

Additive Mixing Modulation for Public Key Encryption Based on Distributed Dynamics

Roy Tenny and Lev S. Tsimring

Abstract—We introduce a public key encryption scheme that is based on additive mixing of a message with chaotic nonlinear dynamics. A high-dimensional dissipative nonlinear dynamical system is distributed between transmitter and receiver. The transmitter dynamics is public (known to all) and the receiver dynamics is private (known only to the authorized receiver). Bidirectional signals that couple transmitter and receiver are transmitted over a public channel. Once the chaotic dynamics which is initialized with a random state converges to the attractor, a message is mixed with the chaotic dynamics at the transmitter. The authorized receiver who knows the entire dynamics can use a simple algorithm to decode the message. An unauthorized receiver does not know the receiver dynamics and needs to use computationally unfeasible algorithms in order to decode the message. Security is maintained by altering the private receiver dynamics during transmission. We show that using additive mixing modulation is more efficient than the attractor position modulation distributed dynamics encryption scheme. We demonstrate the concept of this new scheme by simulating a simple coupled map lattice.

Index Terms—Chaos, nonlinear dynamics, public key encryption.

I. INTRODUCTION

USING chaotic dynamics for encryption is a relatively new field of research that has been studied during the last decade. There are two main types of encryption schemes: public (asymmetric) and private (symmetric). In secret (symmetric) key encryption a secret key shared between transmitter and receiver is used to encrypt the message at the transmitter and decode it at the receiver. In public (asymmetric) key encryption, a public key which is assumed to be known to all, including the unauthorized receiver, is used to encrypt a message, and a private key which is known only to the authorized receiver is used to decode the message. Decoding the message using the public key is made computationally unfeasible. Rivest–Shamir–Adelman (RSA) [3] is the most commonly used public key encryption scheme; however, other methods such as elliptic curves [4], knapsack [5], and El-Gammal [6] exist. A description of various secret and public key encryption schemes can be found in [7].

Manuscript received August 21, 2003; revised May 14, 2004, September 10, 2004. This work was supported in part by the Army Research Office under MURI Grant DAAG55-98-1-0269, and in part by the U.S. Department of Energy, Office of Basic Energy Sciences, under Grant DE-FG03-95ER14516. This paper was recommended by Associate Editor N. Ling.

R. Tenny is with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093-0354 USA (e-mail: roy859@yahoo.com).

L. S. Tsimring is with the Institute for Nonlinear Science, University of California at San Diego, La Jolla, CA 92093-0402.

Digital Object Identifier 10.1109/TCSI.2004.842870

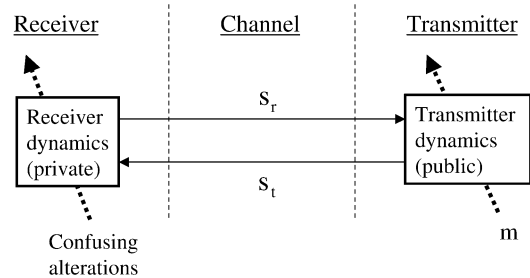


Fig. 1. DDE general scheme.

Unlike traditional encryption schemes that are defined over integer number fields, chaos based encryption schemes are defined over continuous number fields, and can be implemented using analog hardware.

Many secret (symmetric) key chaos based encryption schemes have been proposed during the last decade. Those schemes can be divided into the following three main categories: chaotic shift keying [8], chaos synchronization, [9]–[12], and controlling chaos [13], [14]. Cryptanalysis of such methods is discussed in [15]–[19].

Recently, we introduced a new chaos based public (asymmetric) key encryption scheme based on *distributed dynamics encryption* (DDE) [1], [2]. In DDE, information was transmitted using multiple attractor modulation [20]. In this paper we propose a public key encryption scheme that is based on DDE, however the message is modulated by additive mixing of the message with the chaotic signal. We show that this kind of modulation significantly improves the efficiency of DDE, and yet maintains the same level of security.

This paper is organized as follows. In Section II, we describe the general concept underlying public key encryption schemes that are based on distributed dynamics. In Section III, we describe a new public key DDE scheme with additive mixing modulation. In Section IV we discuss security of DDE. In Section V, we make a comparison between additive mixing and multiple attractor modulation. In Section VI, we demonstrate the concept of DDE through simulation, and in Section VII, we summarize our analysis and suggest directions for future research.

II. DISTRIBUTED DYNAMICS ENCRYPTION

A DDE scheme is based on a high-dimensional nonlinear dynamical system that is distributed into two parts, as illustrated in Fig. 1. One part of the dynamics is placed at the receiver and the other at the transmitter. The transmitter and receiver are coupled through bidirectional signals: s_t transmitted from transmitter

to receiver and s_r from receiver to transmitter. The entire dynamical system is comprised of the transmitter receiver and the coupling signals, and has some measurable characteristic which changes when we modulate the dynamics. We will call this characteristic **modulation signature**. In this paper, the modulation signature used is the position of the attractor to which the entire dynamical system converge, however other modulation properties may be used. The modulation signature depends on both transmitter and receiver dynamics, and can be changed by altering either dynamics. The transmitter dynamics and the transmitted coupling signals are assumed to be known to the unauthorized receiver. The receiver dynamics is private and is known only to the authorized receiver. Data are modulated by altering the transmitter dynamics, which results in a change of the modulation signature, for instance, a shift in the position of the attractor. The modulation signature is also changed by frequently altering the private dynamics of the receiver in order to confuse an unauthorized receiver. The authorized receiver knows the entire dynamics and therefore can simulate the dynamics off-line before transmission begins, in order to determine the mapping between the modulation signature and the value of the transmitted message. During transmission the authorized receiver uses the mapping between the modulation signature and the message to decode the message. The unauthorized receiver does not know the private dynamics of the receiver and can not determine the mapping between the modulation signature and the message.

