Cryptanalysis of Cryptosystems based on Remote Chaos Replication

Th. Beth, D. E. Lazic, A. Mathias

Universität Karlsruhe, Fakultät für Informatik,
Institut für Algorithmen und Kognitive Systeme,
Am Fasanengarten 5, D-76 128 Karlsruhe, Germany

Abstract. In the last five years, many cryptosystems based on the chaos phenomenon have been proposed. Most of them use chaotic maps, i. e., the discrete-time chaos. The recent announcement of a cryptosystem based on continuous-time chaos that is generated by a very simple electronic circuit known as Chua's circuit passed unrecognized by a large part of the cryptographic community. It is an analog to the VERNAM-cipher system, but uses auto-synchronization through remote replication of the chaotic masking signal. After the introductory description of continuous-time chaotic systems and their synchronization a general definition and discussion of cryptosystems based on remote chaos replication is given. A cryptanalytic attack for these systems is developed that can break the cryptosystem using Chua's circuit for all types of information-bearing signals.

1 Introduction

Analog scrambling devices have been a part of classical cryptography ever since secure transmission by wire and radio have been used. Amongst the many procedures for such tasks the method of adding synchronous noise is thoroughly understood from the information theoretic point of view. The well known VERNAM-cipher system [Ver26] as a digital counterpart of this method which has been defined for secure transmission of binary strings was proved unbreakably secure by SHANNON [Sha49], provided the noise sequence has maximal entropy and a secure key/synchronization channel is used. While digital cryptosystems of this kind have successfully been used during the last seven decades, the recent announcement of a by far cheaper and more efficient analog scrambling cryptosystem realized as a simple electronic circuit by L. CHUA and his coworkers [KHE92] passed unrecognized by a large part of the cryptographic community.

The idea, widely acclaimed in the community of control engineers, is that with a cryptosystem based on the continuous-time chaos phenomenon not only secure communication can be guaranteed, but also, what is more, it is implicitly claimed that this is achievable without the need for key management and external synchronization. The principle of this system resembles a modification of the VERNAM-cipher system where the additive scrambling noise is coming from a chaotic analog signal generator. The information-bearing signal is covered in chaotic pseudo noise of high amplitude giving a waveform with a very small

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 318-331, 1994.

signal–to–noise (S/N) ratio thus masked for the interceptor. At the receiver's side, this waveform is used to drive a replicating circuit that is equally tuned as the chaotic signal generator, the parameters being unknown to the interceptor. The auto–synchronizing replicating circuit produces a quite accurate copy of the chaotic noise which is then subtracted from the incoming waveform, thus revealing the buried signal.

In this paper we do not only show how such a system can be broken by well–adapted methods of signal processing. Also, a short discussion about the behavior of this type of cryptosystem in a real communication environment with channel noise and distortions points out the doubtfulness of a simple realization, especially in heavily disturbed communication channels. Besides, the implicated key–free–ness of this auto–synchronizing device is also questionable, although the common parameters of the chaos generating and replicating circuits may eventually be used as a key space. However, even the introduction of such a key doesn't significantly improve the security of the proposed system. Actually, the dominating power of the chaotic noise designed for auto–synchronizing purposes is from an information theoretic point of view the reason why this type of system is generally breakable [Sim79], [Sha93].

2 Continuous Time Chaos

When the behavior of some physical system is well understood, it is often possible to model it in terms of a set of state variables $SV = \{x_1(t), \ldots, x_N(t)\}$ varying in time. The most familiar systems using this approach are dynamical systems. A very common representation of a continuous time dynamical system is that of a system of N simultaneous first-order ordinary differential equations (ODE):

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \mathbf{d}, \boldsymbol{\lambda}, t), \tag{1}$$

where

$$\begin{aligned}
&\mathbf{x} = \mathbf{x}(t) = (x_1(t), \ldots, x_N(t)); \qquad x_n(t) \in SV, n = 1, \ldots, N,\\
&\dot{\mathbf{x}} = \dot{\mathbf{x}}(t) = (\mathrm{d}x_1(t)/\mathrm{d}t, \ldots, \mathrm{d}x_N(t)/\mathrm{d}t),\\
&\mathbf{f} = \mathbf{f}(\mathbf{x}, \ldots): \qquad U \longrightarrow \mathbb{R}^N, \qquad U \subseteq \mathbb{R}^N,\\
&\mathbf{d} = \mathbf{d}(t) = (d_1(t), \ldots, d_M(t)), \qquad d_m(t) \in DF = \{d_1(t), \ldots, d_M(t)\},\\
&\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_L) \in \mathbb{R}^L, \qquad \lambda_l \in SP = \{\lambda_1, \ldots, \lambda_L\},\\
&t \in I = (a, b) \subseteq \mathbb{R}.
\end{aligned}$$

Here, $x_n(t)$, $n = 1, \ldots, N$ are unknown real-valued functions of a real variable t (time) and $\mathbf{f}$ is a known *vector field* which depends on $\mathbf{x}$ and, but not necessarily, on a set DF of real-valued drive functions, on a set SP of real-valued system parameters and on the time t. If $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda}, t)$, the dynamical system is non-driven, and if $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda})$, it is autonomous.

Solving an initial value problem (IVP) of (1) for some given $\boldsymbol{\lambda}_0 \in \mathbb{R}^L$ of system parameters consists of finding N real-valued functions

$$\mathbf{X}(t) = (X_1(t), \ldots, X_N(t)) \tag{2}$$

satisfying (1) and the initial conditions

$$\mathbf{X}(t_0) = \mathbf{X}_0 = (X_1^0, \ldots, X_N^0) \in U \subset \mathbb{R}^N, \tag{3}$$

where $X_1^0, \ldots, X_N^0$ represent a chosen set of initial states of the continuous-time dynamical system at some chosen initial time $t_0 \in I$. The set of points $\{\mathbf{X}(t) \mid \mathbf{X}(t_0) = \mathbf{X}_0, t \in I\}$ is called the *trajectory* through $\mathbf{X}_0$ in the *state space* $\mathbb{R}^N$. If the vector field satisfies certain reasonable conditions, then an IVP has a unique solution in I. In general, different initial conditions at t_0 lead to different IVP solutions. An important property of autonomous systems is that if the IVP: $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda}_0), \mathbf{X}(t_0 = 0) = \mathbf{X}_0$ has the solution $\mathbf{X}(t)$, the IVP: $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda}_0), \mathbf{X}(t_0 \neq 0) = \mathbf{X}_0$ has the solution $\mathbf{X}(t - t_0)$ [GH90], [Per91].

