# Breaking network security based on synchronized chaos

Gonzalo Álvarez [a,*] and Shujun Li [b]

[a] *Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144—28006 Madrid, Spain*

[b] *Department of Electronic Engineering, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Toon, Hong Kong SAR, China*

**Abstract**

Very recently, the use of chaos synchronization as a means of masking information data in a network has been proposed. Although it is claimed that the security breach is not possible and that the proposed encryption approach can be used to secure communications over Internet, we prove that these claims are unfounded, and that the cryptosystem can be broken in different ways.

*Key words:* Chaotic cryptosystems; Cryptanalysis; Network security

## 1 Introduction

During the last decade, there have been many proposals to apply non-linear dynamical systems to cryptography and secure communications under the assumption that chaotic orbits resemble random generators [1]. The well-known Lorenz attractor has been repeatedly used as chaotic generator throughout the years [2–7]. Most of these implementations have been totally or partially broken using many different attacks [8–12]. The work presented in [13] uses the chaotic masking approach based on the Lorenz attractor exactly in the same way as first proposed in [3], but does not add any novelty nor enhance in any way its security, robustness, or efficiency.

⋆ This paper has been published in *Computer Communications*, 27(16):1679-1681, 2004.

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

In [13, §5], a simulation example is given. The communication system is described by the following equations:

$$\text{transmitter} \begin{cases} \dot{x}_1 = \sigma(y_1 - x_1) \\ \dot{y}_1 = r x_1 - y_1 - x_1 z_1 \\ \dot{z}_1 = x_1 y_1 - b z_1 \\ s(t) = x_1 + i(t) \end{cases} \tag{1}$$

$$\text{receiver} \begin{cases} \dot{x}_2 = \sigma(y_2 - x_2) \\ \dot{y}_2 = r s(t) - y_2 - z_2 s(t) \\ \dot{z}_2 = y_2 s(t) - b z_2 \\ \hat{i}(t) = s(t) - x_2 \end{cases} \tag{2}$$

where $i(t)$ is the message or information signal to be masked, $s(t)$ is the transmitted or encrypted signal, and $\hat{i}(t)$ is the decrypted information signal. In [13, §5], the following parameter values are used: $r = 28.0$, $\sigma = 10.0$, and $b = 8/3$. The information signal is $i(t) = 10\cos(60t)\cos(t)$.

In this work, we present still another attack on the allegedly secure system, based on the spectrum analysis of the transmitted signal.

## 2 Description of the attack

Chaotic systems present some properties such as sensitive dependence on parameters and on initial conditions, ergodicity, mixing, and dense periodic points, which make them similar to pseudorandom noise. A fundamental requirement of the pseudorandom noise used in cryptography is that its spectrum should be infinitely broad, flat, and of higher power density than the signal to be concealed within. However, the cryptosystem proposed in [13] does not satisfy this requirement.

In Fig. 1 the ciphertext logarithmic power spectra of the cryptosystem described in [13, §5] is illustrated. It can be observed that the plaintext signal clearly emerges at $59/(2\pi)$ Hz and at $61/(2\pi)$ Hz over the background noise created by the Lorenz oscillator, with a power $-4$ dB relative to the maximum power of the ciphertext spectrum, while the power density of the masking signal, for the same frequency, falls below $-80$ dB.

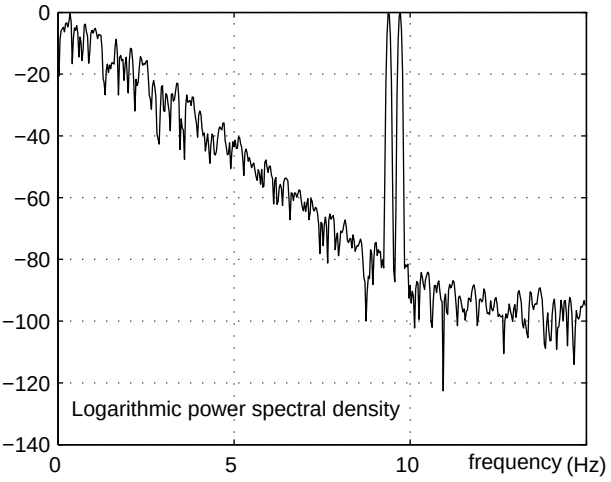


Fig. 1. Power spectral density analysis of the ciphertext signal. The peaks at $59/(2\pi)$ Hz and at $61/(2\pi)$ Hz correspond to the plaintext frequency. The spectrum was calculated using a 4096-point Discrete Fourier Transform with a 4-term Blackman-Harris window.

To break the system, the chaotic transmitter of the examples was simulated with the same parameter values used in [13, §5]. To recover the plaintext no chaotic receiver was used. Instead, the ciphertext was high-pass filtered. The procedure is illustrated in Fig. 2. The result is a perfect estimation of the plaintext. In fact, the plaintext presence in the ciphertext is so evident that it can be appreciated even with the naked eye.

It should be emphasized that our analysis is a blind detection, made without the least knowledge of what kind of non-linear time-varying system was used for encryption, nor its parameter values, and neither its keys, if any. Other avenues of attack are described in [8–12] and will not be repeated here.

## 3 Other weaknesses and inconsistencies found

### *3.1 Precision issues*

In [13] the application of an analog encryption method to digital files is proposed, but no indication is given about how to implement this encryption process. We wonder how the described method, where a series of real number is generated, can be used to encrypt digital values. We are not told in which way the binary digits in the files are mixed with the chaotic orbit generated by the Lorenz attractor. This should have been thoroughly explained.

