Vol 17 No 4, April 2008
1674-1056/2008/17(04)/1202-07

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

# Breaking chaotic shift key communication via adaptive key identification*

Ren Hai-Peng(任海鹏)[a)b)†], Han Chong-Zhao(韩崇昭)[a)], and Liu Ding(刘 丁)[b)]

[a)] *State Key Laboratory for Manufacturing Systems Engineering, Xi'an Jiaotong University, Xi'an 710049, China*

[b)] *School of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710048, China*

(Received 26 April 2007; revised manuscript received 25 August 2007)

This paper proposes an adaptive parameter identification method for breaking chaotic shift key communication from the transmitted signal in public channel. The sensitive dependence property of chaos on parameter mismatch is used for chaos adaptive synchronization and parameter identification. An index function about the synchronization error is defined and conjugate gradient method is used to minimize the index function and to search the transmitter's parameter (key). By using proposed method, secure key is recovered from transmitted signal generated by low dimensional chaos and hyper chaos switching communication. Multi-parameters can also be identified from the transmitted signal with noise.

**Keywords:** chaotic shift key, adaptive synchronization, conjugate gradient method, parameter identification

**PACC:** 0545

## 1. Introduction

Since Pecora and Carroll demonstrated chaos synchronization and its potential application to secure communication,[1,2] chaotic secure communication has been an active area of research for the past few years.[3] Chaotic secure communication has evolved into several forms, including chaotic masking,[4] chaotic shift key[5] and chaotic modulation[6] etc.. The development of chaotic secure communication technique followed a path twisting up the hill of security. Breaking the existing chaotic secure communication schemes and improving security performance of the existing methods became the focus and motivation of the research.[7−24]

The return map[7] was introduced to break original chaotic masking by using simple chaotic attractors proposed by Ref.[4]. The hyper-chaotic attractor was proposed for chaotic masking to improve the security of chaotic masking, because of the more complex dynamics of hyper chaos.[8] Nonlinear dynamic forecast method is used to break the hyper-chaotic masking secure communication.[9,10] A modulation method is used to diffuse the return map and to improve security of chaotic communication.[11] A zero cross detection method is proposed to find the modulation function and to unmask the modulation.[12] A chaotic secure communication scheme with key stream is claimed to possess high secure performance.[13] Nonlinear dynamic forecasting method combined with encryption key stream analysis method[14] is introduced to break the scheme proposed in Ref.[13]. The phase information and phase synchronization are used for cipher text transmitting to prevent from common attack method.[15] Brute force analysis is employed to break the phase synchronization in Ref.[16], because of insensitivity of the key mismatch and arrestive spectrum of cipher text. The intermittent chaos, derived from multiple discrete time dynamical systems driven by random noise, is used for encrypting plaintext to improve security.[17] The flaws of the method in Ref.[17] and the breaking methods are given in detail in Ref.[18]. Chaotic modulation using the Lorenz system is attacked and the modulated cipher text is obtained in Ref.[19]. Chaotic shift key communication is also reported which is broken by short time zero crossing rate,[20] spectrum analysis[21] and generalized synchronization.[22] The confliction of efforts to improve the security and to crash the security impels the development of chaotic secure communication

*Project supported by the China Postdoctoral Science Foundation (Grant No 20060390318), Natural Science Foundation of Shaanxi Province (Grant No 2007F017) and Fok Ying Tong Education Foundation.

†E-mail: renhaipeng@xaut.edu.cn

theory and technology. Both efforts help the development.

In this paper, the adaptive key parameter identification method is proposed to break chaotic shift key secure communication. It is assumed that the structure of transmitter is known, which is also referred to as public-structure encryption system.[25] The task to break the chaotic shift key information is implemented, if the different key parameters can be identified and discriminated from the transmitted information in the public channel. To implement the task, the transmitted signal is used to drive a response system at the eavesdropper end with the same structure as the driving system and tunable parameters. The tunable parameters are adaptively adjusted according to the predefined index function about synchronization error and its conjugate gradient information to the parameters. When the synchronization error tends to zero, the key parameter information can be obtained and the binary information transmitted by chaotic shift key can be recovered by this way.

