Vol 13 No 5, May 2004
1009-1963/2004/13(05)/0625-08

Chinese Physics

© 2004 Chin. Phys. Soc.
and IOP Publishing Ltd

Security analysis of a spatiotemporal-chaos-based cryptosystem*

Lü Hua-Ping(吕华平)[a)b)], Wang Shi-Hong(王世红)[a)c)], Li Xiao-Wen(李晓文)[a)],
Tang Guo-Ning(唐国宁)[a)], Kuang Jin-Yu(匡锦瑜)[d)],
Ye Wei-Ping(叶卫平)[d)], and Hu Gang(胡 岗)[a)e)†]

[a)] *Department of Physics, Beijing Normal University, Beijing* 100875, *China*
[b)] *Department of Physics, Xuzhou Normal University, Xuzhou* 221009, *China*
[c)] *Science school, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[d)] *Department of Electronics, Beijing Normal University, Beijing* 100875, *China*
[e)] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing* 100875, *China*

(Received 3 July 2003; revised manuscript received 19 September 2003)

An S-box modified one-way coupled map lattice is applied as a chaotic cryptograph. The security of the system is evaluated from various attacks currently used, including those based on error function analysis, statistical property analysis, and known-plaintext and chosen-ciphertext analytical computations. It is found that none of the above attacks can be better than the brute force attack of which the cost is exhaustively quantitated by the key number in the key space. Also, the system has fairly fast encryption (decryption) speed, and has extremely long period for finite-precision computer realization of chaos. It is thus argued that this chaotic cryptosystem can be a hopeful candidate for realistic service of secure communications.

Keywords: chaos synchronization, chaotic cryptograph, S-box operation
PACC: 0545, 0437

1. Introduction

Since the pioneering work by Pecora and Carrol on chaos synchronization, chaos communication has attracted much attention in the field of nonlinear science, as one of the most important possible applications of chaos.[1−9] Recently, the study in this field has more and more turned to practical aspects, i.e. to finding chaotic cryptosystems with desirable cryptographic properties, such as security,[10−19] performance,[15,20−22] robustness against channel noise,[23−25] and software and hardware realizations, among which the property of security constitutes the most important part. In this regard, two tasks become significant: to propose some types of chaotic cryptographs with high security, and to evaluate the proposed systems with effective attacks. The latter is the central task of this paper.

In Ref.[17] we used a chaotic one-way coupled map lattice system for a cryptograph to achieve high security. In Ref.[18] this system was further improved by incorporating an S-box operation with the chaotic dynamics. It has been proven that this system, with certain modifications, has very good overall cryptographic properties such as fast encryption (and decryption) speed,[22] and strong robustness against channel noise.[25] This chaotic system may be a very hopeful candidate for a chaotic cryptograph serving in realistic and commercial secure communications. However, the security of the system has still not been confirmed convincingly. In all the above works,[17,18,22] the security of the system is evaluated by an error function attack (EFA) which is assumed to be very effective. Nevertheless, it is not enough to declare the practical security of a cryptosystem by a single attack approach only. This paper will make a systematic evaluation of a spatiotemporal-chaos-based cryptosystem and test its practical security by various currently used attacks.

*Project supported by the National Natural Science Foundation of China (Grant No 10175010) and the Special Funds for Major State Basic Research Projects (Grant No G2000077304).
†Correspondent author. E-mail: ganghu@bnu.edu.cn

The paper is organized as follows. In Sec.2 we present our model and specify the public-structure and known-plaintext conditions for possible attacks. In Sec.3, an error function attack is applied, and particular attention is paid to the possibility of optimal adaptive searching based on this error function. In Sec.4, the statistical behaviour of the keystream produced by the system is investigated in detail numerically, and the difficulties of a number of statistics-based attacks, in both conventional and chaotic cryptanalyses, are discussed. Section 5 is devoted to the discussion of the attack based on analytical computation. In Sec.6 a chosen-ciphertext attack, the strongest attack, is applied for the evaluation. It is shown that our system is secure against all the attacks considered in Sections 3–6 in the sense that no other attack is more effective than the brute force attack in the key space. The last section gives the conclusion and discussion.

2. Model and conditions for attacks

We consider the following one-way coupled chaotic map lattice for cryptograph.

Encryption transformation of the transmitter:

$$\begin{aligned} x_{n+1}(j) =&(1-\varepsilon)f_j[x_n(j)]+\varepsilon f_j[x_n(j-1)],\\ f_j(x) =&(3.75+a_j/4)x(1-x),\quad j=1,\ldots,m; \end{aligned} \tag{1a}$$

$$\begin{aligned} x'_{n+1}(m+1) =&(1-\varepsilon)f[x_n(m+1)]+\varepsilon f[x_n(m)],\\ Q'_n =&[\mathrm{int}(x'_n(m+1)\times 2^{\mu})]\ \mathrm{mod}2^{\nu},\\ Q_n =&\mathrm{Sbox}(Q'_n); \end{aligned} \tag{1b}$$

