An Encryption Architecture Suitable for on Chip Integration With Sensors

Ava Hedayatipour, *Member, IEEE*, and Nicole McFarlane, *Senior Member, IEEE*

***Abstract*— This paper demonstrates a hardware encryption algorithm that can be integrated directly with sensors on the same chip. In contrast to using power-hungry microprocessors and software implementations, the encryption algorithm was based on a Lorenz chaotic system and was implemented as time scaling chaotic shift keying (TS-CSK). The coupled differential equations of TS-CSK were implemented using low power integrators, multiplexers, switches, and passive components. Both a single-ended and differential system was developed. The single-ended based system showed no oscillation, while the differential based system demonstrated oscillation. Experimental measurements of the differential system with an integrated temperature sensor demonstrated the ability to encrypt and decrypt the transmitted signal. The differential encryption/decryption system was implemented in 180 nm technology and operated with a 1.8 V power supply and 1.5 mW of power.**

***Index Terms*— Hardware security, encryption, chaos, chaotic ciphering, ciphering, Internet of Things, IoT, chaotic circuits and systems, security, biomedical applications, next- generation biomedical devices, injectables, implantables, ingestibles, wearables.**

I. Introduction

CMOS based sensors are popular due to the low cost and ability to integrate signal processing and other modules in a low form factor. These sensors are useful in Internet of Things (IoT) applications such as health monitoring or environmental monitoring. Current sensor designs focus on attributes of the sensor, such as improved accuracy or reduced power consumption. It is expected that many of these sensors will be wireless in nature, and much of the sensed information that is transmitted needs to be encrypted to ensure privacy. This encryption is typically implemented using software or microprocessors, which can be power-hungry. To facilitate low power implantable, portable, and wearable sensors, encryption must be integrated directly with the sensor hardware.

Manuscript received December 8, 2020; revised February 26, 2021; accepted April 16, 2021. Date of publication May 3, 2021; date of current version June 14, 2021. This work was supported by the National Science Foundation under Grant 1816703. This article was recommended by Guest Editor N. Karimi. *(Corresponding author: Ava Hedayatipour.)*

Ava Hedayatipour was with the Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville, TN 37996 USA. She is now with the Department of Electrical Engineering, California State University, Long Beach, CA 90840 USA (e-mail: ava.hedayatipour@csulb.edu).

Nicole McFarlane is with the Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville, TN 37996 USA (e-mail: mcfarlane@utk.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JETCAS.2021.3077023.

Digital Object Identifier 10.1109/JETCAS.2021.3077023

There have been numerous demonstrations of the ability to intercept or hack into wearable devices such as insulin pumps and pacemakers [1]–[4]. There has also been some concern over interference on the IoT devices of smart power grids [5], [6]. Biomedical devices can be compromised by attacks on the data, power, memory, processing units, or the sensors and actuators [7]. There have been a number of methods to attempt to mitigate this, typically by including software or microprocessors in the system [7]–[10]. The technologies used to enhance security include the development of standards and algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) as well as physical architectures such as physical unclonable functions (PUfs), public physical unclonable functions (PPUFs), true random number generators (TRNGS), and flash memory.

Chaos is a method of ciphering that has existed since the 1970s but has been reborn in recent years with IoT and wearable devices needing security that can be implemented with low power electronics. The importance of this method lies in the fact that security in most portable devices is neglected [11], since the current methods of symmetric and asymmetric security implementations tend to be higher power and area consumption. Chaos communication prevents a third party from detecting the signals with a receiver (that can be implemented with a few tens of dollars) and limits the deciphering of the signal to implementation of the exact same complex system that is implemented on an integrated chip (where the cost per device is cheap but design and implementation requires thousands of dollars). Even with copying of the circuit, certain parameters, such as offsets or bias voltages, can be changed slightly to move the 3rd party's circuit out of synchronization.

Chaotic oscillators have been previously implemented using devices such as microprocessors and FPGAs. IoT and wearable devices require encryption and ciphering that is lightweight and small. For wearable devices, the power consumption needs to be smaller than a couple of mW. For wearable and implantable devices, digital systems tend to be power-consuming. Microprocessors can implement classic forms of security easily, but can be difficult to fit into μm sized chips. For example, a 32-bit processor in a 180nm process could take up to 1.2 mm $\times$ 1.2 mm. In IoT devices with an increase in the number of nodes, having a microcontroller for each node to cipher a signal can be costly in terms of both size and power.

Fig. 1 shows an overview of the primary system modules for a secure wireless sensor network typical in IoT. The signal

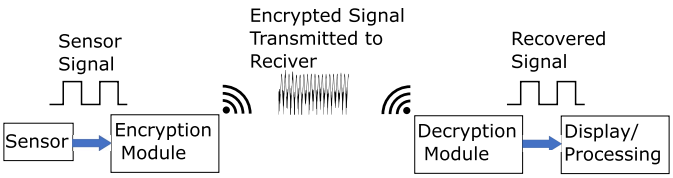

Fig. 1. The signal data from a sensor is encrypted and transmitted over a public channel to the receiver, where it is decrypted before being displayed or further processed.

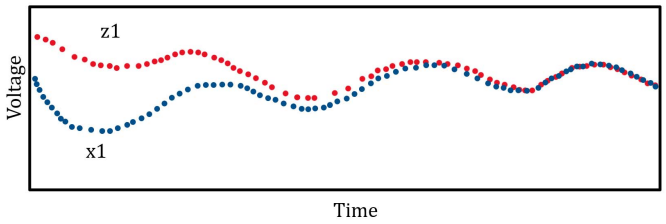

Fig. 2. In chaotic encryption, the signal output of the transmitter x_1 synchronizes to the same state as the receiver z_1 after a certain length of time.

from the sensor is the message that needs to be kept private before being transmitted over a public channel. Encryption has two types. It can be symmetric, where a single secret key that is selectively shared is used to encrypt and decrypt the message. Asymmetric encryption uses two keys, one public and one private, which are mathematically coupled [12]. Chaotic encryption relies on random generation, using a nonlinear system, where the sequence is a function of initial system conditions and system parameters [13]–[16].

Chaotic encryption has been implemented in CMOS with g_m-C modulators and nonlinear resistors. [17], [18]. Different functions such as Newton-Leipnik [19], piecewise-linear (PWL) oscillators [20], and Rössler [21] can also be implemented to achieve chaos. However, the Lorenz system has been relatively popular and robust as a chosen implementation and we focus on the Lorenz based system as our specific implementation. Lorenz based systems [22], and discrete-time chaos generators have been implemented [23]. FPGAs have been used to eliminate issues with parameter mismatch that can occur between the transmitter and receiver [24]–[26].

Discrete components have been used to implement a Lorenz system [27] and a four-dimensional modified Lorenz-Stenflo system to reduce the number of components and power consumption has been simulated [28]. An improved Lorenz chaotic system using active control to reduce synchronization error between the transmitter and the receiver was implemented using discrete components [29]. The requirement for resistors and other passive components was shown to be reduced via simulations of a double-scroll chaotic system based on OTAs [30]. *Lü*'s chaotic oscillator with improved robustness to process, voltage, and temperature (PVT) variations has also been explored [31].

