Vol 16 No 8, August 2007
1009-1963/2007/16(08)/2254-05

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Application of periodic orbit theory in chaos-based security analysis

Long Min(龙 敏)[a] and Qiu Shui-Sheng(丘水生)[b]

[a] *College of Computer and Communication, Changsha University of Science and Technology, Changsha* 410076, *China*

[b] *College of Electronic & Engineering, South China Univ. of Technology, Guangzhou* 510640, *China*

(Received 22 August 2006; revised manuscript received 20 November 2006)

Chaos-based encryption schemes have been studied extensively, while the security analysis methods for them are still problems to be resolved. Based on the periodic orbit theory, this paper proposes a novel security analysis method. The periodic orbits theory indicates that the fundamental frequency of the spiraling orbits is the natural frequency of associated linearized system, which is decided by the parameters of the chaotic system. Thus, it is possible to recover the plaintext of secure communication systems based on chaotic shift keying by getting the average time on the spiraling orbits. Analysis and simulation results show that the security analysis method can break chaos shift keying secure communication systems, which use the parameters as keys.

Keywords: periodic orbit theory, secure communication, chaos-based security analysis
PACC: 0545

1. Introduction

Chaos-based encryption is a popular research area nowadays. Many methods have been put forward,[1−9] and how to evaluate their security is becoming an urgent problem to be resolved. In traditional cryptography, security is mainly based on number theory and difficult problems, while chaos-based cryptography is based on the characteristics of the chaotic signals. For this reason, not all analysis methods for traditional cryptography are suited for chaos-based cryptography, so it is necessary to study secure analysis methods based on chaos theory. Recently, some analysis methods were proposed.[10−14] Short and Parker added cryptanalysis to the chaotic masking secure communication scheme by using nonlinear dynamic forecasting.[10] Yang *et al* added cryptanalysis to the chaotic masking and the chaotic modulating secure communication system by using return maps,[11] and added cryptanalysis to the chaotic shift keying secure communication system by using the spectrogram analysis method.[12] Wang *et al* proposed error function attack[13] and indicated that the security of some secure communications systems based on chaos synchronization is not secure enough. Based on the periodic orbit theory, a novel security analysis method is proposed. The periodic orbit theory indicates that the space-bifurcation region is a rooted cause for sensitive dependence upon initial conditions, and direct motion orbits are the reason for the broadband spectrum of chaotic signal, while the fundamental frequency of the spiraling orbits is the natural frequency of associated linearized system, which is decided by the parameters of the chaotic system. Thus, it is possible to recover the plaintext of secure communication systems based on chaotic shift keying by getting the average time of spiraling motion.

2. Periodic orbit theory

In this section, we overview the periodic orbit theory proposed in Refs.[15,16]. The third-order autonomous dynamical system is considered:

$$\frac{\mathrm{d}x}{\mathrm{d}t} = f(x), \quad x \in R^3, \tag{1}$$

where $f : R^3 \to R^3$ is p-times differentiable ($p \geq 1$) with a continuous derivative, R^3 stands for the three-dimensional real space, and $f(\cdot)$ is a nonlinear function.

x_e is an equilibrium position of Eq.(1) and $f(x_\mathrm{e}) = 0$. The linearized system of Eq.(1) can be written as

$$\frac{\mathrm{d}x}{\mathrm{d}t} = Df(x_\mathrm{e})x, \tag{2}$$

where $Df(x_\mathrm{e})$ is the Jacobian of f evaluated at x_e. Let γ and $\sigma \pm \mathrm{j}\omega_0$ be the eigenvalues of $Df(x_\mathrm{e})$, where