$$f(x)=4x(1-x),\quad x_{n+1}(m+1)=Q_n/2^{\nu},$$

$$\begin{aligned} x_{n+1}(j) =&(1-\varepsilon)f_{j-m-1}[x_n(j)]+\varepsilon f_{j-m-1}[x_n(j-1)],\\ j=&m+2,\ldots,2m+1; \end{aligned} \tag{1c}$$

$$\begin{aligned} x_{n+1}(N) =&(1-\varepsilon)f[x_n(N)]+\varepsilon f[x_n(N-1)],\\ N=&2m+2; \end{aligned} \tag{1d}$$

$$\begin{aligned} S_n =&(K_n+I_n)\ \mathrm{mod}2^{\nu},\\ K_n =&[\mathrm{int}(x_n(N)\times 2^{\mu})]\ \mathrm{mod}2^{\nu}, \end{aligned} \tag{1e}$$

$$x_n(0)=\begin{cases} x_n(0)+\dfrac{1}{8} & S_n/2^{\nu}\le\dfrac{1}{8},\\ x_n(0)-\dfrac{1}{8} & S_n/2^{\nu}\ge\dfrac{7}{8},\\ S_n/2^{\nu} & \text{otherwise,}\end{cases}$$

where the S-box is defined as follows:

$$\begin{aligned} A_1 =&[(Q_n\gg 24)\&255], A_2=[(Q_n\gg 16)\&255],\\ A_3 =&[(Q_n\gg 8)\&255], A_4=[(Q_n\&255],\\ A_0 =&A_1\oplus A_2\oplus A_3\oplus A_4,\\ Q_n =&[A_0\ll 24]+[A_4\ll 16]+[A_3\ll 8]+A_2. \end{aligned} \tag{2}$$

The operation $x\gg y$ denotes a right shift of x by y bits and the & operator is bitwise AND and $\oplus$ means bitwise XOR. After the S-box transformation of (2) all the 32 bits in Q'_n take place in the highest block A_0 in Q_n. This operation greatly enhances the sensitivity of the output S_n to any small mismatch of the secret key.

Decryption transformation of the receiver:

$$\begin{aligned} y_{n+1}(j) =&(1-\varepsilon)f_j[y_n(j)]+\varepsilon f_j[y_n(j-1)],\\ f_j(y) =&(3.75+b_j/4)y(1-y),\quad j=1,\ldots,m; \end{aligned} \tag{3a}$$

$$\begin{aligned} y'_{n+1}(m+1) =&(1-\varepsilon)f[y_n(m+1)]+\varepsilon f[y_n(m)],\\ Q'_n =&[\mathrm{int}(y'_n(m+1)\times 2^{\mu})]\ \mathrm{mod}2^{\nu},\\ Q'_n =&\mathrm{Sbox}(Q'_n); \end{aligned} \tag{3b}$$

$$f(y)=4y(1-y),\quad y_{n+1}(m+1)=Q_n/2^{\nu},$$

$$\begin{aligned} y_{n+1}(j) =&(1-\varepsilon)f_{j-m-1}[y_n(j)]+\varepsilon f_{j-m-1}[y_n(j-1)],\\ j=&m+2,\ldots,2m+1; \end{aligned} \tag{3c}$$

$$y_{n+1}(N)=(1-\varepsilon)f[y_n(N)]+\varepsilon f[y_n(N-1)], \tag{3d}$$

$$\begin{aligned} K'_n =&[\mathrm{int}(y_n(N)\times 2^{\mu})]\\ I'_n =&[S_n-K'_n]\ \mathrm{mod}2^{\nu}, \end{aligned} \tag{3e}$$

$$y_n(0)=x_n(0).$$

In this paper, the system parameters are fixed at m=4, μ=51, ν=32, ε=0.99, a_j=0.5, j=1,2,3,4, where $\boldsymbol{a}=(a_1,a_2,a_3,a_4)$ and $\boldsymbol{b}=(b_1,b_2,b_3,b_4)$ serve as the encryption and decryption keys, respectively, with a_i, $b_i\in(0,1), i$=1,2,3,4. With $\boldsymbol{b}=\boldsymbol{a}$ the receiver can reach chaos synchronization with the transmitter and obtain

$$y_n(N)=x_n(N),\ K'_n=K_n,\ I'_n=I_n, \tag{4}$$

and successfully recover the true plaintext I_n. The cryptosystem (1) and (3) is mainly based on spatiotemporal chaotic dynamics with floating point analytical computation on real numbers, which is incorporated, however, with certain algebraic operations on integers, such as the *int* and *modulo* operations in Eqs.(1e) and (3e) and the S-box operation in

Eqs.(1b), (3b) and (2). These algebraic operations can effectively enhance the sensitivity of chaos synchronization to the system parameters on the one hand, and strengthen the robustness of the communication against computer round-off errors and channel noise on the other hand. The motivations of the analytical chaotic structure and the algebraic operations of (1)–(3) were discussed in Refs.[17,18] in detail. In this paper we focus on its security analysis by applying various typical attacks.

