PHYSICAL REVIEW E **66**, 065202(R) (2002)

Chaos-based secure communications in a large community

Shihong Wang,[1,2] Jinyu Kuang,[3] Jinghua Li,[3] Yunlun Luo,[3] Huaping Lu,[1] and Gang Hu[4,1,*]
[1]*Department of Physics, Beijing Normal University, Beijing 100875, China*
[2]*Science School, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3]*Department of Electronics, Beijing Normal University, Beijing 100875, China*
[4]*China Center for Advanced Science and Technology (CCAST) (World Laboratory), P.O. Box 8730, Beijing 100080, China*
(Received 16 August 2002; published 11 December 2002)

One-way coupled map lattices are used for cryptography in secure communication, based on spatiotemporal chaos synchronization. The sensitivity of synchronization between the encryption and decryption systems can be adjusted by varying the system size. With a suitable parameter combination, the cryptosystem can reach optimal trade-off of security and performance, i.e., it shows high security (resistant against the public-structure and known-plaintext attacks) together with fast encryption (and decryption) speed. An experiment of duplex voice transmission through university network is realized, which confirms the above advantages of our approach.

DOI: 10.1103/PhysRevE.66.065202 PACS number(s): 05.45.Vx

In the last decade, secure communication by applying chaos synchronization has attracted a great deal of attention in both the nonlinear science and the engineering society [1–9]. A considerable advance of chaos communication from the conventional secure communication is expected due to the chaoticity of trajectories. So far, a large variety of models have been proposed for realizing chaos communication [2–9]. However, recent studies show even with chaotic dynamics completely hidden, most of models of chaos communications are insecure [10–18]. For communications among many commercial users, where the structure of chaotic dynamics should be open to the public and only few parameter values can be hidden as a secret key, the security of the known chaos communication methods is even lower. In this paper we find that the insecurity problem of chaos communication results mainly from the insensitivity of synchronization of the nonchaotic receiver to the system parameters, and this problem can be solved by using one-way coupled spatiotemporal chaos in which the sensitivity of chaos synchronization increases exponentially with increasing system size. With this idea, we propose a chaos communication method that has high security together with fast computation speed and short synchronization transient, and is capable of supporting mutual communications in a large community. Using this method, an experiment of duplex voice transmissions through university network is realized, which confirms the above advantages of our approach.

Let us design chaos communications among a large community with M ($M \gg 1$) individuals, each communicates with G ($M-1 \gg G \gg 1$) others. The message transmitted between any pair of individuals should be kept secret from any third party. Each person in the community has a communicator, including chaotic encryption of transmitter,

$$d\mathbf{x}/dt = \mathbf{f}[\mathbf{x}, I(t), S(t), \mathbf{a}], \quad S(t) = h[\mathbf{x}(t), I(t)], \quad \text{(1a)}$$

synchronization decryption of receiver,

$$d\mathbf{y}/dt = \mathbf{f}[\mathbf{y}, I'(t), S(t), \mathbf{b}], \quad I'(t) = h^{-1}[\mathbf{y}(t), S(t)], \quad \text{(1b)}$$

where $\mathbf{x}=(x_1, x_2, \ldots, x_N)$ and $\mathbf{y}=(y_1, y_2, \ldots, y_N)$ are N-dimensional (ND) vectors, and $\mathbf{f}=(f_1, f_2, \ldots, f_N)$ is a ND vector field. $I(t)$, $S(t)$, and $I'(t)$ are scalar functions. $I(t)$ is the plaintext assumed to be private, and $S(t)$, the ciphertext, plays double roles of the message carrier and the driving signal of the receiver for chaos synchronization. Here, $\mathbf{a}=(a_1, a_2, \ldots, a_m)$ and $\mathbf{b}=(b_1, b_2, \ldots, b_m)$ are adjustable control parameters, serving as the secret keys for chaos communication unknown to any third party; h is an invertible function and h^{-1} is its reverse.