γ, σ and ω_0 are real and $\omega_0 \neq 0$. We call x_e a saddle focus (a semi-stable equilibrium point) if

$$\sigma\gamma < 0. \tag{3}$$

Furthermore, if

$$|\gamma| > |\sigma| > 0 \tag{4}$$

then the system satisfies the so-called Shil'nikov inequality. The solution of the linearized system of Eq.(1) is

$$\delta x = \delta x_d + \delta x_s, \tag{5}$$

where $\delta x = x - x_e$ (for small δx) $\delta x_d = k_1 e^{\gamma t}\xi$, $\delta x_s = 2k_2 e^{\sigma t}(\eta_r \cos(\omega_0 t + \phi) - \eta_i \sin(\omega_0 t + \phi))$. Where k_1, k_2 and ϕ are constants, η_r and η_i are the real and imaginary parts of the eigenvectors associated with the complex conjugate pair of eigenvalues, and ξ is the eigenvector associated with the real eigenvalue. A segment of trajectory corresponding to (δx_d) is a typical direct motion, and that corresponding to δx_s is a spiral motion. Fig.1 shows a saddle periodic orbit, which consists of a spiral trajectory segments x_s and a direct motion trajectory segment x'_d. Both are relative to the saddle focus x_e, and x_s is on S_1, while x'_d is on the folded surface S_2. Note that other direct motion trajectories are not on S_1 and S_2.

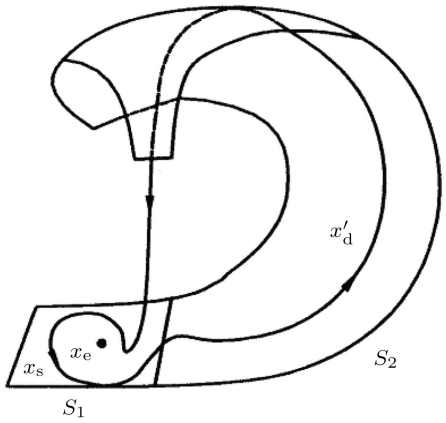


Fig.1. A saddle periodic orbit.

A chaotic attractor consists of many recurving orbits, and there exists a countable sequence t_n (for $n \in (-\infty, +\infty)$) of times at which the nth recurving orbits, consisting of segments $x_{s,n}$ and $x_{d,n}$, start to appear. The dividing point of the nth direction trajectory $x_{s,n}$ and $x_{d,n}$ near SPO can be found by inspecting ρ_L which is defined by

$$\rho_L = \min\{\,|x - x_L|\,\} \quad \text{for} \quad x_L \in L. \tag{6}$$

The dividing point is defined as the point where ρ_L is minimum. Note that $d\rho_L/dt$ has a sharp turning point near the dividing point at which the trajectory moves off rapidly from S. This can be used for computation of the dividing point. Likewise, another dividing point, one between $x_{d,n}$ and $x_{s,n+1}$, corresponds to the minimum value of ρ_e, where

$$\rho_e = |x - x_e|\,. \tag{7}$$

The dividing points of x_s and x_d near the SPO, called space-bifurcation points, form a space-bifurcation region. A moving phase point passing a space-bifurcation point will switch randomly, under perturbation, between a trajectory in S and one in D.

3. Security analysis for chaotic shift keying

The periodic orbits theory indicates that space-bifurcation region is a rooted cause for sensitive dependence upon initial conditions, and appearance of direct motion orbits is the reason for the broadband spectrum of chaotic signal. However, the fundamental frequency of the spiraling orbits is the natural frequency of associated linearized system, which is decided by the parameters of the chaotic system. In Ref.[17], the inherent frequency of the Lorenz attractor is found by decomposing the attractor into two separate scrolls and 1D discrete-time zero-crossing series, that is, the attractor is decomposed into spiral orbits and direct orbits. To some extents, the fundamental frequency of the spiraling orbits is the secret for the chaos secure communication which uses parameters as keys. As a result, a scheme based on short-time period estimation is proposed in Ref.[18] to break some chaotic parameters modulation methods. From Eq.(5), we learn that the rotation angular speed on the spiraling orbits is associated with σ and ω_0, which is decided by the parameters of the system. Therefore, the moving time spent on the spiraling orbits in the systems with different parameters is different. In chaotic secure communication based on parameter modulation, one of the parameters in the system is changed according to the binary information, and one of state variable of the system is transmitted as the ciphertext. Consequently, by collecting the spiral orbits and computing the average rotation time on it, we introduce an easier way in this

