



STEPS TOWARDS CRYPTANALYSIS OF CHAOTIC ACTIVE/PASSIVE DECOMPOSITION ENCRYPTION SCHEMES USING AVERAGE DYNAMICS ESTIMATION

ROY TENNY* and LEV S. TSIMRING

Institute for Nonlinear Science,

**Department of Electrical and Computer Engineering,
University of California, San Diego, La Jolla, CA 92093-0354, USA*

Received July 7, 2003; Revised January 21, 2004

We analyze the security of encryption schemes based on chaos synchronization and active/passive decomposition. The security is quantified by the number of transmitted samples that has to be acquired in order to reconstruct the transmitted message with an accuracy that may compromise the transmitted information. The dynamics is estimated as the average of dynamics of the observed data within a small neighborhood of the time delay embedding phase space. We examine the factors that affect the choice of embedding dimension and neighborhood size by the unauthorized receiver. We show that the security can be enhanced by mixing a large randomly modulated message component with a smaller chaotic component while keeping the message modulation fine grained. This result is in contrast to the common approach to ensure security by adding a small message component to a larger chaotic component. Further, we show that even when a low dimensional chaotic map is used, then the unauthorized receiver is required to use a reconstruction embedding dimension that can be made large by using chaotic dynamics with large conditional negative Lyapunov exponent. This result allows one to avoid the common restriction to use only high dimensional chaotic dynamics to maintain security. We also suggest guidelines for the design of efficient active passive/passive decomposition schemes in order to maintain low transmission power, fast synchronization, and yet preserve security. We demonstrate our analysis using a relatively simple encryption scheme based on a one-dimensional chaotic tent map.

Keywords: Chaos; synchronization; encryption; embedding.

1. Introduction

Secure communication schemes that are based on chaotic dynamics have been studied for nearly a decade. Most of the proposed schemes are based on one of the following approaches: chaos synchronization [Carroll & Pecora, 1993; Volkovskii & Rulkov, 1993; Cuomo & Oppenheim, 1993; Parlitz *et al.*, 1996], chaotic shift keying [Dedieu & Hasler, 1993], and controlling chaos [Hayes *et al.*, 1994; Lai *et al.*, 1999]. Also, chaos based block ciphers were studied in [Kocarev & Jakimoski, 2001].

Conventional encryption schemes which are based on integer number theory have been studied for several decades. Cryptanalysis of such methods is based on well defined mathematical methodologies. A comprehensive introduction to such methods can be found in [van Tilborg, 2000]. Chaotic encryption schemes are relatively new, and the cryptanalysis of such schemes is not as well developed as that of conventional encryption schemes. Chaotic encryption schemes are defined over continuous vector fields, and it is difficult to establish their security analysis on closed

mathematical forms. In order to elevate the analysis of chaotic encryption schemes towards that of conventional encryption it is important to develop a set of evaluators that quantify security. The security level of a chaotic encryption scheme is measured by the ability of an unauthorized receiver to decode a secret message. In some chaotic modulation schemes the encryption is weak, and in some cases the chaotic message can be decoded even without any need for reconstruction of the underlying dynamics of the chaotic modulator. In [Yang *et al.*, 1998a] spectral analysis of the transmitted signal is used to decode a binary transmitted message, eliminating the need to reconstruct the secret dynamics. In [Yang *et al.*, 1998c] a chaos encryption scheme based on Chua’s circuit [Dedieu & Hasler, 1993] is cryptanalyzed using return maps of combinations of minimum and maximum peak values of transmitted waveform and the time intervals between the peaks. In some encryption schemes an unauthorized receiver can assume the general structure of the secret chaotic dynamics, and reconstruct the values of certain system parameters which are the secret key of the system. In [Geddes *et al.*, 1999] an encryption scheme using erbium-doped fiber-ring laser is cryptanalyzed by creating a simple parametric model based on the knowledge of laser dynamics. The ability to parameterize the secret dynamics can result in a significant reduction in the size of the encryption secret key space and reduce the security of the system.

1.1. Chaos synchronization using active/passive decomposition

Active/passive decomposition is a convenient general scheme for design and analysis of chaotic communication schemes [Kocarev & Parlitz, 1995; Ming Dai *et al.*, 1998]. The idea that underlies the active/passive decomposition is to divide a chaotic communication system into active and passive components. The dynamics of the full system has at least one positive Lyapunov exponent. The dynamics of the passive component has negative conditional Lyapunov exponents, and therefore transmitter and receiver with identical dynamics that are initialized at a random initial state and share the same active component synchronize at the rate of the maximal conditional negative Lyapunov exponent λ . Illustrated in Fig. 1 is a discrete time active/passive decomposition encryp-

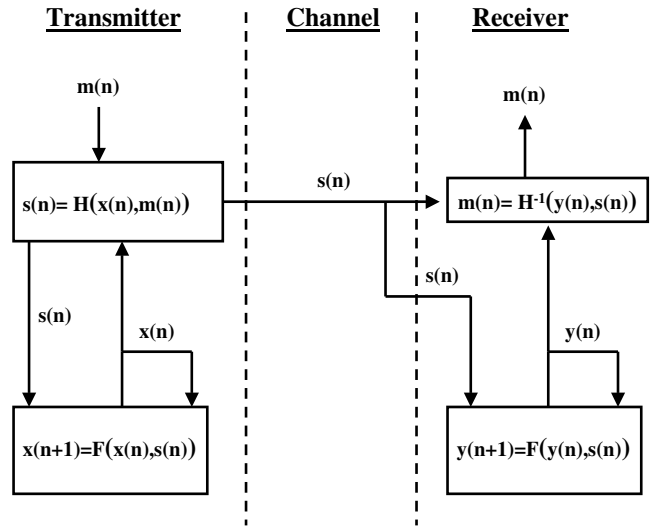


Fig. 1. Active passive decomposition: The receiver state $\mathbf{y}(n)$ synchronizes to the transmitter state $\mathbf{x}(n)$ at the rate of the largest conditional Lyapunov exponent λ , which is conditioned on the transmitted active signal $s(n)$.

tion scheme. The dynamics of the transmitter is governed by the chaotic map

$$\mathbf{x}(n + 1) = \mathbf{F}(\mathbf{x}(n), s(n)). \tag{1}$$

where $\mathbf{F}(\bullet)$ is a vector field that governs the evolution of the state $\mathbf{x}(n)$ in time. The active component $s(n)$ is transmitted from transmitter to receiver and is given by the function

$$s(n) = H(\mathbf{x}(n), m(n)), \tag{2}$$

or by the dynamical system

$$s(n + 1) = H(\mathbf{x}(n), m(n), s(n)). \tag{3}$$

In our analysis we assume that $s(n)$ is scalar, however in the more general case it can also be a vector of higher dimension. The signal $s(n)$ is received at the receiver which has a passive component $\mathbf{y}(n)$ governed by a subsystem which is identical to that of the transmitter passive component $\mathbf{x}(n)$:

$$\mathbf{y}(n + 1) = \mathbf{F}(\mathbf{y}(n), s(n)). \tag{4}$$

Since the largest conditional Lyapunov exponent of the dynamics which is driven by $s(n)$ is negative, the synchronization error between two systems that are driven by the same transmitted sequence $s(n)$ decays exponentially:

$$\begin{aligned} & |(\mathbf{y}(n)|s(0), \dots, s(n)) - (\mathbf{x}(n)|s(0), \dots, s(n))| \\ & \approx |\mathbf{y}(0) - \mathbf{x}(0)| \cdot e^{-|\lambda|n} \end{aligned} \tag{5}$$

We will now introduce some notations that will be used in derivations along this paper:

- $\mathbf{s}(n) = \{s(n), \dots, s(n - D_e + 1)\}$ is a D_e dimensional reconstruction of the transmitter phase space using D_e consecutive samples of the transmitted signal $s(n)$.
- \mathbf{s}_ε are samples of \mathbf{s} that are contained within a small D_e dimensional neighborhood ε of size L_ε . In this paper the neighborhood ε has the shape of a D_e dimensional hyper-cube of size L_ε however a sphere with radius L_ε or any other shape can be used.
- \mathbf{x}_ε is a sample \mathbf{x} preceded by a sequence \mathbf{s}_ε . Similar definition applies to \mathbf{y}_ε , s_ε and m_ε .
- $\langle s_\varepsilon \rangle$ is the average of the available samples of s that are preceded by \mathbf{s}_ε , so that $\langle s_\varepsilon \rangle = (1/N_\varepsilon) \sum_{i=1}^{N_\varepsilon} s_{i,\varepsilon}$ where $s_{i,\varepsilon}$ is the i th sample and N_ε is the total number of sequences \mathbf{s}_ε .

Using the above notations we can write Eq. (5) in a form that will be more useful for derivations along this paper:

$$|\mathbf{y}_\varepsilon - \mathbf{x}_\varepsilon| \approx |\mathbf{y}_* - \mathbf{x}_*| \cdot e^{-|\lambda|D_e} \quad (6)$$

where \mathbf{y}_ε and \mathbf{x}_ε are the states of the identical dynamical systems in Eqs. (1) and (4) after being driven by the same sequence \mathbf{s} for the last D_e iterations (according to our definition the subscript ε in \mathbf{y}_ε and \mathbf{x}_ε implies that both are preceded by sequences \mathbf{s} that are within the same small neighborhood ε). \mathbf{y}_* and \mathbf{x}_* are the states before the common sequence \mathbf{s} began driving both systems. \mathbf{y}_* and \mathbf{x}_* are assumed to be distributed randomly in the volume of the attractor. Driving both dynamical systems with the same sequence \mathbf{s} results in the exponential convergence of the states \mathbf{x} and \mathbf{y} towards each other.

Equation (6) has an important corollary that will be proven later: The uncertainty in forecasting the dynamics using delays of the transmitted signal s decays exponentially with the embedding phase space dimension D_e and the conditional Lyapunov exponent λ .

1.2. Average dynamics reconstruction cryptanalysis

There are many methods to attack chaotic encryption schemes [Yang *et al.*, 1998a; Yang *et al.*, 1998b; Geddes *et al.*, 1999; Yang *et al.*, 1998c; Yang *et al.*, 1998d]. Proving that an encryption scheme is robust against one type of attack does not guaran-

tee security. Many encryption schemes have been repeatedly broken and reinforced. For many encryption schemes specific attack methods have been developed, which quite often rely on some knowledge of the secret dynamical system which enables reduction of the complexity of the dynamics reconstruction by parameterizing the dynamics. Further, knowledge of the type of the transmitted data can make the task of breaking the encryption scheme easier. For instance, in the case of binary transmission, it is not necessary to reconstruct the exact waveform of the modulated signal. Clustering some property of the transmitted data (such as residual prediction error, spectral content, etc.) may enable message decoding. We assume in this paper that the unauthorized receiver does not have a simple parameterization model of the chaotic dynamics. Further, we assume that the message can take continuous values, and that consecutive message samples are statistically independent. This will ensure that a decoding of a message will not be enabled using simple clustering of some feature of the observed data as was done in the case of binary transmission in [Yang *et al.*, 1998a]. Therefore we assume that an unauthorized receiver will need to use some general method in order to decode the message.