For secure communication the transmitter generates its ciphertext $S(t)$ with certain plaintext $I(t)$ by applying an appointed key $\mathbf{a}$, and transmits it in the open channel to the receiver, which can thus run Eq. (1b) with known $S(t)$, $I'(t)=h^{-1}[\mathbf{y}(t), S(t)]$ and the same key $\mathbf{b}=\mathbf{a}$. Due to chaos synchronization, we have

$$\mathbf{y}(t) = \mathbf{x}(t), \quad \text{and then } I'(t) = I(t). \quad \text{(2)}$$

The message transmitted from the transmitter is thus successfully received by the receiver.

Now let us analyze how intruders work in illegally extracting the plaintext $I(t)$ with a certain available information. Any intruder knows the dynamics $\mathbf{f}$ and the decryption function h^{-1}, because all the community members have the same type of communicators, Eqs. (1). Also, the intruder has full data of ciphertext $S(t)$ because $S(t)$ is transmitted in the open channel. By some possible chances, the intruder may know certain part of past plaintext $I(t)$ and the corresponding keystream $\mathbf{x}(t)$. The maximum intention of an attack is to determine the secret key $\mathbf{a}$ from the available knowledge of ciphertexts, some plaintexts, and the dynamics [Eq. (1b)]. Thus, we are dealing with public-structure and known-plaintext attacks on self-synchronizing chaotic cryptosystems [18]. There are a number of well-known attacks evaluating public-structure and known-plaintext cryptosystems [14,17,18], among which we consider the method of error function attack (EFA). By means of EFA, the intruder, knowing a segment of past plaintext $I(t)$, $t_1 < t < t_2$, $T = t_2 - t_1$, can run Eq. (1b) with an arbitrary test key $\mathbf{b}$, and compute the following error function $e(\mathbf{b})$:

*Corresponding author. Email address: hugang@sun.ihep.ac.cn

$$e(\mathbf{b})=\frac{1}{T}\int_{t_1}^{t_2}|h^{-1}(\mathbf{y}(t),S(t))-I(t)|dt. \tag{3}$$

By varying $\mathbf{b}$ and minimizing $e(\mathbf{b})$, the intruder may find the location of $e(\mathbf{b})\approx 0$, which fixes the position of the test key $\mathbf{b}\approx\mathbf{a}$. With the correct $\mathbf{a}$ in hand, the intruder can unmask any transmitted future message $I(t)$.

EFA is very effective in analyzing chaos-based self-synchronizing cryptosystems, because this analysis attacks the weakest point in chaos communication—the receiver system. The essential reason for this weakness is that *the receiver is nonchaotic*. Driven by the transmitted signal, the state of the nonchaotic receiver is independent of the initial condition, and is usually insensitive to the system parameters, including the secret key. With this insensitivity, the error function varies slowly with the test parameters $\mathbf{b}$, this slow variation of desynchronization offers a large $e(\mathbf{b})$ basin around the key position $\mathbf{b}=\mathbf{a}$, allows the intruder to minimize $e(\mathbf{b})$ function by adaptive adjustments, and exposes the key without difficulty. We have tested many known chaos communication systems [2–15], and found that all these systems are insecure against EFA of Eq. (3).

With the above understanding, it is clear that the crucial point for realizing secure chaotic encryption is to find chaos-based cryptosystems whose nonchaotic receivers have sufficiently high sensitivity to certain system parameters (which can serve as the secret key). Usually, increasing sensitivity may lead to the increase of synchronization time and the decrease of computation speed, and these pitfalls are undesirable for practical applications. We need some chaotic cryptosystems reaching the optimal trade-off between security and performance, i.e., having simultaneously high practical security, fast encryption speed, and short synchronization transient time.

We use the following one-way coupled map lattices (OCML) as our cryptosystem.

