Using Distributed Nonlinear Dynamics for Public Key Encryption

Roy Tenny,[1,2] Lev S. Tsimring,[1] Larry Larson,[2] and Henry D. I. Abarbanel[1,3]

[1]*Institute for Nonlinear Science, University of California, San Diego, La Jolla, California 92093-0402*

[2]*Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, California 92093-0354*

[3]*Department of Physics and Marine Physical Laboratory (Scripps Institution of Oceanography), University of California, San Diego, La Jolla, California 92093-0402*

(Received 15 May 2002; published 28 January 2003)

We introduce a new method for asymmetric (public key/private key) encryption exploiting properties of nonlinear dynamical systems. A high-dimensional dissipative nonlinear dynamical system is distributed between transmitter and receiver, so we call the method distributed dynamics encryption (DDE). The transmitter dynamics is public, and the receiver dynamics is hidden. A message is encoded by modulation of parameters of the transmitter, and this results in a shift of the overall system attractor. An unauthorized receiver does not know the hidden dynamics in the receiver and cannot decode the message. We present an example of DDE using a coupled map lattice.

DOI: 10.1103/PhysRevLett.90.047903 PACS numbers: 05.45.Vx, 05.45.Gg, 05.45.Ra

During the last decade there has been a great interest in developing secure communication schemes utilizing chaos. Most of the proposed schemes are based on chaos synchronization [1], controlling chaos [2], and chaotic shift keying [3]. Also, chaos based block ciphers were studied in [4]. In conventional cryptography, all encryption schemes are divided into *symmetric* and *asymmetric* methods [5]. Symmetric methods require sharing of the same key by both transmitter for message encryption and receiver for message decryption. Asymmetric methods have one "public" key known to all users for encoding messages, but another "private" key for use by trusted receivers for decoding the message. Decoding the message using the public key which was used to encrypt the message is made computationally unfeasible. Communications strategies that use asymmetric (or *public key*) methods for encryption have much greater inherent security than symmetric methods since they eliminate the problem of key management, which itself can pose the most serious security risk. However, in the application of ideas from nonlinear dynamics to secure communications, only the equivalent of symmetric encryption methods have been studied to date. It is of general interest then to introduce asymmetric, public/private key techniques into the discussion of communication using nonlinear systems. All known asymmetric schemes are based on the algorithmic complexity of certain inverse integer number problems (factorization, knapsack, discrete logarithms, etc.) [5]. They cannot be utilized directly in nonlinear dynamically based encryption schemes which use real numbers and are implemented using analog components. We propose the first method which uses a different concept based on nonlinear dynamics for realizing asymmetric "public key" secure communication. A general strategy is introduced and then explored in detail within a relatively simple example. The generality of the approach permits one to envision substantially more complex implementations wherein the inherent security can be strengthened as one wishes.

The basic idea of distributed dynamics encryption (DDE) is to split a dynamical system of dimension $D_T + D_R$ into two parts with D_T *transmitter* variables $\mathbf{t}(n) = [t_1(n), \ldots, t_{D_T}(n)]$, and D_R *receiver* variables $\mathbf{r}(n) = [r_1(n), \ldots, r_{D_R}(n)]$. The receiver receives the scalar signal $s_t(n)$ from the transmitter, and the transmitter receives the scalar signal $s_r(n)$ from the receiver. At each discrete time $n = 1, 2, \ldots$, these satisfy

$$\begin{aligned} \mathbf{t}(n+1) &= \mathbf{F}_T(\mathbf{t}(n), s_r(n), m(n)), \\ \mathbf{r}(n+1) &= \mathbf{F}_R(\mathbf{r}(n), s_t(n)), \end{aligned} \tag{1}$$

where $s_t(n) = G_T(\mathbf{t}(n))$ and $s_r(n) = G_R(\mathbf{r}(n))$ are signals transmitted from the transmitter to the receiver and back, respectively. Here $\mathbf{F}_T(\bullet)$ is a D_T dimensional vector field, $\mathbf{F}_R(\bullet)$ is D_R dimensional, $G_R(\bullet)$ and $G_T(\bullet)$ are scalars, and $m(n)$ is the message. Of these quantities $\mathbf{F}_T(\bullet)$ and $G_T(\bullet)$ are public, while $m(n)$, $\mathbf{F}_R(\bullet)$, and $G_R(\bullet)$ are private. Both transmitted signals, s_r and s_t, are public.