In this work, our focus is on encryption for biomedical devices, and we demonstrate a temperature sensor and encryption/decryption system that is fabricated in 180 nm CMOS. Body temperature is an immensely valuable means for diagnosis and mitigation of infections and diseases. It is also useful for lab-on-chip applications where the temperature of a cell culture or electrochemical reaction is monitored. This measurement can be coded into voltage, frequency, or time in a wearable device and transmitted to a server for medical/lab personnel to monitor it. Although we demonstrate a temperature sensor in this paper, the sensor output is quasi-digital in nature. Thus, any other sensor with quasi digital output, such as a pH, [32], or impedance sensor, [33], can be used with this encryption system. The encryption system uses analog circuits to implement the encryption enabling low power operation and portability. The implementation and experimental results of the CMOS Lorenz chaotic based system are demonstrated for both single-ended and differential configurations. The mathematical theory underlying this work has been previously developed, presented [34], and demonstrated using discrete components [35], [36]. These prior implementations consumed a significant amount of power. Thus, this work aimed to reduce power consumption so that the system is suitable for wearable, implantable, and portable sensors. The paper is organized as follows. In section II, we give a brief overview of the mathematical system. In section III we detail the translation of the system diagram to analog circuits. In section IV, we give our simulation and experimental results, and, finally, summarize the work in section V.

II. Time Scaled Chaotic Shift Keying

Two chaotic oscillators that have the same circuit, with different starting initial conditions, can be matched to the same trajectory. This matching is achieved by coupling the two systems with a single state shared from one to the other. This process is known as chaotic synchronization [37]. In this scheme, the driving system (encrypting circuit) is the system that provides the shared state, conversely the second system (decryption circuit) is the driven system. The Lorenz system has a strict tolerance for system parameter matching in order for synchronization to occur. These parameters are formed by the Lorenz coefficients and are implemented by the components of the circuit design. This property of two chaotic systems that have different initial conditions but share a single state can self synchronize, can be exploited to generate an encryption mask. Due to the chaotic nature and synchronization, they can be suitable to be used as ciphers for plain text sensor measurement data. This idea has been applied in areas such as speech and image applications [38]–[41]. The synchronization in this paper, shown in fig.2, is showcased in the deciphered message of the receiver being the same as the message before encryption.

The base Lorenz system is described by coupled differential equations [42],

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

where λ, σ, β, and ρ are parameters whose choice of value results in a chaotic system. $x(t)$, $y(t)$, and $z(t)$ are variables.

Chaotic Shift Keying (CSK), using Lorenz based chaotic oscillators to implement the encryption and decryption modules, will effectively randomize the message. When implemented the shared state between the transmitter and receiver is x. However, it is still vulnerable to attacks where, for example, an attacker could extract the transient features of the system by return map attack [43]–[45]. The return map (RM) attack monitors the transmitted state's local minimum and maximum points to break the reveal the original message. This attack can be defeated by time-scaling the encryption modulation. A time-scaling factor that is only a switching event is not enough, as bit changes would be detectable by observation of the transmitted state for significant changes. In this method, to overcome the security weakness of the CSK system to the RM attack, the encryption of the plain-text message $m(t)$ can be handled instead by a "time scaling function" $\lambda(x(t), m)$. Further details of the time scaling CSK can be found in [34], [46]–[48]. This is known as Time Scaled Chaotic Shift Keying or TS-CSK. The transmitter or encryption module, denoted as the system x, is described as,

$$\begin{aligned} x_1' &= \lambda(x, m)\sigma(x_2 - x_2) \\ x_2' &= \lambda(x, m)((\beta(m) - x_3)x_1 - x_2) \\ x_3' &= \lambda(x, m)(x_1 x_2 - \rho x_3) \end{aligned} \tag{2}$$

where $m(t)$ is the sensor data (the message that is being ciphered) and $\beta(m)$ is,

$$\beta(m) = (\beta_1 - \beta_0)m(t) + \beta_0 \tag{3}$$

and $\lambda(x, m)$ is,

$$\lambda(x, m) = \begin{cases} \lambda_m, & \delta_x = 0 \\ \lambda_{1-m}, & \delta_x = 1 \end{cases} \tag{4}$$

$$\delta(x) = \begin{cases} \delta_z, & x_2(t) < -\sqrt{\rho(\beta - 1)} \\ 1 - \delta_z, & -\sqrt{\rho(\beta - 1)} \le x_2(t) < 0 \\ \delta_z, & 0 < x_2(t) < \sqrt{\rho(\beta - 1)} \\ 1 - \delta_z, & x_2(t) \ge \sqrt{\rho(\beta - 1)} \end{cases} \tag{5}$$

where,

$$\delta_z = \begin{cases} cc1, & x_3(t) \ge \beta - 1 \\ 0, & x_3(t) < \beta - 1 \end{cases} \tag{6}$$

The receiver or decryption module is similar to the encryption and is given by,

$$\begin{aligned} z_1' &= \lambda(z, 0)\sigma(z_2 - z_1) \\ z_2' &= \lambda(z, 0)(\beta(m) - z_3)x_1 - z_2 \\ z_3' &= \lambda(z, 0)(x_1 z_2 - \rho z_3) \end{aligned} \tag{7}$$

where $m(t)$ is the sensor data and the message that is being deciphered, the deciphered output is z_1. The shared state between the transmitter and receiver is x_1. The system diagram for both the transmitter (encoder or encryption module) and receiver (decoder or decryption module) is shown in Fig. 3. The TS-CSK algorithm scheme can theoretically withstand ciphertext-only, known plaintext, and chosen plain text attacks and provides increased keyspace through the time scaling factor [46].

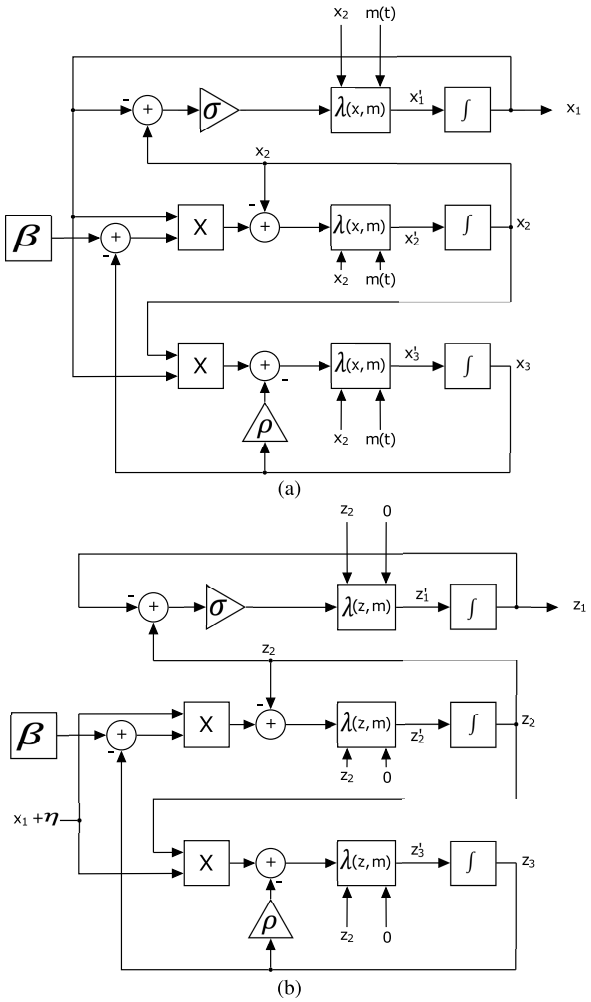

Fig. 3. (a) System diagram of equation (2) representing the transmitter or encryption module (b) System diagram of equation (7) representing the receiver or decryption module. β, σ, and ρ are parameters of the system.