Encryption transformation:

$$x_{n+1}(j)=(1-a_j)f[x_n(j)]+a_j f[x_n(j-1)],\quad j=1,\ldots,m,$$

$$x_{n+1}(j)=(1-\varepsilon_j)f[x_n(j)]+\varepsilon_j f[x_n(j-1)],$$

$$j=m+1,\ldots,N,$$

$$f(x)=4x(1-x),\quad x_n(0)=S_n/2^{\nu}, \tag{4a}$$

$$S_n=(K_n+I_n)\mod 2^{\nu},$$

$$K_n=[\mathrm{int}(x_n(N)\times 2^{\mu})]\mod 2^{\nu}. \tag{4b}$$

Decryption transformation:

$$y_{n+1}(j)=(1-b_j)f[y_n(j)]+b_j f[y_n(j-1)],\quad j=1,\ldots,m,$$

$$y_{n+1}(j)=(1-\varepsilon_j)f[y_n(j)]+\varepsilon_j f[y_n(j-1)],$$

$$j=m+1,\ldots,N,$$

$$y_n(0)=x_n(0). \tag{4c}$$

Equation (4b) specifies the transformation function $h[x_n(N),I_n]$ where int means to take the integer value while mod represents to keep the residual number of 2^{ν} only. The plaintext can be extracted by the receiver as

$$K_n'=[\mathrm{int}(y_n(N)\times 2^{\mu})]\mod 2^{\nu},$$

$$I_n'=(S_n-K_n')\mod 2^{\nu}. \tag{4d}$$

By setting $b_j=a_j$, $j=1,\ldots,m$, the nonchaotic receiver can realize synchronization to the chaotic transmitter and correctly extract the message as

$$y_n(N)=x_n(N),\quad K_n'=K_n,\quad I_n'=I_n. \tag{5}$$

The two operations int and mod in Eq. (4b) make the truncations of $x_n(N)$ for the small and large parts, respectively. The former operation is useful for keeping robustness of communication against noise in the transmission channel due to its integer-valued transmitted signal (a desirable advantage of conventional cryptography), while the latter can greatly enhance the sensitivity of chaos synchronization to the parameter mismatch.

Now let us evaluate the security of Eq. (4) against EFA. Note that the form of Eqs. (4) [including ε_j, $j=m+1,\ldots,N$, and the decryption function (4d)] are known for the intruder. In Figs. 1(a)–(e) we use a single parameter (a_1, $m=1$) as the key, and take $\mu=50$, $\nu=32$, $\varepsilon_j=a_1=0.95$, and compute the error function $e(b_1)$ vs b_1 for different size N's,

$$e(b_1)=\frac{1}{T}\sum_{n=1}^{T}|i_n'-i_n|,\quad i_n=I_n/2^{32},\quad i_n'=I_n'/2^{32}, \tag{6}$$

where I_n' can be computed by the intruder from Eqs. (4c) and (4d) with the accessible S_n and the test key b_1. Each $e(b_1)$ function in Figs. 1(a)–1(d) has a basin structure, and all basins are small, i.e., synchronization of chaos in Eqs. (4) is rather sensitive to the parameter changes. Moreover, the sensitivity increases as the system size N increases. System (4c) has a feature of convective instability, and any perturbation in the head of the lattice chain can be amplified down chain, thus for larger N we have higher sensitivity of keystream K_n to b_1. We define W_N as the width of $e(b_1)$ basin of OCML with length N (see Fig. 1), and plot W_N vs N in Fig. 1(e). The straight line shows a satisfactory exponential dependence

$$W_N=\beta e^{-\alpha N},\quad \beta\approx 2.6\times 10^{-4},\quad \alpha\approx 0.51. \tag{7}$$

With Eq. (7) the length of the spatiotemporal system plays the role of the control parameter of the sensitivity for synchronization to the key. And by choosing suitable N, we can adjust the sensitivity to a sufficiently high level. The security of the above spatiotemporal chaos communication can be further enhanced by increasing m. In Fig. 1(f), we take $m=2$ and plot $e(b_1,b_2)$ in $b_1\sim b_2$ plane for $N=25$. The 2D key basin takes an extremely small part in the key-parameter space.

