Lorenz-based chaotic cryptosystem : a monolithic implementation

Citation for published version (APA):

Gonzales, O. A., Han, G., Pineda de Gyvez, J., & Sanchez-Sinencio, E. (2000). Lorenz-based chaotic cryptosystem : a monolithic implementation. *IEEE Transactions on Circuits and Systems. I, Fundamental Theory and Applications*, 47(8), 1243-1247. <https://doi.org/10.1109/81.873879>

DOI:

[10.1109/81.873879](https://doi.org/10.1109/81.873879)

Document status and date:

Published: 01/01/2000

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.

Lorenz-Based Chaotic Cryptosystem: A Monolithic Implementation

Octavio A. Gonzales, Gunhee Han, José Pineda de Gyvez, and Edgar Sánchez-Sinencio

Abstract—A monolithic implementation of a cryptosystem based on the Corron and Hahs scheme [1] is hereby presented. The baseband chaotic encryption/decryption system has been designed at the transistor level and fabricated using AMI 1.2 μm 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 brief addresses in detail: 1) practical design considerations of the cryptosystem and 2) actual measurement results that verify theoretical findings.

I. INTRODUCTION

Although it has been shown that signal encryption based on chaos is relatively vulnerable [2], [3], there is a niche of applications such as remote keyless entry systems, and wireless telephones, to name a few, that do not require a high level of information security and that could employ an encryption scheme based on chaos. This brief presents a monolithic implementation of such a cryptosystem based on the chaotic secure communication scheme proposed by Corron and Hahs [1]. While the corresponding mathematics have already been developed by the authors, there are several open-ended questions that need addressing for an optimal implementation of the system in silicon. We envision our system as a cryptosystem working at baseband frequencies and embedded in the signal path of a transceiver rather than the system being the actual crypto-modem working at very high frequencies. This approach allows us to relax our design to accommodate the strict requirements imposed on communications systems, e.g., channel bandwidth constraints. Moreover, a system like the Corron and Hahs' presents the advantage of not needing to transmit a key for decryption. It is a scheme based on parameter modulation and filter-based demodulation circuitry. The baseband chaotic encryption/decryption system has been designed for digital input bitstreams and fabricated using AMI 1.2- μm complementary metal-oxide-semiconductor (CMOS) technology available through the MOSIS foundry. In this brief, system and transistor-level monolithic design considerations as well as experimental results are addressed.

II. CORRON AND HAHS CRYPTOSYSTEM MODEL

It has been observed that a straight implementation of the Lorenz system is hindered by the large spread of its coefficients [4]. Although

Manuscript received October 22, 1998; revised February 1, 2000. This paper was recommended by Associate Editor K. Halonen.

O. A. Gonzales is with Motorola, Inc.

G. Han was with Yonsei University, Korea.

J. Pineda de Gyvez was with Texas A&M University, College Station, TX 77843 USA. He is now with Philips Research Laboratories, Eindhoven 5656AA Eindhoven, The Netherlands.

E. Sanchez-Sinencio is with the Department of Electrical Engineering, Texas A&M University, College Station, TX 77843 USA.

Publisher Item Identifier S 1057-7122(00)06333-9.

Fig. 1. Chaotic Lorenz encryption system.

a state variable scaling is possible [4], the spread of the coefficients is still large for a monolithic implementation. We have, thus, generalized the Lorenz-based encryption scheme in an augmented system that includes parameters K_1 , K_2 , K_3 , and K_4 that simplify the hardware implementation in spite of the large dynamical range required by the original coefficients. This system is presented in (1) where we are assuming that the input bit stream α_i is digital and that the encryptor's output is given by the continuous signal $y(t)$. In this system, $r(t) = K_2 r_b (1 + \alpha_i)$ is chosen as the modulation parameter for encryption which is dependent not only on a constant r_b , but also on the digital signal α_i

$$\frac{dx}{dt} = -\sigma_1 x + \sigma_2 y \quad (1a)$$

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

$$\frac{dz}{dt} = -b z + K_4 x y. \quad (1c)$$

Chaos is achieved when the steady states of (1) lose stability via bifurcation to a periodic solution. This condition occurs when the parametric value $r(t) = r_c$, called "critical chaos parameter," exceeds the Hopf bifurcation point given for $r(t) = r_c$. The condition for a Hopf bifurcation is obtained from the eigenvalues of the Jacobian system and is given in (2) where we can see also the critical chaos parameter r_c :

$$r > r_c = \frac{\sigma_1^2 (\sigma_1 + b + 3K_1)}{K_2 \sigma_2 (\sigma_1 - b - K_1)} \quad (2)$$

$$\sigma_1 > b + K_1.$$

Fig. 1 presents the block diagram implementing a fully differential version of the encryption system described by (1) with an addi-