III. Encryption/Decryption Implementation

Fig. 4 shows the TS-CSK system realized from the coupled differential equations and system diagram. Note that the transmitter and receiver are actually represented in the same circuit through the use of the function g. The resistor and transistor sizes were chosen based on the parameters of the differential equations. The resistors sizes in Fig. 4 (a) are, $R_1, R_2 = 10$ kΩ, $R_3, R_4 = 100$ kΩ, $R_5, R_7 = 800$ Ω, and $R_6 = 49.9$ kΩ. The resistor sizes in Fig. 4 (b) are $R_1, R_3 = 1$ kΩ, $R_2 = 59.5$ kΩ, and $R_4 = 59$ kΩ. The initial implementations of the system that was explored used discrete devices. In particular, the integrator was implemented using an opamp and capacitors. These capacitances were very large and not conducive to compact implementation, that is the encryption system should not add significant area (and power) to the biosensor design. Thus, the first attempt at miniaturizing the encryption transmitter/receiver modules involved replacing the discrete components with integrated compact versions.

A. Single-Ended Implementation

The integrator was based on 23 nW integrator designed for implantable devices [49]. It is a low power integrator and

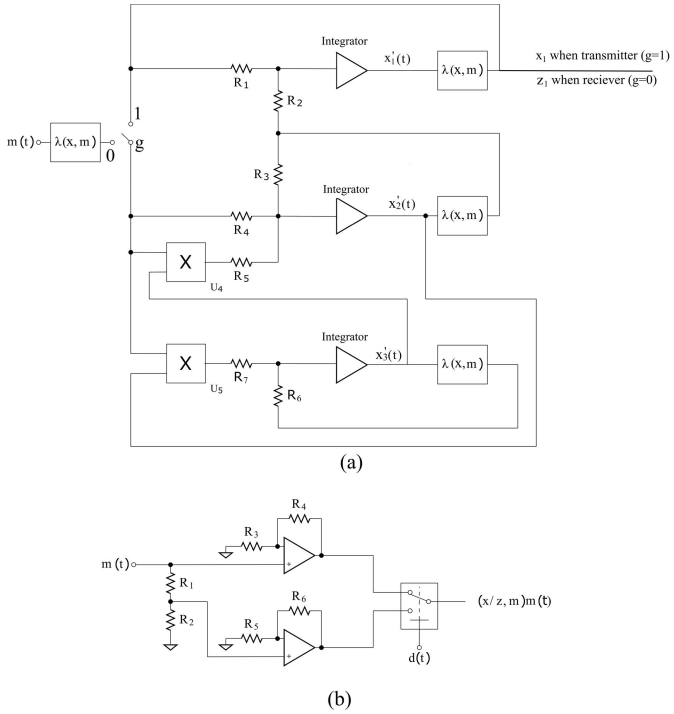

Fig. 4. (a) TS-CSK circuit schematic based on the coupled differential equations. (b) λ modulator circuit schematic.

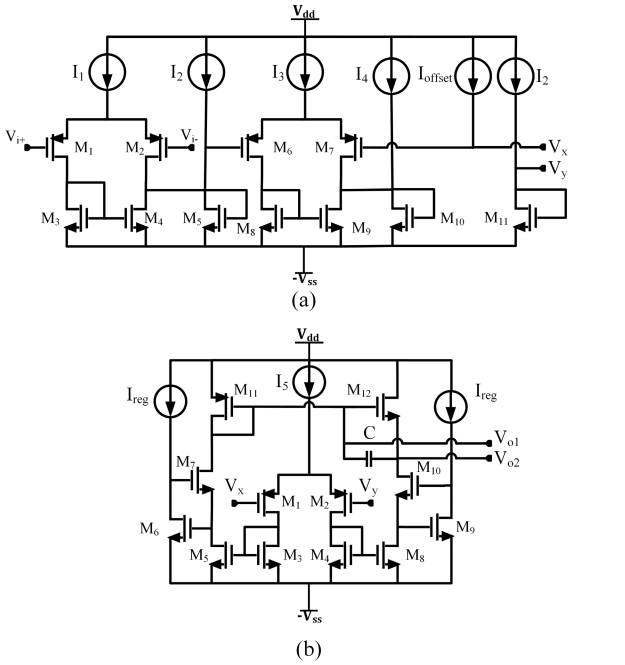

Fig. 5. Integrator circuit consisting of (a) $g_m - 1/g_m$ attenuator stage and (b) OTA-C stage.

consists of a transconductance stage followed by a $1/g_m$ stage that is followed by another transconductance and $1/g_m$ stage. The diode connected $1/g_m$'s are resistances to ground. The series $g_m - 1/g_m$ stages form an attenuator and is shown in Fig. 5 (a). The output of the attenuator is connected to the OTA-C of Fig. 5 (b). The OTA-C is a p-input amplifier with regulated cascode loads. The transistor sizes in 130nm For the $g_m - 1/g_m$ attenuator transistors M_1-M_4, M_6-M_9 are 10μm/5μm and M_5, M_10, M_11 are 90μm/5μm. The transistor sizes of the OTA-C are 10μm/5μm. The capacitor in the OTA-C was 1 pF and was implemented on chip. The integrator was the primary source of accumulating errors and delays in the circuit, and mismatch and process variation can lead to changes in the output signal amplitude and frequency. Having a bias current, I_{offset} facilitated fine tuning of the integrator after fabrication.

The multiplier is shown in Fig. 6. The design used two resistive loads and eight NMOS transistors. The transistor sizes in 130 nm are 18μm/2μm for the input pair, 36μm/2μm for the tail current transistor and 9μm/2μm for other transistors, the resistors are 70 kΩ. For positive input voltage at M_1, M_3, the output is $g_{m5}R_1(In2+ - In2-)$. For negative input voltage at M_4, M_2, the output is $-g_{m5}R_1(In2+ - In2-)$. Two multipliers were used. The inputs were $In1+$ and $In1-$ for the first differential input and $In2+$ and $In2-$ for the second one. The first differential signal ($In1+$ - $In1-$) is multiplied with the second differential signal between $In2+$ and $In2-$, and the output is $Out+$ and $Out-$. In line, with the original discrete implementation, although the outputs of the integrator and multiplier were fully differential, the signals were made to be singled ended based on using a 5 transistor OTA (Fig. 7).

