Transmission of Binary Information with a Chaos Coded Communication System using QDPSK-Modulation*

Andreas Magauer and Soumitro Banerjee[a]

Member IEEE, Abteilung für Elektronik und Informatik, Höhere Technische Bundeslehranstalt Salzburg, A-5020 Salzburg

[a] Member IEEE, Department of Electrical Engineering, Indian Institute of Technology Kharagpur – 721302, India

Z. Naturforsch. **53 a,** 1022–1028 (1998); received November 20, 1998

Synchronisation of chaotic oscillators offers a way of practical application of the theory of Chaos in obtaining secure communication. In this work we introduce a nonautonomous chaotic system with sinusoidal external force for communication of binary signals. The information is applied to the phase position of the sinusoidal forcing signal of the chaotic oscillator using a quadrature difference phase shift keying (QDPSK) modulation. An inverse synchronisation system approach with direct modulation is applied. We describe the system in detail and discuss the requirements of a secure communication system. Issues related to bit error rate, transfer rate, signal to noise ratio, channel bandwidth, bandwidth efficiency and channel capacity are discussed, and the properties of the realized communication system are placed in relation to the requirements of a secure communication system.

Key words: Chaos; Synchronisation; Encryption; Communication; PSK-Modulation.

1. Introduction

The evolution of chaos theory has caused much euphoria among the mathematicians and physicists, while the engineering community has observed the development with scepticism. If an engineer comes across a chaotic phenomenon, he generally tries to suppress it. But recently, the application of chaos for secure communication has opened the possibility of an active role of chaos theory in engineering systems.

In this application one uses a transmitter system with chaotic behavior. An information carrying signal is injected into the chaotic transmission system. The transmitted information thus gets mixed with the chaotic signal, and it becomes almost impossible to distinguish it from a random noise. The receiver performs the inverse operation of the transmitter and recovers the information.

To realize this objective, it is necessary for the receiver to have a chaos generator. Not only that, the chaotic waveform of the receiver should be identical with that of the transmitter. This implies that the two chaotic systems must be *synchronised*.

Not obvious is the question of the conditions for synchronising chaotic systems. Is it possible to synchronise a system running in chaotic mode to another chaotic system? Will not a small difference between the initial values of two identical systems effect an exponential divergence of the oscillation?

It is the driving signal that forces the receiver system to follow the time evolution of the transmitter system. We say that the receiver system synchronises with the transmitter system if

$$\lim_{t \to \infty} |F_{\mathrm{T}}(t) - F_{\mathrm{R}}(t)| = 0$$

for any combination of the initial values. $F_{\mathrm{T}}(t)$ is the transmitted signal and $F_{\mathrm{R}}(t)$ the received signal. In nonautonomous chaotic systems, synchronisation is achieved if the undriven receiver system is asymptotic stable. A generalized synchronization criterion in directionally coupled chaotic systems is explored in [1], and an extension to unidirectionally coupled systems is discussed in [2]. Further, synchronisation has been demonstrated in [3] for a typical nonautonomous system—the RL-diode oscillator.

* Vorgetragen auf der 7. Jahrestagung des Vereins zur Förderung der Erforschung nichtlinearer Dynamik e. V., München, 15. Nov. 1997.

Reprint requests to Dr. A. Magauer; E-mail: magauer@ieee.org.

0932–0784 / 98 / 1200–1022 $ 06.00 © Verlag der Zeitschrift für Naturforschung, Tübingen · www.znaturforsch.com

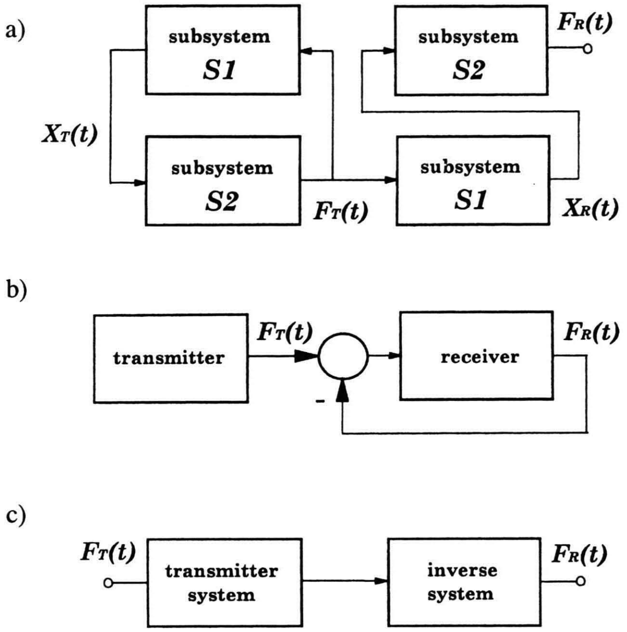

Fig. 1. Block schematic of the synchronisation methods.

