Secure communication circuit simulation using VHDL-AMS

H. Bouraoui, K. Kemih
L2EI Laboratory, BP 98 Ouled Aissa,Jijel University, Algeria

A. Senouci
CRD-DAT/CFDAT-Reghaia, 16036 Reghaia, Algiers, Algeria

M. Ghanes
ECS-ENSEA, 06 Avenue du Ponceau, 95014 Cergy-pontoise Cedex, France

***Abstract*—This paper describes the simulation of a hybrid secure communication circuit with VHDL-AMS. The hybrid chaos synchronization strategy is developed from the point of view of the observer design, where the drive is a combination of a continuous-time hyper-chaotic (5D) system and a discrete time chaotic system (Henon), the response is a composed of a continuous unknown input observer and a discrete full-order state observe. Simulation results show the effectiveness of the proposed approach.**

Keywords: hyperchaotic system, Chaos synchronization, observer, VHDL-AMS.

I. INTRODUCTION

Synchronization of hybrid chaotic systems and its application to secure communication have received considerable attention over the last decade. Since the pioneering work performed by Pecora and Caroll [1], different chaos communication methods have been developed in order to hide the contents of a message using hybrid chaotic signals.

An attractive way to simulate such complex systems in a reasonable amount of time is to use behavioral models to simplify physics and explore interaction between different domains. A modeling environment naturally suited for behavioral modeling of mixed technology problems is VHDL-AMS [3-5]. This high-level hardware description language is an IEEE standard and extension of a digital language VHDL [6]. VHDL-AMS is widely used in electronic design flow for modeling various mixed-signal (analog and digital) circuits and systems including such recent applications as RFID systems [7].

This paper describes the simulation of a hybrid secure communication circuit with VHDL-AMS. In the transmission scheme, we propose a transmitter system combined of a continuous-time hyper-chaotic (5D) system and a discrete-time chaotic system called modified Henon. To make its structure more complex, the states of the continuous-time system are introduced in the dynamic of the discrete-time system. The receiver is composed from a continuous unknown input observer and a discrete full-order state observer. Simulation results are finally presented to visualize the satisfactory synchronization performance.

II. THE HYBRID CHAOS SYNCHRONIZATION SYSTEM

The continuous system is described by the following equations:

$$\dot{z}=A_1 z+f_1(z,s_1,y_1)+B_1 s_1$$

$$y_1 = C_1 z + D_1 s_1 \qquad (1)$$

$z \in R^n$, $y_1 \in R^r$ and $s_1 \in R^m$ denote the state, output and information signal respectively. A_1, B_1, C_1 and D_1 are real known matrices. $f_1(z,s_1,y_1)$ is the nonlinear item of the system.
For simplicity of the presentation we introduce the following notations:

$$E = [I_n \quad 0],\ M = [A_1 \quad B_1],\ H = [C_1 \quad D_1] \text{ and } \varphi = \begin{pmatrix} z \\ s_1 \end{pmatrix} \qquad (2)$$

The discrete-time system is described by the following equations [9]:

$$x(n+1) = A_2 x(n) + B_2 f_2\big(x(n)\big) + C_2 + B_0 s_2(n)$$

$$y_2(n) = d^T x(n) + Kf\big(x(n)\big) + s_2(n) = \xi(n) + s_2(n) \qquad (3)$$

$x \in R^l$, $y_2 \in R^q$ and $s_2 \in R$ denote the state, output and information signal respectively. A_2, B_2 and C_2 are real known matrices. $f_2\big(x(n)\big)$ is the nonlinear item of the system.

We introduce in the dynamics of discrete-time system, the states z_1, z_2, z_3, z_4 and z_5 of the continuous-time system, sampled with a rate T1, to make the structure of the discrete system more complex [2].

The signal y_1 comes from the continuous-time system will be first sampled with a period T2, but only blocked during T1. The signal y_2 comes from the discrete-time system, is sent during 9T1. We obtain a transmission cycle composed of 10 periods T1.

