Determination of the Parameters for a Lorenz System and Application to Break the Security of Two-channel Chaotic Cryptosystems

A.B. Orue[a], V. Fernandez[a], G. Alvarez[a], G. Pastor[a],
M. Romera[a], Shujun Li[b], F. Montoya[a] *

[a] *Instituto de Física Aplicada, CSIC, Serrano 144, 28006 Madrid, Spain*
[b] *Fachbereich Informatik und Informationswissenschaft, Universitt Konstanz, Universittsstraße 10, 78457 Konstanz, Germany*

Abstract

This Letter describes how to determine the parameter of the chaotic Lorenz system used in a two-channel cryptosystem. First the geometrical properties of the Lorenz system are used to reduce the parameter search space. Second the parameters are exactly determined - directly from the ciphertext - through the minimization of the average jamming noise power created by the encryption process.

Key words: Secure communication, Cryptanalysis, Synchronization, Lorenz chaotic system.
PACS: 05.45.Ac, 47.20.Ky.

1 Introduction

In recent years, a growing number of cryptosystems based on chaos synchronization have been proposed [1], many of them fundamentally flawed by a lack of robustness and security.

* Corresponding author: Email: fausto@iec.csic.es

The first cryptographic schemes based on chaos synchronization were based on masking the plaintext message by a variable of the chaotic generator system [2–4]. Sender and receiver must be synchronized in order to regenerate the chaotic signal at the receiver and thus recover the message. However this simple design is easily broken by elemental filtering of the ciphertext signal [5–7].

Recently, some work based on chaotic cryptosystems with an enhanced-plaintext-concealing mechanism have appeared in the literature [8–12]. In some of these cryptosystems the ciphertext consists of a complex non-linear combination of the plaintext and a variable of a chaotic transmitter's generator, from which retrieving a clean plaintext becomes an unattainable goal. As it was not possible to synchronize a chaotic receiver with such ciphertext, a second channel had to be inserted in the system for this purpose. The synchronizing signal was a different chaotic variable generated by the sender, which was transmitted without any additional modification. The same values for the parameters were used at sender and receiver [10–12].

One of the cryptosystems described above, proposed by Jiang [10], made use of the Lorenz chaotic system [13], which is defined by the following equations:

$$\begin{aligned} \dot{x} &= \sigma(y - x), \\ \dot{y} &= \rho x - y - xz, \\ \dot{z} &= xy - \beta z, \end{aligned} \tag{1}$$

where σ, ρ and β are fixed parameters.

The ciphertext s was defined as

$$s = f_1(x, y, z) + f_2(x, y, z)\, m, \tag{2}$$

where m is the plaintext.

The receiver was designed as a reduced-order non-linear observer with a mechanism to achieve efficient partial synchronization under the drive of $x(t)$. It can generate two signals $y_r(t)$ and $z_r(t)$ that converge to the driver system's variables $y(t)$ and $z(t)$, respectively, as $t \to \infty$.

The recovered plaintext $m^*(t)$ was retrieved using the following function:

$$m^* = \frac{s}{f_2(x, y_r, z_r)} - \frac{f_1(x, y_r, z_r)}{f_2(x, y_r, z_r)}. \tag{3}$$

An example with the functions:

$$\begin{aligned} f_1(x, y, z) &= y^2, \\ f_2(x, y, z) &= 1 + y^2, \end{aligned} \tag{4}$$

and the following parameter values: $\sigma = 10$, $\rho = 28$ and $\beta = 8/3$;

and the following initial conditions: $(x(0), y(0), z(0)) = (0, 0.01, 0.01)$ and $(y_r(0), z_r(0)) = (0.05, 0.05)$ was given in [10, §III]. The plaintext was a small-amplitude sinusoidal signal of 30 Hz, $m(t) = 0.05 \sin(2\pi 30t)$. The author claims this cryptosystem guarantees higher security and privacy, showing that an error of 0.05 in the retrieval of y_r due to a poor parameter estimation, gives rise to a serious distortion in the retrieved plaintext.