A general method for attacking a chaotic encryption scheme which does not rely on the knowledge of the parametric model of the secret chaotic dynamics or the transmitted message is described in [Short, 1994; Short & Parker, 1998; Short, 1996]. The method is based on calculating the average dynamics using time delay embedding reconstruction of the high dimensional phase space within a small neighborhood ε .

For simplicity of our analysis we assume that the message \mathbf{m} is added to the transmitted signal, so that Eq. (2) is given by

$$s(n) = H(\mathbf{x}(n)) + m(n). \quad (7)$$

This assumption will also be valid for the broad class of modulation schemes where the message is small enough, so that Eq. (7) can be obtained by linearization of Eq. (2).

We will now formulate the reconstruction of the dynamics in an embedding phase space that is created from a sequence of delays of the transmitted signal s .

Equation (7) is valid for any $\mathbf{x}(n)$, therefore it is also valid when $\mathbf{x}(n)$, $s(n)$ and $m(n)$ are preceded

by a driving sequence $\mathbf{s}(n-1) = \{s(n-1), \dots, s(n-D_e)\}$:

$$s_\varepsilon(n) = H(\mathbf{x}_\varepsilon(n)) + m_\varepsilon(n). \quad (8)$$

Equation (8) is in fact Eq. (7) for the instances in which the preceding sequence of transmitted signal, $\mathbf{s}(n-1) = \{s(n-1), \dots, s(n-D_e)\}$, is contained in a small neighborhood of size L_ε in the D_e dimensional embedding phase space \mathbf{s} where the dynamics is assumed to be approximately constant.

From Eq. (8) we use the expectation of the transmitted signal $s_\varepsilon(n)$ as an estimation P_ε for the dynamics $H(\mathbf{x}_\varepsilon(n))$.

$$\begin{aligned} P_\varepsilon &\equiv E\{H(\mathbf{x}_\varepsilon)\} \\ &= E\{s_\varepsilon\} - E\{m_\varepsilon\} \end{aligned} \quad (9)$$

P_ε is the prediction of the average chaotic dynamics within a neighborhood of size L_ε . We assume that the average of the message m is 0 and the message $m(n)$ is independent of $\mathbf{s}(n-1)$, so that $E\{m_\varepsilon\} = 0$, and Eq. (9) becomes

$$P_\varepsilon = E\{s_\varepsilon\} \quad (10)$$

Given a finite number of samples, we can estimate P_ε by

$$P_\varepsilon \approx \hat{P}_\varepsilon = \langle s_\varepsilon \rangle \quad (11)$$

which is the average of all samples s preceded by the driving sequence \mathbf{s}_ε .

From Eqs. (8) and (11) the unauthorized receiver can estimate the message by

$$\hat{m}_\varepsilon(n) = s_\varepsilon(n) - \hat{P}_\varepsilon \quad (12)$$

2. Factors Affecting Security of Chaotic Encryption

The two main factors that determine the level of security are the amount of data available and the amount of computation required in order to decode a secret message. In the case of secret key encryption both the amount of available data and the amount of computation required are to be considered. In the case of public key encryption schemes [van Tilborg, 2000] the amount of computation required to break an encryption scheme is the only factor to be considered, since from information theoretic perspective, both authorized and unauthorized receiver share the same amount of information about the secret message and the only advantage of the authorized receiver over the unauthorized receiver is the amount of computation that is required

in order to decode the message. In this paper we analyze active/passive decomposition schemes which belong to the category of secret key encryption, and we assume that the unauthorized receiver has infinite computational resources, which implies that the only factor that determines the level of security is the amount of available information about the secret chaotic dynamics. Shannon introduced [1949] the measures of key and message equivocation which evaluate, from information theoretic point of view, the amount of uncertainty about the secret key and the secret message given a certain amount of information contained within the ciphertext. While the cryptanalysis of conventional encryption schemes that are based on integer number fields with respect to the amount of available data has been thoroughly studied for several decades, it nearly does not exist in the case of chaotic encryption schemes that are defined over continuous vector fields. In this paper we present such an analysis, but first we need to define how to quantify the amount of available data, and how to measure the level of security assuming that an unauthorized receiver has a fixed amount of available data.

Quantifying the extent to which an encryption scheme has been broken

A qualitative definition of the breaking of an encryption scheme would be the ability to decode the secret message with accuracy that may compromise it. In the case of chaotic encryption schemes, the transmitted message is typically an analog signal that may represent pure analog data such as voice or video waveforms, or the waveform of modulated digital data. Therefore we need to use a continuous measure for the extent to which an encryption scheme has been broken, and that measure should be application dependent.

A good measure which we use in this paper, is the message reconstruction rms error. The allowed reconstruction error depends on the application and the type of transmitted data. For instance, in the case of the transmission of voice or video analog signals, the allowed error is the amount of reconstruction noise which determines the intelligibility and visibility of the speech or video image, respectively. In the case where the transmitted analog signal is a modulated digital signal, security is maintained by ensuring a high level of reconstruction noise encountered by the unauthorized receiver, that will keep its decoding bit error rate (BER) above a defined threshold.

Quantifying the amount of available data

Various measures for the amount of available data are possible. For instance, from the information theoretic point of view, one may choose to use the amount of information (in bits) in the ciphertext. Information theoretic quantities are appealing candidate estimators for the amount of the available data since they also account for the redundancy of information that might be contained within several data samples, however from a practical point of view those quantities are difficult to evaluate. In this paper we measure the amount of available data by the number of available samples. The advantage in doing so is the relatively simple expressions that can be derived, that relate the number of available samples to the reconstruction accuracy through certain properties of the chaotic dynamical encryption scheme.

Quantifying the security of a chaotic encryption scheme

Since we quantify the extent to which an encryption scheme has been broken using the rms error of reconstructed message, and the amount of available data by the number of available samples, we quantify the security of a chaotic encryption scheme system as the rms error of message reconstruction as a function of the number of available samples. In the following sections we will use the above definition to quantify the security of encryption schemes based on active/passive decomposition of chaotic dynamics.

2.1. Volume and samples density within attractor

We will analyze the security of active/passive encryption scheme against an attack which is based on reconstruction of the average dynamics of the encryption scheme described in Sec. 1.2.

We assume that the dynamics is reconstructed within a neighborhood with the shape of a hypercube and size L_ε . The neighborhood has volume:

$$V_\varepsilon = L_\varepsilon^{D_e}. \quad (13)$$

The size of the cube affects the accuracy of reconstruction. Smaller cube size will result in smaller variations of the dynamics within the cube, and as a consequence the approximation of the dynamics within the hypercube will be more accurate.

Another factor that determines the accuracy of the dynamics reconstruction is the number of

samples within each neighborhood. The larger the number of available samples, the more accurate the dynamics reconstruction is. The number of samples, N_ε , required within a cube neighborhood of size L_ε determines the samples density ρ within the embedding phase space:

$$\rho = \frac{N_\varepsilon}{V_\varepsilon} = \frac{N_\varepsilon}{L_\varepsilon^{D_e}}. \quad (14)$$

The samples density may vary in different locations in the embedding phase space \mathbf{s} , therefore $\rho = \rho(\mathbf{s})$.

The number samples, N , required to reconstruct the dynamics in the entire volume is:

$$N = \int_{\mathbf{s}} \rho(\mathbf{s}) \cdot d\mathbf{s} = \sum_i N_{\varepsilon_i} \quad (15)$$

where the continuous volume of the phase space \mathbf{s} is fully covered with nonoverlapping small neighborhoods ε_i where the i th neighborhood ε_i contains N_{ε_i} samples.

Given a finite number of samples N there is a tradeoff between the size of a neighborhood L_ε and the embedding dimension D_e . Using smaller neighborhood L_ε or larger embedding dimension D_e , will increase the accuracy of reconstruction in case we have an infinite number of samples N , however since we have a finite number of samples, the number of samples within a small neighborhood N_ε will decrease and so will the accuracy of reconstruction. We will now establish the dependency of the accuracy of reconstruction on the embedding dimension, D_e and number of samples within the neighborhood N_ε .

2.2. Dimensions of message and chaotic dynamics

The transmitted signal $s(n)$ results from a combination of two signal sources: the chaotic signal $\mathbf{x}(n)$, and the message signal $m(n)$. If the message samples $m(n)$ are statistically independent then the message dimension is infinite. If the transmitted signal $s(n)$ is generated by adding the transmitted message to the dynamics, i.e. $s(n) = x(n) + m(n)$, and the chaotic signal $x(n)$ and the transmitted message $m(n)$ are statistically independent of each other, the required embedding dimension D_e would be infinite. It implies that no matter how large the embedding dimension D_e it will never be enough to enable full predictability of the combined chaotic and message systems. However, as we will show in the next section, even though the message cannot be

accurately reconstructed, given enough data points it can be reconstructed with a finite reconstruction rms error, that can be made small enough to compromise the secret message.

3. Dynamics Reconstruction Errors

From Eqs. (8) and (12) the error in estimating the message using the average dynamics is

$$e_\epsilon = m_\epsilon - \hat{m}_\epsilon = H(\mathbf{x}_\epsilon) - \hat{P}_\epsilon \tag{16}$$

The estimation error is comprised of several components: An error due to the use of an embedding phase space of finite dimension, an error due to the use of finite number of samples, and an error due to the assumption that the dynamics remains constant within a neighborhood of size L_ϵ . We will now discuss and estimate each of the error components.

