

Copyright © 1991, by the author(s).
All rights reserved.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission.

**SECURE COMMUNICATIONS BY SYNCHRONIZATION
TO A CHAOTIC SIGNAL**

by

J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman,
R. Sherman, A. J. Lichtenberg, J. Y. Huang,
W. Wonchoba, M. Steinberg, and P. Khoury

Memorandum No. UCB/ERL M91/89

26 September 1991

COVER PAGE

**SECURE COMMUNICATIONS BY SYNCHRONIZATION
TO A CHAOTIC SIGNAL**

by

J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman,
R. Sherman, A. J. Lichtenberg, J. Y. Huang,
W. Wonchoba, M. Steinberg, and P. Khoury

Memorandum No. UCB/ERL M91/89

26 September 1991

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

TITLE PAGE

**SECURE COMMUNICATIONS BY SYNCHRONIZATION
TO A CHAOTIC SIGNAL**

by

J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman,
R. Sherman, A. J. Lichtenberg, J. Y. Huang,
W. Wonchoba, M. Steinberg, and P. Khoury

Memorandum No. UCB/ERL M91/89

26 September 1991

**SECURE COMMUNICATIONS BY SYNCHRONIZATION
TO A CHAOTIC SIGNAL**

by

J. Gullicksen, M. de Sousa Vieira, M. A. Lieberman,
R. Sherman, A. J. Lichtenberg, J. Y. Huang,
W. Wonchoba, M. Steinberg, and P. Khoury

Memorandum No. UCB/ERL M91/89

26 September 1991

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

SECURE COMMUNICATIONS BY SYNCHRONIZATION TO A CHAOTIC SIGNAL

J. Gullicksen*, M. de Sousa Vieira, M. A. Lieberman, R. Sherman*, A. J. Lichtenberg,
J. Y. Huang*[†], W. Wonchoba, M. Steinberg*, and P. Khoury

*Department of Electrical Engineering and Computer Sciences
and the Electronics Research Laboratory
University of California
Berkeley CA 94720*

** Loral Aerospace
Western Development Laboratories
3200 Zanker Road, Bldg. 280, X21
San Jose, CA 95161-9041*

ABSTRACT

We apply the idea of chaotic synchronization to a communication system which consists of three coupled digital phase locked loops. The chaotic carrier is generated in a subsystem of two coupled loops. The receiver is driven by a chaotic signal, but is stable in the sense of having only negative Liapunov exponents. We study such systems both numerically and experimentally. We verify numerically that the receiver does synchronize with the transmitter if the stable loops in the transmitter and receiver are identical. In the experimental system each loop consists of a sample-and-hold, level shifter and voltage controlled oscillator. Experimentally we observe synchronization between the stable subsets of loops.

1. Introduction

The concept of synchronized chaos was introduced recently by Pecora and Carroll¹. They showed how two systems linked by a chaotic signal synchronize with each other. One potential application of this concept is to the problem of secure communications. The idea is to have two remote systems linked by the same chaotic signal and still synchronized with each other. In a recent paper² this possibility was explored numerically in a system of coupled Digital Phase Locked Loops (DPLL's). Using two coupled loops as a transmitter of a chaotic signal, we showed how a third loop can synchronize with one of the transmitter elements.

Analog and digital PLL's are electronic devices used in a variety of communication applications such as modulation and demodulation, noise reduction and also as synchronization devices to lock the phase of a receiver to that of a transmitter³. In a single DPLL the phase difference between transmitter and receiver is described by a circle map when the input is a sinusoidal signal with a constant amplitude and frequency^{4,5}. Circle maps have been studied extensively in the past. They

[†] Permanent address: *Electrical Engineering Department, San Jose State University, San Jose, CA 95192.*

present tongues of periodic cycles, quasiperiodic behavior and chaos⁶. For two coupled DPLL's we also observed a complicated behavior characterized by periodicity, quasiperiodicity and chaos².