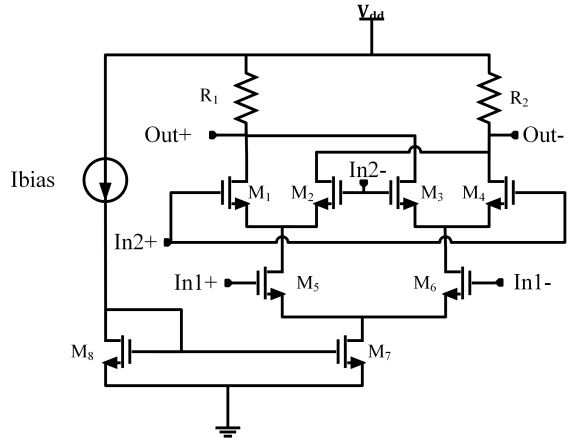

Fig. 6. Multiplier circuit.

The transistor sizes for the OTA were 1μm/0.5μm for the tail current transistor and 3.3μm/0.5μm for PMOS transistors and 2μm/0.5μm for NMOS transistors.

The fabricated chip is shown in Fig. 8 (a). The integrator was experimentally verified with a signal of 5 Hz and 20 mV to confirm the 1 s time constant. The integrator output voltage (V_o) response versus the input is shown in Fig. 9. Changing the biasing current source changes g_m and $1/g_m$ leading to a change in time constant.

The experimental measurement of the basic multiplier for two sinusoidal test inputs is shown in Fig. 10. The multiplication is applied to both the form and amplitude of the signal. This figure shows a square wave and a sine wave voltage as inputs. The output shows that when the amplitude of the square wave changes, from positive to negative, the resulting

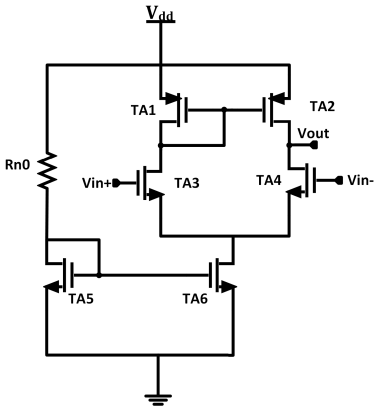

Fig. 7. OTA used for the amplifiers in the system.

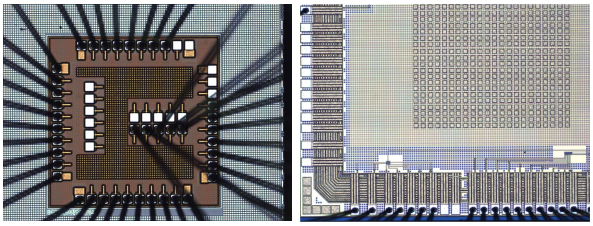

Fig. 8. (a) First implementation of the encryption chip fabricated in 130 nm BiCMOS technology. (b) The second implementation, in 180 nm, showing the integrator module on the bottom left and the multiplier module on the bottom right (β modulator circuit and amplifiers not shown).

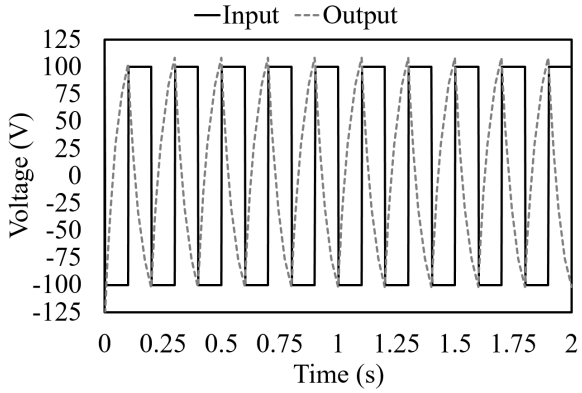

Fig. 9. Experimental transient response of the integrator in a 130 nm process.

sinusoidal voltage is inverted as expected. Using off-chip resistors, the system shown in Fig. 4 was setup. However, no oscillation was achieved experimentally due to the offset caused by the single-ended nature of circuit blocks. This lack of oscillation was verified in simulations after completing the experiment and is shown in Fig. 11 where the outputs of x and y correspond only linearly. This was due to an offset that was formed at the output of single-ended output. To eliminate this offset in discrete designs usually big capacitors, on the order of a few 10 or few 100 μF, can be used. However, for integrated circuit implementation, the elimination of the capacitors along with process variation and mismatch caused a few mV of offset in each cycle, driving the system to saturation.

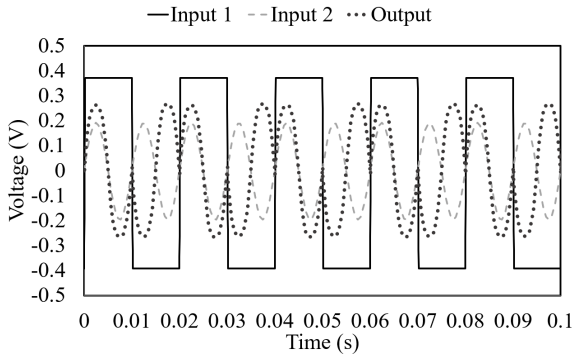

Fig. 10. Experimental transient response of the multiplier implemented in a 130 nm process.

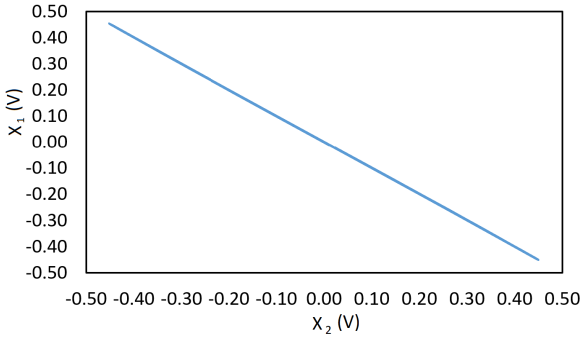

Fig. 11. Single-ended chaotic system, implemented in 130 nm, showed no oscillations.

B. Differential System

To alleviate this issue, a fully differential system was developed (Fig. 12). Although the single-ended design was implemented in 130 nm, changes in process availability required the differential implementation to be developed in a 180 nm process. Thus, the differential system was implemented in a 180 nm technology using the same integrator and multiplier circuits of Figs. 5 and 6. For the multiplier, the resistors are 70 kΩ and the transistor sizes were 9μm/2.25μm. For the $g_m - 1/g_m$ attenuator stage, transistors M_1-M_4, M_6-M_9 were 4μm/2μm and M_5, M_{10}, M_{11} were 9μm/2μm. The current I_2 and I_4 were 24.7 nA and I_1, I_3, and I_5 were 37.9 nA. I_{reg} was 1.7 μA. I_{offset} was adjusted to make the signal symmetric. The transistor sizes of the OTA-C were 4μm/2μm. Using the differential scheme, the offset does not aggregate, preventing the system from being becoming saturated. For the time scaling parameter, an amplifier and transmission gates were connected to the output of integrator and then to the rest of the circuit. Fig. 13 and Fig. 14 show the experimental measurements of the multiplier and integrator.