The remainder of this paper is organized as follows: the adaptive key identification problem is formulated, and the identification principle is outlined in Section 2. The conjugate gradient method is introduced for parameter adaptation because of its fast convergence in Section 3. Some numerical experiments are performed in Section 4, including the Lorenz system, and a hyper-chaotic shift key example. Some conclusion remarks are given in Section 5 to summarize this paper.

## 2. Adaptive identification problem descriptions

Two different chaotic attractors, which are derived simply from the chaotic attractor with different parameter sets, are used as medium to transmit binary information with one attractor encoded as '0' and the other encoded as '1'. At the receiver, the binary information is recovered by using the synchronization error. Two chaotic attractors are elaborately designed to have similar statistical feature and similar shape in phase plant to make the eavesdropper difficult to discriminate the binary information from transmitted signal. This method is referred to as chaotic shift key communication, also known as chaotic switching.

The key of chaotic switching is the sensitive dependence property of chaotic dynamics on its initial values and parameters (i.e., two chaotic attractor with a slightly difference on parameters or initial values will evolve in a 'quite different' manner, and will not synchronize without external force.). It is claimed that the eavesdropper without exact parameters of chaotic transmitter will be difficult to synchronize with the transmitter and recover the binary information carried by the transmitted signal in public channel. The security flaws of chaotic shift key communication and some possible attacking methods have been given in Refs.[20–22]. In this paper, a different approach also using the property of the sensitive dependence on parameters is proposed to adaptively identify the parameters of the transmitter and to recover the binary information.

For a known structure transmitter, if the parameter is also known, the drive-response synchronization[1,2] can be achieved. The principle of drive response synchronization is firstly reviewed here to show later how to identify parameters only from the transmitted signal of the chaotic transmitter with unknown parameters.

A nonlinear system is given as

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{F}_{\boldsymbol{\theta}}(\boldsymbol{x}(t)). \tag{1}$$

Where $\boldsymbol{x}$ is the state vector, $\boldsymbol{\theta}$ is the vector of parameters, suppose that the system can be decomposed into two subsystems $\boldsymbol{F}_{s\boldsymbol{\theta}}$ and $\boldsymbol{F}_{u\boldsymbol{\theta}}$ in such a way that the original system can be rewritten as

$$\begin{aligned} \dot{\boldsymbol{x}}_s(t) &= \boldsymbol{F}_{s\boldsymbol{\theta}}(\boldsymbol{x}_s(t), x_{1u}(t)), \\ \dot{\boldsymbol{x}}_u(t) &= \boldsymbol{F}_{u\boldsymbol{\theta}}(\boldsymbol{x}_u(t), x_{1s}(t)). \end{aligned} \tag{2}$$

Where $[\boldsymbol{x}_s(t), \boldsymbol{x}_u(t)] = \boldsymbol{x}^{\mathrm{T}}(t)$, the two subsystems are coupled via the one-dimensional signals $x_{1s}(t) \in \boldsymbol{x}_s(t)$ and $x_{1u}(t) \in \boldsymbol{x}_u(t)$. In general, such decomposition is not always possible, but there exists such decomposition for a large variety of chaotic system. The coupling variables can have greater dimension. In fact in the following example, we will show that more general form of synchronization can be used to identify the parameter.

We will assume that one of those two coupling variables is chosen as output of the system and transmitted in the public channel, which is referred to as $y(t)$, such that the system (2) can be rewritten as

$$\begin{aligned} \dot{\boldsymbol{x}}_s(t) &= \boldsymbol{F}_{s\boldsymbol{\theta}}(\boldsymbol{x}_s(t), y(t)), \\ \dot{\boldsymbol{x}}_u(t) &= \boldsymbol{F}_{u\boldsymbol{\theta}}(\boldsymbol{x}_u(t), x_{1s}(t)). \end{aligned} \tag{3}$$

For the legal receiver with the known same parameters/key (and same structure as pre-assumed above)

as those of the transmitter, the system dynamics can be given as

$$\begin{aligned}\dot{\hat{\boldsymbol{x}}}_s(t) &= \boldsymbol{F}_{s\boldsymbol{\theta}}(\hat{\boldsymbol{x}}_s(t), y(t)),\\ \dot{\hat{\boldsymbol{x}}}_u(t) &= \boldsymbol{F}_{u\boldsymbol{\theta}}(\hat{\boldsymbol{x}}_u(t), \hat{x}_{1s}(t)).\end{aligned} \tag{4}$$

The transmitted signal $y(t)$ is used as driving signal for the response receiver system, the scheme of Pecora and Carroll's drive response synchronization can be shown in Fig.1.