The term *steady state* refers to the asymptotic behavior of IVP solutions as $t \longrightarrow \infty$ and defines the *limit set* in the state space. For continuous-time dynamical systems there exist four kinds of steady state behaviors: equilibrial, periodical, quasiperiodical and chaotic. The corresponding limit sets are: equilibrium point, closed curve, two-torus and the strange attractor. Chaotic behavior arises only in nonlinear systems for $N \geq 3$, for particular vector fields. A chaotic vector field has chaotic behavior only for particular parameter values, i.e., in *chaotic regime*, and usually has many different strange attractors characterized by the corresponding parameter values.

State variables in the chaotic regime are nonperiodic with a continuous broadband spectrum and exhibit sensitive dependence on initial conditions. Two identical autonomous chaotic systems started at initial conditions arbitrarily close to one another have trajectories which quickly become uncorrelated. Practically, it is impossible to construct two identical, independent chaotic systems with synchronized trajectories. There is always some error in measuring or specifying the initial conditions. Due to sensitive dependence, these errors, however small, will almost always alter the macroscopic behavior of a chaotic system [PC89]. Thus, in a very real sense, chaotic systems are unpredictable, i.e., their IVP solutions in chaotical regime behave similar to random processes. For this reason they are attractive for cryptographic applications. Until now, many cryptosystems based on chaos are proposed, most of them relying on discrete dynamical systems (time discrete variants of dynamical systems where ODE's are replaced by difference equations).

3 Synchronization in Chaotic Dynamical Systems

The vector field of an N-dimensional autonomous dynamical system

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda}) \tag{4}$$

with state variables in SV and with system parameters in SP is *drive decomposable* if it can be split up into the *drive* and *response* subsystems. This means that there is a dimension $N_1 < N$ and corresponding functions $\mathbf{f}^{(1)} : U_1 \longrightarrow$

$\mathbb{R}^{N_1}, U_1 \subseteq \mathbb{R}^{N_1}$ and $\mathbf{f}^{(2)}: U_2 \longrightarrow \mathbb{R}^{N_2}, U_2 \subseteq \mathbb{R}^{N_2}$, $N_2 = N - N_1$ that give two separate subsystems

$$\dot{\mathbf{x}}^{(1)} = \mathbf{f}^{(1)}\left(\mathbf{x}^{(1)}, \boldsymbol{\lambda}^{(1)}\right) \tag{5a}$$

$$\dot{\mathbf{x}}^{(2)} = \mathbf{f}^{(2)}\left(\mathbf{x}^{(2)}, \mathbf{d}^{(2)} = \mathbf{x}^{(1)}, \boldsymbol{\lambda}^{(2)}\right), \tag{5b}$$

where

$$\begin{aligned}
&\mathbf{x}^{(1)} = \mathbf{x}^{(1)}(t) = \left(x_1^{(1)}(t), \ldots, x_{N_1}^{(1)}(t)\right); \qquad \left\{x_i^{(1)}(t)\right\}_{i=1}^{N_1} = SV_1 \subset SV,\\
&\mathbf{x}^{(2)} = \mathbf{x}^{(2)}(t) = \left(x_1^{(2)}(t), \ldots, x_{N_2}^{(2)}(t)\right); \qquad \left\{x_j^{(2)}(t)\right\}_{j=1}^{N_2} = SV_2 \subset SV,\\
&SV_1 \cap SV_2 = \emptyset; \qquad SV_1 \cup SV_2 = SV; \qquad N_1 + N_2 = N,\\
&\boldsymbol{\lambda}^{(1)} = \left(\lambda_1^{(1)}, \ldots, \lambda_{L_1}^{(1)}\right); \qquad \left\{\lambda_i^{(1)}\right\}_{i=1}^{L_1} = SP_1 \subseteq SP,\\
&\boldsymbol{\lambda}^{(2)} = \left(\lambda_1^{(2)}, \ldots, \lambda_{L_2}^{(2)}\right); \qquad \left\{\lambda_j^{(2)}\right\}_{j=1}^{L_2} = SP_2 \subseteq SP,\\
&SP_1 \cup SP_2 = SP, \qquad L_1 + L_2 \geq L.
\end{aligned}$$

The two subsystems are coupled such that the behavior of the second (5b) is dependent on the behavior of the first (5a), but the first is not influenced by the behavior of the second. The first subsystem is called the *drive* and the second the *response*. Theoretically, for every $\boldsymbol{\lambda} \in \mathbb{R}^L$ and every $\mathbf{X}(0) = \mathbf{X}_0 \in U$ the solution of the IVP of (4) should always be equal to the solution of the IVP of the corresponding decoupled system (5) if the initial states $\mathbf{X}^{(1)}(0) = \mathbf{X}_0^{(1)}$, $\mathbf{X}^{(2)}(0) = \mathbf{X}_0^{(2)}$ and system parameters $\boldsymbol{\lambda}^{(1)} \cup \boldsymbol{\lambda}^{(2)}$ of (5) are identical to the corresponding ones in (4).

