2021 43rd Annual International Conference of the
IEEE Engineering in Medicine & Biology Society (EMBC)
Oct 31 - Nov 4, 2021. Virtual Conference

A Wireless Time-Scaling Chaotic Shift Keying Encryption System For Biosensing Systems

Kendra Anderson[1], Ava Hedayatipour[2], and Nicole McFarlane[1]

Abstract— **This work presents a wireless time-scaling chaotic shift keying encryption system that can be used in wireless body area network applications. In wireless sensor nodes, the communication protocol being used provides some security measures and is implemented in software. However, no additional security measures are usually implemented. This paper demonstrates a discrete level real time encryption system using analog circuitry on a printed circuit board. The encryption system uses op amps, multipliers and resistors to implement the encryption. To implement wireless capabilities, commercial wireless microcontrollers using Bluetooth Low Energy were added, and a custom Bluetooth Low Energy profile was created to stream the analog encrypted signal.**

Clinical relevance— **This work demonstrates an encryption system for wireless sensor devices for improved protection of private health information.**

I. Introduction

Wireless body area networks (WBAN) consist of a collection of sensor nodes used to monitor physiological conditions of the human body. The core components of a sensor node are sensors, a microcontroller, and a transceiver. Security in these nodes prove critical, since an attack could have devastating consequences. At best, a hacker could access sensitive and confidential healthcare information; at worst, a hacker could manipulate the technology in a way that is fatal. The communication protocol that a sensor node uses will provide some measures of security. However, this is usually the only method of security that is incorporated, making the sensor node only as secure as its communication technique.

There are numerous reports of potential cyberattacks in different wearable sensors and even IoT devices in general. For example, there was a recall on insulin pumps for potential attack risks by the US Federal Food and Drug Administration [1], and various different Medtronic devices were deomonstrated to be vulnerable to hackers recovering sensitive healthcare information during the Black Hat Conferences [2]. An exploit in the Zigbee protocol was shown to have potentially disastrous effects, and how it could be used to control a wide range of IoT devices was shown in [3]. A vulnerability in Bluetooth Low Energy was discovered by Ohio State University researchers that made devices vulnerable to a fingerprinting attack and eavesdropping [4].

This material is based upon work supported by the National Science Foundation under Grant No. 1816703.

K. Anderson and N. McFarlane are with the Department of Electrical and Computer Science, The University of Tennessee, Knoxville, TN 37996.

A. Hedaytipour was with the Department of Electrical Engineering and Computer Science, University of Tennessee, she is now with the Department of Electrical Engineering, California State University, Long Beach, CA, 90840.

Chaos-based encryption is an appealing method for secure communications because it masks digital data to make it appear as a noise-like signal. In order to decipher the message, the exact same complex chaotic system would need to be implemented to perform chaotic synchronization. Even if there was an attempt to recreate the chaotic system, variations in offsets, mismatch, process, voltage, and temperature (PVT), etc., would most likely result in unsuccessful synchronization of chaotic systems and therefore failed recovery of information.

The security provided in communication protocols use software algorithms such as Advanced Encryption Standard, i.e. AES, to protect information, and are usually implemented in the MAC layer or above. In [10], a chaotic system is used to generate encryption keys for implantable medical devices. Many FPGA implementations of chaotic based encryption methods have been presented in literature, such as in [11]. This work presents a hardware chaotic based encryption method that can be placed directly after a sensor to provide security on the physical layer. Work has already been done to integrate this encryption method to be able to add it to the same chip as a sensor [5]. This work demonstrates, as a proof-of-concept, the whole wireless encryption system with a simulated sensor input using discrete off the shelf components.

The paper is organized as follows. Section II gives an overview of the encryption theory. Section III describes the system implementation. Section IV gives the results and finally section V summarizes the conclusion.