The vast majority of continuous chaotic cryptosystems are based on the synchronization of drive and response subsystems [14,15], in this regard they are similar to the conventional self-synchronizing stream ciphers [16,17]. Their security relies on the secrecy of the chaotic system's parameters, or some other complementary parameters that control how the plaintext is included or other additional masking signals [8,18], which all together play the role of the secret key [19]. Hence, finding these parameters is equivalent to breaking the system. Due to the self-synchronizing mechanism of these systems the initial conditions are not part of the key.

Recently, Solak [20] analyzed the cryptosystem described in [10] and showed how an eavesdropper could identify the value of the parameter ρ, provided that he has the previous knowledge of the remaining two parameters of the transmitter's system β and σ. Solak's approach was based on a novel expression of the Lorenz system. Previously Stojanovski, Kocarev and Parlitz [21] had described a generic method to reveal simultaneously all three parameters of a Lorenz system when one of the variables $x(t)$ or $y(t)$ were known. Such method could be applied to break this cryptosystem.

The present work describes an efficient method of determining the two only unknown parameters ρ and β of [10] needed to build up an intruder Lorenz system's receiver, from the ciphertext alone, i.e. without partial knowledge of any of the transmitter's parameters. First, some geometrical properties of the Lorenz attractor are shown. Then, these are used to minimize, as much as possible, the parameters' search space. Finally, the parameters of the unknown receiver are determined with high accuracy.

2 The Lorenz attractor's geometrical properties

According to [13], the Lorenz system has three equilibrium points. The origin is an equilibrium point for all values of the parameters. For $0 < \rho < 1$ the origin is a globally attracting asymptotically stable sink. For $1 \leq \rho \leq \rho_H$ the origin becomes a non-stable saddle point, giving rise to two other stable twin equilibrium points C^+ and C^-, of coordinates $x_{C^\pm} = \pm\sqrt{\beta(\rho-1)}$, $y_{C^\pm} = \pm\sqrt{\beta(\rho-1)}$ and $z_{C^\pm} = \rho - 1$, being ρ_H a critical value, corresponding to a

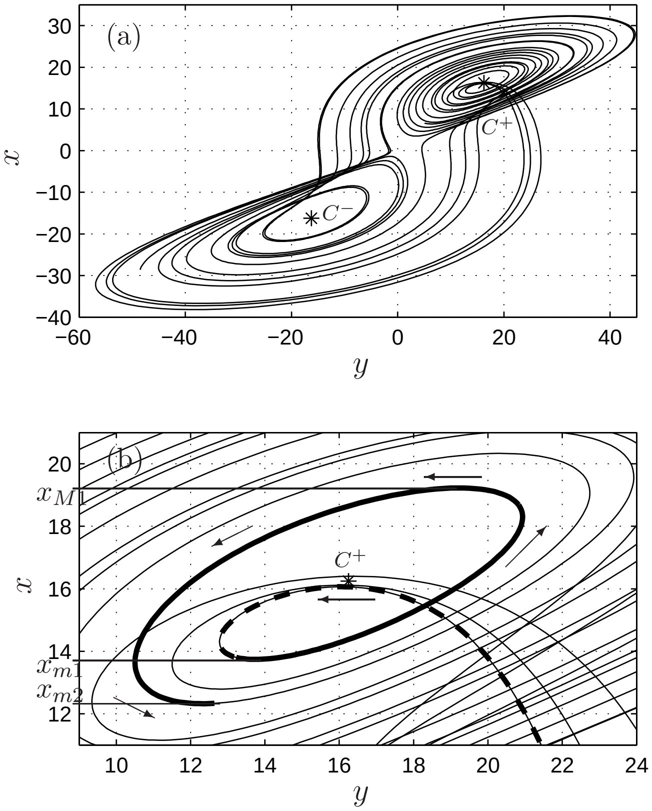

Fig. 1. Lorenz chaotic attractor; (a) $x - y$ plane projection; (b) enlarged view, showing the incoming trajectories portion attracted by the equilibrium point C^+. The flow direction is indicated by arrows. The position of the equilibrium points C^+ and C^- is indicated by asterisks.