An authorized receiver knows all quantities, public and private, and can establish off-line the allowed attractors, or other dynamical aspects of the total system, for all allowed values of $m(n)$. In the present illustration of DDE, we permit only $m(n) = 0$, leading to what we call the "0-attractor" and $m(n) = 1$ yielding the "1-attractor." In windows of time of length L we fix $m(n) = 0$ or $m(n) = 1$. The receiver must decide which of these attractors is present in the total system, and on that basis select whether a "0" or a "1" was transmitted. Other modulation methods are possible with $m(n)$ being a richer waveform, but this simple binary scheme serves to illustrate the method.

In any window of length L containing $m(n) = 0$ or $m(n) = 1$ we iterate the dynamical system L times and on

the basis of the last $L' \leq L$ iterations decide whether it is nearer the 0-attractor or the 1-attractor.

Since $\mathbf{F}_R(\bullet)$, $G_R(\bullet)$, and, of course, $m(n)$ are private, the state of the transmitter system $\mathbf{t}(n)$ is not known to an unauthorized receiver, and the job of the code breaker is to estimate those quantities. The goal of the transmitter is to assure that the computational effort in making such an estimation is extremely difficult. As in all public key encryption schemes, the advantage of the authorized receiver over an unauthorized receiver is computational, not information theoretic.

The essential idea is that the receiver has full knowledge of the dynamics and therefore knows the state space locations of the attractors corresponding to the binary values of the modulation variable $m(n)$. Unauthorized recipients know only the transmitter part of the full dynamics, and the protocol of communication is chosen in such a way that the attractor cannot be reconstructed based on the transmitted signals alone. The attractor can take the form of a limit cycle, a high-dimensional hypersurface, or a chaotic attractor. The nonlinear dynamical system is continuous in the state space and can be either continuous or discrete in time. The public key encryption scheme discussed here is discrete in time and the coupling signals are scalars; however, the concept can be extended to continuous time dynamical systems and systems with multidimensional coupling signals.

Neither an unauthorized nor an authorized receiver knows the complete transmitter state $\mathbf{t}(n)$, so each must replace the "missing" state variables by the time-delay embedding method [6] using the incoming signal from the transmitter s_t. This is embodied in the vector $\mathbf{s}(n) = (s_t(n), ..., s_t[n - (d - 1)])$ with d chosen by various known methods [6] in order to detect the attractor in the reconstructed full phase space $(\mathbf{r}(n), \mathbf{s}(n))$. At the beginning of each transmitted bit, $m(n) = 0$ or $m(n) = 1$, the state of the transmitter is set to a random value, making the reconstruction of $\mathbf{t}(n)$ by an unauthorized receiver more difficult. The combined dynamical system is iterated long enough to ensure that the system moves from the random initial state to one of the two attractors that correspond to the transmission of 0 or 1 as illustrated in Fig. 1. The transmitted bit is decoded by the receiver by choosing the attractor that is closer to the end points of the trajectory. The authorized receiver reconstructs the position of the attractor using the sequence $\mathbf{s}_t$ obtained by simulating off-line the entire dynamical system (transmitter + receiver) before the actual transmission begins. The same simulation is repeated twice: once for $m = 0$ and then for $m = 1$. Each will produce a collection of points that represent each of the two attractors separately. On the other hand, the sequence s_t generated during the real transmission and available to an unauthorized receiver is of a single transient trajectory for only one of the two possible values of m. The transmission is stopped when the trajectory converges to the corresponding attractor. The authorized receiver has the off-line simulations with both values of m which cover the entire attractors, so it can tell to which of the two attractors the currently transmitted sequence has converged. But an unauthorized receiver knows only that the end point of the transmitted sequence lies on one of the two possible attractors, but it cannot tell on which one.

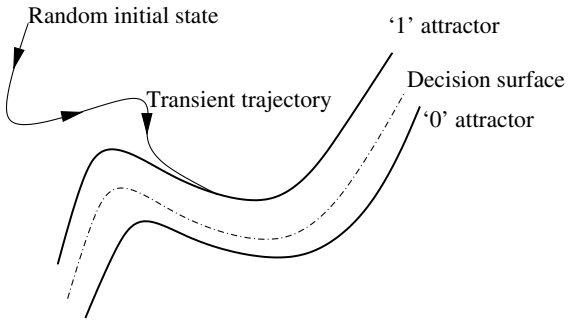

FIG. 1. A trajectory in the reconstructed embedding phase space starts at a random initial state and converges to one of two attractors that correspond to a transmitted "0" or "1." The trajectory shown here goes to the "1-attractor."