II. Theory

The encryption method presented is based on the Lorenz mathematical function,

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

where only certain values of β, ρ, and σ that are real and positive can be used to create a chaotic system. The values are chosen to create a bounded system (i.e. the trajectory's are bounded). Chaotic shift keying (CSK) is an encryption methodology that is based on the Lorenz function. It uses two properties of chaos for encryption and decryption: sensitivity to initial conditions and chaotic synchronization. In the Lorenz function, a small change in initial conditions results in a change in trajectory, which is the basis for encryption. Chaotic synchronization is where two chaotic signals can synchronize and their trajectories can be matched when

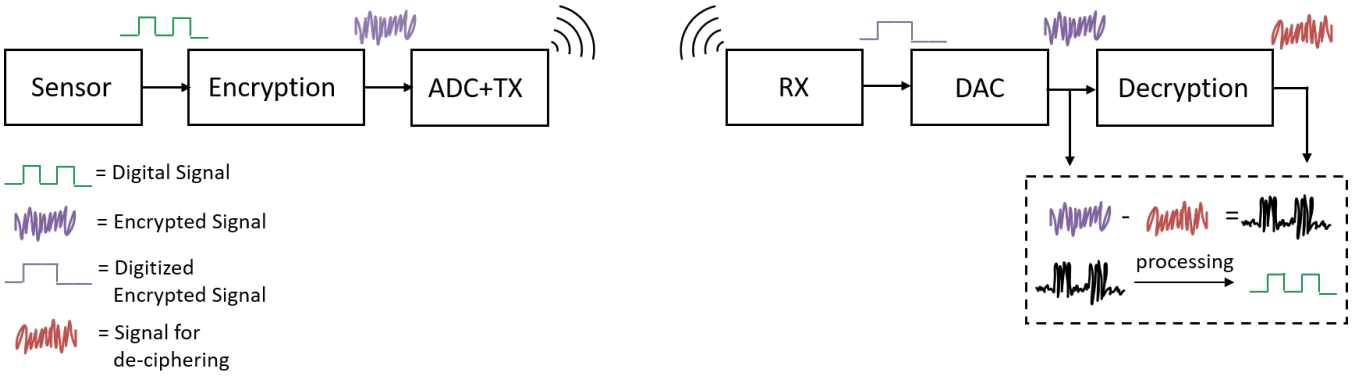


Fig. 1: System overview: digitized sensor signal is encrypted via analog circuits, digitized, and transmitted wirelessly to a receiver where it is decrypted.

they share a common state, despite having different initial conditions. This will only occur if the two systems have the same system parameters (β, ρ, and σ). This property is used to decrypt the signal.

One vulnerability to this encryption method is the return map attack, which monitors local maximum and minimum points of the transmitter's state to distinguish time-varying characteristics of the system. To gain immunity from this, a function, λ(x,m), is added, making the system equations [6],

$$\begin{aligned} \dot{x}_1 &= \sigma(\lambda(x,m)x_2 - \lambda(x,m)x_1) \\ \dot{x}_2 &= \lambda(x,m)(\beta - x_3)x_1 - \lambda(x,m)x_2 \\ \dot{x}_3 &= \lambda(x,m)x_1x_2 - \lambda(x,m)\rho x_3 \end{aligned} \tag{2}$$

$$\begin{aligned} \dot{z}_1 &= \sigma(\lambda(z,0)z_2 - \lambda(z,0)z_1) \\ \dot{z}_2 &= \lambda(z,0)(\beta - z_3)x_1 - \lambda(z,0)z_2 \\ \dot{z}_3 &= \lambda(z,0)x_1z_2 - \lambda(z,0)\rho z_3 \end{aligned} \tag{3}$$

and,

$$\lambda(x,m) = \left\{ \begin{array}{cccc} \lambda_m & if & d_x = 0 \\ \lambda_{1-m} & if & d_x = 1 \end{array} \right\} \tag{4}$$

where the transmitter and receiver states are x_1, x_2, x_3 and z_1, z_2, z_3. Due to the similarity in the transmitter and receiver system equations, they are implemented by identical systems. The constant β is a modulation signal, and m is the message signal. The encrypted signal, which is also the shared state, is the transmitted state x_1. d_x is the decision engine function, which uses a series of logic gates to perform a λ selection and is a function of the message signal, time, and the states of the system. More details are reported in [6].

