Implementation of chaotic cryptography with chaotic synchronization

Rong He*
Department of Thermal Engineering, Tsinghua University, Beijing 100084, China

P. G. Vaidya
Department of Mechanical and Materials Engineering, Washington State University, Pullman, Washington 99164
(Received 27 August 1997)

The idea of combining synchronous chaotic systems with classic cryptography has been presented. A chaotic system sends a driving signal to two chaotic slave systems which have no influence on the generating of the driving signal. These two slave systems are synchronized and used to generate secret keys. The secret keys can be considered as pseudorandom. They are used only once and are not shorter than the message length. In this way, the idea of chaotic cryptography has been demonstrated. Its main advantages include easy implementation and good privacy. [S1063-651X(98)02402-7]

PACS number(s): 05.45.+b

I. INTRODUCTION

Finding good private communication methods has aroused the interest of many researchers. One example is quantum cryptography [1–3]. Since Pecora and Carroll demonstrated an example of synchronization in chaotic systems [4], a lot of research work on using chaotic synchronization in private communications, which mostly focused on masking information with chaotic signal, has been done [5–10]. In this paper, a concept of combining the idea of chaotic synchronization and the traditional cryptography to form a private communication system is presented.

The purpose of a cryptography system, which is often called a cryptosystem, is to transmit confidential messages secretively. Traditionally, cryptography was used mainly for military and diplomatic purposes. However, in recent years the actual and potential applications of cryptography have expanded to include many other areas such as remote log-in protocols, shared control schemes, democratic voting schemes, authenticated distributed computing, electronic money, distributed management of data bases, and so on [11,12]. Since the late 1970s several cryptography systems have been invented, such as public-key cryptography [12]. However, the public-key cryptosystems are much slower to implement for sending messages than the classical systems which were invented before the late 1970s.

In general, synchronous chaotic ordinary differential equations are easy to implement. The cryptosystems are easy to set up with chaotic systems. The chaotic signals are randomlike signals and considered as pseudorandom. The secret keys generated from these chaotic signals can be considered as pseudorandom signals. If the keys are used only once and are not shorter than the message length, this kind of cryptosystem can be reasonably considered as safe. In this paper, the idea of setting these kinds of cryptosystems has been demonstrated.

*Author to whom correspondence should be addressed. Fax number: +86-10-6277-0209.

II. BACKGROUND

The message we want to send is called the plaintext. The disguised message is called the ciphertext. The process of converting a plaintext to a ciphertext is called encryption, and the reverse process is called decryption. Usually the plaintext and ciphertext can be broken up into message units. In the simplest case a message unit is a single letter. These letters can be not only alphabet $A-Z$, but also numerals, punctuation marks, and so on. As an example, in this paper only 26-letter $A-Z$ with equivalents $0,1,\cdots,25$ are used. Let a plaintext message unit be p and ciphertext message unit be c, where p and $c \in \{0,1,\cdots,25\}$. The simplest classic method to encrypt a plaintext message unit is simply to compute $c = p+k \bmod(26)$. To decrypt a ciphertext message unit, compute $p = c-k \bmod(26)$. Here, k is an integer and called the secret ''key.'' This classic cryptosystem can be traced to Julius Caesar in ancient Rome.

The advantages of this classic cryptosystem are its fast sending of messages and its easy implementation. Its drawback is that it is not secure. However, the classic cryptosystem is also reasonably safe if the secret key is not shorter than the message and the key is used only once (single pad key). Furthermore, the key can be randomly generated. If a sender and a receiver happen to generate the same randomly generated keys at the same time, good private communication will always result. It seems that such an idea is attractive, and it is also a difficult goal to achieve. However, it can be easily achieved by unpredictable chaotic systems.