Hopf bifurcation [22], of value:

$$\rho_H = \frac{\sigma(\sigma + \beta + 3)}{(\sigma - \beta - 1)}. \tag{5}$$

When ρ exceeds the critical value ρ_H the equilibrium points C^+ and C^- become non-stable saddle foci, by a Hopf bifurcation, and the strange Lorenz attractor appears. The flow, linearized around C^+ and C^-, has one negative real eigenvalue and a complex conjugate pair of eigenvalues with positive real part. As a consequence, the equilibrium points are linearly attracting and spirally repelling.

Figure 1(a) shows the double scroll Lorenz attractor formed by the projection –on the $x - y$ plane– in the phase space of a trajectory portion extending along 12 s. The parameters are $\sigma = 16$, $\rho = 100$ and $\beta = 8/3$.

It is a well-known fact that the trajectory of the Lorenz attractor draws two 3D loops, in the vicinity of the equilibrium points C^+ and C^-. This trajectory has the shape of a spiral of steadily growing amplitude, jumping from one

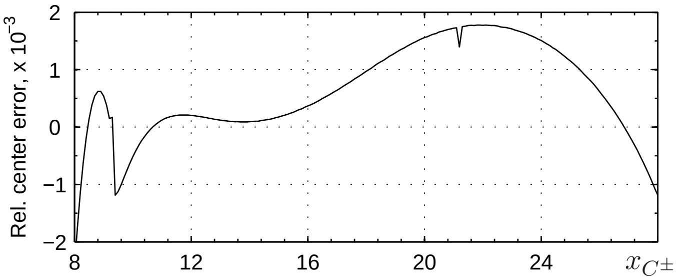

Fig. 2. Relative error associated to the estimation of the equilibrium points $C^{\pm}$, when taking the eye center's coordinate $x^*_{C^\pm}$ instead of its true value $x_{C^\pm}$.

equilibrium point to the other, at irregular intervals, in a random −although deterministic– manner [13]. The trajectory may pass arbitrarily near the equilibrium points, but never reach them while in chaotic regime.

The geometrical properties of the Lorenz system allow for a previous reduction of the search space of the parameters ρ and β, taking advantage of the relationship between them at the equilibrium points of coordinates $x_{C^\pm} = \pm\sqrt{\beta(\rho - 1)}$.

Let us call the two neighborhood regions around the equilibrium points that are not filled with the spiral trajectory the *attractor eyes*. The eyes' centres are the fixed points C^+ and C^-.

The pending problem is to determine the eyes' centres when the inner turns are missing, as it happens in normal chaotic regime. With the drive signal $x(t)$, we solved it experimentally by estimating the middle point value between the trajectory of maxima and minima in the phase space projection on the $x - y$ plane. The most accurate result was obtained by taking into account only the regular spiral cycle closest to the center, shown in Fig. 1(b) as a thick continuous line. The x-coordinate of the eye center was calculated by using the following empirical formula:

$$x^*_{C^\pm} = \frac{0.9\ x_{m1} + 0.1\ x_{m2} + x_{M1}}{2}, \tag{6}$$

where x_{M1} is the minimum value of all the maxima of the spiral trajectory $|x(t)|$ and x_{m1} and x_{m2} are the two minima immediately preceding and following x_{M1}, respectively.

As the spiral has a growing radius, it was necessary to take a weighted mean between the two minima x_{m1} and x_{m2}, being the optimal values of the two weights experimentally determined. Instead of making two computations, one around C^+ and another around C^-, a unique computation was performed on the absolute value of the waveform $x(t)$, $|x(t)|$. It should be noted that the maxima that take place after a change of sign of $x(t)$ and $y(t)$ must be discarded as they belong to the incoming trajectory portion attracted by the equilibrium points $C^{\pm}$ and do not belong to the spiral trajectory. This is illustrated in Fig. 1(b) as a thick dashed line.

