A Temperature Sensing System With Encrypted Readout Using Analog Circuits

Ava Hedayatipour*, Kendra Anderson*, Shaghayegh Aslanzadeh*, Daniel Brown*,
Donatello Materassi† and Nicole McFarlane*
*Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville
†Department of Electrical and Computer Engineering, University of Minnesota, Twin Cities
Email: ahedaya1@vols.utk.edu

***Abstract*—Low power integrated compact sensors for applications such as IoT and arrayed biomedical sensors are essential for today's technology. However, security is not incorporated in these sensors and are typically added after implementation using digital hardware or software. In this paper, we demonstrate a temperature to time sensing system with a discrete level encryption process using real-time analog circuitry and minimal processing power. The encryption uses the chaotic Lorenz attractor system. The temperature sensor, implemented in 130 nm technology, consumes 195 nW with 0.5 V power supply. The encryption module is simulated in Simulink and implemented at the board level using discrete components on a printed circuit board. Experimental results show that the envisioned chaotic system is capable of accurately encrypting and decrypting the digital temperature signal.**

I. Introduction

CMOS sensors can be compact and consume a low amount of power, leading to their popularity in biomedical and other wireless applications. Using a quasi-digital output, where analog and digital devices are combined, and the information is converted into time, frequency, or duty-cycle, provides a level of noise immunity which makes the output signals easier to read [1]. However, security, in the form of encryption, is not usually incorporated directly at the design stage of integrated circuits. Encryption provides privacy and secrecy of the sensitive information being transmitted. This is an important layer to have, especially if a hacker attack can harm users of the sensors as, for example, in implanted biosensors.

Encryption is the process of encoding information so that it cannot be read or understood by unauthorized parties. However, unauthorized parties can use cryptanalysis to decode the encryption and translate the information. With the use of computers, fast and cheap encryption has become possible. However, it has also allowed brute force methods of code cracking. Both asymmetric and symmetric ciphers have been designed to combat these brute force methodologies [2].

There have been a number of approaches in literature for developing encryption systems. Cyber-physical systems have both analog and digital components, and a hybrid theory for both continuous-time and digital signals has been proposed [3]. Analog circuits have been used to exploit the synchronization of oscillators and encode signals using chaotic encryption [4]. CMOS based modulator/demodulator systems that generate controllable continuous-time chaotic signals have been used to encrypt audio signals [5]. In this work, we use chaotic encryption.

This paper demonstrates the concept of using analog security for sensors and takes the first step towards hardware based integrated security encryption in IoT and arrayed sensor systems. Previous work partially developed the temperature sensor design [1] and determined how well the encryption system worked from a security point of view [2]. In this paper, we further previous work by improving the design and experimentally demonstrating the encryption algorithm with a complete low power temperature sensor. To the best of our knowledge, this is the first experimentally demonstrated CMOS temperature sensor with printed circuit board implemented Lorenz based chaotic encryption/decryption system. The full system can be potentially integrated in a single chip.

The paper is organized as follows. In section II we describe the theory and design of the temperature and encryption/decryption modules. In section III, we report simulation and experimental results, and finally, the conclusion is outlined in section IV.

II. Theory and Design

The main components of the encrypted low power temperature sensing system are the front end temperature sensor, a transmitter, and a receiver (Fig. 1). The temperature sensor detects the temperature and translates the data to time in a quasi-digital manner. The digital signal is encoded using a chaotic stream cipher and sent to the transmitter. The receiver then decodes the data once it has received the signal. Combining the temperature sensor with a chaotic stream cipher allows the signal to be protected and secure while the device is being used. The potential advantage of using this particular cipher with the temperature sensor is that the whole system can operate with relatively low power consumption compared with implementation on a microprocessor or in software.