In Fig. 1, $e(b_1)$ curves are completely flat with uniformly distributed fluctuation outside of the basins [see Fig. 1(d)]. In the flat regime one cannot apply adaptive adjustments to approach the key basin by optimally minimizing $e(b_1)$. The statistical reasons for the behavior of $e(b_1)$ curves may be, on one hand, the transmitted signal S_n has very good random

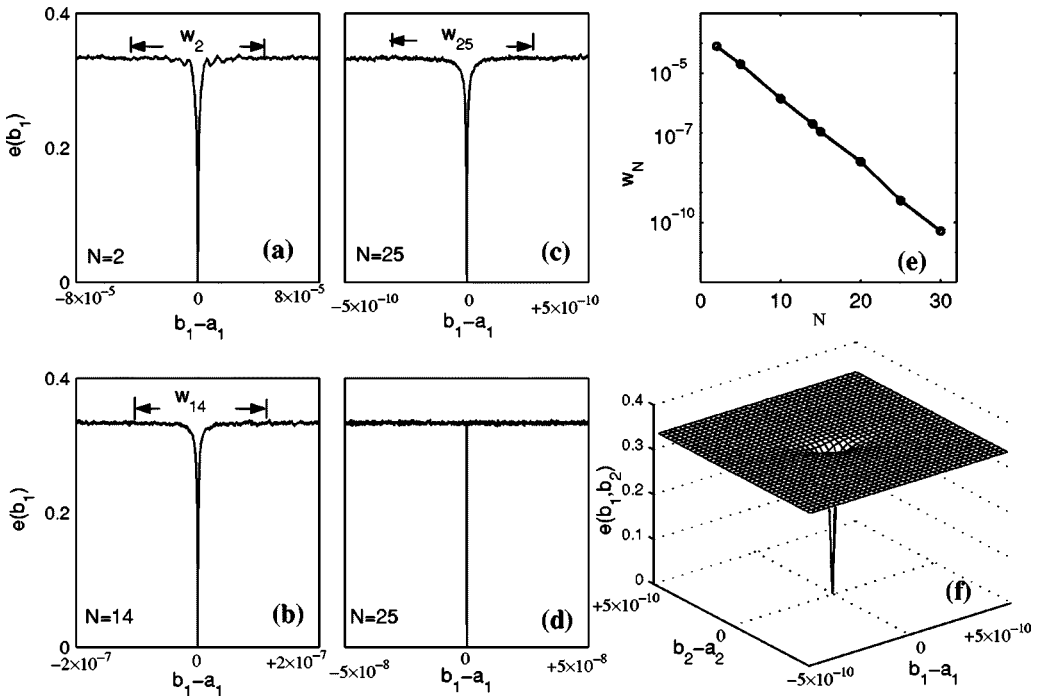

FIG. 1. (a)–(d) The error function $e(b_1)$, defined in Eq. (6). A segment of known plaintexts; I_n with $T=20\,000$ is available; $a_1=0.95$, $\varepsilon_j=0.95$, $j=2,\ldots,N$. (a) $N=2$, (b) $N=14$, (c),(d) $N=25$; W_N is the width of $e(b_1)$ basin of the system with size N, away from which the $e(b_1)$ function is completely flat [see (d)] and denies adaptive minimization adjustments for searching $b_1=a_1$. (e) W_N vs N. A satisfactory exponential decay relation, Eq. (7), is shown. (f) The same as (c) with 2D key parameters b_1,b_2, $a_1=a_2=0.95$; the $e(b_1,b_2)$ basin is so small that the key is well hidden in the key space $b_1,b_2\in(0.5,1)$.

