Attacks on Continuous Chaos Communication and Remedies for Resource Limited Devices

Rahul Vishwakarma
Computer Eng. & Computer Sci.
California State Uni. Long Beach
Long Beach, CA, USA
rahuldeo.vishwakarma01@student.csulb.edu

Ravi Monani
Electrical Engineering
California State Uni. Long Beach
Long Beach, CA, USA
ravi.monani01@student.csulb.edu

Amin Rezaei
Computer Eng. & Computer Sci.
California State Uni. Long Beach
Long Beach, CA, USA
amin.rezaei@csulb.edu

Hossein Sayadi
Computer Eng. & Computer Sci.
California State Uni. Long Beach
Long Beach, CA, USA
hossein.sayadi@csulb.edu

Mehrdad Aliasgari
Computer Eng. & Computer Sci.
California State Uni. Long Beach
Long Beach, CA, USA
mehdad.aliasgari@csulb.edu

Ava Hedayatipour
Electrical Engineering
California State Uni. Long Beach
Long Beach, CA, USA
ava.hedayatipour@csulb.edu

2023 24th International Symposium on Quality Electronic Design (ISQED) | 979-8-3503-3475-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISQED57927.2023.10129355

***Abstract*—The Global Wearable market is anticipated to rise at a considerable rate in the next coming years and communication is a fundamental block in any wearable device. In communication, encryption methods are being used with the aid of microcontrollers or software implementations, which are power-consuming and incorporate complex hardware implementation. Internet of Things (IoT) devices are considered as resource-constrained devices that are expected to operate with low computational power and resource utilization criteria. At the same time, recent research has shown that IoT devices are highly vulnerable to emerging security threats, which elevates the need for low-power and small-size hardware-based security countermeasures. Chaotic encryption is a method of data encryption that utilizes chaotic systems and non-linear dynamics to generate secure encryption keys. It aims to provide high-level security by creating encryption keys that are sensitive to initial conditions and difficult to predict, making it challenging for unauthorized parties to intercept and decode encrypted data. Since the discovery of chaotic equations, there have been various encryption applications associated with them. In this paper, we comprehensively analyze the physical and encryption attacks on continuous chaotic systems in resource-constrained devices and their potential remedies. To this aim, we introduce different categories of attacks of chaotic encryption. Our experiments focus on chaotic equations implemented using Chua's equation and leverages circuit architectures and provide simulations proof of remedies for different attacks. These remedies are provided to block the attackers from stealing users' information (e.g., a pulse message) with negligible cost to the power and area of the design.**

***Index Terms*—CMOS, Hardware security, Chua's Chaotic Equations, Chaos Implantation, IoT**

I. Introduction

With advancements in microelectronic circuit technology and the miniaturization of sensors, the possibility of developing smaller and more reliable Implantable/Wearable Devices (IWDs) is progressive. The Integrated Circuit (IC) design companies have broadened their portfolios to be well composed of these IWDs. These devices are designed to accomplish designated tasks such as monitoring the oxygen level in the blood (Pulse Oximetry test), the glucose level in the blood, the heartbeat, body temperature, hydration level, etc. The impressive improvement in reliability and efficiency of IWDs such as smartwatches, fitness bands, and body patches has brought the medical industry and the IWD manufacturers together to obtain approval as a medical device from the US Food and Drug Administration (FDA). [1] The IWDs provide the real-time data accumulated from the on-chip sensors and enable the utilization of those. These data are collected remotely and can be managed through smartphones. The health organization accesses the data remotely to monitor the patients and keep that process cost-effective. [2] Thus, the accessibility of the features and health data provided by these IWDs has made them functional for many people. [3]

Wearable Technology Market (WTM) is expected to grow to USD 265.4 billion in 2026 from USD 116.2 billion in 2021 at a rate of 18.0 % CAGR (Compound Annual Growth Rate)1 [4]. Wearable devices develop a large consumer base when they are equipped with capabilities such as adaptability, reliability, portability, proper form factor, fault resilience, etc. The devices with these capabilities in the industry top the list of smart wearable devices [5]–[8]. These devices generate a variety of vast and potentially useful data that can be collected and analyzed by wearable device manufacturers [3]. Due to the fact that these devices function with wireless networks like NFC, Zigbee, and Bluetooth, they are vulnerable to cyberattacks.

The informative data collected from devices cannot be classified as secure without certain security regulations or encryption algorithms for the welfare of the consumer. Synchronization of chaos is the foundation for utilizing chaos in communications. The raw and unencrypted data is transformed into a scrambled signal by the chaotic transmitter prior to being transmitted via a public channel, which can either be wireless, like in the case of sensor networks in wearable devices or IoT, or wired, like in power grids. The traditional encryption algorithms for communication are symmetric and asymmetric encryption. In symmetric encryption, just one key is involved,

TABLE I: Cryptographic Algorithms

Algorithm	Purpose
Advanced Encryption Standard (AES)	Confidentiality
Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptography (ECC)	Digital Signatures Key Transport
Diffie-Hellman (DH)	Key Agreement
SHA-1 and SHA-256	Integrality

a private key that needs to be sent separately with the highest level of security. In the latter case, a pair of encryption keys are involved, and the receiver has a private key to decrypt the message.