In this paper we present numerical simulations and experimental results on synchronization of DPLL's. Here, the DPLL's considered in our numerical calculations have a slightly different feature from those ones studied in Ref. 2 and they correspond more closely to the experimental system.

The paper is organized as follows: In section 2 we describe the system studied and report our numerical results. Section 3 is dedicated to the study of the experimental system, and the section 4 gives the conclusions.

2. Numerical Results

We will first give a brief description of a single, first-order, nonuniformly sampling DPLL, whose block diagram is shown in Fig. 1(a). It consists of a sample-and-hold (SH) and a voltage controlled oscillator (VCO). During the operation, the SH takes a discrete sample $v(t^k)$ of the incoming signal at the sampling time t^k when the VCO signals it to do so. The sampled value is used to control the sampling frequency of the VCO according to a given function in such a way as to decrease the phase difference between the incoming signal and the oscillator output. As a result, for a range of parameters, there is a possibility of locked behavior when the oscillator frequency adjusts itself to the input frequency and locks to its phase, hence sampling always at the same point on the input signal. Due to the nonlinearities in the system, orbits with high period, quasiperiodic and chaotic behavior may also appear in a single DPLL⁵.

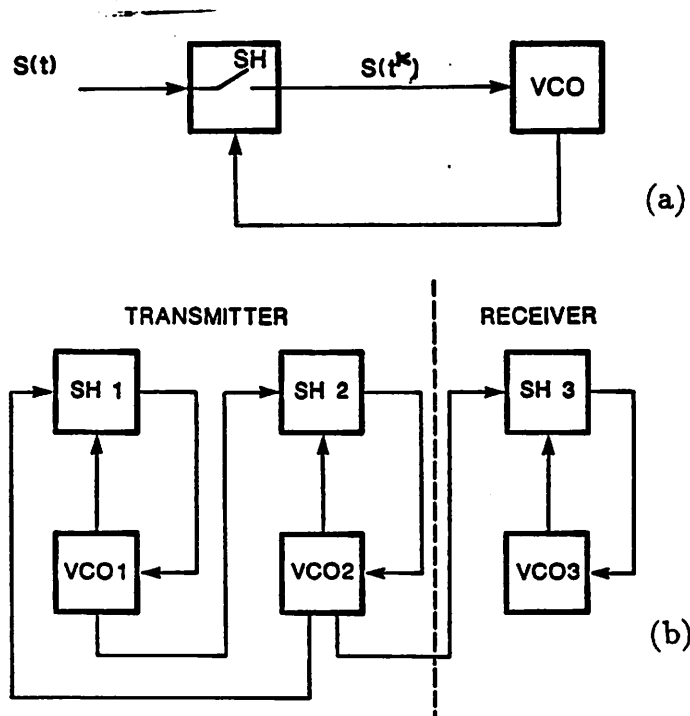


Fig. 1. Schematic representation of (a) a single DPLL and (b) communication system consisting of three coupled DPLL's.

The communication system we study in this paper has a transmitter which consists of two self-synchronized DPLL's, where the input to one loop is the output of the other loop, and vice-versa. The receiver consists of a single loop and receives its input from output of one of the loops in the transmitter, as shown schematically in Fig. 1(b).

We initially discuss the dynamical properties of the coupled loops in the transmitter. In the experimental device studied in section 4 the outputs of the loops are voltages, which have a triangular wave form, which are represented as $v(t) = Ah(\phi(t))$ with

$$h(\phi(t)) = \begin{cases} 4\phi(t) & \text{if } 0 \leq \phi(t) \leq 1/4, \\ -4\phi(t) + 2 & \text{if } 1/4 \leq \phi(t) \leq 3/4, \\ 4\phi(t) - 4 & \text{if } 3/4 \leq \phi(t) \leq 1. \end{cases} \quad (1)$$

where $\phi(t) = ft$, with f the frequency, and $0 \leq t \leq 1/f$. In Ref. 2 the output of the VCO's were taken as sinusoidal, rather than triangular waves.