Figure 2 illustrates the relative error $(x^*_{C^\pm} - x_{C^\pm})/x_{C^\pm}$ of the estimation of $x_{C^\pm}$ when taking the eye center's coordinate $x^*_{C^\pm}$ instead of its true value $x_{C^\pm}$; it can be seen that its magnitude is less than 2×10^{-3}. The parameters of the system were varied in the margins: $\sigma \in (9.7, 37.4)$, $\rho \in (25.6, 94.8)$ and $\beta \in (2.6, 8.4)$. The initial conditions of the system were the same as those described in [10, §III]; the period of the measurement was 20 s and the sampling frequency was 1200 Hz[1].

Therefore the search space of the unknown parameters β and ρ is reduced to a narrow margin defined as $\beta^*(\rho^* - 1) \in \{0.996\, x^{*2}_{C^\pm}, 1.004\, x^{*2}_{C^\pm}\}$. The parameter σ is also unknown; but, as described in Sec. 3, its knowledge is not necessary to assemble an intruder receiver capable of breaking the system.

Applying this method to the proposed example described in [10, §III], whose equilibrium point is $x_{C^\pm} = \sqrt{72}$, the absolute error when determining $x^*_{C^\pm}$ was 7.5×10^{-4}, which is equivalent to a relative error smaller than 0.01%.

3 Breaking of the proposed encryption system

We designed an intruder receiver system based on a homogeneous driving synchronization mechanism [23] between the transmitter's drive Lorenz system and a receiver response subsystem. The receiver response subsystem was a partial duplicate of the drive system reduced to only two variables $y_r(t)$ and $z_r(t)$, driven by the drive variable $x(t)$. The receiver response subsystem was defined by the following equations:

$$\begin{aligned} \dot{y}_r &= \rho x - y_r - x z_r, \\ \dot{z}_r &= x y_r - \beta z_r. \end{aligned} \tag{7}$$

Note that for breaking the system it is only necessary to attain the values of the parameters ρ and β. This means that the parameter σ can be ignored and need not to be determined, unlike in the Solak method [20] where its previous knowledge is required, or in the Stojanovski et al. method [21], where the simultaneous determination of all the three unknown parameters is required.

As it was shown in [14] and [23, §III], when the drive is x and the response is (y_r, z_r), the two conditional Lyapunov exponents of the Lorenz system are negative, thus leading to a very stable system with fast synchronization. The

[1] All the results presented here were based on simulations using MATLAB , the Lorenz integration algorithm was a four-fifth order Runge-Kutta with an absolute error tolerance of 10^{-9} and a relative error tolerance of 10^{-6}.

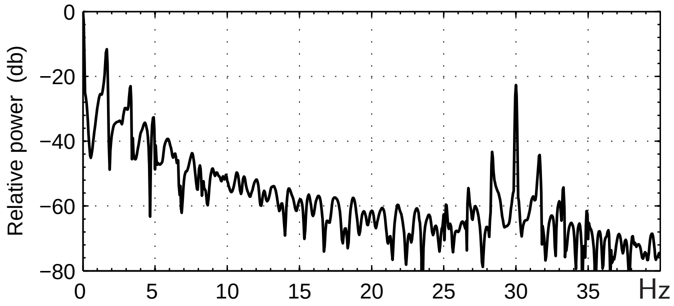

Fig. 3. Logarithmic power spectrum of the retrieved plaintext with a wrong guessing for the response system's parameters.

consequence is that, if the parameters of drive and response systems are moderately different, the drive and response variables will be alike, though not totally identical. This property may be exploited to search the correct parameter values by looking at the retrieved plaintext and applying an optimization procedure to find the parameters that provide the best retrieved-plaintext quality.

When the synchronizing signal is fed to the response system described by Eq. (7) and the parameters of both systems agree, i.e. $\rho^* = \rho$ and $\beta^* = \beta$, then variables y and y_r of the drive an response systems are equal. In this case the recovered text $m^*(t)$ identically follows the plaintext $m(t)$ and the effect of different initial conditions after a very short transient is negligible. If the parameters of both systems do not agree, the recovered text will consist of a noisy distorted version of the original plaintext, growing the noise and distortion as the mismatch between drive and response systems parameters grows.

