CMOS cryptosystem using a Lorenz chaotic oscillator

Citation for published version (APA):

Gonzalez, O. A., Han, G., Pineda de Gyvez, J., & Edgar (1999). CMOS cryptosystem using a Lorenz chaotic oscillator. In *Proceedings of the 1999 IEEE International Symposium on Circuits and Systems, 1999, ISCAS '99, 30 May - 2 June 1999, Orlando, Florida* (Vol. 5, pp. 442-445). Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/ISCAS.1999.777604>

DOI:

[10.1109/ISCAS.1999.777604](https://doi.org/10.1109/ISCAS.1999.777604)

Document status and date:

Published: 01/01/1999

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

CMOS CRYPTOSYSTEM USING A LORENZ CHAOTIC OSCILLATOR

Octavio A. González, Gunhee Han, José Pineda de Gyvez and Edgar

Department of Electrical Engineering

Texas A&M University

College Station, TX 77843, Phone: +1-(409)-8457477, email: gyvez@ee.tamu.edu

Abstract

This paper presents a monolithic implementation of a cryptosystem based on the Corron and Hahs scheme [1]. The baseband chaotic encryption/decryption system has been designed at the transistor level and fabricated using the AM11.2µm CMOS technology available through the MOSIS foundry. While the mathematical model of the Lorenz system is straightforward, its silicon implementation is not. Typical circuit design considerations need to be considered such as the system's dynamic range, internal signal processing mode and basic building blocks all with the intent to provide an optimal design. This paper addresses in detail *i)* a new generalized Lorenz system of equations suitable for hardware implementations, *ii)* practical design considerations of the cryptosystem and *iii)* actual chip-test measurement results that verify theoretical results.

1. Introduction

Data encryption and security are areas of communications that are experiencing a recent boost with all the new available personal communications systems and the expansion of the Internet. Most commonly employed encryption and security schemes are digital in nature since present communication systems are becoming entirely digital. While the appeal of a fully digital transceiver is justified and required for complex communications systems due to their robustness, there are applications that do not require such complex communications systems but still require some type of encryption for information security. Examples of such systems are garage-door openers, remote key-less entry systems, and wireless telephones, to name a few. Typically, simple analog modulation schemes are used in such communications systems in order to keep the system complexity low. Any encryption scheme that is used in conjunction with these analog modulation techniques should be able to withstand the more hostile effects of the analog modulation environment.

Chaotic systems with their inherent non-linearity and dependence on initial conditions[2] have a profound appeal for the secure communications area in which data security and integrity cannot be compromised at any cost. A number of chaotic systems have been presented in the literature[2]. Of all these, the most well known are the Chua's oscillator, the Rossler oscillator and the Lorenz system. With the exception of the Chua's oscillator, the other chaotic systems have their background in mathematical modeling of a natural phenomenon[3]. Due to its simplicity, the Chua's oscillator has been the chaotic system of choice when it comes to hardware implementation[4]. Mathematical presentations of chaotic cryptosystems and sometimes their implementations with discrete components have been reported before in the literature. For example, applications for the masking of an information signal with chaos can be found in [5], an

innovative encryption approach is presented in [1] through the use of parameter modulation and the use of a non-linear filter for decryption, while chaotic modulation techniques have been presented in [6]. Also, the noise-like spectral characteristics of chaotic systems have been proposed for spread-spectrum and multi-user communications in [7]. This paper presents the monolithic implementation of a cryptosystem based on the chaotic secure communication scheme proposed by Corron and Hahs[1]. While the mathematics have already been developed by the authors of this scheme, there are several open-ended questions that need addressing for the optimal implementation of such an encryption scheme on silicon. We chose the Lorenz oscillator as the source of chaos. The baseband chaotic encryption/decryption system has been designed and fabricated using the AM11.2µm CMOS technology available through the MOSIS foundry.

2. Lorenz System for Hardware Implementations

The Lorenz system of equations was published by E. Lorenz more than 30 years ago as a model for two-dimensional fluid convection[3]. The original equations for this 3rd order non-linear system are:

$$\frac{dx}{dt} = -\sigma x + \sigma y, \quad \frac{dy}{dt} = rx - y - xz, \quad \frac{dz}{dt} = -bz + xy \quad (1)$$

