Chaotic Synchronization Signal Shape Alteration as Seen by a Higher-Order Sliding-Mode Observer

Octaviana Datcu*, Mihai Stanciu
University Politehnica of Bucharest, Faculty of Electronics, Telecommunications and Information Technology

Abstract: A method to overcome a correlation function based cryptanalytic attack in the case of chaos-based cryptography was proposed in the literature. The output of the transmitter, the synchronization message, was digitized and the weights of the bits of its binary representation were changed with a secret key consisting in a permutation only known by the two communication partners. The receiver was evolving according to the same equations as the transmitter. The present paper tests the feasibility of such an alteration of the synchronization signal, when the receiver does not have the same structure as the transmitter, being represented by a high-order sliding-mode observer. Simulation results are given for a chaotic Sprott's jerk circuit. Conclusions are drawn with respect to a physical implementation of such a schematic and the steps of the modified algorithm are summarized.

Key Words: chaotic synchronization, sliding-mode observer, cryptography, shape alteration.

1. INTRODUCTION
Applications of chaos theory are found in many domains as true random number generators (Cret, 2012; Ilyas, 2013), economy (Scarlat, 2006), physics (Stan, 2008), management (Scarlat, 2010), communications (Sterian, 2010; Vlădeanu, 2004), symmetric and asymmetric cryptography (Zoghabi, 2013). A survey of existing chaos-based data encryption techniques and their application areas is presented in (Shukla, 2015). Research in the chaos-based field has occasioned its counterpart, cryptanalysis of such ciphers (a survey in (Li, 2007), enabling the formulation of a common framework for the designing of chaos based cryptosystems in (Alvarez, 2006). (Teodorescu, 2012) reviews several methods of determining features of the attractors, characterizing chaotic systems that are suitable in engineering and medical applications, such as control, measurement, and pattern recognition, based on chaotic dynamics.

The present work aims to contribute to the area of symmetric cryptography based on chaotic synchronization (Boccaletti, 2002). The Colpitts oscillator, considered in (DeFeo, 2000) as a paradigm for sinusoidal oscillation, was used as chaotic transmitter and receiver in (Taulieugne, 2014). A countermeasure to autocorrelation function based attacks (see, for example, (Sobhy, 2001) was proposed, by digitizing the synchronization signal, transmitted over the unsecure communication channel, and by changing the weight of the bits in its binary representation. The secret-key was constituted by the bit permutation, the scheme showing good results, even if the parameters and the initial conditions of the transmitter were known by the hacker.

This paper tests the feasibility of such a binary alteration of the synchronization signal, when the two communication partners do not possess the same structure, as in (Taulieugne, 2014). The synchronization between the transmitter and the receiver is achieved, this time, by using a higher-order sliding-mode observer. The fundamental nature of sliding mode control is described in (Spurgeon, 2014). Another difference from the previous work is the inclusion of the secret message in the structure of the transmitter, and not its simple addition to the synchronization signal. The chaotic system used as transmitter in this new communication scheme is the Sprott's jerk circuit (Sprott, 2011).

2. MAIN RESULTS
The chaotic jerk circuit in (2.1) promoted in (Sprott, 2011) is used as transmitter of a secret message. Its output, the signal that will be transmitted over the communication channel, is its first state, as it ensures regular local weak observability. The observability matrix for nonlinear systems, which uses Lie derivatives, is revisited in (Letellier, 2005), showing that such a matrix can be interpreted as the Jacobian matrix of the map between the original phase space and the differential embedding induced by the observable, i.e. the output of the transmitter. See (Letellier, 2006) for a detailed discussion on how the choice of the output of the transmitter influences the reconstruction of its dynamics, by the receiver, in each point of the state space. The secret message is embedded by the dynamics of the transmitter (2.1) by using the inclusion method (Perruquetti, 2005), being added, at each step, to its third equation:

\[
\begin{align*}
\dot{x_1} &= x_2 \\
\dot{x_2} &= x_3 \\
\dot{x_3} &= -x_1 - x_3 - A(e^{Bs_2} - 1) + m \\
y &= x_1
\end{align*}
\]  
(2.1)

where \( A = 10^{-9} \) and \( B = 500/13 \) are the bifurcation parameters.
At the reception, the coordinate change in (2.2), the map between the original phase space and the differential embedding induced by the observable \( y \), is used to recover the state space \((x_1, x_2, x_3)\) of the transmitter and the secret message, \( m \), when the available data series is constituted by the output \( y \) and its derivatives \( \dot{y}, \ddot{y} \).

