



Cairo University

MEMRISTOR-BASED HARDWARE SECURITY ALGORITHMS AND CIRCUITS

By

Hanan Abdel-Hamid Abdel-Salam Rady

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Advanced Materials and Nanotechnology

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

MEMRISTOR-BASED HARDWARE SECURITY ALGORITHMS AND CIRCUITS

By

Hanan Abdel-Hamid Abdel-Salam Rady

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Advanced Materials and Nanotechnology

Under the Supervision of

Prof. Dr. Ahmed Nader Mohieldin

Dr. Hassan Moustafa Hassan

.....

.....

Professor of
Faculty of Engineering, Cairo University

Assistant Professor
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT
2020

MEMRISTOR-BASED HARDWARE SECURITY ALGORITHMS AND CIRCUITS

By

Hanan Abdel-Hamid Abdel-Salam Rady

A Thesis Submitted to the
Faculty of Engineering at Cairo University
in Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
in
Advanced Materials and Nanotechnology

Approved by the
Examining Committee

Prof. Dr. First E. Name, Thesis Main Advisor

Prof. Dr. Second E. Name, Member

Prof. Dr. Third E. Name, Internal Examiner

Prof. Dr. Fourth S. Name, External Examiner

- Write his Work & Place

FACULTY OF ENGINEERING, CAIRO UNIVERSITY
GIZA, EGYPT

2020

Disclaimer

I hereby declare that this thesis is my own original work and that no part of it has been submitted for a degree qualification at any other university or institute.

I further declare that I have appropriately acknowledged all sources used and have cited them in the references section.

Name:

Date: ../../... (it's the date that you handover the thesis)

Signature:

Dedication

"To my mother, my husband, my children and my loyal friends whose unbounded sacrifices have brought me this far."

Hanan Rady

Acknowledgments

First and foremost, I thank **ALLAH**, the most gracious, the ever merciful for helping me finishing this work.

I want to thank all those, who helped me by their knowledge and experience. I will always appreciate their efforts. I would like to offer my sincere thanks to my supervisors Professor Mohamed Sameh Said ((Allah bless your own soul), Professor Ahmed Nader Mohieldin and Doctor Hassan Moustafa for valuable supervision, continuous encouragement, useful suggestions, and active help during this work.

My sincere appreciation and gratitude to my family for their help and patience during the preparation of this work, especially for my mother.

Table of Contents

LIST OF TABLES.....	VI
LIST OF FIGURES.....	VII
NOMENCLATURE	IX
ABSTRACT	IX
CHAPTER 1 : INTRODUCTION	1
1.1. Motivation	1
1.2. Thesis outline.	2
CHAPTER 2 : MEMRISTOR OVERVIEW	3
2.1. Memristor Device Definition	3
2.2. The Missing Element History	3
2.2.1 Preliminaries	3
2.2.2 HP Memristor	4
2.3. Memristor Theory, Operation, and Characteristics	6
2.3.1 Working principle	6
2.3.2 Theory and Operation	7
2.3.3 Characteristics	8
2.3.4 Memristor fingerprints	9
2.3.5 Switching mechanism	10
2.3.6 Memristor switching styles	11
2.4. Memristor Modeling	13
2.4.1 Linear Ion Drift Model	13
2.4.2 Nonlinear Ion Drift Model	14
2.4.3 Simmons Tunnel Barrier Model	14
2.4.4 TEAM "ThrEshold Adaptive Memristor" Model	15
2.5. Memristor-Based Applications	17
2.5.1 Digital Applications	17
2.5.2 Neuromorphic Circuits	17
2.5.3 Analog Circuits	18
CHAPTER 3: MEMRISTOR-BASED HARDWARE SECURITY SOLUTIONS	19
3.1. Background	19
3.2. Rationales for Memristor-based Hardware Security Primitives	20
3.3. Memristor - based Secret Key Generation	22

CHAPTER 4: MEMRISTOR-BASED AES KEY GENERATION FOR LOW POWER IOT HARDWARE SECURITY MODULES. (PROPOSED MODULE)	28
4.1. Introduction	28
4.2. Proposed Module	30
4.2.1 Memristor- Based IV Characteristics	31
4.2.2 Time-Based ADC	31
4.2.3 Key Generator (SIPO Shift Register)	34
4.2.4 AES Algorithm (Encryption and Decryption processes)	36
4.2.5 Mutual Authentication of the generated key at the encryption and decryption processes	41
4.3. Simulation Results	41
CHAPTER 5: DISCUSSION AND CONCLUSIONS	47
5.1. Contributions.....	47
5.2. Published/Submitted Paper	47
5.3. Recommendations for Future Work.....	47
REFERENCES	48