The concept of drive decomposition of an autonomous dynamical system makes a spatial separation of drive and response possible. If the dynamical system models an electronic circuit, the corresponding drive and response can be connected with a communication link that transmits the set of drive functions SV_1 as signals from the transmitting point (drive) to the receiving point (response). If the regime of the whole system is chaotic, such a communication system would represent a source which generates chaotic signals SV_2 driven by remotely generated chaotic signals SV_1 (SV_1 are all different from SV_2). Furthermore, if a second *inverse dynamical subsystem* (circuit)

$$\dot{\mathbf{x}}^{(I)} = \mathbf{f}^{(I)}\left(\mathbf{x}^{(I)}, \mathbf{d}^{(I)} = \mathbf{x}^{(II)}, \boldsymbol{\lambda}^{(I)}\right), \tag{6}$$

where

$$\begin{aligned}
&\mathbf{x}^{(I)} = \mathbf{x}^{(I)}(t) = \left(x_1^{(I)}(t), \ldots, x_{N_I}^{(I)}(t)\right); \quad \left\{x_i^{(I)}(t)\right\}_{i=1}^{N_I} = SV_I \subseteq SV_1,\\
&\mathbf{x}^{(II)} = \mathbf{x}^{(II)}(t) = \left(x_1^{(II)}(t), \ldots, x_{N_{II}}^{(II)}(t)\right); \left\{x_j^{(II)}(t)\right\}_{j=1}^{N_{II}} = SV_{II} \subseteq SV_2,\\
&\boldsymbol{\lambda}^{(I)} = \left(\lambda_1^{(I)}, \ldots, \lambda_{L_I}^{(I)}\right); \quad \left\{\lambda_i^{(I)}\right\}_{i=1}^{L_I} = SP_I \subseteq SP,
\end{aligned}$$

can be constructed at the receiving point which is driven with $SV_{II} \subseteq SV_2$ and generates one or more signals $SV_I \subseteq SV_1$, a remote replica of chaotic signals would be theoretically possible.

For practical realization of such chaotic, synchronized subsystems, the stability of the response and inverse circuit is required. That means,

$$\lim_{t\to 0} \left| x_i^{(I)}(t) - x_i^{(1)}(t) \right| = 0 \qquad i = 1, \ldots, N_I, \tag{7}$$

1. independent of initial conditions $\mathbf{X}_0^{(2)}$ and $\mathbf{X}_0^{(I)}$,
2. when response and inverse circuit have common parameters, and parameters corresponding to the drive are slightly different, and
3. when there is an additive disturbance $\delta(t) = (\delta_1(t), \ldots, \delta_{N_1}(t))$ in the communication channel, i.e., $d_i^{(2)}(t) = x_i^{(1)}(t) + \delta_i(t)$; $i = 1, \ldots, N_1$, with disturbance-to-chaos power ratios D/C_i, $i = 1, \ldots, N_1$, smaller than some upper limit value $\overline{D/C}$.

We will call these three stability conditions *initial value*, *parameter* and *channel disturbance* stability. In practical applications, (7) should converge relatively rapid.

Recently, PECORA and CARROLL [PC90], [PC91] practically showed that if the response is driven only by some subset of the driven system's state variables, it is possible to construct decoupled systems whose common state variables are synchronized even in chaotic regime. This gives a subdivision of the system (4) into three subsystems:

$$\dot{\mathbf{x}}^{(1)} = \mathbf{f}^{(1)}\left(\mathbf{x}^{(1)},\ \mathbf{d}^{(1)} = \mathbf{x}^{(2)},\ \boldsymbol{\lambda}^{(1)}\right), \tag{8a}$$

$$\dot{\mathbf{x}}^{(2)} = \mathbf{f}^{(2)}\left(\mathbf{x}^{(2)},\ \mathbf{d}^{(2)} = \mathbf{x}^{(1)},\ \boldsymbol{\lambda}^{(2)}\right), \tag{8b}$$

$$\dot{\mathbf{x}}^{(3)} = \mathbf{f}^{(3)}\left(\mathbf{x}^{(3)},\ \mathbf{d}^{(3)} = \mathbf{x}^{(1)},\ \boldsymbol{\lambda}^{(3)}\right), \tag{8c}$$

where $\mathbf{f}^{(1)}$ is N_1–dimensional, $\mathbf{f}^{(2)}$ is N_2–dimensional and both together represent the drive, while $\mathbf{f}^{(3)}$ is the N_3–dimensional response ($N_1 + N_2 + N_3 = N$). The special case of (8), in which $\mathbf{f}^{(2)} = \mathbf{f}^{(3)}$ (and thus $N_2 = N_3$), leads to the concept of synchronization of chaotic subsystems. This special case is called *homogeneous driving*. The construction of this system consists of dividing the initial system (4) into two subsystems $\mathbf{f}^{(1)}$ and $\mathbf{f}^{(2)}$. Then the subsystem $\mathbf{f}^{(2)}$ (which will not be used for driving $\mathbf{f}^{(3)}$) is duplicated. This duplicate is applied as response. How to divide the drive is determined by calculating the conditional *Lyapunov exponents* [PC91], [Sch89]. If the conditional Lyapunov exponents of $\mathbf{f}^{(2)}$ driven by $\mathbf{x}^{(1)}$ are all negative, the state variables of $\mathbf{f}^{(2)}$ and $\mathbf{f}^{(3)}$ synchronize.

PECORA and CARROLL apply the idea of homogeneous driving to the Lorenz and Rössler chaotic systems as well as to the hysteretic electronic circuit and its numerical model [PC91]. In all these threedimensional systems, chaotic synchronization is achieved with respect to the initial value and parameter stability conditions. The channel noise stability was not considered.

Based on the homogeneous driving principle and using an inverse subsystem, a model of remote chaos replication can be constructed, as shown in figure 1.