This system is well understood and has been revisited by many researchers over the years[4]. Typical cases of interest are for values of $r > 1$ since this is one of the requirements for its chaotic behavior [4]. The original Lorenz system as presented in (1) has two main problems for its hardware implementation. One of them is the large dynamic range of the system variables. Basically, a large dynamic range calls for a large bias to prevent saturation of the processing blocks[8]. The second problem is the large amount of area needed to implement the system as originally presented by Lorenz since the values of the system parameters needed to ensure chaotic behavior are high and spread out. Hence, instead of using (1) we propose a generalized Lorenz system which is more amenable to hardware implementations. This generalized system is as follows:

$$\begin{aligned} \frac{dx}{dt} &= -\sigma_1 x + \sigma_2 y \\ \frac{dy}{dt} &= -K_1 y + K_2 rx - K_3 xz \\ \frac{dz}{dt} &= -bz + K_4 xy \end{aligned} \quad (2)$$

From an implementation standpoint, the main modifications are the splitting of the σ coefficients and the generalization of the gain of the multiplicands. While there is not a true natural frequency for chaotic systems since they are broadband in nature,

we can speak of a natural frequency for the system which is set by the time constants of the integrator loops. We have found from simulation results that the full bandwidth of the Lorenz system is approximately 10 times the value of the x -subsystem's pole location. It is worth noting that the bandwidth of the system sets a limit on the maximum input frequency that can be processed by the chaotic system. As such, the main modification from an implementation standpoint is to increase the position of the integrator poles to higher frequencies. An additional and similar modification is to increase the location of the pole for the y -subsystem. Note that lossy-integrators can be used for the hardware implementation. Typically, from an implementation standpoint, the use of lossy-integrators is feasible only if the location of the system poles is high. This stems from the fact that for high frequencies the capacitance in the RC constant can be made smaller yielding in this way a full monolithic implementation. The dynamic range of the system parameters can be approximated by the arithmetic distance between the fixed-points:

$$\begin{aligned} S_x &\approx \pm 2 \sqrt{\frac{b(\sigma_2 K_2 r - \sigma_1 K_1)}{\sigma_1 K_3 K_4}} \\ S_y &\approx \pm 2 \frac{\sigma_1}{\sigma_2} \sqrt{\frac{b(\sigma_2 K_2 r - \sigma_1 K_1)}{\sigma_1 K_3 K_4}} \\ S_z &\approx \frac{\sigma_2 K_2 r - \sigma_1 K_1}{\sigma_2 K_3} \end{aligned} \quad (3)$$

Note that in the case of the original Lorenz system with $\sigma_1 = \sigma_2$ [3], the dynamic range for the x and y -subsystems are the same. With the generalization of the Lorenz system, extra degrees of freedom are added which makes it possible to control the dynamic range of the y -subsystem independently from that of the x -subsystem. It can also be seen from (3) that with the generalization of the y -subsystem pole with K_1 , another degree of freedom is provided in controlling the dynamic range of the subsystems. From the expressions presented up to this point, the intuitive advantages of using the generalized Lorenz system can be detailed as follows: 1) Freedom in controlling the dynamic range in each of the subsystems. 2) Ability to apply the Lorenz system for high-frequency signal processing schemes. 3) Full implementation on silicon of the generalized Lorenz system. The condition for a Hopf bifurcation is given by (5) where we can see also the critical chaos parameter r_c :

$$\begin{aligned} b(\sigma_1 + b + K_1) \left(\frac{\sigma_2}{\sigma_1} K_2 r + \sigma_1 \right) &= 2b(\sigma_2 K_2 r - \sigma_1 K_1) \\ \therefore r > r_c &= \frac{\sigma_1^2 (\sigma_1 + b + 3K_1)}{K_2 \sigma_2 (\sigma_1 - b - K_1)} \\ \sigma_1 &> b + K_1 \end{aligned} \quad (4)$$

3. Corron and Hahs Cryptosystem Model

The following presentation will be from an implementation standpoint; nevertheless, we encourage the reader to refer to the original paper. The mathematical equations implementing this chaotic encryption scheme are presented in (5). Note that this encryption scheme employs the generalized Lorenz system of equations previously presented in (2)

$$\frac{dx}{dt} = -\sigma_1 x + \sigma_2 y \quad (5a)$$

$$\frac{dy}{dt} = -K_1 y + K_2 r_b (1 + \alpha_i) x - K_3 xz \quad (5b)$$

$$\frac{dz}{dt} = -bz + K_4 xy \quad (5c)$$

The digital bit-stream to be encrypted is given by α_i and the encryptor output to be transmitted is given by the continuous signal, $y(s)$. The critical chaos parameter r was chosen as the modulation parameter for encryption. This makes the actual parameter be $r(t) = K_2 r_b (1 + \alpha_i)$ which is dependent not only on a constant r_b but also on the digital signal α_i . Fig. 1 presents the block diagram implementing the encryption system described by (5). Observe that we have opted for a fully differential implementation to minimize offsets arising from process imperfections. Fig. 1 shows that the encryption system consists of a stable chaotic Lorenz oscillator with an additional non-linear branch modulating the digital input, α_i . Note that since the input information is digital in nature, a simple switching modulator can be employed instead of a full multiplier.