III. SIMPLE CHAOTIC CRYPTOSYSTEM

Suppose that a sender and a receiver are two users of a cryptosystem. The sender wants to send a secret message to the receiver. The easiest and simplest methods to encrypt a plaintext message unit by the sender and to decrypt a ciphertext message unit by the receiver are simply to compute $c = p+k \bmod(26)$ and compute $p = c-k \bmod(26)$, respectively. Every message unit will use one secret key k and the key k will be used only once. Usually, the message is not one letter. It may be a word, a sentence, or an article. Therefore,

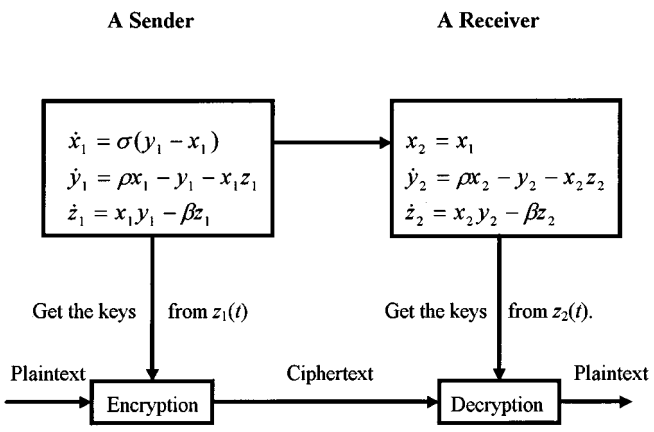

FIG. 1. An illustration of generating the keys from a master-slave type of a synchronous chaotic system.

without loss of generality, the secret keys are a series of numbers $\{k_1,k_2,\ldots,k_n\}$. If the keys are randomly generated, then the transferred message is reasonably safe. However, it is difficult for the sender and receiver to randomly generate the same keys. Now, alternatively they generate the keys from a randomlike chaotic signal. In this way, the transferred message is also quite safe. Now, it is essential for private communication to get the same keys for the sender and receiver at the same time.

One way to get the keys is to use the Pecora and Carroll type of synchronous chaotic systems, as illustrated in Fig. 1. In Fig. 1, a Lorentz system was used by the sender as a master system which sends driving signal $x_1(t)$ to the receiver. The slave system used by the receiver has the identical form as the corresponding part of the master system. After the transient, the slave system will synchronize with the master system [4], i.e., $y_2(t)=y_1(t)$ and $z_2(t)=z_1(t)$. Therefore the sender and receiver have the same randomlike signals at the same time, and they can generate the pseudorandom keys from $y_2(t)$ and $y_1(t)$ [or $z_2(t)$ and $z_1(t)$].

As an example, the sender uses the following system:

$$\dot{x}_1=\sigma(y_1-x_1),$$

$$\dot{y}_1=\rho x_1-y_1-x_1z_1,$$

$$\dot{z}_1=x_1y_1-\beta z_1. \tag{1}$$

The receiver uses the following system:

$$x_2=x_1,$$

$$\dot{y}_2=\rho x_2-y_2-x_2z_2,$$

$$\dot{z}_2=x_2y_2-\beta z_2. \tag{2}$$

They both take the parameters $\sigma=11.5$, $\rho=54.5$, and $\beta=2.8$ [Eqs. (1) and (2) are chaotic under these parameters]. They keep the structure and parameters secret. The sender solves differential equation (1) with arbitrarily chosen initial conditions, for example, $\chi_1=2.5$, $y_1=-1.8$, $z_1=0.5$ at $t=0$. The signal $x_1(t)$ is sent to the receiver. The receiver solves Eq. (2) with the driving signal $x_1(t)$. The initial conditions of Eq. (2) can be arbitrarily chosen. $z_1(t)$ and $z_2(t)$ are synchronized. They agree that, for example, they both pick the data on $z_1(t)$ and $z_2(t)$, respectively, at time $t=20.0,21.0,22.0,...$ for generating the keys. Note that the time interval between two obtained keys should be large enough to get uncorrelated keys. Again, they agree that, for example, the secret keys are taken from the values of the integer parts of $100z$, i.e., $k=\text{Integer}\,(100z)$, where z are the data from $z_1(t)$ and $z_2(t)$. The data from $z_1(t)$ picked up by the sender and the secret keys for enciphering are shown in Table I. The data from $z_2(t)$ picked up by the receiver and the secret keys for deciphering are shown in Table II.

TABLE I. Ciphertext sent by the sender.

