PROBLEMS WITH A PROBABILISTIC ENCRYPTION SCHEME BASED ON CHAOTIC SYSTEMS*

SHUJUN LI† and XUANQIN MOU
Institute of Image Processing, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China

BOLIYA L. YANG
Center for Combinatorics, Nankai University, Tianjin 300071, P. R. China

ZHEN JI and JIHONG ZHANG
College of Information Engineering, Shenzhen University, Shenzhen, Guangdong 518060, P. R. China

Recently S. Papadimitrious et al. have proposed a new probabilistic encryption scheme based on chaotic systems. In this letter, we point out some problems with Papadimitrious et al.'s chaotic cryptosystem: 1) the size of the ciphertext and the plaintext cannot simultaneously ensure practical implementation and high security; 2) the estimated number of all possible virtual states is wrong; 3) the practical security to exhaustive attack is overestimated; 4) the fast encryption speed is dependent on the first defect; 5) problems about the dynamical degradation of digital chaotic systems; 6) no explicit indications are given to explain how to construct the virtual state space with the 2^d virtual attractors, the 2^e virtual states and the permutation matrix $\mathbf{P}$. The detailed analyses and discussions on the above problems show that the proposed chaotic cipher is insecure and unpractical. Also, we give our suggestions on the design of general digital chaotic ciphers, and give some open topics in this area.

1. Introduction

It has been well-known that tight relationship exists between chaos and cryptography [Brown & Chua, 1996]. Many fundamental characteristics of chaos, such as ergodicity, mixing property and sensitivity to initial conditions/control parameters [Hao, 1993], can be connected with some cryptographic properties of good ciphers, such as confusion/diffusion, balance and avalanche property [Schneier, 1996]. As a new source of cryptography, chaos has attracted much attention in recent years. Besides secure communication approaches based on chaos synchronization technique [G. Alvarez et al., 1999], the ideas of using *digital* (i.e., *discrete-value discrete-time*) chaotic systems to construct cryptosystems have also been proposed [E. Alvarez et al., 1999; Baptista, 1998; Frey, 1993; Fridrich, 1998; Habutsu et al., 1991; Hong & Xieting, 1997; Jakimoski & Kocarev, 2001a; Kocarev et al., 1998; Kocarev & Jakimoski, 2001; S. Li et al., 2001a, 2002a; Masuda & Aihara, 2002; Matthews, 1989; Papadimitriou et al., 1997, 1999, 2001; L. Shujun et al., 2001; Tao et al., 1998a,b; Zhou & Ling, 1997a]. At the same time, cryptanalytic works of proposed chaotic encryption schemes have been developed and some chaotic ciphers have been known insecure [G. Alvarez et al., 2000; Biham, 1991; Chambers, 1999; Jakimoski & Kocarev, 2001b; S. Li et al., 2001a, 2002c; Wheeler, 1989; Wheeler & Matthews, 1991]. For the recent progress in chaotic cryptography with digital chaotic systems, please see [Dachselt & Schwarz, 2001; Fridrich, 1998; Kocarev et al., 1998; Kocarev, 2001; S. Li et al., 2002b; Schmitz, 2001; Silva & Young, 2000].

In [Papadimitriou et al., 2001], a new chaotic cipher is presented, which is a probabilistic symmetric encryption scheme based on chaotic systems of difference equations. In this letter, we point out some problems with this chaotic cipher. Some problems make Papadimitriou et al.'s chaotic cipher unpractical and insecure, and other ones show that some remedies should be adopted to improve the performance of this chaotic cipher.

This letter is organized as follows. In the next section, we will give a brief introduction of Papadimitriou et al.'s chaotic cipher. Section 3 gives detailed analyses and discussions about the above problems with Papadimitriou et al.'s chaotic cipher. The conclusion is given in the last section.

*This paper has been published in *International Journal of Bifurcation and Chaos*, 13(10):3063-3077, 2003.
†The corresponding author, contact him via his personal web site `http://www.hooklee.com`.

2. Papadimitriou et al.'s Chaotic Encryption Scheme

For the sake of readers' convenience, in this section, we briefly introduce Papadimitriou et al.'s chaotic encryption scheme and the analyses given in their paper. For more details about the original authors' descriptions and analyses, please refer to their own paper.

Papadimitriou et al.'s cipher is a probabilistic symmetric cipher that encrypts d-bit plaintexts into e-bit ciphertexts ($e > d$), whose encryption and decryption procedure can be depicted as follows. Here, please note that we rearrange the processing steps given in [Papadimitriou et al., 2001] to obtain clearer description.

Encryption: **I**) Given a chaotic system to generate a normalized (scaled into the unit $[0, 1]$) chaotic orbit $\{x(n)\}_{i=1}^{\infty}$. **II**) Use $\{x(n)\}_{i=1}^{\infty}$ to construct a *virtual state space*, i.e., a list of 2^d *virtual attractors* containing 2^e *virtual states* $1 \sim 2^e$ as follows: search $1 \sim 2^e$ in the sequence $\{\text{round}(x(n) \cdot 2^e)\}_{i=1}^{\infty}$ until all integers are found with shuffled orders; select 2^d states as the virtual attractors and (pseud-randomly) allocate the left $2^e - 2^d$ states into the 2^d attractors. **III**) Associate each virtual attractor V_a with a message symbol by means of a permutation matrix $\mathbf{P}$. Here, $\mathbf{P}$ is a zero-indexed 1×2^d vector whose elements are 2^d shuffled virtual attractors between 1 and 2^e. **IV**) Encrypt a message $M_c = 0 \sim 2^d - 1$ as follows: firstly map M_c to a corresponding virtual attractor by $V_a = \mathbf{P}[M_c]$, then pseudo-randomly select a virtual state S_{V_a} allocated into V_a as the ciphertext. Apparently, the last step causes this cipher to be a probabilistic symmetric block cipher.

Decryption: **I & II**) Reconstruct the same *virtual state space* using the same method described in step **I & II** of encryption. **III**) Determine $\mathbf{P}$'s "inverse matrix" $\mathbf{P}^{-1}$, which is a one-indexed 1×2^d vector whose elements are $0 \sim 2^d - 1$. $\mathbf{P}^{-1}$ should satisfy the following requirement: $\forall M_c = 0 \sim 2^d - 1$, $\mathbf{P}^{-1}[\mathbf{P}[M_c]] = M_c$. **IV**) Retrieval the attractor V_a in which the ciphertext S_{V_a} is allocated, and then recover the plain-message by $M_c = \mathbf{P}^{-1}[V_a]$.

Assume the association between 2^e virtual states and 2^d virtual attractors as a surjective (multiple-to-one) map $\boldsymbol{F}_v : \boldsymbol{V}_s \rightarrow \boldsymbol{V}_a$, where V_s, V_a respectively represent the set of all virtual states and the set of all virtual attractors. Based on $\boldsymbol{F}_v$, we can conceptually denote Papadimitriou et al. cipher as follows: encryption – $S_{V_a} = \boldsymbol{F}_v^{-1} \circ \mathbf{P}(M_c)$, decryption – $M_c = \mathbf{P}^{-1} \circ \boldsymbol{F}_v(S_{V_a})$. Because $\boldsymbol{F}_v^{-1}$ is not unique, the encryption is probabilistic, while the decryption is deterministic since $\mathbf{P}^{-1} \circ \boldsymbol{F}_v$ is unique.