IV. Experimental Results

The initial single-ended system was designed in a 7 metal, single poly, 130 nm BiCMOS technology. The differential encryption system, along with the temperature sensor, was implemented in a single chip in a 180 nm process (Fig. 8 (b)). The use of different technologies was due to changes in foundry availability over the course of the project. Fig. 15

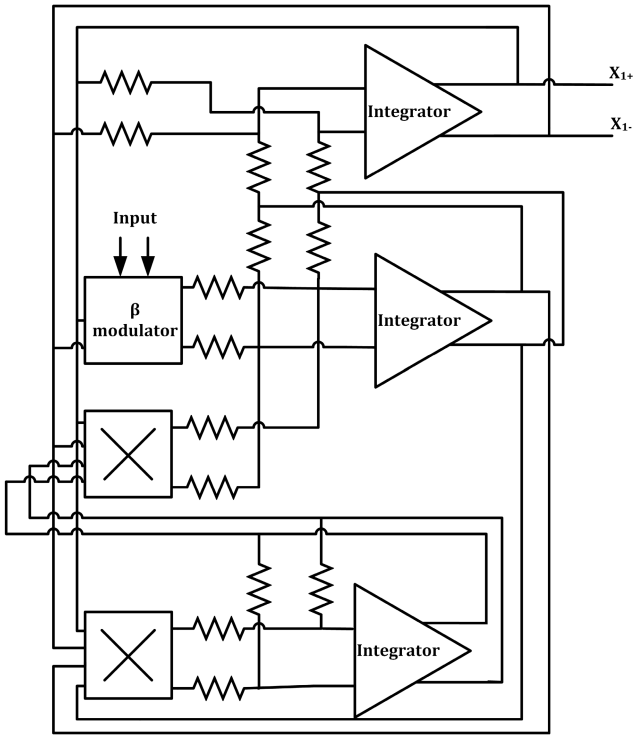

Fig. 12. Fully differential TS-CSK encryption system.

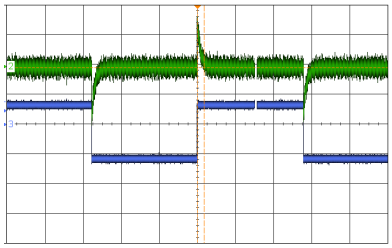

Fig. 13. Oscilloscope screen capture of the experimental output of the integrator circuit in a 180 nm process.

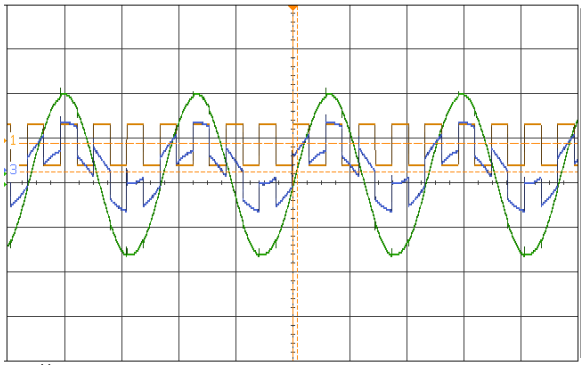

Fig. 14. Oscilloscope screen capture of experimental output of the multiplier circuit in a 180 nm process.

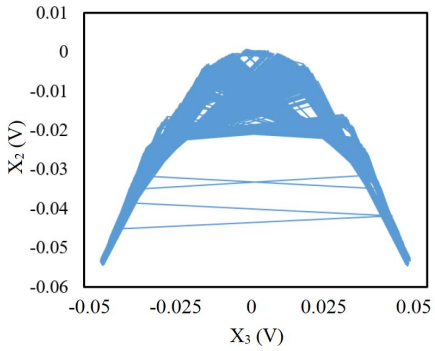

Fig. 15. Simulation results of x_2 and x_3 output of the differential system showing chaotic behaviour of the circuit in 180 nm.

shows the chaotic behavior of the fully differential circuit. The transmitter and receiver, on a prototype board, is shown in Fig. 16. In order to allow maximum flexibility in testing while implementing this first system prototype, the integrators, multipliers, and other modules were separately laid out on the chip. To assemble the transmitter/receiver system, 3 chips were used. The first two chips implemented an integrator-multiplier pair on the bottom half of Fig. 12 and the third integrator was implemented by a third chip. This is seen in Fig. 8, and the biases are implemented off-chip. However, the entire system, including resistors, fits within a 1.5 mm $\times$ 1.5 mm area. The temperature sensor is on each chip, and in this setup, the temperature sensor located on the first chip is used to perform the measurements. In the picture, the red wire is the first state (x_1 shown in Fig. 4) of the system that is used for synchronization between the transmitter (encryption module) and the receiver (decryption module).

The encryption/decryption (transmitter/receiver) modules were tested with the output of the temperature sensor. The temperature sensor used a weak inversion PTAT generation circuit to convert temperature to voltage. The voltage is then converted to frequency using opamps, a capacitor, comparators, a low voltage reference, and an SR latch. The frequency of the temperature sensor is linear over 0 to 50 $^{\circ}C$ with a resolution of 0.2 $^{\circ}C$. Details of the temperature sensor design (in a different process) may be found in [35] and the circuit schematic is shown in Fig. 17. For the 180 nm process, the transistor sizes are 0.5μm/0.36μm for T_1 and T_2, 2μm/2.8μm for T_3, 0.36μm/2.88μm for T_4, 3μm/0.36μm for T_5-T_7 and 1.5μm/0.36μm for T_8-T_9. The experimental result of the chaotic encoded signal is shown in Fig. 18. The input of the system is the temperature sensor (shown in Fig. 18 (a) for 50 °C). This signal is encrypted by the ciphering transmitter and transmitted to the receiver and is shown in Fig. 18 (b). Fig. 18 (c) shows the decoded signal, after thresholding (blue line) and smoothing (black line), at the output of the receiver.

The integrator circuit consumed 2.1μW and the size was 0.006 mm^2. The multiplier consumed 100 μ W with an area of 0.002 mm^2. The total system consumed 1.5 mW for a 0.2 V, 0.1 s test signal. Although tested independently, the entire system, including biases and resistors fits within a 1.5 mm $\times$ 1.5 mm area.

Table I compares the encryption system to other reported chaotic systems in the literature. The developed system has a competitive area compared to recent implementations. Due to the low supply voltage in integrated circuit implementation, the developed system also has lower power consumption

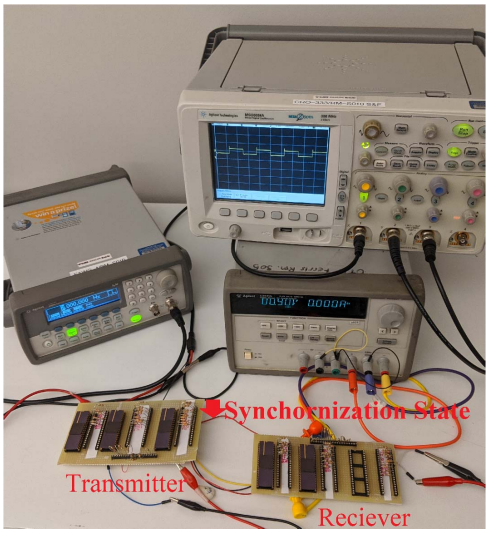

Fig. 16. Implementation of the temperature sensor with the transmitter and receiver on a prototype board. Each chip contains an integrator, multiplier, OTA, and temperature sensor.