3.1. Error due to finite embedding dimension

Even with an infinite number of samples there will be an error, e_1 if one uses a reconstructed embedding phase space of finite dimension. From Eq. (11), given an infinite number of samples, the estimator \hat{P}_ϵ approaches the minimum mean square error predictor P :

$$\hat{P}_\epsilon = \lim_{N_\epsilon \rightarrow \infty} \langle s_\epsilon \rangle = E\{s_\epsilon\} = P_\epsilon \tag{17}$$

Substituting Eq. (17) into Eq. (16) we can calculate the message reconstruction error,

$$\begin{aligned} e_1 &= H(\mathbf{x}_\epsilon) - \hat{P}_\epsilon \\ &= H(\mathbf{x}_\epsilon) - E\{s_\epsilon\} \end{aligned} \tag{18}$$

Since we assume that the number of available samples is infinite, we can choose the neighborhood size L_ϵ to be small enough so that the error due to variations of the dynamics within the neighborhood is negligible. In this case, the error is due to the use of finite embedding dimension D_e . From Eq. (16) the reconstruction error is 0 if the unauthorized receiver can find a predictor \hat{P}_ϵ such that $\hat{P}_\epsilon = H(\mathbf{x}_\epsilon)$. However, since the unauthorized receiver does not know the state \mathbf{x} , then $H(\mathbf{x}_\epsilon)$ is **not** uniquely determined by the sequence \mathbf{s} , and no estimator \hat{P}_ϵ that is equal to $H(\mathbf{x}_\epsilon)$ can be found. This error exists when the unauthorized receiver uses a finite embedding dimension D_e for the reconstructed embedding phase space, even if an infinite number of

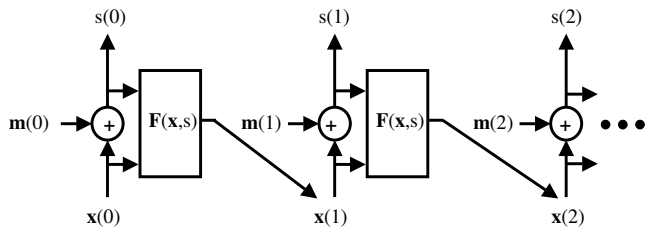


Fig. 2. The evolution along time of the transmitter dynamics given by Eq. (2). Knowledge of the sequence $\mathbf{s}(n - 1) = \{s(n - 1), \dots, s(n - D_e)\}$ does not enable the unauthorized receiver to uniquely determine the value of the next state $\mathbf{x}(n)$, even if it accurately knows the secret transmitter dynamics $F(\bullet)$.

samples N_s are available to reconstruct the dynamics. This phenomenon is illustrated in Fig. 2 where the evolution of the transmitter dynamics is given along time. It is evident from Fig. 2 that knowledge of the sequence \mathbf{s} does not enable the unauthorized receiver to uniquely determine the value of the next state \mathbf{x} , even if it accurately knows the secret transmitter dynamics given in Eqs. (2) and (3). This is due to the fact that the sequence \mathbf{s} can be obtained using many combinations of message sequences m and chaotic dynamics sequences \mathbf{x} . It is impossible to deduce from the sequence $s(n)$ what are the two sequences $\mathbf{x}(n)$ and $m(n)$ that generated it, assuming that the message samples $\mathbf{m}(n)$ are statistically independent. Not being able to accurately predict $\mathbf{x}(n)$ based on previously transmitted samples $\mathbf{s}(n - 1) = \{s(n - 1), \dots, s(n - D_e)\}$, the unauthorized receiver is unable to uniquely determine the transmitted message $m(n)$ using the estimator in Eq. (12)

We will now estimate the message reconstruction error, e_1 , caused by the inability to uniquely determine $H(\mathbf{x}_\epsilon)$ using a predictor \hat{P}_ϵ which relies only on the knowledge of the sequence $\mathbf{s}(n - 1) = \{s(n - 1), \dots, s(n - D_e)\}$, while not knowing the state $\mathbf{x}(n)$. We will first write the predictor \hat{P}_ϵ defined in Eq. (9) in the following form:

$$\hat{P}_\epsilon = E\{s_\epsilon\} = E_{\mathbf{z}_\epsilon}\{H(\mathbf{z}_\epsilon)\} \tag{19}$$

where \mathbf{z} is another notation for the transmitter state \mathbf{x} used for calculating the expectation.

Substituting Eq. (19) into Eq. (18) we obtain

$$\begin{aligned} e_1 &= H(\mathbf{x}_\epsilon) - E_{\mathbf{z}_\epsilon}\{H(\mathbf{z}_\epsilon)\} \\ &= E_{\mathbf{z}_\epsilon}\{H(\mathbf{x}_\epsilon) - H(\mathbf{z}_\epsilon)\} \end{aligned} \tag{20}$$

From Eq. (6) the difference $|\mathbf{x}_\epsilon - \mathbf{z}_\epsilon|$ decreases exponentially with the embedding dimension. This

implies that the uncertainty in predicting the state \mathbf{x} based on previous D_e samples of the transmitted signal s decreases exponentially with the increase in the number of samples D_e . For large enough D_e the difference $|\mathbf{x}_\varepsilon - \mathbf{z}_\varepsilon|$ will be small so we can linearize Eq. (20) to obtain

$$\begin{aligned} e_1 &= E_{\mathbf{z}_\varepsilon} \{ \nabla_{\mathbf{x}_\varepsilon} H \cdot (\mathbf{x}_\varepsilon - \mathbf{z}_\varepsilon) \} \\ &= \nabla_{\mathbf{x}_\varepsilon} H \cdot E_{\mathbf{z}_\varepsilon} \{ (\mathbf{x}_\varepsilon - \mathbf{z}_\varepsilon) \}, \end{aligned} \quad (21)$$

and the absolute value of the error e_1 is bounded by

$$\begin{aligned} |e_1| &\leq |\nabla_{\mathbf{x}_\varepsilon} H| \cdot |E_{\mathbf{z}_\varepsilon} \{ (\mathbf{x}_\varepsilon - \mathbf{z}_\varepsilon) \}| \\ &\leq |\nabla_{\mathbf{x}_\varepsilon} H| \cdot E_{\mathbf{z}_\varepsilon} \{ |\mathbf{x}_\varepsilon - \mathbf{z}_\varepsilon| \} \end{aligned} \quad (22)$$

Substituting Eq. (6) into Eq. (22) we obtain

$$|e_1| \leq |\nabla_{\mathbf{x}_\varepsilon} H| \cdot E_{\mathbf{z}_*} \{ |\mathbf{x}_* - \mathbf{z}_*| \} \cdot e^{-|\lambda|D_e} \quad (23)$$

The above error e_1 is for one sample of \mathbf{x}_* which corresponds to the forecasting error of a single sample. The mean square error can be obtained by averaging square of the error term in Eq. (23) over all samples \mathbf{x}_* :

$$E\{e_1^2\} = E_{\mathbf{x}_*} \{ |e_1|^2 \} \quad (24)$$

We define a scalar c as

$$c = E_{\mathbf{x}_*} \{ |\nabla_{\mathbf{x}_\varepsilon} H| \cdot E_{\mathbf{z}_*} \{ |\mathbf{x}_* - \mathbf{z}_*| \} \} \quad (25)$$

and now we can write Eq. (24) as

$$E\{e_1^2\} \leq c^2 \cdot e^{-2|\lambda|D_e} \quad (26)$$

It is evident from Eq. (26) that even if the unauthorized receiver is given an infinite amount of samples, and uses neighborhood size L_ε small enough to ensure that variations of the predictor P_ε within the neighborhood are negligible, the use of an embedding phase space with a finite dimension will result in an error that decays exponentially with the embedding dimension D_e and with the conditional Lyapunov exponent λ . As we will demonstrate in our simulation, this result can be used to enhance the security of the encryption scheme by using small $|\lambda|$. Even though the choice of small $|\lambda|$ results in slower synchronization between transmitter and receiver, it forces the unauthorized receiver to use large embedding dimension D_e which in turn results in smaller number of samples available within a small neighborhood of the reconstructed embedding phase space \mathbf{s} for estimation of the average of the dynamics.

3.2. Error due to the finite number of samples

The cause of the error discussed in Sec. 3.1 is the use of finite dimension D_e for the embedding phase space \mathbf{s} . The number of samples available for estimation of the average dynamics was assumed to be infinite, and therefore the estimator \hat{P}_ε of the average dynamics within a small neighborhood is the exact average (expectation) of the dynamics at the point \mathbf{s} and therefore was the minimum mean square error estimator P_ε . However, there is also an error due to the use of a finite number of available samples for the reconstruction of the average dynamics. If more samples are available the more accurate the reconstruction will be. The relation between the number of available samples and the accuracy of reconstruction is a crucial factor in estimating the security of the system, since it determines the amount of data that can be transmitted before the encryption scheme security is jeopardized.

Using the estimator given in Eq. (11), which makes use of a finite number of samples, will result in an estimator which is different from the Minimum Mean Square Error (MSE) estimator given in Eq. (17). This, in turn, will result in a message decoding error, e_2 , caused by the use of a finite number of samples is given by

$$\begin{aligned} e_2 &= \hat{P}_\varepsilon - P_\varepsilon \\ &= \hat{P}_\varepsilon - E\{s_\varepsilon\} \end{aligned} \quad (27)$$

By substituting \hat{P}_ε from Eq. (11) into Eq. (27) we obtain

$$e_2 = \langle H(\mathbf{x}_\varepsilon) + m_\varepsilon \rangle - E_\varepsilon\{s\} \quad (28)$$

Substituting Eq. (19) into Eq. (28) we obtain

$$\begin{aligned} e_2 &= \langle H(\mathbf{x}_\varepsilon) \rangle - E_{\mathbf{z}_\varepsilon} \{ H(\mathbf{z}_\varepsilon) \} + \langle m_\varepsilon \rangle \\ &= \langle E_{\mathbf{z}_\varepsilon} \{ H(\mathbf{x}_\varepsilon) - H(\mathbf{z}_\varepsilon) \} \rangle + \langle m_\varepsilon \rangle \end{aligned} \quad (29)$$

The first term, $\langle E_{\mathbf{z}_\varepsilon} \{ H(\mathbf{x}_\varepsilon) - H(\mathbf{z}_\varepsilon) \} \rangle$, in Eq. (29) is similar to the term $E_{\mathbf{z}_\varepsilon} \{ H(\mathbf{x}_\varepsilon) - H(\mathbf{z}_\varepsilon) \}$ in Eq. (20) only this time it is averaged over N_ε samples within the neighborhood ε . Following the derivations in Eqs. (20)–(26) the error due to this term is $(1/N_\varepsilon)c^2 \cdot e^{-2|\lambda|D_e}$.

In order to calculate the contribution of the second term, $\langle m_\varepsilon \rangle$, in Eq. (29) to the variance of the mean square error we assume that the transmitter message has zero mean ($E\{m_\varepsilon\} = 0$) and variance therefore the contribution of the second term would

be $E\{m_\varepsilon^2\} = (1/N_\varepsilon)\sigma_m^2$. Since the first term in Eq. (29) is statistically independent of the second term, the contribution of the first and the second terms can be added to the variance of e_2 to obtain

$$E\{e_2^2\} \leq \frac{1}{N_\varepsilon} \cdot c^2 \cdot e^{-2|\lambda|D_e} + \frac{1}{N_\varepsilon} \cdot \sigma_m^2. \quad (30)$$

Equation (30) shows that there are two sources of error due to the finite number of samples. The first is the use of finite dimension D_e for the reconstructed embedding phase space. This error is similar to the error discussed in Eq. (26), however this time the error is averaged over N_ε samples and therefore is multiplied by a factor $1/N_\varepsilon$. The second source of error is the variance, σ_m^2 , of the transmitted message m . From the point of view of the unauthorized receiver who attempts to reconstruct the average dynamics in the embedding phase space, the message m appears as noise that perturbs the original dynamics, and the unauthorized receiver will need more samples in order to average out the perturbation to the dynamics caused by the message and accurately estimate the chaotic dynamics. As a consequence, from the point of view of the authorized parties, a message m with large variance can be used as an efficient tool to perturb the secret dynamics and enhance security of the encryption scheme.