\[
\begin{align*}
\dot{z}_1 &= y = x_1 \\
\dot{z}_2 &= \dot{y} = x_2 \\
\dot{z}_3 &= \ddot{y} = x_3 \\
\dot{z}_4 &= \dddot{y} = -x_1 - x_3 - A(e^{By_2} - 1) + m
\end{align*}
\]  
\tag{2.2}

A high order sliding mode observer (2.3) inspired by (Levant, 1998) is used to estimate the coordinates \((\hat{z}_1, \hat{z}_2, \hat{z}_3)\). The parameters of the observer are \( K \) and \( L \), whose values are chosen as follows. The derivative of the message with respect to time was neglected, as it is a piece of information the receiver does not possess. The fifth state was added in order to reduce the chattering effect (Fridman, 2002) on the estimates.

\[
\begin{align*}
\dot{\hat{z}}_1 &= \nu_1 = \hat{z}_2 + \alpha_1 \\
\dot{\hat{z}}_2 &= \nu_2 = \hat{z}_3 + \alpha_2 \\
\dot{\hat{z}}_3 &= \nu_3 = \hat{z}_4 + \alpha_3 \\
\dot{\hat{z}}_4 &= \nu_4 = \hat{z}_5 + \alpha_4 \\
\dot{\hat{z}}_5 &= \nu_5 = \hat{z}_3 - \hat{z}_5 - AB e^{B\dot{y}_2} (\hat{z}_4 + B\hat{z}_3^2) + \alpha_5
\end{align*}
\]  
\tag{2.3}

with correction terms \( \alpha_j; j = 1, \ldots, 5 \), expressed by:

\[
\begin{align*}
\alpha_1 &= \lambda_1 \cdot M^{1/5} \cdot |\hat{z}_1 - y|^{4/5} \text{sgn}[K \cdot (\hat{z}_1 - y)] \\
\alpha_2 &= \lambda_2 \cdot M^{1/4} \cdot |\hat{z}_2 - \nu_1|^{3/4} \text{sgn}[K \cdot (\hat{z}_2 - \nu_1)] \\
\alpha_3 &= \lambda_3 \cdot M^{1/3} \cdot |\hat{z}_3 - \nu_2|^{2/3} \text{sgn}[K \cdot (\hat{z}_3 - \nu_2)] \\
\alpha_4 &= \lambda_4 \cdot M^{1/2} \cdot |\hat{z}_4 - \nu_3|^{1/2} \text{sgn}[K \cdot (\hat{z}_4 - \nu_3)] \\
\alpha_5 &= \lambda_5 \cdot M \cdot \text{sgn}[K \cdot (\hat{z}_5 - \nu_4)]
\end{align*}
\]

where \( \lambda_1 = -8, \lambda_2 = -5, \lambda_3 = -3, \lambda_4 = -1.5, \lambda_5 = -1.1 \) as indicated in (Levant, 1998).

The solution of system (2.2) is given by (2.4).

\[
\begin{align*}
\hat{x}_1 &= \hat{z}_1 \\
\hat{x}_2 &= \hat{z}_2 \\
\hat{x}_3 &= \hat{z}_3 \\
\hat{m} &= \hat{z}_1 + \hat{z}_3 + \hat{z}_4 + A(e^{By_2} - 1)
\end{align*}
\]  
\tag{2.4}

The parameters \( L \) and \( K \) are to be chosen such that a good estimation of the original state space of the transmitter and of the included message is done, under as low chattering as possible. Such a good estimation is shown in Fig. 1, for \( L = 5 \cdot 10^4 \) and \( K = 10^{20} \), \((A, B) = (10^{-9}, 500/13), (x_1, x_2, x_3)_{t=0} = (0.1, 0.2, 0.3) \) and \((z_1, z_2, z_3, z_4, z_5)_{t=0} = (x_1, x_2, x_3)_{t=0} = 0.09, 0.90)\). Initial conditions \( z_4_{t=0} \) and \( z_5_{t=0} \) were chosen from a random uniform distribution in \([0,1]\) and truncated to two decimals. The secret message is chosen to be a sine, a square, a sawtooth wave or even a random signal, at frequency \( f = 0.5\text{Hz} \) and amplitude \( U = 0.2V \).

The cutoff frequency of the low-pass first order Butterworth filter used after the deduction of the value of the message from the estimated vector \( \hat{z} = (\hat{z}_1, \hat{z}_2, \hat{z}_3, \hat{z}_4) \) is set at \( f_{-3dB} = 5 \cdot 2\pi f [\text{Hz}] \), in order to have a number of harmonics that allows the reconstruction of the non-sinusoidal messages. The criterion used to appreciate the accuracy of the estimation is the estimation error:

\[
e_m = m - \hat{m}
\]  
\tag{2.4}
The distribution of this error, for the estimation of the message represented by a sine, square, sawtooth, respectively a random wave, is also given in Fig. 1. It can be observed that the error represents less than 10% of the message signal. This will be the accepted threshold in the remainder of our argumentation.