Three methods for synchronisation are available in literature [4, 5]. These are described below and the corresponding block schematics is shown in Figure 1a - c.

1. *Decomposition into subsystems* [6, 7] (Fig. 1a): The receiver and the transmitter are identical systems. Further, it should be possible to decompose the system into two subsystems S1 and S2, interacting only through two signals $X_T(t)$ and $F_T(t)$. $X_T(t)$ runs from S1 to S2 and $F_T(t)$ runs back from S2 to S1. At the identical receiver the input of S1 is disconnected and coupled to the transmission signal. The remaining open output $F_R(t)$ of S2 represents the synchronised output of the receiver. Synchronisation takes place if the transients have decayed and the output signal of S2 at the transmitter $F_T(t)$ and the receiver $F_R(t)$ are identical.

2. *Linear feedback* [8] (Fig. 1b): This method has been derived from automatic control applications. The output of the transmitter $F_T(t)$ and the receiver system $F_R(t)$ are compared and their difference is fed back to the input of the receiver. The amplified difference signal is used to control the state variables and to force the synchronisation of the receiver. The difference signal is zero when the synchronisation state is obtained.

3. *Inverse system* [9, 3, 10] (Fig. 1c): If the receiver system performs an opposite operation by injection of a chaotic signal, the method is called inverse system synchronisation. This method is a direct transposition of the synchronisation of chaotic systems and suitable for nonautonomous systems.

Further, three methods for injection of information to the transmitter system are known:

1. *Chaotic masking* [11, 12]: The additive coupling of the information at the chaotic transmitter signal and their recovery through subtraction from the synchronised receiver signal is called chaotic masking. For the sake of security of transmission, the information signal must be small compared to the chaotic carrier. This fact also demonstrates the sensitivity to channel noise.

2. *Chaotic switching* [13]: If in the transmitter one parameter is switched chaotically between two values the method is called chaotic switching. Two receiver systems R1 and R2 are required, each for one of the different parameter values of the transmitter. Depending on the transmitter stage one of the receivers synchronises with the transmitter after a determined time. Synchronisation of R1 means logic low and synchronisation of R2 means logic high. Hence, the method is only used for binary communications and has the disadvantage of a waiting period for every new synchronisation state. This causes a reduced communication speed.

3. *Chaotic modulation* [9, 5]: If in the transmitter one parameter is directly coupled to the information signal, the method is called chaotic modulation or direct modulation. The receiver operates as an inverse synchronisation system. The synchronised state is held permanently, therefore a high communication speed is obtained.

In the present work we have realized a chaos synchronisation based secure communication system using the inverse system synchronisation approach with direct modulation as information injection. We describe the system and present its properties in relation to the following requirements of a secure communication system from the point of communication engineering:

1. High security against illegal listeners at the transmission line, supported by a close tolerance of the system parameters.

2. Low bit error rate (BER) caused by the immunity against noise and disturbance.

3. High efficiency of the transmission channel, high ratio between maximum value of bit transfer rate and required channel bandwidth, large tolerable range of the channel attenuation.

4. Simple adjustment of the receiver with appropriate tolerance band of the parameters without continuous adjusting.

5. Limited requirement of constancy of the system parameters which are likely to vary depending on the temperature and other environmental influences.