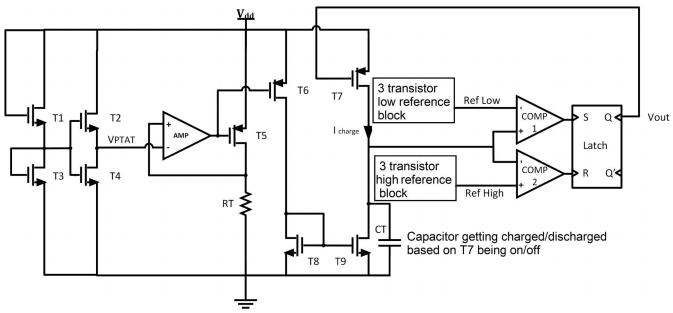

Fig. 17. Temperature sensor circuit with weak inversion MOSFETs.

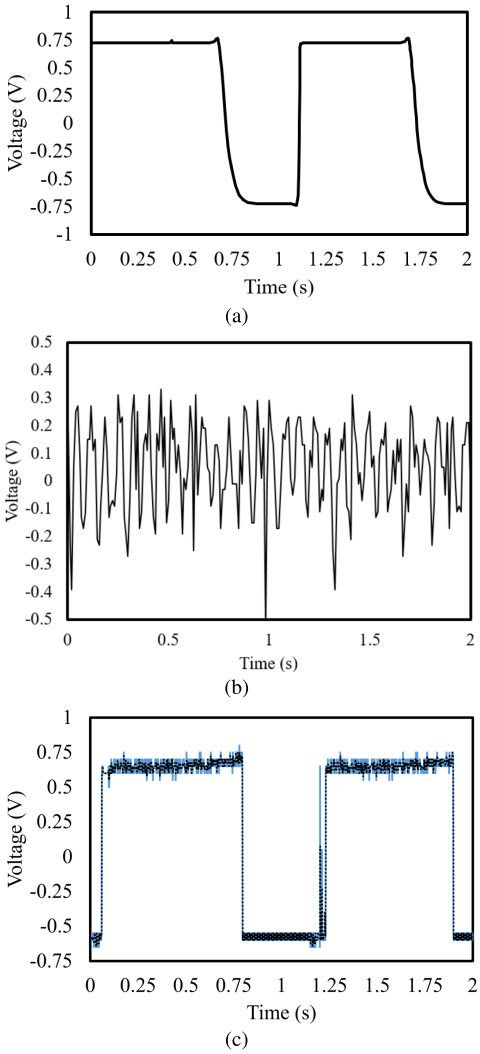

Fig. 18. Experimental measurements of the encrypted and decrypted signal by the ciphering transmitter and receiver implemented in 180 nm. (a) The output of the temperature sensor at the input of the transmitter. (b) The transmitter input and the receiver output. (c) The decoded signal at the output of the receiver.

than other fabricated systems. Our implemented system has a small area primarily due to the use of small capacitors in the integrator and by replacing the traditional integrator with a 1/gm, gm based system. The low power consumption is achieved by using an integrator with power consumption in nano meter range, prioritizing power in the design process, and implementing the circuit in small technology. In order to compare the various systems, a figure of merit (FOM) was defined. The figure of merit decreases as the system moves closer to a portable system. To define the figure of merit, the parameters whose decrease contributed to an improved system were multiplied in the numerator. If a parameter improved the system by increasing, it was included in the figure of merit's denominator. Based on the units chosen, the FOM ranges from thousands to one over thousands. To emphasize the importance of being robust to attacks, if the system was not listed as robust to attacks, the FOM was multiplied by 10. The developed FOM is,

$$FOM = T \times A \times V_{supp} \times P \times N \times V \times t \times AP \qquad (8)$$

were T is the technology node in μm, A is the area in (mm^2), V_{supp} is the supply voltage, P is the power, N is the number of blocks, V is the test signal voltage, t is the test signal time (and inverse of signal frequency), and AP is the attack prevention. The extreme difference in the F.O.M lies in the area difference between discrete and integrated devices. These sizes are in the range of cm^2 for discrete devices and mm^2 for integrated devices. Since many of the discrete devices could be theoretically translated to integrated circuit implementations, a column showing the performance regardless of area is also included. It should be noted that all the systems referenced are focused on implementing the chaotic system and do not mention if or how robust the architectures are to various attack schemes, thus their AP is given a value of 10.

Though the on-chip security system synchronizes, there was still an aggregating delay formed in the system that caused the system to go out of synchronization after a certain number of cycles. The implementation of the β and λ modulators using the amplifier and switch were the cause of this delay. The switches were developed with pass transistors that do contain delay compensating capacitors. To ensure a constant synchronization, the delay should be reduced.

TABLE I
COMPARISON TABLE WITH STATE OF ART CHAOTIC COMMUNICATION

Ref	Year	Design	Area	Supply	Power	Test Signal (1/frequency)	RM Attack Resistance	FOM	FOM/A
[17]	1993	0.35 μm	4 mm^2	$\pm$2.5V	1.8W	0.2 V 0.1 s	No	5.04	1.26
[18]	1995	0.35 μm	4 mm^2	$\pm$2.5 V	1.6W	0.2 V 0.1 s	No	4.48	1.12
[22]	2000	0.35 μm	4.8 mm^2	$\pm$3 V	$<$ 1W [a]	0.5 V, 0.1 ms	No	0.04	0.008
[23]	2005	Simulated 0.6μm	0.1 mm^2	5 V	7.85 mW	-	No	0.01	0.1
[28]	2015	Simulated 0.35 μm	1.5 mm^2	1.4 V	360 mW	-	No	1.32	0.88
[30]	2017	Simulated 0.35 μm	2 mm^2 [b]	$\pm$1.2 V	$<$W [a]	0.2 V, 0.1 s	No	0.67	0.33
[31]	2019	Simulated 0.35 μm	2 mm^2	3.3 V	1.7 mW	-	No	0.01	0.005
[24]	2009	FPGA Xilinx	2 cm^2	3.3 V	5 W [a]	-	No	13.2 k	33
[27]	2013	Discrete Simulated TL084	10 cm^2 [a]	$\pm$15 V	2 W	1 V, 1 s	No	600 k	60
[25]	2013	FPGA Xilinx	2 cm^2	$\pm$15 V	5 W [a]	1 V, 1 s	No	60k	150
[26]	2020	FPGA Xilinx	4 cm^2	3.3 V	300 mW [a]	-	No	1584	0.99
[29]	2016	Discrete	10 cm^2	15 V	$<$10 W [a]	0.2 V, 0.1 s	No	90 k	9
This work	2020	0.18 μm	1.5 mm^2	1.8 V	1.5 mW	0.2 V, 0.1 s	Yes	0.0001	0.000067

a This parameter is estimated based on the article.

b Capacitors implemented off-chip.

