Output Choice of a Chaotic Jerk Circuit Used as Transmitter in Data Secure Communications

Octaviana DATCU[1, 2], Mihai STANCIU[1], Roger TAULEIGNE[2], Corneliu BURILEANU[1], Jean-Pierre BARBOT[2, 3]
[1] *Politehnica University of Bucharest, 060042, Romania*
[2]*QUARTZ EA 7393, IPGP, ENSEA, 6 Avenue du Ponceau, 95014, Cergy-Pontoise, France*
[3]*EPI Non-A, INRIA-Lille Nord Europe*
od@elcom.pub.ro

***Abstract*—Usually, when analyzing a data series, dynamical systems theory is used to reconstruct the state space of the original system. This work aims to determine which of a chaotic system's states is best suited as output when transmitting secret messages. This is the first step prior to designing an actual communication scheme. As an example, the three states of Sprott's jerk circuit are analyzed in terms of the local observability they ensure for the original dynamics when transmitted as a scalar data series. Results show that its first two states enable accurate estimation of the transmitter's dynamics at the receiving end. However, its third state generates, in some regions of the state space, a non-invertible transformation between the original state space and the one the receiver sees. This is due to the exponential nonlinearities present in this state's derivatives. Given that these nonlinearities remain inaccessible to the receiver, they are neglected in order to allow the partial reconstruction of the dynamics of the transmitter. But, since these nonlinearities are essential for the chaotic behavior, this makes the third state unusable for cryptographic purposes. This analysis may be applied to any bipolar junction transistor or diode based chaotic circuit.**

***Index Terms*—chaotic communication, nonlinear dynamical systems, observers, signals analysis, sliding mode control.**

I. Introduction and Problem Statement

Chaos theory studies systems which present dynamical instability, topological mixing (stretching and folding of the phase space) and dense orbits (aperiodic trajectories arbitrary close to an infinite set of periodic orbits). These characteristics, together with their capability of engendering complex behavioral patterns from simple real systems or low dimensional systems given by a small set of equations, make chaotic systems useful for applications in cryptography. The reader may see [1] for a discussion about chaos-based cryptography. A parallel between block ciphers based on chaotic systems and standard block ciphers is made in [2], demonstrating by well-known cryptanalysis techniques that the former are as good as the latter. Some definitions of the so-called chaotic behavior are given in [3]. The potential application of chaotic behavior in weather and climate, population growth in ecology, economy, lasers, chemical reactions, fluid dynamics, or mechanical systems, are pointed out. See paper [4] for a mathematical frame.

A chaotic system is used in [5] to generate random pulses. Chaotic elements are analyzed in applied hydrology in [6]. In [7] some applications of chaos theory in economics are highlighted. Numeric methods based on a modified logistic map can be applied in complexity calculus as suggested in [8], which targets the use of fractal iterative techniques in pattern recognition. It should be noted that the logistics map is the simplest chaotic system from an analytical point of view. Time series representing biomedical signals are analyzed in [9] with chaotic dynamics specific parameters such as the Lyapunov exponents and fractal dimension of the attractor dynamics.

Implementation of chaos-based cryptosystems, key management, and security analysis, aiming at standardizing a framework for their design, are addressed by [10]. The chaos-based ciphers are categorized into digital and analog techniques upon the system they use as transmitter and receiver. Some recommendations regarding practical aspects of analog chaos-based secure communications, such as channel noise, limited bandwidth, and attenuation are made. Chaotic cryptography has been a rich research field and has given the opportunity for many developments in cryptanalysis also. An analysis with respect to the security and performance of such algorithms is made in [11]. Furthermore, [12] presents some main problems in chaos-based cryptography and proposes design rules to overcome them.

Aiming to contribute to the field of chaos-based cryptography, the present work analyzes how suitable as output of a chaotic system each of its states is. The receiver targets the reconstruction of the entire state space of the transmitter, when the only information measured is its output. Depending on the chosen state, observability singularities may appear due to the non-invertibility of the engendered embedding between the original state space and the one the receiver sees. Sprott's jerk system [13], being representative for bipolar junction transistor or diode based chaotic circuits, is used for exemplification. The considered circuit is the simplest autonomous dissipative ordinary differential equation with a quadratic nonlinearity manifesting chaotic behavior as stated by [14] and generalized in [15] to the form:

$$\dddot{x} + \ddot{x} + x + f(\dot{x}) = 0 \qquad (1)$$

where $f(\dot{x}) = I_0 \cdot R \cdot (e^{\dot{x}/\alpha} - 1)$ is a nonlinear function representing the characteristic of an ideal diode, with I_0 being the saturation current, R the resistor from the circuit in [13], and $\alpha = 0.026V$, the thermal voltage at room

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132395.