In this coupled loop system each time that one of the triangular wave signals crosses $v = 0$ with a positive slope, the VCO sends a signal to the respective SH and an input sample v_j is taken from the VCO output of the other loop. The loop i that samples switches its frequency to a new value according to

$$f'_i = f_i^o + b_i[v_j + v_i^{off}], \quad (2)$$

where f^o is the center frequency of the VCO, i.e., its frequency in the absence of applied signal, b is the gain of the VCO and v^{off} is an offset voltage that may be added to the sampled value in order to bring the input signal to the appropriate voltage range of operation in an experimental device.

In Fig. 2 we show a diagram that illustrates the dynamics of the system of two self-synchronized DPLL's with a waveform given by (1). The signals in the figure represent the time varying output of the VCO's. In our simulations we evolve the system according to the algorithm given in Ref. 2.

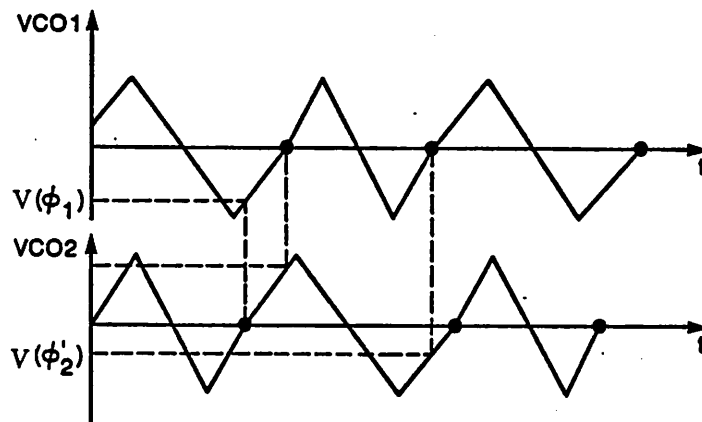


Fig. 2. Schematic representation of the dynamics of two coupled DPLL's.

The coupled system is described by four variables, that is, the frequencies and the phases of the two loops. However, the system state changes only at the sampling instants. As a result, the dynamics lies in the union of two three-dimensional linear subspaces, which have $\phi_1 = 0 \pmod{1}$ or $\phi_2 = 0 \pmod{1}$.

There are eight parameters in the coupled system. For each loop we have the amplitudes A_i , the gains b_i , the center frequencies f_i^o and the offset voltages v_i^{off} . We can normalize the parameters in the following way. The equations that determine the dynamical evolution of the loops are

$$f_1' = f_1^o + b_1[A_2 h(\phi_2) + v_1^{off}] \quad (\phi_1 = 0), \quad (3.a)$$

$$f_2' = f_2^o + b_2[A_1 h(\phi_1) + v_2^{off}] \quad (\phi_2 = 0). \quad (3.b)$$

Dividing Eq. (3) by $f_2^o + b_2 v_2^{off}$ we obtain

$$\bar{f}_1' = f^o + B_1 h(\phi_2), \quad (4.a)$$

$$\bar{f}_2' = 1 + B_2 h(\phi_1), \quad (4.b)$$

where

$$\bar{f}_i' = \frac{f_i'}{f_2^o + b_2 v_2^{off}}, \quad f^o = \frac{f_1^o + b_1 v_1^{off}}{f_2^o + b_2 v_2^{off}}, \quad B_i = \frac{b_i A_j}{f_2^o + b_2 v_2^{off}}. \quad (4.c)$$

Thus there are three dimensionless fundamental parameters in the system, which are the two normalized gains B_1 and B_2 and the normalized center frequency f^o of one of the two loops, say loop 1. Since the frequencies of these discrete time systems are positively defined, we must have from Eqs. (4) that $B_1 < f^o$ and $B_2 < 1$, since $h(\phi) \in [-1, 1]$.

By varying these three parameters we observe numerically in the system of two coupled loops, regular, quasiperiodic and chaotic behavior^{2,7}.