III. System Implementation

Fig. 1 shows a block diagram of the entire cipher system. It starts off with a low frequency, digital signal that is similar to what a sensor would output. This type of sensor output can be found in quasi-digital sensors such as temperature [7], pH [8], and impedance sensors [9] where the analog sensor measurement, in voltage or current, is converted to a frequency modulated digital output. The signal is input to the encryption module (Fig. 2), which masks the signal and turns

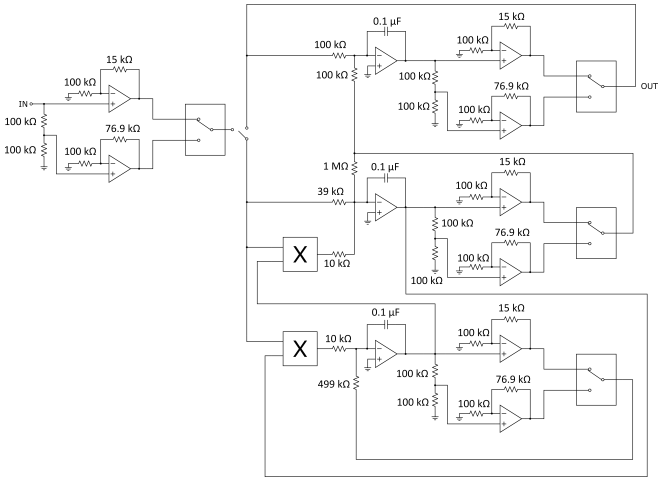


Fig. 2: Encryption and decryption circuit schematics.

BLE Custom Profile: CipherService	
GATT Primary Service Declaration	
GATT Characteristic Declaration	
CipherValue:	Contains 20-byte array of sampled data from ADC buffer
Client Characteristic Configuration:	Read and notify properties
GATT Characteristic Declaration	
StreamEN:	Write "01" to turn on streaming and "00" to turn off

Fig. 3: BLE custom profile for streaming.

it into an analog signal, where the digital highs and lows are no longer detectable. After it is sent to the transmitter, a built-in 12-bit ADC samples the data continuously. A custom BLE profile was implemented for streaming this signal, shown in Fig. 3. The profile implements only one custom service, called CipherService. The service contains two characteristics: CipherValue and StreamEN. CipherValue holds the value of the sampled data in a 20-byte array, which is the largest size array that can be sent in one notification. This value has read and notify properties. StreamEN has read and write properties, and is used to enable or disable streaming. When a "01" is written to it, it starts the ADC

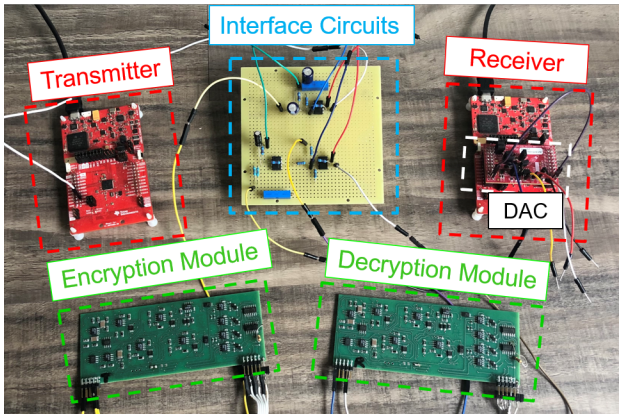


Fig. 4: Wireless encryption system implementation.

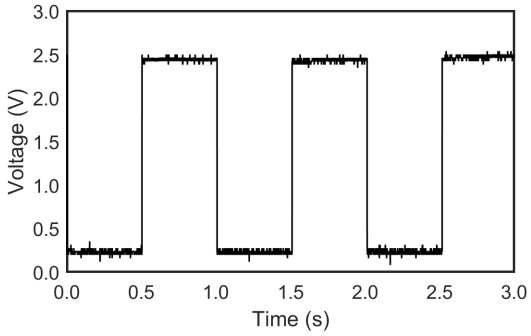
buffer to continuously sample data. When the ADC buffer is full, a notification is sent to update the receiver. To disable this cycle, streaming is turned off by setting StreamEN to ”00”. In order to stream the data continuously and at the correct rate, the minimum connection interval for BLE is used, at 7.5 ms.

On the receiver side, the Bluetooth data packet is collected and processed. After processing the notification signal and extracting the sent data, called the payload, the receiver communicates the value to an external DAC through SPI to convert it back to an analog signal. The encrypted analog signal goes through the cipher again to get another chaotic signal for decryption (chaotic synchronization), and the two signals are subtracted in circuitry to recover the original signal information.