Digital Object Identifier 10.4316/AECE.2015.04008

temperature. We recall that a nonlinear function which gives the third-time derivative of the position *x,* corresponding to the first time derivative of acceleration, in a mechanical system, is called a *jerk function*. By setting $x_1 = x, x_2 = \dot{x}, x_3 = \ddot{x},$ with $f(x_2) = a(e^{bx_2} - 1)$, system (1) can be rewritten as follows:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = x_3 \\ \dot{x}_3 = -x_1 - ae^{b \cdot x_2} - x_3 + a \end{cases} \quad (2)$$

where $a = I_0 R$ and $b = 1/\alpha$ are chosen such that the transmitter (2) manifests chaotic behavior. Thus, the parameter a is equal to $10^{-9} V$, which corresponds to a current $I_0 = 10^{-12} A$ multiplied by a resistance $R = 10^3 \Omega$, and $b = (500/13) V^{-1}$.

The Lyapunov exponents characterizing the rate of divergence of two trajectories initially situated in a small vicinity in the three coordinates of system (2) are computed using the algorithm described in [16], and compared to the values obtained by Sprott, $(\lambda_1, \lambda_2, \lambda_3) = (0.07, 0, -1.07)$ for the above-mentioned parameters and initial conditions $x_1(0) = x_3(0) = 0V$ and $x_2(0) = 0.4V$. The results obtained by using the algorithm [16] are $(\lambda_1, \lambda_2, \lambda_3) = (0.08, 0, -1.08)$. We recall that the positive value of the greatest Lyapunov exponent attests the instability of the investigated system, therefore its chaotic behavior.

The second section of this paper recalls the theoretical tools used, based on chaotic synchronization [17-18]. The third section analyzes the three possible choices for the output y of the chaotic transmitter (2): either one of the states x_1, x_2, x_3. The analysis is performed in terms of the observability they engender for the original dynamics. Observability singularities are highlighted for the third state as output, while the first two states allow accurate estimation of the entire state space of the transmitter. The fourth section is dedicated to graphical illustration of the recovery of the transmitter's dynamics by using a higher-order sliding mode observer [19]. Given that the nonlinearities present in the third state's derivatives remain inaccessible to the receiver, they are neglected, in simulation, in order to allow the partial reconstruction of the transmitter's dynamics. Conclusions are drawn with respect to these approximations and the proper use of the analyzed circuit for cryptographic purposes.

II. Generalities on Observability Singularity Manifolds

Let us consider the continuous-time dynamical system described by (3):

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \quad (3)$$

where $x(t) = (x_1(t), x_2(t), ..., x_n(t))^T$ is the *n*-dimensional state vector, y is the *p*-dimensional output of the system and f and h are infinitely derivable vector fields, i.e. defined in C^∞.

Often, only one variable is measurable, and we subsequently call it observable. When analyzing a data series, dynamical systems theory is used to reconstruct the state space of the system generating the investigated information. Although the vector field f is not usually known, one can reconstruct a state space equivalent to the original flow. Chaotic time series are predicted in [20]. The method is based on the redundancy of the information contained by a physical system, in the sense that any variable chosen as output of the analyzed system has its temporal evolution connected with that of all the other variables in the considered system.

In this paper the original flow (3) has three dimensions. Thus, it can be written as in (4).

$$\begin{cases} \dot{x}_1 = f_1(x_1, x_2, x_3) \\ \dot{x}_2 = f_2(x_1, x_2, x_3) \\ \dot{x}_3 = f_3(x_1, x_2, x_3) \end{cases} \quad (4)$$

The evolution of only one of these states, a scalar temporal data series, is known. The goal is to find a differential embedding of the dynamics (4), in a standard [21] or canonic system form [22], starting from the measured variable belonging to the original system. Assuming the known evolution that of the variable x_2, the obtained standard system is described in (5):

$$\begin{cases} \dot{z}_1 = \dot{x}_2 = z_2 \\ \dot{z}_2 = \ddot{x}_2 = z_3 \\ \dot{z}_3 = \dddot{x}_2 = F_2(x_1, x_2, x_3) \end{cases} \quad (5)$$

A coordinate change which allows the transformation from the state space of the original system defined by variables (x_1, x_2, x_3) to the state space (z_1, z_2, z_3) is expressed by:

$$\Phi_2 : \begin{cases} z_1 = x_2 \\ z_2 = f_2(x_1, x_2, x_3) \\ \dot{z}_3 = (\partial f_2 / \partial x_1) f_1 + (\partial f_2 / \partial x_2) f_2 + (\partial f_2 / \partial x_3) f_3 \end{cases} \quad (6)$$

This application must be a local diffeomorphism, as the reconstructed space has the same dimension as the original one. How the choice of the observable may influence the analysis of non-linear dynamical systems is discussed in [23]. An approach concerning synchronization in such systems is considered in [24]. The local inversion theorem from [25] states that the transform Φ_2 defines a diffeomorphism if the determinant of its Jacobian $\Delta\Phi_2$ - the observability matrix is non-null over the entire state space. When the observability matrix has a zero valued determinant, i.e. it is singular, system (6) becomes undetermined, and it either has multiple solutions or none at all. This corresponds to regular local weak observability singularity. Regular means that we derive only to the *(n-1)* derivative.