The maximum intention of any intruder is to expose the secret key by various attacks. According to the strength of analysis, or precisely, to the information accessible to the intruder, one can order all attacks to the following classes:[16] ciphertext-only attack, plaintext-known attack, chosen-plaintext attack and chosen-ciphertext attack. For communications among multiple commercial users in a large community, all the community members use the same communication machines, thus the cryptographic structure of the secure communications must be open to all the community members, i.e. open to intruders, and only the values of some system parameters, serving as the secret key, can be kept private for protecting the security: this is referred to as the Kerckhoff principle.[16]

In the following sections we will evaluate system (1)–(3) by various currently used attacks (some are among the strongest ones) to show that with the combinative applications of spatiotemporal chaotic dynamics and suitable algebraic operations, our system has extremely high practical security, and can serve as one of the best cryptographic candidates for realistic applications.

3. Error function attack and the associated adaptive searching method

Since the intruder is assumed to have all information the legal receiver has, including the dynamic structure Eqs.(1)–(3), ciphertext S_n and past plaintext I_n of arbitrary length T, except for the precise values of the secret key $\boldsymbol{a}$, he can run the receiver system Eq.(3) with the test key $\boldsymbol{b}$ to produce I'_n, and then compare the output I'_n with the true plaintext I_n to reveal the location of $\boldsymbol{a}$. Specifically, the intruder can compute the following error function:

$$e(\boldsymbol{b}) = \frac{1}{T}\sum_{n=1}^{T} |i'_n - i_n|\,, \quad i_n = \frac{I_n}{2^\nu}, \quad i'_n = \frac{I'_n}{2^\nu}, \tag{5}$$

from which he can try to extract the secret key $\boldsymbol{a}$ by minimizing the error function

$$e(\boldsymbol{b}) = 0 \quad \text{at} \quad \boldsymbol{b} = \boldsymbol{a}.$$

This attack is called as error function attack (EFA). For chaotic cryptosystems, $e(\boldsymbol{b})$ has a basin with finite width around the key position $\boldsymbol{b} = \boldsymbol{a}$ due to the nature of the analytical computation of chaos;[17] this basin structure may help the intruder to catch the trace of the secret key. This is why EFA is particularly effective in evaluating a chaotic cryptograph.

In Eqs.(1)–(3) we incorporate algebraic operation S-box in the basic spatiotemporal chaotic dynamics, and effectively shrink the basin of the error function. The security of the system against EFA is greatly enhanced. In Fig.1 we fix $b_1 = b_2 = b_3 = a_i = 0.5$ and plot $e(b_1)$ vs b_1 for different resolutions of detections and for different T. It is shown that $e(b_1)$ rises rapidly to $\frac{1}{3}$ with certain fluctuation for extremely small mismatch $|b_1 - a_1| \geq 2^{-45}$. The same behaviour can be observed for b_2, b_3, b_4. Therefore, our chaotic system has effective key number of 2^{180} against EFA evaluation. If we define the secret key $\boldsymbol{a} = (a_1, a_2, a_3, a_4)$ such that each a_i has length of 45 bits, EFA is no more effective than the brute force attack, which needs maximum cost of 2^{180} tests:

$$\text{cost} \approx 2^{180} \approx 10^{54}. \tag{6}$$

A crucial problem for EFA is whether we can find some adaptive methods with the error function $e(\boldsymbol{b})$ for conducting optimal searchings more effective than the brute force attack. To study this possibility we present Fig.2 with much finer resolutions of $e(b_1)$, where two characteristic features are observed. First, it is further confirmed that we have $e(b_1) = 0$ for $b_1 = a_1$, and $e(b_1) \approx \frac{1}{3}$ for any other $b_1 \neq a_1$ with 2^{-45} resolution. There is no tendency indicating the location of a_1 even as b_1 is in the 2^{-45} vicinity of a_1, and without this tendency any adaptive searching can hardly be effective. Second, due to the large fluctuation there are numerous local minima, which can frequently trap adaptive searching paths to various local minima and destroy any optimization. We have tried some adaptive methods, and none is better than the brute force attack.