Papadimitriou et al. adopted the following chaotic systems with difference equations to construct the normalized chaotic orbit: $i = 1, \ldots, K$,

$$x_i(n+1) = \sum_{j=1}^{K} a_{ij} \cdot f_i\left(b_{ij} \cdot x_j(n) \bmod R_i + L_i\right), \quad (1)$$

where $R_i = U_i - L_i$ and $[L_i, U_i]$ is the definition domain of f_i, and the functions f_i $(i = 1 \sim K)$[1] are suggested being *piecewise linear* functions with N break points, because the piecewise linearity is helpful to simplify the implementation and can ensure perfect properties of the above chaotic systems. Since there are K chaotic sub-systems in total, any one sub-orbit or the combination of some of them may be available to generate virtual state spaces for encryption/decryption[2].

On the security of the chaotic cipher, two possible attacks are analyzed in [Papadimitriou et al., 2001]: 1) directly reconstructing the virtual state space; 2) accurately mimicking the chaotic dynamics that leads to the construction of the virtual state space. The complexity of the first attack is calculated based on the estimated number of all possible virtual state spaces, which is derived to be $(k!)^m \cdot k^{n-k \cdot m}$, where $k = 2^d$ is the number of all virtual attractors and $n = 2^e$ is the number of all virtual states (m is the least number of the virtual states allocated in each virtual attractor)[3]. The complexity of the second attack can be calculated using the similar method given in another Papadimitriou et al.'s paper [Papadimitriou et al., 1997, 1999].

Other merits claimed by Papadimitriou et al. include: 1) piecewise linearity of the selected chaotic system makes the computational complexity rather sufficient and the cipher easy to be scaled; 2) experiments show that this cipher can run much faster than many other conventional ciphers, such as DES, IDEA and RC5.

---

[1] In [Papadimitriou et al., 2001], the authors mistook $f_i, i = 1 \sim K$ for $f_i, i = 1 \sim K - 1$.

[2] This issue is not explicitly mentioned by Papadimitriou et al., but the first sub-orbit is used in their C++ codes, which are available upon request to S. Papadimitriou's e-mail address: `stergios@heart.med.upatras.gr`.

[3] In [Papadimitriou et al., 2001], N, K, M are used here, among which N, K are easily confused with the number N and K in Eq. (1). To avoid such a confusion, we use the lowercase formats n, k, m to replace N, K, M in [Papadimitriou et al., 2001].

3. Problems with Papadimitriou et al.'s Chaotic Cipher

In this section, we will point out and give detailed discussions on the following problems with Papadimitriou et al.'s chaotic cipher. In the last subsection, we will also point out some positive points about this chaotic cipher.

1. Paradox exists between the practical implementation and high security: the size of the ciphertext and the plaintext (d and e) should be large enough to ensure high security, while it should be small enough to enable practical implementation.

2. The value of the number of all possible virtual states is deduced by a wrong way.

3. The security analysis given in [Papadimitriou et al., 2001] is inadequate and the security to exhaustive attack is overestimated.

4. The merit of fast encryption speed is dependent on the defect about the values of d and e.

5. When digital chaotic systems are realized in finite precision, the dynamical degradation will arise and some remedy should be employed to improve it.

6. No explicit instructions are given to show how to select the 2^d virtual attractors from the 2^e integers, how to allocate the 2^e virtual states into the 2^d attractors, and how to generate the permutation matrix $\mathbf{P}$.

3.1. *Paradox on the values of d and e*

In Papadimitriou et al.'s cipher, the plaintext size is d and the ciphertext size is e. To provide high security, d and e should be large enough. However, we note that d and e must be small enough to make the construction and storage of the virtual state space practical, considering the following two facts: i) the time consuming on the construction of virtual states space is $O(2^e)$; ii) the number of required memory units to store the constructed virtual state space is $O(2^e)$. Apparently, e cannot be too large, generally, $e > 30$ may be unpractical for the implementation on a PC ($2^{30} = 1$G, so large a number will make the construction of the virtual state space **very very slow** and the storage **impossible** for a PC with less memory than 1G Bytes). In addition, since d and e will not be too large, an eavesdropper can exactly reconstruct the virtual state space to break the cipher once you get $O(2^e)$ ciphertexts and the corresponding plaintexts. That is to say, the cipher is insecure to known-plaintext, chosen-plaintext and chosen-ciphertext attack [Schneier, 1996]. In weaker conditions, it may be possible for an eavesdropper to deceive legal users with faked ciphertexts, if he can get enough (but less than 2^e) plaintexts and the corresponding ciphertexts.

Actually, in conventional cryptography, the kernel task is to design nonlinear bijective maps from the plaintexts to the ciphertexts controlled by a single secret key, where the bijective nonlinear maps play the same role as the virtual state space used in [Papadimitriou et al., 2001]. Generally speaking, the nonlinear maps used to encrypt the plaintext and decrypt the ciphertext are represented by the nonlinear operations of the plaintexts and the secret keys, not pre-calculated in advance like the virtual state space in [Papadimitriou et al., 2001]. Then why not directly use pre-calculated and pre-stored bijective maps? It is because that the representation and storage of the map will become entirely unpractical if the size of the plaintext and the ciphertext is large enough. For example, let us consider DES: the size of the plaintext/ciphertext is 64, it is obviously impossible to represent and store a map from 2^{64} plaintexts to 2^{64} ciphertexts with limited memory units ($2^{64} = 16$GG!!). Here, we would like to cite what B. Schneier written in his book "Applied Cryptography" [1996, Sec. 14.10.7]: *it will be rather easy to design a secure block cipher if you have a HUGE memory device to store HUGE-size S-Boxes.* From such a viewpoint, the basic idea of virtual state space used in Papadimitriou et al.'s cipher is **unpractical** and **insecure**.

3.2. *Wrong deduction of the number of all possible virtual state spaces*

To estimate the security of the proposed cipher to the attack of reconstructing the virtual state space, the number of all possible spaces is deduced to be $(k!)^m \cdot k^{n-k\cdot m}$ by Papadimitriou et al. Based on the above result, it is claimed that the security of the proposed cipher is much higher than many other traditional ciphers, such as DES, IDEA and RSA.

In this subsection, we point out that the deduction given in [Papadimitriou et al., 2001] is not correct and the right number is not $(k!)^m \cdot k^{n-k\cdot m}$. The reason can be explained by the following two problems: 1) the number may be **underestimated** since different mk states may be selected in the first stage; 2) the number may be **overestimated** since some placements are repeatedly enumerated. For the second problem, we can give one example. The following

two placements A and B are same and will be repeatedly enumerated by Papadimitriou et al.'s deduction: all states are allocated into the same attractors for placement A and B, but a state S_{V_a} is allocated in attractor V_a in the **first** stage for placement A, and S_{V_a} is allocated in attractor V_a in the **second** stage for placement B. Since the two problems influence the result in paradoxical ways, the right number may be smaller or larger than $(k!)^m \cdot k^{n-k\cdot m}$.