Time t	$z_1(t)$	Keys k	Plaintext p	Ciphertext $c=p+k$ mod(26)
20.0	48.6182 . . .	4861	G (6)	31
21.0	38.3121 . . .	3831	O (14)	23
22.0	49.1034 . . .	4910	O (14)	36
23.0	47.2184 . . .	4721	D (3)	18
24.0	25.2603 . . .	2526	M (12)	16
25.0	57.7316 . . .	5773	O (14)	15
26.0	33.5745 . . .	3357	R (17)	20
27.0	66.7262 . . .	6672	N (13)	29
28.0	71.2735 . . .	7127	I (8)	11
29.0	65.4459 . . .	6544	N (13)	31
30.0	73.2694 . . .	7326	G (6)	26

Comparing Table I and Table II, it is seen that the sender and the receiver can obtain the same secret keys at the same time. These secret keys are only used once. In the next communication, the sender will change the initial conditions of Eq. (1) randomly. Since the chaotic differential equations are very sensitive to the initial conditions, the next time the sender will send the different $x_1(t)$. Thus, following the same procedure, the sender and receiver will get the same secret keys at the same time, and these keys are different from the keys they got the first time. An example of the procedure for encryption and decryption of the sender saying ''GOOD MORNING'' to the receiver is also shown in Tables I and II.

Actually, the ''real'' keys in this kind of cryptosystem are the structure of the chaotic systems and their parameters. The

TABLE II. The plaintext deciphered by the receiver.

Time t	$z_2(t)$	Keys k	Ciphertext c	Plaintext $p=c-k$ mod(26)
20.0	48.6182 . . .	4861	31	6 (G)
21.0	38.3121 . . .	3831	23	14 (O)
22.0	49.1034 . . .	4910	36	14 (O)
23.0	47.2184 . . .	4721	18	3 (D)
24.0	25.2603 . . .	2526	16	12 (M)
25.0	57.7316 . . .	5773	15	14 (O)
26.0	33.5745 . . .	3357	20	17 (R)
27.0	66.7262 . . .	6672	29	13 (N)
28.0	71.2735 . . .	7127	11	8 (I)
29.0	65.4459 . . .	6544	31	13 (N)
30.0	73.2694 . . .	7326	26	6 (G)

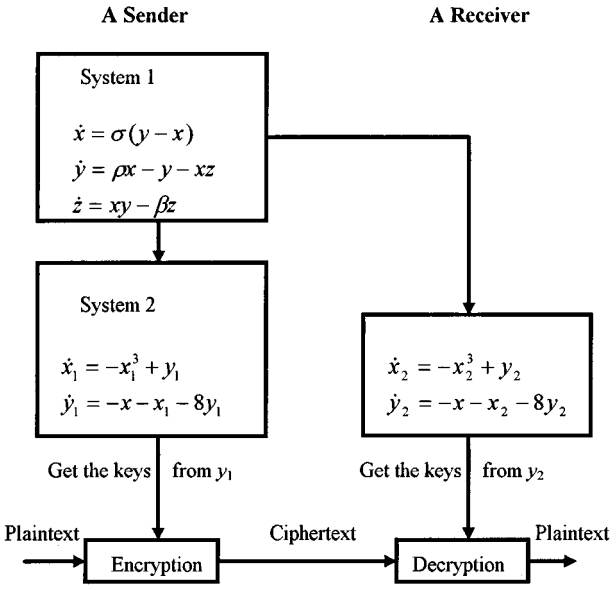

FIG. 2. An illustration of a private chaotic cryptosystem.

safety of this kind of cryptosystem depends on the complexity of the chaotic systems and the correlation between the driving signal and the synchronous signal such as $x_1(t)$ and $z_1(t)$ in Fig. 1. There are infinite chaotic differential equations and it is reasonable to assume that a very complex chaotic system can be chosen and the correlation between the driving signal and synchronous signal is small enough. Thus it is extremely difficult for an intruder to identify this chaotic system when he just detects the driving signal. However, in theory the driving signal contains all the information of the chaotic system. Therefore there always exists the possibility for the intruder to break into this kind of cryptosystem. This kind of cryptosystem is not safe enough.