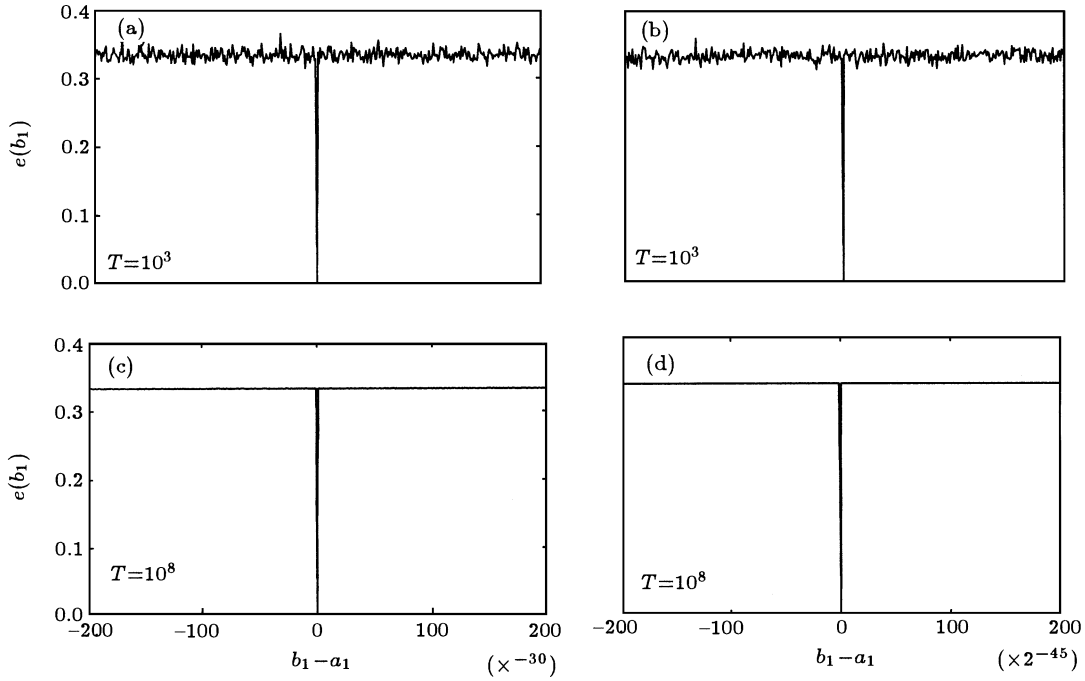


Fig.1. Error function $e(b_1)$ defined in Eq.(5) vs the decryption key parameter b_1 with different b_1 detection resolutions and different lengths of plaintext T. (a),(b) $T = 10^3$; (c),(d) $T = 10^8$. We observe $e(b_1) = 0$ for $b_1 = a_1$, and $e(b_1) \simeq \frac{1}{3}$ whenever b_1 has any mismatch from a_1 larger than or equal to 2^{-45}.

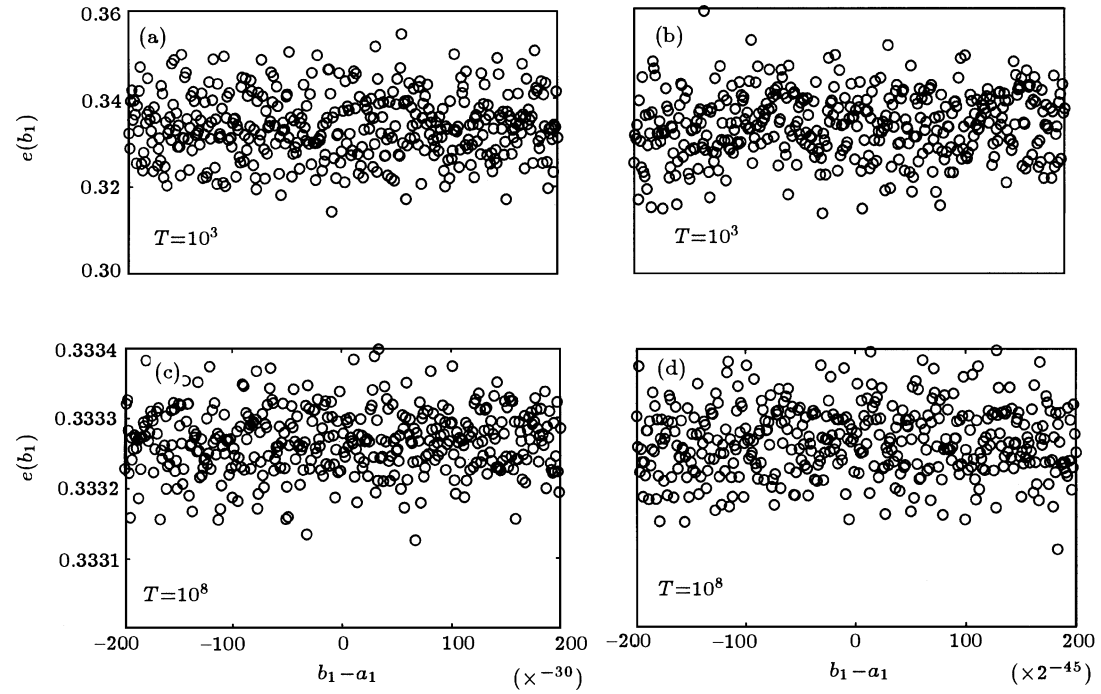


Fig.2. As Fig.1, but with $e(b_1)$ greatly amplified around $e(b_1) = \frac{1}{3}$. Numerous local minima caused by inevitable fluctuations make any adaptive searching method ineffective.

4. Statistical-property-based attacks

The analysis of EFA is directly based on the dynamics of chaotic system. A large class of attacks are based on the statistical properties of ciphertexts. It is thus important to investigate the statistics of the transmitted signal S_n (or equivalently, keystream K_n)

in order to qualify the practical security of our system.

The statistics of the keystream is obviously determined by the chaotic transmitter (note: EFA is applied to evaluate the nonchaotic receiver system). We first investigate various order-q probability distributions of the keystream K_n (precisely, $k_n = K_n/2^\nu$) for arbitrary initial condition and plaintext at the secret key a_i=0.5, $i = 1, 2, 3, 4$. For $q = 1$ and 2 we find very good uniform distributions $\rho(k_n)$ and $\rho(k_n, k_{n-1})$ in Figs.3(a) and (b), respectively (we use 10^2 meshes for (a) and $10^2 \times 10^2 = 10^4$ meshes for (b) for computing the probabilities). We have computed the order-q probability distributions $\rho(k_n, \ldots, k_{n-q-1})$ for $q \leq 20$, and found uniform random distributions in all these orders.