For optimal chaotic synchronization between the receiver and the transmitter, it is necessary that the chaotic synchronous subsystem employed at the receiver be independent of the encrypting signal[1]. In simpler terms, for the case presented in

Figure 1: Chaotic Lorenz Encryption System

(5) the synchronous subsystem at the receiver must not contain the critical chaos parameter $r(t)$. The presence of this parameter in the synchronous subsystem could undermine the communication robustness since modulation effects and unavoidable parameter mismatches could impose dire effects[1]. Since for the Lorenz system, the only two stable synchronous subsystems are the yz and xz subsystems[5], the choice of the xz subsystem is clear from the previous observations. The expression presented in (6) describes the generalized Lorenz xz synchronous subsystem employed to achieve chaotic synchronization between the transmitter and receiver. This subsystem appears between dotted lines in Fig. 1.

$$\frac{dx_r}{dt} = -\sigma_1 x_r + \sigma_2 y \quad (6a)$$

$$\frac{dz_r}{dt} = -bz_r + K_4 x_r y \quad (6b)$$

In (6) the subscript r is used to distinguish system variables that correspond to the receiver. As noted before, since the synchronous xz subsystem does not depend on the encrypting signal, theoretically the chaotic systems will be perfectly synchronized[1]. The generalized equations for the non-linear recovery filter are given by[1]:

$$\frac{d\omega_o}{dt} = (k - K_1)y - K_3x_rz_r - k\omega_o \quad (7a)$$

$$\frac{d\omega_1}{dt} = K_2x_r - k\omega_1 \quad (7b)$$

$$\frac{dr_f}{dt} = \frac{q \operatorname{sgn}(\omega_1)}{1 + |\omega_1|} (y - \omega_o - \omega_1 r_f) \quad (7c)$$

where y refers to the input signal applied at the decryptor and the variables with the r subscript refer to the state-variables of the synchronous xz subsystem described in (6). Equation (7c) corresponds to the non-linear filter used to filter out singularities and to provide a continuous estimation of the original information[1]. The difference between (7) and the original equation in [1] stems from the fact that for hardware implementations the signal levels being processed are small in magnitude implying that $\omega_1 \ll 1$ and that the original expression $1 + |\omega_1|$ can be simply approximated to 1. From a hardware implementation standpoint, there are several advantages obtained from (7). Namely, the division function typically requires more hardware to implement[8] and as such savings in area are obtained by the implementation of (7). Additionally, the signum modulation can be implemented with a comparator and some switches.

Figure 2: Non-linear filter of Chaotic Lorenz Decryption System

All of the non-linear recovery filter parameters in (7) are determined by the specific values employed in the Lorenz encryptor except for the k and q parameters. Presumably these parameters can be chosen arbitrarily[1]. However, intuitively it is seen that the k parameter is a time-constant for the estimation part of the non-linear filter. Since this part of the filter is continuously processing the chaotic signal, the optimal k value depends on the highest frequency component expected in the chaotic signal. The q parameter is a low-pass filter parameter which is used to filter out singularities in the recovered signal[1]. As such, the optimal value for this parameter depends on the highest frequency component expected from the information signal. The block diagram implementing the complete analog nonlinear recovery filter is presented in Fig. 2. Fig. 3 shows the chip's microphotograph.

Fig. 3. Cryptosystem microphotograph

4. Experimental Verification

The famous Lorenz attractors are presented in Fig. 4. Note that these attractors correspond to the base Lorenz system which in the complete cryptosystem is for the case when $\alpha_i = -3V$. The grid scales of Fig. 4 are $x=500mV/div$, $y=200mV/div$ and $z=200mV/div$.