In all public key encryption schemes the advantage of the authorized receiver over the unauthorized receiver is a computational one and not information theoretic one, and the unauthorized receiver can always decode the message given a large enough computational power. A secure public key encryption scheme requires the unauthorized receiver to use computationally unfeasible algorithms to decode the message. In DDE, the receiver dynamics, which are the private key, enables the authorized receiver to establish the mapping between the modulation signature and decode the message. The unauthorized receiver does not know the receiver dynamics, and is forced to use computationally unfeasible algorithms to decode the message.

III. DDE SCHEME BASED ON ADDITIVE MIXING

The transmitted message is divided into blocks of length T_m samples (criterion for choosing T_m will be discussed later). The public key encryption scheme we propose in this paper is comprised of two phases that are used to encrypt each message block.

A. Phase-I: Convergence to Attractor

During the first phase (Fig. 2), the entire dynamical system (transmitter, receiver, and coupling signals) is allowed to converge from a random initial state to the attractor. No message is transmitted during this phase. The attractor position is the modulation signature discussed in the previous section, and is determined by the transmitter public dynamics and the receiver private dynamics. Only the authorized receiver who knows the entire dynamics knows the position of the attractor. Knowing the position of the attractor enables prediction of the dynamics on

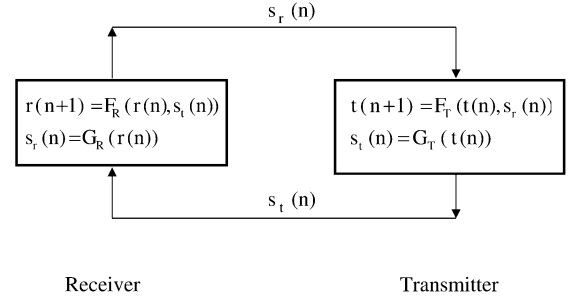


Fig. 2. Phase-I: (convergence). The dynamics is initialized with a random state and is then iterated long enough to allow the convergence to the attractor. No message is transmitted during this phase.

the attractor, and the use of a computationally feasible algorithm for decoding the message that will be described in Section III-B. The transmitter dynamics is given by

$$\mathbf{t}(n+1) = \mathbf{F}_T(\mathbf{t}(n), s_r(n)). \quad (1)$$

$\mathbf{t}(n) = [t_1(n), \dots, t_{D_T}(n)]$ is a D_T -dimensional transmitter state, known only to the transmitter. $s_r(n)$ is a public scalar transmitted from receiver to transmitter. $\mathbf{F}_T(\bullet)$ is a D_T -dimensional vector field which is public. The scalar s_t transmitted from transmitter to receiver is given by the public function $G_T(\bullet)$

$$s_t(n) = G_T(\mathbf{t}(n)). \quad (2)$$

The receiver dynamics is given by

$$\mathbf{r}(n+1) = \mathbf{F}_R(\mathbf{r}(n), s_t(n)). \quad (3)$$

$\mathbf{r}(n) = [r_1(n), \dots, r_{D_R}(n)]$ is a D_R -dimensional receiver state, and is private. $s_t(n)$ is a public scalar transmitted from transmitter to receiver. $\mathbf{F}_R(\bullet)$ is a D_R -dimensional vector field, and is kept private. The public scalar s_r transmitted from receiver to transmitter is given by the private function $G_R(\bullet)$

$$s_r(n) = G_R(\mathbf{r}(n)). \quad (4)$$

Once the dynamics has converged to the attractor, the second phase of transmission begins.

B. Phase-II: Message Modulation

A scheme of DDE during the second phase is illustrated in Fig. 3. The transmitter dynamics is the same as in phase-I, and are given by (1) and (2). However, in phase-II, the signal s_m transmitted from transmitter to receiver is generated by adding the message m to the signal $s_t(n)$

$$s_m(n) = s_t(n) + m(n). \quad (5)$$

The receiver needs to “strip off” the message component from the received signal s_m to recover the chaotic component $s_t(n)$. Feeding an estimation $\hat{s}_t(n)$ of the chaotic component $s_t(n)$ to the receiver dynamics which is given by

$$\mathbf{r}(n+1) = \mathbf{F}_R(\mathbf{r}(n), \hat{s}_t(n)) \quad (6)$$

$$s_r(n) = G_R(\mathbf{r}(n)) \quad (7)$$

will cause the overall dynamics to converge to the same attractor it converged to on phase-I when no message was added to the dynamics.

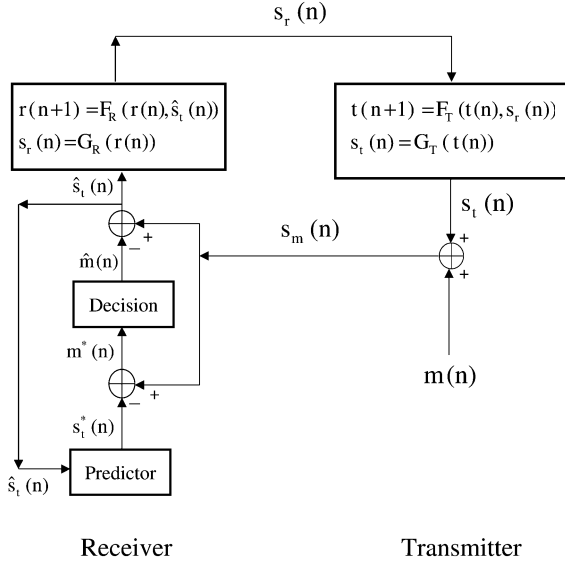


Fig. 3. Phase-II: (modulation). A message is added at the transmitter. At the receiver the message is decoded and “stripped off” the received signal. The addition and subtraction of message is transparent to the chaotic dynamics, and the trajectory remains on the attractor.