3.3. Error due to finite neighborhood size

We assume that since the unauthorized receiver does not know the general type of the chaotic dynamics he will need to use local model approximation of the local dynamics within a neighborhood of finite size. In [Farmer & Sidorowich, 1987] the authors estimated the approximation mean square error $E\{e_3^2\}$ by

$$E\{e_3^2\} = k' e^{2(p+1)\lambda_{\max}^+ T} r^{2(p+1)} \quad (31)$$

where k' is a constant, r is the average distance between two nearest neighbors, p is the order of the approximation, λ_{\max}^+ is the largest positive Lyapunov exponent, and T is the prediction time interval between the current sample and the future sample. In their paper, Farmer and Sidorowich claim that first order approximation ($p = 1$) may be more accurate than a zero order one ($p = 0$), however there is no significant improvement in using higher order approximations which are also difficult

to perform in more than two dimensions. Also, using high order approximations may in fact degrade approximation accuracy using a finite number of samples N_s in a very noisy environment, since high order approximation requires the estimation of a large number of coefficients.

In this paper we use a zero order approximation for the local dynamics so that $p = 0$ in Eq. (31). From the point of view of the unauthorized receiver, the message m is a large noise that perturbs the chaotic dynamics so he needs to represent the local dynamics by its average [Eq. (11)]. Since the local neighborhoods in our analysis are hypercubes of size L_ε then the accuracy of interpolation using a polynomial of degree p depends on the hypercube size L_ε . This dependency is similar to the dependency of the interpolation error in Eq. (31) on the interpolation distance r so we estimate the interpolation error assuming that $r \propto L_\varepsilon$. The unauthorized receiver generates a model that attempts to predict the next sample using previous D_e samples, so that $T = 1$ in Eq. (31). Substituting $p = 0$, $T = 1$ and $r = L_\varepsilon$ into Eq. (31) we obtain

$$E\{e_3^2\} \approx k L_\varepsilon^2 \quad (32)$$

where $k = k' e^{2\lambda_{\max}^+}$

3.4. Total error

The total error is the sum of errors described in the previous subsections: e_1 — the error due to finite embedding state dimension (assuming infinite samples), e_2 — the error due to the use of a finite number of samples, and e_3 — the error due to the use of finite neighborhood size L_ε . We obtain an approximation of the total error by assuming that the errors e_1 , e_2 , e_3 are statistically independent, and therefore the mean square of the total error is

$$\begin{aligned} E\{e^2\} &= E\{e_1^2\} + E\{e_2^2\} + E\{e_3^2\} \\ &= c^2 \cdot e^{-2|\lambda|D_e} + \frac{1}{N_\varepsilon} \cdot c^2 \cdot e^{-2|\lambda|D_e} \\ &\quad + \frac{1}{N_\varepsilon} \cdot \sigma_m^2 + k L_\varepsilon^2 \end{aligned} \quad (33)$$

There are four components to the error given in Eq. (33): The first term, $c^2 \cdot e^{-2|\lambda|D_e}$ was derived in Eq. (26) and is due to the difference between the actual value of $H(\mathbf{x}|\mathbf{s})$ and its predicted expectation, P_ε , given in Eq. (9). Note, as mentioned in Sec. 3.1, since the unauthorized receiver can observe only the transmitted active component \mathbf{s} and does not know the value of the transmitter state \mathbf{x} , then from his

point of view the quantity $H(\mathbf{x}|\mathbf{s})$ is a random variable with mean P_ε and variance $c^2 \cdot e^{-2|\lambda|D_e}$ around its average.

The second error component, $1/N_\varepsilon \cdot c^2 \cdot e^{-2|\lambda|D_e}$, [which is the first component of the error e_2 in Eq. (30)], results from the fact that we approximate the average dynamics $P(\mathbf{s}) \equiv E\{H(\mathbf{x}|\mathbf{s})\}$ by the estimator $\hat{P}(\mathbf{s})$ given in Eq. (11) which utilizes a finite number of samples N_ε that are available within the neighborhood ε of \mathbf{s} . We assume that $N_\varepsilon \gg 1$ and therefore the second term is small compared to the first term, and can be ignored.

The third term, $1/N_\varepsilon \cdot \sigma_m^2$ is the error in estimating $P(\mathbf{s})$ which results from perturbations to the dynamics caused by the message m . Those perturbations are not completely averaged out in case the unauthorized receiver uses a finite number of samples N_ε that are available within the neighborhood of \mathbf{s} while calculating $\hat{P}(\mathbf{s})$.

As mentioned before, the fourth term, kL_ε^2 , is the error due to the assumption that the dynamics remains constant within a neighborhood of finite size L_ε .

Assuming that the number of available samples is large we may write

$$E\{e^2\} \approx c^2 \cdot e^{-2|\lambda|D_e} + \frac{1}{N_\varepsilon} \cdot \sigma_m^2 + kL_\varepsilon^2 \quad (34)$$

3.5. Reconstruction of the dynamics within a given accuracy

We can now use Eq. (34) in order to quantify the level of security based on Sec. 2 where security is defined by the number of samples that is required in order to reconstruct the message with a given accuracy. For an encryption scheme to be secure, we require that the message reconstruction error will exceed a maximum value, e_{\max}^2 . The number of samples N_ε is then given by

$$N_\varepsilon \leq \frac{\sigma_m^2}{e_{\max}^2 - kL_\varepsilon^2 - c^2 \cdot e^{-2|\lambda|D_e}} \quad (35)$$

under the constraint

$$e_{\max}^2 - kL_\varepsilon^2 - c^2 \cdot e^{-2|\lambda|D_e} > 0, \quad (36)$$

or equivalently

$$D_e \geq D_{\min} = -\frac{1}{2|\lambda|} \cdot \ln\left(\frac{e_{\max}^2 - kL_\varepsilon^2}{c^2}\right) \quad (37)$$

From the point of view of the unauthorized receiver, the above constraint implies that the

embedding dimension, D_e has to be large enough, so that the error caused by the use of finite embedding dimension (described in Sec. 3.1) will not exceed the maximum allowed error e_{\max}^2 . If this constraint is not met, even the use of an infinite number of samples N_ε will not result in a message reconstruction error that is lower than e_{\max}^2 .

3.6. Message component in transmitted signal is larger than chaotic component

By assumption the transmitted signal s is the sum of $H(\mathbf{x})$ and the message m [see Eq. (7)]. An important factor to consider in our cryptanalysis is the magnitude of the transmitted message m relative to the magnitude of the chaotic signal $H(\mathbf{x})$. If the transmitted message is larger than the chaotic component, i.e. $|m| \gg |H(\mathbf{x})|$, then the distribution of the transmitted signal s will be similar to that of the message m . By choosing message samples m statistically independent and identically distributed random variables with uniform distribution of span L_m , the trajectory in the reconstructed embedding phase space \mathbf{s} will be confined within a hypercube of dimension D_e and of size L_m . The volume of the reconstructed attractor is

$$V_s = (L_m)^{D_e} \quad (38)$$

and the number of samples N_ε within a neighborhood with a hypercube shape of size L_ε is given by

$$N_\varepsilon = N_s \left(\frac{L_\varepsilon}{L_m}\right)^{D_e} \quad (39)$$

By substituting Eq. (39) into Eq. (34) we obtain

$$E\{e^2\} = c^2 \cdot e^{-2|\lambda|D_e} + \frac{\sigma_m^2}{N_s} \cdot \left(\frac{L_m}{L_\varepsilon}\right)^{D_e} + kL_\varepsilon^2 \quad (40)$$

From the first term of Eq. (40), use of larger embedding dimension D_e results in smaller error due to the use of finite embedding dimension. However from the second term of Eq. (40), larger D_e results in smaller number of samples N_ε available for estimating the local dynamics. Also, from the second term, use of small neighborhood size L_ε will result in small number of samples available for estimating the local dynamics, yet the use of large L_ε will result in approximation error due to the third term in Eq. (40). As a consequence, there exist optimal values D_e^{opt} and $L_\varepsilon^{\text{opt}}$ for the embedding dimension and

the local neighborhood size respectively. It is possible to calculate those values by solving the following set of equations

$$\frac{\partial e_{\max}^2}{\partial D_e} = 0, \quad \frac{\partial e_{\max}^2}{\partial L_\varepsilon} = 0 \quad (41)$$

In practice though, the error in Eq. (40) is based on numerous assumptions and approximations, therefore it is better to obtain the optimal values through simulation, as we will show in Sec. 5.

Another interesting consequence of Eq. (40) is that the number of samples N_s required in order to maintain an error below a maximal value e_{\max}^2 can be approximated by

$$N_s = \frac{\sigma_m^2}{e_{\max}^2 - kL_\varepsilon^2 - c^2 \cdot e^{-2|\lambda|D_e}} \cdot \left(\frac{L_m}{L_\varepsilon}\right)^{D_e} \quad (42)$$

From the point of view of the authorized receiver, N_s in Eq. (42) is the number of samples that can be securely transmitted before the unauthorized can decode the message with a reconstruction error that is smaller than e_{\max}^2 .

3.7. Message component in transmitted signal is smaller than dynamics component

From Eq. (7) the contribution of the message, m , to the transmitted signal s is smaller than the contribution of the chaotic signal \mathbf{x} if $|m| \ll |H(\mathbf{x})|$. If the message samples m are i.i.d. random variables with uniform distribution of span L_m , then increasing the message span from 0 to L_m will cause the attractor's volume an expansion of size L_m in all D_e directions of the D_e dimensional reconstructed embedding phase space. The volume of the attractor in the D_e dimensional reconstructed embedding phase space is given by

$$V_s = V_a(L_m) \cdot L_m^{D_e - D_a} \quad (43)$$

where $V_a(L_m)$ is the volume component which depends on the topology of the D_a dimensional chaotic attractor of the chaotic dynamics, and $L_m^{D_e - D_a}$ is the inflation in $D_e - D_a$ directions which are orthogonal to the attractor D_a dimensional shape.

Once the message dynamic range L_m becomes larger than the dynamic range of the chaotic attractor, then $V_a(L_m) \rightarrow L_m^{D_a}$, and the volume V_s in Eq. (43) approaches the volume V_s in Eq. (38). As will be shown in our simulation, the inflation in the volume of the attractor in the reconstructed embedding phase space due to the increase in the message

dynamic range L_m will require the unauthorized receiver to use more samples to reconstruct the secret dynamics, and therefore is a useful tool to increase the security of the encryption scheme.