Figure 4. Lorenz attractors (a) xy attractor (b) xz attractor

Cryptosystem Verification

A 2Kb/s, $\pm 3V$ pulse was applied at the α_i input of the encryptor. The digital input bit-stream is shown in the bottom window of Fig. 5(a). The x-axis grid corresponds to $250\mu s/div$ from which it can be verified that the symbol time frame is equal to $500\mu s$. The y analog output of the encryptor is presented in the top window of Fig. 5(a). Notice that this output exhibits the expected chaotic behavior. A better picture of the effect of modulation on the chaotic system is obtained by looking at the attractors. The effect of the data encryption on the Lorenz attractors is shown in Fig. 5(b). The effect of data encryption on the system attractors is more visible in the XZ attractor presented in that figure. The presence of two stable Lorenz systems can be verified from this plot. Recall that the data encryption consists of mapping each of the bit values to one of the systems. The spectrum for both cases of the Lorenz oscillator, e.g. $\alpha_i = -3V$ and $\alpha_i = +3V$, is shown in Fig. 6. These results were obtained using the FFT capabilities of the HP54600A digital oscilloscope. The axes scales are $48.8KHz/div$ for the x-axis and $10dBV/div$ for the y-axis.

Figure 5. (a) Signal encryption (b) Effect on xz attractor

Figure 6. Chaotic Frequency Spectrum. (a) input bit Logic "0" (b) input bit Logic "1"

Figure 7. (a) Output of nonlinear filter. (b) Output after A/D conversion for a 10Kb/s bit stream

To verify the complete system, a digital bit-stream at 1Kb/s was applied at the input of the encryptor and the analog output of the non-linear filter was monitored. The observed results are presented in Fig. 7(b). Note that the analog output of the non-linear filter shown in Fig. 7(a) resembles the digital input bit-stream shown in the bottom window of Fig. 7(a). Note that the input bit-stream has been successfully recovered. Also note that for this low data rate the delay and bit-timing of the input bit-stream are not distorted too much at the output. We obtained successful recovery of data rates of up to 10Kb/s with this cryptosystem. The results with the A/D conversion are shown in Fig. 7(b). For data rates higher than about 10Kb/s, recovery of the digital data is no longer possible with this specific cryptosystem.

The Bit Error Rate (BER) measure is commonly used to quantify the performance of communication systems to noise and channel distortion. The performance of the cryptosystem was quantified by sending a bit-stream of $\pm 3V$ pulses, adding a certain level of noise to the analog encrypted signal and obtaining the estimate of the bit-stream using the decryptor. A comparison between the original bit-stream and the obtained output bit-stream of the cryptosystem is used to determine whether an error was made by the decryptor's estimate. By dividing the number of errors over the total number of transmitted pulses, a rough BER can be obtained. A C-program was written to utilize a National Instruments data acquisition board available in the lab to do the bit transmission, reception and BER determination for the cryptosystem. In this program, the data rate as well as the number of bits to transmit can be programmed by the user. The main problem in this approach is that it is difficult to determine the required noise level to obtain a true SNR. As a result, a brute-force approach was used in which only certain amount of

noise levels were used to measure the performance of the cryptosystem. These noise levels were based on the maximum peak-to-peak swing of the encryptor's output which was found to be approximately 560mV. Fig. 8 shows the cryptosystem's BER.

Figure 8. Bit Error Performance of the cryptosystem

5. Conclusions

The research was motivated by the many promises that chaotic circuits offer for the secure communication area. The experimental results obtained for the chaotic cryptosystem show that a secure communication system on a chip is viable for digital data transmission. The complete chaotic cryptosystem was implemented using a $1.2\mu\text{m}$ technology in a $2.2\text{mm} \times 2.2\text{mm}$ die. The choice of fully-differential operation and current-mode internal processing led to a compact silicon implementation. Since the implemented chaotic cryptosystem transforms a digital bit-stream into an analog chaotic waveform, its natural place in a communication system is directly before the modulation stage. Additional gains in BER can be obtained by using digital coding before encrypting the bit-stream.

References

- [1] N. J. Corron and D. W. Hahs, "A New Approach to Communications Using Chaotic Signals," *IEEE Transactions on Circuits and Systems I*, vol. 44, pp. 373-382, May 1997.
- [2] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, Springer-Verlag, New York, NY 1990.
- [3] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmospheric Sci.*, vol. 20, pp. 130-141, Mar. 1963.
- [4] R. Madan, "Chua's Circuit: A Paradigm for Chaos" World Scientific, 1993.
- [5] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic *Phys. Rev. Lett.*, vol. 64, pp. 821-824, Feb. 1990.
- [6] H. Dedieu, M. Kennedy and M. Hasler, "Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits," *IEEE Transactions on Circuits and Systems II*, vol. 40, pp. 634-642, Oct. 1993.
- [7] G. Heidari-Bateni and C.D. McGillem, "Chaotic Sequences for *Proc. IEEE International Conference on Selected Topics in Wireless Communications*, pp. 437-440, June 1992.
- [8] P. E. Allen and D. Holberg, *CMOS Analog Circuit Design*. Harcourt Brace Jovanovich College Publishers, New York, NY 1987.