We now describe how the authorized receiver decodes the message $m(n)$, and obtains an estimation $\hat{s}_t(n)$ of the chaotic component $s_t(n)$. Before actual transmission begins, the authorized receiver simulates off-line the dynamics of phase-I, and stores a set of points that represents the position of the attractor in a time-delay embedding $\mathbf{s}_t(n) = (s_t(n), \dots, s_t(n - (D_e - 1)))$, with D_e chosen by various known methods [21], [22]. Knowing the position of the attractor enables to obtain a preliminary prediction $s_t^*(n)$ of the sample $s_t(n)$ using previous $D_e - 1$ final estimations $\hat{s}_t(n - 1)$ of the sequence $s_t(n)$. The preliminary prediction is valid only on the attractor, and is given by

$$s_t^*(n) = P(\hat{s}_t(n - 1)). \quad (8)$$

We can also obtain a preliminary estimation $m^*(n)$ for the message $m(n)$, given by

$$m^*(n) = s_m(n) - s_t^*(n) = s_m(n) - P(\hat{s}_t(n - 1)). \quad (9)$$

The preliminary estimation error $e_m^*(n)$ is defined by

$$e_m^*(n) = m(n) - m^*(n). \quad (10)$$

We can obtain a decision $\hat{m}(n)$ about the message $m(n)$ using the preliminary estimation $m^*(n)$

$$\hat{m}(n) = \text{Decide}(m^*(n)). \quad (11)$$

The decision can be based on a maximum likelihood approach, minimum distance, or any other method described in the literature. Assuming that the error $e_m^*(n)$ is not large enough to cause a decision error, the estimation $\hat{m}(n)$ will be accurate, so that $\hat{m}(n) = m(n)$. The receiver can now use the message estimation $\hat{m}(n)$ to obtain an improved estimation $\hat{s}_t(n)$ for the signal $s_t(n)$ using

$$\hat{s}_t(n) = s_m(n) - \hat{m}(n). \quad (12)$$

The estimation $\hat{s}_t(n)$ is used by the predictor in (8) to obtain preliminary estimations s_t^* in following iterations.

IV. SECURITY ANALYSIS

From (5), it is evident that in order to decode the message $m(n)$ the unauthorized receiver needs to estimate the chaotic component $s_t(n)$ given the sequences $s_m(n)$ and $s_r(n)$. The authorized receiver obtains an estimation $\hat{s}_t(n)$ of $s_t(n)$ by simulating the entire chaotic dynamics off-line, in order to find the position of the attractor. The attractor position is then used to obtain the estimation sequence $\hat{s}_t(n)$ using the algorithm described in the previous section.

Knowing the private dynamics and the attractor position allows the authorized receiver to use computationally feasible algorithms to decode the message. An unauthorized receiver may attempt to decode the message without using receiver private dynamics, by considering only the transmitter public dynamics, and the public signals s_t and s_r . However, we will show that these types of attack can be made computationally unfeasible.

In this section, we describe several methods that can be used by the unauthorized to decode the message $m(n)$, and the corresponding ways to protect against such attacks.

A. Driving the Transmitter Dynamics With Receiver Signal

1) *Attack*: Since the dynamics of the transmitter $\mathbf{F}_T(\bullet)$, $G_T(\bullet)$, and the transmitted signals $s_t(n)$, $s_r(n)$ are public, the unauthorized receiver can duplicate the transmitter dynamics and drive it with the receiver signal $s_r(n)$ to recover the sequence $s_t(n)$. Using (5), the unauthorized receiver can recover the message by using $\hat{m}(n) = s_m(n) - s_t(n)$.

2) *Protection*: The transmitter dynamics is chaotic and is not slaved by the sequence $s_r(n)$. Therefore, driving the duplicate transmitter dynamics with the same sequence $s_r(n)$ will not result in the same sequence $s_t(n)$ unless the transmitter initial state $\mathbf{t}(0)$ is accurately known. The unauthorized receiver does not know the transmitter random initial state $\mathbf{t}(0)$, and can not recover the sequence $s_t(n)$ nor decode the message $m(n)$ by driving the transmitter dynamics with the sequence $s_r(n)$.

B. Reconstructing the Attractor Position

1) *Attack*: The unauthorized receiver may attempt to reconstruct the attractor position using time delays of the transmitted signal $s_t(n)$. The attractor position is then used to decode the message using the same algorithm as the authorized receiver.

2) *Protection*: During phase-I the state of the dynamical system converges to the attractor, and except for the last few iterations most samples lay on a transient of the dynamics and do not reveal enough information about the attractor position. During phase-II the dynamics lies on the attractor, however the receiver secret dynamics is altered before the trajectory provides enough samples to reconstruct the attractor position and the predictor $P(\bullet)$ with a high enough accuracy which is sufficient to decode the message. For this reason, the modulation used should be fine grained so the unauthorized receiver will need more samples to reconstruct the attractor position and the predictor $P(\bullet)$ with sufficient accuracy. For instance, if the pulse amplitude modulation (PAM) shown in Fig. 4 is

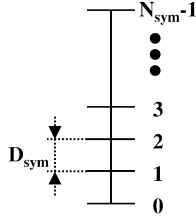


Fig. 4. PAM modulation.

used, the distance between adjacent symbols, D_{sym} , should be kept as small as possible in order to force the unauthorized receiver to reconstruct the dynamics with a higher accuracy, and to allow a longer message transmission duration T_m before the unauthorized receiver can decode the message. Yet, the distance D_{sym} should be large enough to enable decoding by the unauthorized receiver in the presence of noise in the channel or the components (see Section VI).

C. Reconstructing the Receiver Private Dynamics

1) *Attack*: The unauthorized receiver can use the receiver input $s_t(n)$ and output $s_r(n)$ to reconstruct the transmitter private dynamics $\mathbf{F}_R(\bullet)$, $G_R(\bullet)$. Knowing the transmitter dynamics the unauthorized receiver can iterate the entire dynamics off-line in order to reconstruct the position of the attractor, and decode the message using the same algorithm the authorized receiver uses.