section to analyse chaotic secure communication system based on parameter modulation, and this method can be not only used in the double-scroll Lorenz-like chaotic attractors, but also in single-scroll Rossler-like chaotic attractors. However, how to get the spiraling orbits? In Ref.[19], authors use the magnitude of one of the variables to determine the dividing points (space-bifurcation points). We adopt this method to determine which orbits belong to the spiraling orbits. For example, when the direct orbits go between the neighbourhoods of the two saddle foci, as shown in Fig.2(a), we can get spiraling orbits when x satisfies

$$x > m_1 \quad \text{or} \quad x < m_2. \tag{8}$$

When the direct orbits return to the neighbourhood of the same saddle focus, we may use

$$x < m \tag{9}$$

to get spiraling orbits. See Fig.2(b).

After getting the spiral orbits of corresponding messages, we can compute the average rotation time of the spiral orbits. We may find the difference in the average rotation time corresponding different parameters, and the difference is much enough to distinguish the messages. The Lorenz system, Chua's system and Rossler system are employed to show the efficiency of this method.

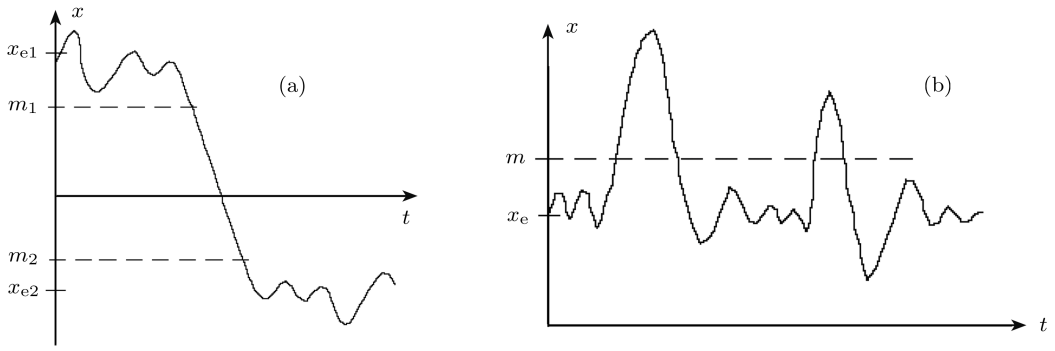


Fig.2. Getting the spiral orbits by measuring the magnitude: (a) direct orbits traverse between neighbourhoods of two saddle foci; (b) direct orbits returns to the neighbourhood of the same saddle focus.

The Lorenz system is

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1), \\ \dot{x}_2 &= cx_1 - x_1x_2 - x_2, \\ \dot{x}_3 &= x_1x_2 - b_1x_3. \end{aligned} \tag{10}$$

When $a = 16$, $b = 8/3$, $c = 45.6$, the Lorenz system has a double-scroll chaotic attractor which is shown in Fig.3(a). The moving phase point passing a space-bifurcation point will switch randomly between spiral orbits and direct orbits. If it switches to direct orbits, the phase point will jump form one scroll to the other scroll and then move on another spiral orbit. In chaos shift keying,[20] parameter b is controlled by the binary information m which is shown in Fig.3(b). $b = 8/3$ and $b = 10/3$ mean that messages $m = 0$ and 1 respectively. x_2 is the transmitted signal as shown in Fig.3(c). As discussed in the previous text, the rotation angular speed on the spiraling orbits is different when $b = 8/3$ and $b = 10/3$, so the average rotation time on the spiraling orbits is also different. Firstly, we collect all the spiraling orbits of the corresponding message according to the above method, and then compute the average rotation time $A(t)$ as shown in Fig.3(d). We can find that each $A(t)$ corresponding to each bit of the plain-signal is long or short, and the difference between $A(t)$ corresponding to the plaintext '0' and $A(t)$ corresponding to the plaintext '1' is enough to distinguish, so we can recover the original messages shown in Fig.3(e). It should be pointed out that each $A(t)$ corresponding to same messages is irregular because the moving phase point passing on the spiral orbits is just nearly periodic, and the method to get the spiraling orbits by the magnitude is not an accurate way. Sometimes it will result in errors in the recovering of the plaintext, but the bit error rate (BER) is less than 10^{-3}.