The observability matrix is given in (7). See [26] for a rank condition for local weak observability: system (3) is local, i.e. in x_0, weakly observable if the rank of the observability matrix equals the dimension of its state space.

$$d\Phi(f,h)=\left[\begin{array}{c} dh \\ dL_f h \\ ..... \\ dL_f^{n-1}h \\ dL_f^{n}h \end{array}\right]_{x_0} \quad (7)$$

where $L_f^i h$ is the Lie derivative [27].

The observability singularity manifold S_O of a system is the mathematical space in which, seen from the measured variable, the system loses its observability property. For a three dimensional system, the regular observability singularity space is given in (8), where i is the number of the observed state.

$$S_{O,i}=\{(x_1,x_2,x_3)\in R^3 \mid \Delta\Phi_i=0\} \quad (8)$$

Some definitions are given in the case of the discrete-time chaotic Rössler system in [28].

We conclude this section by some comments with respect to the extra difficulty to obtain, in addition to the state-space, the unknown input, e.g. the message. This problem is known in the literature as the left invertibility problem [29]. A simple example is given in order to show some left invertibility drawbacks. Let as consider the continuous time system (9), with $u\in R$ the unknown input.

$$\begin{cases} \dot{x}_1=(1+x_1)x_2 \\ \dot{x}_2=(1-x_2^2)u \\ y=x_1 \end{cases} \quad (9)$$

The regular observability singularity manifold is:

$$S_{O,1}=\{(x_1,x_2)\in R^2 \mid 1+x_1=0\} \quad (10)$$

At this observability singularity manifold a new difficulty adds, when aiming to obtain the unknown input. The derivative of x_2 allows the estimation of the unknown input u only if $1-x_2^2\neq 0$. In conclusion, the set of singularity manifolds for the left invertibility problem is given by:

$$S=\{(x_1,x_2)\in R^2 \mid (1+x_1)(1-x_2^2)=0\} \quad (11)$$

This extension of the singularity set is interesting in data secure transmission. See for example [30].

III. The Observability Properties of Sprott's Jerk Circuit

A. The first state as output

If the output of system (2) is $y=x_1$, the recovery of its entire dynamics by an authorized receiver who knows the bifurcation parameters (a,b), and disposes of the information embedded in the manifold Φ_1 from:

$$\Phi_1:\begin{cases} z_1=x_1 \\ z_2=\dot{x}_1=x_2 \\ z_3=\ddot{x}_1=\dot{x}_2=x_3 \end{cases} \quad (12)$$

is trivial. The output and its first and second derivative are needed, at the reception, in order to obtain the estimated states vector:

$$\hat{x}=(\hat{x}_1,\hat{x}_2,\hat{x}_3)^T \quad (13)$$

System (12) can be easily inverted due to the fact that its corresponding observability matrix is the identity matrix.

B. The second state as output

When $y=x_2$ is the output of system (2) the information available at the reception is embedded in:

$$\Phi_2:\begin{cases} z_1=x_2 \\ z_2=\dot{x}_2=x_3 \\ z_3=\ddot{x}_2=\dot{x}_3=-x_1-ae^{bx_2}-x_3+a \end{cases} \quad (14)$$

The associated observability matrix $J(\Phi_2)=\partial\Phi_2/\partial x,$ given in (15), has the determinant $\Delta\Phi_2=-1$ which, again, guarantees the existence of its inverse.

$$J(\Phi_2)=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -abe^{bx_2} & -1 \end{bmatrix} \quad (15)$$

The states of the transmitter are well recovered, when the transmission is done over a noiseless channel, as it can be observed from (16).

$$\begin{cases} \hat{x}_2=z_1 \\ \hat{x}_3=z_2 \\ \hat{x}_1=-ae^{bz_1}-z_2-z_3+a \end{cases} \quad (16)$$