We illustrate DDE using the dynamics of a coupled map lattice. The receiver dynamics $\mathbf{F}_R(\bullet)$, $G_R(\bullet)$ is given by the map $(i = 1, \ldots, D_R)$

$$r_i(n+1) = a_{i,i-1} r_{i-1}^2(n) + a_{i,i} r_i^2(n) + a_{i,i+1} r_{i+1}^2(n) + b_i s_t^2(n) + c_i, \tag{2}$$

and the transmitter dynamics $\mathbf{F}_T(\mathbf{t}(n), s_t, m)$ by $(j = 1, \ldots, D_T)$

$$t_j(n+1) = d_{j,j-1} t_{j-1}^2(n) + d_{j,j} t_j^2(n) + d_{j,j+1} t_{j+1}^2(n) + e_{j,j} |t_j(n)| + f_j s_r^2(n) + g_j. \tag{3}$$

The signal sent from the receiver to the transmitter is

$$s_r(n) = \sum_{i=1}^{D_R} h_i r_i^2(n); \tag{4}$$

the signal sent from the transmitter to the receiver is

$$s_t(n) = w \sum_{j=1}^{D_T} |t_j(n)| + Am(n). \tag{5}$$

We selected $D_T = 12$, $D_R = 2$ and chose parameters such that the attractors are chaotic for both $m = 0, 1$. During each transmission window we allowed the system to converge to its attractor (Fig. 2) for $L = 50$ iterations. The bit was decoded (either a 1 or a 0 was selected) using the last $L' = 10$ points on the trajectory (Fig. 1). All the parameters and other details of our simulation may be found in [7].

The decoding bit error rate (BER) encountered by the authorized receiver, depends on the modulation parameter A determining the separation between the 0 and

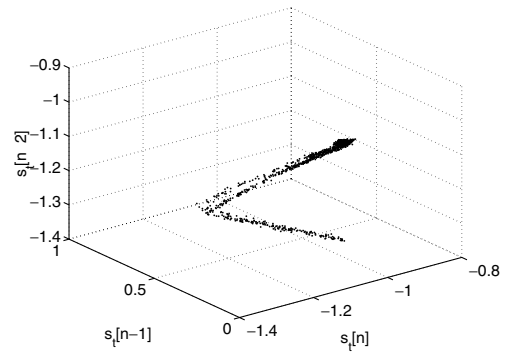

FIG. 2. An enlargement of a part of the 0-attractor in the reconstructed phase space, $(s_t(n), s_t(n-1), s_t(n-2))$.

the 1 attractors. In Fig. 3 we show the sensitivity of the BER on A.

Cryptanalysis.—An unauthorized receiver may attempt various methods to attack DDE and decode the secret message $m(n)$. One such method is to reconstruct the positions of the attractors that correspond to transmission of 0 and 1 by storing and clustering samples of many transmitted bits. Knowing the positions of the attractors would enable the unauthorized receiver to decode the message using the same method as the authorized receiver. We protect against such an attack by altering the dynamics of the receiver $\mathbf{F}_R(\bullet), G_R(\bullet)$ at the beginning of each transmitted bit, which results in a change in the attractors positions. Since the attractor's location is different for each bit, it cannot be reconstructed using samples of many transmitted bits. Reconstruction of the receiver secret dynamics, $\mathbf{F}_R(), G_R()$ can be avoided by altering the receiver dynamics and choosing large receiver dimension D_R. An unauthorized receiver cannot decode the message m by monitoring the public signals $s_r(n), s_t(n)$ and by generating the transmitter output signal $\mathbf{s}_t$ using public $\mathbf{F}_T(), G_T()$ and $\mathbf{s}_r$ since the initial state $\mathbf{t}(0)$ needs to be accurately known for that. Therefore the unauthorized receiver would need to solve for the initial state $\mathbf{t}(0)$ using the set of equations