2. System Equation and Synchronisation Principle

The chaos generator used in the present work is a sinusoidal forced nonautonomous piecewise linear oscillator similar to the Duffing oscillator. Its chaotic behavior has been reported in [14] in detail. The state equation is

$$\omega_0^2 X''(t) + 2D\,\omega_0\, X'(t) + X(t) = f(X) + Z(t)\ ,(1)$$

where the nonlinear function is given by

$$f(X(t)) = U(t) = \tfrac{1}{2}\,\mathrm{sign}[X(t)] \qquad (2)$$

and the sinusoidal forcing signal is

$$Z(t) = A\,\cos[\omega_F\, t + \Phi]\,. \qquad (3)$$

The system parameters, i.e., the normalised amplitude A of external action, the frequency $f_F = \omega_F/2\pi$ of external forcing, damper coefficient D and resonance frequency $f_0 = \omega_0/2\pi$ of the linear subsystem are chosen at the values $A = 0.5$, $f_F = 10.3$ kHz, $D = 0.055$ and $f_0 = 10.0$ kHz, to provide oscillations in the chaotic mode. Figure 2 shows the corresponding experimentally obtained Poincaré map of the signals $X'(t)$ and $X(t)$. The variables have been sampled at the zero crossing of the sinusoidal external action.

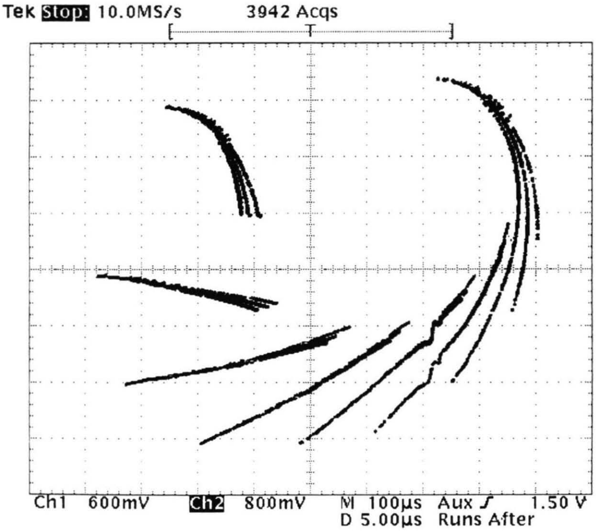

Fig. 2. Poincaré-map in chaotic mode.

We adopt the following notation for the initial conditions: X_0 the initial value of the signal $X(t)$, X_0' the corresponding initial value of the derivative of $X'(t)$ with respect to time, and Φ the starting phase of the forcing signal.

The linear subsystem derived from the homogenous part of the differential equation (1) can be described by Laplace transform. The corresponding transfer function $G(s)$ in the s-domain is

$$G\ (s) = \frac{1}{\frac{s^2}{\omega_0^2} + 2\,D\,\frac{s}{\omega_0} + 1}\,. \qquad (4)$$

This function allows the preparation of a schematic block diagram like Figure 3. $f(X)$ and $G(s)$ with the forcing signal $Z(t)$ give a simple feedback system, which runs in chaotic mode for some parameter values. The synchronisation is based on the inverse system synchronisation approach with direct modulation as information injection. The phase position Φ of the forcing signal (3) was used as the modulation parameter. Figure 3 shows the transmitter, the chaotic synchronisation line, and the receiver.

The second subsystem $G(s)$ at the transmitter denotes the linear filtering of the sinusoidal signal $Z(t)$ to $F_T(t)$. After the transients have decayed, the synchronised state is reached and the signals $F_R(t)$ at the receiver and $F_T(t)$ at the transmitter are identical. While in the transmitter the subsystem $G(s)$ receives the signal $U(t) + Z(t)$, at the receiver only the signal $U(t)$ is filtered to $Y(t)$ by $G(s)$. Because of the linear behavior of $G(s)$ the output signal $X(t)$ at the transmitter can also be composed by superposition of the filtered parts of $Z(t)$ and $U(t)$. Therefore the difference between the output of $G(s)$ at the transmitter and that at the receiver is $Z(t)$ filtered by $G(s)$ to $F_R(t)$. This difference is obtained by subtraction at the output of the receiver