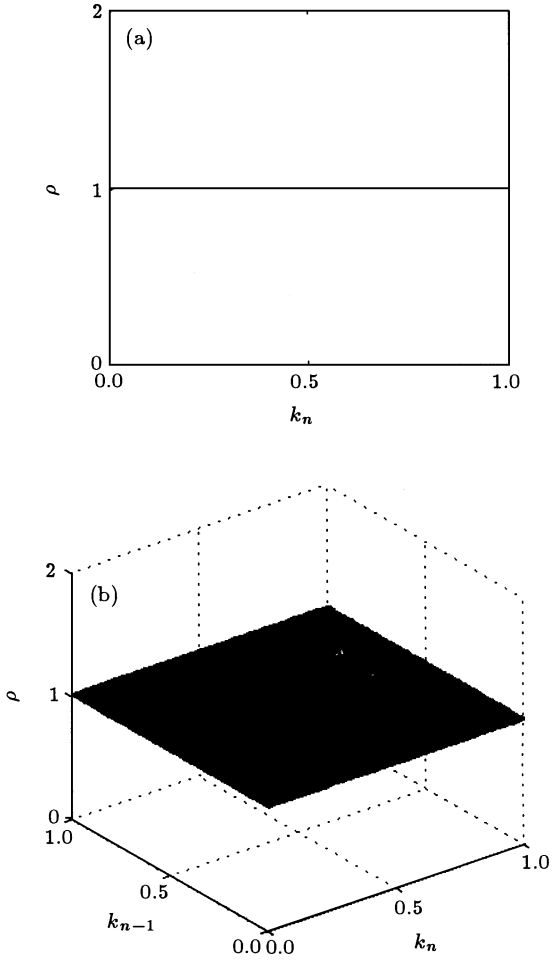


Fig.3. Probability distributions of keystream $\rho(k_n, \ldots k_{n-q+1})$ of order-1 and order-2 plotted vs k_n with $k_n = K_n/2^\nu$. (a) $q = 1$; (b) $q = 2$. Probability distributions are satisfactorily uniform.

In Eq.(1) the keystream K_n is represented by a binary sequence. It is interesting to find that in the sequence bit 0 and bit 1 have the same probabilities to appear. We compute the probabilities of 0 runs of length n $\underbrace{10\ldots01}_{n}$ [or 1 runs of length n $\underbrace{01\ldots10}_{n}$] $P_0(n)$ [$P_1(n)$], and plot the probabilities $P_{0,1}(n)$ vs n in Fig.4.

$$P_{0,1}(n) = \frac{M_{0,1(n)}}{M_{0,1}}, \quad M_{0,1} = \sum_{n=1} M_{0,1}(n), \qquad (7)$$

with $M_{0,1}(n)$ being the numbers of 0 runs and 1 runs of length n, respectively. In Fig.4 squares (circles) represent the numerical results of $P_0(n)$ [$P_1(n)$] of K_n sequence of our system (10^9 bits are used). For a truly random binary sequence of infinite length we should have $P_{0,1}(n) \propto \left(\frac{1}{2}\right)^n$ (solid curve). The almost complete agreement between the numerical data and theoretical further verifies the good randomness-like statistical properties of our chaotic keystream K_n.

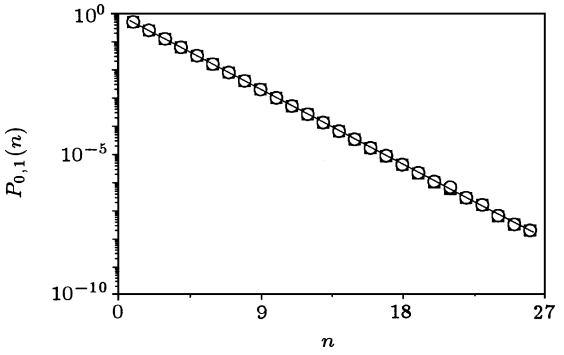


Fig.4. $P_{0,1}(n)$ vs n with $P_{0,1}(n)$ defined in Eq.(7). Squares and circles show the numerical data for 0 runs and 1 runs of length n, respectively, and the solid line denotes the statistics of purely random $\{0, 1\}$ sequences $P(n) \propto \left(\frac{1}{2}\right)^n$. Both numerical and theoretical results are practically indistinguishable.

With the satisfactory random statistics of the keystream K_n, one can predict excellent random properties of the transmitted signal S_n (or $s_n = S_n/2^\nu$) for arbitrary plaintext I_n. In Figs.5(a)–(c), we plot order-2 probability distributions of the transmitted signal S_n, $\rho(s_n, s_{n-1})$, for three plaintexts, $I_n = 0$ [(a)], $I_n = 2^{31}$ [(b)], and I_n=int$\left[\frac{1}{2}\left(1+\sin\frac{\pi n}{10}\right)\times 2^{32}\right]$ [(c)], respectively. For characteristically different plaintexts we observe statistically same probability distributions of ciphertexts. From Figs.5(a)–(c), it is clear that the characteristics of plaintext are well hidden in the corresponding ciphertext, and one can hardly catch any trace of plaintext from the available ciphertext. In conclusion, all the tested order-q distributions in Figs.3–5 show maximum Shannon information entropy under the resolutions adopted. We would like to emphasize that it is observed, for the first time to our

knowledge, that a chaotic cryptosystem can produce keystream and transmitted signal with such satisfactory random statistical properties, and these statistical properties are desirable for secure communications.