C. The singular case - the third state as output

When $y=x_3$ is the measured state, the information available at the reception is embedded in:

$$\Phi_3:\begin{cases} z_1=x_3 \\ z_2=\dot{x}_3=-x_1-ae^{bx_2}-x_3+a \\ z_3=\ddot{x}_3=-\dot{x}_1-ab\dot{x}_2e^{bx_2}-\dot{x}_3= \\ \quad =x_1-x_2+x_3+ae^{bx_2}(1-bx_3)-a \end{cases} \quad (17)$$

The associated observability matrix $J(\Phi_3),$ given in (18), has the determinant $|O_3|=1+ab^2x_3\exp(bx_2)$ which, for $x_3=-1/(ab^2e^{bx_2})$ does not allow the observability of the dynamics (2), because in this case the inverse does not exist.

$$J(\Phi_3)=\begin{bmatrix} 0 & 0 & 1 \\ -1 & -abe^{bx_2} & -1 \\ 1 & -1+abe^{bx_2}(1-bx_3) & 1-abe^{bx_2} \end{bmatrix} \quad (18)$$

The intersection between the state space of system (2) for initial conditions given in the next section and the observability singularity manifold:

$$S_{O,3}=\{(x_1,x_2,x_3)\in R^3 \mid x_3=-1/(ab^2\exp(bx_2))\}$$

is given in Fig. 1. In this case, $y=x_3,$ local exact formal computation of Φ_3^{-1} is not obvious and some approximations are done, in the next section, aiming to recover the original dynamics. The theoretical results obtained above are exemplified for certain parameters and initial conditions, in the next section. Graphical representations are interpreted.

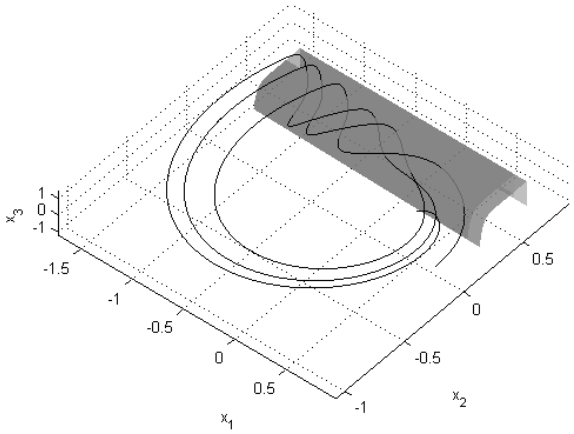

Figure 1. The intersection between the state space of the transmitter and the observability-singularity manifold (gray), when the output is $y = x_3$.

IV. Recovery of the Original Dynamics Through High-Order Sliding Mode Observers

This section is dedicated to graphical illustrations of the estimation of the dynamics of transmitter (2), with parameters $(a,b) = (10^{-9}V, 500/13V^{-1})$, and their interpretation. Initial conditions are $(x_1, x_2, x_3)|_{t=0} = (0.34, 0.15, 0.27)[V]$, for the transmitter (2), and $(z_1, z_2, z_3, z_4)|_{t=0} = (0.09, 0.91, 0.63, 0.27)[V]$, for the fourth order sliding mode observer (19):

$$\begin{cases} \dot{\hat{z}}_1 = \nu_1 = \hat{z}_2 - 5M^{1/4}\left|\hat{z}_1 - y\right|^{3/4}\operatorname{sgn}(\hat{z}_1 - y) \\ \dot{\hat{z}}_2 = \nu_2 = \hat{z}_3 - 1.5M^{1/3}\left\|\hat{z}_2 - \nu_1\right\|^{2/3}\operatorname{sgn}(\hat{z}_2 - \nu_1) \\ \dot{\hat{z}}_3 = \nu_3 = \hat{z}_4 - 3M^{1/2}\left\|\hat{z}_3 - \nu_2\right\|^{1/2}\operatorname{sgn}(\hat{z}_3 - \nu_2) \\ \dot{\hat{z}}_4 = E_j - 1.1M\operatorname{sgn}(\hat{z}_4 - \nu_3) \end{cases} \quad (19)$$

with $M = 10^5$. The additional state $z_4 = \dot{z}_3$ was added in order to avoid chattering in the estimated values $\hat{z}_j, j = \{1,2,3\}$. The notations $\dot{\hat{z}}_j \overset{not.}{=} \nu_j; j = \{1,2,3\}$ were used for the ease of writing and for conformity with [31], where detailed explanations about the high order sliding mode differentiators can be found. The expression $E_j = \ddot{z}_3|_{y=x_j}; j = \{1,2,3\}$ depends on the chosen output $y = x_j$ as follows:

$$\begin{aligned} E_1 &= \dddot{z}_3|_{y=x_1} = \hat{z}_1 - \hat{z}_2 + \hat{z}_3 + ae^{b\hat{z}_2}(1 - b\hat{z}_3) - a, \\ E_2 &= \dddot{z}_3|_{y=x_2} = -\hat{z}_2 - \hat{z}_4 - abe^{b\hat{z}_1}(\hat{z}_3 + b\hat{z}_2^2), \\ E_3 &= \dddot{z}_3|_{y=x_3} = -\hat{z}_2 - \hat{z}_4 \end{aligned} \quad (20)$$

where z_1, z_2, z_3 are according with the chosen output y, and the term $-abe^{bx_2}[b\hat{z}_1(b\hat{z}_1^2 + 3\hat{z}_2) + \hat{z}_3]$ in E_3 was neglected, as it remains unknown to the receiver.