**Figure 1** Estimation of the secret message and the corresponding errors. The observer is initialized with the same initial conditions as the transmitter and \((L, K) = (5 \cdot 10^7, 10^{35})\). Original signal in solid, estimated in dashed line.

a) sinusoidal message; b) rectangular message.

c) sawtooth message; d) random message.

As the observer was initialized from the same state as the transmitter for the distributions in Fig. 1, when computing the estimation error, all the samples of the messages were considered, the synchronization being established from the beginning. If the initial conditions of the observer are different from those of the transmitter, as in Fig. 2, the samples prior to synchronization will be dropped. In Fig. 2, the first period of the message was not considered when the distribution of the error was computed. Initial conditions \(\{z_1, z_2, z_3, z_4, z_5\}_{k=0} = (x_1|_{k=0}, 0.27, 0.63, 0.09, 0.90)\) were chosen from a random uniform distribution in \([0,1]\) and truncated at two decimals, except for the one corresponding to the transmitted state, i.e. \(z_1|_{k=0}\). The estimation error is, again, under the desired threshold, i.e. 10% of the magnitude of the message.
Figure 2 Estimation of the secret message and the distribution of the corresponding error. The observer is with 
\[ (z_1, z_2, z_3, z_4, z_5) \big|_{t=0} = (x_1)_{t=0} = 0.27, 0.63, 0.09, 0.90 \]. The bifurcation parameters for the observer and the 
transmitter are the same (left), while \( B_2 = 38.5 \neq B_1 = 500/13 \) (right). In solid line, the original signal, in 
dashed line, the estimation.

Once the synchronization conditions are established in analog transmission, the observer is correctly tuned 
for accurate estimation, the analog to decimal conversion of the signal transmitted over the communication channel, 
\( y = x_1 \) is done, and the weights of the bits from its binary representation are changed according to a secret 
permutation known only by the two legal communication partners. The message considered in the following is 
sinusoidal, and the cutoff frequency of the filter is diminished at \( f_{-3dB} = 2\pi \), as the magnitude of the signal is 
contained by the fundamental frequency for a sine-wave.

To decide how many bits are necessary for the binary representation of the synchronization signal, the 
transmitter has to look at the accuracy obtained, in analog transmission, when estimating its states by using the high-
order sliding-mode observer with the chosen parameters \( L \) and \( K \). The error in the digital-to-analog conversion of 
the synchronization signal must be approximately equal to the error done by the high-order sliding-mode observer 
when estimating the first state of the transmitter. Thus, the error \( e_{x_1} \) from (2.5) is considered, given that the 
synchronization signal, the output of the transmitter (2.1), is \( x_1 \).

\[
e_{x_1} = x_1 - \hat{x}_1; e_{x_2} = x_2 - \hat{x}_2; e_{x_3} = x_3 - \hat{x}_3;
\]

(2.5)

Thus, for the chosen parameters \( L = 5 \cdot 10^4 \) and \( K = 10^{20} \), the least significant bit voltage must be approximately 
\( V_{LSB} = \frac{\max(x_i) - \min(x_i)}{2^n - 1} = 10^{-13}V \), as presented in Fig. 3, which implies 
\( n = \log_2 \left\{ \frac{\max(x_i) - \min(x_i)}{10^{13} + 1} \right\} \) bits. As the range covered by the output of the transmitter is 
\( \max(x_i) - \min(x_i) \approx 2.56V \), the number of necessary bits is \( n \approx 44.5 \) bits. It is obvious that such a precision is 
out of question due to the delicacy implied by the technology needed to overcome the sensitivity to noise of circuits 
designed to achieve a resolution of \( V_{LSB} = 0.1pV \).
Figure 3 Estimation of the states $x_1, x_2, x_3$ and the corresponding probability distribution functions for the estimation errors. The observer is initialized with the same initial conditions and parameters as the transmitter.

Parameters $L = 5 \cdot 10^4$ and $K = 10^{20}$.

Nevertheless, the distribution of the error corresponding to the estimation of the sinusoidal message in Fig. 1 shows that, for the error $e_{x_1} \cong 10^{-13} V$, the error $e_m \in (-0.6, 0.6) mV$, which is lower than the established threshold $\pm 20 mV$, representing 10% of the amplitude of the message. By comparing Fig. 4, results obtained for $n = 35 bits$, and Fig. 5, for $n = 34$ bits one can conclude that, for the established threshold of $\pm 20 mV$, for the estimation error $e_m$, there are necessary at least $n = 35$ bits.