3.1 Determination of the systems's parameters

In the particular case described in [10, §III], the encryption and decryption functions were:

$$s = y^2 + (1+y^2)\, m, \tag{8}$$

$$m^* = \frac{s}{1+y_r^2} - \frac{y_r^2}{1+y_r^2}\,. \tag{9}$$

Equation (9) of the recovered text can be rewritten as:

$$m^* = m\,\frac{1+y^2}{1+y_r^2} + \frac{y^2-y_r^2}{1+y_r^2}. \tag{10}$$

The first term of this equation is a function of the plaintext message $m(t)$ and the variables y and y_r. When $y = y_r$ this term is reduced to the undistorted

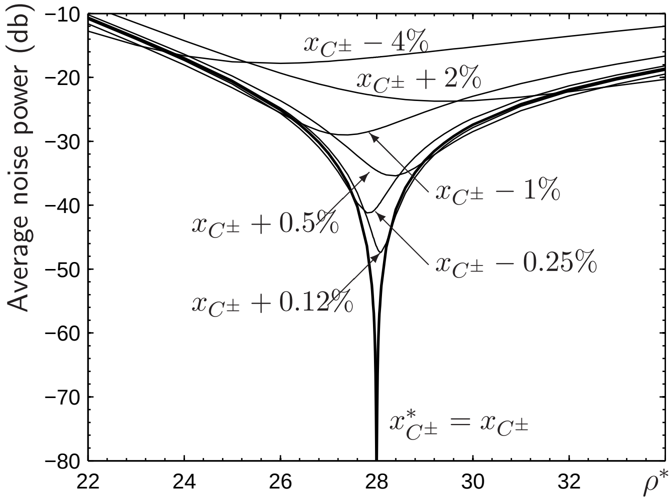

Fig. 4. Logarithmic representation of the mean of the recovered ’s noise power $\overline{\varepsilon^2}$, for several values of $x^*_{C^\pm}$.

plaintext, but if $y \neq y_r$ a noticeable distortion will appear. The second term of Eq. (10) is a function of y and y_r and can be considered as a jamming noise. Figure 3 depicts the spectrum of the recovered text corresponding to this example using a wrong guessing of the response system’s parameters of: $\rho^* = 28.01$ and $\beta^* = 2.667$. It can be seen that the spectrum has two main frequency bands: one around the plaintext $m(t)$ frequency of 30 Hz, which corresponds to the distorted plaintext, and another near 0 Hz that corresponds to the jamming noise. Assuming the plaintext will always consist of an a.c. band limited signal without d.c. component, as in the numerical example given in [10], it is clear from Fig. 3 that the second term of Eq. (10) may be isolated from the first one by means of a suitable filter.

The most important band of the jamming noise ε was isolated by means of a finite-impulse-response low-pass filter with 2048 terms and a cutoff frequency of 0.2 Hz, which suppressed the contribution of the plaintext $m(t)$ and most of the frequency terms generated by the modulation with the chaotic signal $y^2(t)$. Figure 4 illustrates the mean value of the squared noise $\overline{\varepsilon^2}$, i.e. the average noise power, as a function of ρ^*, with the eye center $x^*_{C\pm}$ as parameter, with the same parameters of the transmitter’s system of the numerical example presented in [10] and the intruder receiver’s system described by Eq. (7). The mean of ε^2 was computed along the first 20 s, after a delay of 2 seconds, to let the initial transient finish. It is clearly seen that the noise grows monotonically with the mismatch between the transmitter’s and receiver’s parameters $|\rho^* - \rho|$. It can also be noticed that the minimum error corresponds to the case where the parameters of the receiver’s system ρ^* exactly match those of the transmitter’s ρ, when $x^*_{C\pm} = x_{C^\pm} = \sqrt{\beta(\rho - 1)} = \sqrt{72}$.

The search for the correct values of the parameters β^* and ρ^* was carried out using the following procedure:

(1) Determine the approximate value of the eye center $x^*_{C\pm}$ from the $x(t)$ waveform, as described in Section 2.
(2) Keep the previous value obtained for $x^*_{C\pm}$ and vary the value of ρ^* until a minimum of the average noise power is reached.
(3) Keep the previous value of $\rho^*$and vary the value of eye center $x^*_{C\pm}$ until a new minimum of the average noise power is reached.
(4) Repeat steps (2) and (3) until a stable result of the average noise power is reached and retain the last values obtained for ρ^* and $x^*_{C\pm}$ as the final ones.
(5) Calculate the value of β^* as $\beta^* = (x^*_{C\pm})^2/(\rho^* - 1)$.