$$F_R(t) = X(t) - Y(t)\,.$$

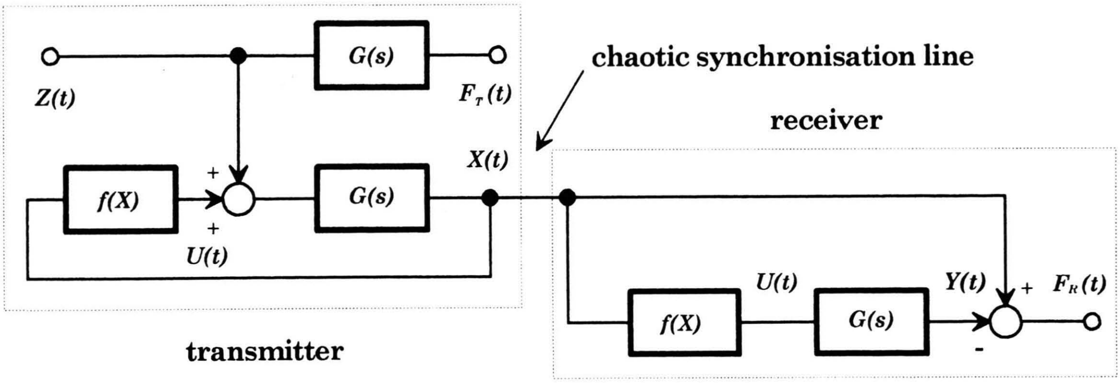

Fig. 3. The synchronisation principle.

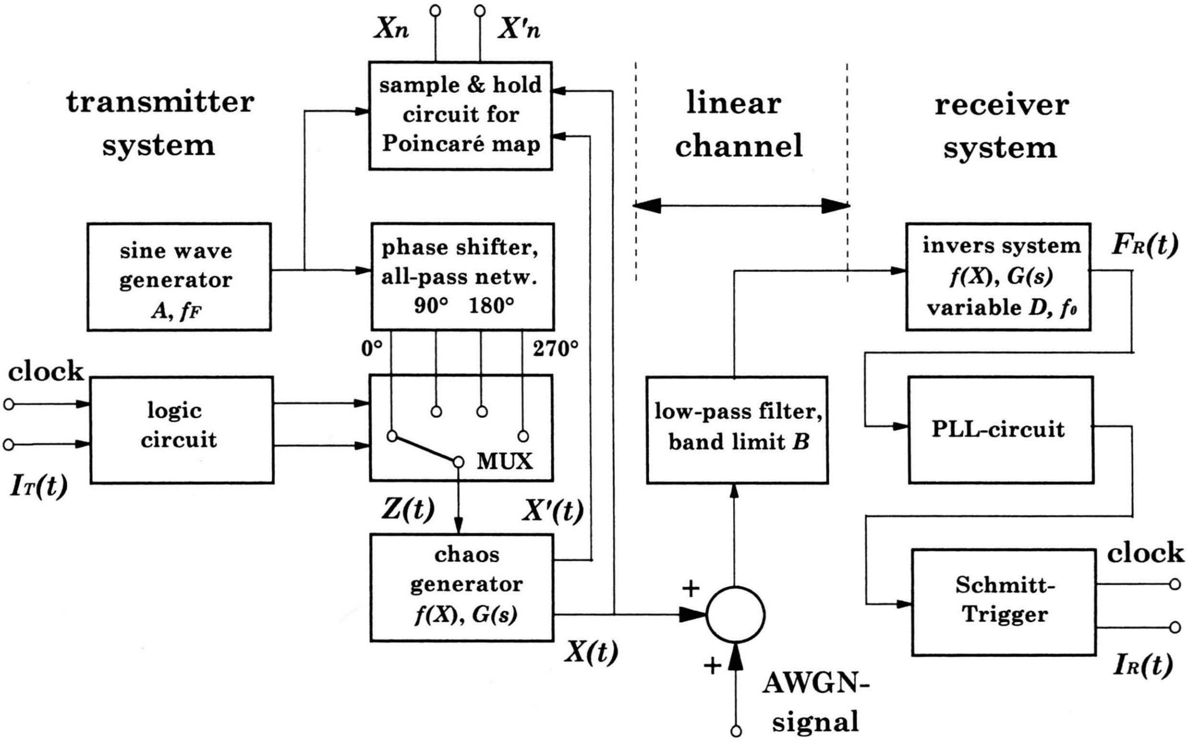
Xn
X'n
transmitter system
sample & hold circuit for Poincaré map
linear channel
receiver system
sine wave generator A, fF
phase shifter, all-pass netw. 90° 180°
0°
270°
invers system f(X), G(s) variable D, f0
FR(t)
clock
logic circuit
MUX
IT(t)
low-pass filter, band limit B
PLL-circuit
Z(t)
X'(t)
chaos generator f(X), G(s)
X(t)
+
+
AWGN-signal
Schmitt-Trigger
clock
IR(t)

Fig. 4. Block schematic diagram of the communication system.

