) $D_L(\cdot) = \text{floor}_L(\cdot)$ b) $D_L(\cdot) = \text{ceil}_L(\cdot)$

c) $D_L(\cdot) = \text{round}_L(\cdot)$

Fig. 3. $\log_2(\alpha(L, L+1, p))$ with respect to p, where $L = 8$

of p). Generally speaking, the smaller the resolution of p is, the more serious the dynamical degradation will be. Following such a statement, the weakest key will be $p = 1/4$ since it has the smallest resolution $i = 2$, which agrees with Fact 2 obtained from the experimental data in Fig. 3.

Of course, because $m > L > 1$, the rigorous result about P_i and the resolution of p cannot directly extend to explain the value of $\alpha(L, m, p) = Pr[T_L^m(x, p) = 0]/2^{-L}$ with respect to p. Observe Fig. 3, besides the control parameters with small resolutions, we can see some ones with large resolutions also become very weak, such as $p = 29/128$ and $p = 31/128$ (both with the resolution of $i = L - 1 = 7$). It means the dynamical degradation of computerized chaotic systems will become more and more serious and complicated as m increases.

5 How to improve Zhou's encryption scheme?

In the last section, we have shown that there are many weak keys in Zhou's cryptosystem to cause large information leaking. Can we use some countermeasures to enhance its security? In this section, we will discuss three simple

remedies and their performances. As a result, we find that none of them can essentially improve the security.

Using higher finite precision: This is the simplest way to improve Zhou's encryption scheme. But experiments show that the weak keys cannot be improved rapidly as the finite precision L increases. In Fig. 4, some results are given for $p = 3/8$, $1/16$ and $13/64$ when $L = 6 \sim 19$. We can see that $\alpha(L, L+1, p)$ becomes larger and larger in general as L increases. Actually, from the theoretical results proved in [8], we have known that the control parameter p will not become stronger when the finite precision L increases because its resolution i does not change at all for any precision $L \geq i$. Then how the condition will be if we avoid using some weak keys (such as all keys with resolution $i \leq L/2$)? Consider there is not an exact method to distinguish all weak keys (recall $p = 29/128$ and $p = 31/128$ when $L = 8$ and $D_L(\cdot) = \text{floor}_L(\cdot)$), it becomes rather difficult to avoid using all weak keys. Consequently, the security of Zhou's encryption scheme cannot be essentially improved by using larger L.

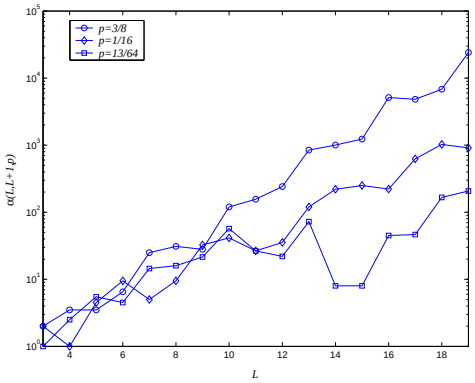


Fig. 4. $\alpha(L, L+1, p)$ with respect to $L = 6 \sim 19$ (logarithmic Y-axis is used)

Realizing the computerized chaotic systems via pseudo-random perturbation: As a practical solution to the dynamical degradation of computerized chaotic systems, some researchers have suggested realizing computerized chaotic systems via pseudo-random perturbation [35–37]. Experiments have shown that such a simple remedy can improve the dynamical properties of computerized (digital) chaos to some extent. However, for the PWLCM (1), in [8] we have pointed out that the pseudo-random perturbation should be **secretly** exerted on the computerized chaotic system to avoid the exposing of the resolution of the secret key p. What's more, the dependence of the resolution of p on the secretly-exerted perturbation will make the final key entropy smaller than the sum of the two sub-entropies. That is to say, Zhou's encryption scheme cannot be essentially improved by this method, either.

