Improving Security of a Chaotic Encryption Approach

Shujun Li *, Xuanqin Mou and Yuanlong Cai

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

Abstract

E. Alvarez et al. presented a new chaotic encryption approach recently. But soon G. Alvarez et al. broke it with four cryptanalytic methods and found some other weaknesses. In this letter we point out why the original scheme is so vulnerable to the proposed four attacks. The chief reasons are two essential defects existing in the original scheme. Based on such a fact, we present an improved encryption scheme to obtain higher security. The cryptographic properties of the improved scheme are studied theoretically and experimentally in detail.

Key words: chaotic cryptosystem; encryption; cryptanalysis

1 Introduction

E. Alvarez et al. presented a new cryptosystem based on the iteration of a chaotic system [1]. It is a symmetric block cipher and encrypts every plain-block into a 3-tuple cipher-block. Different from other conventional block ciphers, its block size is variable. Based on a d-dimensional chaotic system $x_{n+1} = f(x_n, x_{n-1}, \cdots, x_{n-d+1})$, the encryption and decryption procedure can be depicted as follows. Firstly, select the control parameter of the system as the secret key, and an integer b_{max} as the maximal block size of plaintext. For one plain-block, whose size is $b_i = b_{max}$, choose a threshold U_i to generate a bit chain C_i from the chaotic orbit $\{x_n\}$ according to such a rule: $x_n \leq U_i \rightarrow 0$ and $x_n > U_i \rightarrow 1$. Find the position at which the plain-block appears in C_i and record $(U_i, b_i, \mathbf{X}_i)$ as the cipher-block corresponding to the plain-block, where $\mathbf{X}_i = (x_i, x_{i-1}, \cdots, x_{i-d+1})$ is the state of the chaotic map at the position. If

⋆ This paper has been published in *Physics Letters A*, 290(3-4):127-133, 2001.

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

the plain-block cannot be found in a large enough catalog C_i, $b_i = b_i - 1$ and the search is restarted. The tent map is used to demonstrate the performance of such a chaotic cipher.

However, only some months later after the proposal of this cipher, G. Alvarez et al. pointed out that it is very easy to be broken when the tent map is used [2]. In their paper, they presented four kinds of attacks, which are chosen-ciphertext attack, chosen-plaintext attack, known-plaintext attack and ciphertext-only attack. They also pointed out some other weaknesses of the chaotic encryption system. As the result, the authors claimed that the new chaotic cipher is not secure at all, even if other chaotic systems are used instead of the tent map.

In this letter, we study why the new chaotic cipher is vulnerable to so many attacks, and propose a solution to improve its security. We find that two essential cryptographic defects existing in the original scheme, which make the four attacks available. If the two defects are avoided, the four attacks proposed in [2] will be unfeasible, and the chaotic cryptosystem will be stronger from the cryptographic viewpoint. Our proposed encryption scheme is based on the above fact. Further theoretical and experimental analyses show that the new encryption system has prefect cryptographic properties, so it also can resist some potential attacks in the future.

2 Two essential defects and other weaknesses

2.1 The occurrence of $\mathbf{X}_i$ in ciphertext

The first essential defect lies in the occurrence of $\mathbf{X}_i$ in ciphertext. Considering the dynamics of the employed chaotic system relies not only on the secret key (control parameter) but also on the initial conditions, an eavesdropper may obtain some useful information from $\mathbf{X}_i$ to lessen attack complexity of the encryption system.

Actually, there does exist information leaking in the chaotic encryption system, which is not less than $E(1/b_i)$, where $E(x)$ represents the mean value of x. Apparently, $b_i \leq b_{max} \rightarrow E(1/b_i) \geq 1/b_{max}$. Given one cipher-block $(U_i, b_i, \mathbf{X}_i)$, let us consider how the b_i bits of the plain-block $P_i = P_{i,0}P_{i,1}\cdots P_{i,b_i-1}$ is deciphered from it. Since the legal users know the secret key (control parameter), they can calculate the b_i iterating values $\{x_{i+j}\}_{j=0}^{b_i-1}$ from $\mathbf{X}_i$. Then the plain-block P_i can be obtained from $\{x_{i+j}\}$ and the threshold U_i as follows:

for $j = 0$ to $b_i - 1$ do
    if $x_{i+j} \leq U_i$ then $P_{i,j} = 0$

else $P_{i,j} = 1$
end

Obviously, b_0 can be obtained from $\mathbf{X}_i$ just by comparing the two values x_i and U_i, without the secret key. Therefore, an illegal user can obtain b_0 in each plain-block under ciphertext-only attack. That is to say, at least $1/b_i$ information of the plain-block leaks from the cipher-block. As a whole, the information leaking will be not less than $E(1/b_i) \geq 1/b_{max}$. Generally speaking, b_{max} cannot be too large, or the encryption speed will be rather slow. Then the information leaking is relatively large to make the cryptosystem insecure in many serious applications.