We show in Fig. 3 a bifurcation diagram for ϕ_1 versus $B \equiv B_1 = B_2$ with $f^o = 1$ on the surface of section $\phi_2 = 0$. Contrary to the case of sinusoidal output² where the route to chaos is via period doubling, here we observe that the bifurcation sequence is truncated, and beyond the period two orbit a complex entrance into chaos is observed. We have studied the complete phase diagram of the coupled loops, which is situated in a tri-dimensional space, and the results of our investigations will be reported elsewhere⁷.

Now we discuss the synchronization to a chaotic signal produced by the coupled DPLL's². The synchronization is obtained by transmitting a variable of the chaotic driving system (the transmitter) to be a corresponding variable of the response system (the receiver) while the driving system remains unperturbed. A necessary condition for the system to follow the master system is that it have only negative Liapunov exponents.

We apply such ideas to the communication system shown in Fig. 1(b). We observe numerically that if loops 1 and 3 are completely identical, then the syn-

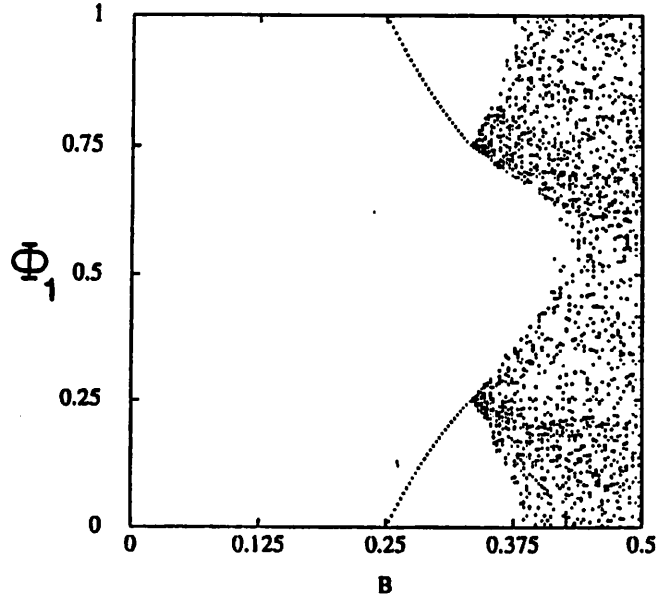


Fig. 3. Bifurcation diagram for $\phi_1(\phi_2 = 0)$ as a function of $B \equiv B_1 = B_2$ with $f_1^o = 1$.

chronization between them is observed in certain regions of the parameter space, even when the transmitter is chaotic. In this situation, the outputs of loops 1 and 3 are exactly the same. This may occur when the Liapunov exponents associated with loops 1 and 3 are negative, and positive for loop 2⁸. However, even when these conditions are satisfied, the synchronization between loops 1 and 3 may not be observed due to the presence of more than one basin of attraction, or to other factors. If the parameters of loops 1 and 3 are not identical, the synchronization between them is degraded².

3. Experimental System

In this section we show the results of chaotic synchronization obtained experimentally for our coupled DPLL's. The experimental circuit for a single DPLL, shown in Fig. 4, is composed of two main parts: (1) the sampler and associated support circuitry and (2) the VCO and associated circuitry. For the sampler a National Semiconductor LF398 Monolithic Sample and Hold circuit is used. An 0.001 μF polystyrene capacitor is used for its low dielectric loss properties as the hold capacitor. The sample time is set by a 74LS123 retriggerable monostable multivibrator. The pulse width of the multivibrator is set with $R_{ext} = 20 \text{ k}\Omega$ and $C_{ext} = 680 \text{ pF}$ which gives a predicted pulse duration of about 6.7 μs ⁹ and a measured pulse duration of about 6.0 μs . The maximum frequency of the input signal is about 4.0 kHz. Therefore, our sampling duration is about 1.2% of the signal period in the worst case and less than 1% on average. Hence, our sampling error should be much less than 1%.