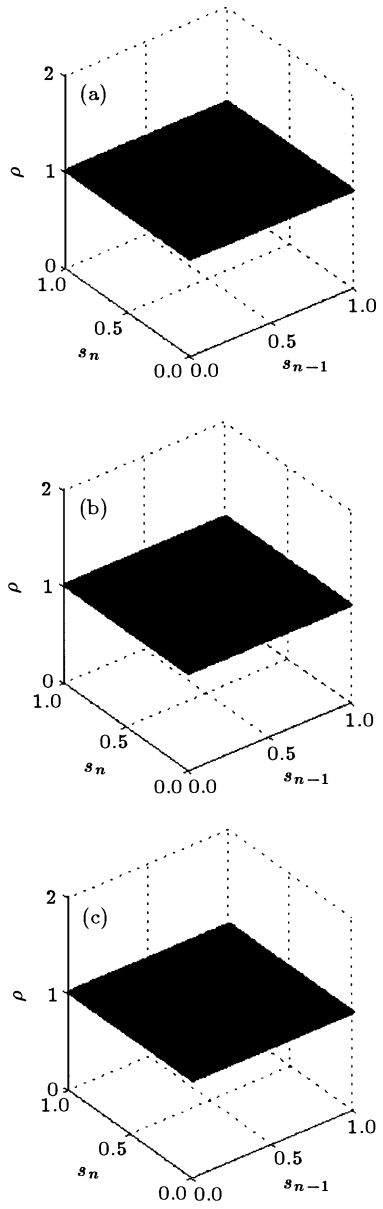


Fig.5. $s_n = S_n/2^\nu, i_n = I_n/2^\nu$.(a)–(c) Order-2 probability distributions $\rho(s_n, s_{n-1})$ with different plaintexts I_n. (a) $I_n = 0$; (b) $I_n = 2^{31}$; (c) $I_n = \text{int}\left[\frac{1}{2}\left(1+\sin\frac{\pi n}{10}\right)\times 2^{32}\right]$. Uniform distributions are identically observed in all figures (a)–(c).

All attacks based on analysing the statistical properties of the transmitted signals, such as linear attacks and differential attacks in conventional cryptanalysis, are actually attacking the transmitters of which the trajectories are chaotic and dependent on both the secret key $\boldsymbol{a}$ and the initial variables $x_0(j), j = 1, 2, \ldots, N$. In analysing chaotic cryptosystems these attacks are often much less effective than EFA (Eq.(5)) (which attacks receivers with nonchaotic dynamics and thus with no sensitivity to the initial conditions) unless the statistical behaviour of S_n shows some serious weakness. With the random-like features demonstrated in Figs.3–6, the statistics-based attacks are practically invalid: e.g., linear attacks [26] are certainly ineffective with the properties of Figs.1, 2, and 5 and differential attacks [27] can hardly work with the statistical relations of Figs.3–5. Incidentally, we have checked the random properties of the transmitted signal S_n with the 16 types of NIST Standard Evaluations [28] for arbitrary plaintexts. Our system passes all the checks satisfactorily. According to the analysis of this section, our system has such appropriate random-like statistical behaviours that there is no weakness (within the resolution and sampling data adopted) left for statistics-based attacks, which can therefore hardly be more effective than the EFA method or the brute force attack.

In chaotic cryptanalysis, some attacks like nonlinear dynamics forecasting and dynamics reconstruction [11–14] are currently very popular. These attacks all belong to the private-structure attacks (the Kerckhoff principle not required). Without having the information of system dynamics these attacks are incomparably less effective than EFA. Moreover, with the uniform and random-like distributions of the return maps of Figs.3–5, system dynamics reconstruction and secret key extraction are hardly possible. In conclusion, these attacks must be weaker than the EFA method and the brute force attack with its evaluation efficiency.

5. Plaintext-known attacks based on analytical solutions

Since the cryptosystem Eqs.(1)–(3) is based on analytical computation of chaos; one must investigate the possibility of attacks by directly solving the secret key from known plaintexts, public systems dynamics, and accessible ciphertexts. The cost of the analytical solution attack can be roughly estimated as follows. In Eq.(1d), given $x_n(N)$ and $x_{n-1}(N)$ we can solve $x_n(N-1)$ (there are two $x_n(N-1)$ solutions for a given $f[x_n(N-1)]$), and with known $x_n(N), x_{n-1}(N)$ and $x_{n-2}(N)$ we can solve $x_n(N-1), x_{n-1}(N-1)$ and then $x_n(N-2)$ successively. With an $x_n(N)$ sequence of $N+1$ successive iterations $x_n(N), \ldots, x_{n-N}(N)$, we