List of Tables

Table 2.1: A comparison between the four memristor device models submitted in [9]	16
Table 3.1: the acronyms and definitions used for the proposed security technique that submitted in [25].	27
Table 4.1: represents the corresponding 3-bit T-ADC binary states with respect to the Memristor output voltage values at 'X'	43
Table 4.2: Five Plaintext messages in Hexadecimal and the corresponding encrypted messages as a result of using the generated 128-bit key through AES encryption algorithm	46

List of Figures

Figure 2.1: Four fundamental circuit elements [10]	3
Figure 2.2: Memristor device structure presented by S. Williams and his research group at HP Laboratories. [39]	4
Figure 2.3: The memristor under the electrical behavior [39]	5
Figure 2.4: (a) Memristor structure, (b) Memristor Equivalent circuit model, and (c) Memristor symbol [10]	5
Figure 2.5: Working of a Memristor [40]	7
Figure 2.6: Memristor I-V pinched hysteresis loop [7]	9
Figure 2.7: The hysteresis loop collapses to a straight line for high frequencies [8]	10
Figure 2.8: Schematics of resistive switching phases as stated by the filamentary conduction model [4].	11
Figure 2.9: Schematic diagram of Memristor switching characteristics for (a) unipolar style; (b) bipolar style. [4]	12
Figure 2.10 Linear ion drift model [9]	13
Figure 2.11 Simmons tunnel barrier memristive device Physical model [9] ..	15
Figure 2.12 Schematic illustration of using memristors as synapses between neurons [6]	18
Figure 3.1: Crossbar array of memristors [45]	21
Figure 3.2: Schematic of a memristor device [22]	22
(a) Initial oxygen vacancies profile.	
(b) The obtained new profile after applying a certain voltage for a certain time	
Figure 3.3: Conceptual geometry for an oxide memristor. [24]	22
Figure 3.4: Host A and B communication scenario [22]	23
Figure 3.5: initial vacancies profile for TiO ₂ memristor	23
Figure 3.6: Initial profiles (master keys) generated using identical memristor devices.	24
Figure 3.7: Electrical characteristics of different fabricated memristor devices [25]	25

Figure 3.8: Memristor-based security approach. Hosts A and B can initiate communication through TTP [25]	26
Figure 4.1: Internet-of-things (IoT) paradigm [18]	29
Figure 4.2: The Proposed Module	30
(a) Encryption process at Device A.	
(b) Decryption process at Device B	
Figure 4.3: T- ADC architecture [31]	31
Figure 4.4: Block diagram of digitizing Memristor I-V curve	32
Figure 4.5: the starved inverter	33
Figure 4.6: Implementation of the memristor I-V characteristic curve digitization process by using the two stages of T-ADC, VTC, and TDC.....	33
Figure 4.7: 128-bit key generation Block Diagram	34
Figure 4.8: 128-bit Serial-In Parallel-out (Right-shift) Shift Register	35
Figure 4.9: Output Waveform of n-bit Right-Shift SIPO Shift Register [33] ..	35
Figure 4.10: AES Block Diagram for a 128-bit key size.....	37
Figure 4.11: SubBytes step	38
Figure 4.12: ShiftRows step	39
Figure 4.13: The resulting matrix after shift operation	39
Figure 4.14: Mix Columns step	40
Figure 4.15: AddRoundKey step.....	40
Figure 4.16: Mutual Authentication of the generated key between the encryption and decryption processes	41
Figure 4.17: Memristor I-V Characteristics by sweeping the input current from (-35 μ A to +35 μ A) at frequency=100 MHz , stop time = 15ns and initial state=zero.	42
Figure 4.18: Memristor I-V Characteristics by sweeping the input current from (-35 μ A to + 35 μ A) at frequency =100MHz, stop time=10ns and initial stat = zero.	43
Figure 4.19: Inserting the128-bits generated key and a Text message into AES.vhd	44
Figure 4.20: Flowchart of the Sequencing steps of AES encryption process which simulated through Xilinx Vivado.	45

Nomenclature

AES	Advanced Encryption Standard algorithm
DES	Data Encryption Standard algorithm
CIM	computing-in-memory
IoT	Internet of Things
HSM	Hardware Security Module
HRS	high resistance state
LRS	low resistance state
M	Memristance
MIM	Metal-Insulator-Metal
NIST	National Institute of Standards and Technology
nvLogics	NonVolatile logics
NVM	NonVolatile Memory
PUFs	Physical-Unclonable Functions
NanoPPUF	nanoelectronic public PUF
TEAM	ThrEshold Adaptive Memristor model
TTP	Trusted Third Party
T-ADC	Time-based Analog to Digital Converter
TDC	Time-to-Digital Converter
VTC	Voltage-to-Time Converter
SIPO	Serial in- Parallel out
SoC	System-on-Chip
RTL	Register Transfer Level
ReRAM	Resistive Random-Access Memory
CRRAM	Contact-Resistive Random-Access Memory
STTRAM	Spin Torque-Transfer Random-Access Memory
OSTRAM	Orthogonal Spin Transfer Random Access Memory