For the VCO a National Semiconductor LM566C Voltage Controlled Oscillator integrated circuit is used. The frequency of the VCO is given approximately by the formula¹⁰

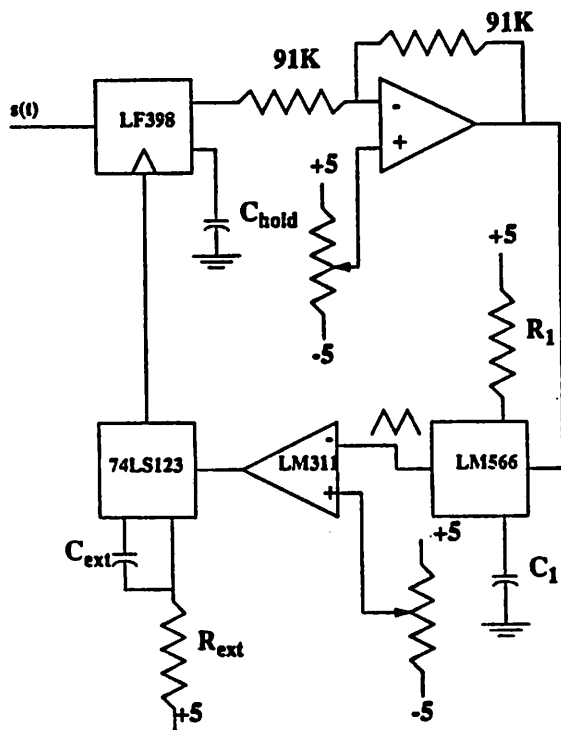


Fig. 4. Block diagram of the experimental implementation of the nonuniformly sampling first order DPLL.

$$f = \frac{2.4(V^+ - v_5)}{R_1 C_1 V^+}, \quad (5)$$

where $V^+ = 5V$, v_5 is the control voltage input (the voltage on pin 5 minus the voltage on pin 1 of the integrated circuit), $R_1 = 10 \text{ k}\Omega$ and $C_1 = 0.022 \text{ }\mu\text{F}$.

Due to the relatively loose tolerances of R_1 and C_1 and the temperature dependence of these components, equation (5) is useful primarily for design purposes. The center frequency and gain of such a DPLL, which obeys $f = f^\circ + bv$, with v being referenced to zero, were obtained from a linear least squares fit of the data⁵, and it was found that $f^\circ = 5259.1 \text{ Hz}$ and $b = 1217.4 \text{ Hz/V}$ for the voltage range we use. The output of the VCO has an amplitude of 0.9 V and a D.C. offset of -0.9 V. To use this VCO in a DPLL it is necessary to add a DC offset voltage either to the input signal to the sampler or to the output signal of the sampler so that the input signal to the VCO will be in the proper voltage range. The operational amplifier circuit shown in Fig. 4 is used to adjust the offset voltage. A hard limiter LM311 with a reference of -0.9 V was included at the triangle wave output of the VCO to cause sampling at the zero crossing, as opposed to sampling at the peak, as in the case of the circuit studied in Ref. 5.

We studied the synchronization to a chaotic signal in an experimental system consisting of such DPLL's coupled according to Fig. 1(b). As predicted in our nu-