A requirement for the synchronisation is the equality of $f(X)$ and $G(s)$ at the receiver and the transmitter. Consequently, the parameters D and ω_0 at the two points have to be identical. The exact agreement of all parameters at the transmitter and the receiver is not realistic in real systems, so the synchronisation can only be done approximately. Therefore the relation between $F_R(t)$ and $F_T(t)$ must be corrected to $F_R(t) \sim F_T(t)$ at the synchronised state.

3. Realisation

The block diagram in Fig.4 shows the realisation of the communication system. The binary information

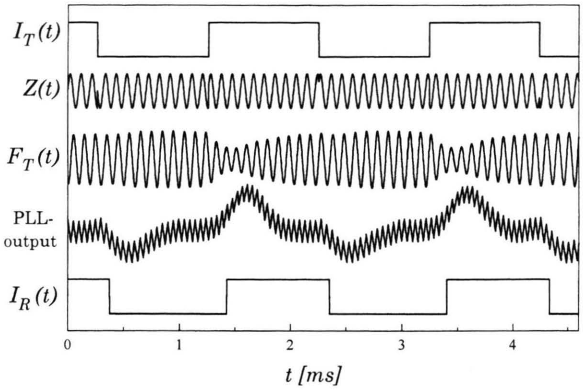

Fig. 5. Binary information signals with phase steps of +90° and −90°.

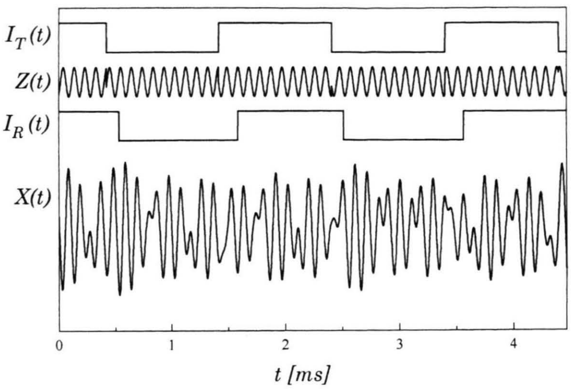

Fig. 6. The information and the corresponding chaotic transmission signal.

is injected into the transmitter as the phase position Φ of the forcing signal $Z(t)$ (3) by phase steps of +90° and −90°. According to the sign of the phase step the logic states high (sign +) and low (sign −) of the information signal $I_{\mathrm{T}}(t)$ follow. This method is called QDPSK (quadrature difference phase shift keying). Also a 8-DPSK modulation is sometimes used, where a minimum phase step of 45° allows a tripling of the transfer rate. At the transmitter four sinusoidal signals with the same amplitude and shifted by 90° are generated by an all-pass network. The binary information is retrieved at the receiver through conversion of the phase information into an electrical voltage using a PLL (Phase Locked Loop). A Schmitt-Trigger improves the signal quality of the PLL output and provides the TTL voltage range of the information signal $I_{\mathrm{R}}(t)$. Figure 5 shows the information signals $I_{\mathrm{T}}(t)$ at the transmitter and $I_{\mathrm{R}}(t)$ at the receiver, the forcing signal $Z(t)$ with phase steps, the filtered signal $F_{\mathrm{R}}(t)$ and the PLL output signal. To make the picture of the different signals easy to survey, it has been prepared by simulation.

To approach a real communication system, we implement a band limitation and add an additive white Gaussian noise (AWGN) signal to the transmission channel. The variation of the channel bandwidth and the RMS-value of the noise signal allows the determination of the signal to noise ratio and the bandwidth demand of the communication system. The PSK modulation is also chosen because of the non-stringent requirement on the quality of the channel. This includes a small signal to noise ratio. A bandwidth demand reduction also takes place because of the filtering of the signal $Z(t)$ by $G(s)$ at the transmitter. Further, this action has the advantage of improving the security of the system. The frequency spectrum of the filtered phase step lies inside the frequency spectrum of the chaotic signal. Therefore it is very difficult for an illegal listener to encode the information from the transmission line. Certainly, the improved security is achieved at the cost of a reduced maximum transfer rate. This is usual in communication with encrypted information. In the actual system the signal $Z(t)$ passes for a finite length of time, depending on the damper D until the phase step can be detected in the signal $F_{\mathrm{R}}(t)$. Figure 5 shows the delay time between the phase step of signal $Z(t)$ and the PLL output signal. The higher the delay time, the lower is the maximum transfer rate.