property, and on the other hand, any two S_n sequences generated by different b_1 parameters, of which the difference is larger than the basin width, are completely uncorrelated. This intuitive understanding can be well confirmed by the following evidence. The average value and the variance of the difference function of two completely uncorrelated and purely random sequences uniformly distributed in the region [0, 1] can be exactly computed as $\langle e\rangle\equiv\frac{1}{3}$, and $\sigma=\langle[e-\langle e\rangle]^2\rangle \equiv(1/18\sqrt{T})$. By careful checking, we found that our numerical results of $\langle e(b_1)\rangle$ and $\sigma(b_1)$ are indistinguishable from these theoretical predictions if b_1 is away from the basin. Therefore, the best way for breaking the system security is to use brute force analysis for finding $e(\mathbf{b})$ basin and then to use adaptive adjustments to reach the key $\mathbf{b}=\mathbf{a}$ in the basin. Since the number of the tests for the latter is incomparably smaller than that of the former, the resistance of the system against EFA is mainly determined by the cost of finding $e(\mathbf{b})$ basin. For $m=1$, the probability to find the secret key by an arbitrary test is proportional to the key basin width as $P_1 \approx W_N/L$, with L being the range of a_1 available for chaos synchronization ($L\approx 0.5$ in our case).

To evaluate the practical security of our approach, we have investigated in detail the statistical properties of the ciphertexts S_n [19,20], and studied the resistance of the system against various standard known attacks in both conventional and chaos-based cryptographies [10–18]. We find that all other attacks tested are incomparably less effective than EFA. The detailed analysis in this regard will be given in our forthcoming paper.

From the above discussion, the practical security of the cryptography and the size of keyspace are essentially determined by EFA, and can be calculated explicitly. If we take m parameters $(a_1,\ldots,a_m)$ as our secret key, then the volume of a key basin in the mD parameter space is computed from Eq. (7) as

$$V_m=\beta^m e^{-\alpha m(N-[m-1/2])}. \tag{8}$$

The total volume of the parameter space is L^m, thus the number of keyspace reads

$$J_m=L^m/V_m=[(L/\beta)\,e^{\alpha(N-[m-1/2])}]^m. \tag{9}$$

With an arbitrary test, the intruder has probability $P_m=1/J_m$ to find the secret key.

Let us come back to the task raised at the beginning of this paper. Suppose we have a billion ($M=10^9$) individuals in the community, each has links $G=10^3$. We take system (4) with $N=25$, $\mu=50$, $\nu=32$, and $m=4$, which can be easily handed in practice. We now need 10^{12} keys, while the available number of keyspace is about $V_4\approx 10^{35}$. The distribution density of keys is as rare as to distribute, on average, a single 0.01-mm^2 hole over the whole earth's surface. If an intruder wants to find a given key basin, he needs to make 10^{35} tests approximately. With $T=100$ known plaintexts and with our CPU of 750-MHz PC, we need about 70 s for 10^6 tests. Thus, the intruder should use the best computer in the world (which should be around 10^7 times faster than our PC) to compute 10^{16} years, which is much longer than the age of our universe (10^{10} years). Thus, the illegal unmasking of

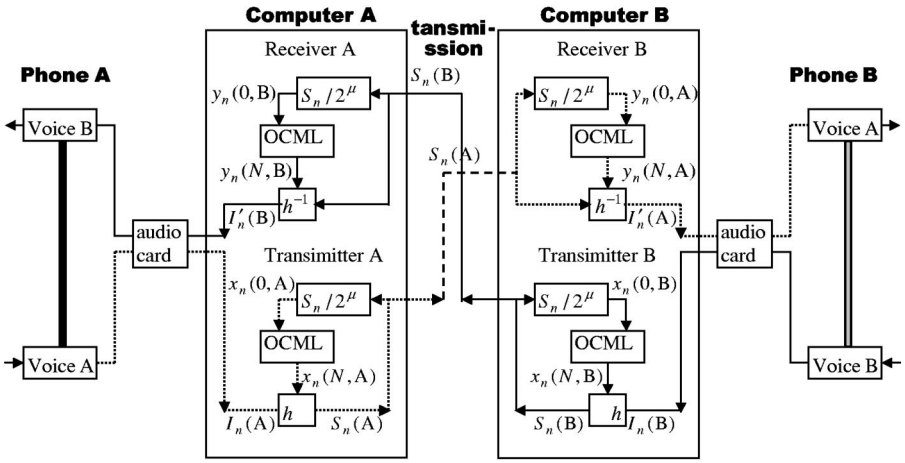

FIG. 2. Schematic figure of the experimental set of duplex voice transmissions through the university local network by applying system (4).

system (4) is practically impossible for EFA and for other currently known attacks (for caution's sake, the possibility of some unknown attack methods which may break our cryptosystem in a more effective manner is still not excluded).

