# WIRELESS HARDWARE ANALOG ENCRYPTION FOR SECURE, ULTRA LOW POWER TRANSMISSION OF DATA

Donatello Materassi[1] Nicole McFarlene[2]
University of Minnesota [1] University of Tennessee [2]

## Introduction

- Wearable biosensing devices have become ubiquitous, with applications in the medical domain [8], biometrics [1], and human-computer interaction [3], among others.
- Biosensing devices terminology:
  - Sensor: two- node network, one-way communication
  - Actuator: two-node network, two-way communication
  - Networks of sensors

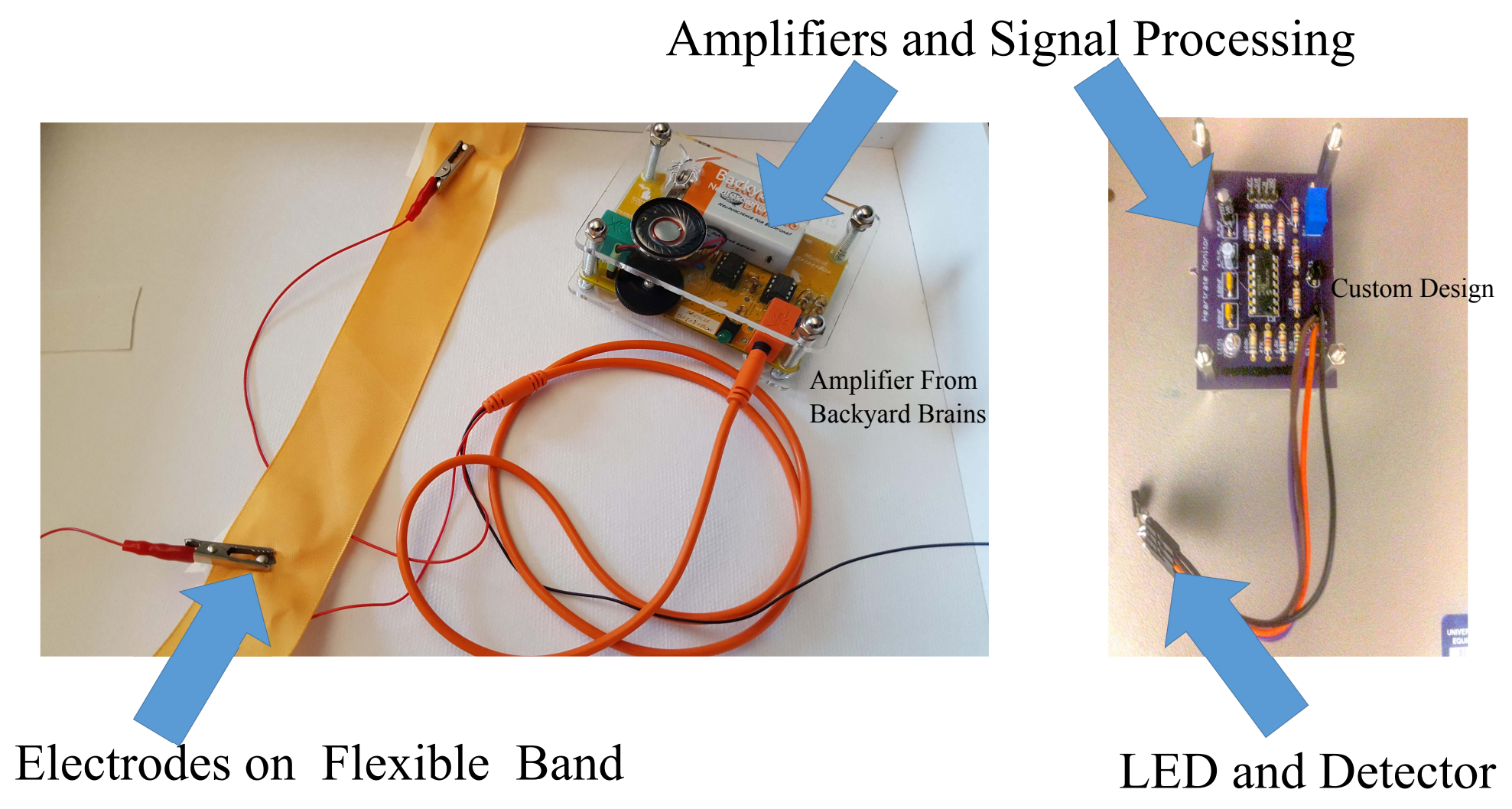


Fig. 1: Example biosensing electronics. Left: amplifier commercially available from backyardbrains. Center: custom biosensing electronics developed by the PI.

