

Cryptanalysis

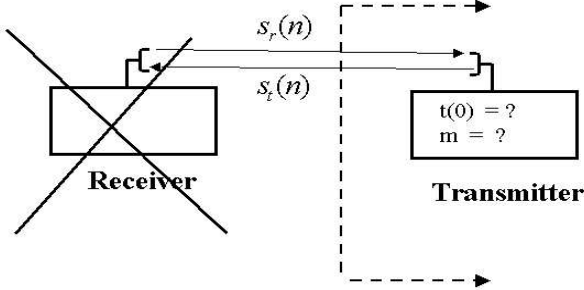


Figure 1. Eavesdropper attempts to estimate message m and hidden initial state of transmitter $\mathbf{t}(0)$ without knowing secret dynamics and secret state of receiver.

Several cryptanalysis methods that can be used to attack the DDE. We suggest several methods to protect against those attacks. We focus our cryptanalysis on ciphertext attacks and plaintext attacks. A ciphertext attack is an attempt to break an encryption scheme by using only the cyphertext (In DDE - the coupling transmitted signals $s_t(n), s_r(n)$). In a plaintext attack an unauthorized receiver attempts to break an encryption scheme using a sample of both a cyphertext and the corresponding plaintext (In DDE - $s_t(n), s_r(n), m(n)$). Since an unauthorized receiver does not know the dynamics of the receiver he may attempt to decode the secret message $m(n)$ by using methods that do not rely on knowledge of the receiver dynamics as illustrated in Fig.1

1 Plain text attack: Attractor reconstruction using trajectory ends

Attack:

An eavesdropper can get a sample of a transmitted secret message (plaintext) and the corresponding transmitted signals $s_t(n), s_r(n)$ (ciphertext) and may attempts to reconstruct the attractors that correspond to the transmission of '0' and '1'. Although the trajectories for each transmitted bit starts at a random initial state, the trajectories endpoints lie on the attractor. The attractors can be estimated by interpolating the end points of the trajectories as shown in Fig. 2.

Protection:

Altering the secret dynamics of the receiver will shift the position of the attractors. Therefore an endpoint of a trajectory that lies on the attractor that corresponds to the transmission of '0' for one receiver dynamics can lie on

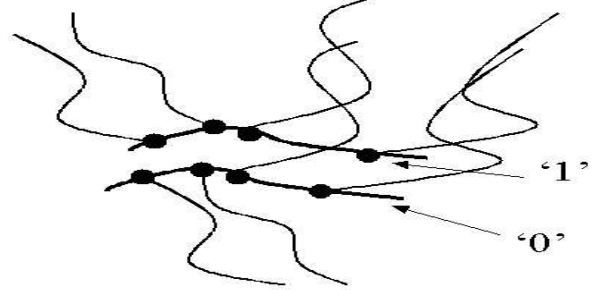


Figure 2. An unauthorized receiver attempts to reconstruct trajectories that correspond to transmitted '0' and transmitted '1' by interpolating end points of trajectories that lie on the attractors.

the attractor that correspond to the transmission of '1' for a different transmitter dynamics. Since the unauthorized receiver can not assume that close trajectory endpoints will always correspond to transmission of the same bit he can not interpolate a set of endpoints and find the attractor position corresponding to the transmission of '0' or '1'.

2 Cyphertext attack: Solving transmitter public dynamics equations for transmitter state and message

Attack:

An eavesdropper can monitor the receiver's public input and output signals ($s_t(n), s_r(n)$), and by using the public dynamics $\mathbf{F}_T(\bullet), G_T(\bullet)$ solve the following set of equations for the transmitted bit $m(n)$ and Initial state $\mathbf{t}(0)$:

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

Protection:

Use transmitter dynamics $\mathbf{F}_T(\bullet)$ which depends on the power of order p of the transmitter state components t_i : $\mathbf{F}_T(\bullet) = f((t_i)^p)$. The term $\mathbf{t}(D_{Tr})$ in Eq. (1) will have components of the form: $[t_i(0)]^{p^{D_{Tr}}}$. By choosing large