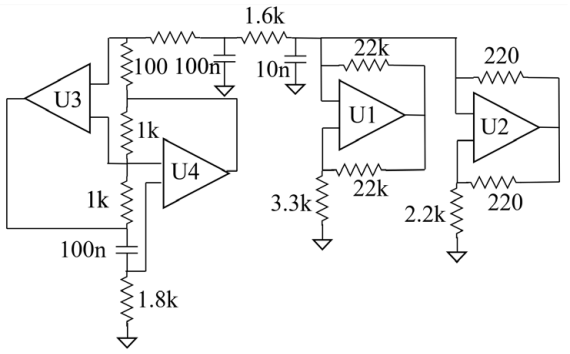
The remainder of this paper is organized as follows. First, Chua's model is introduced in Section II. Some of the known security attacks that IWDs can face are analyzed and explained in Sections III and IV. The experimental and simulation results follow the attack explanations in Section III for physical attacks and Section IV for encryption attacks, and the paper concludes with Section V.

II. Encryption Using Chua's Circuit

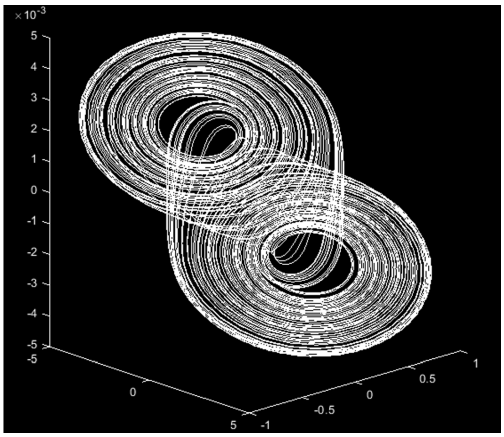
The discovery of chaos is considered a major breakthrough when it comes to ciphering. There have been multiple attempts to use chaos in the fields of encryption [9]–[14]. However, the objective still remains challenging when we aim to bring chaos to the CMOS level. In [15] different modes of chaotic equations have been compared for various performance metrics, and in [16] an encryption architecture suitable for communication of on-chip sensors using different chaotic equations is implemented.

The algorithms listed in Table I can be used depending on the target Internet of Things (IoT) application, as they vary in resources such as memory and power. The symmetric encryption administers the shared private key between sender and receiver, whereas in the asymmetric encryption, the sender provides the public information and the receiver decrypts that with the private information [17]. The usually used symmetric encryption is the Advanced Encryption Standard (AES) block cipher [18]. However, AES is not considered a guaranteed reliable communication [19]. Asymmetric encryption was introduced by Diffie and Hellman and is also called public-key cryptography [20]. Famous asymmetric encryptions are Rivest-Shamir-Adelman (RSA) and the Diffie-Hellman (DH) asymmetric key agreement algorithm [21]. The downside of these algorithms is that they require more hardware utilization due to their computational requirements and factorization complexity [22].

There are determined researches claiming that the traditional encryption can be broken with way less textitqubits compared to the existing encryption [23]. The thorough analysis of post-quantum era and the block-chain cryptography to quantum computing attacks has been done in literature [24]. There are no post-quantum block-chain algorithms available at present that can provide low-power implementation, low computational complexity, and lower execution time. These are critical characteristics for any resource-constrained devices



(a)



(b)

Fig. 1: (a) Chua's circuit (n) MATLAB simulation results of attractor for Chua's circuit

like IWDs [25]. Therefore, methods of encryption other than symmetric and asymmetric security are gaining in importance and quickly becoming necessary. Starting to implement chaos on the hardware, this paper focuses on implementing Chua's circuit and its robustness against various attacks.

Chua's circuit is a non-repeating chaotic system that requires a nonlinear element, a locally active resistor, and three or more energy storage elements [26]. In contrast to other common chaotic equations, like the Lorenz equations, Chua's circuit is more sensitive to its initial conditions. By varying the value of one of the parameters from 1.0 to 1.1, the trajectories of x(t) are extremely different. Most importantly, the Chua's circuit is "one of the simplest robust experimental proof of chaos and can be easily implemented in different ways" [26]. As demonstrated by Chua's Fig. 1, the butterfly effect and double scroll attractor are shown, portraying the chaotic behavior and three non-linear ordinary differential equations. Chua's circuit, with its three unstable equilibrium points, exhibits more chaos than prior systems.