## Problem

- Most of the biomedical devices are not designed with security priorities [4]
- Networks of sensors are also not designed with security as a top priority
- Main reason for lack of security: Digital encryption schemes typically require power-hungry microprocessors, while the power sources of sensors (both battery-powered and energy harvesting sensors) have limited capacity
  - Software implementations on a smartphone can consume $500mAh$ [6].
  - Field Programmable Gate Array (FPGA) implementations can consume from $170$ to $300mW$ [10].

## Proposed Solution: Wireless Hardware Analog Encryption

- Hardware Encryption: layer of hardware security directly incorporated into the sensors as an integral part of the design process will protect the privacy of users
- Analog Encryption: requires lower power and a smaller area on a chip

## Applications and Impact

- Biomedical Devices: secure and portable wireless biosensors can be deployed in both hospital and non-hospital settings improving the care received by the patients
- Sensor Networks: Internet of Things (IOT), monitoring of infrastructures in smart cities, coordination of unmanned vehicles, and tracking of wildlife.

## Chaos as an analog way to encrypt data

### Features of chaotic systems:

- Deterministic behavior that has the appearance of being stochastic
- Identical chaotic systems, with slightly different initial conditions, will diverge
- Despite high sensitivity w.r.t. initial conditions, if appropriately coupled, two chaotic systems can synchronize their states [9]

### Principle of Chaotic Encryption Schemes

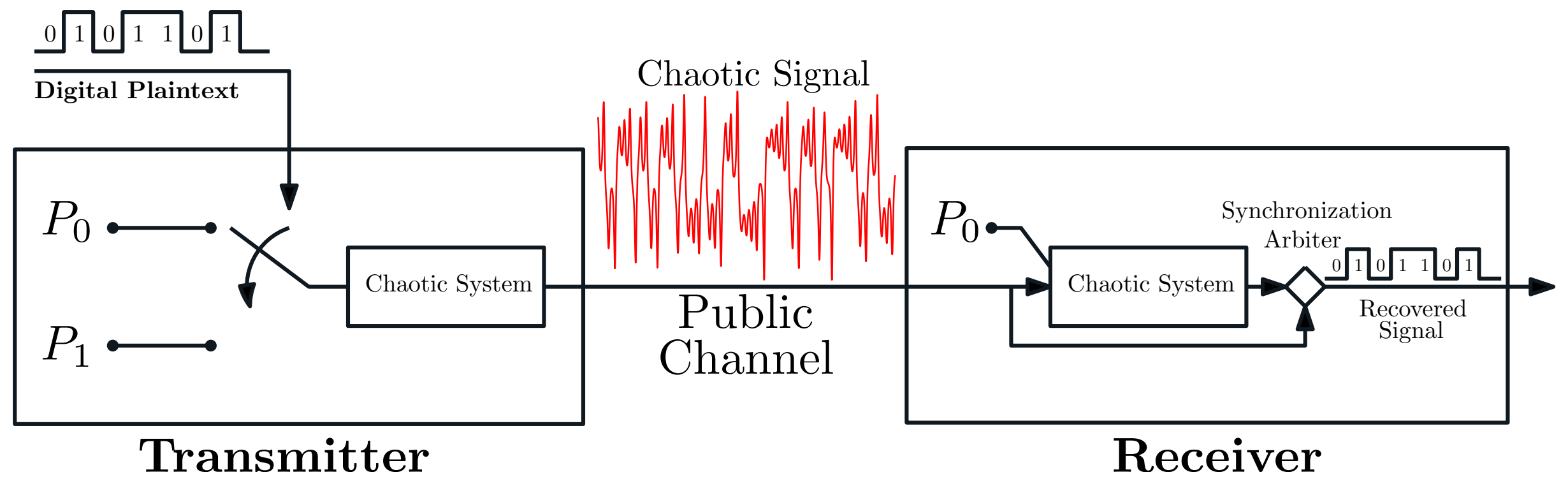


Fig. 2: Chaotic Shifting Key scheme: the digital plaintext modulates the switching of a chaotic circuit in the transmitter between two configuration parameters $P0$ and $P1$; the receiver has a copy of the chaotic circuit tuned on the parameter $P0$; a comparator determines if synchronization is achieved: in case of synchronization the decoded bit is $0$, otherwise the decoded bit is $1$.