IV. PRIVATE CHAOTIC CRYPTOSYSTEM

It is possible to build a good private chaotic cryptosystem. One idea is that the driving signal is independent of the subsystems which produce the secret keys. Some literature [13,14] has shown that it is possible to construct a master-slave type synchronous chaotic system in which the slave system has a different form from that of the master system. In this case, the generating of the driving signal is independent of the slave system. As an illustration, we use Fig. 2 to show the idea of ''private chaotic cryptosystem.'' The sender uses a Lorenz system as the master system:

$$\dot{x} = \sigma(y - x),$$

$$\dot{y} = \rho x - y = xz,$$

$$\dot{z} = xy - \beta z. \tag{3}$$

The driving signal is sent to the slave system:

$$\dot{x}_1 = -x_1^3 + y_1,$$

$$\dot{y}_1 = -x - x_1 - 8y_1 \tag{4}$$

and the receiver's system:

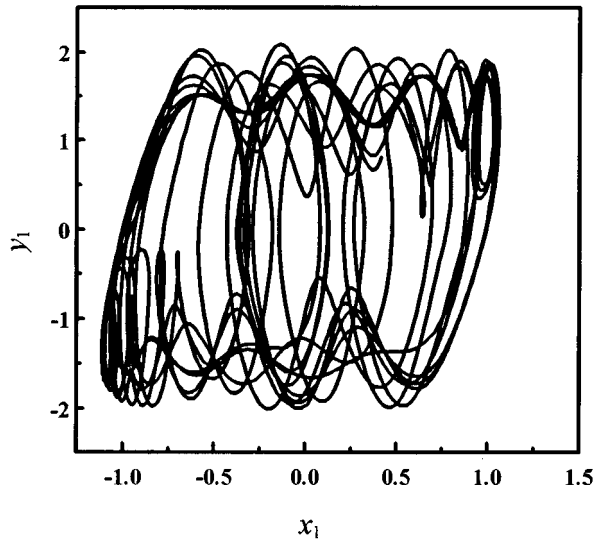

FIG. 3. System (4) is chaotic.

$$\dot{x}_2 = -x_2^3 + y_2,$$

$$\dot{y}_2 = -x - x_2 - 8y_2. \tag{5}$$

Figures 3 and 4 show that Eqs. (4) and (5) are chaotic and synchronized. The secret keys can be gotten from y_1 and y_2. The process of generating the driving signal $x(t)$ depends only on Eq. (3) and is completely independent of Eqs. (4) and (5). Even if Eq. (3) is identified by an intruder through the driving signal $x(t)$, the system (4) or (5) is still unknown and is impossible to be broken into without further information.

Equations (4) and (5) are chaotic and synchronized, as shown in Figs. 3 and 4. It can be theoretically proven that Eq. (4) synchronizes with Eq. (5). Let Eq. (4) subtract Eq. (5) and denote the difference with ''*'':

$$\dot{x}^* = \dot{x}_1 - \dot{x}_2 = -(x_1^3 - x_2^3) + y_1 - y_2 = -x^*(x_1^2 + x_1 x_2 + x_2^2) + y^*,$$

$$\dot{y}^* = \dot{y}_1 - \dot{y}_2 = -x^* - 8y^*. \tag{6}$$

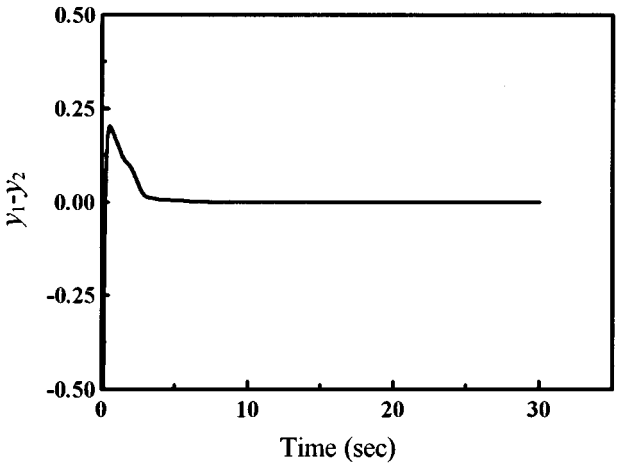

FIG. 4. The systems (4) and (5) are synchronized.