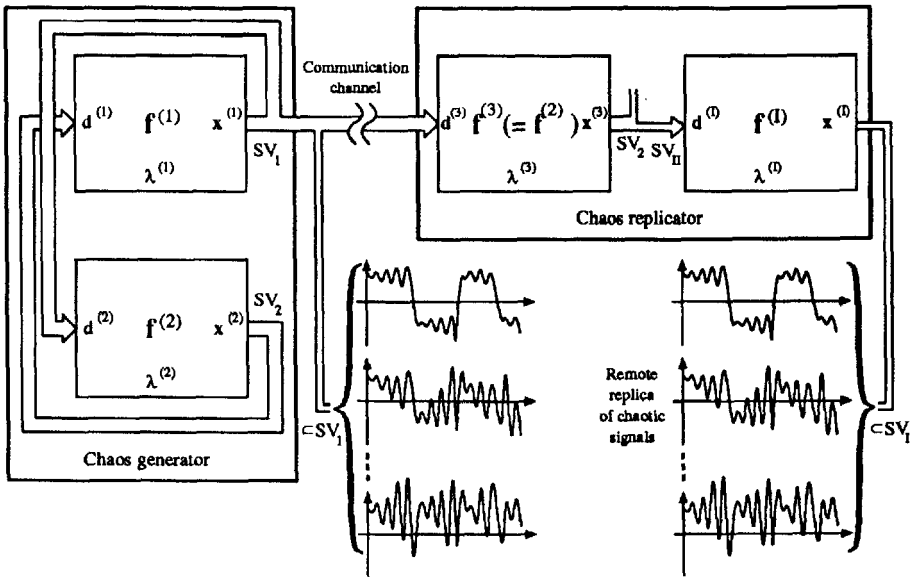

Fig. 1. The model of remote chaos replication.

4 Cryptosystems based on Remote Chaos Replication

Using the model of remote chaos replication, a secret key cryptosystem for analog communication channels can be formulated. For this purpose, only one replica of the chaotic signals in SV_1 is required, i.e., $N_1 = 1$, $\mathbf{x}^{(1)}(t) = x_1^{(1)}(t)$, $\mathbf{x}^{(I)}(t) = x_1^{(I)}(t)$ and $\lim_{t\to\infty} \left| x_1^{(I)}(t) - x_1^{(1)}(t) \right| = 0$. At the transmitter side, this system is an analog variant of the VERNAM–cipher system, because the chaotic signal $x_1^{(1)}(t)$ is added (real addition) to the information–bearing signal $s(t)$ so that their sum $c(t)$ represents the channel input signal (see figure 2). The random key space could be the subset $\boldsymbol{\lambda}_k \subseteq \boldsymbol{\lambda}^{(2)} \cup \boldsymbol{\lambda}^{(I)}$ of all values of parameters of $(\mathbf{f}^{(2)} \cup \mathbf{f}^{(I)}) \cap (\mathbf{f}^{(2)} \cup \mathbf{f}^{(1)})$ that cause chaotic regime in the chaos generator with mutually different strange attractors.

At the receiver side, this system principally differs from VERNAM–cipher systems. Here, the channel disturbance stability of the subsystem $\mathbf{f}^{(3)}$ in the chaos replicator enables the auto–synchronization and the recovery of the information–bearing signal $s(t)$. The additive disturbance $\delta(t) = \delta_1(t)$ in the communication channel is $\delta_1(t) = s(t) + n(t)$, where $n(t)$ represents the equivalent additive channel noise. If the actual disturbance–to–chaos ratio D/C is smaller than the limit

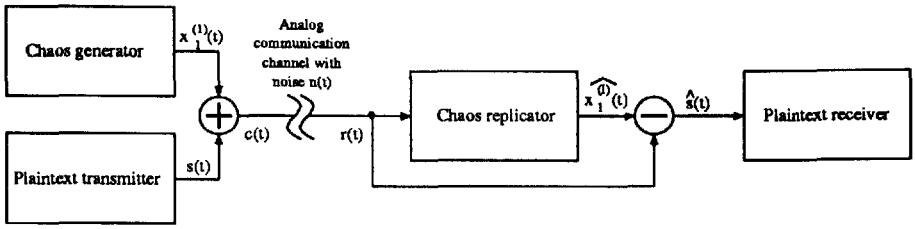

Fig. 2. The model of the cryptosystem based on remote chaos replication.

value $\overline{D/C}$, the chaos replicator with input signal $r(t) = c(t) + n(t)$ yields the chaotic signal $\widehat{x_1^{(I)}}(t) = x_1^{(I)}(t) + \sigma(t)$ at its output, which is more or less synchronized with the output $x_1^{(1)}(t)$ of the chaos generator at the transmission side. Here, $\sigma(t)$ represents the equvalent additive synchronization noise caused by momentary losses of synchronization. By subtraction of $\widehat{x_1^{(I)}}(t)$ from $r(t)$ an additive mixture of information–bearing signal, channel and synchronization noise is obtained. If the power of the signal $x_1^{(1)}(t)$ is much greater than the power of $s(t)$, then the information–bearing signal $s(t)$ will be masked by the unpredictable chaotic signal. However, the information–bearing signal must have some minimal power in order not to be masked by channel and synchronization noise.

This cryptosystem was proposed by A. OPPENHEIM and his coworkers without specifying what is the key, if any, in the system [OWIC92]. An example of masking and recovering a segment of a speech signal using the chaotic LORENTZ–system was demonstrated by computer simulation. The influence of the channel noise and the parameter stability of the system was not considered.