### Example chaotic system: Lorenz system

$$\left\{\begin{array}{l}\dot{x}_1=\sigma(x_2-x_1)\\ \dot{x}_2=(\beta(m)-x_3)x_1-x_2\\ \dot{x}_3=x_1x_2-\rho x_3\\ \beta(m)=\left\{\begin{array}{l}\boxed{\beta_0 \text{ if } m=0}\\ \beta_1 \text{ if } m=1\end{array}\right.\end{array}\right. \quad \text{Synchronization: } ||x_1-z_1|| \text{ is small} \quad \xrightarrow{s=x_1} \quad \left\{\begin{array}{l}\dot{z}_1=\sigma(z_2-z_1)\\ \dot{z}_2=(\beta_0-z_3)s-z_2\\ \dot{z}_3=z_1z_2-\rho z_3)\\ e=z_1-s\end{array}\right.$$

Transmitter Receiver

### Problem with Chaotic Shifting Key scheme

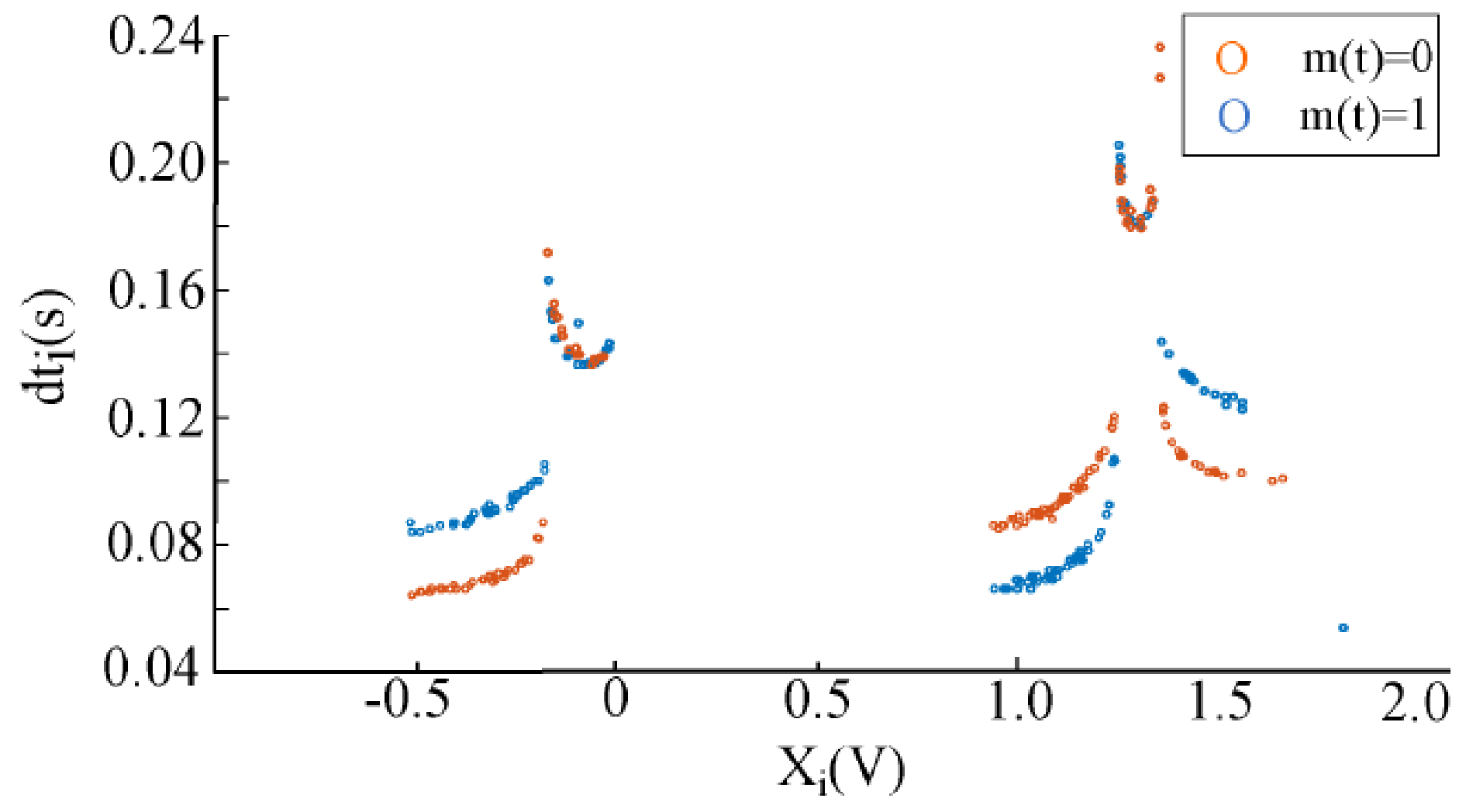


Fig. 4: Different patterns of peaks in public key when transmitting $0$ and $1$ are detectable.