Employing other chaotic maps: As we know, many different chaotic systems have been used to construct chaotic cryptosystems. If we use other

chaotic maps to replace the PWLCM (1), how about the security of the modified cryptosystem? A class of piecewise nonlinear chaotic maps introduced in [19] can be considered as possible candidates:

$$F(x) = \begin{cases} \frac{1}{a_i}\left(\sqrt{4a_i\left(\frac{x-c_i}{c_{i+1}-c_i}\right)+(1-a_i)^2}-1\right) & , x \in [c_i, c_{i+1}) \\ 1 & , x = 1 \\ F(-x) & , x \in [-1, 0) \end{cases}, \quad (7)$$

where $0 = c_0 < c_1 < \cdots < c_N = 1$, $a_i \in (-1, 0) \cup (0, 1)$ and $\sum_{i=0}^{N-1}(c_{i+1}-c_i)\cdot a_i = 0$. It has been proved that the above maps also have uniform invariant density functions $f(x) = 0.5$ [19], which is a significant property of the PWLCM (1) used in Zhou's encryption scheme. Are such maps OK? It is rather hard to give the right answer. It has been reported that the dynamical degradation of the computerized PWLCM (1) also exists in many different computerized chaotic maps [27,35,36,39]. Theoretically speaking, the dynamical degradation cannot be avoided for any computerized chaotic system (recall the discussion in Sec. 3). Because there is not yet an established theory to measure the exact dynamical properties of computerized chaotic systems, it is rather difficult to select a "really" better chaotic map than the PWLCM (1) to improve the security of Zhou's encryption scheme. In the future, more studies on computerized chaos should be made to answer this question.

6 Conclusion

This paper points out that a chaotic encryption scheme proposed by H. Zhou et al. [17, 18] is not secure enough, because of the dynamical degradation of the computerized chaotic map (1) used in the cryptosystem. Three simple countermeasures to enhance the chaotic cryptosystem are also discussed, but none of them can essentially improve the security. To design a "really" secure encryption system using computerized chaotic systems, more extensive works should be done to exploit the dynamical degradation of computerized chaos.

Acknowledgements

This work was supported by a grant from the National Natural Science Foundation of China (No. 30070225), and supported by a grant from the National High Technology Research and Development Program of China ("863" Program) during the 10th Five-Year Plan Period (No. 2001AA114152).

References

[1] A. Lasota, M. C. Mackey, Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics, 2nd Edition, Springer-Verlag, New York, 1997.

[2] Hao Bai-Lin, Starting with Parabolas: An Introduction to Chaotic Dynamics, Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993.

[3] M. Blank, Discreteness and Continuity in Problems of Chaotic Dynamics, Vol. 161 of Translations of Mathematical Monographs, American Mathematical Society, Providence, Rhode Island, 1997.

[4] R. Brown, L. O. Chua, Clarifying chaos: Examples and counterexamples, Int. J. Bifurcation and Chaos 6 (2) (1996) 219–249.

[5] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcation and Chaos 8 (1998) 1259–1284.

[6] B. Schneier, Applied Cryptography – Protocols, algorithms, and souce code in C, 2nd Edition, John Wiley & Sons, Inc., New York, 1996.

[7] G. Alvarez, G. P. F. Monotoya, M. Romera, Chaotic cryptosystems, in: Proc. IEEE 33^{rd} Annual Int. Carnahan Conf. Security Technology, IEEE, 1999, pp. 332–338.

[8] S. Li, Q. Li, W. Li, X. Mou, Y. Cai, Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding, in: Cryptography and Coding–8th IMA Int. Conf. Proc., Lecture Notes in Computer Science 2260, Springer-Verlag, 2001, pp. 205–221.

[9] F. Dachselt, W. Schwarz, Chaos and cryptography, IEEE Trans. Circuits and Systems–I 48 (12) (2001) 1498–1509.

[10] R. Matthews, On the derivation of a 'chaotic' encryption algorithm, Cryptologia XIII (1) (1989) 29–42.

[11] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, in: Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science 0547, Spinger-Verlag, Berlin, 1991, pp. 127–140.

[12] M. S. Baptista, Cryptography with chaos, Physics Letters A 240 (1998) 50–54.

[13] W.-K. Wong, L.-P. Lee, K.-W. Wong, A modified chaotic cryptographic method, Computer Physics Communications 138 (2001) 234–236.

[14] G. Jakimoski, L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, IEEE Trans. Circuits and Systems–I 48 (2) (2001) 163–169.

[15] E. Alvarez, A. Fernández, P. García, J. Jiménez, A. Marcano, New approach to chaotic encryption, Physics Letters A 263 (1999) 373–375.

[16] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits and Systems–I 49 (1) (2002) 28–40.

[17] H. Zhou, X.-T. Ling, Problems with the chaotic inverse system encryption approach, IEEE Trans. Circuits and Systems–I 44 (3) (1997) 268–271.