The ciphering block was designed to specifically work with our developed temperature sensor, which is a slow signal. However, as can be seen from table I, most chaotic systems operate in a similar bandwidth. In this initial implementation of the system, the different modules were implemented on different chips for maximum testing flexibility. Implementing the circuits on the same chip will decrease the noise and parasitics of each block, improving synchronization. Additionally, including techniques such as dynamic feedback will facilitate synchronization at higher frequencies [50], [51].

V. CONCLUSION

In this work, an encryption system was demonstrated using CMOS based analog circuits. The system can be integrated directly with sensors on a single chip lowering the system weight, size, and power. An initial one-to-one translation of the previously implemented discrete system to an integrated system was done by replacing the opamps and capacitors with a low power integrator and using multipliers and amplifiers to implement the remainder of the system. Experimental measurements and subsequent simulations showed that the single-ended implementation did not oscillate and was thus not suitable for encryption. The development of a differential system, however, showed successful oscillation and encryption/decryption of a sensor signal.

The core of the system used multipliers and continuous-time integrators with a large time constant to realize the Lorenz chaotic oscillator based chaotic stream. The differential system was experimentally verified with the output from a temperature sensor, located on the same chip, whose output frequency is proportional to the temperature. Although all circuits were tested on separate chips to avoid biasing issues, the entire system, including the temperature sensor, fits on a single 1.5 mm $\times$ 1.5 mm area. Experimental measurements indicated the system was suitable for low frequency data and is appropriate for many biological and environmental monitoring applications.

This paper represents a step forward in the integration of encryption and sensors in the same hardware and on the same chip. Although implemented in separate chips, comparison with other implementations indicate reduced power and size, particularly when compared to FPGA and discrete implementations. The chaotic system implemented here was assumed to be robust, however, there are alternative implementations and architectures that could further lower the power and area. This is important given that an implantable or wearable biosensor will need to be wireless with an additional transceiver module

along with regulation and sensor calibration contributing to the total power and area budget. The use of optimization techniques or feedback for delay reduction and the use of alternative chaotic oscillator systems could make the encryption system more suitable for higher frequency data and present even further power and size savings; while calibration and feedback techniques might potentially solve issues caused to process variations.

REFERENCES

[1] US Food and Drug administration FDA, "Certain medtronic MiniMed insulin pumps have potential cybersecurity risks: FDA safety communication," FDA, White Oak, MD, USA, Tech. Rep., Jun. 2019. Accessed: Feb. 2020. [Online]. Available: https://www.fda.gov/medical-devices/safety-communications/certain-medtronicminimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safetycommunication

[2] Cybersecurity and Infrastructure Security Agency. (Jun. 4, 2020). *ICS Medical Advisory (ICSMA-19-080-01), Medtronic Conexus Radio Frequency Telemetry Protocol (Update B)*. Accessed: Feb. 2020. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01

[3] S. Faezi *et al.*, "Oligo-snoop: A non-invasive side channel attack against DNA synthesis machines," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, Feb. 2019, pp. 1–15.

[4] C. Tankard, "The security issues of the Internet of Things," *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, Sep. 2015.

[5] J. M. Navya, H. A. Sanjay, and K. Deepika, "Securing smart grid data under key exposure and revocation in cloud computing," in *Proc. 3rd Int. Conf. Circuits, Control, Commun. Comput. (I C)*, Bangalore, India, Oct. 2018, pp. 1–4.

[6] D. Liu *et al.*, "Research on technology application and security threat of Internet of Things for smart grid," in *Proc. 5th Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Zhengzhou, China, Jul. 2018, pp. 496–499.

[7] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Minimum on-the-node data security for the next-generation miniaturized wireless biomedical devices," in *Proc. IEEE Int. Midwest Symp. Circuits Syst.*, Springfield, MA, USA, Aug. 2020, pp. 1068–1071.

[8] S. S. Ghoreishizadeh, T. Yalçın, A. Pullini, G. De Micheli, W. Burleson, and S. Carrara, "A lightweight cryptographic system for implantable biosensors," in *Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS)*, Lausanne, Switzerland, Oct. 2014, pp. 472–475.

[9] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. Int. Conf. Parallel Process. Workshops,* Kaohsiung, Taiwan, Oct. 2003, pp. 432–439.

[10] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[11] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr. 2015.

[12] C. Xie and Y. Xu, "Chaos control and synchronization of a new chaotic system," in *Proc. Int. Workshop Chaos-Fractal Theories Appl.*, Hangzhou, China, Oct. 2010, pp. 43–47.

[13] G. Makris and I. Antoniou, "Cryptography with chaos," in *Proc. Int. Conf. Chaotic Modeling Simulation*, Athens, Greece, Jun. 2012, pp. 12–15.

[14] J. M. Liu and L. S. Tsimring, *Digital Communications Using Chaos and Nonlinear Dynamics*. Berlin, Germany: Springer, 2006.

[15] J. Lu, X. Wu, and J. Lü, "Synchronization of a unified chaotic system and the application in secure communication," *Phys. Lett. A*, vol. 305, no. 6, pp. 365–370, Dec. 2002.

[16] P. R. Castañeda-Aviña, E. Tlelo-Cuautle, and L. G. de la Fraga, "Single-objective optimization of a CMOS VCO considering PVT and Monte Carlo simulations," *Math. Comput. Appl.*, vol. 25, no. 4, p. 76, Dec. 2020.

[17] M. Delgado-Restituto and A. Rodriguez-Vazquez, "A CMOS analog chaotic oscillator for signal encryption," in *Proc. Eur. Solid-State Circuits Conf.*, Seville, Spain, Sep. 1993, pp. 110–113.

[18] M. Delgado-Restituto, A. Rodriguez-Vazquez, and M. Linan, "A modulator/demodulator CMOS IC for chaotic encryption of audio," in *Proc. Eur. Solid-State Circuits Conf.*, Lille, France, Sep. 1995, pp. 170–173.

[19] M. R. Dar, N. A. Kant, and F. A. Khanday, "Electronic implementation of fractional-order Newton Leipnik chaotic system with application to communication," *J. Comput. Nonlinear Dyn.*, vol. 12, no. 5, pp. 054502-1–054502-5, 2017.

[20] R. Trejo-Guerra *et al.*, "Integrated circuit generating 3-and 5-scroll attractors," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 11, pp. 4328–4335, 2012.

[21] M. R. Dar, N. A. Kant, and F. A. Khanday, "Realization of Integrable incommensurate-fractional-order-Rössler-system design using operational transconductance amplifiers (OTAs) and its experimental verification," *Int. J. Bifurcation Chaos*, vol. 27, no. 5, 2017, Art. no. 1750077.

[22] O. A. Gonzalez, G. Han, J. P. De Gyvez, and Edgar, "CMOS cryptosystem using a lorenz chaotic oscillator," in *Proc. IEEE Int. Symp. Circuits Syst. VLSI (ISCAS)*, Prlando, FL, USA, Aug. 1999, pp. 442–445.

[23] V. D. Juncu, M. Rafiei-Naeini, and P. Dudek, "Integrated circuit implementation of a compact discrete-time chaos generator," *Anal. Integr. Circuits Signal Process.*, vol. 46, no. 3, pp. 275–280, Mar. 2006.