A. Temperature Sensor

The temperature sensor uses a quasi-digital output to enable low power consumption and low area for portable and miniaturized applications. The sensor uses a proportional to absolute temperature (PTAT) voltage generation circuit. The PTAT generation circuit detects the temperature using weak inversion MOSFETs (T1-T4) and converts the temperature into a voltage

978-1-7281-2788-0/19/$31.00 ©2019 IEEE

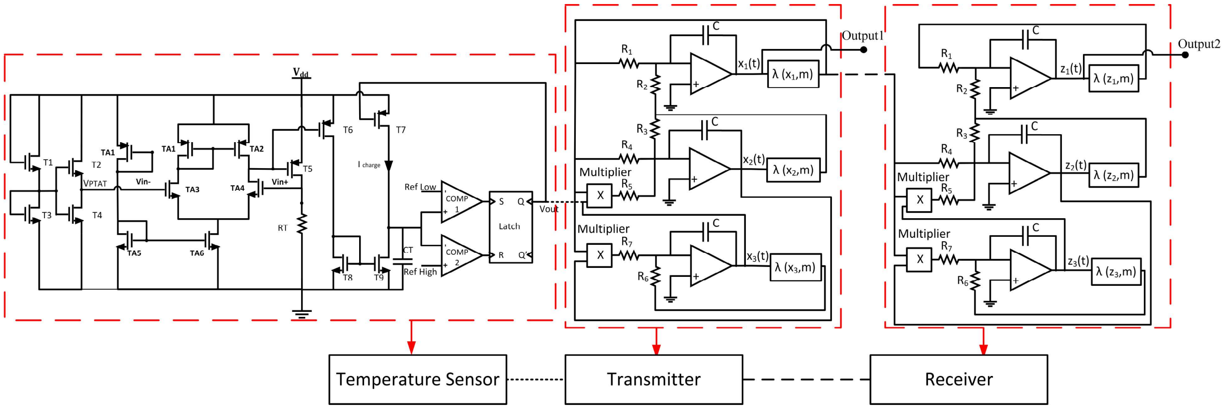

Fig. 1. Time based temperature sensing system using weak inversion MOSFETs along with encrypting transmitter and receiver. The connection between the transmitter and receiver may be wired or wireless.

signal. The voltage signal is fed into an amplifier (TA1-TA6) and a scaling transistor (T5), which amplifies and converts it to a current signal. This is mirrored and used to charge and discharge a capacitor (T6-T9, CT). A standard comparator compares the voltage of the capacitor to two reference voltages (V_{ref} low and high) to determine if the capacitor (1 pF) is charged or discharged. In this implementation off-chip voltage references were used to allow for tunability. An SR latch captures the data from the comparators and turns it into a digital output. The frequency or pulse width of the digital output is proportional to the temperature.

B. Encryption and Decryption

The algorithm for encryption/decryption uses time scaling chaotic shift keying to obtain return map immunity and provide relatively low power consumption. Chaotic encryption relies on two systems which can be synchronized. In this work, a Lorenz based chaotic shift keying (CSK) system is used. The system equations are [2], [6],

$$\begin{array}{cc} \dot{x}_1 = \sigma(x_2 - x_1) & \dot{z}_1 = \sigma(z_2 - z_1) \\ \dot{x}_2 = (\beta(m) - x_3)x_1 - x_2 & \dot{z}_2 = (\beta_0 - z_3)x_1 - z_2 \\ \dot{x}_3 = x_1x_2 - \rho x_3 & \dot{z}_3 = x_1z_2 - \rho z_3 \end{array} \tag{1}$$

In these equations, x_1, x_2, and x_3 are three states of transmitter. z_1, z_2, and z_3 are the three states of receiver. β(m) is the modulated message. The system diagram of the basic CSK system is shown in Fig. 1. The constant β_0 is the system modulator. The encrypted signal, and the receiver's input, is the transmitted state x_1. This state is summed with a band-limited Gaussian noise, η.

One vulnerability of the CSK algorithm is the return map attack. In this attack, time varying characteristics can be decoded by monitoring local maxima and minima. To mitigate this, the cipher uses time scaling chaotic shift keying. This time Scaling chaotic shift keying or TS-CSK encryption is implemented using λ(x,m), a time scaling factor, where m is the message that can be 0 or 1 (representing low and high). The system equations are [2],

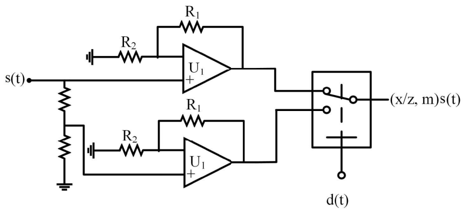

Fig. 2. Implementation of time scaling factor, λ.