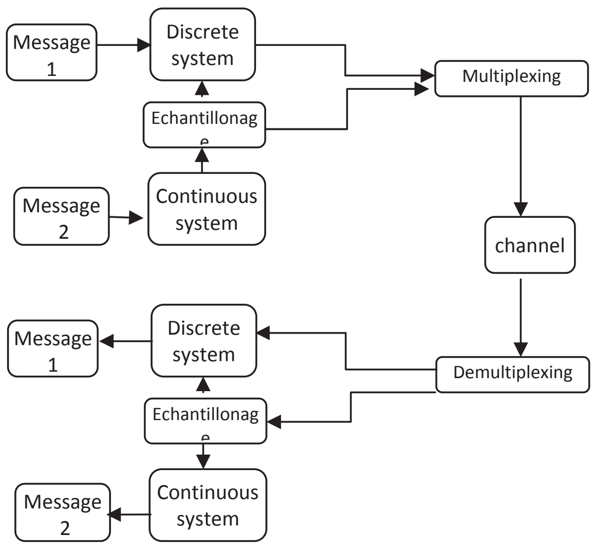

Fig.1. Transmission chain based on a hybrid dynamical system

In the receiver, The Continuous-time system proposed is in the form [8], [11]:

$$\dot{\hat{z}} = N\hat{z} + Ly_1 + g(\hat{z}, y_1)$$

$$\hat{\varphi} = \hat{z} + Qy_1 \tag{4}$$

Where $\hat{\varphi}$ denotes the state estimation vector of φ. Q is a real matrix that verified $PE + QH = I_{n+m}$ with P is a real matrix. Matrices N, L and the nonlinear vector field $g(\hat{z}, y_1)$ should be determined such that $\hat{\varphi}$ converges asymptotically to φ.

Consider the error vector:

$$e_1 = \hat{\varphi} - \varphi \tag{5}$$

In order to recover the message s_1, the following condition must be verified: $\begin{pmatrix} N^TR + RN + \varepsilon\lambda^2 I_{n+m} & RP \\ P^TR & -\varepsilon I_{n+m} \end{pmatrix} < 0$ is solvable with R a positive symmetric matrix, ε a positive number.

The Discrete-time receiver system is described by:

$$\hat{x}(n+1) = A_2\hat{x}(n) + B_2 f_2(\hat{x}(n)) + C_2 + B_0(y_2(n) - \hat{\xi}(n))$$

$$\hat{\xi}(n) = d^T\hat{x}(n) + Kf(\hat{x}(n)) \tag{6}$$

Let $\hat{s}_2 = (y_2 - \hat{\xi})$

Where $\hat{x}$ denotes the state estimation vector of x. Matrices B_0, d^T and K should be determined such that $\hat{s}_2$ converges to s_2.

Defining the synchronization error:

$$e_2 = \hat{x} - x \tag{7}$$

And if the following condition are verified,

- $B_0 = b/K$
- $K \neq 0$
- d^T satisfies: $\lambda_i(A - bd^T/K) < 1$ i=1,……,n

We can recover the message s_2.

The received signal is first demultiplexed on two signals y_1 and y_2. The signal y_1 is first memorized during a period T2 = 10T1. Then, the signals y_1, y_2 are introduced, respectively, in continuous and discrete observers.

III. VHDL-AMS SIMULATION

In this paper, all VHDL-AMS simulations have been simulated with simulator HAMSTER. The continuous time chaotic system has initial conditions: $(z_1(0), z_2(0), z_3(0), z_4(0), z_5(0)) = (1, 3, 1, 0.5, 2)$, and the discrete time has: $(x_1(0), x_2(0), x_3(0)) = (0.1, 0.1, 0.1)$. All of these numerical experiments were performed using the fourth-order Runge-Kutta integration algorithm with integration step of 0.00001s.

The equations of the continuous time hyper-chaotic 5D system are as follows [10]:

$$\dot{z} = \begin{bmatrix} -a_1 & a_1 & 0 & 0 & 0 \\ a_2 & a_2 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -a_3 & 0 \\ -a_5 & 0 & 0 & a_4 & -a_4 \end{bmatrix} z + \begin{bmatrix} z_2z_3z_4z_5 \\ -z_1z_3z_4z_5 \\ 0.1z_1^2 \\ z_1z_2z_3z_5 \\ z_1z_2z_3z_4 \end{bmatrix} + \begin{bmatrix} 0 \\ 30 \\ 0 \\ 0 \\ 0 \end{bmatrix} s_1$$

$$y_1 = [0\ 1\ 0\ 0\ 0]z + s_1$$

Where $a_1 = 37, a_2 = 14.5, a_3 = 10.5, a_4 = 15, a_5 = 9.5$.