Chua's system with cubic nonlinearity is[21]

$$\begin{aligned} \dot{x}_1 &= k\alpha(x_2 - bx_1^3 - cx_1), \\ \dot{x}_2 &= k(x_1 - x_2 + x_3), \\ \dot{x}_3 &= -k\beta x_3, \end{aligned} \tag{11}$$

where $k = 4$, $\alpha = 10$, $c = -0.143$, $\beta = 14$. The chaotic attractors are shown in Fig.4(a). In chaos shift keying,[20] parameter β is controlled by the bi-

nary messages m as shown in Fig.4(b). $\beta = 14$ and $\beta = 15$ means that the message $m = 0$ and 1 respectively. x_1 is the transmitted signal as shown in Fig.4(c). The average rotation time $A(t)$ is shown in Fig.4(d), and the recovered messages are shown in Fig.4(e). The BER in recovering the plaintexts is less than 4×10^{-3}.

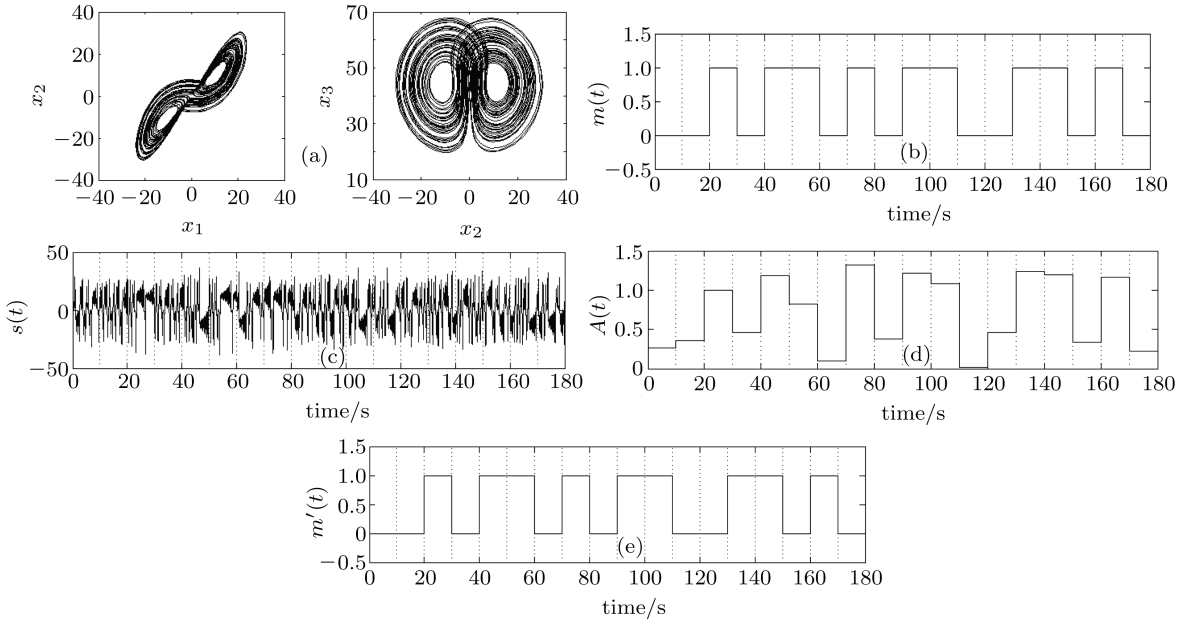


Fig.3. (a) Attractor of Lorenz. (b) Messages. (c) Transmitted signal. (d) $A(t)$. (e) Recovered messages.