All initial conditions for the observer are particular instances of a random uniformly distributed variable in $[0,1]$, truncated to two digits. Also, [32] points out the advantages high order sliding mode observers have when applied to the case of AC motors where some similar observability singularities occur.

The output of the transmitter is x_1 for Fig. 2 and x_2 for Fig. 3. As previously demonstrated from a theoretical point of view, all three estimates converge to the corresponding original states. The fixed step used in the Euler solver is 10^{-6}. Simulations are run in Matlab-Simulink R2013a.

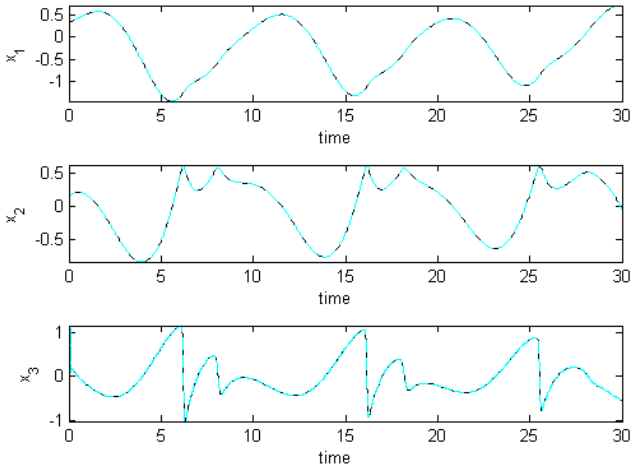

Figure 2. The estimation of the states of the transmitter when the output is $y = x_1$. Original signals in solid line, estimated in dashed.

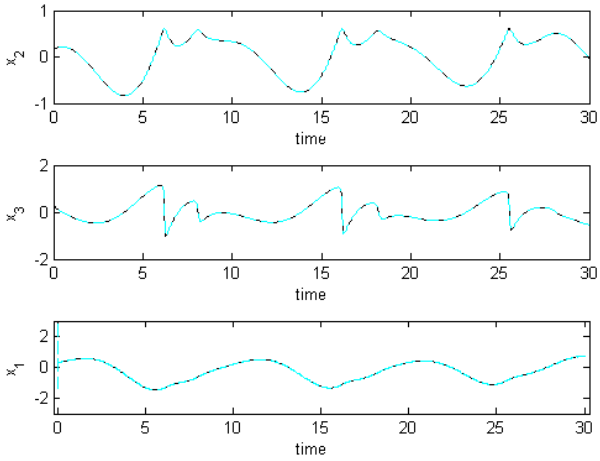

Figure 3. Estimation of the states of the transmitter when the observable is $y = x_2$. Original signals in solid line, estimated in dashed.

When the observable is $y = x_3$ getting the inverse of the observability matrix (18) is not possible for $x_3 = -1/(ab^2e^{bx_2})$ due to its singularity for these values. Moreover, it is not at the ease of the receiver to get the solution of equation $\hat{x}_2 + ab\hat{z}_1\exp(b\hat{x}_2) = -\hat{z}_2 - \hat{z}_3$, deduced from (17) by considering the output x_3 and its derivatives $\dot{x}_3$ and $\ddot{x}_3$. Nevertheless, Sprott's chaotic jerk circuit studied in this paper obeys the physics laws and its parameters a and b are chosen accordingly. Thus, in the considered case, $(a,b) = (10^{-9}V, (500/13)V^{-1})$, the unknown term is $ab\hat{z}_1e^{bx_2} \cong 3.85 \cdot 10^{-8} \cdot \hat{z}_1e^{bx_2}[V]$. Therefore, the regular observability singularity is situated at values much greater than the domain in which the state x_3 is bounded, i.e. (-1,1).