At the transmitter the binary information is latched onto the rising edge of a clock signal. The frequency of the forcing signal f_{F} is chosen in the kHz range to reduce cost. Increase of the frequency to higher values is possible without loss of validity of the results. For controlling the chaotic mode, the Poincaré map of the transmitter is permanently monitored at an oscilloscope. For testing the sensitivity to the variation of system parameters at the receiver, the inverse system is equipped with potentiometers for damper D and frequency f_0.

4. Results

Experimental results obtained with the realised system are listed below corresponding to the numbering in Section 1.

1. Fig. 6 shows the simulation results of the information signal $I_{\mathrm{R}}(t)$ at the receiver, the forcing

signal $Z(t)$ with 90° phase steps and the corresponding chaotic signal $X(t)$ at the transmission line. No relation between the information and the chaotic signal can be observed. The security of the system is apparent from this criterion. More detailed analyses in terms of privacy and security can be found in the theory of encryption, which will not be discussed here.

2. Applying a PSK modulation in the binary communication system, the insensitiveness of signal noise at the channel is obtained. The required signal to noise ratio of the complete communication system is similar to that of the QDPSK modulation. In the literature [15, 16], a signal to noise ratio of $R = 14$ dB at a bit error rate BER = 10^{-4} is specified. In a practical digital communication system, communication is not possible if the BER is above 10^{-3}; so we only consider operation below this range. The measurement at the real system shows also a significant increase of information errors if the signal to noise ratio is decreased below the 14 dB limit.

3. Further, the simulation of the system confirms a demand of the channel bandwidth $B = 15$ kHz. The bandwidth B and the signal to noise ratio R give the required channel capacity C. Using the approach given in [15] we obtain

$$C \sim \frac{B}{3} R = 70\,\text{kbits/s}.$$

Simulation and experiment confirm a maximum information transfer rate of approximately $T \sim 3$ kbit/s. This can be increased by using the 8-DPSK modulation to $T \sim 9$ kbit/s without further demand to the channel bandwidth. The bandwidth efficiency β [17] of the channel can be calculated from the maximum transfer rate and the required channel bandwidth:

$$\beta = \frac{T}{B} \sim 20 - 60\%.$$

This factor is just good for a system of information encryption. The channel attenuation must be within a range of 6 dB without loss of synchronisation. If a higher value is required, an additional amplifier has to be applied. At least it allows the hope that a further tuning of the performance makes an industrial realisation promising.

4. First the relevant parameters which affect the equality of the transmitter and the receiver have to be clarified. The important components are the nonlinear function $f(X)$ and the linear subsystem $G(s)$ shown in Figure 3. By (4), $G(s)$ is given only by the known parameters: damper D and resonant frequency f_0. However, the variation of the characteristic of $f(X)$ is not obvious. Further, the difference between the formula (2) and the practical realisation has to be considered. In (2) only the multiplication factor 1/2 can be identified as a value which can be adjusted. At the real circuit the signum function is built by a comparator switching at the zero crossing of the input signal. Therefore the symmetry or the offset of the comparator function also has to be adjusted. If the equality of the four parameters damper D, resonant frequency f_0, multiplication factor 1/2 and the symmetry of $f(X)$ is guaranteed, we can say the receiver satisfies the inverse function of the transmitter exactly. To hold the system in the chaotic range also the frequency f_F and the amplitude A of the forcing signal $Z(t)$ have to be retained.

Departures from the nominal value of damper D and resonant frequency f_0 have been examined. It was noticed that a $\pm 50\%$ variation of D does not prevent synchronisation. Therefore the adjustment of D is simple. The specified departure is not large as compared to the possible parameter range of D. On the other hand, the permissible variation of the resonant frequency f_0 is in the range of $\pm 2\%$ for the synchronised state. A small range for f_0 improves the security of the system but presupposes a fine adjustment. So we can say that each parameter has to be studied separately, and improved security implies high requirement at the adjustment.