With the traditional encryption algorithms, the IWDs achieve the designated tasks; however, they are not considered reliable when it comes to the security of the personal data generated by the device or its sensor, and they suffer so many security breaches. The process of making IWDs secure and

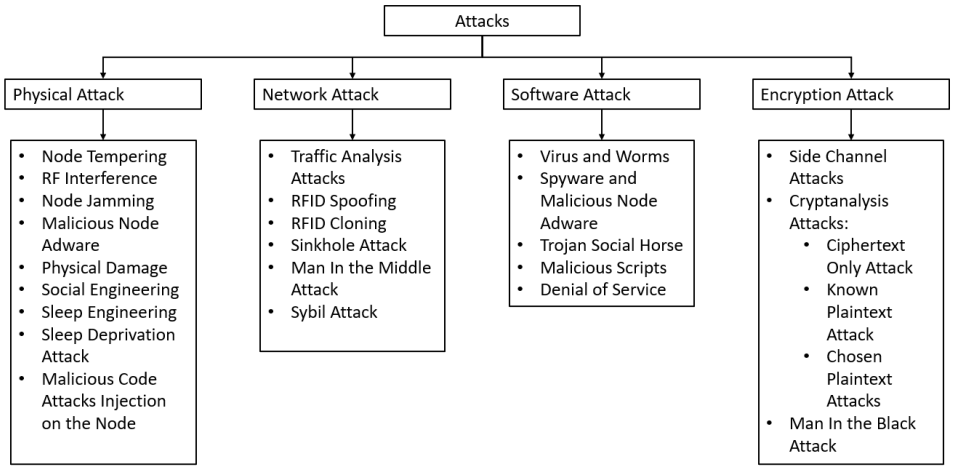


Fig. 2: Security attacks [27]

reliable is complex, as they require security to be implemented at each layer, as Fig. 2 shows potential risks. Some of the security breach examples force the IWDs industry to advance research in the field of cryptography. These include a recent data leak that exposed the data of Fitbit and Apple's over 61 million users from around the world [28]. For IWDs, vulnerable attacks are targeted on cardiac implants [29], [30]; implantable insulin delivery pumps [31], [32]; and neurological implants [33]. Thus, this encourages research toward improving the traditional encryption algorithms in terms of hardware utilization as well as making them a secure and robust encryption architecture.

In this paper, we will be focusing on physical attacks and encryption attacks. As our device is not dependent on RFID, network attacks will not be discussed in this paper. Also, due to the hardware encryption of the design, no data can be extracted from the encrypted message in the public channel. The attacker needs the exact copy of the circuit implemented to be able to decrypt the data. We will also not discuss the software attacks in which the attacker performs the attack by using viruses, worms, spyware, adware, etc. to steal data or deny the services which are not applicable to our hardware-oriented design.

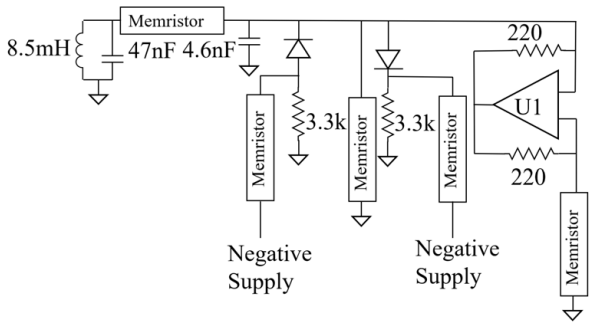
III. Physical Attacks on Wireless Devices

Physical attacks are concentrated on hardware devices in the system.

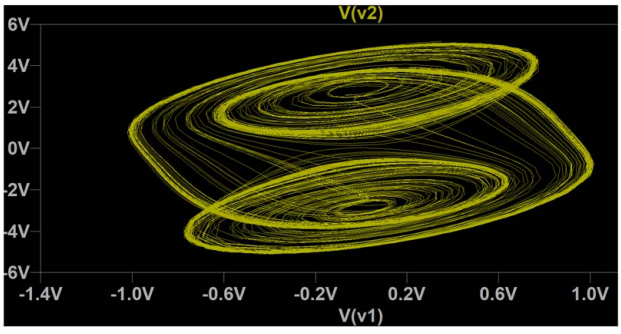
A. Node Tampering

The adversary can perform the attack on the IoT system by damaging or tampering with some nodes. In this attack, the attacker physically alters the compromised node and can obtain sensitive information such as the encryption key. To tamper with nodes in our design, the attackers need access to the physical location of the transmitter and receiver circuits. They also need to extract the schematics of the transmitter and receiver to extract the node.