The first transmitted information signal is: $s_1(t) = 0.5\,sin(60\pi t)$. The discrete time chaotic system used is the modified Henon given by:

$$x(n+1) = \begin{bmatrix} 0 & 0 & -b \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x(n) + \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix} x_2^2(n) + \begin{bmatrix} a \\ 0 \\ \alpha_1 z_1(n) + \alpha_2 z_2(n) + \alpha_3 z_3(n) + \alpha_4 z_4(n) + \alpha_5 z_5(n) \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix} s_2(n)$$

$$y_2(n) = [0 \quad 0 \quad 0.1]\, x(n) + x_2^2(n) + s_2(n) = \xi(n) + s_2(n)$$

With $a = 1.76, b = 0.1$.
The coefficients of continuous states are chosen as: $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = 0.0001$.
The second transmitted information signal is: $s_2(t) = 0.5\, sin(60\pi t)$.
Matrices P, Q, N and L of the continuous unknown input observer are:

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \end{bmatrix} L = \begin{bmatrix} 0 \\ 30 \\ 0 \\ 0 \\ 0 \\ -30 \end{bmatrix}$$

$$g = \begin{bmatrix} \hat{z}_2\hat{z}_3\hat{z}_4\hat{z}_5 \\ -\hat{z}_1\hat{z}_3\hat{z}_4\hat{z}_5 \\ 0.1\hat{z}_1^2 \\ \hat{z}_1\hat{z}_2\hat{z}_3\hat{z}_5 \\ \hat{z}_1\hat{z}_2\hat{z}_3\hat{z}_4 \\ \hat{z}_1\hat{z}_3\hat{z}_4\hat{z}_5 \end{bmatrix} Q = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$N = \begin{bmatrix} -37 & -35.84 & 0 & 0 & 0 & -72.84 \\ 14.50 & -66.92 & 0 & 0 & 0 & -51.42 \\ 0 & 0 & -1.00 & 0 & 0 & 0 \\ 0 & 7.66 & 0 & -10.50 & 0 & 7.66 \\ -9.5 & 54.19 & 0 & 15.00 & -15.00 & 54.19 \\ -14.5000 & 31.80 & 0 & 0 & 0 & 16.30 \end{bmatrix}$$

Initials conditions are given as: $\left(\hat{z}_1(0), \hat{z}_2(0), \hat{z}_3(0), \hat{z}_4(0), \hat{z}_5(0)\right) = (3, 2, 2, 5, 4)$.
Initials conditions of the discrete full-order state observer are given as: $\left(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0)\right) = (0.15, 0.2, 0.1)$.

```
LIBRARY IEEE;
USE IEEE.std_logic_1164.ALL;
USE IEEE.math_real.ALL;
ENTITY mixte IS
END mixte;
ARCHITECTURE a_mixte OF mixte IS
  CONSTANT a                    : real := 1.76;
  CONSTANT b                    : real := 0.1;
  CONSTANT dt                   : real := 0.1;
  CONSTANT a1                   : REAL := 37.0;
  CONSTANT a2                   : REAL := 14.5;
  CONSTANT a3                   : REAL := 10.5;
  CONSTANT a4                   : REAL := 15.0;
  CONSTANT a5                   : REAL := 9.5;
  CONSTANT c1, c2, c3, c4, c5        : real := 0.0001;
  SIGNAL e1, e2, e3, r1, r2, r3,
      s, s2, ns1, ns2, ni1, ni2, se2, ch1, ch10          : real := 0.0;
  SIGNAL clk, m10                                        : BIT  := '1';
  SIGNAL m1, m2, m3, m4, m5, m6, m7, m8, m9              : BIT  := '0';
  QUANTITY x1, x2, x3, x4, x5, xx1, xx2, xx3, xx4, xx5,
       z1, z2, z3, z4, z5, z6, zz1, zz2, zz3, zz4, zz5,  y1, y2, y3,
       y4, y5,msge1, s1, ss1, msg1, msg2, msge2        : REAL;

BEGIN
break   e1 => 0.1 ,e2 => 0.1,  e3 => 0.1,  r1 => 0.15 ,r2 => 0.2,
        r3 => 0.1, se2 => 0.1, x1=> 3.0 , x2 => 2.0, x3 => 2.0,
        x4 => 5.0, x5 => 4.0 , z1=> 3.0 , z2 => 2.0, z3 => 2.0,
        z4 => 2.0, z5 => 5.0, z6 => 4.0;
  msg1 == 0.5*sin(60.0*math_pi*now);
  x1 == (a1*x2+x2*x3*x4*x5-x1'dot)/a1;
  x2 == (-a2*x1+x1*x3*x4*x5+x2'dot-30.0*msg1)/a2;
  x3 == 0.1*x1*x1-x3'dot;
  x4 == (x1*x2*x3*x5-x4'dot)/a3;
  x5 == (x1*x2*x3*x4-a5*x1+a4*x4-x5'dot)/a4;
```