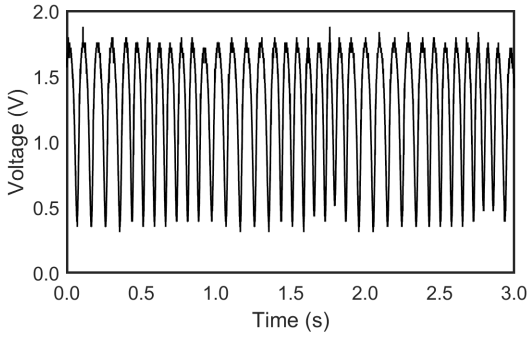
Interface circuits were added before the ADC and after the DAC to enable correct operation. They were used as buffer stages to prevent loading. On the transmitter side, they also added a DC offset to shift the encrypted signal’s voltage range for the ADC to sample it. On the receiver side, this offset was removed and a low-pass filter was added to smooth out the high-frequency components introduced from the DAC. The circuit to subtract the two signals is in a difference op amp configuration with unity gain. As a note, the ADC and DAC are only required due to the choice of Bluetooth LE which can only transmit digital signals.

IV. Results

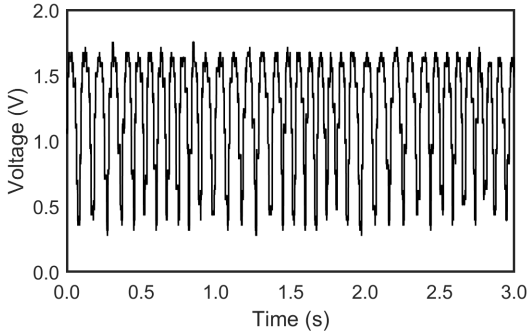
Fig. 4 shows the physical setup of the system. The transceiver evaluation boards are the LAUNCHXL-CC26X2R1 boards from TI. The encryption and decryption modules use the LT1057 operational amplifiers, AD633 multipliers, and DG419 switches. The resistor values were chosen to set the system parameters of β, σ, and ρ. The LM741 operational amplifiers are used in the interface circuitry. Fig. 5 show the results of the system. Fig. 5a is the digital information signal used at the input. This input signal is simulated based on actual measured signals from quasi-digital sensors. The signal that is transmitted is shown in Fig. 5b, and after the signal processing that is described in the



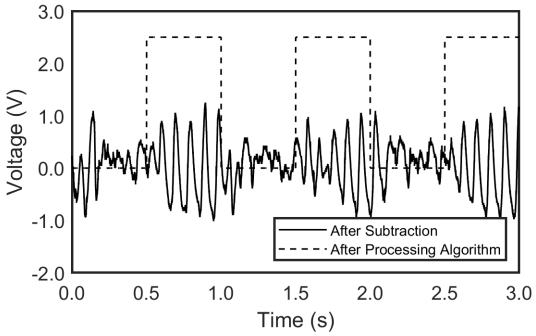
(a) The simulated digital input signal.



(b) The transmitted encrypted signal.



(c) The received encrypted signal after being sampled and transmitted.



(d) The decrypted signal and the digital output the signal produces after post-processing.

Fig. 5: Experimental Results.

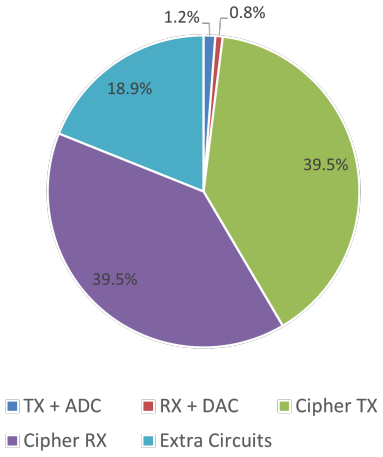


Fig. 6: Power consumption of each module.

system implementation section, the received signal is shown in Fig. 5c. The decrypted signal is shown in Fig. 5d, along with the digital signal the decrypted signal will produce after going through a processing algorithm.

The system operates on a dual supply rail of $\pm$ 12 V and a 5 V supply rail. Total power consumption for transmitting and receiving is 2.8 W, and a breakdown of the power can be shown in Fig. 6. The largest contributors to power consumption are the encryption and decryption modules, consuming 79% of the power, or 1.1 W for each board. The second largest contributor is the interfacing circuits, which consume 528 mW or about 19% of the overall power. The transmitter and ADC consume 34 mW, and the receiver and the DAC consume 21 mW; each contributor is close to 1% of the overall power.