2) *Protection*: Protection against this type of attack can be obtained by altering the receiver dynamics frequently. Before the unauthorized receiver will collect enough samples to reconstruct the receiver private dynamics the receiver dynamics will be altered, and the previous receiver dynamics will not be relevant during future transmissions.

D. Solving Transmitter Public Dynamics Equations for Message

1) *Attack*: The dynamics of the transmitter is public, and so are its input s_r and output s_t . An unauthorized receiver may attempt to obtain an estimation for the message m and the transmitter initial state $\mathbf{t}(0)$ that will reproduce the transmitter output s_t given the transmitter input s_r . In principle, this can be done by solving the following set of equations for m and $\mathbf{t}(0)$:

$$\begin{cases} s_t(0) = G_T(\mathbf{t}(0), m) \\ \mathbf{t}(1) = \mathbf{F}_T(\mathbf{t}(0), s_r(0), m) \\ \vdots \\ s_t(D_T) = G_T(\mathbf{t}(D_T), m) \\ \mathbf{t}(D_T + 1) = \mathbf{F}_T(\mathbf{t}(D_T), s_r(D_T), m). \end{cases} \quad (13)$$

2) *Protection*: Solving (13) can be made computationally unfeasible by using a high dimension D_T for the transmitter state, and by using transmitter dynamics $\mathbf{F}_T(\bullet)$ which is a polynomial of high degree p . Doing so will result in having (13) containing polynomial components of the form $[t_i(0)]^{p^{D_T}}$. For example, in case we use transmitter dimension $D_T = 10$ and $p = 4$ (13) will contain polynomials of the form $(t_i(0))^{1,048,576}$. By using sufficiently large D_T and p solving for (13) can be made computationally unfeasible.

In the absence of analog circuitry noise, the difficulty in recovering $t(n)$ and the message m is equivalent to the difficulty in recovering the random initial state $t(0)$. If circuitry noise is present, recovery of the secret transmitter state $t(n)$ can be done by quantization of the continuous transmitter high-dimensional phase space and generating a hidden Markov model (HMM) for the dynamics. $t(n)$ can then be reconstructed by using Viterbi algorithm to obtain a maximum likelihood estimator. By increasing the transmitter dynamics D_t and increasing the required reconstruction accuracy we can force the unauthorized receiver to use fine grained quantization in a high-dimensional phase space which results in a computationally unfeasible number of states in the Viterbi algorithm. Detailed analysis of the computational difficulty in reconstruction of $t(n)$ using an HMM model is beyond the scope of this paper and can be found in [2].

E. Known Plaintext Attack

1) *Attack*: The unauthorized receiver may obtain a plaintext sequence $m(n)$ and the corresponding ciphertext sequence $s_m(n)$, and recover $s_t(n)$ by using $s_t(n) = s_m(n) - m(n)$. He then may use the sequence $s_t(n)$ to obtain a predictor $P(\bullet)$ and use it to decode other messages.

2) *Protection*: By altering the receiver dynamics at the beginning of each transmitted message block we can change the position of the attractor. By doing so we ensure that a predictor $P(\bullet)$ used for one message block will not be useful during the transmission of another message block since the position of the attractor has changed.

V. ADDITIVE MIXING VERSUS MULTIPLE ATTRACTOR MODULATION

When compared to DDE scheme based on attractor modulation ([1], [2]), the additive mixing modulation scheme described in this paper provides higher symbol rate and simpler implementation of M-ary modulations.

A. Higher Symbol Rate

In a DDE scheme that is based on attractor position modulation ([1], [2]) the state of the dynamical system is initialized with a random value and the dynamical system iterates until the state converges to one of several allowed attractors. Therefore, the symbol rate is bounded by the time it takes to converge to one of the allowed attractors. The bit rate R_b is then given by

$$R_b = \frac{1}{T_a} \log_2(M) \quad (14)$$

where M is the number of allowed attractors, and T_a is the time (continuous dynamical system) or the number of iterations (discrete map) that takes the trajectory to converge to the attractor.

In the additive mixing scheme described in this paper the bit rate R_b^* is given by

$$R_b^* = \frac{T_m}{T_a + T_m} \log_2(N_{\text{sym}}) \quad (15)$$

where T_m is the number of samples during the modulation phase and N_{sym} is the number of allowed symbols. The bit rate in the additive mixing modulation scheme is larger than the bit

rate in the multiple attractor modulation scheme by a factor of $(T_m T_a / (T_m + T_a)) \log_M(N_{\text{sym}})$. The bit rate of both modulation schemes can be increased by decreasing the convergence duration T_a . The bit rate R_b^* of the additive mixing modulation can be increased by using large T_m . However, as mentioned in Section IV-B, the modulation phase duration T_m should not be long enough to enable the unauthorized receiver to reconstruct the dynamics on the attractor.

B. Simple Implementation of M-ary Modulations

Using multiple attractor modulation with a large number of attractors M may be difficult to implement, since it requires to simulate all allowed attractors off-line before transmission begins, and to store the position of all attractors. Also the decoding algorithm can require intensive computation since it needs to measure the distance between the converged state and all allowed attractors.

Using additive mixing enables simple modulations and decoding of M-ary modulations such as PAM, or quadrature amplitude modulations (QAM). The simplicity is due to the fact that the message is added to the chaotic dynamics and is not part of it, and once the message component m is separated from the chaotic component s_t at the receiver, decoding is independent of the chaotic dynamics.

VI. SIMULATION

In order to demonstrate feasibility we simulated an additive mixing DDE scheme using a simple coupled map lattice. We used transmitted state dimension $D_T = 12$ and receiver state dimension $D_R = 2$. All details of our simulation may be found in [23].