[18] H. Zhou, X.-T. Ling, J. Yu, Secure communication via one-dimensional chaotic inverse systems, in: Proc. IEEE Int. Symposium Circuits and Systems 1997, Vol. 2, IEEE, 1997, pp. 9–12.

[19] S. Tao, W. Ruili, Y. Yixun, The theoretical design for a class of new chaotic feedback stream ciphers, Acta Eletronica Sinica (In Chinese) 27 (7) (1999) 47–50.

[20] L. Shujun, M. Xuanqin, C. Yuanlong, Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography, in: Progress in Cryptology - INDOCRYPT 2001, Lecture Notes in Computer Science 2247, Springer-Verlag, Berlin, 2001, pp. 316–329.

[21] S. Li, X. Mou, Y. Cai, Improving security of a chaotic encryption approach, Physics Letters A 290 (3-4) (2001) 127–133.

[22] S. Li, X. Zheng, X. Mou, Y. Cai, Chaotic encryption scheme for real-time digital video, in: Real-Time Imaging VI, Proceedings of SPIE vol. 4666, 2002, pp. 149–160.

[23] S. Li, X. Mou, Z. Ji, J. Zhang, Y. Cai, Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems, Physics Letters A 307 (1) (2003) 22–28.

[24] S. Li, X. Mou, B. L. Yang, Z. Ji, J. Zhang, Problems with a probabilistic encryption scheme based on chaotic systems, accepted by Int. J. Bifurcation and Chaos, initially scheduled to be published in vol. 13, no. 10, 2003, preprint available online at `http://www.hooklee.com/pub.html`.

[25] M. J. Ogorzatek, H. Dedieu, Some tools for attacking secure communication systems employing chaotic carriers, in: Proc. IEEE Int. Symposium Circuits and Systems 1998, Vol. 4, IEEE, 1998, pp. 522–525.

[26] K. M. Short, Signal extraction from chaotic communications, Int. J. Bifurcation and Chaos 7 (7) (1997) 1579–1597.

[27] D. D. Wheeler, R. Matthews, Supercomputer investigations of a chaotic encryption algorithm, Cryptologia XV (1991) 140–151.

[28] E. Biham, Cryptanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91, in: Advances in Cryptology - EuroCrypt'91, Lecture Notes in Computer Science 0547, Spinger-Verlag, Berlin, 1991, pp. 532–534.

[29] G. Jakimoski, L. Kocarev, Analysis of some recently proposed chaos-based encryption algorihtms, Physics Letters A 291 (6) (2001) 381–384.

[30] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic encryption system, Physics Letters A 276 (2000) 191–196.

[31] L. Kocarev, Chaos-based cryptography: A brief overview, IEEE Circuits and Systems Maganize 1 (3) (2001) 6–21.

[32] R. Schmitz, Use of chaotic dynamical systems in cryptography, J. Franklin Institute 338 (4) (2001) 429–441.

[33] U. Feldmann, M. Hasler, W. Schwarz, Communication by chaotic signals: The inverse system approach, Int. J. Circuit Theory and Applications 24 (5) (1996) 551–579.

[34] A. Baranovsky, D. Daems, Design of one-dimensional chaotic maps with prescribed statistical properties, Int. J. Bifurcation and Chaos 5 (6) (1995) 1585–1598.

[35] J. Černák, Digital generators of chaos, Physics Letters A 214 (3-4) (1996) 151–160.

[36] P. M. Binder, R. V. Jensen, Simulating chaotic behavior with finite-state machines, Physical Review A 34 (1986) 4460–4463.

[37] S. Tao, W. Ruili, Y. Yixun, Perturbance-based algorithm to expand cycle length of chaotic key stream, Electronics Letters 34 (9) (1998) 873–874.

[38] F. Robert, Discrete Iterations: A Metric Study, Springer Series in Computational Mathematics vol. 6, Springer-Verlag, Berlin, 1986.

[39] C. Beck, G. Roepstorff, Effects of phase space discretization on the long-time behavior of dynamical systems, Physica D 25 (1-3) (1987) 95–97.

Figure Captions

Fig. 1 The PWLCM used by H. Zhou et al. in [17, 18]

Fig. 2 Computerized chaotic iterations with finite precision

Fig. 3 $\log_2(\alpha(L, L+1, p))$ with respect to p, where $L = 8$

Fig. 4 $\alpha(L, L+1, p)$ with respect to $L = 6 \sim 19$ (logarithmic Y-axis is used)