Furthermore, if one knows the approximate value (r') of the secret key, he can guess the plain-block by the symbolic dynamics of the chaotic system from the initial condition $\mathbf{X}_i$. The closer the secret key is to r', the better such a guess works. This fact means that the encryption system is not sensitive to secret key, which is undesired for a good cryptosystem [3]. The authors of [2] employed such a fact to develop a ciphertext-only attack when $r' = 2$. It is found that such a guess can conceal the plain-block with high possibility when the secret key is close to 2. Of course, the success ratio will decrease as the right key departs from 2, but bear in mind that the information leaking of this chaotic cryptosystem will not be less than $1/b_{max}$ for all available keys.

In addition, the chosen-ciphertext attack described in [2] is also based on the fact that $\mathbf{X}_i$ in ciphertext can expose some useful information about the secret key. By choosing $\mathbf{X}_i$ sufficiently close to zero and observing the corresponding plaintext, one can get the secret key in a small number of steps.

2.2 Different dynamics with different keys

For the tent map used in [1], the dynamics with different secret keys (control parameters) is much different, such as different visited interval of the orbit, different Lyapunov exponent, different Kolmogrov entropy and the occurrence of periodic window at many control parameters [4]. Since such difference can be extracted from $\mathbf{X}_i$, it can be used to develop some available attacks. It is the second essential defect.

The different visited interval of the orbit with different key is easily used to realize chosen-plaintext attack and known-plaintext attack as described in [2]. When control parameter is r, the visited interval will be $[r(1 - r/2), r/2]$. By the statistics of enough ciphertexts one can get the approximate lower (upper) bound of the visited interval, then obtain the secret key r approximately. As we have mentioned above, the chaotic encryption system is not sensitive to the secret key, so the approximate secret key is enough to decrypt the ciphertext

with high success possibility. Of course, one can find the exact value of the secret key by searching it in a small neighbor area of the approximate value, which will need much less computation complexity than searching it in the whole key space.

Since $\mathbf{X}_i$ must be known to make such statistics, the known-plaintext attack and chosen-plaintext attack in [2] depend on the both defects. Hence, if the first defect is avoided, all the four attacks in [2] are infeasible. But in order to avoid other possible attacks in the future, both defects should be mended. We will do so in the improved scheme.

2.3 Other weaknesses

There are also some other weaknesses pointed out in [2]. They are the use of too low computing precision, the lack of exact directions about how to choose the initial condition and the secret key, and the non-sensitivity of ciphertext to the secret key. The last weakness has been discussed in the last two subsections. Others are not crucial for the original encryption scheme, and can be solved by carefully re-consider the realization of original scheme.

Besides the above weaknesses, there still exists another serious problem in the original scheme, which is about the slow encryption speed. It is obvious that the encryption speed is chiefly determined by the search for the occurrence of plain-block in C_i. Assume C_i is balanced on $\{0, 1\}$, then the probability of the occurrence of every plain-block is $1/2^{b_i}$, so the search procedure can be regarded as Bernoulli experiments with probability $p = 1/2^{b_i}$. The number of experiments satisfies geometric distribution, and its mathematical expectation is 2^{b_i} [5]. If C_i is not balanced, the average number of experiments will be larger than 2^{b_i}. Because b_i cannot be very small to avoid the brute-force attack, the encryption speed will be much slower as compared with other conventional ciphers. On the other hand, b_i will not be too large since the search will be restarted with $b_i = b_i - 1$ if the plain-block cannot be found for a long time. Such a paradox will make the selection of b_{max} very difficult to obtain both considerable security and encryption speed. In [1], $b_{max} = 16$ is adopted, which makes the chaotic cipher insecure and the encryption speed relatively slow.

3 The improved scheme

3.1 Description

An improved scheme is proposed in this letter. It can avoid the two existent defects and other weaknesses of the original one, and has higher security.