can specify 2^N equations

$$\begin{aligned} x_n(0) =& \frac{S_n}{2^\nu} \\ =& G_i[x_n(N), x_{n-1}(N), \ldots, \\ & x_{n-N}(N), a_1, a_2, \ldots, a_m], \\ i =& 1, 2, \ldots, 2^N, \end{aligned} \tag{8}$$

with functions G_i explicitly given, but only one of the 2^N equations gives the correct solutions of a_j. Since there are m secret parameters $(a_1, a_2, \ldots, a_m)$, we need a set of m algebraic equations of (8) for fixing $a_j, j = 1, \ldots m$. This can be easily done by collecting m signal sequences, each having $N+1$ successive elements,

$$\begin{aligned} \frac{S_{n_j}(j)}{2^\nu} =& G_{ij}[x_{n_j}(N), x_{n_j-1}(N), \ldots, \\ & x_{n_j-N}(N), a_1, a_2, \ldots, a_m], \\ j =& 1, 2, \ldots, m, \end{aligned} \tag{9}$$

where we have again $i = 1, 2, \ldots, 2^N$. In Eq.(9), the sequences $x_{n_j}(N)$ cannot be directly observed by the intruder; this is related to the accessible keystream K_{n_j} by the modulo operation Eq.(1e). $x_{n_j}(N)$ can be obtained from K_{n_j}, not one to one, but one K_{n_j} to $2^{\mu-\nu}$ possible x_{n_j}. Considering also the modulo operation in Eq.(1b), we need to deal with $2^{mN+2m(N+1)(\mu-\nu)}$ possible forms of Eq.(9), from which only one gives the secret values of a_j. Since the parameters are fixed, take $N = 10, m = 4, \mu = 50, \nu = 32$, we should test about

$$2^{mN+2m(N+1)(\mu-\nu)} = 2^{1936} \approx 10^{580} \tag{10}$$

equations of Eq.(9). This attack is obviously much less effective than EFA as well as the brute force attack.

6. Chosen-ciphertext attack based on analytical solution

The chosen-ciphertext attack belongs to the strongest attacks according to the classification of Sec.2 (see Ref.[16]). This method is particularly effective for attacking chaotic cryptosystems because analytical computation can greatly enhance the efficiency of the chosen-ciphertext evaluations.

Here we apply the chosen-ciphertext attack for evaluating our system. For the m parameters of the secret key $\boldsymbol{a}$ we input m ciphertext constants

$$S_n(j) = A_j, \quad j = 1, 2, \ldots, m, \tag{11a}$$

which yield the corresponding m constant keystreams

$$K_n(j) = B_j, \quad j = 1, 2, \ldots, m. \tag{11b}$$

According to the arguments of Eqs.(8) and (9), we obtain 2^{mN} equations

$$\begin{aligned} \frac{A_j}{2^\nu} =& G_{ij}[B_j; a_1, a_2, \ldots, a_m], \quad i = 1, 2, \ldots, 2^N, \\ j =& 1, 2, \ldots, m \end{aligned} \tag{11c}$$

for determining the secret key $\boldsymbol{a}$.

(i) Without the modulo operation of Eq.(1e) and the S-box of Eq.(1b), we have $x(N, j) = B_j$, and there are 2^{mN} sets of nonlinear algebraic equations, each set containing m equations for m variables $(a_1, a_2, \ldots, a_m)$. One of these 2^{mN} sets gives correct solutions of $(a_1, a_2, \ldots, a_m)$. The cost of the chosen-ciphertext attack is of order 2^{mN}. For $m = 4, N = 10$, the cost is about 2^{40}, which is incomparably smaller than the brute force attack.

(ii) With the modulo operation Eq.(1e) and without the S-box of Eq.(1b), each B_j may be truncated from $2^{\mu-\nu}$ possible $x(N, j)$; there are thus $2^{mN+m(\mu-\nu)}$ sets of equations, each set again contains m equations for m variables $(a_1, a_2, \ldots, a_m)$. In these sets, only one set can yield correct solutions of the key parameters. In our case we take $\mu - \nu = 20$, and the cost of the attack is of order 2^{120} which is still considerably less than that of the brute force attack 2^{180}.

(iii) With both the modulo Eq.(1e) and the S-box Eq.(1b), i.e. considering the full analytical computation and the algebraic operations of Eqs.(1), the parameters $(a_1, a_2, \ldots, a_m)$ can no longer be computed by the analytical algebraic equations of Eq.(11c). In order to expose the secret key one has to test all possible bit chains of $(a_1, a_2, \ldots, a_m)$, and the number of tests in (ii) should be multiplied of the attack by a factor of 2^{mh} with h being the length of bits of parameter a_i. Thus the cost reads approximately as

$$\text{cost} \approx 2^{mN+m(\mu-\nu)} \cdot 2^{mh}.$$

With $m = 4$, $N = 10$, $\mu - \nu = 20$ and $h = 45$, we obtain

$$\text{cost} \approx 2^{308} \approx 10^{90}, \tag{12}$$

which is much larger than the cost of the brute force attack. It is noticed that the cost of Eq.(12) (for the chosen-ciphertext attack) is greatly reduced from Eq.(10) (for the plaintext-known attack). This is reasonable since for the former the intruder can freely choose constant ciphertext drivings which can be used

to expose the secret key much more efficiently while for the latter this convenience cannot be enjoyed.