In the following context, we try to solve this problem in another way. Please note such a fact: the orders of all virtual states allocated into a same attractor cannot influence the decryption of one ciphertext, although it may make the ciphertexts different for a same plaintext. Hence, the number of all possible virtual state spaces can be re-described as the solution of the following combinatorial problem: *place n* ***different*** *balls into k* ***different*** *boxes with at least m balls in each box ($n \geq mk$), how many possible placements are there?*

Then what is the right solution to the above combinatorial problem? In fact, to the best of our knowledge, no explicit solution to this problem has been reported till now, except some special ones (the Stirling's number of the second kind is the special case when $m = 1$ [Yang, 1997]). Assume the number is $g(n)$, the best solution to this problem is a recursive one:

When $n = mk$:

$$g(n) = \binom{mk}{m, m, \cdots, m} = \frac{(mk)!}{(m!)^k}. \tag{2}$$

When $n > mk$:

$$g(n) = \frac{\sum_{t=mk}^{n-1} g(t)\left(k \cdot \binom{n+m-1}{t} - \binom{n+m-1}{t-1}\right)}{\frac{n-mk}{k} \cdot \binom{n+m-1}{n}}. \tag{3}$$

For the deduction of the above solution, please see Appendix. The above solution is utterly different from the one given in [Papadimitriou et al., 2001]. For example, when $n = mk$, the right number should be $\frac{(mk)!}{(m!)^k}$, but the number is $(k!)^m$ as the deduction in [Papadimitriou et al., 2001]. In many cases, the number derived by Papadimitriou et al. is **smaller** than the actual one. Then can we say that the security of Papadimitriou et al.'s cipher may also be underestimated sometimes? The answer is **negative**, which will be explained in the next subsection with more details.

3.3. *Inadequate security analysis*

In the last subsection, we have shown that the number of all possible virtual state spaces $g(n)$ should be the value expressed by Eq. (2) and (3), not $(k!)^m \cdot k^{n-k\cdot m}$ obtained in [Papadimitriou et al., 2001]. In this subsection, we point out that the value of $g(n)$ and the number of all possible secret keys cannot be directly used to show the high security of the proposed cipher as Papadimitriou et al. did in [2001]. It is a natural result of the following four facts **F1**∼**F4**.

F1) *Most virtual state spaces are too "similar" to ensure the high security of the chaotic cipher.* To quantitatively measure the similarity of two different virtual state spaces A, B, we firstly give a notation $d(A, B)$ called the **distance** of A and B as follows: $d(A, B) = \sum_{i=1}^{n} \mathrm{Com}(A_i, B_i)$, where A_i, B_i are the virtual attractors containing the i^{th} virtual states in A, B, and

$$\mathrm{Com}(A_i, B_i) = \begin{cases} 1, & A_i \neq B_i \\ 0, & A_i = B_i \end{cases}. \tag{4}$$

Here, $d(A, B) = 1 \sim n$ represents the number of virtual states allocated into different attractors in A, B. Apparently, the smaller $d(A, B)$ is, the more similar the two virtual state spaces A and B are.

As a result of the property of the distance $d(A, B)$, similar virtual state spaces will generate similar ciphertexts with uniformly distributed plaintexts. Thus, an eavesdropper can use a similar virtual state space instead of the real one to decrypt most plaintexts (the more similar the used one is to the real one, the more plaintexts will be decrypted). To obtain enough high security, the distance between any two available virtual state spaces A,B should be large enough ($d(A, B) = n$ will be really perfect and $d(A, B) \geq n/2$ may be acceptable in many cases), but the number of such "**good**" virtual state spaces will be **much much smaller** than the number given by Eq. (2) and (3).

F2) *Not all possible virtual state spaces can be constructed with the chaotic system (1).* Once the chaotic orbit $\{x(i)\}_{i=1}^{\infty}$ and the algorithm to construct the virtual state space is given, the generated virtual state space will be uniquely determined. The above fact means that the number of all possibly generated virtual state spaces is also controlled by the number of all possible chaotic orbits as well, not only by Eq. (2) and (3). Then what is the number of all possible chaotic orbits? Apparently, it is determined by the number of all possible secret keys, i.e., all possible control parameters and initial conditions.

In Papadimitriou et al.'s cipher, the following control parameters of Eq. (1) are used as the secret keys[4]: $a_{ij}, b_{ij} (i, j = 1 \sim K)$, $R_i, L_i (i = 1 \sim K)$

[4]The initial conditions are not involved as part of the secret

and NK break point values of $f_1 \sim f_K$ (only N break point values if $f_1 = f_2 = \cdots = f_K$)[5]. Assume the computed sensitivities of the above parameters are all 2^{-L} (L is the adopted finite computing precision) and all parameters are confined in $[0, 1]$, we can roughly calculate the number of all possible secret keys[6]: $\mathcal{N}_\mathcal{K} = (K^2 + 2K) \cdot 2^L + K \cdot \prod_{i=0}^{N-1}(2^L - i)/N!$. Generally, $2 < N \ll 2^L$ and $2 < K \ll 2^L$, then $\mathcal{N}_\mathcal{K} \approx K \cdot 2^{LN}/N!$ (when $f_1 = f_2 = \cdots = f_K$, $\mathcal{N}_\mathcal{K} \approx 2^{LN}/N!$).

F3) *Different secret keys may generate the same virtual state space.* This fact is obviously right if $\mathcal{N}_\mathcal{K} > g(n)$. Together with the above fact **F3**, we can see the upper bound of the security of the proposed chaotic cipher should be $\min(g(n), \mathcal{N}_\mathcal{K})$. Thus, although $g(n)$ may be rather HUGE when $n = 2^e$ and $m = 2^d$ are large enough ($d = e = 8$ may be OK), the actual security of Papadimitriou et al.'s cipher will be limited by $\mathcal{N}_\mathcal{K}$. From the approximate value of $\mathcal{N}_\mathcal{K}$ derived in the last paragraph, the key entropy of Papadimitriou et al.'s cipher to exhaustive attack will be about $LN - \log_2(K/N!)$ in general cases, or even smaller than $LN - \log_2(K/N!)$ if d and e are small enough to make $g(n) < \mathcal{N}_\mathcal{K}$.

F4) *Papadimitriou et al.'s chaotic cipher is insecure to the known-plaintext, chosen-plaintext and chosen-ciphertext attacks, because of the defect about the small values of d and e.* This issue has been discussed in Sec. 3.1. We can see the key entropy of Papadimitriou et al.'s cipher to the three attacks will be e, generally, which will be much smaller than $LN - \log_2(K/N!)$.

3.4. *Other problems*

The dependence of the perfectly fast encryption speed on the essential defect about the values of d and e. In Table 2 of [Papadimitriou et al., 2001], a comparison of the encryption speed of the proposed chaotic cipher with some traditional ciphers is given on a Celeron 433 MHz PC with 96 MB RAM. Papadimitriou et al.'s chaotic cipher can run at a very high speed 327.2 Mbps, which is much faster than other ones. The prefectly fast encryption speed can be explained by the following fact: once the virtual state space has been constructed, the encryption and decryption procedure (step **IV**) can be realized by simple *Look-Up-Table* operations. But please keep in mind that this merit owes to the defect that the whole virtual state space must be firstly constructed and then stored in memory, which makes the cipher unpractical and insecure as we have mentioned in Sec. 3.1.