Without loss of generality, we employ a one-dimensional chaotic map to construct the new cryptosystem. Assume a chaotic map defined on the interval $I = [a, b]$ is given: $x_{n+1} = f(x_n, p)$, where p is the control parameter. The following requirement should be satisfied: the chaotic map is ergodic on I with unique invariant density function [6]. This requirement is needed to avoid the second essential defect, and can make the statistical cryptanalysis impossible.

We can give some examples of such chaotic maps. It has been known that the piecewise linear chaotic maps are ergodic and have uniform invariant density function on their definition intervals [7]. Moreover, the piecewise linear maps are the simplest kind of chaotic maps in practice (only several additions and one division are needed). So they are the best candidates for our scheme. Among them the simplest one can be denoted by eq. (1), which is similar to but essentially different from the tent map used in [1]:

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

Another example is the chaotic map used in [8], which is also rather simple and a little more complex than the map above:

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

Based on such a chaotic map, the improved scheme can be described as follows.

- *The secret key*: $K = (x_0, p)$, where x_0 is the initial condition of the chaotic map.
- *The input – plaintext*: $P_1 P_2 \cdots P_i \cdots$, where the size of P_i is $b_i \leq b_{max}$.
- *The encryption procedure* is quite similar to the original scheme. For the first plain-block P_1 whose size is $b_1 = b_{max}$, run the chaotic map from x_0, and select a threshold U_1 to generate a bit chain C_1 as the same rule in the

original scheme. Find the position at which P_1 appears in C_1, and record (U_1, b_1, n_1) as the cipher-block, where n_1 is the number of iterations of the chaotic map from x_0. If P_1 cannot be found in a large enough catalog C_1, $b_1 = b_1 - 1$ and the search restarts. For the second and the following plain-blocks, the encryption procedure is just like above, except that the chaotic map runs from the position after the last plain-block is encrypted, not x_0.

- *The output – ciphertext*: $(U_1, b_1, n_1)\ (U_2, b_2, n_2) \cdots (U_i, b_i, n_i) \cdots$. In fact, the threshold U_i can be fixed for all plain-blocks, then the ciphertext will be simplified to $(b_1, n_1)(b_2, n_2) \cdots (b_i, n_i) \cdots$. Generally speaking, the threshold should be selected to make C_i balanced on $\{0, 1\}$, i.e., $P\{C_i = 0\} = P\{C_i = 1\}$. It can be derived from the invariant density function of the chaotic map. For the two chaotic maps above-mentioned, the threshold is 0.5, the midpoint of $I = [0, 1]$.
- For the legal users knowing the secret key, *the decryption procedure* is easy to be realized by re-generating C_i for each cipher-block.

We can see the both defects in original scheme are avoided in the above scheme. What's more, different from the original scheme, the improved one is a stream cipher, not a block cipher. Such a fact means that smaller b_{max} can be used and the paradox between the security and the encryption speed will be overcome to some extent.

3.2 Discussion

In our scheme, one important problem should be considered carefully, since it can cause weak keys in the whole key space of the chaotic cryptosystem. It is about the statistical degradation of the digital chaotic map. In the recent years, many researchers have found: when chaotic systems are discretely realized in finite precision, some serious problems will arise, such as short cycle length, non-ideal distribution and correlation functions [9–16]. Among these problems, short cycle length is very crucial. When the finite computing precision is L(bits), the cycle length of the chaotic orbit will be much smaller than 2^L for many control parameters and initial conditions. What's worse, there are many control parameters and initial conditions making the chaotic orbit converge on fixed value after some iterations. For the chaotic map defined by (1), an extreme example is as follows: assume $p = 1/2$, for each x_0, both the chaotic orbit and C_i will lead to zero after L iterations. Such a fact will make the encryption procedure stop, and make the encryption system infeasible.

Apparently, we must remedy this problem in our scheme. While in fact, there is yet not an established theory to measure the statistical properties of discrete-time chaotic maps and direct how to improve them. Only several engineering methods are proposed to escape from such a problem: using higher finite preci-

sion [10,11], perturbation-based algorithm by pseudo-random number [12,13], and cascading multiple chaotic systems [15]. In our scheme, the perturbation-based algorithm proposed in [13] is suggested, which can be briefly depicted as follows.