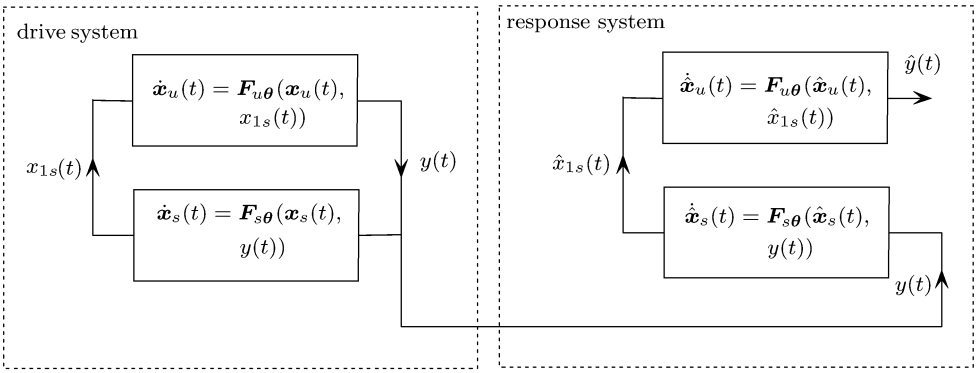



**Fig.1.** General scheme of drive response synchronization.

If the receiver (response) system possesses all negative conditional Lyapunov exponents, the synchronization will occur between transmitter (driving) system and the receiver system, i.e. $\lim\limits_{t\to 0} e(t) = \lim\limits_{t\to 0} |\hat{y}(t) - y(t)| \to 0$.

For a transmitter with unknown parameters, synchronization can not be achieved because of the sensitive dependence of above scheme on parameter mismatch, which is the critical point for chaotic switching to be secure. In the following part of this section, we will show that the aforementioned point can also be used by eavesdropper to identify the unknown parameters of the transmitter and to break the chaotic shift key communication. It has been noticed that the synchronization can be achieved for the receiver with the identical parameters as the transmitter after a period of transient procedure, although the initial values of the receiver are different from those of the transmitter. If the parameters are not identical, synchronization error $e(t)$ will not tend to zero. Therefore, an index function with respect to synchronization error can be defined. The receiver parameters can be adaptively adjusted to minimize the index function and synchronization error. When the synchronization error is zero, the transmitter parameters can be found and the chaotic shift key can be broken.

The idea of adaptively adjusting parameters of the receiver can be described as follows.

Sample the transmitted signal $y(t)$ at a predefined rate, sampled data $y(n)$ represents the value of $y(t)$ at time $t = n\Delta T$, the index function can be defined as

$$V(\hat{\boldsymbol{\theta}}) = e^2(n). \tag{5}$$

Where $e(n) = y(n) - \hat{y}(n)$ is the synchronization error at time $t = n\Delta T$, and $\hat{\boldsymbol{\theta}}$ is the adjustable parameter at the receiver end, which corresponds to the unknown parameters $\boldsymbol{\theta}$ of the transmitter. It is observed that we can get perfect synchronization with $V(\hat{\boldsymbol{\theta}}) = e^2(n) = 0$.

The extremum of the index function Eq.(6) should satisfy the following equation

$$\frac{\partial V(\hat{\boldsymbol{\theta}})}{\partial \hat{\boldsymbol{\theta}}} = -\frac{\partial \hat{y}(n)}{\partial \hat{\boldsymbol{\theta}}} e(n) = 0. \tag{6}$$

Obviously the transmitter parameter $\boldsymbol{\theta}$ is the global minimum of the index function Eq.(5). Therefore, an optimizing method[26] with good performance can be used to adjust $\hat{\boldsymbol{\theta}}(n)$ to ensure

$$\lim_{n\to\infty} \hat{\boldsymbol{\theta}}(n) = \boldsymbol{\theta}. \tag{7}$$

The scheme is given in Fig.2.