From (17), $\hat{Z} = J(\Phi_3) \cdot X + [0, a, -a]^T$, but as we approximated $ab\hat{z}_1\exp(bx_2)$ to zero, the observability matrix (18) can be rewritten as in (21). Also, abe^{bx_2} and $a = 10^{-9}V$ are neglected.

$$J(\Phi_3)^{aux} = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & -1 \\ 1 & -1 & 1 \end{bmatrix} \quad (21)$$

Due to the linearity and invertibility ($\Delta[J(\Phi_3)^{aux}]=1$) of the matrix (21), system (17) has the solution given in (22).

$$[J(\Phi_3)^{aux}]^{-1} \begin{bmatrix} \hat{z}_1 \\ \hat{z}_2 \\ \hat{z}_3 \end{bmatrix} = \begin{bmatrix} -\hat{z}_1 - \hat{z}_2 \\ -\hat{z}_2 - \hat{z}_3 \\ \hat{z}_1 \end{bmatrix} = \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \end{bmatrix} \quad (22)$$

The $\hat{z}$ estimates are obtained with the fourth order sliding mode observer (19) where $E_j = E_3$ from (20). Numerical results are given in Fig. 4 where the estimates $\hat{x}_2$ and $\hat{x}_3$ converge to the original states (22), for the regions where $ab\hat{z}_1 e^{bx_2} \cong 0V$.

We can conclude that the difficulties in recovering the dynamics of the jerk system (2) when its third state is chosen as output have two causes: the approximations in the exponential terms and bifurcation parameters illustrated in Fig. 4, and those due to the observability singularities highlighted in Fig. 5, where the gradient algorithm, with initial guess $(x_1(0), x_2(0))$, was used.

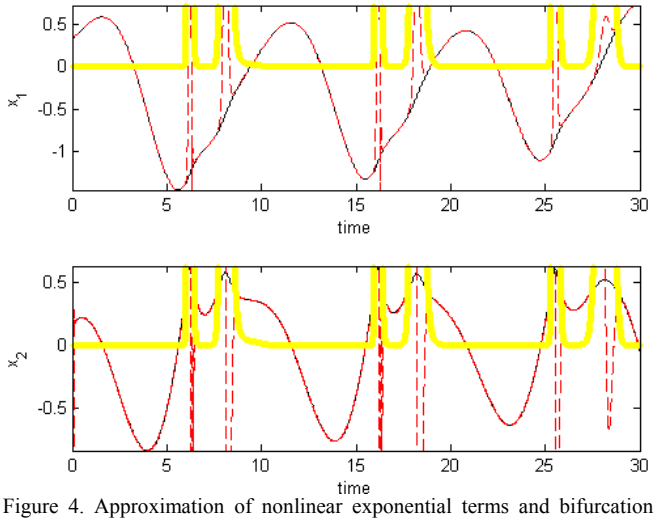

Figure 4. Approximation of nonlinear exponential terms and bifurcation parameter a to zero. The output of the transmitter is $y = x_3$. Estimation of its first and second state. Original signals in solid line, estimates in dashed line. In bold line $abx_3 \exp(bx_2)$.

Nevertheless, even if a great part of the transmitter's dynamics can be recovered by using these approximations, the neglected nonlinearities are essential for the chaotic behavior. This makes the third state unusable for cryptographic purposes.

V. Conclusion

The three states of the Sprott's jerk circuit were analyzed in terms of the local observability they ensure for the original dynamics when transmitted as a scalar data series.

The states x_1 and x_2 guarantee the full reconstruction of the transmitter's state space, the transformation they engender between the original state space and the one the receiver sees being a local diffeomorphism.

The third state generates a non-invertible transformation, in some regions of the state space, due to the appearance in its derivatives of the exponential nonlinearities which induce the chaotic behavior. Given that the unmeasured state variables containing these nonlinearities remain inaccessible to the receiver, some approximations were made, allowing the partial reconstruction of the dynamics of the transmitter. But, since these nonlinearities are essential for the chaotic behavior, this makes the third state unusable for cryptographic purposes.

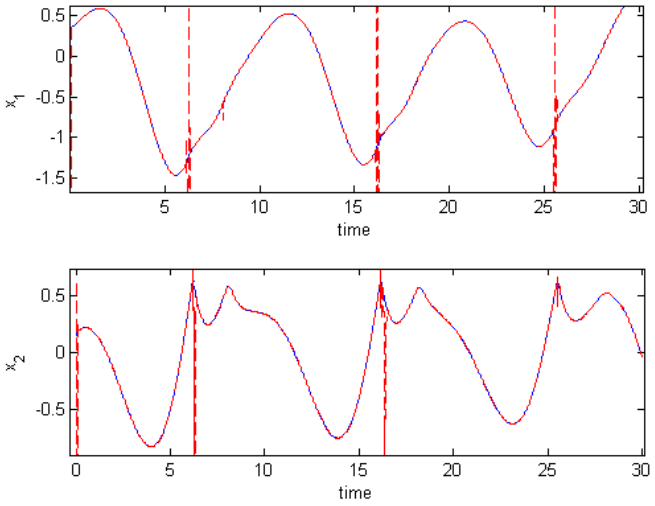

Figure 5. The gradient algorithm applied to the estimation of the first and the second state of the transmitter when its output is $y = x_3$. Original signals in solid line, estimates in dashed line.