Fig.2. VHDL-AMS code

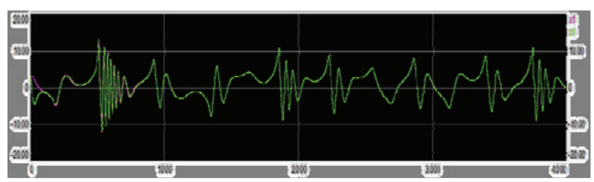

Fig3: Time response of z_1 and $\hat{z}_1$

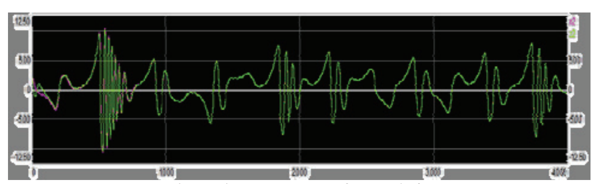

Fig4: Time response of z_2 and $\hat{z}_2$

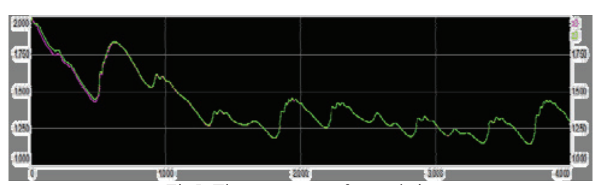

Fig5: Time response of z_3 and $\hat{z}_3$

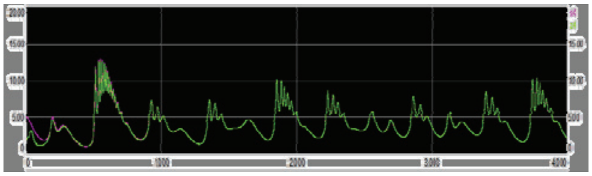

Fig6: Time response of z_4 and $\hat{z}_4$

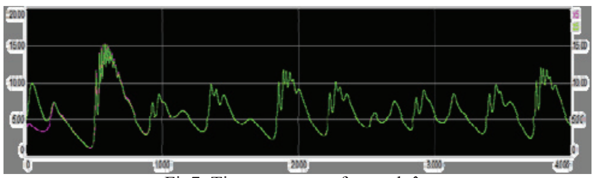

Fig7: Time response of z_5 and $\hat{z}_5$

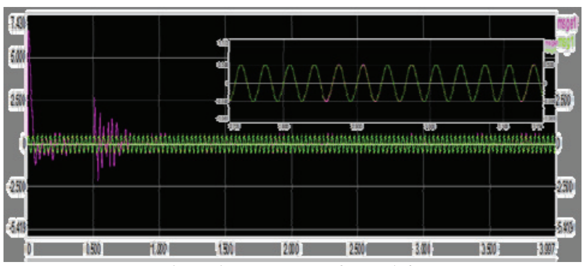

Fig8: Time response of s_1 and $\hat{s}_1$

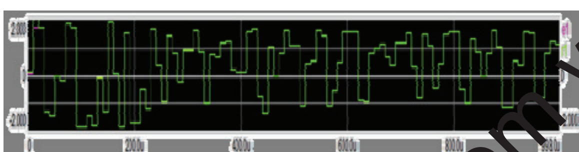

Fig9: Time response of x_1 and $\hat{x}_1$

Fig10: Time response of x_2 and $\hat{x}_2$

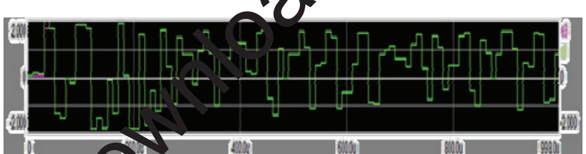

Fig11: Time response of x_3 and $\hat{x}_3$

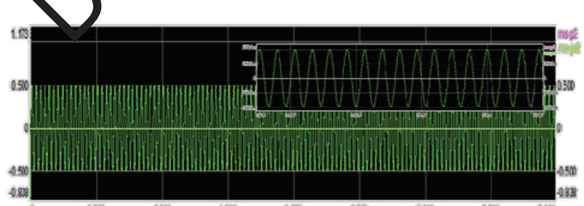

Fig12: Time response of s_2 and $\hat{s}_2$

Figure (2) present the VHDL-AMS code for this system. Figures (3)-(7) give the continuous states and their corresponding estimations, figures (9)-(11) give the discrete states and their estimations. We can note that all the states are perfectly estimated by the continuous and the discrete observer. Figures (8) and (12) show that the transmitted signals can be reconstituted successfully.

IV. CONCLUSION

This paper explores the circuit simulation of a new transmission scheme for chaos synchronization via hybrid dynamical system using VHDL-AMS. Several sufficient conditions for driving the synchronization error to zero and recovering the transmitted signals have been proposed. A typical illustrative example accompanied by their VHDL-AMS implementation and simulation results has shown satisfactory control performance.

REFERENCES

[1] L.M. Pecora and T.L. Carroll, “Synchronization in chaotic systems”, Physicals Review and Letters, pp.821-824, 1990.