Use a PRNG (Pseudo-Random Number Generator) to generate a signal to perturb the orbit of the chaotic map at regular intervals. Assume the cycle length of the sequence generated by the PRNG is T and the perturbing interval is Δ, the cycle length of the perturbed chaotic orbit will be $\sigma \cdot \Delta \cdot T$, where σ is a positive integer. Generally, the maximal length LFSR (Linear Feedback Shift Register [3]) is used as the perturbing PRNG, when its degree equals to the finite computing precision L, the cycle length of the perturbed chaotic orbit will be $\sigma \cdot \Delta \cdot (2^L - 1) > 2^L$. Such a long length can improve the discrete ergodicity of the chaotic map in the finite precision. For the piecewise linear chaotic maps, it hints the uniform distribution of the chaotic orbit in the discrete space, which is desired for a good cipher.

As argued in [13], the amplitude of the perturbing signal should be much smaller than the one of chaotic signal. But our experiments show that: the larger the perturbing signal is, the better the results coincide with the theoretical analyses and the faster the encryption system runs. It is because the chaotic orbit will be more uniformly with larger perturbing signal. So we suggest using larger perturbing signal instead of smaller one, then the perturbed chaotic system can be considered as a compound system of nonlinear dynamics and pseudo-randomness of the perturbing PRNG. Here, the nonlinearity of the chaotic systems ensures the security and the PRNG mends the degraded digital statistical properties of discrete chaotic systems.

3.3 Cryptographic properties

In this section, we give the following statement firstly. Since b_i in ciphertext just indicates the block size of the corresponding plain-block, we will only regard n_i as the "real" ciphertext.

As we know, two chief cryptographic properties of a good cipher are confusion and diffusion, which are commonly ensured by the balance and avalanche properties of the ciphertext in conventional cryptography [3]. But our chaotic cipher has rather different property: the ciphertext is not balanced, since the larger n_i, the smaller the possibility of its occurrence in the ciphertext. Assume C_i is a balanced i.i.d. bit sequence, the search procedure can be considered as Bernoulli experiments with probability $1/2^{b_i}$; then we can deduce the discrete

distribution of n_i:

$$P\{n_i = k\} = \frac{1}{2^{b_i}} \cdot \left(1 - \frac{1}{2^{b_i}}\right)^{k-1}, \tag{3}$$

which is independent and identical for different secret keys and plaintexts theoretically.

Actually, there are four corresponding facts on the distribution of the ciphertext: 1) for different plaintexts, the ciphertext has the same distribution function; 2) for different secret keys (control parameters and initial conditions), the ciphertext has the same distribution function; 3) for two plaintexts even with only one bit difference, the ciphertext is rather different; 4) for two secret keys even with only one bit difference, the ciphertext is rather different. The first two facts denote confusion, and the other two denote diffusion.

Because our improved scheme avoids the two essential defects, and satisfies the confusion and diffusion properties, we can use smaller b_{max} compared to the original scheme. Thus the encryption speed will be faster. However, since the time-consuming search procedure is still used, the encryption speed is still slower than most conventional ciphers. Assume the speed of iterating the chaotic map is s iterations per second; the average encryption speed will not be faster than $s \cdot b_{max}/2^{b_{max}}$ bps (bits per second). Hence, such a chaotic encryption scheme only can be used in non-real-time applications, such as the secure transmission of short messages over network or the secure storage of small files in computers.

At last, let us discuss the key entropy of the improved scheme. When the finite computing precision is L(bits), the control parameter and initial conditions are represented as a fixed-point binary decimal. So the key entropy of the improved scheme is $2L$. In most computers $L = 32$ or 64, then the key entropy is 64 or 128, which is enough as a secure cipher. If higher security is wanted, larger L is suggested being used.

3.4 Compression after encryption

There is a notable problem in the chaotic cipher: the block size of ciphertext is much (> 2 times) larger than the one of plaintext. Compressing ciphertext can solve it. Since the ciphertext is not balanced, it can be consequently compressed with lossless statistical encoding methods, such as Huffman coding algorithm [17]. Firstly, divide the ciphertext into two bit streams: $b_1 b_2 \cdots b_i \cdots$ and $n_1 n_2 \cdots n_i \cdots$. Then compress the two sub-streams with Huffman coding separately. For the stream $n_1 n_2 \cdots n_i \cdots$, the average size of compressed

cipher-block will be b_{max} according to eq. (3). For the stream $b_1 b_2 \cdots b_i \cdots$, the average size of compressed cipher-block will be close to 1 since each b_i in ciphertext trends to be b_{max}. Hence, the average size of compressed cipher-block will be close to $b_{max}+1$, only 1 bit more than the maximal size of plain-block.