In conclusion, for Sprott's circuit, any of its first two states, chosen as output, enables accurate estimation of the transmitter's dynamics, while its third state is to be avoided when designing a communication scheme. The considered system is intended to be used as transmitter in an extension of the scheme proposed in [32] for the Colpitts chaotic oscillator [33].

The analysis may be applied to any other chaotic circuit whose functionality is based on bipolar junction transistors or diodes, due to the exponential nonlinearity specific to the Ebers-Moll model, being the first step prior to designing the actual communication scheme.

References

[1] L. Kocarev, "Chaos-based cryptography: a brief overview", Circuits and Systems Magazine, IEEE 1 (3), 6-21. Inst. for Nonlinear Sci., California Univ., San Diego, La Jolla, 09/2002. DOI: 10.1109/7384.963463

[2] G. Jakimoski, L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps", IEEE Transactions On Circuits And Systems—I: Fundamental Theory And Applications, Vol. 48, No. 2, February 2001. [Online]. Available: http://dx.doi.org/10.1109/81.904880

[3] C. Pellicer-Lostao, R. López-Ruiz, "Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem", Chapter 12 from Applied Cryptography and Network Security, edited by Jaydip Sen, ISBN 978-953-51-0218-2, Published: March 14, 2012 under CC BY 3.0 license, DOI: 10.5772/36419. [Online]. Available: http://dx.doi.org/10.5772/36419

[4] R.L. Devaney, "An introduction to Chaotic Dynamical Systems", Perseus Books (Second Ed. 1989).

[5] V. Grigoraș, C. Grigoraș, "A Novel Chaotic System for Random Pulse Generation", Advances in Electrical and Computer Engineering: AECE, Vol. 14, Issue: 2, 2014, ISSN: 1582-7445, eISSN: 1844-7600. [Online]. Available: http://dx.doi.org/10.4316/AECE.2014.02018

[6] S. Vlad, Ş-Gh. Pentiuc, "Searching of Chaotic Elements in Hydrology", Journal of Applied Computer Science & Mathematics, no. 16 (32), 2014, Suceava.

[7] S. Vlad, P. Pascu, N. Morariu, "Chaos Models in Economics", Journal of Computing, Vol. 2, Issue 1, January 2010, ISSN 2151-9617, pp. 79-83.

[8] G. Mahalu, A. Graur, "The Fractal Techniques Applied in Pattern Recognition", The Eighth All-Ukrainian International Conference, Ukrobrez'2006, 28-31 August, 2006, Kyjiv, Ukraine, ISSB/ISBN: ISBN 966-02-4096-1, pp. 35-38, (2006).

[9] S. Pohoață, O. German, A. Graur, "Dual tasking: gait and tremor in Parkinson's disease – acquisition, processing and clustering", Rev. Roum. Sci. Techn. – Électrotechn. et Énerg., 58, 3, p. 324–334, Bucharest, 2013.

[10] G. Alvarez, S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006. [Online]. Available: http://dx.doi.org/10.1142/S0218127406015970

[11] G. Jakimoski, L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms", Physics Letters A 291 (2001) 381–384, 17 December 2001. [Online]. Available: http://dx.doi.org/10.1016/S0375-9601(01)00771-X

[12] G. Alvarez, J.- M. Amigo, D. Arroyo, S. Li, "Lessons learnt from the cryptanalysis of chaos-based ciphers", Chapter 8, Chaos-Based Cryptography: Theory, Algorithms and Applications, pp. 257-295, Springer-Verlag GmbH, 2011. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-20542-2_8

[13] J. C. Sprott, "A new chaotic jerk circuit", J. C. IEEE Transactions on Circuits and Systems-II: Express Briefs 58, 240-243, 2011. [Online]. Available: http://dx.doi.org/10.1109/TCSII.2011.2124490

[14] Z. Fu and J. Heidel, "Non-chaotic behaviour in three-dimensional quadratic systems", Nonlinearity 10 (1997) 1289–1303, Printed in the UK, PII: S0951-7715(97)78288-4. [Online]. Available: http://dx.doi.org/10.1088/0951-7715/10/5/014

[15] B. Mumuangsaen, B. Srisuchinwong, J.C. Sprott (2011), "Generalization of the Simplest Autonomous Chaotic System", Physics Letters A, Vol. 375, No. 12, March, pp. 1445-1450. [Online]. Available: http://dx.doi.org/10.1016/j.physleta.2011.02.028

[16] A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano, "Determining Lyapunov exponents from a time series", Physica D, Vol. 16, pp. 285-317, 1985. [Online]. Available: http://dx.doi.org/10.1016/0167-2789(85)90011-9

[17] H.-T. Yau, Y.-C. Pu, S. Cimin Li, "Application of a Chaotic Synchronization System to Secure Communication", ISSN 1392 – 124 X Information Technology And Control, 2012, Vol.41, No.3.