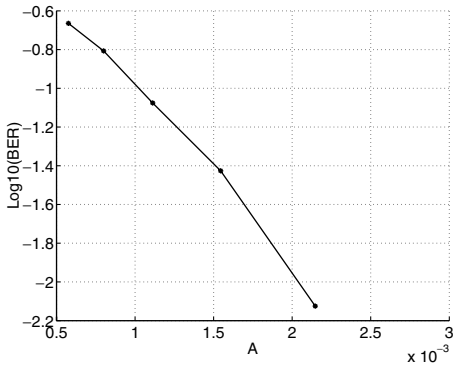

FIG. 3. Authorized receiver bit error rate versus modulation parameter A.

$$\begin{cases} s_t(0) = G_T(\mathbf{t}(0), m) \\ \mathbf{t}(1) = \mathbf{F}_T(\mathbf{t}(0), s_r(0), m) \\ \vdots \\ s_t(D_T) = G_T(\mathbf{t}(D_T), m) \\ \mathbf{t}(D_T + 1) = \mathbf{F}_T(\mathbf{t}(D_T), s_r(D_T), m) \end{cases} \tag{6}$$

From Eq. (3) the term $\mathbf{t}(D_T)$ in Eqs. (6) is a polynomial of the unknown $t_i(0)$ of order 2^{D_T}, and by choosing a large transmitter state dimension D_T solving Eq. (6) can be made computationally unfeasible. For instance, in our experimental system $D_T = 12$ and Eqs. (6) will be a polynomial of $t_i(0)$ of order 4096.

Noise in the communication channel or in analog components of the receiver and transmitter will add a small stochastic component to the observed signals. In this case, the unauthorized receiver can quantize the unknown transmitter state variables $\mathbf{t}(n)$, generate a hidden Markov model (HMM) for the quantized dynamical system, and obtain a maximum-likelihood (ML) estimation $\hat{m}_{\mathrm{ML}}$ for the message m using the probability of the sequence of measurements $s_t(n)$ conditioned on $m = 0, 1$:

$$\hat{m}_{\mathrm{ML}} = \max_{m \in (0,1)} p(s_t(1), \ldots, s_t(D_T + 1) \mid m). \tag{7}$$

We can protect against such an attack by making the number of states N_s in the HMM model prohibitively large. The number of states N_s can be approximated by

$$N_s \approx \left(\frac{L_T}{L_q}\right)^{D_T}, \tag{8}$$

where L_T is the range and L_q is the quantization size of each transmitter state variable t_i. It can be shown that if an unauthorized receiver uses quantization size L_q for each transmitter state component t_i, the quantization noise will result in decoding error probability P_u that is bounded below by

$$P_u \geq 1 - Q\left(\tfrac{1}{2}\sqrt{\frac{12A^2T_{\mathrm{bit}}}{D_T L_q^2 w^2}}\right), \tag{9}$$

where $Q(x) = (1/\sqrt{2\pi}) \int_{-\infty}^{x} e^{-(z^2/2)} dz$. From Eqs. (8) and (9), an unauthorized receiver who attempts to keep the decoding error probability below P_u, has to use an HMM model with a number of states N_s that is bounded below by

$$N_s \geq \left[\frac{2wL_T}{A}\sqrt{\frac{D_T}{12T_{\mathrm{bit}}}}Q^{-1}(1 - P_u)\right]^{D_T}. \tag{10}$$

In order to maximize security, namely, maximize N_s, we used the smallest A that is large enough to ensure low decoding error rate encountered by the authorized receiver $P_a \leq 0.01$.

Implementation of a DDE transmitter using analog hardware will add noise to the dynamics of the

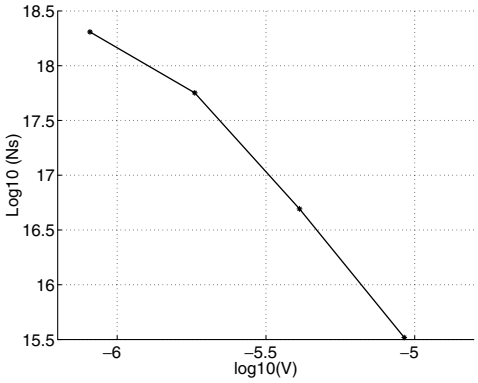

FIG. 4. Unauthorized receiver Viterbi states number N_s versus transmitter noise variance V.

transmitter and blur the separation between the 0 and 1 attractors. Therefore, in the presence of noise a larger A will be required in order to increase the separation between the attractors and maintain a low receiver decoding error P_a. However, from Eq. (10) larger A allows the unauthorized receiver to use a smaller number of states N_s implying reduced security. We simulated component accuracy by adding zero mean Gaussian noise with variance V to each transmitter state component t_i. We calculate N_s using Eq. (10), requiring $P_u \leq 0.2$. From Fig. 4 it is evident that the use of more accurate analog components at the transmitter results in higher security, namely, larger N_s. Indeed, note that N_s of order 10^{15-17} implies an enormous computational burden.