Dynamical degradation of chaotic systems realized in finite computing precision. When chaotic systems are realized in finite precision, their dynamical properties will be far different from the properties of continuous-value systems and some dynamical degradation will arise, such as short cycle length and decayed distribution. This phenomena has been reported and analyzed by many researchers [Binder & Jensen, 1986; Blank, 1997; S. Li et al., 2001b; Palmore & Herring, 1990; Wheeler, 1989; Wheeler & Matthews, 1991]. Essentially speaking, the dynamical degradation can be attributed to the discrete iterations in finite-state machine [Robert, 1986; Waelbroeck & Zertuche, 1999]. Generally speaking, it is rather difficult to exactly analyze such dynamical degradation of digital chaotic systems. But some useful theoretical results have been obtained for some special chaotic systems, such as a class of piecewise linear chaotic maps [S. Li et al., 2001b]. Since the dynamical degradation may worsen the cryptographic properties of Papadimitriou et al.'s chaotic cipher, some remedies must be used to overcome this defect. Fortunately, several engineering methods can be used to fulfill such a task, such as the perturbation algorithms suggested in [Černák, 1996; Tao et al., 1998a,b; Zhou & Ling, 1997b].

The lack of explicit instructions on how to select the 2^d virtual attractors, how to allocate the 2^e virtual states into the 2^d attractors and how to generate **P**. This problem is not so serious since many different pseudo-random coding algorithms can be used to do the above three operations. Of course, different algorithms may lead to different performances on the pseudo-randomness of the selection of the 2^d virtual attractors, the allocation of the 2^e virtual states the permutation matrix **P**. In addition, if we know the algorithm used in the cipher, it may be possible to analyze the generated virtual state space. Such analysis may be useful to develop some new attack whose complexity is less than the exhaustive attack's (at least under some special conditions). Some further research should be made to investigate this issue.

---

keys in [Papadimitriou et al., 2001]. 0.1 is used to initialize $x_1(0) \sim x_K(0)$ in Papadimitriou et al.'s C++ codes.

[5] In [Papadimitriou et al., 2001], the number of break point values of f_i are denoted by N in Sec. 2.2 and by n in Sec. 3. In this letter, we use N at all time.

[6] Papadimitriou et al. didn't give the deduction of $\mathcal{N}_\mathcal{K}$ in [2001] and only referred the readers to their another two previous papers [1997; 1999]. Here, we use a somewhat different way to calculate the value of $\mathcal{N}_\mathcal{K}$.

3.5. *A Concrete Example*

To emphasize the paradox between insecurity and infeasibility of Papadimitriou et al.'s chaotic cipher, now let us give a concrete example for future explanation. Considering the chaotic system is just used to generate the virtual states with higher key entropy, we will use logistic map $f(x) = 4x(1-x)$ instead of the chaotic system suggested in [Papadimitriou et al., 2001], which will not make essential influence on the performance of this cipher. Assume $d = 6, e = 8$, the secret key is the initial condition of logistic map $x_0 = 0.1111$. Without loss of generality, assume $m = 3$, and the 2^d virtual attractors, the allocations of other $2^e - 2^d$ virtual states (i.e., the map $\boldsymbol{F}_v$) and the permutation matrix $\mathbf{P}$ are all pseudo-randomly generated[7] with the control of the embedded system function `rand` initialized by a (secret or public) seed $s = 0.2222$. Here, please note neither x_0 or s is specially chosen to support our negative result. The constructed map $\boldsymbol{F}_v$ (i.e., the association between the virtual states and the virtual attractors) and the permutation matrix $\mathbf{P}$ are respectively shown in Fig. 1 and 2.

For such a encryption system, if we can get enough known/chosen plaintext/ciphertext pairs, it is possible to obtain the unique decryption function $\mathbf{P}^{-1} \circ \boldsymbol{F}_v$. Since d, e is not too large, we can store this function as a look-up table in the computer to decrypt all future ciphertexts. What about the number of required known/chosen plaintexts? In Fig. 3, under the assumption that the plaintext is uniformly distributed in the discrete set $\{0, 1, \cdots, 2^d - 1\}$, we give the experimental result of the relationship between the number of obtained virtual states/attractors and the number of known/chosen plaintexts. We can see $O(2^e)$ plaintexts are enough to obtain all 2^e virtual states (i.e., all possible ciphertexts) and $O(2^d)$ plaintexts are enough to obtain all 2^d virtual attractors. What $O(2^e)$ plaintexts mean? Consider the plaintexts are 6-bit numbers, $O(2^8)$ plaintexts mean only $O(192)$ bytes, which approximates to the length of a short article. Once all 2^e virtual states are obtained, we can reconstruct the ciphertext-plaintext map (i.e., the decryption function) $\mathbf{P}^{-1} \circ \boldsymbol{F}_v$. Apparently, such insecurity defect is induced by the small values of d, e. But if we increase d, e to resist such attacks, the construction and storage of $\boldsymbol{F}_v$ will become impractical either.

Finally, let us see the number of all possible maps

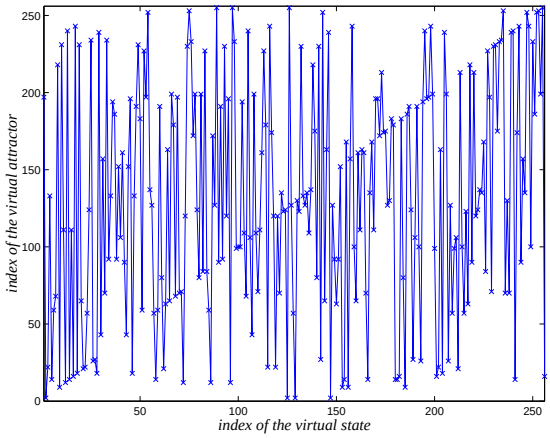

Fig. 1. The association map $\boldsymbol{F}_v$

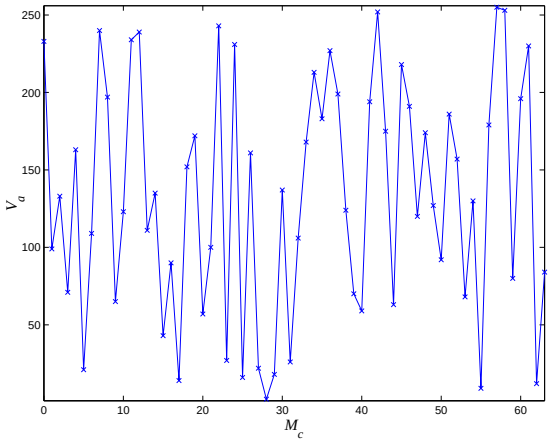

Fig. 2. The permutation matrix $\mathbf{P}$

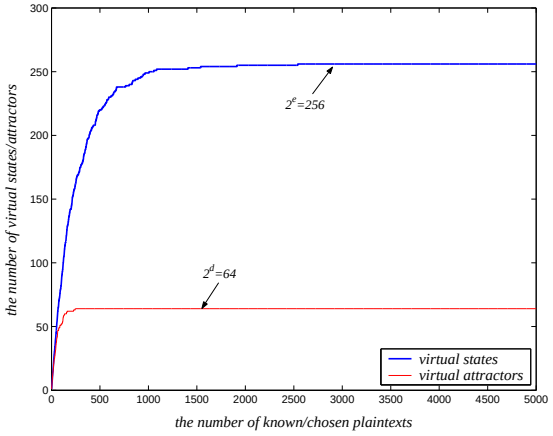

Fig. 3. The number of obtained virtual states from known/chosen plaintexts

$\boldsymbol{F}_v$. When $n = 2^e = 256, m = 3, k = 2^d = 64$, the number of all possible placements of n balls in k boxes (each one at least m balls) is so great that it even cannot be calculated with most scientific computing software: $g(n) \gg 10^{308} \approx 2^{1023}$. However, the number of all possible initial conditions x_0 is generally much much smaller than $g(n)$. When x_0 is a

[7] As we have pointed out in Sec. 3.4, no explicit instructions are given to direct how to generate them.