$$\begin{array}{c} \dot{x}_1 = \sigma(x_2 - x_1)\lambda(x,m) \\ \dot{z}_1 = \sigma(z_2 - z_1)\lambda(z,0) \\ \dot{x}_2 = ((\beta(m) - x_3)x_1 - x_2)\lambda(x,m) \\ \dot{z}_2 = ((\beta(m) - z_3)x_1 - z_2)\lambda(z,0) \\ \dot{x}_3 = (x_1x_2 - \rho x_3)\lambda(x,m) \\ \dot{z}_3 = (x_1z_2 - \rho z_3)\lambda(z,0) \end{array} \tag{2}$$

where,

$$\lambda(x,m) = \left\{ \begin{array}{ccc} \lambda_m & if & d_x = 0 \\ \lambda_{1-m} & if & d_x = 1 \end{array} \right\} \tag{3}$$

where $\delta(x)$ is the decision engine function. The use of η depends on whether the transmitter encryption module or receiver decryption module is being utilized and tests the system's robustness to line noise. Environmental noise is used as η during experiments. The full system realizing these equations is shown in Fig. 1. The circuit diagram of the time scaling factor, λ, that implements the change of any input signal $(s(t))$ is shown in Fig. 2. The message extraction technique uses a periodic averaging approach with thresholding that uses the state x of the transmitter/encrypter for synchronization. To reduce error and noise, the difference between the receiver and transmitter is used. Bit error rate (BER) and the response to different attacks is detailed in [2].

III. Results

Fig. 3 shows the test setup with the temperature sensor, transmitter, and receiver. The cavity of the fabricated temperature sensor is kept open to ensure the integrated circuit

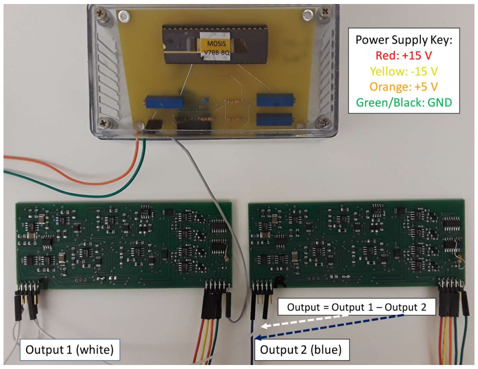

Fig. 3. Experimental setup of temperature sensor, transmitter, and receiver system.

is at the same temperature as the environment. The TS-CSK transmitter system with decision board and TS-CSK receiver system with decision board are also shown. A power supply was for biasing the PCB boards and the temperature sensor. The encrypted signal of the transmitter and decrypted signal of the receiver were measured using an oscilloscope. The transmitter and receiver were implemented in simulation using Matlab Simulink and experimentally on PCB boards using discrete multipliers and opamps (Fig. 3).

The temperature to time sensor was fabricated in a standard 130 nm process. V_{PTAT} was experimentally measured for temperatures from 25°C to 150 °C. The measurements showed a linear change from 47 mV to 62 mV for V_{PTAT} over this temperature range (Fig. 4). Though the voltage range seems small (in mV range), this voltage amplified deferentially and converted to current improved the system sensitivity. The voltage output was measured twice, once while heating the chip and then when cooling the chip. The experimental measurement for a sinusoidal voltage applied to the positive input (Input+) and a DC voltage applied to the negative input (Input-) of the comparator is shown in Fig. 5. The comparator's experimentally exhibits rail-to-rail voltage change as Input+ and Input- change. The switching voltage was set to 0.1 V, a relatively low voltage, to provide a larger window of comparison. The capacitor value was minimized to reduce the area occupied and allow for a fast charging and discharging rate. A larger comparison window improves system accuracy. Four different chips were tested with similar results.

For the temperature to time measurements, the system was set up as shown in Fig. 6. The temperature chamber sets the ambient temperature, and the pulse width of the output signal was measured. The temperature was changed for 25 °C to 75 °C in 2.5 °C increments. The chip was then cooled down to 25 °C again. The pulse width was recorded for both increasing and decreasing the temperature. The experimental results for this chamber test is shown in Fig. 7. In this figure, the temperature is linear up to 60°C, after which the slope changes. Since the PTAT generation is fairly linear, the non-linearity after 60° is due to the voltage to time conversion.