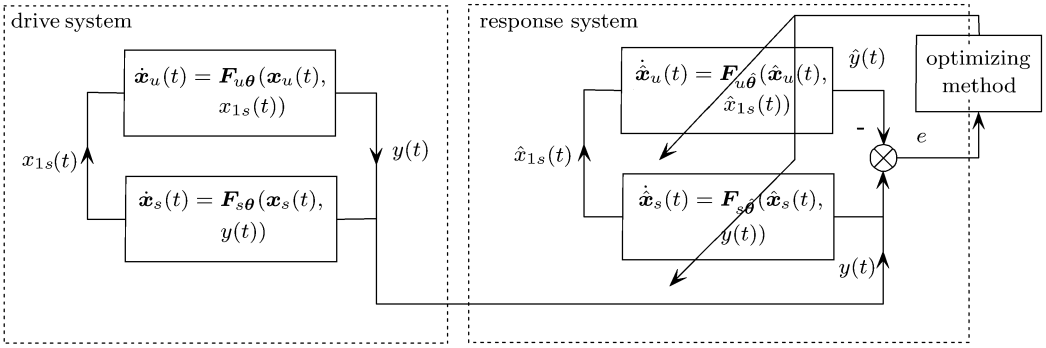



**Fig.2.** Schematic diagram of transmitter parameter/key identification procedure.

From Fig.2, it can be known that the sensitive dependence of chaotic transmitter on system parameters can also be used for the parameter identification and binary information recovery.

The candidate optimizing method will be given in the next section.

# 3. Conjugate gradient method for adaptive identification

To minimize the index function Eq.(5), the parameter adaptation should follow the direction that makes the index function descent. The parameter adaptation algorithm can be given as

$$\hat{\boldsymbol{\theta}}(n+1) = \hat{\boldsymbol{\theta}}(n) - \lambda(n)\boldsymbol{d}(n), \tag{8}$$

where vector $\boldsymbol{d}(n)$ is the direction that makes the index function descent, and $\lambda(n)$ is the step length for adaptation at moment $n$ (i.e., time $t = n\Delta T$).

Here, vector $\boldsymbol{d}(n)$ is chosen as the conjugate gradient, because of its good performance. The conjugate gradient method combines the conjugate property with gradient information of optimizing problem. The conjugate gradient method seeks the point to make the index function minimum along a set of the directions, which is derived from the gradient and conjugate direction of a set of former points. The convergence speed of the conjugate gradient method is very fast.

The steps to seek the parameters can be given as follows.

**Step 1** initialization, set $n = 1$, choose the initial parameter $\hat{\boldsymbol{\theta}}(1)$ randomly, in general, the initial parameter can be chosen according to the known information about the transmitter. Calculate the gradient of the index function about parameter $\hat{\boldsymbol{\theta}}(1)$, which can be given as $\boldsymbol{g}(1) = \nabla V(\hat{\boldsymbol{\theta}}(1))$. If $\|\boldsymbol{g}(1)\| < \varepsilon(\varepsilon$ is predetermined little positive number), then the seeking procedure stops, because the first parameter is the seeking value $\boldsymbol{\theta}$, else set

$$\boldsymbol{d}(1) = -\boldsymbol{g}(1). \tag{9}$$

Where $\boldsymbol{d}(1)$is the initial gradient.

$$\lambda(1) = -\frac{\boldsymbol{g}^{\mathrm{T}}(1)\boldsymbol{d}(1)}{2\boldsymbol{d}^{\mathrm{T}}(1)\boldsymbol{d}(1)}. \tag{10}$$

Where $\lambda(1)$ is the initial step length.

**Step 2** $n = n + 1$, calculate

$$\hat{\boldsymbol{\theta}}(n) = \hat{\boldsymbol{\theta}}(n-1) + \lambda(n-1)\boldsymbol{d}(n-1), \tag{11}$$

$$\boldsymbol{g}(n) = \nabla V(\hat{\boldsymbol{\theta}}(n)). \tag{12}$$

If $\|\boldsymbol{g}(n)\| < \varepsilon$, then go Step 6, else go Step 3

**Step 3** calculate

$$\boldsymbol{d}(n) = -\boldsymbol{g}(n) + \beta(n)\boldsymbol{d}(n-1). \tag{13}$$

Where

$$\beta(n) = \frac{\boldsymbol{d}^{\mathrm{T}}(n-1)\boldsymbol{g}(n)}{\boldsymbol{d}^{\mathrm{T}}(n-1)\boldsymbol{d}(n-1)}. \tag{14}$$

**Step 4** calculate step length

$$\lambda(n) = -\frac{\boldsymbol{g}^{\mathrm{T}}(n)\boldsymbol{d}(n)}{\boldsymbol{d}^{\mathrm{T}}(n)\boldsymbol{d}(n)}. \tag{15}$$

**Step 5** if $n < NL$, where $NL$ is the number of predefined largest seeking steps, then go Step 2; else stop seeking, and show the seeking failure information.