Assuming access to the schematic and physical nodes in an untrusted foundry, we resolve this issue by replacing the resistors in the circuit with memristors. A memristor [34] is a two-terminal electrical component relating electric charge to magnetic flux linkage. It can be viewed as a form of non-volatile memory that is based on resistance switching, which



(a)



(b)

Fig. 3: (a) Memristor-based Chua's circuit (b) Double scroll attractor for memristor U3 in Chua's chaotic circuit with memristor values R_{on}=0.8K R_{off}=1.65K R_{init}=1.65K D=70N uv=10F p=1

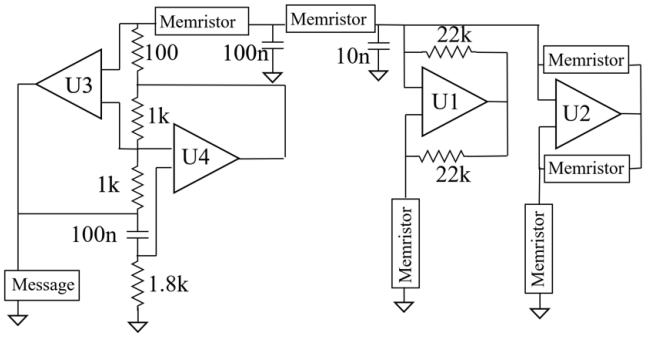


Fig. 4: The transmitter and receiver design of the communication system With this scheme, the message is encrypted by the sender, moved through a public channel, and decrypted by the receiver

increases the flow of current in one direction and decreases the flow in the opposite direction. Here we use a logic locking mechanism [35]–[37] based on the use of memristors as the keys for securing the circuit design against untrusted foundries. A Chua's circuit implemented with memristors is shown in Fig. 3a. The chaotic behavior of our designed circuit is shown in Fig. 3b as a double scroll attractor by plotting I-V characteristics for memristor U3 in the circuit. The values of the other memristors are tuned in a range such that they satisfy the chaotic equations and exhibit chaotic behavior.

Most of the researchers have focused on designing a system to reliably transmit information from the sender to the receiver by making improvements to the way the chaotic circuit is designed. Here, to have a transmitter and receiver scheme, we replace the resistors in Chua's design with memristors, as shown in Fig.4. Fig. 5 shows the simulation of chaotic communication using Chua's memristor-based circuit.

By using memristors, a reliable and secure chaotic transceiver that is resistant both to eavesdroppers and untrusted factories is achieved. In this case, even if the attacker has the schematic of the design, stored from the foundry, they will not have the value that the memristor is set on, hence unable to replicate the design. The approach is effective due to the large key space created by implementing memristors in the circuit, along with the logic locking.

When working with memristors, however, process variations of these devices should be taken into account. Due to the non-deterministic nature of the Nanoimprint Lithography (NIL) used to form the electrodes and crossbars, a significant amount of process variability exists in memristors [38]. The deposition and etching procedures involved in forming the thin oxide film [39], and via-etching through the dielectric also make memristors particularly prone to variations. The ensuing misalignment, size mismatch, and change in dopant concentration inside the dielectric, breaks, openings, and shorts have a negative impact on the behavior of the memristor device and consequently, our security synchronization [40].

The chaotic behavior, however, is not just bound by the strict values of the memristors. Driving eigenvalues of the

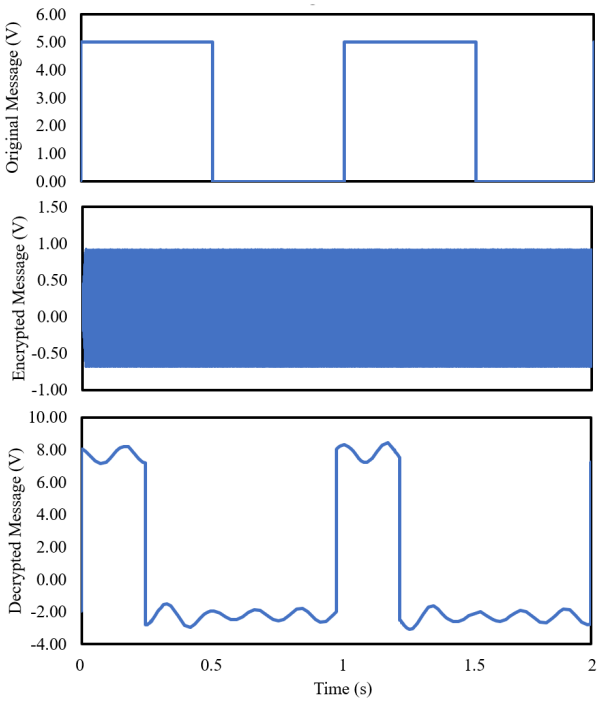


Fig. 5: Original, encrypted, and decrypted message for memristor-based Chua's chaotic circuit

Jacobian matrix for chaotic equations as shown in [41], chaotic behavior is seen for a range of values instead of a single value. Hence, despite small changes in memristor value due to process variation, this will not affect the overall chaotic behavior of our system.