For the complete system, the output of the temperature sen-

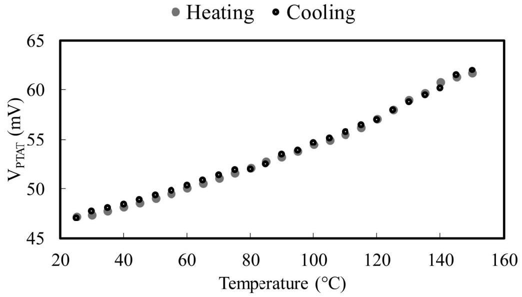

Fig. 4. Output voltage as a function of temperature for 25 °C to 150 °C.

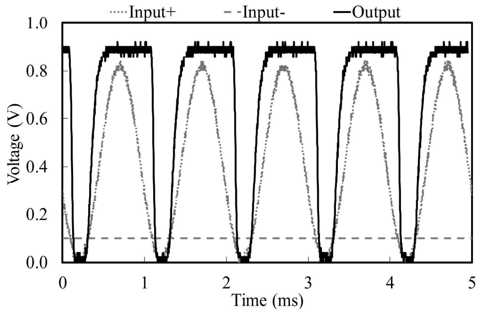

Fig. 5. Experimental verification of the comparator.

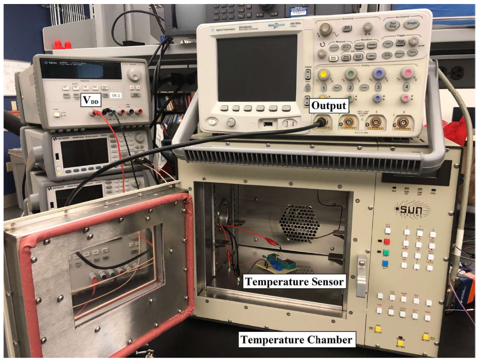

Fig. 6. Experimental setup for temperature to time sensor using a temperature chamber.

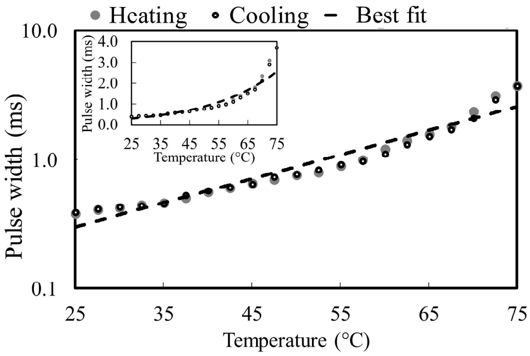

Fig. 7. Experimental measurements of temperature to time sensor using a temperature chamber.