Fig. 2. Chaotic Lorenz decryption system. To avoid cluttering all lossy integrators are drawn with only the integrator symbol. (a) Receiver and (b) nonlinear filter.

tional nonlinear branch modulating the digital input α_i . The various building blocks are implemented as transconductance multipliers, as transresistance integrators and as transconductance gain stages, respectively. Note that since the input information is digital in nature, a simple switching modulator that occupies less silicon area can be employed instead of a full multiplier. The scheme of Corron and Hahs requires, in addition to a subsystem without $r(t)$, a nonlinear filter for extracting the information signal from the chaotically modulated one. The generalized equations for the nonlinear recovery filter are given by [8]

$$\frac{d\omega_o}{dt} = (k - K_1)y - K_3x_rz_r - k\omega_o \quad (3a)$$

$$\frac{d\omega_1}{dt} = K_2r_bx_r - k\omega_1 \quad (3b)$$

$$\frac{dr_f}{dt} = q \operatorname{sgn}(\omega_o)(y - \omega_o - \omega_1r_f) \quad (3c)$$

where y refers to the input signal applied at the receiver (decryptor) and the variables with the r subscript refer to the state-variables of the

Fig. 3. Microphotograph of Lorenz cryptosystem.

synchronous x - z subsystem at the receiver. The difference between (3c) 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 expression $1 + |\omega_1|$ can be simply approximated to 1. From a hardware implementation

standpoint the division function typically requires more hardware and as such savings in area are obtained by the implementation of (3c). Additionally, the signum modulation can be implemented with a comparator and some switches. In the nonlinear filter, the parameter k sets the time-constant of the estimation part of the filter. Thus, the optimal k value depends on the highest dynamics of the information signal, e.g., the period of the bitstream. The q parameter is a low-pass filter parameter which is used to filter out singularities in the recovered signal [11]. As such, the optimal value for this parameter depends also on the smallest time period expected from the information signal. The block diagram implementing the complete analog decryption system is presented in Fig. 2.

We chose the system's full bandwidth to be approximately 17 KHz; this yields $\sigma_1 = 1 \times 10^5$ rad/s, $K_1 = b = 0.3 \times 10^5$ rad/s. Once the locations of the poles are chosen, then the rest of the system parameters can be obtained from the desired signal swings. These signal swings cannot be chosen arbitrarily since they are limited by power consumption and area requirements. To decrease the dynamic range in the y -subsystem, σ_2 was chosen as $\sigma_2 = 3\sigma_1 = 3 \times 10^5$ rad/s. The chosen base value for the chaos parameter was $K_2 r = 10 \times 10^5$ to be insensitive to process variations. From (1), it can be seen that the product of K_3 and K_4 affect the dynamic range of both the x and y -subsystems while K_3 alone affects that of the z -subsystem. For reasons of higher immunity to noise as well as area and power consumption, a maximum dynamic range of ± 1.5 V was chosen as the target for the subsystems. Keeping this in mind, the values needed for the multiplier gains are $K_3 = 20$ and $K_4 = 10$. Finally, we chose $q = 2.13 \times 10^5$ rad/s and $k = 1 \times 10^6$, which through simulations, gave us the best bit error rate performance.

III. CRYPTOSYSTEM CIRCUIT DESIGN

Through extensive simulations, we found that a parameter mismatch between encryptor and decryptor of more than 10% is detrimental. We observed that while the information content was still discernable, the timing of the information was distorted. To make matters worse, the amount of distortion appeared to be correlated with the mismatch value. To account for fading and attenuation effects in the channel, we simulated the effect of band-limiting the output of the encryptor using an eighth-order low-pass Butterworth filter. The simulation results showed that the main effect of the filter turns into a considerable increase in the phase delay between the synchronized Lorenz drive/response systems leading to singularities in the recovered signal and to high error rates. All these aspects were taken into account in the final implementation of the system. In this section, a succinct outline and technical specs of the main building blocks of the complete cryptosystem are presented. Except for the integrator capacitors, the whole system has been fully integrated in silicon. Fig. 3 shows a photograph of the actual integrated circuit. The system uses ± 3 V power supplies and accepts an input digital stream of ± 3 V.