A. Dynamics of Phase-I

During the convergence of the dynamics from a random initial state to the attractor, the transmitter dynamics $\mathbf{F}_T(\bullet)$ is controlled by the map

$$t_j(n+1) = d_{j,j-1} \cdot t_{j-1}^2(n) + d_{j,j} \cdot t_j^2(n) + d_{j,j+1} \cdot t_{j+1}^2(n) + e_{j,j} \cdot |t_j(n)| + f_j \cdot s_r^2(n) + g_j, \quad j = 1, \dots, D_T \quad (16)$$

and $s_t(n)$ is given by

$$s_t(n) = w \cdot \sum_{j=1}^{D_{tr}} |t_j(n)|. \quad (17)$$

The receiver dynamics $\mathbf{F}_R(\bullet)$ is given by

$$r_i(n+1) = a_{i,i-1} \cdot r_{i-1}^2(n) + a_{i,i} \cdot r_i^2(n) + a_{i,i+1} \cdot r_{i+1}^2(n) + b_i \cdot \hat{s}_t^2(n) + c_i, \quad i = 1, \dots, D_R \quad (18)$$

and the transmitted signal $s_r(n)$ is given by

$$s_r(n) = \sum_{i=1}^{D_R} h_i \cdot r_i^2(n). \quad (19)$$

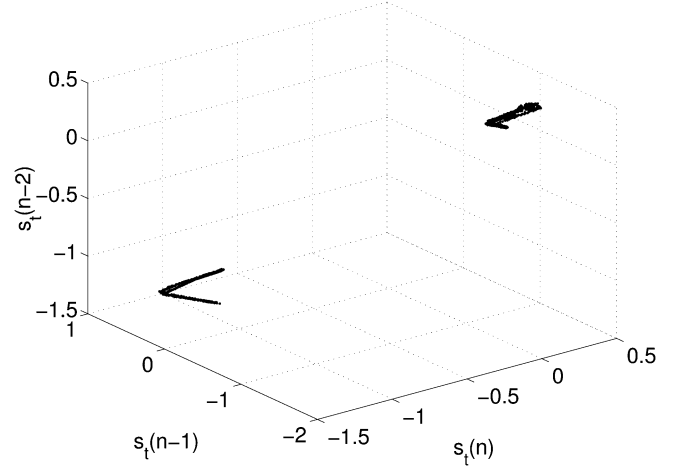


Fig. 5. A 3-D time delays embedding of the attractor to which the sequence $s_t(n)$ converges. The attractor position is obtained by off-line simulation performed before real transmission begins. During phase-I the trajectory converges to this attractor and during phase-II the sequence $\hat{s}_t(n)$ remains on it.

We chose the parameters $a, b, c, d, e, f, g, h, w$, such that the system attractor is chaotic. Values of parameters can be found in [23].

B. Dynamics of Phase-II

During phase-II, a message was added to the transmitted signal. The transmitter dynamics is controlled by the map given in (16), (17) and the transmitted signal $s_m(n)$ is given by

$$s_m(n) = s_t(n) + m(n) \quad (20)$$

where $m(n)$ is a random message generated by using the modulation shown in Fig. 4 with parameters D_{sym} and N_{sym} .

The receiver dynamics $\mathbf{F}_R(\bullet)$ is given by

$$r_i(n+1) = a_{i,i-1} \cdot r_{i-1}^2(n) + a_{i,i} \cdot r_i^2(n) + a_{i,i+1} \cdot r_{i+1}^2(n) + b_i \cdot \hat{s}_t^2(n) + c_i, \quad i = 1, \dots, D_R. \quad (21)$$

(Note: in phase-I we used s_t in the receiver dynamics equations, where in phase-II we used the estimation \hat{s}_t). The signal $s_r(n)$ is given by

$$s_r(n) = \sum_{i=1}^{D_R} h_i \cdot r_i^2(n). \quad (22)$$

The dimensions D_T, D_R and the parameters a, b, c, d, e, f, g, h are given the same values used during phase-I. The prediction model $\mathbf{P}(\bullet)$ in (8) was generated by simulating the dynamics of phase-I off-line and storing N_r samples \mathbf{s}_t lying on the attractor. The embedding dimension used was $D_e = 3$. The prediction model $\mathbf{P}(\bullet)$ was used to obtain the preliminary estimation $s_t^*(n)$. A preliminary estimation $m^*(n)$ for the message $m(n)$ was given by (9). A decision $\hat{m}(n)$ was made by choosing the nearest bin to $m^*(n)$, and an estimation $\hat{s}_t(n)$ was obtained using (12).

Shown in Fig. 5 is a reconstruction of the attractor obtained in off-line simulations. The attractor shown in Fig. 5 is plotted in a three-dimensional (3-D) time delay embedding phase space.

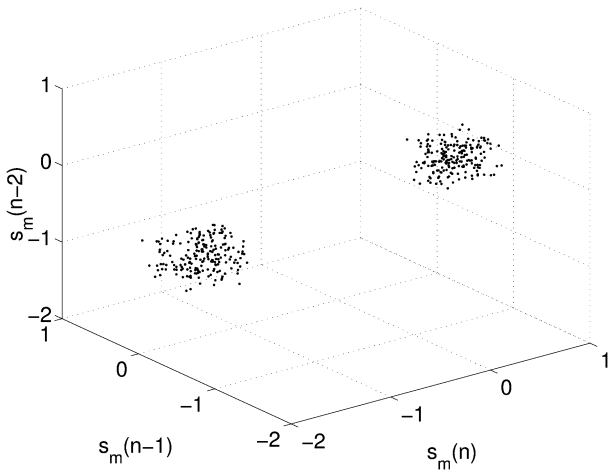


Fig. 6. A 3-D time delay embedding of the sequence $s_m(n)$ transmitted during phase-II. The addition of a message sequence $m(n)$ perturbs the attractor of $s_m(n)$ around the attractor of $s_t(n)$ shown in Fig. 5. Modulation parameters: $D_{\text{sym}} = 0.05$, $N_{\text{sym}} = 10$.

