Secure Communications Via Chaotic Synchronization in Chua's Circuit and Bonhöeffer-Van der Pol equation: Numerical Analysis of the Errors of the Recovered Signal

R. LOZI
Laboratoire de mathématiques, U.R.A. 168,
Université de Nice-Sophia Antipolis,
Parc Valrose, 06108 NICE Cedex 2, France
phone: 33. 93.52.98.73
fax: 33. 93.51.79.74 & 33. 93.52.90.39
e.mail: lozi@math.unice.fr

***Abstract*— The signal recovered from the first reported experimental secure communication system via chaotic synchronization contains some inevitable noise which degrades the fidelity of the original message. By *cascading* the output of the receiver in the original system into an *identical* copy of this receiver, it had be shown by computer experiments that this noise can be significantly reduced. We discuss the heuristic laws governing the errors of the recovered signal which are observed in a new series of very careful computer experiments. This discussion is done comparing these laws to the results obtained using the linear filtering theory. Some discrepancy appears. In order to understand the origin of the discrepancy we consider another simpler model based on the Bonhöeffer-Van der Pol equation where no chaos occurs. In this case both two heuristic laws are in good agreement with the linear filtering theory.**

I. Secure Communications Via Chaotic Synchronization in Chua's Circuit

The first laboratory demonstration of a secure communication system which uses a *chaotic* signal for *masking* purposes and which exploits the chaotic *synchronization* techniques to recover the signal was reported three years ago [1]. The main particularity of the system used in this demonstration is that the " receiver " actually contains *two* subsystems of the " chaotic " transmitter (Chua's circuit in this case). In both implementations - electronic circuit realization or computer simulation - there is an inevitable error introduced by the signal s(t).

In [2],[4] it is shown by computer experiments that by connecting two *identical* receivers in cascade, a significant amount of the noise can be reduced, thereby allowing the recovery of a much higher quality signal. Two copies of the receiver are made and connected as shown in Fig. 1. Although no two electronic circuits can be made perfectly identical in practice, this ideal situation can now be approached with the help of the integrated circuit technology demonstrated recently in [3]. By fabricating several identical Chua's circuits on the *same* silicon chip, the resulting circuits are almost " clones " of each other. This technique has the additional security advantage in that even if someone else has discovered the parameters (α, β) used in the system, integrating it into *another* silicon chip invariably introduces discrepancies due to the different processing parameters from different silicon " foundries " .

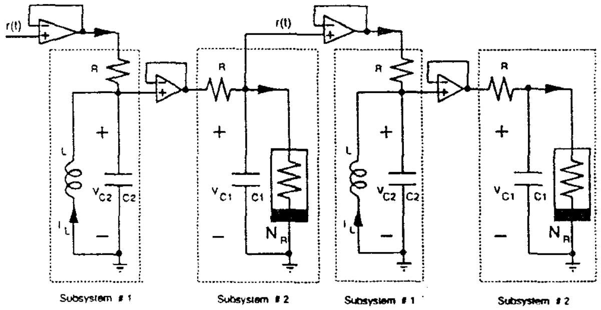

Figure 1: Electronic circuit implementation of the two-stage " receiver " consisting of two identical copies of the circuit given in Fig. 2 (b) of [1].

0-7803-2570-2/95 $4.00 ©1995 IEEE

A. NOISE REDUCTION VIA CASCADING

A.1. Single chaotic synchronization

The basic building block is a Chua's circuit, the dynamics of which is given by the Chua's equation

$$\left\{ \begin{array}{rcl} \dot{x} & = & \alpha(y - x - f(x)), \\ \dot{y} & = & x - y + z, \\ \dot{z} & = & -by, \end{array} \right. \qquad (1)$$

where

$$f(x) = bx + \frac{1}{2}(a-b)[\mid x+1 \mid - \mid x-1 \mid] \qquad (2)$$

Here, $x(t)$ is used as a noise-like " masking " signal. Let $s(t)$ be an information-bearing signal. The transmitted signal is $r(t) = x(t) + s(t)$, where the power level of $s(t)$ is assumed to be significantly lower than that of $x(t)$, in order to have the signal effectively hidden. The receiver consists of two subsystems. The first one is driven by the transmitted signal $r(t)$:

$$\left\{ \begin{array}{rcl} \dot{y}_1 & = & r(t) - y_1 + z_1, \\ \dot{z}_1 & = & -\beta y_1, \end{array} \right. \qquad (3)$$