Consider the Lyapunov function

$$E = \tfrac{1}{2}\ (x^{*2} + y^{*2}). \tag{7}$$

It has

$$\dot{E} = x^*\dot{x}^* + y^*\dot{y}^* = -x^{*2}(x_1^2 + x_1x_2 + x_2^2) - 8y^{*2} \leqslant 0. \tag{8}$$

Therefore Eq. (6) is globally asymptotically stable. Thus the systems (4) and (5) are synchronized. This proving procedure is similar to that in [15].

The sender and receiver get the keys from y_1 and y_2. In order to have high safety of the communication system, the correlation between y_1 and x should be small. Figure 5 shows that the cross-correlation between x and y_1 is small. Following a procedure similar to that in the preceding section, the secret keys can be gotten from y_1 and y_2. Here, the ''advanced keys'' become the structure and parameters of Eq. (4). These ''advanced keys'' are extremely difficult to be broken with only known driving signal x. If the time interval between obtained keys from y_1 and y_2 is large enough, the ciphertext should be randomlike and give little help for breaking Eq. (4). Therefore the setup in Fig. 2 can reasonably be considered as a good private chaotic cryptosystem.

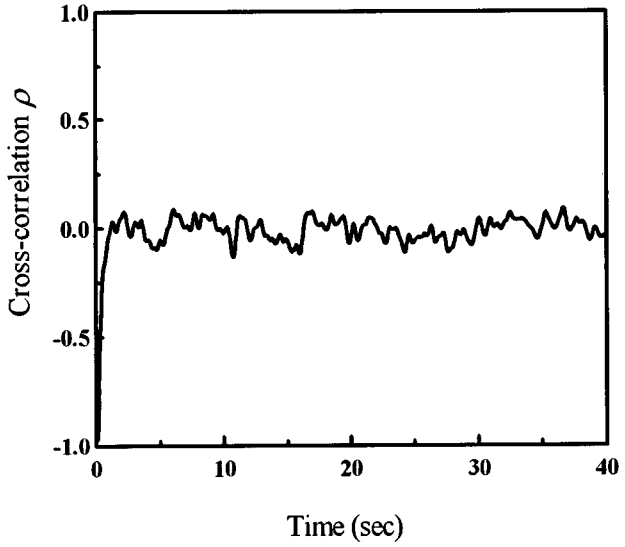

FIG. 5. The cross-correlation between x and y_1 in Eqs. (3) and (4), respectively.

V. CONCLUSION

The idea of making use of synchronous chaotic systems to set up private communication systems has been presented. A chaotic master system drives two identical slave systems which have different form from the master system. The secret keys can be obtained from these two synchronous slave systems. In principle, the keys are used only once and the message lengths do not exceed the keys. If the keys are totally random, this kind of cryptosystem is quite safe. In this paper, the keys are generated from chaotic systems and are pseudorandom. Therefore the cryptosystems are reasonably safe. The slave systems do not influence the generating of the driving signal. By synthesizing complex slave systems, the safety can be increased. Here, two signals have to be sent. One is the driving signal. Another is the ciphertext. To reduce the transmit channels, the ciphertext may be mixed with the driving signal.

[1] Faye Flam, Science **253**, 858 (1991).
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).
[4] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[5] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[6] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Trans. Circuits Syst. **40**, 626 (1993).
[7] J. H. Peng, E. J. Ding, M. Ding, and W. Yang, Phys. Rev. Lett. **76**, 904 (1996).
[8] T. L. Carroll, J. F. Heagy, and L. M. Pecora, Phys. Rev. E **54**, 4676 (1996).
[9] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E **53**, 4351 (1996).
[10] Y.-Y. Chen, Europhys. Lett. **34**, 245 (1996).
[11] Neal Koblitz, *A Course in Number Theory and Cryptography* (Springer-Verlag, New York, 1987).
[12] *Public-Key Cryptography: State of the Art and Future Directions*, edited by Th. Beth, M. Frisch, and G. J. Simmons (Springer-Verlag, New York, 1992).
[13] N. F. Rulkov *et al.* Phys. Rev. E **51**, 980 (1995).
[14] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **76**, 1816 (1996).
[15] Rong He and P. G. Vaidya, Phys. Rev. A **46**, 7387 (1992).