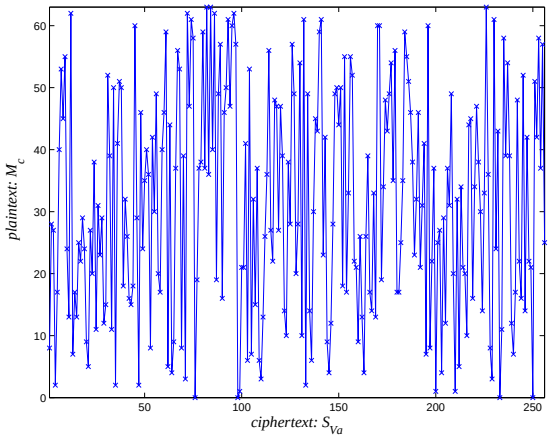

Fig. 4. The reconstructed ciphertext-plaintext map $\mathbf{P}^{-1} \circ \boldsymbol{F}_v$ with $O(2^e)$ known/chosen plaintexts

IEEE-standard 64-bit floating-point decimal [IEEE, 1985], then $\mathcal{N}_k = 2^{62} \ll g(n)$. Thus, the complexity against brute force attack will be $O(\min(g(n), \mathcal{N}_k)) = O(2^{62})$. However, from the analysis in Sec. 3.1 and the above experimental data in this subsection, the complexity against known/chosen plaintext attack is only $O(2^e) = O(2^8) \ll O(2^{62})$.

3.6. *Positive points about Papadimitriou et al.'s chaotic cipher*

Although Papadimitriou et al.'s chaotic cipher has some problems and its general structure is not suitable as a basis to construct more secure chaotic block ciphers, some basic ideas used in the cipher may still be helpful in cryptography.

One useful point is about the possibility to change Papadimitriou et al.'s chaotic cipher from a block cipher to a stream cipher, which may disable the attacks based on the re-construction of the virtual attractors list and the permutation matrix $\mathbf{P}$ (via known/chosen plaintexts). A possible method is to generate time-variant permutation matrix $\mathbf{P}$, or use a stream sub-cipher to confuse the ciphertext of the Papadimitriou et al.'s chaotic cipher. Applications of such an idea in the design of digital chaotic ciphers can be found in [Baptista, 1998; S. Li et al., 2001a, 2002a].

Another point is the idea to construct virtual state space from a chaotic orbit, which can be extended as a new way to generate nonlinear $n \times m$ S-Boxes without trapdoors [Schneier, 1996]. Apparently, such chaotic S-Boxes can be dependent on the secret key, and then be incorporated into some conventional key-driven ciphers to construct new chaos based ciphers. In fact, such cryptosystems based on chaotic S-Boxes have been proposed by some researchers [Jakimoski & Kocarev, 2001a; Kocarev & Jakimoski, 2001; S. Li et al., 2002a], but more detailed studies should be done to analyze the performance of such ciphers.

4. More Discussions on Digital Chaotic Ciphers

As we know, the initial boom of digital chaotic ciphers happened near the year of 1990 (almost together with the occurrence of secure communication approaches based on chaotic synchronization [G. Alvarez et al., 1999]): **Three** papers [Matthews, 1989; Wheeler, 1989; Wheeler & Matthews, 1991] appeared in a same journal – *Cryptologia* and another **three** papers [Biham, 1991; Forre, 1993; Habutsu et al., 1991] appeared in a same conference – EuroCrypt'91. After a short silent period[8], the second boom started from 1997 and lasts till now[9]: many entirely new chaotic ciphers have been proposed and cryptanalyzed, and some reviews have been published to summarize the ideas of using chaos to design cryptosystems [G. Alvarez et al., 1999; Dachselt & Schwarz, 2001; Götz et al., 1997; Kocarev et al., 1998; Kocarev, 2001; Schmitz, 2001; Silva & Young, 2000]. Some discussions on the future research in chaotic cryptography have been given in [Dachselt & Schwarz, 2001; Kocarev, 2001; Schmitz, 2001]. L. Kocarev suggest that the future research should focus on the essential relationships between the chaos and cryptography, not *ad hoc* designs of more and more novel chaotic encryption schemes [Kocarev, 2001]. W. Schwarz et al. have made some research connecting conventional ciphers with chaos [Dachselt & Schwarz, 2001; Götz et al., 1997]. In this section, we would like to show our opinions on the future research about digital chaotic ciphers, based on the contributions and comments of other researchers.

4.1. *Suggestions for the Design of a Good Chaotic Cipher*

Carefully investigate all current known chaotic ciphers, we can give some suggestions on the design of a "good" chaotic cipher, where the term "good" means three aspects of a cipher: high practical security, fast

[8] In that time, a lot of papers are contributed to another similar but different topic: secure communication approaches based on synchronization of analog chaotic circuits.

[9] As our statistics, at least **15** technical papers (most ones are journal articles) have been published since 2001. Please refer to the references list of [S. Li et al., 2002b].

encryption speed and simple implementation.

Suggestion 1 – Realizing digital chaotic systems via pseudo-random perturbation, or using discretized chaotic systems whose dynamical properties have been proven. As we have mentioned, there exists degradation on the dynamical properties of digital chaotic systems realized in finite precision. Under the situation that no systematic theory to measure such degradation, some remedies must be adopted to improve the dynamical properties of digital chaos. The perturbation algorithm by a simple PRNG (such as a m-sequence generator) is suggested by us, since it has considerable performance in practice. The quantized versions of some continuous-value chaotic maps may be also OK, but it is desired that the designers prove (at least "explain with some convincing experimental evidences") their dynamical (i.e., cryptographic) properties.

Suggestion 2 – Avoiding the use of multiple iterations for one ciphertext in chaotic block ciphers. The slow encryption speed of most chaotic block cipher is chiefly induced by the use of multiple iterations for one ciphertext. Some newly proposed chaotic block ciphers [Jakimoski & Kocarev, 2001a; Kocarev & Jakimoski, 2001; S. Li et al., 2002a; Papadimitriou et al., 2001] overcome this problem and can be used as good references.