Table 1 shows the evolution of the relative eye center error, the relative ρ^* parameter error and the average jamming noise power. It can be seen that the procedure converges rapidly to the exact values of $\rho^* = \rho = 28$ and $x^*_{C\pm} = x_{C\pm} = \sqrt{72}$.

Table 1
Evolution of the relative eye center error, the relative ρ^* parameter error and the average jamming noise power.

Step	Relative eye center error	Relative ρ^* error	Average noise
	$(x^*_{C\pm} - x_{C\pm})/x_{C\pm}$	$(\rho^* - \rho)/\rho$	power $\overline{\varepsilon^2}$
1	8.90×10^{-5}		
2	$8.90 \times 10^{-5\bullet}$	-3.57×10^{-8}	5.2×10^{-8}
3	2.72×10^{-8}	$-3.57 \times 10^{-8\bullet}$	8.9×10^{-12}
4	$2.72 \times 10^{-8\bullet}$	0	6.5×10^{-13}
5	0	$0^\bullet$	6.1×10^{-13}
6	$0^\bullet$	0	6.1×10^{-13}

• = old data held from the previous step

The value of the unknown parameter β^* was deduced using the estimated values of ρ^* and $x^*_{C\pm}$ from Eq. (6)and $\beta^* = \frac{(x^*_{C\pm})^2}{(\rho^* - 1)} = \frac{8}{3}$.

Note that this method also works for the general case described by Eqs. (2) and (3). These equations have similar structure to Eqs. (8) and (9), which describe the special case described in [10, §III], which was chosen here for experimental demonstration.

3.2 Retrieving of the plaintext

As the system's parameters are equivalent to the system's key, once the exact values of β^* and ρ^* are known, the ciphertext can be efficiently decrypted by the intruder receiver system defined by Eq. (7). Figure 5 shows the three

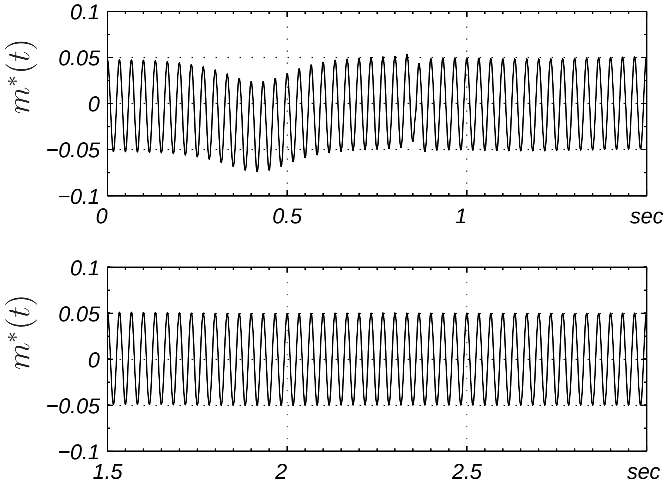

Fig. 5. Retrieved plaintext with the ultimate values of the response system parameters.

first seconds of the retrieved plaintext using the response system described by Eq. (7), corresponding to the ciphertext used in [10, §III]. It can be seen that the plaintext is perfectly recovered after a short transient period of less than one second.

4 Simulations

All the results presented here were based on simulations using MATLAB , the Lorenz integration algorithm was a four-fifth order Runge-Kutta with an absolute error tolerance of 10^{-9} and a relative error tolerance of 10^{-6}.

5 Conclusions

A simple method was proposed to reduce the parameter search space of the Lorenz system, based on the determination of the system's equilibrium points from the analysis of the waveform of one of its variables $x(t)$. This method was then applied to the cryptanalysis of the cryptosystem [10], showing that this is rather weak since it can be broken without knowing the values of its parameters. The total lack of security discourages the use of this algorithm for secure applications. However the system security can be moderately improved if the functions described by Eq. (2) and Eqs. (4) were made considerably more complicated than those used in [10, §III] and dependent from several unknown parameters, composing part of the key.