Abstract

Hardware security has emerged as a very important field aimed towards mitigating issues like counterfeiting, side-channel attacks, and reverse engineering. Hardware security primitives are utilized in ensuring the integrity and authenticity of integrated circuits (ICs). To provide robust security with minimal area and power, Nanoelectronics-based hardware security solutions, which maintain the aforementioned merits are used whereas providing novel security techniques. In addition, Nanoelectronics-based security solutions are more robust than typical CMOS security solutions as the complexity of a Nanoelectronics security primitive violation is comparable to the troublesome of solving a set of nonlinear equations of a large system.

Memristor is a preferable candidate in security applications due to the unique electrical response from one type of Memristor to another. Consequently, the response of individual devices is difficult to predict by a specified mathematical model. Hence, it is a challenge to predict the memristor response that is integrated into the hardware implementation. In addition, what provides memristors a unique advantage over many other nano-devices is the compatibility with modern CMOS manufacturing technologies.

In this work, a hardware security module (HSM) based on a memristor-based key generation scheme is presented. The scheme relies on the unique behavior of the I-V characteristics of the Memristor devices. The generated Memristor based key is used through AES (Advanced Encryption Standard) encryption and decryption processes. The module depends on Memristor-based AES key generation relying mainly on the uniqueness of Memristor devices due to fabrication process variations.

In Time-based ADCs, the input voltage is first converted to a pulse delay time by using a Voltage-to-Time Converter (VTC) circuit that makes the power hungry Sample-and-Hold circuit unnecessary and eliminates the preprocessing analog signals blocks. The pulse delay time is converted to a digital word by using a Time-to-Digital Converter (TDC) circuit that uses the Vernier delay line that consists of two parallel delay chains and a sense amplifier based on the D-flip flops. Therefore the time-based ADC (T-ADC) has the advantage of being highly digitally oriented, thus the scaling of CMOS which provides better timing accuracy with low power consumption at high frequencies is a fundamental advantage to it as opposed to traditional analog circuits. In addition, the proposed T-ADC circuit need one starved inverter and the number of delays and D-flip flops are determined using this formula $(2^n - 1)$ where n, represents number of bits, hence T-ADC eliminates the dependence on comparators and reference array resistors existing in Flash ADCs.

AES (Advanced Encryption Standard) is a symmetric-key cryptographic algorithm. AES has a fixed block size of 128 bits and three key sizes to choose from 128, 192 and 256. Therefore, AES offers strong security and high flexibility. AES cryptographic algorithm has proved its immunity against attacks. AES has become the perfect choice for various applications, including not only wireless standards but also, the security of smart cards and bit-stream security in FPGAs. The AES algorithm is found to be the most suitable algorithm for IoT hardware security applications.

In addition to taking into consideration the aforementioned powerful properties and features of the Time-based ADC and AES cryptographic algorithm, the proposed hardware security module meets the needs of modern technology such as secure communication between IoT embedded devices.

Chapter 1 : Introduction

1.1 Motivations

Information security has emerged as a remarkable system and can be considered as an application metric [1]. It includes preventing or eliminating the chance of unauthorized access, deletion, modification, or inspection of important information. Classical security both were mathematical models or algorithmic models have produced security solutions and protocols. It is unfortunate that the classical security techniques are inefficient due to its high-energy consumption and slow operation. Also it vulnerable to physical and side-channel attacks such as exposure to radiation or high temperatures. Moreover, Classical solutions utilize techniques that meet a few emerging security requirements, frequently at high-energy and performance expense.

Over the last forty years, technologies in the security field have been developed to achieve approaches of physical security that deployed to large high-speed computers until even possible to apply security approaches recently to high-performance, low-power, low-cost, and lightweight sensors, tablets, and mobile phones. Hardware security has emerged as a very important area with the aim of studying the mitigating of critical issues such as side-channel attacks, counterfeiting, and Piracy. It worthy noted that the software security primitives are significantly less secure than their hardware equivalents due to the fact that software solutions make use of shared memory space, the security level of a software-based cryptographic module is upper-limited by the security level of the mechanism that protects the secrecy and integrity of the memory space it uses. In addition, the software cryptographic modules are running on top of an operating system and are more fluid in terms of ease of modification. Software based solutions are more vulnerable to attacks that are based on power consumption analysis. On the other side, hardware-based solutions can apply special measures that mask the fluctuation in power consumption, to prevent the attacker from collecting power consumption information that can assist in the compromise of the secret key. Hardware security primitives can be implemented for key generation, authentication, device identification, data encryption, and tamper detection. In addition, hardware security approaches succeed in dealing with the above-mentioned restriction with less energy and performance overhead [2]. Research in CMOS technology-based hardware security at higher levels of abstraction both was circuit and architecture has seen consistent growth over the past decade, but the past several years have seen an uptick in research on the security of nanodevices [18].