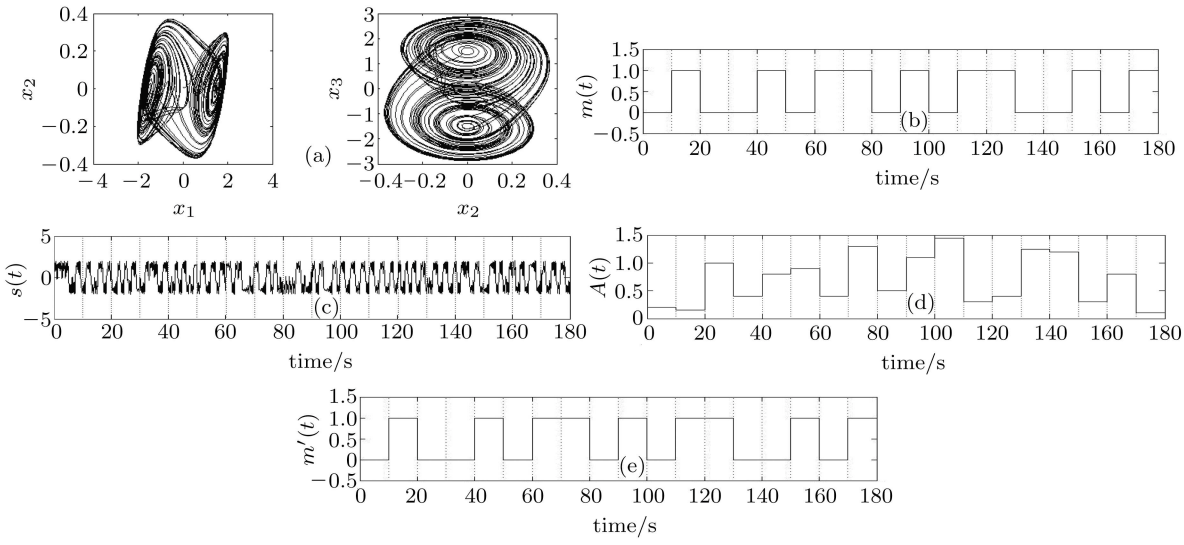


Fig.4. (a) Attractors of Chua's system with cubic nonlinearity. (b) Messages. (c) Transmitted signal. (d) $A(t)$. (e) Recovered messages.

The Rossler system is

$$\begin{aligned} \dot{x}_1 &= -(x_2 - x_3), \\ \dot{x}_2 &= x_1 + a x_2, \\ \dot{x}_3 &= x_3(x_1 - c) + b. \end{aligned} \tag{12}$$

When $a = 0.2$, $b = 0.2$ and $c = 4.7$, the system has a single-scroll attractor as shown in Fig.5(a). In chaos shift keying,[20] parameter c is controlled by the binary messages m, as shown in Fig.5(b). $c = 5$ and $c = 4.5$ mean that the message $m = 0$ and 1 respectively. v_1 is the transmitted signal, as shown in Fig4.(c). We can collect the spiraling orbits as the method described in

Fig.2 (b), and the average rotation time $A(t)$ is shown in Fig.4 (d), and the recover the messages is shown in Fig4.(e). The BER in recovering the plaintexts is less than 2×10^{-3}.