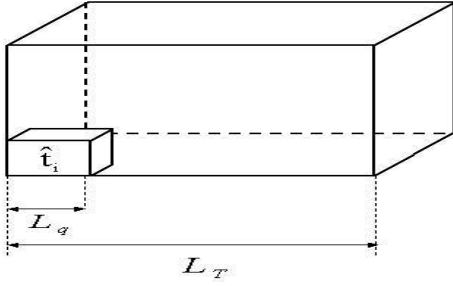


Figure 3. The space of the transmitter state $\mathbf{t}(n)$ is larger or at least equal to a cube of dimension D_T and size L_T . The transmitter continuous state is quantized into discrete cubes of dimension D_T and size L_q .

transmitter state dimension D_T Eq. (1) become computationally unfeasible. For example, by choosing transmitter dynamics which is polynomial with $p = 4$ and dimension of transmitter state $D_T = 10$ the term $\mathbf{t}(D_T)$ in Eq. (1) will depend on the term $(t_i)^{1,048,576}$. Further increase in D_T and p will make solution of Eq. (1) unfeasible.

3 Ciphertext attack: State quantization and Maximum Likelihood estimation

Attack:

An unauthorized receiver can quantize the continuous state space of the transmitter $\mathbf{t}(n)$, calculate a Hidden Markov Model (HMM) for the transmitter dynamics and obtain a Maximum Likelihood (ML) estimation of the secret transmitter message $m(n)$ and the initial transmitter state $\mathbf{t}(0)$. We assume that the space of the transmitter state $\mathbf{t}(n)$ is larger or at least equal to a cube of dimension D_T and size L_T as illustrated in Fig. 3. This assumption can be guaranteed by initializing the transmitter state at the beginning of each transmitted bit with a random value $\mathbf{t}(0)$ which is taken from a uniform distribution with the shape of a cube with dimension D_T and size L_T . The transmitter state space \mathbf{t} is quantized into N_s cubes $\hat{\mathbf{t}}_i, i = 1 \dots N_s$ of dimension D_T and size L_q . The transition probability $p(\hat{\mathbf{t}}_i \rightarrow \hat{\mathbf{t}}_j)$ which is the probability of transition from the quantized state $\hat{\mathbf{t}}_i$ to the quantized state $\hat{\mathbf{t}}_j$ can be estimated using the transmitter public dynamics $\mathbf{F}_T(\bullet)$ and the public signal s_r . The observation probability $p(s_t(n) | \hat{\mathbf{t}}_i)$ which is the probability of observing the signal $s_t(n)$ transmitted from transmitter to receiver given the transmitter quantized state $\hat{\mathbf{t}}_i$ can be estimated using the transmitter public function $G_T(\bullet)$. The state transition probability $p(\hat{\mathbf{t}}_i \rightarrow \hat{\mathbf{t}}_j)$ and the observation probability $p(s_t(n) | \hat{\mathbf{t}}_i)$ are used to construct a Hidden Markov Models (HMM) for the quantized dynamics of the receiver (Fig. 4). Two HMM models are constructed, one for each transmitter dynamics that correspond to the transmission of either '0' or '1'. Once the unauthorized receiver monitors a transmitted sequences

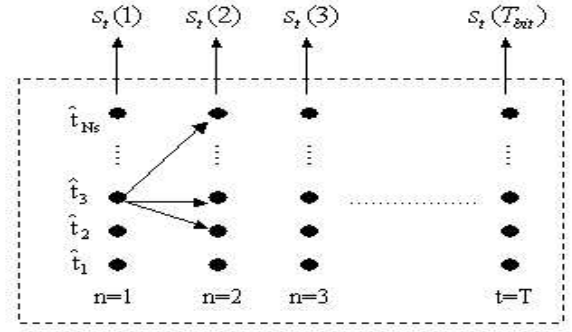


Figure 4. A Hidden Markov Model (HMM) is used to model the dynamics of the quantized transmitter state $\hat{\mathbf{t}}(n)$.

$s_r^{T_{bit}} = (s_r(0), \dots, s_r(T_{bit}))$, $s_t^{T_{bit}} = (s_t(0), \dots, s_t(T_{bit}))$ he can use the HMMs to calculate the conditional probabilities $p(s_t^{T_{bit}} | m = 0)$ and $p(s_t^{T_{bit}} | m = 1)$ which are the probabilities of observing the transmitted sequence $s_t^{T_{bit}}$ given the transmission of either '0' or '1'. The estimation of the transmitted bit \hat{m}_{ML} is the one that maximizes the likelihood of the observations:

$$\hat{m} = \max_{m \in \{0,1\}} p(s_t^{T_{bit}} | m). \quad (2)$$

Protection:

The encryption scheme can be protected by forcing the eavesdropper to use an impractically large number of states for the HMM model. The number of cubes of size L_q that are contained in a cube of size L_T of dimension D_T is given by :

$$N_s = \left(\frac{L_T}{L_q} \right)^{D_T}. \quad (3)$$

We can make N_s large by choosing transmitter dynamics with large state dimension D_T and large cube size L_T . By choosing attractors for transmission of '0' and '1' that are as close as possible we force the eavesdropper to use small quantization size L_q . Large L_q will result in quantization noise that will prevent separation between the two close attractors as shown in Fig. 5. We will now obtain an upper bound for the the state quantization size L_q that corresponds to a lower bound for the HMM states number N_s in Eq. (3). The use of quantized transmitter state $\hat{\mathbf{t}}(n)$ instead of the accurate transmitter state $\mathbf{t}(n)$ results in quantization error $\mathbf{e}(n)$:

$$\mathbf{e}(n) = \hat{\mathbf{t}}(n) - \mathbf{t}(n). \quad (4)$$

The quantization error $\mathbf{e}(n)$ is comprised from two components :

$$\mathbf{e}(n) = \mathbf{e}_{prev}(n) + \mathbf{e}_{curr}(n), \quad (5)$$

Where $\mathbf{e}_{prev}(n)$ is the error in the current state $\mathbf{t}(n)$ caused by quantization of the transmitter state in previous states $\mathbf{t}(n-1), \mathbf{t}(n-2), \dots$ due to memory of the dynamics. $\mathbf{e}_{curr}(n)$ is the error caused by quantization of the

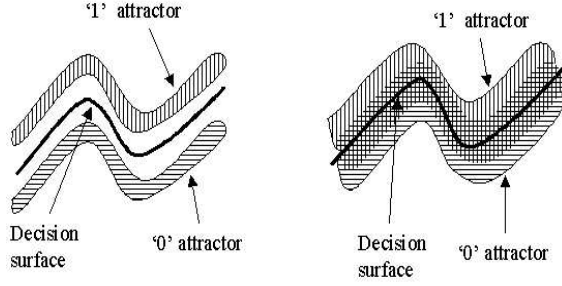


Figure 5. Left: Small noise, attractors can be separated. Right: Larger noise, attractors overlap results in larger decoding error

current state $\mathbf{t}(n)$. $\mathbf{e}_{prev}(n)$, $\mathbf{e}_{curr}(n)$ are independent and therefore uncorrelated. We obtain a lower bound for the variance of the quantization error of transmitter state $\mathbf{t}(n)$:

$$\begin{aligned} Var(\mathbf{e}(n)) &= Var(\mathbf{e}_{prev}(n)) + Var(\mathbf{e}_{curr}(n)) \\ &\geq Var(\mathbf{e}_{curr}(n)) \end{aligned} \quad (6)$$

We now calculate $Var(\mathbf{e}_{curr}(n))$. The quantization error of the i 'th component of the transmitter state $e_{i,curr}(n)$, has uniform distribution :

$$\begin{aligned} e_{i,curr}(n) &\sim U\left[-\frac{L_q}{2}, \frac{L_q}{2}\right] \\ Var(e_{i,curr}(n)) &= \frac{L_q^2}{12} \end{aligned} \quad (7)$$

The dynamics of the transmitter remains nonlinear since $\mathbf{F}_T(\bullet)$ is nonlinear. The quantization error components $e_{i,curr}(n)$, $e_{j,curr}(n)$ of state components $t_i(n)$, $t_j(n)$ are independent for $i \neq j$. The mean and covariance matrix of the quantization noise $\mathbf{e}_{curr}(n)$ are given by:

$$\begin{aligned} Mean(\mathbf{e}_{curr}(n)) &= 0 \\ Var(\mathbf{e}_{curr}(n)) &= \begin{pmatrix} \frac{L_q^2}{12} & 0 & \dots & 0 \\ 0 & & \ddots & \vdots \\ \vdots & & & 0 \\ 0 & \dots & 0 & \frac{L_q^2}{12} \end{pmatrix} \end{aligned} \quad (8)$$