The second subsystem is driven by the signal $y_1(t)$ and $s(t)$ is recovered as

$$\begin{array}{rcll} \dot{x}_2 & = & \alpha(y_1(t) - x_2 - f(x_2)) & (4) \\ s_2(t) & = & r(t) - x_2(t) \approx s(t) & (5) \end{array}$$

Actually the dynamics of the experimental set up (see Fig. 1) is described by

$$\left\{ \begin{array}{rcl} \dot{x}_2 & = & \alpha(y_1(t) - x_2 - f(x_2)), \\ \dot{z}_2 & = & -\beta y_1(t). \end{array} \right. \qquad (6)$$

However, as long as we do not need $z_2(t)$ to recover $s_2(t)$, we will continue to use Eq. (5) instead of Eq. (6) in the following improved system.

A.2. Cascade chaotic synchronization

In order to improve the previous method to recover a signal nearer to $s(t)$ than $s_2(t)$, we couple two receivers in cascade in the following way. The second receiver consists also of two subsystems. The first one is driven by the signal $x_2(t)$ which is assumed to be more synchronized to $x(t)$ than the transmitted signal $r(t)$:

$$\left\{ \begin{array}{rcl} \dot{y}_3 & = & x_2(t) - y_3 + z_3 \\ \dot{z}_3 & = & -\beta y_3 \end{array} \right. \qquad (7)$$

The second subsystem of the second receiver is then driven by the signal $y_3(t)$ from Eq. (7) and $s(t)$ is recovered as

$$\begin{array}{rcll} \dot{x}_4 & = & \alpha(y_3(t) - x_4 - f(x_4)) & (8) \\ s_4(t) & = & r(t) - x_4(t) \approx s(t) & (9) \end{array}$$

B. NUMERICAL EXPERIMENTS

B.1. Single tone signal

Four parameters (a,b,α,β) completely characterized Chua's equation, which is known to exhibit an immensely rich variety of behaviors . We have performed our numerical results with the parameter values (a = -1/7, b = 2/7, α = 9.7633, β = 15.5709) for which the signal $x(t)$ is chaotic [2],[4]. In this subsection we assume that the input (information-bearing) signal $s(t)$ is a single tone (sine wave) of amplitude k belonging to the range $0 < k < 10.0$:

$$s(t) = k \sin(\omega t) \qquad (10)$$

Let us define *the errors*

$$\|e_s(k,\omega,t)\|_2 = \|s_2(t) - s(t)\|_2 = \|x_2(t) - x(t)\|_2 \qquad (11)$$

$$\|e_c(k,\omega,t)\|_2 = \|s_4(t) - s(t)\|_2 = \|x_4(t) - x(t)\|_2 \qquad (12)$$

and

$$\frac{\|e_s(k,\omega,t)\|_2}{\|s(t)\|_2} = E_s(k,\omega) \qquad (13)$$

$$\frac{\|e_c(k,\omega,t)\|_2}{\|s(t)\|_2} = E_c(k,\omega) \qquad (14)$$

where

$$\|f(t)\|_2 \triangleq \lim_{T\to\infty} \frac{1}{T}\left[\int_0^T f^2(t)dt\right]^{1/2}$$

denotes the *quadratic norm* of $f(t)$.

Our numerical computations are done using the most common fourth-order Runge-Kutta algorithm. All computations are performed with 17 decimal-digit numbers. In order to obtain reliable numerical results, the step size of the Runge-Kutta algorithm is chosen to be equal to 10^{-5}. Three sets of different initial values are chosen for the transmitter and both the receivers. The errors are averaged on a very long period of time (the first 3×10^7 steps are ignored (transient regime), the averaging uses the steps $3 \times 10^7 + 1$ to 19×10^7).

RESULTS: We first found that for the values $1 \leq \omega \leq 15$. both $E_s(k,\omega)$ and $E_c(k,\omega)$ are independent of k, increasing with ω from 1 to 6, decreasing after. Instead for the values $15 \leq w \leq 409,600$ a power regression analysis leads us to both the heuristic laws 1 and 2 which are obtained with a correlation coefficient better than 0.999, 999 (0.999, 999, 996 if we use only the data corresponding to $400 \leq \omega \leq 102,400$).