[2] H. Hamiche, M. Ghanes, J.-P. Barbot, S. Djennoune, “Secure Digital Communication based on Hybrid Dynamical Systems”, IEEE, IET Inter. Symp. on COMMUNICATION SYSTEMS, NETWORKS AND DIGITAL SIGNAL PROCESSING, 2010.

[3] E. Christen, K. Bakalar, “VHDL-AMS a hardware description language for analog and mixed-signal applications”, IEEE Trans. Circuits Syst. II Analog Digital Signal Process. 46 (10) (1999) 1263–1272.

[4] A. Doboli, R. Vemuri, “Behavioral modeling for high-level synthesis of analog and mixed-signal systems from VHDL-AMS”, IEEE Trans. Comput. Aided Des. Integrated Circuits Syst. 22 (1) (2003) 1504–1520.

[5] P.J. Ashenden, G.D. Peterson, D.A. Teegarden, “The System Designer’s Guide to VHDL-AMS”, 2003.

[6] G. Sirakoulis, “A TCAD system for VLSI implementation of the CVD process using VHDL”, VLSI J. Integration 37 (1) (2004) 63–81.

[7] V. Beroulle, R. Khouri, T. Vuong, S. Tedjini, “Behavioral modeling and simulation of antennas: radio-frequency identification case study”, Proceedings of the International Workshop on Behavioral Modeling and Simulation, 2003, pp. 102–106.

[8] M. Boutayeb et al., “Generalized State-Space Observers for Chaotic Synchronization and Secure Communication”, IEEE Trans. Circuits Syst. I 49(3), pp. 345-349 (2002).

[9] Lu Jun-Guo, Xi Yu-Geng Chinese Phys. 14, 274 (2005).

[10] H. Bouraoui and K. Kemih, “Observer-Based Synchronization of a New Hybrid Chaotic System and its Application to Secure Communications”, ACTA PHYSICA POLONICA A, Vol. 123 (2013), No. 2, pp. 96-99.

[11] H. Wang, X. J. Zhu, S. W. Gao, Z. Y. Chen, “Singular observer approach for chaotic synchronization and private communication”, Commun Nonlinear Sci Numer Simulat 16 (2011), pp. 1517–1523.