Suggestion 3 – Using fixed-point arithmetic instead of floating-point arithmetic. Apparently, floating-point arithmetic will lower the encryption speed and increase the realization complexity and cost. Thus, fixed-point arithmetic is suggested. In addition, the fixed-point arithmetic is also helpful to improve the portability between different software platforms or hardware structures. There are another defect about floating-point arithmetic: the floating-point decimals are not distributed uniformly in the discrete space, which will make it much more complicated and difficult to theoretically analyze the degradation of digital dynamical properties. Of course, some chaotic systems cannot realized with fixed-point arithmetic, if they are expressed by complicated functions (such as sine). Such complicated chaotic systems should be avoided as possible in practice (see also the following suggestion).

Suggestion 4 – Using the simplest chaotic systems as possible, piecewise linear chaotic systems are good candidates. Many complicated chaotic systems are usually suggested to ensure the security of developed chaotic ciphers. But the use of complicated chaotic systems will lower the encryption speed twofold: i) the more complicated the chaotic systems are, the more time the chaotic iterations (i.e., the encryption/decryption procedure) will consume; ii) many complicated chaotic systems must run with floating-point arithmetic, which makes the iterations further slower. Generally speaking, we suggest using piecewise linear chaotic systems (such as the class of chaotic maps whose digital dynamical properties has been partially proved in [S. Li et al., 2001b]), from the considerations of security, speed, and implementation. If piecewise linear chaotic maps cannot be used in some applications, choose the simplest chaotic systems that are available.

Suggestion 5 – Using multiple chaotic systems instead of one single one in chaotic stream ciphers. Almost all digital chaotic ciphers are claimed to be secure by the authors when they are proposed, but many of them are actually not. Then what about the security of other "secure" chaotic ciphers? Because of the lack of related theory, no perfect solutions can be found at present. We can only give a useful suggestions: use multiple chaotic systems instead of a single one, since the combination of multiple chaotic systems "should" make the cryptanalysis much more difficult, especially when each chaotic system has different equation and/or different initial condition (and/or control parameters). Such an idea has been used in some chaotic cipher [S. Li et al., 2002a; Protopopescu et al., 1995; L. Shujun et al., 2001] and chaotic spread spectrum communication approaches [Heidari-Bateni & McGillem, 1994], it seems that more perfect performance can be obtained. Also, please note that Papadimitriou et al.'s chaotic cipher also employed multiple chaotic systems to make the cryptanalysis difficult. Of course, to support the correctness and rationality of this suggestion, further investigations are needed.

Suggestion 6 – Avoiding all known weaknesses of previous digital chaotic ciphers. It is natural that we should avoid all security defects that have been reported by cryptanalysts, which is a basic principle widely-acknowledged in cryptology community [Schneier, 1996].

4.2. *Some Open Topics about Digital Chaotic Ciphers*

In [Kocarev, 2001], L. Kocarev suggested that the future research in chaotic cryptography should focus on the relationships between chaos and cryptography, not the *ad hoc* design of new chaotic ciphers. Basically, we agree to their opinion. The following are some open topics in chaotic cryptography. Of course, new structures of chaotic ciphers may still be useful, if some really novel ideas are introduced and better performance is provided.

Theory about chaos in discretized space. To

estimate the dynamical properties of digital chaotic systems, a systematic theory about chaos in discrete space is needed. But such a theory has not been established yet. The most comprehensive discussion on this topic can be found in [Blank, 1997]. In 1999, H. Waelbroeck and F. Zertuche tried to translate the definitions of deterministic chaos to the context of discrete state space (called "discrete chaos"). Some results on the dynamical properties of digital piecewise linear chaotic maps have been given in [S. Li et al., 2001b].

Cryptographical properties of the pseudo-randomness generated by digital chaos. The pseudo-random sequences generated by digital chaos are kernel parts in many chaotic ciphers. How to measure the cryptographical properties of the chaotic pseudo-random sequences is an unsolved problem. In continuous chaos theory, *information entropy* can be used to depict the rate of the information loss as the chaotic systems are iterated [Hao, 1993]. Similar concept may be also used to qualitatively explain the unpredictability of pseudo-random numbers generated by digital chaos, the idea is used in [Bernstein & Lieberman, 1990; L. Shujun et al., 2001]. Of course, more strict analysis is desired. Some theoretical contributions have been done to explore the correlation of pseudo-random bits generated by continuous chaos, such as the work made by T. Kohda and A. Tsuneda in [Kohda & Tsuneda, 1997]. In the future, some theoretical works on cryptographical properties of the pseudo-random sequence generated by digital chaos should be made.

Chaos in conventional ciphers. From essential viewpoint, any conventional cipher can be considered as a chaotic or pseudo-chaotic cipher, since the confusion and diffusion are the basic tools to realize security [Schneier, 1996]. Some chaotic behaviors hiding in conventional ciphers have been reported by W. Schwarz et al. [Götz et al., 1997]. In the future research, answers to the following questions will be useful for the design of both conventional and chaotic ciphers: 1) Can we use chaos theory to explain the nonlinear functions and operations used in conventional ciphers? For example, can the mod function defined on finite filed be considered as a discretized chaotic map[10]? 2) Can we re-define the confusion and diffusion property of a good cipher with chaos theory? 3) Can we find a way to connect the security measurement (such as linear complexity in stream-cipher cryptography) in conventional cryptography with the measurements (such as the information entropy) in chaos theory?

General models for the design of digital chaotic ciphers. Several general models have been proposed in [Jakimoski & Kocarev, 2001a,b; Kocarev et al., 1998; L. Shujun et al., 2001], further efforts on the proposed models will be helpful to exploit the relationship between chaos and cryptography. The idea of combing chaotic block cipher and chaotic stream cipher to construct product cipher is also promising, such as the chaotic ciphers presented in [E. Alvarez et al., 1999; Baptista, 1998; S. Li et al., 2002a].

Cryptanalysis and enhancement of known digital chaotic ciphers. As we know, the recent advances in today's block-cipher cryptology are promoted by the emergence of the differential and linear cryptanalysis, which shows the importance of the cryptanalysis in cryptology [Schneier, 1996]. We believe any new attacks of some chaotic ciphers will impulse the progress of chaotic cryptography. Recently, two similar chaotic cryptosystems proposed in [E. Alvarez et al., 1999; Baptista, 1998] have been cryptanalyzed and improved recently by many researchers [G. Alvarez et al., 2000; García et al., 2002a,b; Jakimoski & Kocarev, 2001b; S. Li et al., 2001a; Wong et al., 2001; Wong, 2002], which reveals a fact that many useful knowledge about how to design a good chaotic cipher can be found in such active arguments.

5. Conclusion

Recently, a new probabilistic symmetric cipher based on chaotic systems has been presented in [Papadimitriou et al., 2001]. In this letter, we point out some defects of this chaotic cipher: 1) d and e are too small to ensure both practical implementation and high security; 2) the deduction of the number of all possible virtual state spaces is wrong; 3) inadequate analysis leads to overestimated security; 4) fast encryption speed is the result of the first defect; 5) dynamical degradation of digital chaotic systems should be remedied; 6) no detailed instructions about the construction of the virtual state space are given.