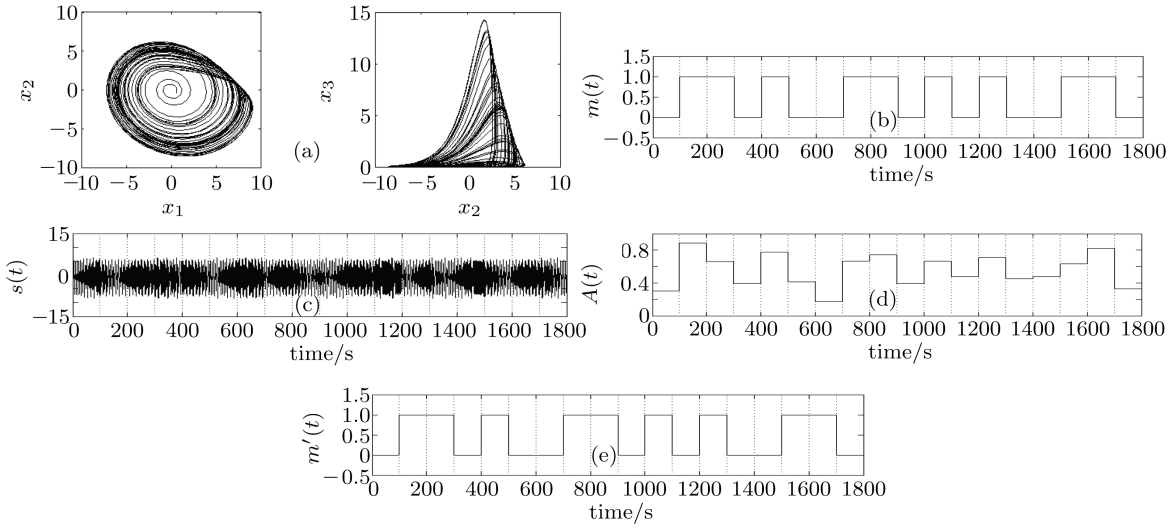


Fig.5. (a) Attractors of Rossler. (b) Messages. (c) Transmitted signal. (d) $A(t)$. (e) Recovered messages.

4. Conclusions

Based on the periodic orbit theory, a novel security analysis method is proposed. It can successfully break chaos shift keying secure communication systems without complex computation by getting the average time on the spiraling orbits. Compared with security analysis methods such as return maps and nonlinear prediction, the proposed method is simple and can be easily realized.

References

[1] Zhang J S and Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese)

[2] Li G H, Xu D M and Zhou S P 2004 *Acta Phys. Sin.* **53** 706 (in Chinese)

[3] Li J F, Li N and Lin H 2004 *Acta Phys. Sin.* **53** 1694 (in Chinese)

[4] Li J G and Xi Y G 2005 *Chin. Phys.* **14** 274

[5] Zhang L H, Liao X F and Wang X B 2005 *Chaos, Solitons and Fractals* **24** 759

[6] Yu L H and Fang J C 2005 *Acta Phys. Sin.* **54** 4012 (in Chinese)

[7] Peng F, Qiu S S and Long M 2005 *Acta Phys. Sin.* **54** 4562 (in Chinese)

[8] Celikovsky S and Chen G R 2005 *IEEE Trans. Automation Control.* **50** 76

[9] Sun L and Jiang D P 2006 *Acta Phys. Sin.* **55** 3283 (in Chinese)

[10] Short K M and Parker A T 1998 *Phys. Rev.* E **58** 59

[11] Yang T, Yang L B and Yang C M 1998 *Phys. Lett.* A **245** 495

[12] Yang T, Yang L B and Yang C M 1998 *Phys. Lett.* A **247** 105

[13] Wang X G, Zhan M and Lai C H 2004 *Chaos* **14** 128

[14] Lü H P, Wang S H, Li X W, T G N, K J Y, Ye W P and Hu G 2004 *Chin. Phys.* **13** 625

[15] Qiu S S 2003 *Journal of Circuits and Systems* **8** 1

[16] Qiu S S 2004 *Journal of Circuits and Systems* **9** 1

[17] Alvarez G, Li S J, Lü J H and Chen G R 2004 ArXiv: nlin. CD/0406031

[18] Alvarez G and Li S J 2004 ArXiv: nlin.CD/0406039

[19] Qiu S S, Tse C K and Zhou Y F 2002 *Int. Symp. Nonl. Theory Appl. Xi'an* 215

[20] Dedieu H, Kennedy M P and Hasler M 1993 *IEEE Trans. Circutis and System* II **40** 634

[21] Huang A, Pivka L and Wu C W 1996 *Int. J. Bif. Chaos.* **6** 2175