4. Choosing Modulation for Digital Data

The security of the encryption scheme relies on the accuracy of the reconstruction of the secret chaotic dynamics. Using fine grained randomly modulated message with large dynamical range will require the unauthorized receiver to reconstruct the perturbed chaotic attractor in a large volume due to the large

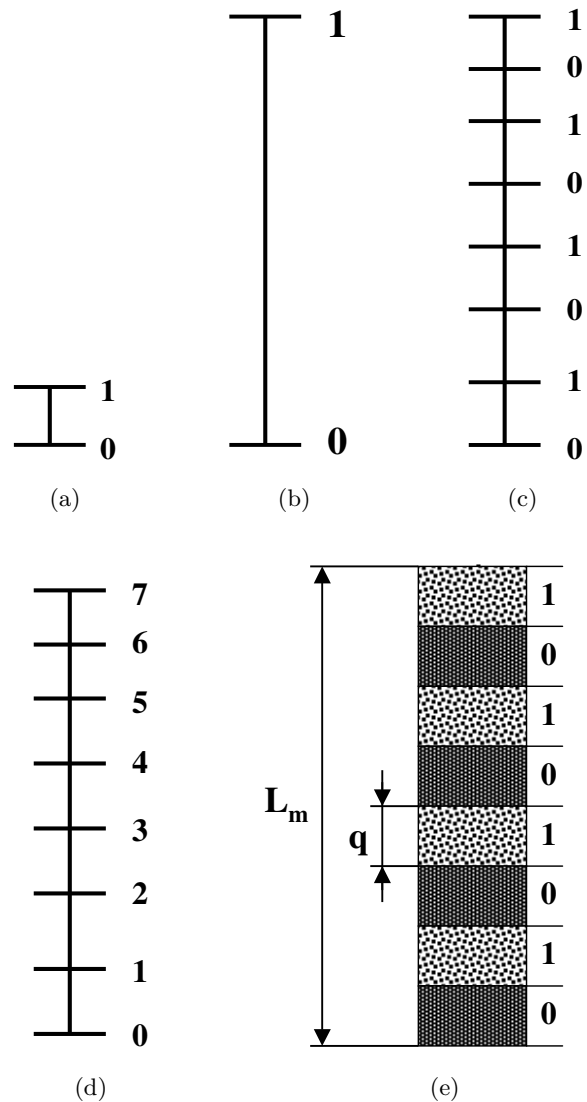


Fig. 3. Modulations with: (a) Small span, high sensitivity, low security. (b) Large span low sensitivity, low security. (c) Large span, high sensitivity, high security, low efficiency. (d) Large span, high sensitivity, medium security.

message dynamical range as implied by Eq. (38). Fine grained modulation which is sensitive to reconstruction errors will require high reconstruction accuracy. The need to reconstruct the dynamics with high accuracy in an embedding phase space of large volume requires the unauthorized receiver to use a larger number of samples N_s , which implies that the encryption scheme is more secure. Shown in Fig. 3 are several modulation schemes for transmitting digital data. In Fig. 3(a) the modulation is of a binary signal that can take the values “0” or “1”. This modulation has small dynamical range (amplitude) and high sensitivity to reconstruction inaccuracy, due to the small distance between the “0” and “1” amplitudes. In Fig. 3(b) the modulation has larger dynamical range yet low sensitivity to reconstruction error because of the larger distance between “0” and “1”. In order to maintain security we require the modulation scheme to have both a large dynamical range and high sensitivity to reconstruction error, as shown in the modulation in Fig. 3(c). Whenever we transmit “0” or “1” we choose randomly one of the possible values corresponding to “0” or “1” respectively. This modulation has both the large dynamical range of the modulation Fig. 3(b) and the high sensitivity to reconstruction error as modulation Fig. 3(a). Although the modulation in Fig. 3(c) is more secure than the modulation in Fig. 3(a), it is less efficient since more power is required to transmit the same number of bits. In order to avoid large transmitted power one can use Chaotic Frequency Modulation (CFM) [Volkovskii & Tsimring, 1999] or Chaotic Pulse Position Modulation (CPPM) [Rulkov *et al.*, 2001] that will trade the large transmitted power with large transmitted bandwidth (CFM), or with lower bit rate (CPPM). In Fig. 3(d) a modulation which has large dynamical range and high sensitivity to reconstruction error is shown. The modulation is more efficient than the modulation shown in Fig. 3(c) since each symbol can take values other than “0” or “1”, and therefore conveys more information bits. However, even though this modulation is as sensitive to reconstruction error as the modulation shown in Fig. 3(c) due to the small spacing between adjacent symbols, it is less secure since even though a large reconstruction error will result in a decoding error it may still reveal from which group of symbols the transmitted symbol was chosen from.

The security of modulations Figs. 3(a)–3(d) can be compromised since the modulated message can

take a finite number of discrete values. As we have shown in the previous section, the message perturbs the chaotic dynamics and makes the reconstruction of the chaotic dynamics more difficult. If the modulated message can take a finite number of values, the perturbation of the dynamics caused by the message will be less rich, and the encryption scheme security can be compromised. In order to transmit messages which can take continuous values we use the modulation shown in Fig. 3(e) where each transmitted bit does not take discrete values, but is chosen randomly from a finite interval. Also, the interval itself is chosen randomly, as in the modulation in Fig. 3(c). Choosing both the intervals and the value within the interval with equal probability, the modulated message no longer takes a finite number of possible values. It now has uniform and continuous distribution with large dynamical range, and high sensitivity to reconstruction error, and the encryption scheme is more secure than when we use the modulation shown in Fig. 3(c).

5. Simulation

In order to test our estimates for security, we simulated an active passive decomposition encryption scheme using a one-dimensional chaotic tent map. The transmitter evolution is governed by the chaotic map

$$\begin{aligned}x(n+1) &= \text{Tent}(s(n)) - b \cdot x(n) \\s(n) &= x(n) + m(n)\end{aligned}\quad (44)$$

where

$$\begin{aligned}\text{Tent}(x) &= \begin{cases} ax' - \frac{h}{2}, & \text{if } x' \leq \frac{w}{2} \\ \frac{3h}{2} - ax', & \text{if } x' > \frac{w}{2} \end{cases} \\w &= \frac{2h}{a} \\x' &= x \bmod(w)\end{aligned}\quad (45)$$

The parameter h is the height, a is the slope, and w is the width of the tent map. The parameter values used in this simulation are $h = 0.3$ and $a = 1.5$. Unless stated otherwise, $b = 0.5$. The receiver dynamics is

$$y(n+1) = \text{Tent}(s(n)) - b \cdot y(n) \quad (46)$$

The conditional Lyapunov exponent $|\lambda|$ [which is conditioned on the transmitted scalar $s(n)$] is given by $\lambda = \ln(b)$. The receiver state synchronizes to the

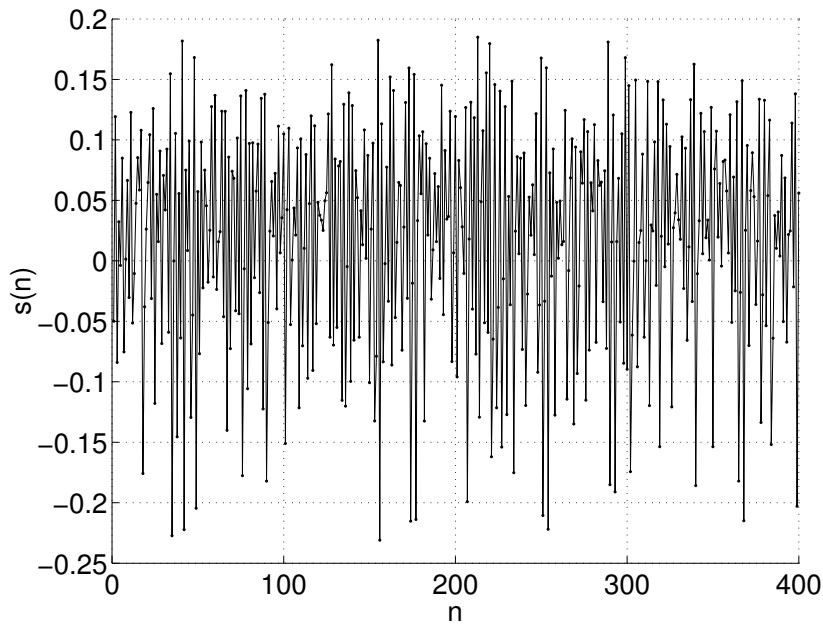


Fig. 4. Time series of transmitted chaotic active component $s(n)$.

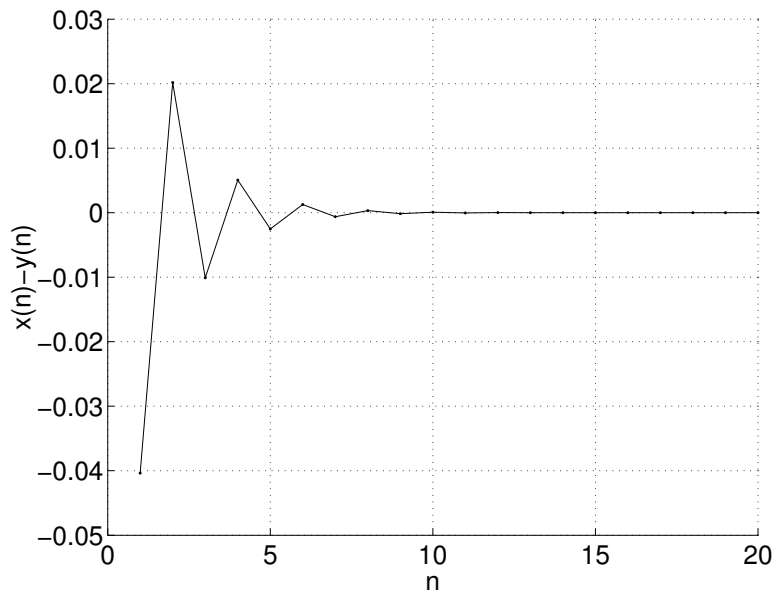


Fig. 5. Synchronization error between transmitter state $x(n)$ and receiver state $y(n)$ decays exponentially with the conditional Lyapunov exponent λ which is conditioned on the transmitted active component $s(n)$.

transmitter state at the rate of the conditional Lyapunov exponent: $|e(n)| = |e(0)| \cdot e^{\lambda n} = |e(0)| \cdot b^n$, and by choosing $|b| < 1$ we guarantee synchronization. In our simulation the message samples $m(n)$ are uniformly distributed, so

$$m \sim U \left[-\frac{L_m}{2}, \frac{L_m}{2} \right] \tag{47}$$

where L_m is the dynamic range of the message.