An experimental demonstration of the cryptosystem based on remote chaos replication was recently realized using Chua's circuit as chaos generator [KHE92]. This circuit is a very simple and robust electronic circuit built up with four linear elements and one nonlinear element called Chua's diode (CD). The circuit is shown in figure 3(a), and the state equations are given by

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \boldsymbol{\lambda}) = \begin{cases} \dot{x_1} = f_1(x_1, x_2, \lambda_1, \lambda_4, \lambda_5, \lambda_6, \lambda_7) = \frac{1}{\lambda_1}\left(\frac{x_2 - x_1}{\lambda_4} - h\right), \\ \dot{x_2} = f_2(x_1, x_2, x_3, \lambda_2, \lambda_4) \quad\quad = \frac{1}{\lambda_2}\left(\frac{x_2 - x_1}{\lambda_4} + x_3\right), \\ \dot{x_3} = f_3(x_2, \lambda_3) \quad\quad = \frac{1}{\lambda_3}(-x_2), \end{cases} \tag{9}$$

where $h = h(x_1, \lambda_5, \lambda_6, \lambda_7)$ is the piecewise linear characteristic of Chua's diode, as shown in figure 3(b). Here, x_1 is the voltage across the capacitor $C_1 = \lambda_1$, x_2 is the voltage across the capacitor $C_2 = \lambda_2$, and x_3 is the current through the inductor $L = \lambda_3$. The parameter λ_4 is the resistance R, while λ_5 and λ_6 are slopes of the inner and outer regions of h, and λ_7 indicates the breakpoints of h (for details see [Ken92]).

Using the principle of homogeneous driving, the Chua's circuit was decomposed in the following way: $\mathbf{f}^{(1)} = f_1$, $\mathbf{f}^{(2)} = (f_2, f_3)$, and $\mathbf{f}^{(I)} = f_1$, so that

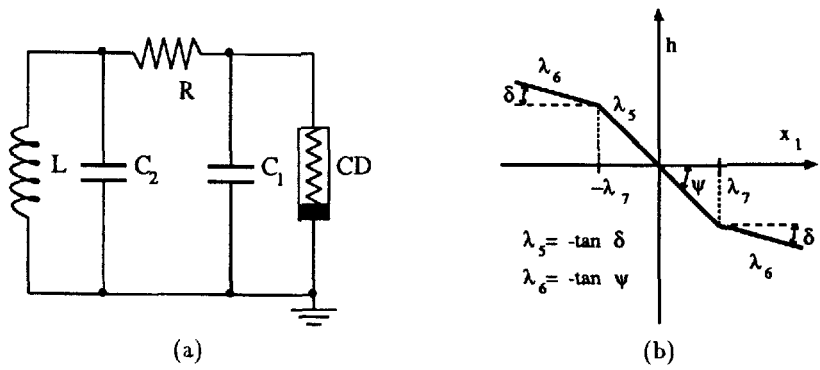

Fig. 3. (a) Chua's circuit, (b) the characteristic of Chua's diode.

$x_1(t) = x_1^{(1)}(t)$ (voltage across C_1) was used as a masking signal. The information-bearing signal $s(t)$ was a sine wave of frequency taken from the interval between 10% and 90% of the natural frequency of the RÖSSLER-type attractor. With an S/N-ratio (in this case D/C-ratio) of approximately -6 dB, the signal loss at the receiver was limited to less than -2 dB (-4 dBV). This signal loss is affected by momentary losses of synchronization which occur during some transitions between two Rössler-type attractors. The influence of the channel noise and the parameter stability was not considered.

Using these arguments and the fact that the sine wave $s(t)$ was not recognizable in the spectrum of $x_1(t)$, the authors of [KHE92] believe that this is sufficient to demonstrate a secure communication. It was not considered whether there should be a key in the proposed system, what it should consist of, and how it would be managed.

5 Cryptanalysis of Cryptosystems based on Remote Chaos Replication

There are basically three possibilities for the cryptanalysis of cryptosystems based on remote chaos replication:

- The extraction of the information-bearing signal $s(t)$ from the channel output signal $r(t)$,
- the extraction of the chaotic masking signal $x_1(t)$ from $r(t)$, and
- the estimation of parameters of the chaos replicator, which are chosen from the key space $\boldsymbol{\lambda}_k$ of the cryptosystem.

The extraction of the information-bearing signal is generally possible if $s(t)$ is a periodic signal or consists of periodic frames with sufficient duration, e. g., different types of low-rate digital modulations. Detection by autocorrelation and

crosscorrelation used in radar signal processing and various other communication systems enables an effective extraction of $s(t)$ even at very low S/N–ratio [Lee64]. As these techniques are commonly known, we won't explain their use here. It should be noted that the demonstration of security in [KHE92] was done using just a periodical signal.

If the information–bearing signal doesn't contain long–term periodical components, the next possibility is the extraction of the masking signal $x_1(t)$ from $r(t)$. Lower–dimensional continuous time systems in chaotic regime always generate signals containing unpredictable repetitions of similar signal patterns that can generally be described as one parameterized function with a small number of parameters. Finding such a function and estimation of its actual parameters using the channel output signal $r(t)$ is the main task at this approach. From an information theoretic point of view, this parameter estimation can be done with sufficient accuracy since the S/N–ratio for the masking signal $x_1(t)$ is very high so that this communication system operates far below the channel capacity which makes it unsecure as a cryptosystem. The approach is demonstrated for the cryptosystem based on Chua's circuit.

Since the Chua's circuit contains the piecewise linear Chua's diode, the chaotic masking signal $x_1(t)$ behaves in a linear fashion as long as $x_1(t)$ remains within one linear segment of the characteristic shown in figure 3(b). For each of these time frames, the Laplace transform of $x_1(t)$ can be calculated and is of the following form:

$$X_1(s) = \frac{P(s)}{Q(s)} = \frac{s^3a_3 + s^2a_2 + sa_1 + a_0}{s(s-s_1)(s-s_2)(s-s_3)} = \frac{s^3a_3 + s^2a_2 + sa_1 + a_0}{s(s^3 + s^2b_2 + sb_1 + b_0)}, \tag{10}$$

where

$$s_1 = U + V - \frac{b_2}{3},$$
$$s_2 = -\frac{3U + 3V + 2b_2}{6} + i\sqrt{3}\frac{U - V}{2},$$
$$s_3 = -\frac{3U + 3V + 2b_2}{6} - i\sqrt{3}\frac{U - V}{2},$$

$$U = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}, \quad V = \sqrt[3]{-\frac{q}{2} - \sqrt{D}}, \quad D = \frac{p^3}{27} + \frac{q^2}{4},$$

$$p = b_1 - \frac{b_2^2}{3}, \quad q = \frac{2b_2^3}{27} - \frac{b_2}{3} + b_0,$$

$$b_0 = \frac{\lambda^* + \lambda_4}{\lambda_1\lambda_2\lambda_3\lambda_4\lambda^*}, \quad b_1 = \frac{\lambda_1\lambda_4\lambda^* + \lambda_3}{\lambda_1\lambda_2\lambda_3\lambda_4\lambda^*}, \quad b_2 = \frac{\lambda_2\lambda^* + \lambda_1\lambda^* + \lambda_2\lambda_4}{\lambda_1\lambda_2\lambda_4\lambda^*}.$$