**Step 6** stop seeking, get the optimum value $\boldsymbol{\theta}$.

By using the above method, the minimum point of the index function can be obtained. In Sec.4, some simulation examples will be given to show the procedure and effectiveness of the method.

# 4. Numerical experiments

In this section, some simulation examples are given to show the procedure of parameter identification and information recovery.

## 4.1. Breaking chaotic shift key for low dimensional chaotic transmitter

In first example, the Lorenz system is chosen as the transmitter, which can be given as follows:

$$\begin{aligned}\dot{x}_1 &= a(x_2 - x_1),\\ \dot{x}_2 &= bx_1 - x_2 - x_1x_3,\\ \dot{x}_3 &= x_1x_2 - cx_3.\end{aligned} \tag{16}$$

Where $\boldsymbol{x} = [\, x_1 \;\; x_2 \;\; x_3 \,]^{\mathrm{T}}$ is state vector, $x_1$ is chosen as the transmitted signal to the receiver. Parameter $a$ can be chosen as chaotic key, which varies alternatively between values $a_1 = 15.7$ and $a_2 = 16$ according to the binary information to be sent. The transmitted binary information, the signal in the public channel and the synchronization error of the legal receiver are given in Figs.3(a), 3(b) and 3(c) respectively.

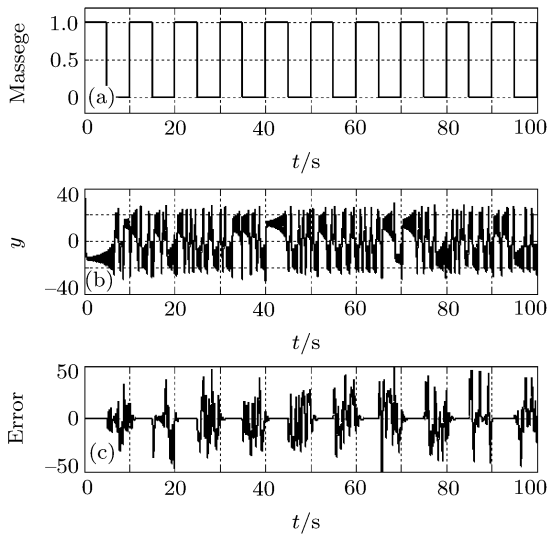



**Fig.3.** (a) The transmitted binary information, (b) transmitted signal in public channel, (c) the synchronization error for legal receiver in chaotic shift key communication.

The eavesdropper can build a system with the same structure as that of the transmitter, which is written as

$$\begin{aligned}\dot{\hat{x}}_1 &= \hat{a}(\hat{x}_2 - \hat{x}_1),\\ \dot{\hat{x}}_2 &= by - \hat{x}_2 - y\hat{x}_3,\\ \dot{\hat{x}}_3 &= y\hat{x}_2 - c\hat{x}_3.\end{aligned} \tag{17}$$

The key recovery results are given in Fig.4. The transmitter's parameter and identified parameter are shown in dashed and solid line respectively in Fig.4, from which, we know that the binary information can be recovered only from the transmitted signal. In fact, it is not necessary for the identified parameter to be identical to that of the transmitter. It is enough for the adaptive identification procedure to converge to different values with respect to different binary information, which can be discriminated by the eavesdropper. In this low dimensional transmitter example, the chaotic shift key communication is attacked successfully. In the following subsection, hyper chaotic attractor with more than one positive Lyapunov exponents will be used as transmitter to test the proposed method.