Summary.—We have proposed a method for public key encryption using our distributed dynamical encryption scheme [7]. A high-dimensional dissipative dynamical system is separated into two parts: one part is placed at the transmitter and the other at the receiver. In our illustrative modulation scheme a bit is transmitted by choosing one of two values for the modulation parameter and then iterating the dynamical system until its transient trajectory settles onto an attractor. An authorized receiver knows the full dynamics and can simulate the system *a priori* in order to find the state space location of the two attractors corresponding to 0's or 1's. This receiver is able to decode the message by observing the convergence of the system trajectory to the 0-attractor or to the 1-attractor in a reconstructed phase space as illustrated in Fig. 1. An unauthorized receiver does not know the dynamics of the receiver and is forced to use computationally unfeasible algorithms. (The authors know no other method besides the use of computationally unfeasible algorithms described in the paper for an attacker to try to break the system.)

A promising future direction for DDE may be a hardware implementation (analog electronics/optics) using continuous time dynamics with large transmitter state dimension. High-dimensional coupled map lattices which contain hundreds of cells have been investigated [8] and can be used to implement encryption schemes with a very large state dimension and a very high level of security. Such implementations may be appealing for applications which require a very high level of security but where transmission bandwidth and power efficiency are not crucial factors. New design methods aimed at selecting efficient and secure dynamical systems for use in DDE would be quite attractive. Finally, it is possible that the specific implementation we used in this paper embodied in the particular map and modulation method will prove to be weak encryption. The general concept proposed in this paper appears quite robust, and it is likely that a large set of dynamical systems resistant to system-specific attacks may be found.

This work was partially supported by the Army Research Office under MURI Grant No. DAAG55-98-1-0269, by the U.S. Department of Energy, Office of Basic Energy Sciences, Division of Engineering and Geosciences, under Grants No. DE-FG03-90ER14138 and No. DE-FG03-95ER14516, by a grant from the National Science Foundation, NSF PHY0097134, and by a grant from the Office of Naval Research, N00014-00-1-0181.

[1] T. L. Carroll and L. M. Pecora, Physica (Amsterdam) **67D**, 126 (1993); A. R. Volkovskii and N. Rulkov, Tech. Phys. Lett. **19**, 97 (1993); K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993); U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, Phys. Rev. E **53**, 4351 (1996).

[2] S. Hayes, C. Grebogi, E. Ott, and A. Mark, Phys. Rev. Lett. **73**, 1781 (1994); Y. Lai, E. Bollt, and C. Grebogi, Phys. Lett. A **255**, 75 (1999).

[3] H. Dedieu, M. P. Kennedy, and M. Hasler, IEEE Trans. Circuits Syst. II **40**, 634 (1993).

[4] T. Habitsu, Y. Nishio, I. Sasase, and S. Mori, in *Advances in Cryptology—Eurocrypt '91* (Springer, Berlin, 1991), p. 127; M. S. Baptista, Phys. Lett. A **540**, 50 (1991); L. Kocarev and G. Jakimoski, Phys. Lett. A **289**, 199 (2001).

[5] Henk C.A. van Tilborg, *Fundamentals of Cryptology* (Kluwer Academic Publishers, Dordrecht, 2000).

[6] H. D. I. Abarbanel, R. Brown, J. J. Sidorowich, and L. S. Tsimring, Rev. Mod. Phys. **64**, 1331 (1993); H. D. I. Abarbanel, *The Analysis of Observed Chaotic Data* (Springer, New York, 1996).

[7] All the details of our simulation may be found at http://inls.ucsd.edu/~roy/DDE/MainPage/.

[8] K. Kaneko, *Theory and Applications of Coupled Map Lattices*, Nonlinear Science Theory and Applications (Wiley, New York, 1993).