Here, λ^* represents a time–variable parameter (Chua's diode inner resistance) which depends on the momentary value of the voltage $x_1(t)$, i.e.,

$$\lambda^* = \begin{cases} \frac{1}{\lambda_6} & x_1(t) < -\lambda_7, \\ \frac{1}{\lambda_5} & -\lambda_7 \leq x_1(t) < \lambda_7, \\ \frac{1}{\lambda_6} & x_1(t) \geq \lambda_7. \end{cases}$$

Accordingly, the masking signal $x_1(t)$ can be viewed as a sequence of three separate types of time frames: lower, middle and upper signal time frame with corresponding variable durations τ_l, τ_m, and τ_u in varying order, as shown in fig. 4.

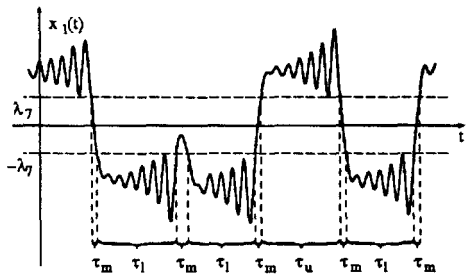

Fig. 4. A typical sample of the chaotic masking signal $x_1(t)$.

In all three types of time frames, the masking signal is, according to the inverse Laplace transform of (10), of the following form

$$x_1(t) = Ae^{at}\cos(\omega t - \phi) + Be^{bt} + g, \tag{11}$$

if $D > 0$ and s_1, s_2 and s_3 are mutually different and different from zero, which is the necessary condition for a chaotic regime. The exponents a and b and the frequency ω depend only on the poles of (10) and thus on λ_1, λ_2, λ_3, λ_4, λ_5 and λ_6

$$a = Re(s_2), \quad \omega = Im(s_2), \quad b = s_1, \tag{12}$$

while the amplitudes

$$A = 2\frac{P(s_2)}{Q'(s_2)}, \quad B = 2\frac{P(s_1)}{Q'(s_1)}, \quad g = \frac{a_0}{b_0} \tag{13}$$

and the initial phase

$$\phi = \arctan \frac{Im\frac{P(s_2)}{Q'(s_2)}}{Re\frac{P(s_2)}{Q'(s_2)}} \tag{14}$$

additionally depend on coefficients in the numerator of (10)

$$a_0 = -\frac{\lambda^0}{\lambda_1\lambda_2\lambda_3}, \tag{15}$$

$$a_1 = \frac{\lambda_1\lambda_4 x_1(0) + \lambda_3 x_3(0) - \lambda_3\lambda^0}{\lambda_1\lambda_2\lambda_3\lambda_4},$$
$$a_2 = \frac{\lambda_1 x_1(0) - \lambda_2\lambda_4\lambda^0 + \lambda_2 x_2(0)}{\lambda_1\lambda_2\lambda_4},$$
$$a_3 = x_1(0),$$

and thus on $x_1(0)$, $x_2(0)$ and $x_3(0)$ representing initial values of state variables at the beginning of each new time frame. λ^0 is, like λ^*, a time–variable parameter (Chua's diode constant current) which depends on the momentary value of the voltage $x_1(t)$, i.e., on the actual time frame

$$\lambda^0 = \begin{cases} \lambda_7(\lambda_5 - \lambda_6) & x_1(t) < -\lambda_7, \\ 0 & -\lambda_7 \le x_1(t) < \lambda_7, \\ \lambda_7(\lambda_6 - \lambda_5) & x_1(t) \ge \lambda_7. \end{cases}$$

Having a general form (11) of the masking signal, this cryptanalysis approach (the extraction of the chaotic masking signal $x_1(t)$ from $r(t)$) reduces to the classical techniques of multiple real parameter estimation of the known signal form in the presence of additive noise [vT71]. Here, an adaptive suboptimal estimation method will be used which is relatively simple but accurate enough to demonstrate the extraction of the masking signal.

By iterated differentiation of (11) one finds the following series of equations:

$$-(a^2+\omega^2)b(x_1(t)-g) + (a^2+\omega^2+2ab)x_1^{(1)}(t) + \\ -(2a+b)x_1^{(2)}(t) + x_1^{(3)}(t) = 0 \qquad (16a)$$

$$-(a^2+\omega^2)bx_1^{(k)}(t) + (a^2+\omega^2+2ab)x_1^{(k+1)}(t) + \\ -(2a+b)x_1^{(k+2)}(t) + x_1^{(k+3)}(t) = 0, \qquad (16b)$$

where $x_1^{(k)}(t)$ is the k–th order derivative of $x_1(t)$. Since the power of $x_1(t)$ dominates that of $s(t)$ in order to allow auto–synchronization of the chaos replicator, the parameters of $x_1(t)$ can be estimated quite accurately with appropriately smoothed derivatives of the sampled channel output signal $r(t) = x_1(t) + s(t)$, so that