### Secure Chaotic Shifting Key scheme: Time-Shifting CSK [7]

$$\left\{\begin{array}{l}\dot{x}_1=[\sigma(x_2-x_1)]\lambda(x,m)\\ \dot{x}_2=[(\beta-x_3)x_1-x_2]\lambda(x,m)\\ \dot{x}_3=[x_1x_2-\rho x_3]\lambda(x,m)\\ \lambda(m)=\left\{\begin{array}{l}\lambda(x,0) \text{ if } m=0\\ \lambda(x,1) \text{ if } m=1\end{array}\right.\end{array}\right. \quad \xrightarrow{s=x_1} \quad \left\{\begin{array}{l}\dot{z}_1=[\sigma(z_2-z_1)]\lambda(z,m)\\ \dot{z}_2=[(\beta-z_3)s-z_2]\lambda(z,m)\\ \dot{z}_3=[z_1z_2-\rho z_3)]\lambda(z,m)\\ e=z_1-s.\end{array}\right.$$

Transmitter Receiver

## Realization

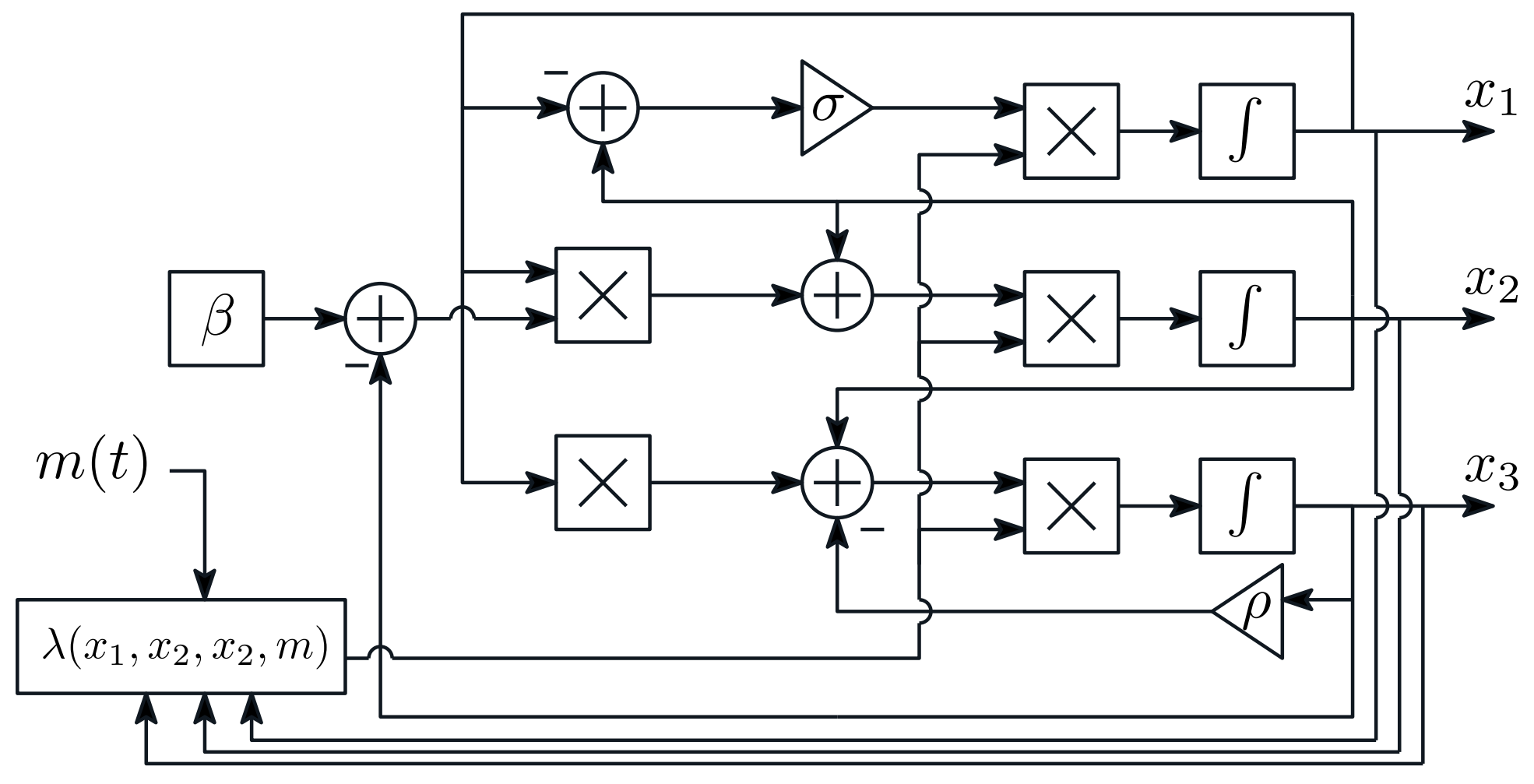
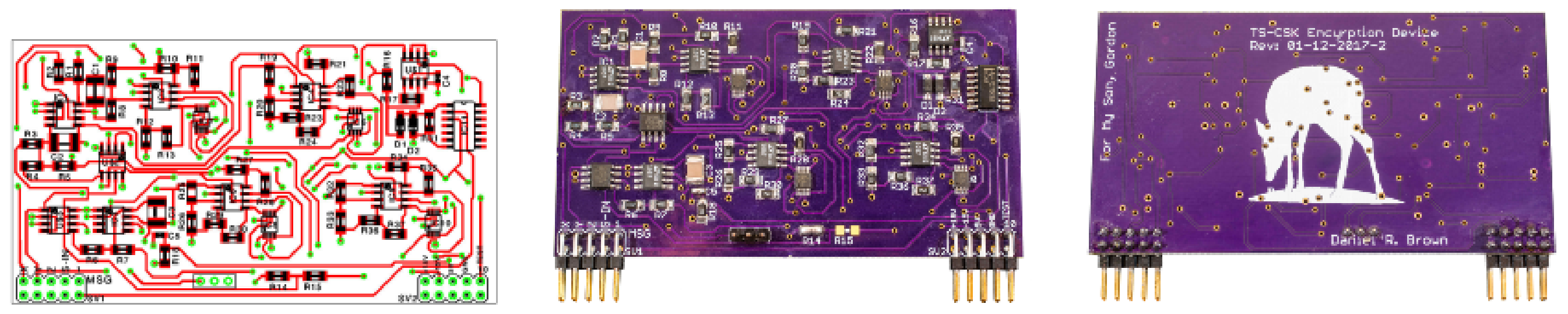