1) *Transresistance Lossy-Integrator*: A transresistance lossy-integrator is employed in the implementation of the chaotic system. Fig. 4(a) presents the transistor level diagram of the chosen lossy-integrator [5]. This integrator is based on a cross-coupled current mirror which is ideal for high-speed operation [6]. Note that both the input and output occur at the same nodes, however, the input is a differential current while the output is a differential voltage. Besides the location of the pole and the effective transresistance, an additional constraint imposed on the integrator is to have the dc value of the

Fig. 4. (a) Fully-differential lossy-integrator with linearized common mode feedback. (b) Folded Gilbert fully-differential CMOS transconductor multiplier with inputs V_x and V_y , and output I_o . (c) Switching modulator; inputs are V_I and α_i .

input/output nodes as close as possible to ground. To decrease power consumption of the system as a whole, a value of $10 \mu\text{A/V}$ for the effective transconductance (b , K_1 , σ_1) and a feedback biasing current of $I_{bf} = 55 \mu\text{A}$ were chosen.

2) *Transconductance Block with Common-Mode Feedback*: The fully differential transconductor [7]–[9] with linearized common

mode feedback is presented in Fig. 4(b). While the amount of gain in a block is of importance, an equally important challenge in the design of any viable signal-processing block is the maximum input–output signal swing. Typically, tradeoffs in area and power consumption have to be made to accommodate large swings [7]–[9]. The cryptosystem requires two transconductors, namely one with a gain of $G_m = 100 \mu\text{A/V}$ (for $K_2 r_b$) and the other with $G_m = 30 \mu\text{A/V}$ (for σ_2). A differential input–output voltage swing of 1.5 V and tail biasing current of $I_B = 25 \mu\text{A}$ were chosen as well.

3) *Transconductance Multiplier*: A folded Gilbert multiplier that overcomes the typical low input range of its variables was chosen to implement the nonlinear feedback in the Lorenz chaotic system [10]. Two Gilbert multipliers with $G_m = 100 \mu\text{A/V}$ (for K_4) and $G_m = 200 \mu\text{A/V}$ (for K_3) were implemented. An input–output voltage swing of 1.5 V and base bias current of $100 \mu\text{A}$ were used as additional requirements for the block.

4) *Switching Modulator*: The encryption of the digital information is accomplished by modulating the critical chaos parameter $K_2 r_b$ [1]. Since only digital information is being considered in this implementation, a simpler switching modulator suffices for the implementation on silicon. The transistor level diagram of a mixer is presented in Fig. 4(c). The digital bit-stream consists of $\pm 3 \text{ V}$ pulses and the desired transconductance gain for the mixer is $G_m = 100 \mu\text{A/V}$ in order to double the $K_2 r_b$ parameter value when $\alpha_i = +3 \text{ V}$ is transmitted. Input and output voltage swings of 1.5 V were imposed in the design procedure.

5) *CMOS Cross-Coupled Comparator*: A high-gain, fast-response comparator is needed in the $\text{sgn}(\omega_1)$ function required for the nonlinear recovery filter. Another comparator with hysteresis is employed for the A/D conversion at the output of the nonlinear filter. A comparator function can be implemented simply by using a high-gain amplifier. Clamping is typically used in the comparator to have similar rise and fall times [7]–[9]. A tail current of $I_{ss} = 50 \mu\text{A}$ and a gain of 1000 V/V (40 dB) or better were used as starting points. The trip points for the comparator with hysteresis are at $\pm 0.1 \text{ V}$.