Figure 4 The probability distribution functions for the estimation errors. Digitization of the synchronization signal is on $n = 35$ bits. The observer is initialized with the same initial conditions and parameters as the transmitter.

Parameters $L = 5 \cdot 10^4$ and $K = 10^{20}$.
The probability distribution functions for the estimation errors. Digitization of the synchronization signal on $n = 34$ bits. The observer is initialized with the same initial conditions and parameters as the transmitter.

Parameters $L = 5 \cdot 10^4$ and $K = 10^{20}$.

In conclusion, even if the proposed scheme is feasible, the cost of such a practical circuit is too high to justify its implementation at large scale, due to the high precision it requires (at least $\pm 3 \cdot 10^{-11}V$).

Nevertheless, if the algorithm would be applied, its steps could be summarized as follows: (1) choose a chaotic transmitter; (2) analyze its observability properties in order to decide which is its best output state, from this point of view; (3) choose the appropriate wave, its amplitude and frequency, corresponding to the secret message included in the dynamics of the transmitter; (4) set the order and the cutoff frequency of the low-pass filter needed to recover the secret message from the estimated state-space of the transmitter; (5) build the model of the communication scheme with the chosen transmitter, its output being sent to a high-order sliding-mode observer, which recovers the state-space of the transmitter; (6) deduce the expression of the secret message as a function of the states of the transmitter (the left inversion stage); (7) test the built configuration, in an analog configuration, for different values of the parameters of the observer until the desired precision is achieved; (8) knowing the dynamic range of the output and the desired estimation accuracy, deduce the number of bits necessary for the analog-to-digital conversion of the synchronization signal; (9) alter the output by changing the weights of its binary representation according to a certain permutation; (10) exchange the secret key with the communication partner; it consists in the values of the parameters of the observer, established at step (7), the permutation chosen at (9), and the initial conditions and the parameters; the frequency of the low-pass filter is a useful information; (11) at the reception end, digitize the received signal on a number of bits equal to the number of the columns of the secret permutation and apply its inverse to retrieve the real synchronization signal; (12) reconvert in analog; (13) apply the obtained signal at the input of the assigned high-order sliding-mode observer; (14) obtain the state-space of the transmitter; (15) use the function existing between the secret message and the states of the transmitter to obtain it from the estimation of the state-space; (16) filter the result of the step (15) and process the secret message, according to the desired application.

The communication scheme proposed in this paper differs from the previous work, essentially in the following aspects: the receiver evolves according to different equations compared to the ones corresponding to the transmitter; the chaotic system chosen as the transmitter is, here, the Sprott’s jerk circuit, and not the Colpitts oscillator; the message is included in the structure of the transmitter, and not added to the synchronization signal.

More simulations and the executables, obtained from Matlab-Simulink version R2013a, are given at http://catedra.elcom.pub.ro/~od/.

3. CONCLUSIONS

A previous work, (Tauleigne, 2014), proposed a method to overcome a correlation function based cryptanalytic attack in the case of chaos-based cryptography. The output of the transmitter, the synchronization message, was digitized and the weights of the bits of the binary representation were changed with a secret key consisting in a permutation only known by the two communication partners. The receiver was evolving according to the same equations as the transmitter. Once the synchronization signal was correctly restored, the receiver has no difficulty in achieving the same dynamics as the transmitter and recovers the secret message.

The present paper tests the feasibility of such an alteration of the synchronization signal, when the receiver does not have the same structure as the transmitter. This time, the receiver has knowledge only on the output of the transmitter and its derivatives. The assigned observer estimates the synchronization signal and, by using its
derivatives, restores the other states of the transmitter, and the secret message included in its dynamics. The reconstruction of the dynamics of the transmitter is done with a certain error, associated with the parameters chosen for the observer. This error has to be approximately equal to the one engendered by the digitization, in order to obtain the estimation of the message with a required precision. The threshold was established here at $\pm 10\%$ of the magnitude of the message.

Given the dynamical range of the considered system, the Sprott's jerk chaotic circuit, and the magnitude of the message, which has to be small enough so that it does not alter the chaotic behavior of the transmitter, the number of bits required for the digitization is too high to justify its implementation at large scale, due to the high precision it requires. The resolution required by the digital-to-analog (analog-to-digital) conversion, when the observer is a higher-order sliding-mode differentiator, is about $15nV$, corresponding to 34 bits converters. This implementation is usually not feasible with common technology. Nevertheless, it still remains possible that the bit-alteration of the synchronization signal method works well with other types of observers, other that the high-order sliding-modes.

ACKNOWLEDGEMENTS

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.

REFERENCES


24