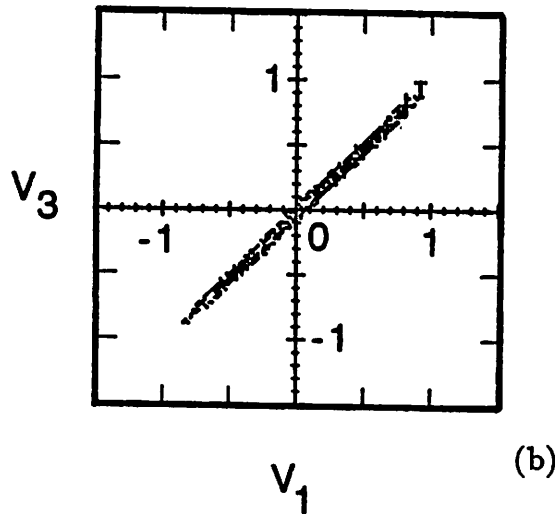
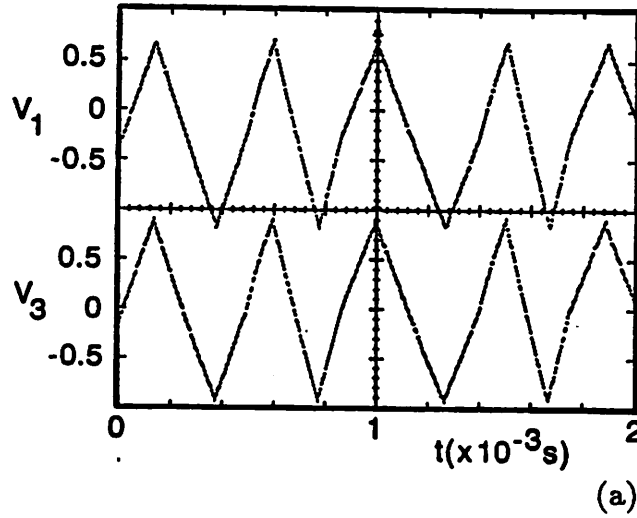


Fig. 5. (a) Temporal evolution of the output voltages of VCO 1 and VCO 3 (in volts) for the parameters values $v_5 = 0.819V$ in loops 1 and 3 and $v_5 = 1.062V$ in loop 2. (b) Output voltage of VCO 1 versus the output voltage of VCO 3 for the same parameter values.

merical simulations, we observe in the experimental device a parameter region where synchronization in the chaotic regime is obtained. We illustrate this by showing in Fig. 5(a) the time evolution of the output voltage of loop 1 and the corresponding quantity for loop 3. The figure shows that the two loops are synchronized. This can also be seen by plotting the output of loop 1 versus the output of loop 3, as shown in Fig. 5(b).

4. Conclusions

We studied the synchronization to a chaotic signal in a system of coupled DPLL's both numerically and experimentally. We have shown that the receiver does synchronize with the chaotic transmitter in a certain region of the parameter

space. This indicates that DPLL devices may be useful for secure communication applications. Presently we are working on modulation techniques for the transmission of information.

Acknowledgements

This work was partially supported by NSF Grant ECS - 8910762 and by DARPA Grant W-SO-242614-T-12/91.

References

1. L. M. Pecora and T. L. Carroll, *Phys. Rev. Lett.* **64** (1990) 821.
2. M. de Sousa Vieira, A. J. Lichtenberg and M.A. Lieberman, to appear in *International Journal of Bifurcation and Chaos*.
3. R. E. Best, *Phase Locked Loops* (McGraw-Hill Books Company, 1984); W. C. Lindsey and C. M. Chie, *Proc. IEEE* **69** (1981) 410 .
4. S. Gil and S. C. Gupta, *IEEE Trans. Commun.* **20** (1972) 454; S. Gil and S. C. Gupta *IEEE Trans. Aerosp. Electron. Syst.* **8** (1972) 615.
5. G. M. Bernstein, M. A. Lieberman and A. J. Lichtenberg, *IEEE Trans. Commun.* **37** (1989) 1062; G. M. Bernstein and M. A. Lieberman, *IEEE Trans. Circuits Systems* **37** (1990) 1157; G. M. Bernstein, *Nonlinear Oscillations, Synchronization and Chaos*, PhD thesis, University of California, Berkeley, 1988.
6. S. J. Shenker, *Physica* **5D** (1982) 405.
7. M. de Sousa Vieira, J. Gullicksen, A. J. Lichtenberg, R. Sherman, M. A. Lieberman, J. A. Huang, W. Wonchoba, M. Steinberg and P. Khoury, *in preparation*.
8. We calculated the largest Liapunov exponent using the algorithm given by A. Wolf, J. B. Swift, H. L. Swinney and J. A. Vastano, *Physica* **16D** (1985) 285.
9. Texas Instruments Incorporated, *The TTL Data Book for Design Engineers*, Dallas, TX 1981.
10. National Semiconductor Corporation, *Linear Databook*, Santa Clara, CA 1982.