On the other hand, once the information is encrypted, as it is an analogous signal, it should be converted to a digital one to allow its transmission through

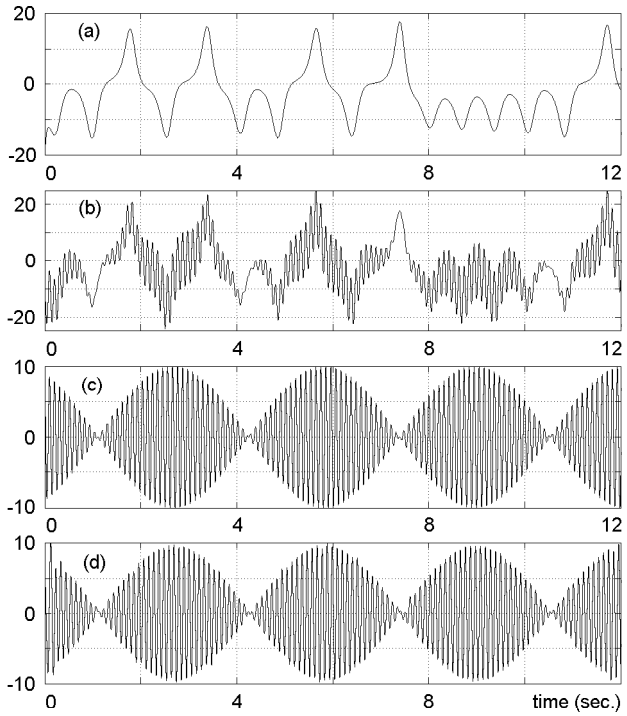


Fig. 2. Plaintext recovery with ciphertext filtering attack. The high-pass filter employed was a four-pole Butterworth with a frequency cutoff of 33 rad/s. Time histories of: (a) $x$ component of the Lorenz chaotic attractor; (b) the ciphertext, $s(t)$; (c) the plaintext, $i(t) = 10\cos(60t)\cos(t)$; (d) the recovered plaintext with a high-pass filter.

the Internet. It should be clarified with how many bits per sample the conversion will be implemented and how the limited precision may affect to the chaotic transmission system.

### *3.2 The key*

In [13] it is not specified what the key is. It is hinted that the key might consist of the initial conditions of the chaotic system, but it is not clearly stated which conditions, which their range is and what their precision or sensibility is. Furthermore, the synchronization and thus the decryption are independent of the initial conditions. Consequently, initial conditions should not be part of the key.

## 4 Conclusions

In [13], the use of the Lorenz chaotic attractor was proposed for secure communications over Internet, but in the same way as introduced in classical papers

such as [3]. Therefore, all the same mistakes that have been pointed out in the past ten years are reproduced. We have presented an attack based on filtering the ciphertext which successfully recovers the plaintext. Furthermore, we have highlighted some other weaknesses and inconsistencies found in the proposed secure communication system. As a consequence of this analysis, we conclude that the system completely lacks security, it is impractical for the transmission of digital data through a digital channel as is the Internet, and thus should not be used for applications where security is a strong requirement.

## Acknowledgements

This research was supported by Ministerio de Ciencia y Tecnología, Proyecto TIC2001-0586 and SEG2004-02418.

## References

[1] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Chaotic cryptosystems. In Larry D. Sanson, editor, *33rd Annual 1999 International Carnahan Conference on Security Technology*, pages 332–338. IEEE, 1999.

[2] C. W. Wu and L. O. Chua. A simple way to synchronize chaotic systems with applications to secure communications systems. *Int. J. Bifurc. Chaos*, 3:1619–1627, 1993.

[3] K. M. Cuomo, A. V. Openheim, and S. H. Strogatz. Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst. – II*, 40:626–633, 1993.

[4] K. M. Cuomo and A. V. Openheim. Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.*, 71:65–68, 1993.

[5] M. Feki. An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons and Fractals*, 18:141–148, 2003.

[6] T. L. Liao and N. S. Huang. An observer based approach for chaotic synchronization with application to secure communications. *IEEE Trans. Circuits Syst. – I*, 46:1144–1150, 1999.

[7] M. Boutayeb, M. Darouach, and H.Rafaralahy. Generalized state-space observers for chaotic syncronization and secure communication. *IEEE Trans. Circuits Syst. – I*, 49:345–349, 2002.

[8] G. Pérez and H. A. Cerdeira. Extracting messages masked by chaos. *Phys. Rev. Lett.*, 74:1970–1973, 1995.

[9] K. M. Short. Unmasking a modulated chaotic communications scheme. *Int. J. Bifurc. Chaos*, 6:367–375, 1996.

[10] T. Yang, L. B. Yang, and C. M. Yang. Cryptanalyzing chaotic secure communications using return maps. *Phys. Lett. A*, 245:495–510, 1998.

[11] G. Hu, Z. Feng, and R. Meng. Chosen ciphertext attack on chaos communication based on chatotic synchronization. *IEEE Trans. Circuits Syst. – I*, 50:275–279, 2003.

[12] G. Álvarez, F. Montoya, M. Romera, and G. Pastor. Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons & Fractals*, In print, 2004.

[13] Qurban Memon. Synchronized chaos for network security. *Computer Communications*, 26:498–505, 2003.