B. RF Interference and Node Jamming

The attacker can perform a Denial-of-Service (DoS) attack by sending noise signals over radio frequency signals, or by using a jammer, the attacker can disturb the wireless communication. The jammer emits a radio signal and can be implemented using either a waveform generator that continuously sends a radio signal [42] or a normal wireless device that continuously sends out random bits to the channel. One method to address this issue is spatial retreats, in which jammed nodes try to evacuate jammed regions. Spatial retreats are suitable for mobile sensor networks. The spatial movement of our ciphered signal here is related to Chua's equation as follows:

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

To show that certain parameter choices lead to asymptotic stability rather than chaotic behavior, one can use a Lyapunov function as shown in [9]. Solving these functions proves that we can achieve chaos with a variety of σ and β parameters. In our design, changing these parameters results in a change

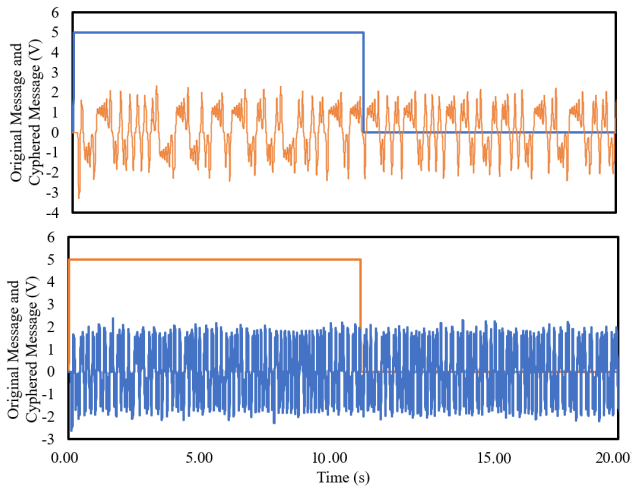


Fig. 6: Frequency change by changing coefficients in Chua's equation

in the cyphered signal frequency. In Fig. 6, the input is a 5-second pulse, and the high-frequency ciphered signal is also shown. The top picture shows a chaotic ciphered signal with a frequency of 20-100 times the frequency of the message. The σ and β parameters are then changed by adjusting the resistances in the circuit which increase the frequency of the chaotic ciphered signal to 80-400 times the frequency of the message as seen in the bottom picture Fig. 6. The deciphering of both signals is done successfully in this case, showing that in the event of jamming or RF interference by the attacker, a dynamic frequency change can be performed to move the ciphered signal in the public channel to a safe region.

C. Physical Damage

With the attacker having access to the physical locations of the transmitter and receiver, they can be physically damaged. However, since our transmitter and receiver are aimed to be used as ICs, they can be replaced for only a few dollars. When designing ICs the Non-Recurring Engineering (NRE) costs, such as teams, equipment resources, and materials other than the ICs, can add up to a couple of million dollars. However, ICs produced in the range of a million parts per wafer will divide the cost by the number of ICs produced per wafer. The costs of fabrication processes and NRE costs to build commercial ICs are therefore divided by millions; thus, the price of commercial ICs, produced in millions, does not go much higher than a few dollars.

D. Social Engineering

The attackers can physically interact with and manipulate users of an IoT system to obtain sensitive information to achieve their goals. This attack is not applicable to our design as the user is not aware of the schematic details of the transmitter and receiver. Unlike many software security systems, which rely on the user providing a password, in our hardware-based ciphering, the user does not have access to any sensitive information.

IV. Encryption Attacks on Wireless devices

These attacks depend on destroying encryption techniques and obtaining the private key.

A. Side Channel Attacks

The attacker takes advantage of the side-channel information emitted during the encryption process on devices. This information is distinct from both the plaintext and the ciphertext, and it can include details about the power consumption, operation time, fault frequencies, etc. With this information, the attacker can uncover the encryption key. In our design, one method for a side-channel attack is the attacker plugging into the power line and trying to extract the message pattern from the power line. Due to the isolation of the message from the power line, as shown in Fig. 7, no correlation is seen between the positive and negative power lines and the message. As another scenario, the side-channel attack can be mapped as a Return Map (RM) attack, discussed in the next subsection, which is a method of monitoring the transmitted state's local minimum and maximum points to distinguish changing system characteristics.