The message standard deviation σ_m^2 is therefore given by

$$\sigma_m^2 = \frac{L_m^2}{12} \tag{48}$$

In Fig. 4 a sample of the transmitted active signal $s(n)$ is shown. The synchronization error between the transmitter state $x(n)$ and the receiver state $y(n)$ decays exponentially at a rate characterized

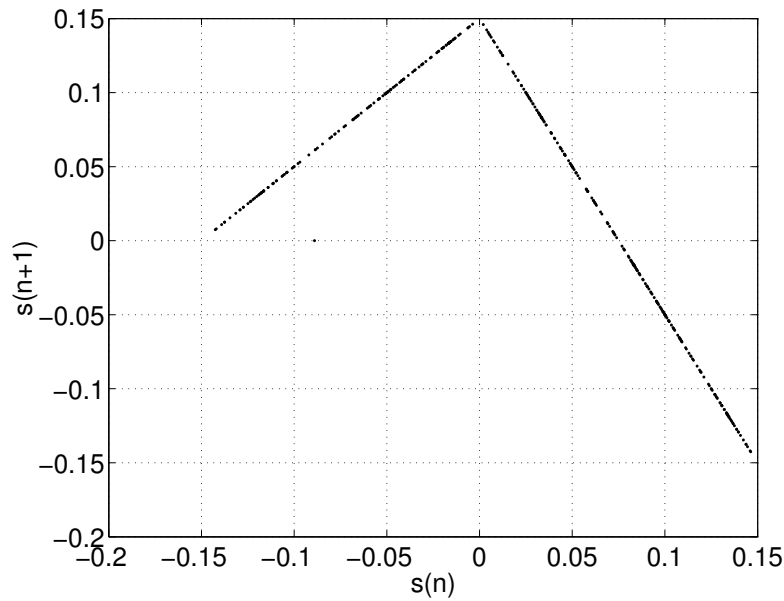


Fig. 6. Dynamics in a reconstructed embedding phase space generated using time delays of the transmitted sequence $s(n)$. No message added to the dynamics ($m(n) = 0$).

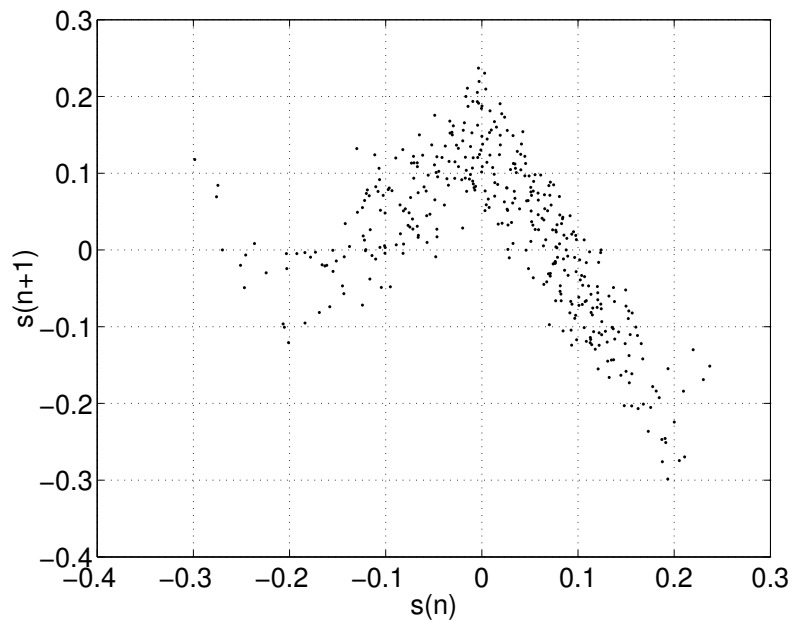


Fig. 7. Dynamics in a reconstructed embedding phase space generated using time delays of the transmitted sequence $s(n)$. Statistically independent and uniformly distributed message samples, $m(n)$, perturb the “clean” chaotic dynamics.

by the conditional Lyapunov exponent λ , as shown in Fig. 5.

A reconstruction of the dynamics using time delay embedding of the sequence $s(n)$, is shown in Fig. 6. No message was added to the dynamics ($m(n) = 0$). It is evident from Fig. 6 that even though the transmitted sequence $s(n)$ is chaotic in

the time domain, it is well defined in the reconstructed phase space, and the structure of the underlying tent map is revealed. In Fig. 7 a message was added to the chaotic dynamics of the transmitter. The message samples $m(n)$ are statistically independent and uniformly distributed. The clear shape of the dynamics observed in Fig. 6 is now

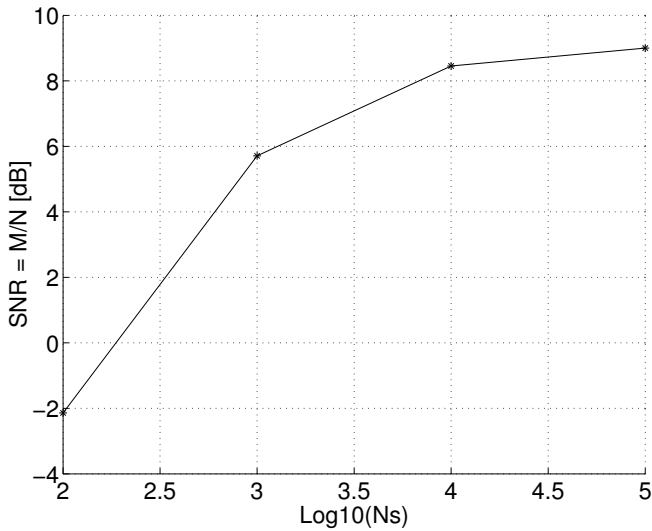


Fig. 8. Signal to noise ratio of reconstructed message ($\text{SNR} = M/N$) versus the number of samples available for reconstruction N_s . $D_e = 3$, $b = 0.5$.

perturbed by the additional message in Fig. 7, and the unauthorized receiver needs more samples in order to average out the perturbations to the dynamics caused by the message. Further, in the absence of a message signal $m(n)$ the transmitted signal $s(n+1)$ can be accurately predicted by the previous sample $s(n)$, while in the presence of a message, it can be predicted only with finite accuracy that increases exponentially with the conditional Lyapunov exponent λ and the embedding dimension D_e , as implied by the first term of Eq. (34). We now define the following quantities:

$$\begin{aligned} M &= 10 \text{Log}_{10}[\sigma_m^2] \\ N &= 10 \text{Log}_{10}[E\{e^2\}] \\ X &= 10 \text{Log}_{10}[E\{(H(\mathbf{x}))^2\}] \end{aligned} \quad (49)$$

The reconstruction signal to noise ratio M/N as a function of the number of samples N_s that are available for reconstruction is shown in Fig. 8. The reconstruction parameters used are $D_e = 3$ and $L_\varepsilon = 0.02$. Clearly, the reconstruction signal to noise ratio increases with the number of samples N_s that are available for reconstruction. However, the signal to noise ratio reaches an asymptotic value which is determined by the error caused by the use of finite embedding dimension D_e and neighborhood size L_ε . An increase in N_s enables an increase of the embedding dimension D_e and a decrease in the neighborhood size L_ε and the reconstruction error will approach zero as the number of samples N_s is increased to infinity, however we keep D_e and

L_ε constant in Fig. 8. The choice of optimal values for the embedding dimension D_e and the neighborhood size L_ε given a fixed number of samples N_s for dynamics reconstruction will be discussed next. In case we use a modulation of the kind shown in Fig. 3, the signal to noise ratio can be arbitrarily decreased by increasing the message dynamic range L_m , and security can be maintained by keeping small bin size L_ε . As a consequence, the signal to noise ratio is not a good measure for security since a randomly modulated message with large dynamical range may have large reconstruction signal to noise ratio, and yet the unauthorized receiver may not be able to decode the message if the modulation is fine grained and the reconstruction error exceeds its sensitivity to noise. In the analysis to follow, instead of using signal to noise ratio of the reconstructed message we will use the ‘‘cleaning factor’’ C defined by

$$C = \frac{X}{N}. \quad (50)$$

Since from the point of view of an unauthorized receiver the chaotic signal which is added to the message is an undesired kind of noise, the cleaning factor C measures the fraction of the chaotic signal (noise from the unauthorized receiver point of view) that has been cleaned from the message by using nonlinear dynamic forecasting. Unlike the message reconstruction signal to noise ratio M/N , the noise cleaning factor $C = X/N$ does not increase as the message mean square M increases, but as we will show it actually decreases, due to the decrease in reconstruction accuracy, and therefore is a better measure of the encryption scheme security.

Shown in Fig. 9 are the simulation and theoretic results for the chaotic signal cleaning factor C as a function of the reconstruction embedding dimension D_e , for various values of the parameter b that determines the conditional Lyapunov exponent $\lambda = \ln(b)$. The theoretic results were calculated using the error estimation in Eq. (40) with the following modifications: A constant offset, Δ , was added to the error. Also, in the simulation samples where no nearest neighbors found were discarded, then also in the theoretic error estimation, whenever the number of samples within a small neighborhood was less than one ($N_\varepsilon < 1$), we set $N_\varepsilon = 1$. This clamps the estimation error, so it cannot be larger than the chaotic signal X , and the cleaning factor C cannot be less than 0. The parameters used in simulation are $N_s = 25e6$, $M = -13\text{db}$, $L_\varepsilon = 0.02$.

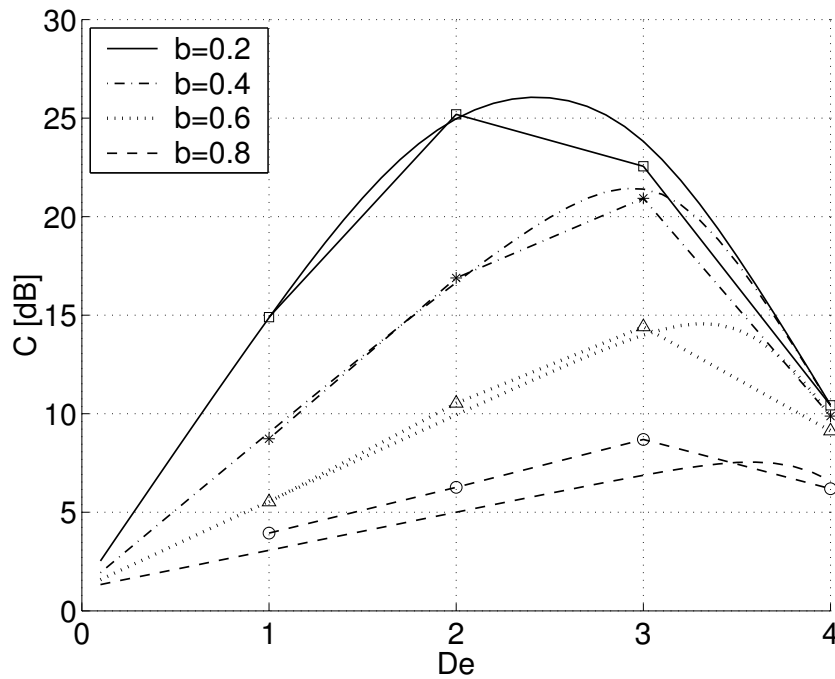


Fig. 9. Simulation (symbols) and theoretical values (lines) of chaotic signal cleaning C as a function of the reconstruction embedding dimension D_e for various values of parameter b which determines the conditional Lyapunov exponent $\lambda = \ln(b)$. Simulation parameters: $N_s = 2.5e7$, $M = -13$ dB, $L_\varepsilon = 0.02$. Theoretical estimation parameters: $c = 0.22$, $k = 0.3$, $\Delta = 9$ dB.