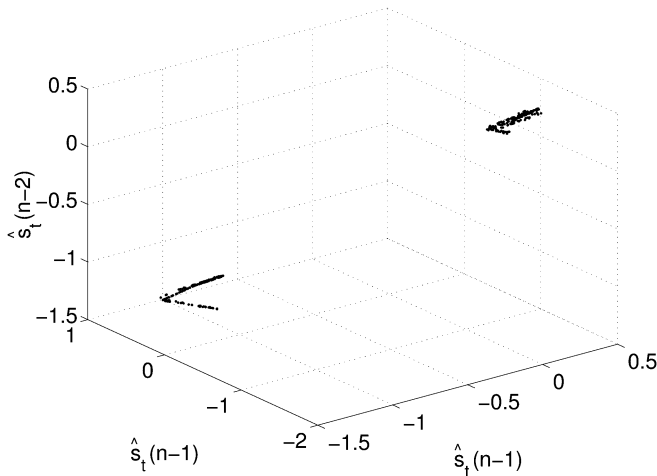


Fig. 7. A 3-D time delay embedding of the attractor of the sequence $\hat{s}(n)$ obtained at the receiver during phase-II. This attractor is an estimation of the attractor shown in Fig. 5 obtained by stripping of the message from the transmitted sequence s_m that lies on the attractor shown in Fig. 6.

This attractor is used during transmission to obtain the predictor $P(\bullet)$ given by (8).

Shown in Fig. 6 is the transmitted signal $s_m(n)$ in a 3-D time delay embedding phase space. The message that has been added to $s_m(n)$ in (5) perturbs the trajectory around the attractor of $s_t(n)$ shown in Fig. 5. Shown in Fig. 7 is a 3-D time delay embedding of the estimation $\hat{s}_t(n)$ which was calculated at the receiver. This attractor is in fact an estimation of the reference attractor shown in Fig. 5 using the sequence $s_m(n)$ that lies on the attractor shown in Fig. 6.

Shown in Fig. 8 is the mean square of the preliminary prediction error $e_s^*(n) = s^*(n) - s(n)$ as a function of the number of samples N_r that were used to store the position of the reference attractor and generate the predictor $P(\bullet)$ in (8). The more points that are available, the more accurate the predictor is.

We used a large value, $D_{\text{sym}} = 5$ while estimating the error e_s^* (Figs. 8 and 9) in order to mitigate decision errors generated by the decision block (Fig. 3). The large value for D_{sym} is used only for the purpose of estimating e_s^* , and in the actual system

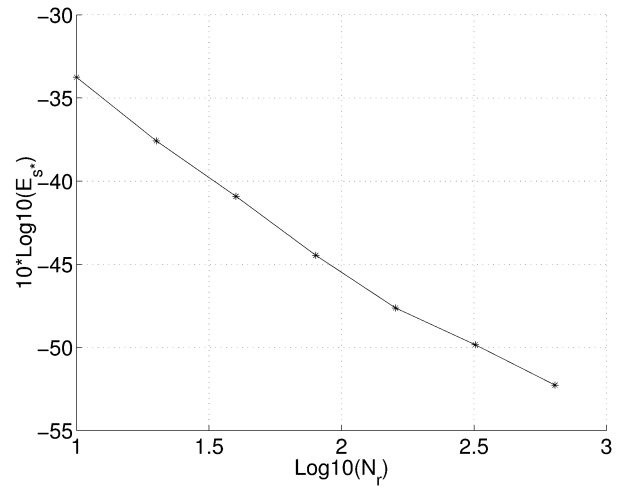


Fig. 8. Mean square of preliminary estimation error e_s^* as a function of the number of samples N_r used to represent the reference attractor and generate the predictor $P(\bullet)$. $T_a = 100$, $N_{\text{sym}} = 10$. Modulation dependent decision errors at the receiver were eliminated by using large distance between adjacent symbols: $D_{\text{sym}} = 5$.

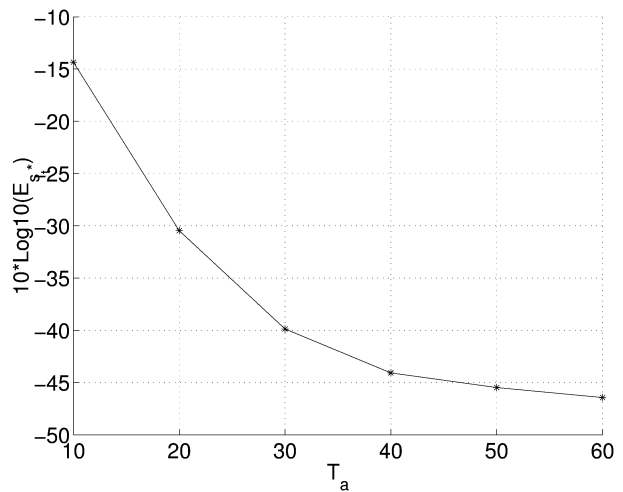


Fig. 9. Mean square of preliminary estimation error e_s^* during the first two iterations of phase-II (modulation phase) as a function of the number of iterations T_a performed during phase-I in order to converge from a random initial state to the attractor. $N_r = 100$, $N_{\text{sym}} = 10$. Modulation dependent decision errors at the receiver were eliminated by using large distance between adjacent symbols: $D_{\text{sym}} = 5$.

we used $D_{\text{sym}} = 0.05$ (Fig. 6). Those errors might propagate from the decision block back to the predictor block, and result in an estimation of e_s^* which is larger than the true prediction error encountered by an unauthorized receiver who may use various techniques to limit error propagation through the decision block. A too large estimation of e_s^* will result in the assumption that the reconstruction error encountered by the unauthorized receiver is actually larger than it really is and that the unauthorized receiver cannot decode the message due to the large error while in fact the actual error is smaller and the unauthorized receiver can decode the message. By using large $D_{\text{sym}} = 5$ we avoid the propagation of errors generated by the decision block back into the predictor, and obtain an error estimation for e_s^* which is purely due to the error in reconstructing the receiver dynamics and not due to erroneous decisions in decoding the symbols. The actual

error encountered by the unauthorized receiver will be equal to e_s^* in case it can completely mitigate decision error propagation, or larger in case it cannot. Therefore, by using $D_{\text{sym}} = 5$ we obtain a lower bound for the error e_s^* encountered by the unauthorized receiver. This lower estimation of e_s^* is pessimistic from the point of view of the authorized receiver, however it decreases the chance of decoding the message by the unauthorized receiver and enhances the security of the encryption scheme.