Each module in the system occupies the following area: the encryption/decryption boards occupy 131 $\times$ 56 mm^2, the transceiver evaluation boards occupy 96 $\times$ 59 mm^2, the DAC occupies 51 $\times$ 31 mm^2, and the interface circuits occupy 50 $\times$ 50 mm^2. Since the DAC sits directly on top of the receiver, it does not add any additional area to the system. The effective area for the system (in a 2D configuration) is approximately 285 cm^2. However, a stacked configuration with each module would allow for a smaller area, making the effective area of the system equal to 73.4 cm^2. Further reduction in area could be obtained through implementing the interface circuitry in SMD components on a PCB and making a custom PCB for the transceiver module instead of using an evaluation board.

V. Conclusion

This work demonstrates a wireless time-scaling chaotic shift keying encryption system. The full system is implemented on a PCB using discrete opamps, multipliers, and passive components. Commercially available transceivers, that use Bluetooth Low Energy, are added to the encryption system to enable wireless capabilities. For decryption, chaotic synchronization is implemented through the wireless shared state, and a Bluetooth Low Energy profile was created to stream this shared state. Even though power consumption was very high, this work shows a proof of concept that an extra layer of security can be added at the hardware level to protect wireless sensor nodes. When implemented in an integrated circuit format, the sensor is directly connected to the encryption module. This prevents an attacker from physically determining the parameters of the encryption circuit. The encryption system has already been demonstrated in a custom chip [5], and future work will integrate a custom transceiver for a fully integrated wireless encrypted sensor system.

Acknowledgment

The authors thank D. Brown and D. Materassi for helpful discussions.

References

[1] US Food and Drug administration FDA, emph"Certain medtronic MiniMed insulin pumps have potential cybersecurity risks: FDA safety communication," FDA, White Oak, MD, USA, Tech. Rep., Jun. 2019. Accessed: May 2020. [Online]. Available: https://www.fda.gov/medicaldevices/safety-communications/certain-medtronicminimed-insulinpumps-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: May 2020. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01

[3] E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, *"IoT Goes Nuclear: Creating a ZigBee Chain Reaction,"* IEEE Symposium on Security and Privacy, 2017, pp. 195-212.

[4] J. Loughran, *"Bluetooth vulnerability leaves smart home devices vulnerable to hackers,"* Engineering and Technology. Nov. 2019. Accessed: May 2020. [Online]. Available: https://eandt.theiet.org/content/articles/2019/11/bluetooth-low-energy-vulnerability-lets-hackers-eavesdrop-on-smart-home-devices/

[5] A. Hedayatipour and N. McFarlane, *"An Encryption Architecture Suitable for on Chip Integration With Sensors,"* in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 395-404, June 2021.

[6] 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.

[7] A. Hedayatipour, K. Anderson, S. Aslanzadeh, D. Brown, D. Materassi and N. McFarlane, *"A Temperature Sensing System With Encrypted Readout Using Analog Circuits,"* IEEE International Midwest Symposium on Circuits and Systems, Dallas TX, 4 pages, Aug 2019.

[8] S. Aslanzadeh, M. Smalley, A. Hedayatipour and N. McFarlane, *"A Portable CMOS Based pH Sensor,"* IEEE International Midwest Symposium on Circuits and Systems, Springfield, MA, USA, pp. 525-528, Aug 2020.

[9] 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,"* in IEEE Transactions on Biomedical Circuits and Systems, vol. 14, no. 5, pp. 1108-1121, Oct. 2020.

[10] T. Belkhouja, A. Mohamed, A. K. Al-Ali, X. Du and M. Guizani, *"Light-weight encryption of wireless communication for implantable medical devices using henon chaotic system (invited paper),"* International Conference on Wireless Networks and Mobile Communications, Rabat, Morocco, pp. 1-6, Nov 2017.

[11] M. F. Tolba, W. S. Sayed, A. G. Radwan, S. K. Abd-El-Hafiz and A. M. Soliman, *"Hardware Speech Encryption Using a Chaotic Generator, Dynamic Shift and Bit Permutation,"* International Conference on Microelectronics, Sousse, Tunisia, pp. 100-103, Dec 2018.