The estimation parameters were $c = 0.22$, $k = 0.3$ and $\Delta = 9$ dB.

Each graph which corresponds to a different value of the parameter b has an optimal value for the embedding dimension D_{opt} where the largest value of the cleaning factor C is obtained. Use of embedding dimension larger than D_{opt} will result in a decrease in C due to a decrease in N_ε , the number of samples that are available for nonlinear dynamics forecasting within a small neighborhood of size L_ε . Use of embedding dimension smaller than D_{opt} will result in an increase of error reconstruction due to the use of a finite embedding dimension D_e to approximate the required infinite embedding dimension of the chaotic dynamics and the statistically independent message samples, as implied by the first term of the error in Eq. (34). It is evident from Fig. 9 that the conditional Lyapunov exponent λ can be used to increase the security of an encryption scheme by increasing the value of the parameter b (larger conditional negative Lyapunov exponent λ) so that the optimal embedding dimension D_{opt} increases, and the cleaning factor C decreases, and the unauthorized receiver will need more samples in a higher dimensional reconstructed embedding phase space in order to reconstruct the message with high accuracy.

Shown in Fig. 10 are the simulation and theoretical estimation of the chaotic signal cleaning factor C as a function of the nonlinear dynamics forecasting neighborhood size L_ε for various values of the embedding dimension D_e . The theoretical estimation used was similar to the estimation used to obtain Fig. 9, only this time the offset parameter was $\Delta = 9$ dB.

Each graph in Fig. 10 has an optimal value for the neighborhood size L_ε which results in the largest value of the cleaning factor C for a given value of the embedding dimension D_e . Using neighborhood size L_ε which is smaller than the optimal value will result in a larger reconstruction error due to the decrease in the number of samples N_ε that are available within a neighborhood of size L_ε for averaging out the perturbation caused to the chaotic signal by the message sequence $m(n)$. Using neighborhood size L_ε which is larger than the optimal value will result in larger interpolation error of the reconstructed dynamics. An unauthorized receiver, when given a finite number of samples N_s to reconstruct the chaotic dynamics will attempt to find the optimal values for the embedding dimension D_e and neighborhood size L_ε that will maximize the chaotic signal cleaning factor C and thus minimize the reconstruction error of the message m . In Fig. 10 the

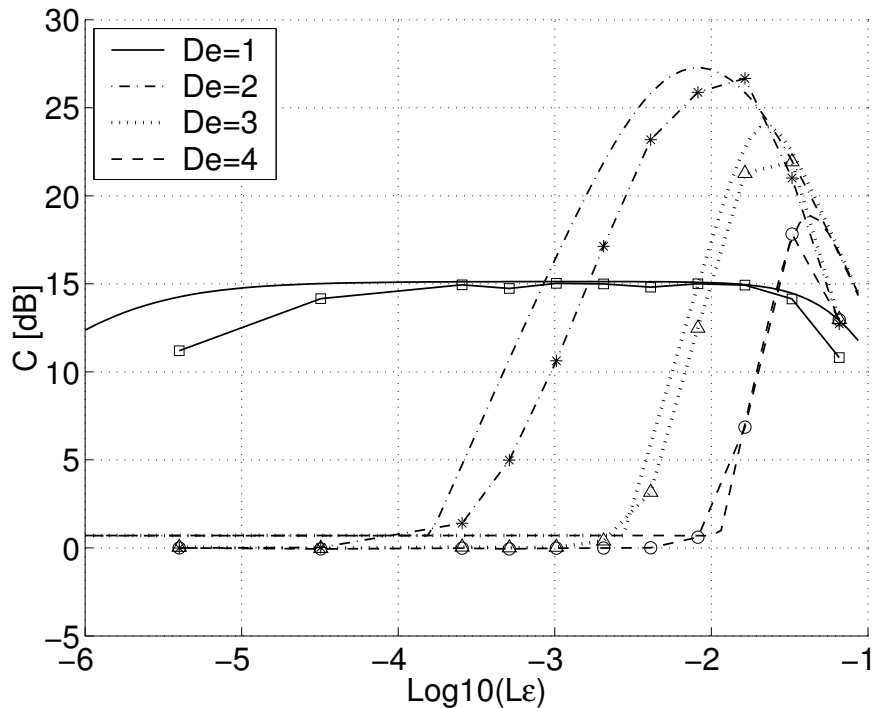


Fig. 10. Simulation (symbols) and theoretical values (lines) of noise cleaning C as a function of the neighborhood size L_ϵ for various values of embedding dimension D_e . Simulation parameters: $N_s = 25e6$, $M = -13$ dB, $b = 0.2$. Theoretical estimation parameters: $c = 0.22$, $k = 0.3$, $\Delta = 9$ dB.

maximal value for the chaotic cleaning factor C is obtained for $D_e = 2$ and $L_\epsilon = 0.016$.

The volume of the attractor in the D_e dimensional embedding phase space increases as the message dynamical range is increased. As a consequence, given a fixed number of samples N_s the density of samples decreases, and the number of samples that are available for nonlinear dynamics forecasting in a small neighborhood of size L_ϵ in the reconstructed D_e dimensional embedding phase space decreases.

We define P as the fraction the number of samples N_ϵ within a small neighborhood of size L_ϵ out of the total number of samples N_s , so that:

$$P = \frac{N_\epsilon}{N_s} \tag{51}$$

Figure 11 shows the value of P as a function of the message mean square M for various values of the embedding dimension D_e . The value of P decreases as the message mean square M increases, due to the inflation in the volume of the chaotic attractor. The inflation of the attractor volume implies that the unauthorized receiver needs to reconstruct the dynamics in a larger number of small neighborhoods of size L_ϵ in the reconstructed embedding phase space,

and if the number of samples N_s is fixed, each neighborhood will contain a smaller number of samples N_ϵ . We can think of it as if there are more possible sequences $\mathbf{s}(n) = \{s(n), \dots, s(n - D_e + 1)\}$ from which we need to forecast the next average sample $s(n) = \hat{P}(\mathbf{s})$ in order to reconstruct the message using Eq. (12). Increasing the message mean square error M will enhance the security of the encryption scheme by inflating the volume of the attractor in the reconstructed embedding phase space (Fig. 11) and by increasing the perturbation magnitude of the chaotic dynamics caused by the message M . Given a fixed number of samples N_s that are available for reconstruction of the chaotic dynamics, the inflation of the attractor volume will result in a smaller number of neighbors in a small neighborhood of the reconstructed embedding phase space that are available for averaging out the perturbation to the chaotic dynamics caused by the message, and the increase in the perturbation magnitude will increase the forecasting error. Figure 12 shows the chaotic signal cleaning factor C as a function of the message power M for various values of number of samples N_s that are used for nonlinear dynamics forecasting. As explained above, the larger the message power M the larger the reconstruction error

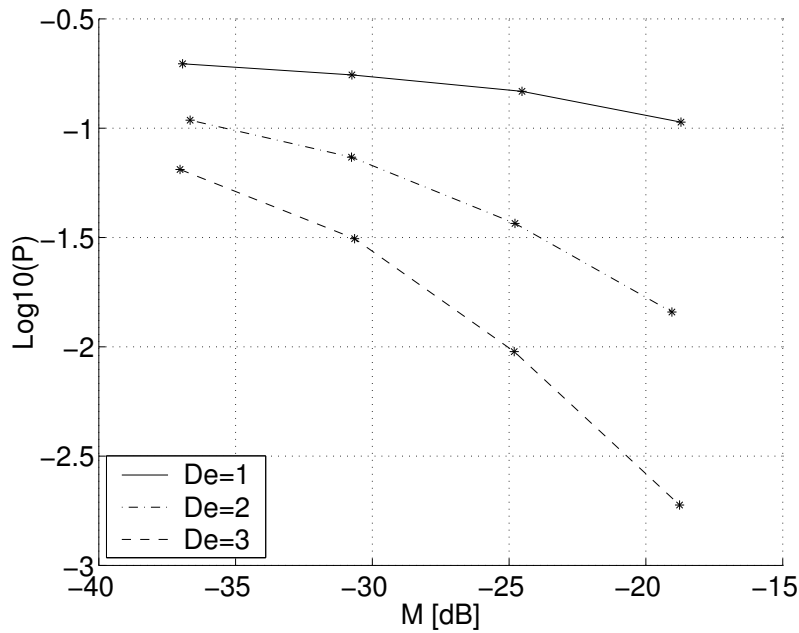


Fig. 11. The neighbors fraction $P = N_\varepsilon/N_s$ as a function of the message mean square power M , for various values of the reconstruction embedding dimension D_e . $N_s = 10^5$, $b = 0.5$, $L_\varepsilon = 0.03$.

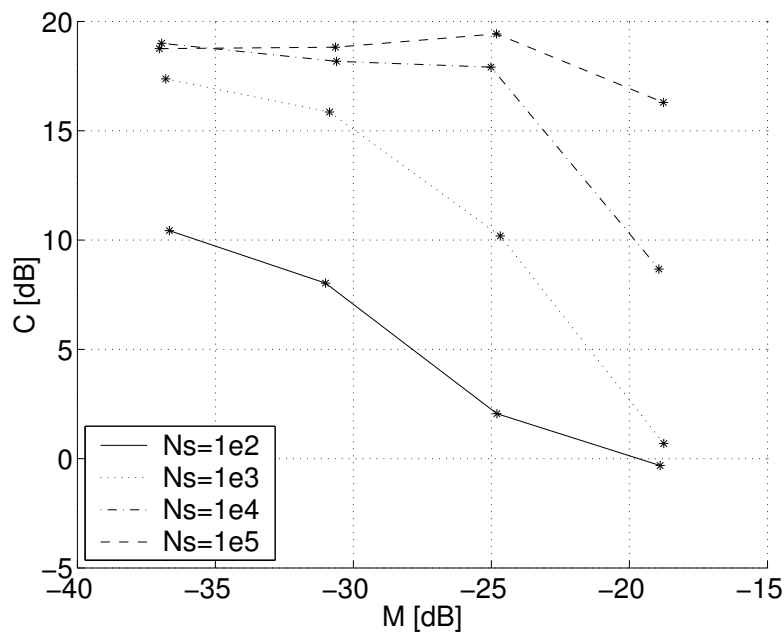


Fig. 12. Chaotic signal cleaning, C , as a function of the message mean square power M , for various number of samples N_s that are used for reconstruction. $D_e = 3$, $b = 0.5$, $L_\varepsilon = 0.03$.

and the chaotic cleaning factor C is smaller. As a consequence, the security of the encryption scheme can be enhanced by increasing the message power M while maintaining high sensitivity to reconstruction noise N by using a fine grained modulation as described in Sec. 4.