Heuristic law 1.

$$E_s(k,\omega) = 81.46/\omega^2 \qquad (15)$$

Heuristic law 2.

$$E_c(k,\omega) = 1329.17/\omega^3 \qquad (16)$$

ANALYSIS: The analysis of these heuristic laws leads us to consider that the receivers are working as filters cutting down the high frequencies added to the signal $x(t)$. The heuristic law 1 is in concordance with the linear filtering theory even if Chua 's circuit is not linear, however there is a discrepancy between the heuristic law 2 and the linear filtering theory, because this theory points out that $E_c(k, \omega)$ should be of the form $\frac{C}{\omega^4}$ instead of $\frac{C}{\omega^3}$. We suspect that the double precision used in the computations is not enough precise to obtain such a result. In part II, we consider another model based on the Bonhöeffer-Van der Pol equation (where no chaos occurs) in order to compare the corresponding heuristic laws with the linear filtering theory.

B.2. Multi-tone signal

We have performed the same numerical experiments with various multi-tone signals instead of the single tone signal.

$$s(t) = ksin(\omega t) + ksin(n\omega t) + ksin(m\omega t) \qquad (17)$$

In a first approximation whatever are the values of n and m we find that both the errors $E_s(k, \omega)$ and $E_c(k, \omega)$ related to the multi-tone signal are equal to 60 % of the corresponding single-tone signal errors.

B.3. Discrepancies between the parameters

We have also tested the possible discrepancies between the parameter values of the transmitter and both the receivers. For this, α is replaced with $\alpha \times (1 + \delta_\alpha)$ in Eqs. (4), (6) (8), while kept the same in Eq. (1) and β is replaced with $\beta \times (1 + \delta_\beta)$ in Eqs. (3), (6) (7), while kept the same in Eq. (1). A power regression analysis is pointed out from the preliminary observations (where δ_α takes 15 values between 0.0001 to 0.08 and δ_β takes 12 values between 0.001 to 0.08) with correlation coefficients better than 0.99: The results are independent with respect to ω.

Observation 1.

$$E_s(k, \omega) = 64 \times \|\delta_\alpha\|^{1.07} \qquad (18)$$

Observation 2.

$$E_s(k, \omega) = 123 \times \|\delta_\beta\|^{1.08} \qquad (19)$$

Observation 3.

$$E_c(k, \omega) = 216 \times \|\delta_\alpha\|^{1.08} \qquad (20)$$

Observation 4.

$$E_c(k, \omega) = 354 \times \|\delta_\beta\|^{1.06} \qquad (21)$$

These observations have to be detailed carefully in order to understand better the mathematical theory hidden behind the chaotic synchronization.

II. Secure Communications Via Periodic Synchronization in Bonhöeffer-Van der Pol equation:

A. THE SIMPLER MODEL

In order to compare the corresponding heuristic laws with the linear filtering theory, we consider another simpler model based on the Bonhöeffer-Van der Pol equation where no chaos occurs. Of course the purpose here is not the implementation of a secure communication system because the information-bearing signal cannot be masked by a periodic signal, but only the analysis of this system as a " non-linear " filter. The basic building block is a Bonhöeffer-Van der Pol equation

$$\left\{ \begin{array}{rcl} \dot{x} & = & \frac{1}{\epsilon}(y + x - \frac{x^3}{3}), \\ \dot{y} & = & -x + a + by, \end{array} \right. \qquad (22)$$

As in Part I, the transmitted signal is $r(t) = x(t) + s(t)$. The first receiver consists of two subsystems. The first one is driven by the transmitted signal $r(t)$:

$$\dot{y_1} = -r(t) + a - by_1, \qquad (23)$$

The second subsystem is driven by the signal $y_1(t)$ and $s(t)$ is recovered as

$$\begin{array}{rcl} \dot{x_2} & = & \frac{1}{\epsilon}(y_1 + x_2 - \frac{x_2^3}{3}), \qquad (24) \\ s_2(t) & = & r(t) - x_2(t) \approx s(t) \qquad (25) \end{array}$$