IV. CRYPTOSYSTEM VERIFICATION

The effect of parameter modulation on the popular XZ Lorenz attractor is presented in Fig. 5(a). Note that the grid scale is $z = 200 \text{ mV/div}$. Fig. 5(b) shows the corresponding time domain output of the XZ subsystem. To verify the complete system, a digital bit-stream at 1 kb/s was applied at the input of the encryptor and the analog output of the nonlinear filter was monitored. The observed results are presented in Fig. 6. Note that the analog output of the nonlinear filter shown in Fig. 6(a) [top window] resembles the digital input bit-stream shown in the bottom window. The results with the A/D conversion are shown in Fig. 6(b). 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 10 kb/s with this cryptosystem. For data rates higher than about 10 kb/s, recovery of the digital data is no longer possible with this specific cryptosystem. The performance of the cryptosystem was quantified by sending a bit-stream of $\pm 3 \text{ V}$ pulses, adding a certain level of noise to the analog encrypted signal and obtaining the estimate of the noisy bit-stream using the decryptor. An amplitude-controlled noise generator was used in our experiment [12]. The noise magnitude generated by this circuit was based on the maximum peak-to-peak swing of the encryptor's output (approximately 560 mV) and added

(a)

(b)

Fig. 5. (a) XZ attractor ($x = 200 \text{ mV/div}$, $y = 100 \text{ mV/div}$) during parameter modulation. (b) Time-domain representation of chaotic encryption of 2 kb/s digital data analog. Top window: Encrypted output. Bottom window: 2 kb/s input bit-stream XZ attractor.

at the output of the encryptor. A comparison between the original bit-stream and the obtained bit-stream of the cryptosystem was used to determine whether an error was made by the decryptor's estimate. Fig. 6(c) shows the cryptosystem's error sensitivity. The horizontal axis shows the ratio of signal to noise amplitudes, and the vertical axis depicts the corresponding sensitivity. From this first silicon prototype, a null error could not be obtained. We attribute this problem to mismatches between the transmitter and the receiver and to some small offset present in the integrators.

V. CONCLUSION

The very large scale integration (VLSI) implementation of a specific case of the chaotic encryption scheme proposed by Corron and Hahs was presented. We opted for a system employing a Lorenz oscillator whose complexity was overcome by developing a new Generalized Lorenz System suitable for hardware implementations. The complete chaotic cryptosystem was implemented using a $1.2\text{-}\mu\text{m}$ technology in

Fig. 6. Experimental recovery of 1 kb/s bit-stream: (a) analog output of nonlinear filter, (b) digitized output. In both cases, the bottom window displays the input bitstream, and (c) bit error sensitivity.

a 2.2 mm $\times$ 2.2 mm die. The choice of fully differential operation and current-mode internal processing led to a compact silicon implementation.

REFERENCES

- [1] N. J. Corron and D. W. Hahs, "A new approach to communications using chaotic signals," *IEEE Trans. Circuits Systems I*, vol. 44, pp. 373–382, May 1997.
- [2] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcation Chaos*, vol. 4, no. 4, pp. 959–977, 1994.
- [3] —, "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurcation Chaos*, vol. 6, no. 2, pp. 367–375, 1996.
- [4] K. V. Cuomo and A. V. Oppenheim, "Circuit Implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, July 1993.
- [5] J. Varrientos, E. Sánchez-Sinencio, and A. Rodríguez-Vázquez, "A current-mode synchronous circuit for signal encryption," in *Proc. 37th Midwest Symp. Circuits Syst.*, vol. 1, Aug. 1994, pp. 133–137.
- [6] S. L. Smith and E. Sánchez-Sinencio, "Low voltage integrators for high frequency CMOS filters using current mode techniques," *IEEE Trans. Circuits Syst. II*, vol. 43, pp. 39–48, Jan. 1996.
- [7] P. E. Allen and D. Holberg, *CMOS Analog Circuit Design*. New York: Harcourt Brace Jovanovich, 1987.
- [8] R. Geiger, P. E. Allen, and N. Strader, *VLSI Design Techniques for Analog and Digital Circuits*. New York: McGraw-Hill, 1990.
- [9] K. Laker and W. Sansen, *Design of Analog Integrated Circuits and Systems*. New York: McGraw-Hill, 1994.
- [10] J. Ramírez-Angulo and S. Ming-Shen, "The folded Gilbert cell: A low voltage high performance multiplier," in *Proc. 35th Midwest Symp. Circuits Syst.*, vol. 1, Aug. 1992, pp. 20–23.
- [11] N. J. Corron, "An approach to communication with chaos," in *Proc. 4th Exp. Chaos Conf.*. Singapore: World Scientific, 1998, pp. 395–406.
- [12] R. F. Graf, *Encyclopedia of Electronic Circuits*. New York: McGraw-Hill, 1992, vol. 1.