Generally speaking, because of the small values of d and e, Papadimitriou et al.'s chaotic cipher is unpractical and insecure to known/chosen-plaintext and chosen-ciphertext attack. Its merit of fast encryption speed may disappear if the defect about d and e is cancelled. In addition, from our discussions in Sec. 3.3, the security of the cipher is not so high as analyzed in [Papadimitriou et al., 2001], and the key entropy to exhaustive attack will be not larger than $LN - \log_2(K/N!)$.

[10] Consider the digital tent map realized in fixed-point discrete space.

We believe it is a promising and interesting idea to use digital chaos as the new source of cryptosystems, but more detailed studies should be done on the way to reach a really good digital chaotic cipher.

Acknowledgement

This work was mainly 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).

As a conjunct project of Xi'an Jiaotong University and Nankai University, this work was also supported by the auspices of the Key Laboratory of Pure Mathematics and Combinatorics of the Ministry of Education of China, and the 973 Project on Mathematical Mechanization of the Ministry of Science and Technology of China.

In addition, the authors would like to thank Prof. Richard A. Stong at Rice University, and Dr. Jeb Faulkner Willenbring at Yale University, for their suggestions on the solution to the combinatorial problem in Sec. 3.2. We also thank the valuable comments from anonymous reviewers, which stir our efforts to enhance the content of this letter. At last, we should give special thanks to Yanghui Cao, Ying Chu and Ying Long at Xi'an Jiaotong University for their kindly helps in the preparation of this letter.

Appendix – The Recursive Solution of the Combinatorial Problem in Sec. 3.2

Here, we give the deduction of Eq. (2) and (3).

Assume $g(n)$ is the number of all possible placements with respect to n. Because

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{a_1+a_2+\cdots+a_k=n} \binom{n}{a_1, a_2, \cdots, a_k} x_1^{a_1} x_2^{a_2} \cdots x_k^{a_k}, \tag{5}$$

We have

$$g(n) = \sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \binom{n}{a_1, a_2, \cdots, a_k}. \tag{6}$$

Consider the following exponential generating function:

$$\begin{aligned} \sum_{n\geq mk} g(n)\frac{x^n}{n!} &= \sum_{n\geq mk} \left(\sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \binom{n}{a_1, a_2, \cdots, a_k} \right) \frac{x^n}{n!} \\ &= \sum_{n\geq mk} \left(\sum_{\substack{a_1+a_2+\cdots+a_k=n \\ a_i \geq m}} \frac{n!}{a_1! \cdot a_2! \cdots a_k!} \right) \frac{x^{a_1+a_2+\cdots+a_k}}{n!} \\ &= \left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k . \end{aligned} \tag{7}$$

Consequently, $\left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k$ is the generating function of $g(n)$.

Apparently, it is hard to derive the explicit equation of $g(n)$ denoted by n, m, k, so let us investigate the recursive expression of $g(n)$.

Rewrite Eq. (7) as $\sum_{i\geq mk} g(i)\frac{x^i}{i!} = \left(\sum_{a\geq m} \frac{x^a}{a!} \right)^k$, and solve the derivatives of both sides, we can have:

$$\sum_{i\geq mk-1} g(i+1)\frac{x^i}{i!} = k \cdot \left(\sum_{j\geq m} \frac{x^j}{j!} \right)^{k-1} \cdot \left(\sum_{j\geq m-1} \frac{x^j}{j!} \right), \tag{8}$$

Multiply the both sides of the above equation by $\sum_{j\geq m}\frac{x^j}{j!}$,

$$\begin{aligned}\left(\sum_{j\geq m}\frac{x^j}{j!}\right)\cdot\left(\sum_{i\geq mk-1}g(i+1)\frac{x^i}{i!}\right) &= k\cdot\left(\sum_{a\geq m}\frac{x^a}{a!}\right)^k\cdot\left(\sum_{j\geq m-1}\frac{x^j}{j!}\right)\\ &= k\cdot\left(\sum_{a\geq mk}g(a)\frac{x^a}{a!}\right)\cdot\left(\sum_{j\geq m-1}\frac{x^j}{j!}\right)\end{aligned}. \tag{9}$$

The left hand side (LHS) of Eq. (9) is

$$\begin{aligned}\text{LHS} &= \sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}\left(\frac{g(t+1)}{s!t!}x^i\right)\right)\\ &= \sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}g(t+1)\binom{i}{s}\right)\frac{x^i}{i!}.\end{aligned} \tag{10}$$

The right hand side (RHS) of Eq. (9) is

$$\begin{aligned}\text{RHS} &= k\cdot\sum_{i\geq mk+m-1}\left(\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}\left(\frac{g(t)}{s!t!}x^i\right)\right)\\ &= \sum_{i\geq mk+m-1}k\cdot\left(\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}g(t)\binom{i}{s}\right)\frac{x^i}{i!}.\end{aligned} \tag{11}$$

Thus, we can know the following fact: when $i\geq mk+m-1$,

$$\sum_{\substack{s+t=i\\ s\geq m\\ t\geq mk-1}}g(t+1)\binom{i}{s}=k\cdot\sum_{\substack{s+t=i\\ s\geq m-1\\ t\geq mk}}g(t)\binom{i}{s}. \tag{12}$$

Since $s+t=i$, $\binom{i}{s}=\binom{i}{t}$, then the above equation can be transformed to:

$$\sum_{t=mk-1}^{i-m}g(t+1)\binom{i}{t}=k\cdot\sum_{t=mk}^{i-m+1}g(t)\binom{i}{t}. \tag{13}$$

Substitute $t'=t+1$ into the left hand side of the above equation, we can get:

$$\sum_{t'=mk}^{i-m+1}g(t')\binom{i}{t'-1}=k\cdot\sum_{t=mk}^{i-m+1}g(t)\binom{i}{t}. \tag{14}$$

Based on Eq. (14), we can derive the recursive solution of $g(n)$.

When $n=mk$:

$$g(n)=\binom{mk}{m,m,\cdots,m}=\frac{(mk)!}{(m!)^k}. \tag{15}$$

When $n>mk$: assume $i-m+1=n$, $i=n+m-1$. Substitute $i=n+m-1$ into Eq. (14), we can get:

$$\sum_{t=mk}^{n}g(t)\binom{n+m-1}{t-1}=k\cdot\sum_{t=mk}^{n}g(t)\binom{n+m-1}{t}. \tag{16}$$

Simplify the above equation:

$$g(n)=\frac{\sum_{t=mk}^{n-1}g(t)\left(k\cdot\binom{n+m-1}{t}-\binom{n+m-1}{t-1}\right)}{\frac{n-mk}{k}\cdot\binom{n+m-1}{n}}. \tag{17}$$

From Eq. (15) and (17), this problem is solved.

References

Alvarez, E., Fernández, A., García, P., Jiménez, J. & Marcano A. [1999] "New approach to chaotic encryption," *Physics Letters A*, **263**:373–375.

Alvarez, G., Pastor, G., Monotoya, F., & Romera, M. [1999] "Chaotic cryptosystems," *Proc. IEEE Int. Carnahan Conf. Security Technology 1999*, 332–338.

Alvarez, G., Montoya, F., Romera, M. & Pastor, G. [2000] "Cryptanalysis of a chaotic encryption system," *Physics Letters A*, **276**:191–196.