3.5 Experimental Results

Based on the chaotic map defined in eq. (1), we construct an experimental cryptosystem and test its cryptographic properties. Here the computing precision is $L = 32$(bits), $b_{max} = 8$, and the perturbing PRNG is a maximal length LFSR (m-LFSR), whose degree is L and primitive polynomial is $1+x+x^{27}+x^{28}+x^{32}$. The perturbing interval Δ is L (note $\gcd(L, 2^L-1) = 1$), and all bits of the m-LFSR are used to perturb the chaotic orbit.

As we have mentioned above, the discrete distribution of n_i is denoted by eq. (3) theoretically. When the plaintext is distributed uniformly, the experimental result coincides with the theoretical curve as shown in Fig. 1. When the plaintext is 59 59 $\cdots$ 59 $\cdots$, the experimental result is shown in Fig. 2. The number of encrypted plain-block is 50,000. When the secret keys (control parameters and initial conditions) are selected as different values randomly, similar results are obtained. So the confusion property is confirmed.

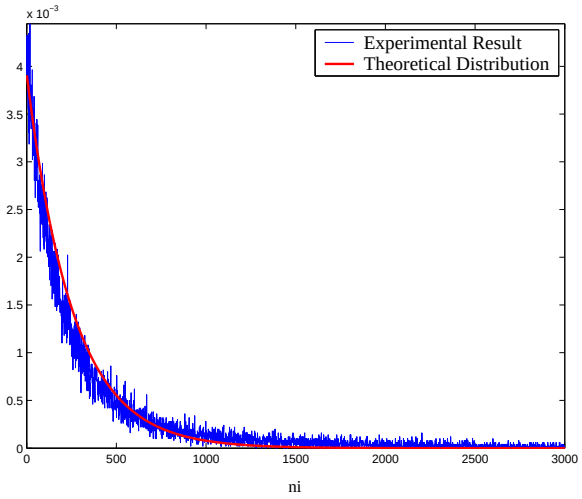

Fig. 1. The distribution of n_i with uniformly distributed plaintext

Some other experiments are made to verify the diffusion property. The difference of n_i in two ciphertexts is shown in Fig. 3–5, with the least different plain-texts, control parameters and initial conditions, respectively. The different parameters are listed as follows:

The least different plaintexts (see Fig. 3): **195** 195 $\cdots$ 195 $\cdots$ and **196** 195

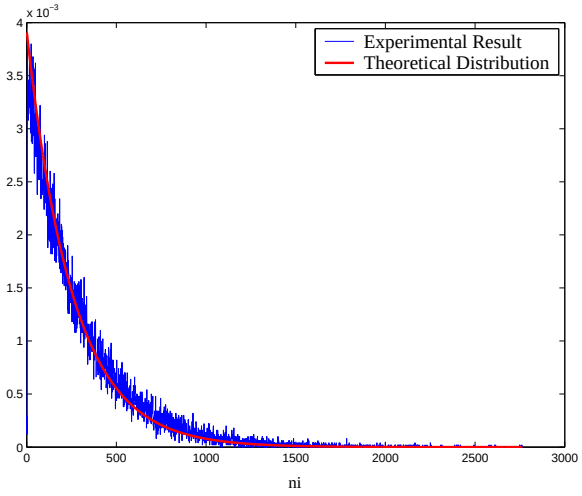

Fig. 2. The distribution of n_i with fixed plaintext 59 59 $\cdots$ 59 $\cdots$ $\cdots$ 195 $\cdots$

The least different control parameters (see Fig. 4): $p_1 = \mathbf{31849}/2^{32}$ and $p_2 = \mathbf{31848}/2^{32}$.

The least different initial conditions (see Fig. 5): $x_{0,1} = \mathbf{40332}/2^{32}$ and $x_{0,2} = \mathbf{40333}/2^{32}$.

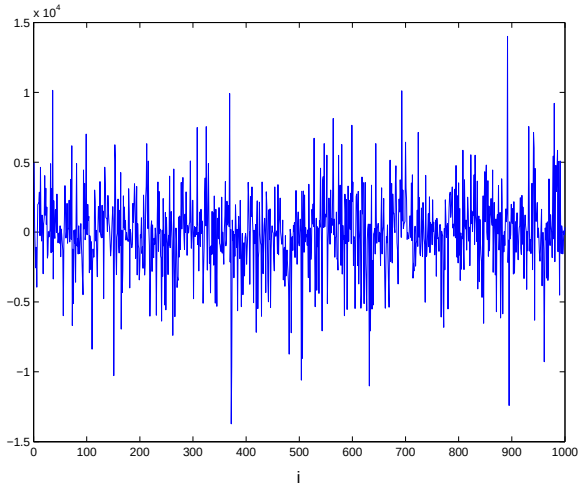

Fig. 3. The difference of n_i with two least different plaintexts

4 Conclusion

In this letter, we point out two essential defects existing in the chaotic encryption scheme proposed in [1], and propose a new scheme to improve its security by avoiding the two defects and solving other weaknesses. Our scheme is immune to the four attacks presented in [2] and has desired cryptographic properties.