Fig. 6: Block diagram of a TS-CSK transmitter [2]



(Board scheme) (PCB Board Top) (PCB Board bottom)

Fig. 7: A discrete implementation of a TS-CSK encryption scheme [2]

### A Temperature Sensor with TS-CSK Analog Encryption [5]

## What's Next?

1. Develop and evaluate integrated CMOS circuitry to implement a TS-CSK communication scheme.
2. Develop and test the TS-CSK communication scheme on a wireless EEG sensor.

## References

[1] Savvas Argyropoulos et al. "Biometric template protection in multimodal authentication systems based on error correcting codes". In: *Journal of computer security* 18.1 (2010).

[2] Daniel Brown et al. "Practical realisation of a return map immune Lorenz-based chaotic stream cipher in circuitry". In: *IET Computers & Digital Techniques* 12.6 (2018).

[3] Yu Mike Chi et al. "Dry and noncontact EEG sensors for mobile brain–computer interfaces". In: *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 20.2 (2011).

[4] Mary Beth Hamel et al. "FDA regulation of mobile health technologies". In: *The New England journal of medicine* 371.4 (2014), p. 372.

[5] Ava Hedayatipour, Kendra Anderson, and Nicole McFarlane. "Live Demonstration: A Temperature Sensor with Analog Encryption". In: *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE. 2019, pp. 1–1.

[6] Mohammad Masoud et al. "The power consumption cost of data encryption in smartphones". In: *2015 International Conference on Open Source Software Computing (OSSCOM)*. IEEE. 2015, pp. 1–6.

[7] Donatello Materassi and Michele Basso. "Time scaling of chaotic systems: Application to secure communications". In: *International Journal of Bifurcation and Chaos* 18.02 (2008).

[8] Christoph M Michel et al. "EEG source imaging". In: *Clinical neurophysiology* 115.10 (2004).

[9] Louis M Pecora and Thomas L Carroll. "Synchronization in chaotic systems". In: *Physical review letters* 64.8 (1990).

[10] Shady Mohamed Soliman, Baher Magdy, and Mohamed A Abd El Ghany. "Efficient implementation of the AES algorithm for security applications". In: *2016 29th IEEE International System-on-Chip Conference (SOCC)*. IEEE. 2016, pp. 206–210.