[18] D. I. R. Almeida, J. Alvarez, J. G. Barajas, "Robust synchronization of Sprott circuits using sliding mode control", Chaos, Solitons and Fractals Vol. 30(1), 2006, 11-18. [Online]. Available: http://dx.doi.org/10.1016/j.chaos.2005.09.011

[19] A. Levant, "Robust exact differentiation via sliding mode technique", Automatica, vol. 34, no. 3, pp. 379–384, 1998. [Online]. Available: http://dx.doi.org/10.1016/S0005-1098(97)00209-4

[20] N. H. Packard, J. P. Crutchfield, J. D. Farmer, R. S. Shaw, "Geometry from a time series", Physical Review Letters, 45 (25), pp.712-716, 1980. Available: http://dx.doi.org/10.1103/PhysRevLett.45.712

[21] G. Gouesbet, "Reconstruction of Standard and Inverse Vector Fields Equivalent to a Rössler system", Physical Review A, 44 (26), pp. 6264-6280, 1991. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.44.6264

[22] G. B. Mindlin, H. G. Solari, M. A. Natiello, R. Gilmore, X. J. Hou, "Topological Analysis of Chaotic Time Series Data from the Belousov-Zhabotinski", Journal of Nonlinear Sciences, 1, pp. 147-173, 1991. [Online]. Available: http://dx.doi.org/10.1007/BF01209064

[23] C. Letellier, L. A. Aguirre and J. Maquet, "How the choice of the observable may influence the analysis of non linear dynamical systems", Communications in Nonlinear Science and Numerical Simulation, Vol. 11 (5), 555-576, 2006. [Online]. Available: http://dx.doi.org/10.1016/j.cnsns.2005.01.003

[24] C. Letellier and L. A. Aguirre, "Interplay between synchronization, observability, and dynamics", Physical Review E, Vol. 82, 016204, 2010. Available: http://dx.doi.org/10.1103/PhysRevE.82.016204

[25] M. Demazure, "Catastrophes et Bifurcations", Ellipse, Paris, 1989.

[26] R. Hermann and A. Krener, "Nonlinear controllability and observability", IEEE Transactions on Automatic Control, vol. 22, no. 5, pp.728–740, 1977. [Online]. Available: http://dx.doi.org/10.1109/TAC.1977.1101601

[27] A. Trautman, "Remarks on the history of the notion of Lie differentiation", Variations, Geometry and Physics in honour of Demeter Krupka's sixty-fifth birthday O. Krupková and D. J. Saunders (Editors) Nova Science Publishers, pp. 297-302, 2008.

[28] M. Frunzete, J.-P. Barbot, and C. Letellier, "Influence of the singular manifold of observable states in reconstructing chaotic attractors", Physical Review E, vol. 86, 2012. PMid:23005843

[29] J.-P. Barbot, D. Boutat, and T. Floquet, "An observation algorithm for nonlinear systems with unknown inputs", Automatica, vol. 45, no. 8, pp.1970-1974, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.automatica.2009.04.009

[30] H. Hamiche, M. Ghanes, J. P. Barbot, K. Kemih, S. Djennoune, "Hybrid dynamical systems for private digital communication", International Journal of Modelling Identification and Control 01/2013; 20(2):99-113. [Online]. Available: http://dx.doi.org/10.1504/IJMIC.2013.056182

[31] T. Boukhobza and J-P Barbot, "High Order Sliding Modes Observer", Proceeding of the 37th IEEE CDC, Tampa USA, pp. 1912-1917, 1998. [Online]Available: http://dx.doi.org/10.1109/CDC.1998.758591

[32] R. Tauleigne, O. Datcu, and M. Stanciu, "Thwarting cryptanalytic attacks based on the correlation function", The 10th International Conference on Communications (COMM 2014), Bucharest, May 2014. [Online]. Available: 10.1109/ICComm.2014.6866745

[33] M. P. Kennedy, "Chaos in the Colpitts oscillator", IEEE Transactions On Circuits and Systems - 1 CAS, 41 (27):771-774, 1994. [Online]. Available: http://dx.doi.org/10.1109/81.331536