[24] M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Dandache, "Real-time FPGA implementation of Lorenz's chaotic generator for ciphering telecommunications," in *Proc. Joint IEEE North-East Workshop Circuits Syst. TAISA Conf.*, Toulouse, France, Jun. 2009, pp. 1–4.

[25] I. Koyuncu, A. T. Ozcerit, and I. Pehlivan, "An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system," *Optoelectronics Adv. Mater.-Rapid Commun.*, vol. 7, pp. 635–638, Sep./Oct. 2013.

[26] A. H. Elsafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Enhanced hardware implementation of a mixed-order nonlinear chaotic system and speech encryption application," *AEU-Int. J. Electron. Commun.*, vol. 125, Oct. 2020, Art. no. 153347.

[27] H.-C. Chen, B.-Y. Liau, and Y.-Y. Hou, "Hardware implementation of lorenz circuit systems for secure chaotic communication applications," *Sensors*, vol. 13, no. 2, pp. 2494–2505, Feb. 2013.

[28] Y.-L. Wu, C.-H. Yang, Y.-S. Li, and C.-H. Wu, "Nonlinear dynamic analysis and chip implementation of a new chaotic oscillator," in *Proc. IEEE 12th Int. Conf. Netw., Sens. Control*, Taipei, Taiwan, Apr. 2015, pp. 554–559.

[29] L. Xiong, Y.-J. Lu, Y.-F. Zhang, X.-G. Zhang, and P. Gupta, "Design and hardware implementation of a new chaotic secure communication technique," *PLoS ONE*, vol. 11, no. 8, Aug. 2016, Art. no. e0158348.

[30] M. R. Dar, N. A. Kant, and F. A. Khanday, "Realization of fractional-order double-scroll chaotic system using operational transconductance amplifier (OTA)," *J. Circuits, Syst. Comput.*, vol. 27, no. 1, Jan. 2018, Art. no. 1850006.

[31] V. H. Carbajal-Gomez, E. Tlelo-Cuautle, J. M. Muñoz-Pacheco, L. G. de la Fraga, C. Sanchez-Lopez, and F. V. Fernandez-Fernandez, "Optimization and CMOS design of chaotic oscillators robust to PVT variations: INVITED," *Integration*, vol. 65, pp. 32–42, Mar. 2019.

[32] S. Aslanzadeh, A. Hedayatipour, and N. McFarlane, "ISFET digital readout circuit with an on-chip MIPS processor," in *Proc. IEEE SENSORS*, Rotterdam, The Netherlands, Oct. 2020, pp. 1–4.

[33] A. Hedayatipour, S. Aslanzadeh, S. H. Hesari, M. A. Haque, and N. McFarlane, "A wearable CMOS impedance to frequency sensing system for non-invasive impedance measurements," *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 5, pp. 1108–1121, Oct. 2020.

[34] D. Brown, A. Hedayatipour, M. B. Majumder, G. S. Rose, N. McFarlane, and D. Materassi, "Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry," *IET Comput. Digit. Techn.*, vol. 12, no. 6, pp. 297–305, Nov. 2018.

[35] A. Hedayatipour, K. Anderson, S. Aslanzadeh, D. Brown, D. Materassi, and N. McFarlane, "A temperature sensing system with encrypted readout using analog circuits," in *Proc. IEEE 62nd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Dallas, TX, USA, Aug. 2019, pp. 152–155.

[36] A. Hedayatipour, K. Anderson, and N. McFarlane, "Live demonstration: A temperature sensor with analog encryption," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Sapporo, Japan, May 2019, p. 1.

[37] L. M. T. L. Pecora amd Carroll, "Synchronization of chaotic systems," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 25, no. 9, 2015, Art. no. 097611.

[38] E. Tlelo-Cuautle, V. H. Carbajal-Gomez, P. J. Obeso-Rodelo, J. J. Rangel-Magdaleno, and J. C. Nuñez-Pérez, "FPGA realization of a chaotic communication system applied to image processing," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1879–1892, Dec. 2015.

[39] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[40] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP J. Audio, Speech, Music Process.*, vol. 2017, no. 1, pp. 1–11, Dec. 2017.
[41] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map," *Multimedia Tools Appl.*, vol. 79, pp. 1–19, Feb. 2020.
[42] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, Mar. 1963.
[43] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, p. 65, 1993.
[44] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 634–642, Oct. 1993.
[45] G. Pérez and H. A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, no. 11, p. 1970, 1995.
[46] D. Materassi and M. Basso, "Time scaling of chaotic systems: Application to secure communications," *Int. J. Bifurcation Chaos*, vol. 18, no. 2, pp. 567–575, Feb. 2008.
[47] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *J. Inf. Secur. Appl.*, vol. 50, p. 02421, 2020.
[48] X. Gao, M. Cheng, L. Deng, M. Zhang, S. Fu, and D. Liu, "Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system," *Opt. Exp.*, vol. 28, no. 8, pp. 10847–10858, 2020.
[49] R. Rieger, A. Demosthenous, and J. Taylor, "A 230-nW 10-s time constant CMOS integrator for an adaptive nerve signal amplifier," *IEEE J. Solid-State Circuits*, vol. 39, no. 11, pp. 1968–1975, Nov. 2004.
[50] C. Liang, Q. Zhang, J. Ma, and K. Li, "Research on neural network chaotic encryption algorithm in wireless network security communication," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–10, Dec. 2019.
[51] S. Hu, S. Yu, Y. Hu, Z. Wang, and B. Zhou, "A novel 1–6 GHz chaotic signal oscillator for broadband communication systems," in *Proc. Prog. Electromagn. Res. Symp. (PIERS-Toyama)*, Toyama, Japan, Aug. 2018, pp. 1550–1554.

Ava Hedayatipour (Member, IEEE) received the B.S. degree in electrical engineering from the Iran University of Science and Technology, Iran, in 2012, the M.S. degree in electrical engineering from Shahid Rajaee Teacher Training University, Tehran, Iran, in 2015, and the Ph.D. degree from the Department of Electrical Engineering and Computer Science, The University of Tennessee at Knoxville, Knoxville, in 2020. She joined the Department of Electrical Engineering, California State University Long Beach (CSULB), as an Assistant Professor, in Fall 2020. Her research interests include analog integrated circuit designs, bio-implantable and biomedical devices, low power and low noise designs, microelectronics, mixed signal VLSI designs, and semiconductor devices.

Nicole McFarlane (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Howard University, Washington, DC, USA, in 2001 and 2003, respectively, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2010. She is currently a TCE Advance Professor and an Associate Professor with The University of Tennessee at Knoxville, where she is involved in developing smaller and more efficient circuits and devices for sensing systems. Her research interests include III-V-nitrides, information and power efficiency tradeoffs in mixed-signal integrated circuit design, CMOS biosensors, and CMOS/MEMS integration for lab-on-a-chip technologies. Her research group uses mixed signal VLSI to work on integrated smart sensors, hardware security and encryption, and device nanofabrication for applications in biological portable, wearable, and implantable sensing, environmental monitoring, and nuclear science.