In order to simplify the analysis we choose $G_T(\bullet)$ to be a linear function of the state $\mathbf{t}(n)$ and the modulated data m :

$$\begin{aligned} s_t(n) &= G_T(\mathbf{t}(n), s_r(n), m(n)) \\ &= C^T \cdot \mathbf{t}(n) + A \cdot m \end{aligned} \quad (9)$$

where : $C^T = w \cdot [1, 1, \dots, 1]$

We will now assume that an unauthorized receiver knows the quantized hidden state of the transmitter $\hat{\mathbf{t}}(n)$ and the

error he makes in estimating m is due to the quantization of $\mathbf{t}(n)$. This assumption will result in a lower bound for the message decoding error rate since in practice the unauthorized receiver does not know the quantized transmitter state $\hat{\mathbf{t}}(n)$ and its estimation will result in additional error. Using Eq. (9) the unauthorized receiver can obtain an estimation $\hat{m}(n)$ for the transmitted bit m using the observation $s_t(n)$ while the quantized transmitter state $\hat{\mathbf{t}}(n)$ is assumed to be known. Also, it is assumed that the transmitted signal $s_t(n)$ is measured by the eavesdropper accurately without any noise :

$$\begin{aligned} \hat{m}(n) &= \frac{1}{A} \left[s_t(n) - f_2(\hat{\mathbf{t}}(n), m=0) \right] \\ &= \frac{1}{A} [s_t(n) - C^T \cdot \hat{\mathbf{t}}(n)] \end{aligned} \quad (10)$$

Using Eq. (10) and Eq. (8) the mean and variance of the estimator $\hat{m}(n)$ are given by:

$$\begin{aligned} Mean(\hat{m}(n)) &= m \\ Var(\hat{m}(n)) &= \frac{1}{A^2} \cdot C^T \cdot Var(\mathbf{e}_{curr}(n)) \cdot C \\ &= \frac{w^2}{A^2} \cdot D_T \cdot \frac{L_q^2}{12} \end{aligned} \quad (11)$$

The estimator $\hat{m}(n)$ depends on the sum of D_T random i.i.d. error components $e_{i,curr}(n)$ and by using the central limit theorem we can estimate its probability density function as gaussian:

$$\hat{m}(n) \sim Normal\left(m, \frac{w^2 \cdot D_T \cdot L_q^2}{12 \cdot A^2}\right) \quad (12)$$

Assuming that each transmitted bit length is T_{bit} samples the unauthorized receiver can improve the decoding performance by averaging T_{bit} estimations of $\hat{m}(n)$:

$$\hat{m} = \frac{1}{T_{bit}} \sum_{n=1}^{T_{bit}} \hat{m}(n) \quad (13)$$

\hat{m} distribution is given by:

$$\hat{m} \sim Normal\left(m, \frac{w^2 \cdot D_T \cdot L_q^2}{12 \cdot T_{bit} \cdot A^2}\right) \quad (14)$$

A Maximum Likelihood (ML) estimation of the transmitted bit m (assuming that the quantized state $\hat{\mathbf{t}}$ is known) is :

$$\begin{aligned} \hat{m}_{ML} &= \max_{m \in \{0,1\}} p(\hat{m} | m) \\ &= \begin{cases} 0, & \text{if } \hat{m} \leq \frac{1}{2} \\ 1, & \text{if } \hat{m} > \frac{1}{2} \end{cases} \end{aligned} \quad (15)$$

The error rate P_u , encountered by an unauthorized receiver is given by:

$$P_u \geq 1 - Q\left(\frac{1}{2} \sqrt{\frac{12A^2 T_{bit}}{D_T L_q^2 w^2}}\right), \quad (16)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{z^2}{2}} dz$. The quantization size L_q must be smaller than an upper bound L_q^{max} in order to maintain classification error rate below a level P_u :

$$L_q \leq L_q^{max} = \frac{A}{2 \cdot w} \cdot \sqrt{\frac{12 \cdot T_{bit}}{D_T}} \cdot \frac{1}{Q^{-1}(1 - P_u)}. \quad (17)$$

The lower bound for the number of states N_s is obtain by substituting Eq. (17) into Eq. (3):

$$N_s \geq \left[\frac{L_T \cdot w}{A} \cdot \sqrt{\frac{D_T}{3 \cdot T_{bit}}} \cdot Q^{-1}(1 - P_u) \right]^{D_T}. \quad (18)$$

The number of states N_s can be made large enough to make decoding using quantization of transmitter state computationally unfeasible. Large N_s can be achieved by choosing small modulation parameter A and large transmitter dimension D_T .