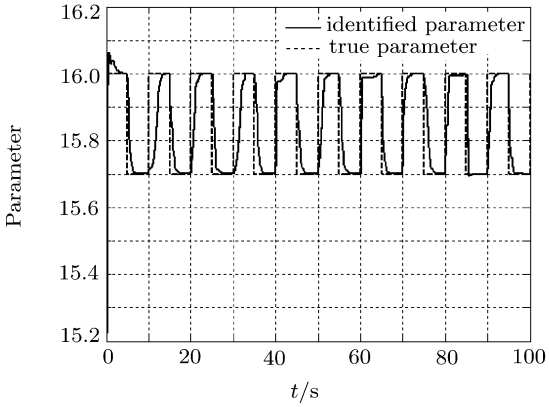



**Fig.4.** The true parameter and identified parameter in breaking chaotic shift key communication.

## 4.2. Breaking chaotic shift key for hyper chaotic transmitter

A general chaos synchronization scheme is proposed and a hyper chaos synchronization is used for secure communication,[27] the hyper chaos transmitter is given as

$$\begin{aligned}\dot{x}_1 &= 2 + x_1(x_2 - 4),\\ \dot{x}_2 &= -x_1 - x_3,\\ \dot{x}_3 &= x_2 - a_1x_3 + s_{\mathrm{aux}},\\ s_{\mathrm{aux}} &= 3x_3,\\ \dot{x}_4 &= -10x_4 + s,\\ \dot{x}_5 &= 28x_4 - x_5 - x_4x_6,\\ \dot{x}_6 &= x_4x_5 - 2.666x_6,\\ s &= 10x_5 + 90x_3/x_6.\end{aligned} \tag{18}$$

Where $a_1$ is the parameter which can be used as key in chaotic shift key communication, the scalar signal $s$ is transmitted in the public channel.

The receiver is given as

$$\begin{aligned}
\dot{y}_1 &= 2 + y_1(y_2 - 4),\\
\dot{y}_2 &= -y_1 - y_3,\\
\dot{y}_3 &= y_2 - a_1 y_3 + t,\\
t &= (s - 10y_5)y_6/30,\\
\dot{y}_4 &= -10y_4 + s,\\
\dot{y}_5 &= 28y_4 - y_5 - y_4 y_6,\\
\dot{y}_6 &= y_4 y_5 - 2.666y_6.
\end{aligned} \tag{19}$$

The synchronization error can be redesigned as $e = t - 3y_3$. The proposed method is used, identification results are shown in Fig.5, from which, we know that the proposed method can be used for parameter identification with the hyper-chaos as the transmitter.

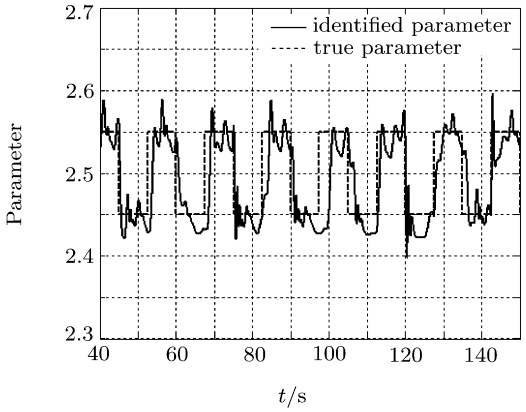



**Fig.5.** Recovering information from hyper chaotic shift key communication.

### 4.3. A case study for breaking chaotic shift key with the transmitted signal polluted by noise

In fact, the transmitted signal might be polluted by the noise from the public transmission channel. At the same time, the multiple parameters (keys) might need to be identified (this case has been beyond the assumption of the common public structure attacking). In this subsection, two parameters are identified from the transmitted signal polluted by the (white) channel noise with the amplitude 1 percent of the amplitude of the transmitted signal. The results are shown in Fig.6. Fig.6(a) is the key recovery result for $a$, Fig.6(b) is the key recovery result for $b$, and Fig.6(c) is the corresponding transmitted information. From Fig.6, we know that the proposed method can also discriminate the transmitted binary information, though the identification procedure might be effected by channel noise.