Acknowledgments

The authors are grateful to the anonymous reviewers for their valuable comments. The work described here was supported by Ministerio de Ciencia e Innovación of Spain, research grant TSI2007-62657 and by CDTI in collaboration with Telefónica I+D, project SEGUR@ (CENIT 2007-2010).

References

[1] T. Yang, A survey of chaotic secure communication systems, Int. J. Comput. Cognit. 2 (2004) 81.

[2] M. Boutayeb, M. Darouach, H. Rafaralahy, Generalized state-space observers for chaotic synchronization and secure communication, IEEE T. Circuits-I 49 (3) (2002) 345.

[3] Q. Memon, Synchronized chaos for network security, Comput. Commun. 26 (2003) 498.

[4] S. Bowong, Stability analysis for the sinchronization of chaotic systems with different order: application to secure communication, Phys. Lett. A 326 (1-2) (2004) 102.

[5] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking two secure communication systems based on chaotic masking, IEEE T. Circuits-II 51 (10) (2004) 505.

[6] G. Alvarez, S. Li, Breaking network security based on synchronized chaos, Comput. Communicat. 27 (2004) 1679.

[7] G. Alvarez, L. Hernandez, J. Muñoz, F. Montoya, S. Li, Security analysis of a communication system based on the synchronization of different order chaotic systems, Phys. Lett. A 345 (4-6) (2005) 245.

[8] J. Y. Chen, K. W. Wong, L. M. Cheng, J. W. Shuai, A secure communication scheme based on the phase synchronization of chaotic systems, Chaos 13 (2003) 508.

[9] S. Bu, B.-H. Wang, Improving the security of chaotic encryption by using a simple modulating method, Chaos Solitons Fractals 19 (2004) 919.

[10] Z. P. Jiang, A note on chaotic secure communication systems, IEEE T. Circuits-I 49 (1) (2002) 92.

[11] B.-H. Wang, S. Bu, Controlling the ultimate state of projective synchronization in chaos: application to chaotic encryption, Int. J. Mod. Phys. B 18 (17–19) (2004) 2415.

[12] Z. Li, D. Xu, A secure communication scheme using projective chaos synchronization, Chaos Solitons Fractals 22 (2004) 477.

[13] E. N. Lorenz, Deterministic non periodic flow, J. Atmos. Sci. 20 (2) (1963) 130.

[14] L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (1990) 821.

[15] L. M. Pecora, T. L. Carroll, G. A. Johnson, D. J. Mar, J. F. Heagy, Fundamentals of synchronization in chaotic systems, concepts, and applications, Chaos 7 (4) (1997) 520.

[16] J. M. Amigo, L. Kocarev, J. Szczepanski, Theory and practice of chaotic cryptography, Phys. Lett. A 366 (2007) 211.

[17] G. Millerioux, J. Amigo, J. Daafouz, A connection between chaotic and conventional cryptography, IEEE T. Circuits-I 53 (6) (2008) 1300.

[18] S. M. Shahruz, A. K. Pradeep, R. Gurumoorthy, Design of a novel cryptosystem based on chaotic oscillators and feedback inversion, J. Sound and Vibration 250 (2002) 762.

[19] S. Li, G. Alvarez, Z. Li, W. Halang, Analog chaos-based secure communications and cryptanalysis: A brief survey, arXiv:0710.5455v1 [nlin.CD] (2007).

[20] E. Solak, Partial identification of lorenz system and its application to key space reduction of chaotic cryptosystems, IEEE T. Circuits-II 51 (10) (2004) 557.

[21] T. Stojanovski, L. Kocarev, U. Parlitz, A simple method to reveal the parameters of the Lorenz system, J. of Bifurcation adn Chaos 6 (12B) (1996) 2645.

[22] C. Sparrow, The Lorenz equations, Applied mathematical sciences, Springer-Verlag, 1982.

[23] L. M. Pecora, T. L. Carroll, Driving systems with chaotic signals, Phys. Rev. A 44 (1991) 2374.