Baptista, M. S. [1998] "Cryptography with chaos," *Physics Letters A*, **240**:50–54.

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

Bernstein, G. M. & Lieberman, M. A. [1990] "Secure random number generation using chaotic circuits," *IEEE Trans. Circuits and Systems* **37**(9), 1157–1164.

Biham, E. [1991] "Cryptoanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91," In *Advances in Cryptology - EuroCrypt'91*, *Lecture Notes in Computer Science* **0547** (Berlin: Spinger-Verlag), 532–534.

Binder, P. M. & Jensen, R. V. [1986] "Simulating chaotic behavior with finite-state machines," *Physical Review A* **34**(5), 4460–4463.

Blank, M. [1997] *Discreteness and Continuity in Problems of Chaotic Dynamics* (Providence, Rhode Island: American Mathematical Society), Translations of Mathematical Monographs, vol. 161.

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

Černák, J. [1996] "Digital generators of chaos," *Physics Letters A* **214**, 151–160.

Chambers, W. G. [1999] "Comments on 'Chaotic digital encoding: An approach to secure communication'," *IEEE Trans. Circuits and Systems–II*, **46**(11):1445–1447.

Dachselt, F. & Schwarz, W. [2001] "Chaos and Cryptography," *IEEE Trans. Circuits and Systems–I* **48**(12), 1498–1509.

Frey, D. R. [1993] "The Hénon attractor as a keystream generator," In *Advances in Cryptology – EuroCrypt'91*, *Lecture Notes in Computer Science* **0547** (Berlin: Spinger-Verlag), 76–81.

Frey, D. R. [1993] "Chaotic digital encoding: An approach to secure communication," *IEEE Trans. Circuits and Systems–II*, **40**(10):660–666.

Fridrich, J. [1998] "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos* **8**(6), 1259–1284.

García, P., Parravano, A., Cosenza, M. G., Jiménez, J. & Marcano, A. [2002a] "Coupled map networks as communication schemes," *Physical Review E* **65**(4), art no. 045201(R).

García, P. & Jiménez, J. [2002b] "Communication through chaotic map systems," *Physics Letters A* **298**(1), 34–40.

Götz, M., Kelber, K. & Schwarz, W. [1997] "Discrete-time chaotic encryption systems–Part I: Statistical design approach," *IEEE Trans. Circuits and Systems–I* **44**(10), 963–970.

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

Hao, Bailin [1993] *Starting with Parabolas: An Introduction to Chaotic Dynamics* (Shanghai, China: Shanghai Scientific and Technological Education Publishing House).

Heidari-Bateni, G. & McGillem, C. D. [1994] "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Communications* **42**(2/3/4), 1524–1527.

Hong, Z. & Xieting, L. [1997] "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurcation and Chaos* **7**(1), 205–213.

IEEE Computer Society [1985] "IEEE standard for binary floating-point arithmetic," IEEE Standard 754-1985.

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

Jakimoski, G. & Kocarev, L. [2001b] "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters A*, **291**(6):381–384.

Kocarev, L., Jakimoski, G., Stojanovski, T. & Parlitz, U. [1998] "From chaotic maps to encryption schemes," In *Proc. IEEE Int. Sym. Circuits and Systems 1998* **4**, 514–517.

Kocarev, L. & Jakimoski, G. [2001] "Logistic map as a block encryption algorithm," *Physics Letters A*, **289**(4-5), 199–206.

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

Kohda, T. & Tsuneda, A. [1997] "Statistics of chaotic binary sequences," *IEEE Trans. Information Theory* **43**(1), 104–112.

Lasota, A. & Mackey, M. C. [1997] *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics* (New York: Springer-Verlag), Second Ed.

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

Li, S., Li, Q., Li, W., Mou, X. & Cai, Y. [2001b] "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-

random coding," *Cryptography and Coding – 8th IMA Int. Conf. Proc.*, *Lecture Notes in Computer Science* **2260**, 205–221.

Li, S., Zheng, X., Mou, X. & Cai, Y. [2002a] "Chaotic encryption scheme for real-time digital video," *Real-Time Imaging VI*, *Proceedings of SPIE* **4666**, 149–160.

Li, S., Mou, X. & Cai, Y. [2002b] "Digital chaos in cryptography: State-of-the-art, problems and solutions," Internal report, available upon request via `hooklee@mail.com`.

Li, S., Mou, X., Gong, L. & Cai, Y. [2002c] "On the security of a chaotic cipher to Biham's attacks," submitted.

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

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

Palmore, J. & Herring, C. [1990] "Computer arithmetic, chaos and fractals," *Physica D* **42**, 99–110.

Papadimitriou, S., Bezerianos, A. & Bountis, T. [1997] "Secure Communication with chaotic systems of difference equations," *IEEE Trans. Computers* **46**(1), 27–38.

Papadimitriou, S., Bezerianos, A. & Bountis, T. [1999] "Radial basis function networks as chaotic generators for secure communication systems," *Int. J. Bifurcation and Chaos* **9**(1), 221–232.

Papadimitriou, S., Bountis, T., Mavroudi, S. & Bezerianos, A. [2001] "A probabilistic symmetric encryption scheme for very fast secure communication based on chaotic systems of difference equations," *Int. J. Bifurcation and Chaos* **11**(12), 3107–3115.

Protopopescu, V. A., Santoro, R. T. & Tollover, J. S. [1995] *Fast and secure encryption – decryption method based on chaotic dynamics*, US Patent No. 5479513

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

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

Schneier, B. [1996] *Applied Cryptography – Protocols, Algorithms, and Souce Code in C* (New York: John Wiley & Sons, Inc.), Second Ed.

Shujun, L., Xuanqin, M. & Yuanlong, C. [2001] "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," In *Progress in Cryptology – INDOCRYPT 2001*, *Lecture Notes in Computer Science* **2247**, 316–329.

Silva, C. P. & Young, A. M. [2000] "Introduction to chaos-based communications and signal processing," *Proc. IEEE Aerospace Conf. 2000*, 279–299.

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

Tao, S., Ruili, W. & Yixun, Y. [1998b] "Clock-controlled chaotic keystream generators," *Electronics Letters* **34**(20), 1932–1934.

Waelbroeck, H. & Zertuche, F. [1999] "Discrete chaos," *J. Physics A* **32**, 175–189.

Wheeler, D. D. [1989] "Problems with chaotic cryptosystems," *Cryptologia* **XIII**(3), 243–250.

Wheeler, D. D. & Matthews, R. [1991] "Supercomputer investigations of a chaotic encryption algorithm," *Cryptologia* **XV**(2), 140–151.

Wong, W.-K., Lee, L.-P. & Wong K.-W. [2001] "A modified chaotic cryptographic method," *Computer Physics Communications* **138**(3), 234–236.

Wong, W.-K. [2002] "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A* **298**(4), 238–242.

Yang, Z.-S. [1997] *Combinatorial Mathematics and Algorithms* (Hefei, China: University of Science and Technology of China Press), in Chinese.

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

Zhou, H. & Ling, X. [1997b] "Realizing finite precision chaotic systems via perturbation of m-sequences," *Acta Eletronica Sinica* (In Chinese) **25**(7), 95–97.