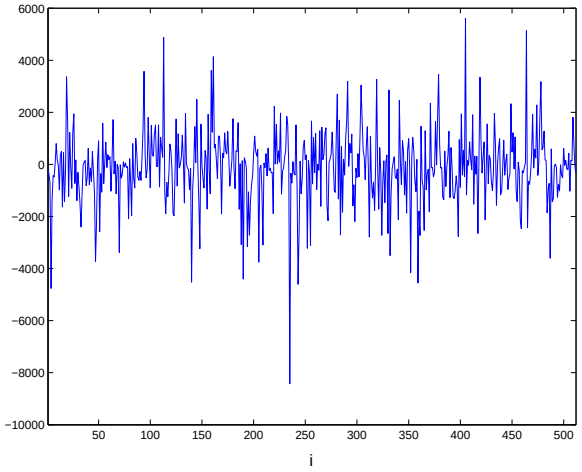

Fig. 4. The difference of n_i with two control parameters having 2^{-L} difference

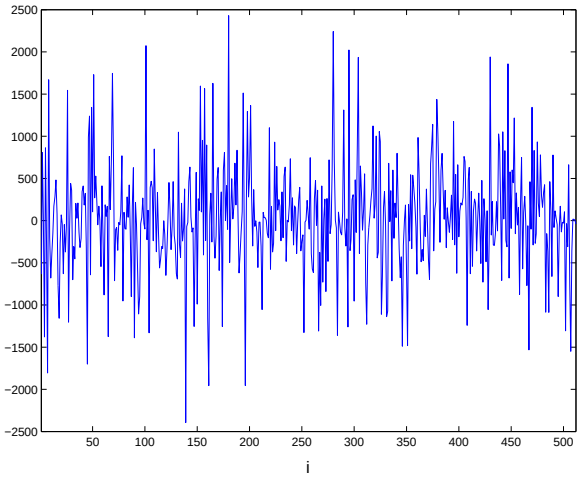

Fig. 5. The difference of n_i with two initial conditions having 2^{-L} difference

Although the security of the original scheme can be improved, its encryption speed cannot be essentially improved much because of the time-consuming search procedure. Therefore, its encryption speed is still rather slower than most conventional ciphers. It is a remained weakness in our improve scheme. We will try to find the solution to this problem in the future, but perhaps any possible solution will lead to entirely different chaotic cryptosystem from the original one proposed in [1].

In addition, as we know, the public-key cryptosystem is generally used to encrypt the secret keys of symmetric ciphers, which are used to encrypt the plaintext transmitted via public channel. Apparently, they are not so sensitive to the encryption speed. Another open research in the future is extending this symmetric chaotic cipher to a public-key one.

Acknowledgements

The authors would like thank Miss Han Lu at Xi'an Foreign Language University for her help in the preparation of this paper.

References

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

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

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

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

[5] The Committee of *Modern Applied Mathematics Handbook*, Modern Applied Mathematics Handbook – vol. Probability Theory and Stochastic Process, Tsinghua University Press, Beijing, China, 2000.

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

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

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

[9] J. Palmore, C. Herring, Computer arithmetic, chaos and fractals, Physica D 42 (1990) 99–110.

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

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

[12] Zhou Hong, Ling Xieting, Realizing finite precision chaotic systems via perturbation of m-sequences, Acta Eletronica Sinica(In Chinese) 25 (1997) 95–97.

[13] Sang Tao, Wang Ruili, Yan Yixun, Perturbance-based algorithm to expand cycle length of chaotic key stream, Electron. Lett. 34 (1998) 873–874.

[14] Li Shujun, Li Qi, Li Wenmin, Mou Xuanqin, Cai Yuanlong, 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, Berlin, 2001, pp. 205–221.

[15] G. Heidari-Bateni, C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, IEEE Trans. Comm. 42 (1994) 1524–1527.

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

[17] K. R. Castleman, Digital Image Processing, Prentice Hall Inc., New York, 1996.