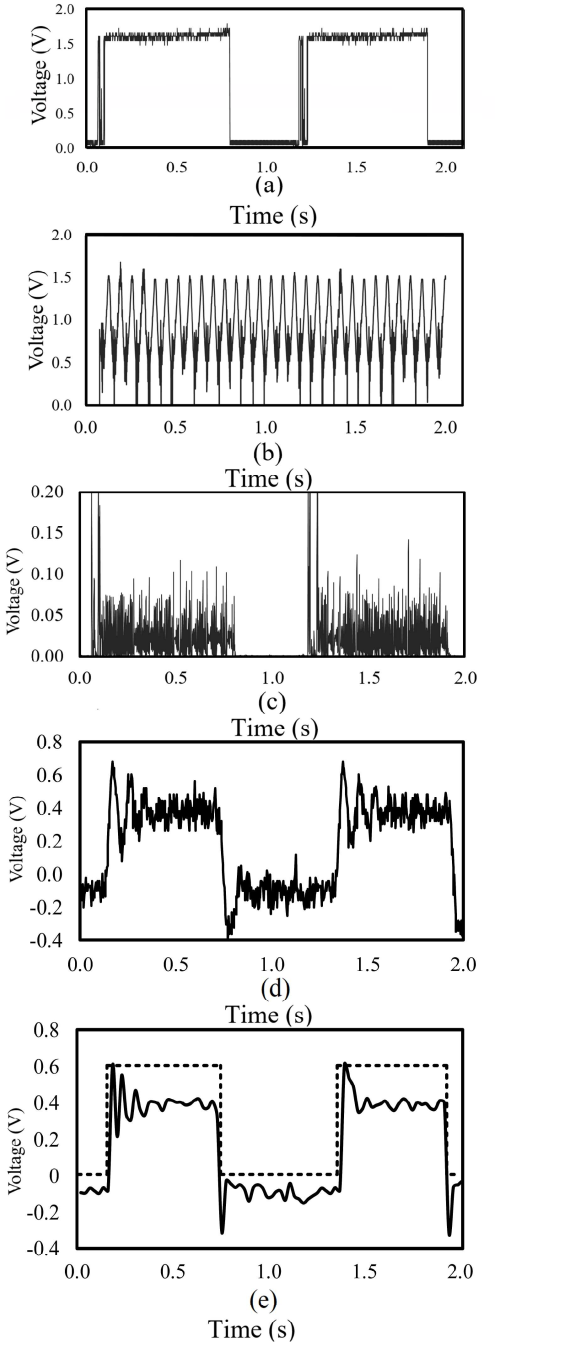

Fig. 8. Experimental measurements. (a) V_{PTAT} temperature measurement at 50°C, that is sent to transmitter to be encoded. (b) The encoded temperature at the transmitter output. (c) The simulated decoded temperature signal using a Matlab Simulink receiver model. (d) The experimental decoded temperature signal in receiver. (e) Experimental decoded temperature signal with local peak detection to remove noise (solid line) and thresholding (dashed line).

sor was applied to the transmitter as the message signal. The experimental message signal that was fed to the transmitter board is shown in Fig. 8 (a). One state of the transmitter and receiver are coupled to provide synchronization. The transmitter sends the ciphered signal to the receiver. The experimental transmitter data, which is the coded temperature sensor signal, is shown in Fig. 8 (b). It must be noted that this signal is also not in phase with the input signal. The receiver then decodes the encrypted message. Fig. 8 (c) shows the decoded temperature data using Matlab Simulink, and Fig. 8 (d) shows the experimental decoded temperature data. As can be seen in this figure, the noisy signal makes it difficult to discern the actual pulses. However, by using local mean calculation and/or peak detection, the temperature pulse can be extracted (Fig. 8 (e)), these smoothing techniques are implemented using default Matlab toolboxes. For integrated circuit implementation, a comparator can be used to recover the decoded digital temperature sensor signal by comparing it to a pre-determined threshold voltage.

IV. Conclusion

In this paper, we have demonstrated an encrypted temperature sensor. The temperature sensor is implemented in a 130 nm process and the encryption/decryption system is implemented on a PCB board. Experimental results of the temperature system shows good linearity of the output PTAT voltage, while the voltage to pulse width conversion introduced some non-linearities. The encryption is based on the Lorenz chaotic system and is relatively simple to implement in analog circuits. To the best of our knowledge, this is the first time a sensor has been integrated with chaotic analog encryption. The system has great advantages over more common digital encryption methods including lower power and size. The power consumption of the overall system is 0.85 W which is smaller than micro-controller implementation of security systems ranging typically from 2 W to 5 W. In the future, the encoding system will be integrated directly with the temperature sensor, and a wireless module included to provide a truly integrated encrypted wireless sensing system.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1816703 and by the U.S. Department of Energy, Office of Science, Office of Basic Energy Sciences under Award Number DE-SC0017414.

References

[1] A. Hedayatipour, M. A. Haque, and N. McFarlane, *"Quasi-Digital Output Low Power CMOS Temperature Sensor,"* IEEE International Midwest Symposium on Circuits and Systems, Windsor, ON, Canada, pp. 992 - 995, Aug 2018.

[2] D. Brown, A. Hedayatipour, M. Majumder, G. Rose, N. McFarlane, and D. Materassi, *"A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry,"* IET Computers & Digital Techniques, vol. 12, no. 6, pp. 297-305, Nov 2018.

[3] S. Green, I. Cicek, and C. K. Koc, *"Continuous-time computational aspects of cyber-physical security,"* IEEE Fault Diagnosis and Tolerance in Cryptography Workshop, pp. 59-62, 2016.

[4] M. Delgado-Restituto and A. Rodriguez-Vazquez, *"A CMOS analog chaotic oscillator for signal encryption,"* Solid-State Circuits, vol. 1, pp. 110-113, 1993.

[5] M. Delgado-Restituto, A. Rodriguez-Vazquez, and M. Linan, *"A modulator/demodulator CMOS IC for chaotic encryption of audio,"* Solid-State Circuits Conference, pp. 170-173, 1995.

[6] D. Materassi and M. Basso, *"Time scaling of chaotic systems: Application to secure communications,"* International Journal of Bifurcation and Chaos, vol.2, pp. 567-575, 2008.