5.1. Setting parameter values of encryption scheme

The encryption scheme parameters need to be properly set to maintain both security and communication efficiency. In our analysis we show that the

unauthorized receiver may use the optimal values for the embedding dimension D_e and the reconstruction neighborhood size L_e that maximizes the cleaning factor C given a fixed number of samples N_s to reconstruct the secret chaotic dynamics. In the design of a chaotic encryption scheme one can increase security of an encryption scheme by using large conditional Lyapunov exponent λ , large dynamic range for the message modulation scheme L_m , and a modulation that fine-grained, and therefore is sensitive to reconstruction noise. However, those values cannot be chosen arbitrarily, since large conditional Lyapunov exponent λ will result in slower synchronization between transmitter and receiver (or even loss of synchronization), large message dynamical range L_m will require high transmission power, and fine-grained modulation that is sensitive to reconstruction error may also be sensitive to channel noise and noise present in the analog circuits that are used to implement the transmitter and receiver.

In order to optimize transmitter performance while maintaining security, the following procedure can be used to set the values of the parameters of an encryption scheme:

- Choose modulation with the highest possible sensitivity to reconstruction error (as fine-grained as possible), that is not too sensitive, so that the channel noise and the circuit noise will not cause decoding errors by the authorized receiver. This can be done by choosing bin size q for the modulation shown in Fig. 3(c) that is larger than the expected channel and circuitry noise.
- Determine the minimum level of reconstruction mean square error e_{\min} that can be allowed for the unauthorized receiver to reconstruct the chaotic dynamics without compromising the secret message. This value is determined depending on the type of data that is transmitted (audio, video, digital modulation).
- Determine the maximal number of samples N_s that the authorized receiver may need to transmit. Assume that those N_s samples will be available to the unauthorized receiver for reconstruction of the secret chaotic dynamics using the methods discussed in this paper.
- Determine the values for the conditional Lyapunov exponent λ and the message dynamical range L_m that will ensure that the unauthorized receiver will not be able to reconstruct the message with a reconstruction mean square

error lower than the error we allow e_{\min} using the N_s transmitted samples of the signal $s(n)$. Security is increased by decreasing $|\lambda|$ and increasing L_m , however those quantities should be as small as possible in order to obtain fast receiver synchronization rate and low transmission power, respectively.

6. Summary

In this paper we laid out a methodology for quantifying the security of chaos and synchronization encryption schemes based on active/passive decomposition. The amount of data that is available to the unauthorized receiver is measured by the number of transmitted samples N_s . The security of an encryption scheme is measured by the mean square error of the reconstructed dynamics as a function of the number of transmitted samples N_s available for the unauthorized receiver. Since the unauthorized receiver does not have access to the true transmitter state variables $\mathbf{x}(n)$, he needs to reconstruct the transmitter dynamics in the embedding phase space using time delays of the transmitted sequence $s(n)$. In our analysis we assumed that the unauthorized receiver had no knowledge of any general model that can reduce the task of the reconstruction to the estimation of a small number of parameters, and therefore needs to reconstruct the secret chaotic dynamics at every neighborhood of the embedding phase space. If this assumption fails, a severe degradation in the security of the encryption scheme may occur. If message samples are statistically independent, the dimension of the transmitted signal is infinite even if the dimension of the chaotic dynamics is small. An attempt to reconstruct the chaotic dynamics using a finite embedding dimension D_e results in a reconstruction error even if an infinite number of samples is available for the reconstruction. The reconstruction error that is caused by the use of a finite embedding dimension D_e decays exponentially with the largest conditional Lyapunov exponent λ and the reconstruction embedding phase space D_e .

In the encryption scheme a chaotic signal x is mixed with the message m to hide the message, however the opposite is also true: The message can be used to mask the secret chaotic dynamics by perturbing it, so that more samples are needed in order to accurately reconstruct the chaotic dynamics. If a finite number of samples is available, the embedding dimension D_e cannot be increased arbitrarily,

since a large D_e will result in a small number of neighbors within a fixed size neighborhood and a poor averaging out of message perturbations to the chaotic dynamics. In our analysis we derived the optimal embedding dimension which is a compromise between choosing D_e as large as possible in order to approximate the infinite embedding dimension of the statistically independent message samples, and yet as small as possible in order to have a large number of samples available in each neighborhood of the reconstructed embedding phase space in order to average out the perturbation to the chaotic dynamics caused by the message.

One can increase the security of an encryption scheme by increasing the number of samples required to reconstruct the chaotic dynamics by choosing a random modulation scheme with large dynamical range, and yet fine-grained. This will require a more accurate reconstruction of the chaotic dynamics in an embedding phase space of larger volume.

In this paper we developed an algorithm for choosing the parameters of an encryption scheme so that security is maintained, and communication is efficient. In particular, we gave guidelines for choosing the conditional Lyapunov exponent λ , and the modulation dynamic range L_m and bin size q , so that the reconstruction error encountered by the unauthorized receiver will be large enough and yet fast synchronization, low transmission power are maintained.

We demonstrated our security analysis using a relatively simple chaotic tent map, however our analysis can be applied to encryption schemes that use more complicated chaotic dynamics of higher dimension. We assumed that the unauthorized receiver estimates the dynamics using zero order polynomial approximation, however it may use other estimation methods, such as higher order polynomials and splines. Using such methods may result in a more accurate estimation that uses the finite number of available samples more efficiently than we used in our simulation. However, the essence of our analysis is not in the absolute numbers obtained in our simulation, but rather the introduction of appropriate measures and factors that affects security that holds also for dynamics reconstruction of higher order.

Finally, the analysis described in this paper is one step in the attempt to quantify the cryptanalysis of chaotic encryption schemes and elevate it from the heuristic and intuitive level to a more solid and

rigorous framework. More research needs to be done for the design of more secure and more efficient encryption schemes, and the analysis of factors which were beyond the scope of this paper, such as the use of higher order polynomial approximations by the unauthorized receiver for reconstructing the chaotic dynamics.

Acknowledgments

This work was partially supported by the Army Research Office under MURI grant DAAG55-98-1-0269, by the U.S. Department of Energy, Office of Basic Energy Sciences, under Grants No. DE-FG03-95ER14516, and No. DE-FG03-96ER14592.

References

- Abarbanel, H. D. I. [1996] *Analysis of Observed Chaotic Data* (Springer).
- Carroll, T. L. & Pecora, L. M. [1993] "Cascading synchronized chaotic systems," *Physica* **D67**, 126–140.
- Cuomo, K. M. & Oppenheim, A. V. [1993] "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* **71**, 65–68.
- Dedieu, H., Kennedy, M. P. & Hasler, M. [1993] "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst.-II* **40**, 634–642.
- Farmer, J. D. & Sidorowich, J. J. [1987] "Predicting chaotic time series," *Phys. Rev. Lett.* **59**, 845–848.
- Geddes, J. B., Short, K. M. & Black, K. [1999] "Extraction of signals from chaotic laser data," *Phys. Rev. Lett.* **83**, 5389–5392.
- Hayes, S., Grebogi, C., Ott, E. & Mark, A. [1994] "Experimental control of chaos for communication," *Phys. Rev. Lett.* **73**, 1781–1784
- Kocarev, L. & Parlitz, U. [1995] "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.* **74**, 5028–5031.
- Kocarev, L. & Jakimoski, G. [2001] "Logistic map as a block encryption algorithm," *Phys. Lett.* **A289**, 199–206.
- Lai, Y., Bollt, E. & Grebogi, C. [1999] "Communicating with chaos using two-dimensional symbolic dynamics," *Phys. Lett.* **A255**, 75–81.
- Ming Dai, Y. Z., Hua, Y., Ni, W. & Du, G. [1998] "Digital communication by active-passive decomposition synchronization in hyperchaotic systems," *Phys. Rev.* **E58**, 3022–3027.
- Parlitz, U., Kocarev, L., Stojanovski, T. & Preckel, H. [1996] "Encoding messages using chaotic synchronization," *Phys. Rev.* **E53**, 4351–4361.
- Rulkov, N. F., Sushchik, M. M., Tsimring, L. S. & Volkovskii, A. R. [2001] "Digital communication using

- chaotic pulse position modulation," *IEEE Trans. Circuits Syst.* **48**, 1436–1444.
- Shannon, C. E. [1949] "Communication theory of secrecy systems," *Bell Syst. Techn. J.* **28**, 656–715.
- Short, K. M. [1994] "Steps toward unmasking secure communications," *Int. J. Bifurcation and Chaos* **4**, 959–977.
- Short, K. M. [1996] "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurcation and Chaos* **6**, 367–375.
- Short, K. M. & Parker, A. T. [1998] "Unmasking a hyperchaotic communication scheme," *Phys. Rev.* **E58**, 1159–1162.
- van Tilborg, H. C. A. [2000] *Fundamentals of Cryptology* (Kluwer Academic Publishers).
- Volkovskii, A. R. & Rulkov, N. [1993] "Synchronous chaotic response of a nonlinear oscillating system as a principle for the detection of the information component of chaos," *Tech. Phys. Lett.* **19**, 97–99.
- Volkovskii, R. & Tsimring, L. S. [1999] "Synchronization and communication using chaotic frequency modulation," *Int. J. Circuit Th. Appl.* **27**, 569–576.
- Yang, T., Yang, L. & Yang, C. [1998a] "Breaking chaotic secure communication using a spectrogram," *Phys. Lett.* **A247**, 105–111.
- Yang, T., Yang, L. & Yang, C. [1998b] "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst.-I: Fund. Th. Appl.* **45**, 1062–1067.
- Yang, T., Yang, L. & Yang, C. [1998c] "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett.* **A245**, 495–510.
- Yang, T., Yang, L. & Yang, C. [1998d] "Application of neural networks to unmasking chaotic secure communication," *Physica* **D124**, 248–257.