$$\widehat{x_1^{(k)}}(t) = r(t) * g^{(k)}(t) = r^{(k)}(t) * g(t), \qquad (17)$$

where

$$g(t) = \frac{s}{\sqrt{2\pi}} e^{-\frac{(st)^2}{2}}$$

is the Gaussian bell curve controlled by the scaling factor s, $s > 0$, and $*$ denotes convolution. Using (16b) for three consecutive values of k yields the following system of linear equations

$$\begin{pmatrix} \widehat{x_1^{(k)}} & \widehat{x_1^{(k+1)}} & \widehat{x_1^{(k+2)}} \\ \widehat{x_1^{(k+1)}} & \widehat{x_1^{(k+2)}} & \widehat{x_1^{(k+3)}} \\ \widehat{x_1^{(k+2)}} & \widehat{x_1^{(k+3)}} & \widehat{x_1^{(k+4)}} \end{pmatrix} \begin{pmatrix} \hat{b}(\hat{a}^2+\hat{\omega}^2) \\ -\hat{a}^2-\hat{\omega}^2-2\hat{a}\hat{b} \\ 2\hat{a}+\hat{b} \end{pmatrix} = \begin{pmatrix} \widehat{x_1^{(k+3)}} \\ \widehat{x_1^{(k+4)}} \\ \widehat{x_1^{(k+5)}} \end{pmatrix}, \qquad (18)$$

whose solution is

$$\begin{pmatrix} \hat{b}(\hat{a}^2+\hat{\omega}^2) \\ -\hat{a}^2-\hat{\omega}^2-2\hat{a}\hat{b} \\ 2\hat{a}+\hat{b} \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \tag{19}$$

$$= \frac{1}{-\widehat{x_1^{(k+2)}}+2\widehat{x_1^{(k+1)}}\widehat{x_1^{(k+2)}}\widehat{x_1^{(k+3)}}-\widehat{x_1^{(k)}}\widehat{x_1^{(k+3)}}^2-\widehat{x_1^{(k+1)}}^2\widehat{x_1^{(k+4)}}+\widehat{x_1^{(k)}}\widehat{x_1^{(k+2)}}\widehat{x_1^{(k+4)}}} \cdot$$

$$\begin{pmatrix} -\widehat{x_1^{(k+3)}}^2+\widehat{x_1^{(k+2)}}\widehat{x_1^{(k+4)}} & \widehat{x_1^{(k+2)}}\widehat{x_1^{(k+3)}}-\widehat{x_1^{(k+1)}}\widehat{x_1^{(k+4)}} & -\widehat{x_1^{(k+2)}}^2+\widehat{x_1^{(k+1)}}\widehat{x_1^{(k+3)}} \\ \widehat{x_1^{(k+2)}}\widehat{x_1^{(k+3)}}-\widehat{x_1^{(k+1)}}\widehat{x_1^{(k+4)}} & -\widehat{x_1^{(k+2)}}^2+\widehat{x_1^{(k)}}\widehat{x_1^{(k+4)}} & \widehat{x_1^{(k+1)}}\widehat{x_1^{(k+2)}}-\widehat{x_1^{(k)}}\widehat{x_1^{(k+3)}} \\ -\widehat{x_1^{(k+2)}}^2+\widehat{x_1^{(k+1)}}\widehat{x_1^{(k+3)}} & \widehat{x_1^{(k+1)}}\widehat{x_1^{(k+2)}}-\widehat{x_1^{(k)}}\widehat{x_1^{(k+3)}} & -\widehat{x_1^{(k+1)}}^2+\widehat{x_1^{(k)}}\widehat{x_1^{(k+2)}} \end{pmatrix} \cdot \begin{pmatrix} \widehat{x_1^{(k+3)}} \\ \widehat{x_1^{(k+4)}} \\ \widehat{x_1^{(k+5)}} \end{pmatrix}$$

Solutions of the system of nonlinear equations (18) in $\hat{b}$, $\hat{a}$, and $\hat{\omega}$ represent the estimations of b, a and ω

$$\hat{b} = u + v + \frac{\gamma}{3}, \tag{20}$$

$$\hat{a} = \frac{-\hat{b}-\gamma}{2}, \tag{21}$$

$$\hat{\omega} = \sqrt{-\hat{a}^2 - 2\hat{a}\hat{b} - \beta}, \tag{22}$$

where

$$f = -\beta - \frac{\gamma^2}{3}, \quad h = -\frac{2\gamma^3}{27} + \frac{\gamma}{3} - \alpha,$$

$$d = \frac{f^3}{27} + \frac{h^2}{4}, \quad u = \sqrt[3]{-\frac{h}{2} + \sqrt{d}}, \quad v = \sqrt[3]{-\frac{h}{2} - \sqrt{d}}.$$

The DC term g is estimated by substitution of $\hat{a}$, $\hat{b}$ and $\hat{\omega}$ in equation (16a). The equations

$$\chi = Ae^{at}\widehat{\cos(\omega t - \phi)} = \frac{(\hat{b}^2 - 2\hat{a}\hat{b})(\widehat{x_1} - \hat{g}) + 2\hat{a}\widehat{x_1^{(1)}} - \widehat{x_1^{(2)}}}{(\hat{a}-\hat{b})^2 + \hat{\omega}^2}$$

$$\sigma = Ae^{at}\widehat{\sin(\omega t - \phi)} =$$

$$\frac{\hat{b}(\hat{a}\hat{b} - \hat{a}^2 + \hat{\omega}^2)(\widehat{x_1} - \hat{g}) + \widehat{x_1^{(1)}}(\hat{a}^2 - \hat{b}^2 - \hat{\omega}^2) + \widehat{x_1^{(2)}}(\hat{b} - \hat{a})}{\hat{\omega}((\hat{a}-\hat{b})^2 + \hat{\omega}^2)}$$

obtained from (11) and its derivatives, allow the estimations of ϕ, Ae^{at} and Be^{bt}

$$\hat{\phi} = \arctan\frac{\sigma}{\chi}, \tag{23}$$

$$\widehat{Ae^{at}} = \sqrt{\sigma^2 + \chi^2} \tag{24}$$

$$\widehat{Be^{bt}} = \frac{(\widehat{x_1} - \hat{g})(\hat{a}^2 + \hat{\omega}^2) - 2\hat{a}\widehat{x_1^{(1)}} + \widehat{x_1^{(2)}}}{(\hat{a}-\hat{b})^2 + \hat{\omega}^2}. \tag{25}$$