The second receiver consists also of two subsystems. The first one is driven by the signal $x_2(t)$ which is assumed to be more synchronized to $x(t)$ than the transmitted signal $r(t)$:

$$\dot{y_3} = -x_2 + a - by_3, \qquad (26)$$

The second subsystem is driven by the signal $y_1(t)$ and $s(t)$ is recovered as

$$\begin{array}{rcl} \dot{x}_4 & = & \frac{1}{\epsilon}(y_3 + x_4 - \frac{x_4^3}{3}), \qquad (27) \\ s_4(t) & = & r(t) - x_4(t) \approx s(t) \qquad (28) \end{array}$$

B. NUMERICAL EXPERIMENTS

Using the same notations previously defined in Part I, we found the following heuristic laws :

Heuristic law 3.

$$E_s(k, \omega) = 5.99 \times k/\omega^2 \qquad (29)$$

Heuristic law 4.

$$E_c(k, \omega) = 1635.99 \times k/\omega^4 \qquad (30)$$

III. Conclusion:

Even if the Bonhöeffer-Van der Pol equation is definitely non linear both heuristic laws 3 and 4 are in accordance with the linear filtering theory. This seems to be an unexpected result. We have to perform multi-precision computation in the case of Chua's circuit system in order to understand whether the discrepancy between law 2 and the linear filtering theory comes from numerical errors or from the innermost structure of this system. Finally a sequence of receivers can be added to both Chua and Bonhöeffer-Van der Pol systems.
For example in the last system

$$\begin{aligned}
\dot{y}_5 &= -x_4 + a - by_5, && (31)\\
\dot{x}_6 &= \frac{1}{\epsilon}(y_5 + x_6 - \frac{x_6^3}{3}), && (32)\\
s_6(t) &= r(t) - x_6(t) && (33)\\
\dot{y}_7 &= -x_6 + a - by_7, && (34)\\
\dot{x}_8 &= \frac{1}{\epsilon}(y_7 + x_8 - \frac{x_8^3}{3}), && (35)\\
s_8(t) &= r(t) - x_8(t) && (36)\\
&\vdots \quad \vdots\\
&\vdots \quad \vdots
\end{aligned}$$

With the corresponding errors

$$\begin{aligned}
\|e_{cc}(k,\omega,t)\|_2 &= \|s_6(t) - s(t)\|_2 && (37)\\
\|e_{ccc}(k,\omega,t)\|_2 &= \|s_8(t) - s(t)\|_2 && (38)
\end{aligned}$$

and

$$\begin{aligned}
E_{cc}(k,\omega) &= \frac{\|e_{cc}(k,\omega,t)\|_2}{\|s(t)\|_2} && (39)\\
E_{ccc}(k,\omega) &= \frac{\|e_{ccc}(k,\omega,t)\|_2}{\|s(t)\|_2} && (40)
\end{aligned}$$

If linear filtering theory can be applied to these additional receivers, $E_{cc}(k,\omega)$ and $E_{ccc}(k,\omega)$ should be of the form $\frac{C}{\omega^6}$ and $\frac{C}{\omega^8}$ however, still now, in the computations with double precision we have found that they are equal to $\frac{C}{\omega^4}$ only. Multi-precision computations have to be done in this case also.

References

[1] Kocarev, Lj, Halle, K.S., Eckert, K. and Chua, L.O. " Experimental demonstration of secure communication via chaotic synchronization, " Int. J. of Bifurcation and Chaos , 2, (3) , 709 - 713, 1992.

[2] Lozi, R & Chua, L.O. " Secure communications via chaotic synchronization II: Noise reduction by cascading two identical receivers, " Int. J. of Bifurcation and Chaos , 3, (5) , 1319 - 1325, 1993.

[3] Delgado-Restituto, M. & Rodriguez-Vasquez, A. " A CMOS monolithic Chua's circuit," J. of Circuits, Systems and Computers, (3) 2, 259-268, 1993.

[4] Lozi, R & Aziz-Alaoui, A. " Secure Communications via Chaotic Synchronization in Chua's Circuit: Numerical Analysis of the Errors of the Recovered Signal, " Proceedings of the 1994 Symposium on Nonlinear Theory and its Applications , Kagoshima, Japan,145 - 148, 1994.