Fig. 8 also provides an estimation for the accuracy with which the unauthorized receiver can reconstruct the chaotic dynamics and the predictor P given N_r samples and therefore can be used to determine the maximum number of samples T_m that can be safely transmitted before the unauthorized receiver can decode the message. Shown in Fig. 9 is the mean square error of the preliminary prediction error e_s^* at the beginning of phase-II (during the first two samples of the modulation phase), as a function of the number of samples T_a used to allow the trajectory to converge to the attractor during phase-I. This graph can be used to determine the minimum value of convergence time T_a that is required in order to ensure low prediction error e_s^* and low message decoding error rate at the beginning of phase-II. We also simulated DDE by using $T_a = 50$ and $D_{\text{sym}} = 0.02$ and $N_{\text{ref}} = 1e4$. The resulting decoding error rate encountered by the authorized receiver was $P_a = 2E - 3$. Since we used a small value for D_{sym} then P_a included also the effect of decision errors at the receiver. We can now use Fig. 8 to determine the maximum number of samples that can be transmitted. We assume that the prediction noise encountered by the unauthorized receiver is gaussian. To ensure that the decoding error rate encountered by the unauthorized receiver will be at least $P_u \geq 0.3$, given that distance between symbols is $D_{\text{sym}} = 0.02$ we need to keep the noise standard deviation above $\sigma \geq 0.02$ ($20 * \log_{10}(\sigma) \geq -34$ dB). From Fig. 8, the maximum number of samples that can be safely transmitted before the receiver private dynamics should be altered is ten. This scheme is capable of transmitting ten times the number of symbols that can be transmitted by the DDE based on multiple attractors modulation described in [1], [2].

We can increase the number of samples that can be transmitted by decreasing D_{sym} , so that the unauthorized receiver will need more samples to reconstruct the dynamics on the attractor with higher accuracy. However decreasing D_{sym} will result in more errors encountered by the authorized receiver. In our simulation the error encountered by the authorized receiver is caused by the finite accuracy of the predictor $P(\bullet)$ which is based on $N_r = 10,000$ samples lying on the attractor that were obtained during the off-line simulation before transmission begins. We can increase the predictor accuracy by using larger N_r , thus allowing the use of smaller D_{sym} while keeping low error rate P_a encountered by the authorized receiver. However in a real communication channel D_{sym} should be large enough to allow low decoding error rate in the presence of channel noise.

VII. SUMMARY

In this paper, we presented a new scheme for public key encryption based on chaotic distributed nonlinear dynamics. The dynamics are distributed between transmitter and receiver

that are coupled bi-directionally through the communication channel. The dynamics of the transmitter and the coupling signals are public. The dynamics of the receiver is private, and known only to the authorized receiver. At the beginning of transmission the dynamical system is initialized with a random state. The dynamics is dissipative and during the first phase it is iterated long enough to allow it to converge to the attractor. Once the dynamics has converged to the attractor, a message is added to the signal transmitted from transmitter to receiver. At the receiver, the message is decoded by predicting the signal that would have been transmitted if a message was not added to the transmitter signal. This prediction is possible on the attractor, and requires knowledge of the attractor structure.

Only the unauthorized receiver who knows the dynamics of both receiver and transmitter can simulate the system off-line to obtain the position of the attractor that is required to decode the message. An unauthorized receiver does not know the private receiver dynamics, can not determine the attractor position, and is forced to use computationally unfeasible algorithms in order to decode the message. In this paper, we presented several methods an unauthorized receiver can use to decode the message and suggested methods to protect against such attacks. We showed that security can be enhanced by using the following guidelines.

- Initialize the transmitter dynamics with a random value at the beginning of each transmitted block.
- Alter the private receiver dynamics between two consecutive transmitted blocks.
- Use high-dimensional receiver and transmitter dynamics.
- Use a small message transmission duration T_m in order to prevent the unauthorized receiver from reconstructing the reference attractor.
- Use fine grained modulation (small D_{sym} in Fig. 4) in order to force the unauthorized receiver to reconstruct the reference attractor with higher accuracy in order to decode the message.

Comparison between the DDE and traditional public key encryption schemes such as RSA, elliptic curves and El-Gammal, reveals substantial differences: The major difference is the fact that DDE is defined over continuous number fields while traditional schemes are defined over integer number fields. As a consequence, DDE transmitter can in principle be implemented directly using analog components while implementation of traditional schemes requires digital hardware.

Also, the underlying concepts of the two are different: traditional schemes use one way functions which are relatively simple to calculate in one direction yet computation of their inverse can be made difficult. DDE, on the other hand, is based on enabling message decoding by off-line simulation of the high-dimensional nonlinear dynamical system which is entirely known to the authorized receiver, while an unauthorized receiver which has only partial knowledge of the dynamics is required to use computationally demanding methods. DDE can be implemented using a rich variety of chaotic functions, while traditional schemes are based on a limited pool of algorithmic procedures (typically exponentiation over Galois Fields).

DDE has the advantage of being the first chaotic dynamics based public key encryption scheme that can be defined entirely over continuous number fields. As such, it eliminates the need

for a secure key exchange between transmitter and receiver required in existing continuous state chaos based symmetric encryption schemes.