Though in Fig. 1(d) the synchronization is highly sensitive to the parameter mismatch, the transient time for synchronization of the receiver is rather short. The computing time for chaos synchronization of our system is much shorter than that for synchronizing two single Lorenz equations. The reasons for simultaneously achieving both sensitivity and quick synchronization are: while our receiver system has exponentially increasing sensitivity in space [Eq. (7)], its largest Lyapunov exponent λ_1 is negative with large absolute value ($\lambda_1 \approx -2.39$), i.e., any desynchronous elements can die away very rapidly in time. Another favorable and important advantage of our system is that its encryption speed is fast. The fast speed is due to the single-round 32-bit encryption structure and the simple dynamical form of Eqs. (4). With our 750-MHz CPU computer, we can produce 45M-bit ciphers per second, which is of the same speed order as the Advanced Encryption Standard (AES) [21], which has 96-Mbit, 80-Mbit, and 67-Mbit ciphers per second for 128-bit, 192-bit, and 256-bit key sizes (for a 600-MHz-CPU PC), respectively. In comparison with other known stream cipher systems, including both conventional and chaos-based cryptosystems, our system has obvious advantages of high practical security, together with fast encryption.

For confirming all the above advantages of security, capacity, convenience, and reliability, we have tried a duplex voice transmission experiment by taking system (4) with $N=25$, $\mu=50$, $\nu=32$, and by using local network in university campus. The schematic figure of the experiment is given in Fig. 2. A dialogue can be performed between phones *A* and *B* with standard speed and standard quality, and with definite certainty for arbitrarily long time if both computers use the same appointed keys. Communications can be implemented robustly in the local network environment and communication instruments, where inevitable pertubations (though, very weak) may exist. But if any side switches his first coupling a_1 (or b_1) to a mismatch of 1.0×10^{-11}, the transmitted signal becomes nothing but pure noise.

In conclusion, we have suggested and experimentally realized (by software implementation) a secure communication approach by using spatiotemporal chaos. The approach can be directly applied in voice and document transmissions in internet. There is no essential difficulty for hardware implementation, and this is the further work of our research. With this work we hope to simulate new investigations towards promoting chaos communication into practical public service.

[1] L.M. Pecora and T.L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).
[2] L.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
[3] L. Kocarev *et al.*, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 709 (1992).
[4] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).
[5] J.H. Xiao *et al.*, Phys. Rev. Lett. **77**, 4162 (1996).
[6] G. Hu *et al.*, Phys. Rev. E **56**, 2738 (1997).
[7] D.G. Van Wiggeren and R. Roy, Science **279**, 1198 (1998).
[8] S. Sundar and A.A. Minai, Phys. Rev. Lett. **85**, 5456 (2000).
[9] J. Garcia-Ojalvo and R. Roy, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 1491 (2001).
[10] K.M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **4**, 959 (1994).
[11] G. Perez and H. Cerdeira, Phys. Rev. Lett. **74**, 1970 (1995).
[12] K.M. Short, Int. J. Bifurcation Chaos Appl. Sci. Eng. **6**, 367 (1996).
[13] K.M. Short and A.T. Parker, Phys. Rev. E **58**, 1159 (1998).
[14] Ch.S. Zhou and C.H. Lai, Phys. Rev. E **60**, 320 (1999).
[15] Ch.-S. Zhou and C.-H. Lai, Phys. Rev. E **59**, 6629 (1999).
[16] A.T. Parker and K.M. Short, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 624 (2001).
[17] L. Kocarev, IEEE Circuits Syst Magz. **1**, 6 (2001).
[18] F. Dachselt and W. Schwarz, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **48**, 1498 (2001).
[19] C.E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[20] C.E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[21] See J. Nechvatal *et al.*, http://csrc.nist.gov/encryption/aes