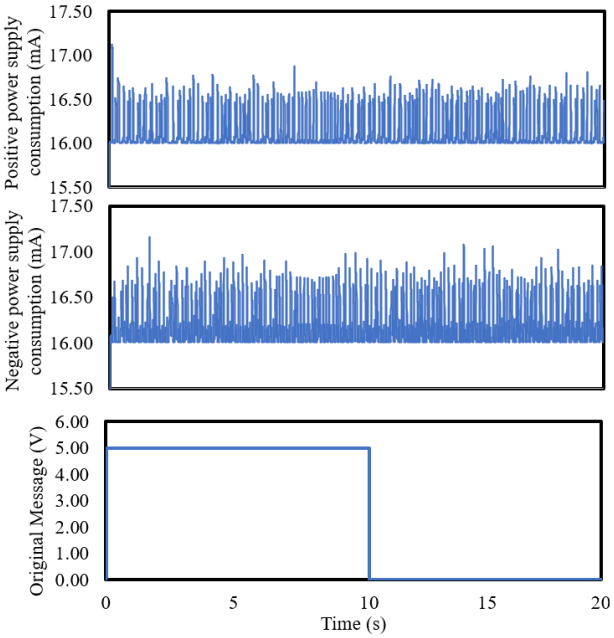


Fig. 7: Current consumption of the system shows no relevance compared to the message

B. Ciphertext-Only Attack

The RM is a type of Ciphertext-Only Attack (COA). RM attack can be defeated by performing the encryption modulation in a time-scaling factor. Chaotic Shift Keying (CSK) security vulnerabilities to RM attacks can be mitigated using a "time scaling function", $\lambda(x(t), m)$ to encrypt the plain-text message, $m(t)$. For any autonomous dynamical system,

$$\frac{d}{dt}x = f(x) \tag{2}$$

where the time scaling function is defined by,

$$\begin{aligned} \frac{dt}{d\tau} &= \lambda(x) \\ \tau(t_0) &= \tau_0 \\ 0 < \lambda(x) &< \infty \end{aligned} \tag{3}$$

It is clear that then,

$$\frac{d}{d\tau}x = \lambda(x)f(x) \tag{4}$$

From equation (3) τ, is strictly monotonic and increases with time, t [43]. From equation (4), the $\lambda(x)$ does not alter the phase space of x with respect to its attractors or equilibrium, and the only effect here is reaching a stable time [44]. The RM attack can be thwarted by encoding the message, $m(t)$, with the time scaling factor. This occurs due to the dependence on the variation of the state phase space.

We apply this time-scaling factor to a Chua's chaotic system by using a function, λ(x,m), to create a Time Scaling Chaotic Shift Keying (TS-CSK) encryption system. Here, x is the transmitter parameter, and z are the receiver parameters. The system equations then become,

$$\begin{aligned} \dot{x}_1 &= \sigma(x_2 - x_2 - f(x))\lambda(x,m) \\ \dot{z}_1 &= \sigma(z_2 - z_1 - f(x))\lambda(z,0) \\ \dot{x}_2 &= (x_1 - x_2 + x_3)\lambda(x,m) \\ \dot{z}_2 &= ((z_1 - z_2 + z_3)\lambda(z,0) \\ \dot{x}_3 &= (-\beta x_2)\lambda(x,m) \\ \dot{z}_3 &= (-\beta z_2)\lambda(z,0) \end{aligned} \tag{5}$$

where,

$$\lambda(x,m) = \left\{ \begin{array}{ccc} \lambda_m & if & \delta_x = 0 \\ \lambda_{1-m} & if & \delta_x = 1 \end{array} \right\} \tag{6}$$

Here $\delta(x)$ is the decision engine. To have stable security, $\delta(x)$ should be selected such that the switching event of $\lambda(x,m)$ cannot be decoded or extracted from the signal that is being communicated. There are several options for (x) that satisfy these conditions. [44], uses $\delta(x)$ such that,

$$\delta(x) = \left\{ \begin{array}{cc} 0 & \frac{\upsilon^T x}{h} iseven \\ 1 & \frac{\upsilon^T x}{h} isodd \end{array} \right\} \tag{7}$$

where the unitary selection vector υ is,

$$\Phi_{sync} = \left[\begin{array}{c} \upsilon_1 \\ \upsilon_2 \\ \upsilon_3 \end{array} \right] \tag{8}$$

However, the implementation of this decision engine gets increasingly difficult and expensive when the oscillation rate of Chua's system is higher. Based on these considerations and starting with the idea of simplifying to two regions, the initial decision engine was designed.

$$\delta(x) = \left\{ \begin{array}{cc} 0 & \upsilon^T x < 0 \\ 1 & \upsilon^T x \geq 0 \end{array} \right\} \tag{9}$$

The decision engine described by equation 7 is immune to return map attacks [44]. As the return map does not modify the underlying Chua's function in correlation with the orbital foci, TS-CSK encryption mitigates the RM attack. As long as x, for the TS-CSK system of equation (5), is chosen so that the underlying Chua's system is chaotic, then the system is protected from RM attacks. Return time-map attacks require the message, $m(t)$ to somewhat obscure the time difference between orbits. It must be noted that this immunity does not hold for plus-minus TS-CSK (PM TS-CSK) decision engines with a reasonable time difference between bits, instead requiring a marginally more complicated decision engine. This is borne out the system equations,

$$\delta(x) = \left\{ \begin{array}{cc} \delta_z & x_2(t) < -\sqrt{\rho(\beta-1)} \\ 1-\delta_z & -\sqrt{\rho(\beta-1)} \leq x_2(t) < 0 \\ \delta_z & 0 < x_2(t) < \sqrt{\rho(\beta-1)} \\ 1-\delta_z & x_2(t) \geq \sqrt{\rho(\beta-1)} \end{array} \right\} \tag{10}$$

where,

$$\delta_z = \left\{ \begin{array}{cc} 1 & x_3(t) \geq \beta - 1 \\ 0 & x_3(t) < \beta - 1 \end{array} \right\} \tag{11}$$