With these results, a program with graphic interaction was written that reads in the sampled channel output signal, performs the calculations and displays the estimated parameters of (11). It then synthesizes a signal which is subtracted from the input signal, leaving the signal for which masking was attempted with considerably reduced chaotic masking component. Experiments with this program using speech signals 15 dB below the masking signal that were initially not audible reproduced the speech signals in clearly understandable quality. The influence of the channel noise and parameter stability of the system was not considered. It should be noted that in the upper and lower signal time frames the exponent b is always negative and the component Be^{bt} is rather weak. Its neglection leads to a much simpler estimation process and gives relatively good results, too.

The third mentioned cryptanalysis approach consisting of the estimation of the chaos replicator's parameters directly follows from the presented results. It was not addressed here since the described method gives sufficient results for the cryptanalysis of the cryptosystem based on Chua's circuit. We only point out that the back–substitution of the estimated parameters in (10), (12), (13) and (14) or the coefficient comparison of (9) in its third order differential equation form with (16) makes the estimation of the unknown parameters from the key space λ_k possible.

6 Conclusions

The presented cryptanalysis method of extracting the chaotic masking signal from the channel output signal breaks the cryptosystem using Chua's circuit for all types of information–bearing signals. This method is applicable for all other cryptosystems based on the remote chaos replication principle where the functional form of the masking signal or its dominating components can be revealed from the structure of the chaos generator. For three–dimensional and some other lower–dimensional chaotic continuous–time systems this is always possible by using adequate linearization techniques. Having the functional form, the dominating power of the chaotic masking signal necessary for the auto–synchronization of the cryptosystem always enables a sufficiently accurate estimation of remaining unknown parameters. Cryptosystems of this type based on higher–dimensional continuous–time chaotic systems would require much higher cryptanalytic effort. For such systems however, the realization of auto–synchronization based on only one state variable (the masking signal) is still an open problem [PC91].

Acknowledgements

We would like to thank Michael Pal, student at our institute, for his valuable aid in the verification of the presented methods.

References

[BVKC93] Belykh, V. N., Verichev, N. N., Kocarev, Lj., and Chua, L. O., "On chaotic synchronization in a linear array of Chua's circuits", *Journal of Circuits, Systems and Computers*, Vol. 3, no. 2, pp. 579–589, 1993.

[CKEI92] Chua, L. O., Kocarev, Lj., Eckert, K., and Itoh, M., "Experimental chaos synchronization in Chua's circuit", *IBID*, pp. 705–708, 1992.

[GH90] Guckenheimer, L. and Holmes, P., *Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields*, Applied Mathematical Sciences, Springer-Verlag, 1990.

[Ken92] Kennedy, M. P., "Robust op amp realization of Chua's circuit", *Frequenz*, Vol. 46, no. 3–4, pp. 66–80, 1992.

[KHE92] Kocarev, Lj., Halle, K. S., Eckert, K., Chua, L. O., and Parlitz, U., "Experimental demonstration of secure communications via chaotic synchronization", *International Journal of Bifurcation and Chaos*, Vol. 2, no. 3, pp. 709–713, 1992.

[Lee64] Lee, Y. W., *Statistical Theory of Communication*, John Wilcy & Sons, 1964.

[OWIC92] Oppenheim, A. V., Wornell, G. W., Isabelle, S. H., and Cuomo, K. M., "Signal processing in the context of chaotic signals", *Proc. 1992 IEEE ICASSP*, Vol. IV, pp. 117–120, 1992.

[PC89] Parker, T. S. and Chua, L. O., *Practical Numerical Algorithms for Chaotic Systems*, Springer-Verlag, 1989.

[PC90] Pecora, L. M. and Carroll, T. L., "Synchronization in chaotic systems", *Physical Review*, Vol. 64, no. 8, pp. 821–824, 1990.

[PC91] Pecora, L. M. and Carroll, T. L., "Driving system with chaotic signals", *Physical Review*, Vol. 44, no. 4, pp. 2374–2383, 1991.

[PCK92] Parlitz, U., Chua, L. O., Kocarev, Lj., Halle, K. S., and Shang, A., "Transmission of digital signals by chaotic synchronization", *International Journal of Bifurcation and Chaos*, Vol. 2, no. 4, pp. 937–977, 1992.

[Per91] Perko, L., *Differential Equations and Dynamical Systems*, Texts in Applied Mathematics, Springer–Verlag, 1991.

[Sch89] Schuster, H. G., *Deterministic Chaos*, VCH, Germany, 1989.

[Sha49] Shannon, C. E., "Communication theory of secrecy systems", *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.

[Sha93] Shannon, C. E., "Analogue of the Vernam system for continuous time series", In Sloane, N. J. A. and Wyner, A. D., editors, *Claude Elwood Shannon: Collected Papers*, Memorandum MM 43–110–44, Bell Laboratories, 1943, pp. 144–147, IEEE Press, 1993.

[Sim79] Simmons, G. J., "The mathematics of secure communication", *Math. Intell. 1*, pp. 233–246, 1979.

[Ver26] Vernam, G. S., "Cipher printing telegraph systems for secret wire and radio telegraphic communications", *J. Am. Inst. Elec. Eng.*, Vol. 55, pp. 109–115, 1926.

[vT71] van Trees, H. L., *Detection, Estimation and Modulation Theory*, Number Part I, II and III, John Wiley and Sons, Inc., New York, 1968, 1971, 1971.