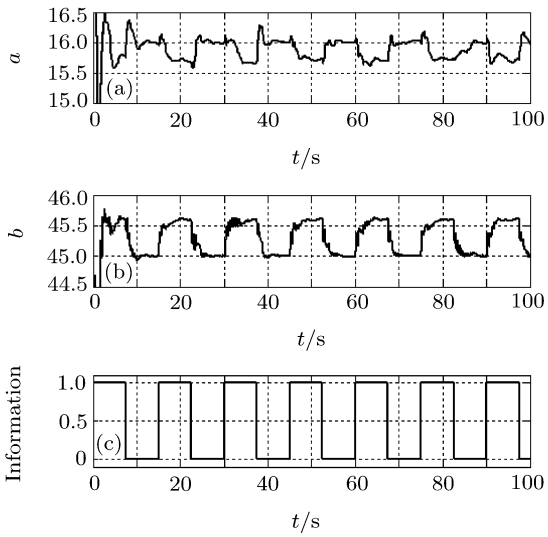



**Fig.6.** Attacking the multiple parameters from the noisy transmitted signal.

## 5. Conclusion remarks

To break the chaotic shift key communication, the key step is to find the (key) parameters used at the transmitter end from the signal transmitted in the public channel. In this paper, a parameter adaptive identification method using the predefined index function about the synchronization error is proposed to break chaotic shift key communication. The result shows the effectiveness of the method in breaking chaotic shift key communication, and hyper-chaotic attractor can not provide higher security as expected, which is identical to the former results.[21,22] Chaos synchronization and parameters identification are implemented at the same procedure. Compared with the other synchronization methods,[27−32] this method only uses scalar transmitter information in transmitted channel. The efforts in this paper will help for improving the security of existing chaotic communication method.

# References


[1] Pecora L M and Carroll T L 1990 *Phys. Rev. Lett.* **64** 821
[2] Pecora L M and Carroll T L 1991 *Phys. Rev.* A **44** 2374
[3] Abel A and Schwarz W 2002 *Proceeding of IEEE* **90** 691
[4] Cuomo K M and Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65
[5] Parlitz U, Chua L O, Kocarev L, Halle K S and Shang A 1992 *Int. J. Bifurc. Chaos* **2** 973
[6] Yang T 2004 *Int. J Computational Cognition* **2** 81
[7] Pérez G and Cerdeira H A 1995 *Phys. Rev. Lett.* **74** 1970
[8] Kocarcv L and Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028
[9] Short K M 1994 *Int. J Bifurc. Chaos* **4** 959
[10] Short K M and Parker A T 1998 *Phys. Rev.* E **58** 1159
[11] Bu S and Wang B H 2004 *Chaos, Solution and Fractal* **19** 919
[12] Chee C Y, Xu D and Bishop S R 2004 *Chaos, Solution and Fractals* **21** 1129
[13] Yang T, Wu C W and Chua L O 1997 *IEEE Trans. on CAS* I **44** 469
[14] Parker A T and Short K M 2001 *IEEE Trans. on CAS* I **48** 624
[15] Chen J Y, Wang K W, Cheng L M and Shuai J W 2003 *Chaos* **13** 508
[16] Álvarez G, Montoya F, Pastor G and Romera M 2004 *Chaos* **14** 274
[17] Minai A A and Pandian T D 1998 *Chaos* **8** 621
[18] Li S,Álvarez G, Chen G and Mou X 2005 *Chaos* **15** 137
[19] Short K M 1996 *Int. J. Bifurc. Chaos* **6** 367
[20] Yang T 1995 *Int. J. Circuits Theory and Application* **23** 611
[21] Yang T, Yang L B and Yang C M 1998 *IEEE Trans. on CAS* I **45** 1062
[22] Yang T, Yang L B and Yang C M 1998 *Phys. Lett.* A **247** 105
[23] Li J F and Li N 2002 *Chin. Phys.* **11** 1124
[24] Mu J, Tao C and Du G H 2003 *Chin. Phys.* **13** 381
[25] Wang X, Zhan M, Lai C H and G Hu 2004 *Chaos* **14** 128
[26] Chen B 1989 *Theory and Algorithm of Optimum* (Beijing: Tsinghua University Press) p334
[27] Kovarev L and Parliz U 1995 *Phys. Rev. Lett.* **74** 5028
[28] Sun M X, He X X and Yu L 2006 *Chin. Phys.* **15** 2883
[29] Yu Y and Zhang S 2004 *Chaos, Solutions and Fractals* **21** 643
[30] Wu X and Wang X 2006 *Acta Phys. Sin.* **55** 6261 (in Chinese)
[31] Hua C C and Guan X P 2004 *Chin. Phys.* **13** 1391
[32] Liu Y Z, Jiang C S, Lin C S and Jiang Y M 2007 *Chin. Phys.* **16** 660