5. A possible problem of the proposed scheme stems from the fact that fluctuations of the system parameters can bring the system out of chaos into a periodic oscillation mode. In that case the communication is not prevented but security is lost. Therefore the system parameters have to be chosen in a chaotic range with immunity against small drifts of the parameters. The system should not drift into a periodic window in case of temperature related fluctuation of some system parameters. Standard electronic components like resistors and capacitors are available within a range of dependence of $\pm 10^{-4}/K$ on the ambient temperature. In the system under study, this was enough to hold the system in chaotic mode. Our studies have shown that the sensitivity of the electronic components to temperature fluctuations is not very important. However, the frequency f_F must be within a tolerance band of $\pm 0.1\%$. If the frequency of the forcing signal is fixed based on a quartz oscillator, the

offered constancy is sufficient. It has recently been shown that robustness of chaos is obtainable in piecewise smooth maps which are realizable by switching circuits [18]. Therefore, if the chaos generator is made with a suitably designed switching circuit, the chaotic orbit can be robust against quite large variations of the parameters.

5. Conclusions

In this paper we have reported the implementation of a chaos-synchronisation-based secure communication system. Security has been demonstrated through experiment as well as simulation. A channel capacity of $C \sim B/3R$ = 70 kbit/s, maximum information transfer rate of $T \sim$ 3 kbit/s and a bandwidth efficiency of $\beta = T/B \sim 20 - 60\%$ have been achieved. A significant increase of the information error is observed if the signal to noise ratio is decreased below 14 dB. The observations raise the hope that with fine tuning the performance can be further improved, making chaos-based communication systems a commercially viable proposition.

A theoretical requirement for synchronisation of chaos is the equality of the system parameters in the transmitter and the receiver. This study has shown that the system can tolerate a $\pm 50\%$ variation of the damper coefficient D and a $\pm 2\%$ variation of the resonant frequency f_0 without losing synchronism. Therefore we conclude that the sensitivity of the system to the variation of each parameter has to be investigated and specified separately. Further, the system parameters have to be so chosen that inadvertent fluctuation of parameters does not drive the system out of chaos into a periodic window. This can be guaranteed by standard electronic components. The frequency of the forcing signal has to be held within a range of $\pm 0.1\%$. A frequency generation based on a quartz oscillator offers a sufficient constancy.

Acknowledgement

The authors thank Prof. M. Hasler for valuable comments and discussion on the draft of this paper.

[1] N. F. Rulkov, M. M. Sushchik, and L. S. Tsimring and H. D. I. Abarbanel, Phys. Rev. E, **51**, 980 (1995).

[2] L. Kocarev and U. Parlitz, Phys. Rev. Lett. **76**, 1816 (1996).

[3] F. Bohme, W. Schwarz, and A. Bauer, "Information transmission by chaotizing", in Proc. NDES '94 workshop, Crakow, Poland 1994, pp. 163-168.

[4] J. M. Ogorzalek, IEEE Trans. Circuits and Syst. I **40**, 693 (1993).

[5] M. Hasler, Synchronization principles and applications, Circuit and systems tutorials, Ed. C. Toumazu, N. Battersby, and S. Porta, IEEE Press, New York (1996).

[6] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett., **64**, 821 (1990).

[7] T. L. Carroll and L. M. Pecora, IEEE Trans. Circuits and Syst. I **38**, 453 (1991).

[8] G. Chen and X. Dong, Int. J. Bifurc. Chaos **3**, 1389 (1993).

[9] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, International Journal of Bifurcation of Chaos **3**, 477 (1993).

[10] F. Bohme and W. Schwarz, IEEE Trans. Circuits and Syst. I **43**, 596 (1996).

[11] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signalprocessing in the context of chaotic signals", in Proc. IEEE ICCASP '92, 1994, pp. IV-117 - IV-120.

[12] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, International Journal of Bifurcation of Chaos **2**, 709 (1992).

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

[14] A. Magauer, "Bilder und Klänge des chaotischen Zweipunktreglers", in Proc. der 6. Jahrestagung des Vereins zur Förderung der Erforschung der nichtlinearen Dynamik e. V., Technical University of Munich, Ed. R. Mayer-Spasche, M. Rast, and C. Zenger, Akademischer Verlag 1996, pp. 71 - 82.

[15] E. Herter and W. Lörcher, Nachrichtentechnik, 6th ed., Hanser, Munich 1992.

[16] G. Kolumbán, M. P. Kennedy, and L. O. Chua, IEEE Trans. Circuits and Syst. I **44**, 927 (1997).

[17] S. S. Haykin, Communication Systems, 3rd ed., Wiley, New York 1994.

[18] S. Banerjee, J. A. Yorke, and C. Grebogi, Phys. Rev. Lett. **80**, 3049 (1998).