Since chosen-ciphertext attacks are among the most effective attacks for cryptanalysis, we expect that the security determined by EFA in Figs.1 and 2 and Eq.(6) may be the practical security of systems (1)–(4).

7. Conclusion and discussion

It is emphasized that the above security estimates by various attacks are valid under the condition that the periodicity of chaos realization by finite-precision computers does not play a role. The problem of periodicity of computer realization of chaos has been investigated in detail in the past.[29−32] Recently, we have made an estimate of the length of period of our system as $T \propto 10^{(\alpha+\beta h)N}$ with $\alpha \approx -0.35$, $\beta \approx 0.47$ and 10^{-h} being the precision of computer simulation. For double precision computation we have approximately $h = 16$. Therefore, T can be roughly estimated in our system ($N = 10$) as $T \approx 10^{70} \approx 2^{230}$, which restricts the level of the highest security. It is obvious that the security estimate of Eq.(6) is not affected. If a security criterion requires a cost up to T iterations, one should use our system Eq.(1) with size N,

$$N > \frac{1}{\alpha + \beta h} \log_{10} T. \tag{13}$$

Otherwise any security declaration equal to or larger than T is meaningless due to the limitation of the periodicity of computer realization of chaos.

Apart from the desirable property of high security, our system has also some optimal overall cryptographic properties with slight modifications and improvements. For instance, the encryption (decryption) speed can be faster than that of AES with parallel encryption (decryption) operations of multiple space units.[22] It is confirmed that all the security estimates in the present paper remain practically unchanged when the multiple-channel encryptions (decryptions) are performed in parallel.

References

[1] Pecora L M and Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
[2] Cuomo L M and Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65
[3] Kocarev L, Halle K S, Eckert K, Chua L O and Parlitz U 1992 *Int. J. Bif. Chaos* **3** 709
[4] Kocarev L and Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028
[5] Xiao J H, Hu G and Qu Z L 1996 *Phys. Rev. Lett.* **77** 4162
Hu G, Xiao J H and Yang J Zh 1997 *Phys. Rev.* E **56** 2738
[6] Van Wiggeren D G and Roy R 1998 *Science* **279** 1198
[7] Sundar S and Minai A A 2000 *Phys. Rev. Lett.* **85** 5456
[8] Garcia-Ojalvo J and Roy R 2001 *IEEE Trans. Circuits Syst.* I **48** 1491
[9] Luo X S and Fang J Q 2000 *Chin. Phys.* **5** 333
[10] Short K M 1994 *Int. J. Bif. Chaos.* **4** 1491
[11] Perez G and Cerdeira H 1995 *Phys. Rev. Lett.* **74** 1970
[12] Short K M 1996 *Int. J. Bif. Chaos* **6** 367
Short K M and Parker A T 1998 *Phys. Rev.* E **58** 1159
[13] Zhou C S and Lai C H 1999 *Phys. Rev.* E **60** 320
Zhou C S and Lai C H 1999 *Phys. Rev.* E **59** 6629
[14] Parker A T and Short K M 2001 *IEEE. Trans. Circuits Syst.* I **48** 624
[15] Kocarev L 2001 *IEEE Circuits Syst. Magn.* **1** 6
[16] Dachselt F and Schwarz W 2001 *IEEE Trans. Circuits Syst.* I **48** 1498
[17] Wang S H, Kuang J Y, Li J H, Luo Y L, Lu H P and Hu G 2002 *Phys. Rev.* E **66** 065202
[18] Tang G N, Wang S H, Lu H P and Hu G 2003 *Phys. Lett.* A **318** 388
[19] Kuang J Y, Deng K and Huang R H 2001 *Acta Phys. Sin.* **10** 1856 (in Chinese)
[20] Wong W K 2002 *Phys. Lett.* A **298** 238
[21] Pareek N K, Patidar V and Sud K K 2003 *Phys. Lett.* A **309** 75
[22] Wang S H, Ye W P, Lu H P, Kuang J Y, Li J H, Luo Y L and Hu G 2003 *Commun. Theor. Phys.* **40** 57
[23] Murali K 2001 *Phys. Rev.* **E 63** 016217
[24] Leung H, Yu H and Murali K 2002 *Phys. Rev.* E **66** 036203
[25] Lu H P, Wang S H, Li X W, Tang G N, Kuang J Y, Ye W P and Hu G, submitted; also see, http://arxiv.org, nlin.CD/0305012
[26] Matsui M 1994 *Advances in Cryptology—Eurocrypt'93 Proc.* (Berlin: Springer) p386
[27] Biham E and Shamir A 1991 *J. Crypt.* **4** 3
[28] A. Rukhin *et al NIST Special Publication 800-22* http://csrc.nist.gov/encryption/aes
[29] Matthews R 1989 *Cryptologia* **13** 29
[30] Wheeler D D 1989 *Cryptologia* **13** 243
[31] Grebogi C, Ott E and Yorke A 1988 *Phys. Rev.* A **38** 3688
[32] Bastolla U and Parisi G 1987 *J. Phys. A: Math. Gen.* **30** 5613