DDE is a new scheme, and it is too early to make any confident statements about its level of security or lack of security when compared to traditional public key encryption schemes. The process of building confidence in the security of any new encryption scheme may take years and several iterations of breaking and reinforcing the method may take place, and DDE is no exception. Yet, since to the best of our knowledge, DDE is currently the only public key encryption scheme that is defined entirely on continuous number fields it may be the only public key encryption scheme available in situations where digital implementation is undesirable.

The new scheme we presented in this paper is more efficient than the scheme described in [1], [2] which was based on the multiple attractor modulation since it enables the transmission of more than one symbol each time the dynamics converges from a random initial state to the attractor. Also, this new scheme enables the use of M-ary modulations such as PAM which are simpler to implement than a multiple attractor communication scheme with a large number of attractors that correspond to different symbols.

Finally, we demonstrated the principle of DDE based on additive mixing using a relatively simple chaotic system, and it is possible that the specific implementation used in this paper can be broken. However, DDE represents a new approach to public key encryption rather than a specific implementation, and we believe that given the large variety of high-dimensional systems that can be used, it is highly likely that a class of systems robust to a specific type of attack can be found.

ACKNOWLEDGMENT

The authors would like to thank H. D. I. Abarbanel, and L. E. Larson for helpful discussions.

REFERENCES

- [1] R. Tenny, L. S. Tsimring, L. E. Larson, and H. D. I. Abarbanel, "Using distributed nonlinear dynamics for public key encryption," *Phys. Rev. Lett.*, vol. 90, no. 4, 2003.
- [2] R. Tenny, L. S. Tsimring, H. D. I. Abarbanel, and L. E. Larson, "Asymmetric key encryption using distributed chaotic nonlinear dynamics," in *Proc. IASTED Int. Conf. Communications Internet and Information Technology*, St. Thomas, U.S. Virgin Islands, Nov. 2002, pp. 338–345.
- [3] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Comm. ACM*, vol. 21, pp. 120–126, Feb. 1978.
- [4] V. S. Miller, "Use of elliptic curves in cryptology," in *Crypto*, vol. 85, 1978, pp. 417–426.
- [5] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 5, pp. 525–530, Sep. 1978.
- [6] T. El-Gamal, "A public key cryptosystem and signature scheme based on discrete logarithms," in *Proc. Crypto Advances in Cryptology*, vol. 84, Berlin, Germany, 1985, pp. 10–18.
- [7] H. C. A. Van-Tilborg, *Fundamentals of Cryptology*. Norwell, MA: Kluwer, 2000.
- [8] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 634–642, Oct. 1993.

- [9] T. L. Carroll and L. M. Pecora, "Cascading synchronized chaotic systems," *Phys. D*, vol. 67, pp. 126–140, 1993.
- [10] A. R. Volkovskii and N. Rulkov, "Synchronous chaotic response of a nonlinear oscillating system as a principle for the detection of the information component of chaos," *Tech. Phys. Lett.*, vol. 19, pp. 97–99, 1993.
- [11] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with application to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, 1993.
- [12] U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, "Encoding messages using chaotic synchronization," *Phys. Rev. E*, vol. 53, pp. 4351–4361, 1996.
- [13] S. Hayes, C. Grebogi, E. Ott, and A. Mark, "Experimental control of chaos for communication," *Phys. Rev. Lett.*, vol. 73, no. 13, pp. 1781–1784, 1994.
- [14] Y. Lai, E. Bollt, and C. Grebogi, "Communicating with chaos using two-dimensional symbolic dynamics," *Phys. Lett. A*, vol. 255, pp. 75–81, 1999.
- [15] T. Yang, L.-B. Yang, and C.-M. Yang, "Breaking chaotic secure communication using a spectrogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998.
- [16] —, "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 45, no. 10, pp. 1062–1067, Oct. 1998.
- [17] J. B. Geddes, K. M. Short, and K. Black, "Extraction of signals from chaotic laser data," *Phys. Rev. Lett.*, vol. 83, no. 25, pp. 5389–5392, 1999.
- [18] M. K. Short, "Steps toward unmasking secure communications," *Int. J. Bifurc. Chaos*, vol. 4, no. 4, pp. 959–977, 1994.
- [19] —, "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurc. Chaos*, vol. 6, no. 2, pp. 367–375, 1996.
- [20] T. L. Carroll and L. M. Pecora, "Using multiple attractor chaotic systems for communication," *Chaos*, vol. 9, no. 2, pp. 445–451, Jun. 1999.
- [21] H. D. I. Abarbanel, *Analysis of Observed Chaotic Data*. New-York: Springer-Verlag, 1996.
- [22] H. D. I. Abarbanel, R. Brown, J. J. Sidorowich, and L. S. Tsimring, "The analysis of observed chaotic data in physical systems," *Rev. Mod. Phys.*, vol. 65, pp. 1331–1392, 1993.
- [23] Univ. California at San Diego. DDE Overview. [Online]. Available: <http://inls.ucsd.edu/~roy/DDE/MainPage/> 2003



Roy Tenny was born in Tel-Aviv, Israel, in 1967. He received the B.Sc. and M.Sc. degrees in electrical engineering from Tel Aviv University, Israel in 1989 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering (signal and image processing) from the University of California, San Diego, in 2003.

His research interests are in the areas of nonlinear dynamics, signal processing, pattern recognition, parameter estimation, and neural networks. Currently, he is a Consultant in the fields of signal processing

and algorithms development.



Lev S. Tsimring was born in Saratov, Russia, in 1959. He received the graduate and the Ph.D. degrees in physics and mathematics from the Gorky State University, Gorky, U.S.S.R., and the P.P. Shirshov Institute of Oceanology, Moscow, U.S.S.R., in 1980, and 1985, respectively.

Presently, he is a Research Scientist with the Institute for Nonlinear Science, at the University of California, San Diego. His research interests include nonlinear dynamics, chaotic synchronization, spatiotemporal chaos, pattern formation, and nonlinear signal

processing.