The regions of operation and switching about the equilibrium of the system are derived from this new decision engine. When the third dynamic, $x_3(t)$, crosses from one side of its equilibrium to the other the system switches. The system splits the second dynamic into four regions to increase the number of regions of operation. These regions are below the negative focus, between the negative focus and the origin, between the origin and the positive focus, and above the positive focus. Equations (10) and (11) describe the 8-section TS-CSK system.

C. Known-Plaintext and Chosen-Plaintext Attacks

These attacks are derived from inserting a known plain-text message and comparing it to the responding "ciphertext". Any circuitry-implemented CSK system is immune to this type of attack, as the message will just extract the orbitals or orbital speed system for the CSK and TS-CSK frameworks responsively. This attack, which is a repetition of the ciphertext, is only useful when the same initial conditions of the system with the transmitter can be guaranteed, which is impossible within a circuit without internal knowledge of Chua's system and significantly accurate measurements of the state values.

V. Conclusion

Resource-limited devices depend on low-power modes of security to transmit data. Due to the dependence of synchronous and asynchronous encryption on power-consuming processors, implementing these modes of security on resource-limited devices is becoming more challenging day by day.

To develop a new mode of security, chaotic encryption is gaining more interest. This work contributes toward the goal of achieving the efficient chaos ciphering implemented on the chip along with the sensors to encode the data at its very origin.

The study of attacks on hardware-implemented Chua's chaotic equations with simulation in multiple platforms, i.e., MATLAB Simulink and LTSpice enables a closer move to the desired security level that can operate in a post-quantum era. In this work, we thoroughly examined the attacks, in the two subgroups of physical and cryptographic attacks, on continuous chaotic systems in devices with limited resources, as well as any viable defenses through simulations. A promising method simulated in this paper is the use of memristors to avoid node tampering. Memristors are capable of acting as the keys for securing the circuit design with negligible power consumption added to the circuit. The paper also proves in simulation the robustness of Chua's encryption to common side-channel attacks.

ACKNOWLEDGMENT

This research is based upon work supported by the National Science Foundation under Grant No. 2131156.

REFERENCES

[1] "FDA offers proposed guidance on when a wellness product becomes a medical device." Available: https://medcitynews.com/2015/01/fda-proposed-guidance-rewards-companies- using-vague-references-improving-health/, Jan 2015.

[2] "Health wearables: Early days." Available: https://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/pwc-hri- wearable-devices.pdf, May 2014.

[3] C. Erdmier, J. Hatcher, and M. Lee, "Wearable device implications in the healthcare industry," Journal of Medical Engineering Eechnology, vol. 40, no. 4, pp. 141–148, 2016.

[4] "Wearable technology market by product, type, application, and geography - global forecast to 2026." Available: https://www.marketsandmarkets.com/Market-Reports/wearable-electronics-market-983.html, Oct 2021.

[5] "Top AI-powered wearable to look out for in 2021." Available: https://analyticsindiamag.com/top-ai-powered-wearables-to-look-out-for-in-2021/, Mar 2021.

[6] "Jbuds frames wireless audio for your glasses." Available: https://www.jlab.com/products/jbuds-frames-wireless-audio-for-your-glasses, Oct 2022.

[7] "Bioheart - the most sophisticated heart health monitoring device." Available: https://www.biotricity.com/bioheart/, Oct 2022.

[8] "Top 10 innovative wearable IoT devices." Available: https://iotdesignpro.com/articles/top-10-innovative-wearable-iot-devices, Nov 2019.

[9] 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 Computers & Digital Techniques 12, no. 6 (2018): 297-305.

[10] E. Tlelo-Cuautle and M. Duarte-Villaseñor, "Designing Chua's circuit from the behavioral to the transistor level of abstraction," Applied Mathematics and Computation, vol. 184, pp. 715–720, 01 2007.

[11] Z. Wei, "Dynamical behaviors of a chaotic system with no equilibria," Fuel and Energy Abstracts, vol. 376, 05 2011.

[12] S. Vaidyanathan, "Hybrid synchronization of Liu and Lu chaotic systems via adaptive control," International Journal of Advanced Information Technology, vol. 1, pp. 13–32, 12 2011.

[13] A. Hedayatipour and N. McFarlane, "An encryption architecture suitable for on chip integration with sensors," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 11, no. 2, pp. 395–404, 2021.

[14] M. Jalilian, A. Ahmadi, and M. Ahmadi, "Hardware implementation of a chaotic pseudo random number generator based on 3d chaotic system without equilibrium," In 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 741–744, 2018.

[15] A. Hedayatipour, R. Monani, A. Rezaei, M. Aliasgari, and H. Sayadi, "A comprehensive analysis of chaos-based secure systems," In Proceedings of Silicon Valley Cybersecurity Conference (SVCC), pp. 90-105, 2021.

[16] R. Monani, B. Rogers, A. Rezaei, and A. Hedayatipour, "Implementation of chaotic encryption architecture on FPGA for on-chip secure communication," In Proceedings of IEEE Green Energy and Smart Systems Conference (IGESSC), pp. 1-6, 2022.

[17] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," In Proceedings of 38th Annual Symposium on Foundations of Computer Science, pp. 394–403, 1997.

[18] Announcing the Advanced Encryption Standard (AES). FIPS Pub.; 197, Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2001.

[19] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," IEEE Transactions on Computers, vol. 52, no. 4, pp. 492–505, 2003.

[20] J. Nechvatal, Public-key cryptography. NIST special publication ; 800-2, Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology, 1991.

[21] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," In International Conference on Computer Science and Electronics Engineering, vol. 3, pp. 648–651, 2012.

[22] P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, S. Bal, S. Roy, M. K. Sarkar, S. Kumar, and R. Das, "Acafp: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. a review on RSA algorithm," In Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), pp. 332–337, 2017.

[23] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," arXiv preprint quant-ph/0301141, 2003.

[24] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," IEEE Access, vol. 8, pp. 21091–21116, 2020.

[25] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the internet of things," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457–6480, 2020.

[26] L. Fortuna, "Chua's circuit implementations: Yesterday, today and tomorrow," World Scientific Series on Nonlinear Science, series A, vol 65, 2009.

[27] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," In International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37, 2017.

[28] J. Fowler, "Fitness tracker data breach exposed 61 million records and user data online." Available: https://www.websiteplanet.com/blog/gethealth-leak-report/, 2020.

[29] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," In IEEE Symposium on Security and Privacy (S & P), pp. 129–142, 2008.

[30] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC), pp. 226–236, Association for Computing Machinery, 2016.

[31] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," In IEEE 13th International Conference on e-Health Networking, Applications and Services, pp. 150–156, 2011.

[32] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADAa system," In Black Hat conference presentation slides, vol. 2011, 2011.

[33] L. Pycroft, S. G. Boccard, S. L. Owen, J. F. Stein, J. J. Fitzgerald, A. L. Green, and T. Z. Aziz, "Brainjacking: Implant security issues in invasive neuromodulation," World Neurosurgery, vol. 92, pp. 454–462, 2016.

[34] L. Chua, "Memristor-the missing circuit element," IEEE Transactions on Circuit Theory, vol. 18, no. 5, pp. 507-519, 1971.

[35] A. Rezaei, J. and H. Zhou, "Hybrid memristor-CMOS obfuscation against untrusted foundries," In IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 535-540, 2019.
[36] A. Rezaei, Y. Shen, and H. Zhou, "Rescuing logic encryption in post-SAT era by locking & obfuscation," In Proceedings of 23rd Design, Automation and Test in Europe Conference & Exhibition (DATE), pp. 13-18, 2020.
[37] R. Afsharmazayejani, H. Sayadi, and A. Rezaei, "Distributed logic encryption: Essential security requirements and low-overhead implementation," In Proceedings of Great Lakes Symposium on VLSI (GLSVLSI), pp. 127-131, 2022.
[38] A. Chaudhuri and K. Chakrabarty, "Analysis of process variations, defects, and design-induced coupling in memristors," In IEEE International Test Conference (ITC), pp. 1-10, 2018.
[39] Q. Xia et al., "Memristor-CMOS hybrid integrated circuits for reconfigurable logic," ACS Nano Letters, vol. 9, pp. 3640–3645, 2009.
[40] Y. Pang , B. Gao, B. Lin, H. Qian, H. Wu, "Memristors for hardware security applications". Advanced Electronic Materials. vol. 5, no.9, pp. 1800872, 2019.
[41] D. R. Brown, "A practical realization of a return map immune Lorenz based chaotic stream cipher in circuitry," University of Tennessee, Knoxville, 2017.
[42] W. Xu, T. Wood, W. Trappe, and Y. Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service," In Proceedings of the 3rd ACM workshop on Wireless security, pp. 80-89. 2004.
[43] M. Sampe and K. Furuta, "On time scaling for nonlinear systems: Application to linearization," IEEE Transactions on Automatic Control, 31, (5), pp. 459–462, 1986.
[44] D. Materassi and M. Basso, "Time scaling of chaotic systems: Application to secure communications," International Journal of Bifurcation and Chaos, 18, (02), pp. 567–575, 2008.