Nanoelectronics-based security approaches offer higher robustness when comparable with CMOS security ones. They can be premised for explicit security in an information-theory concept due to the complexness of exposing nanoelectronics-based security primitive is similar to the troublesome of solving a set of nonlinear mathematical equations [2]. Emerging nanoelectronics-based

techniques offer the production of computing systems with low-power consumption, low computation times, small form factors, with respect to CMOS technologies.

Various materials and devices to name a few such as Memristor, quantum dots and plasmonics are researched and investigated for using as nanoelectronics candidates. In [1] the security capabilities of several emerging nanoelectronics devices to name a few: Memristor, orthogonal spin transfer random access memory OSTRAM, contact-resistive random-access memory CRRAM, spin torque-transfer random-access memory STTRAM, silicon nanowire field-effect transistors, resistive random-access memory RRAM, and phase change memories, are presented.

Memristor devices can play a very important role in hardware security approaches because of their unique characteristics as:

1- Memristor physical parameters that could be controlled during the fabrication process significantly affect its behavior. Therefore, it is a challenge to get identical devices. This unique feature makes it difficult to predict the definite behavior of a Memristor device so the attacker's job is particularly challenging.

2-The current-voltage characteristics of a Memristor are highly non-linear and exhibit a hysteresis pinched loop which is considered as a most important Memristor fingerprint.

3-The Memristor is a non-volatile device that remembers its resistance state changes that is a function of the applied stimuli even if the power is turned off.

Thesis Outline

This thesis is structured as follows:

Chapter 2 Memristor Overview. **Chapter 3** introduces the literature contributions of Memristor-Based Hardware Security Solutions. **Chapter 4** introduces the Memristor –based AES Key Generation for low power IoT Hardware Security Modules (the proposed module). **Chapter 5** Discussion and Conclusions.

Chapter 2 : Memristor Overview

2.1 Memristor Device Definition

Memristor (a contraction of memory resistor) is the passive two-terminal fourth element of the electrical circuit and its resistance depends on the entire past applied current, or voltage [3]. Inherent novel applications of Memristor are neuromorphic circuits, spintronic devices, ultra-dense storage, and hardware security schemes. In 1971, Leon Chua assumed the presence of the fourth fundamental circuit element and coined it as Memristor [4]. It was suggested as a missing element that relates the electric charge (q) and the magnetic flux (ϕ), as illustrated in Figure 2.1. This property could not be captured by any set of the three basic elements, the capacitor, the resistor, and the inductor.

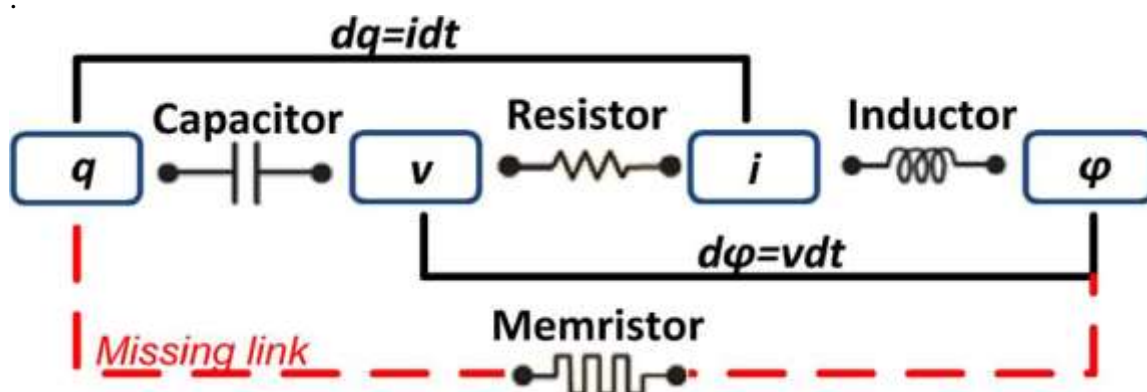


Figure 2.1: Four fundamental circuit elements [10].

2.2 The Missing Element History

2.2.1 Preliminaries

As mentioned in the previous section, in 1971, Memristor has been identified as the missing fourth circuit element that predicted by L. Chua. In 1976, Chua and Kang published their work to define a generous classification of memristive systems [5]. Accordingly, Memristor concept is generalized to a more extensive classification of nonlinear systems namely the memristive systems that is described in general by the equations [7]:

$$v(t) = R(w, i) \cdot i(t) \quad (2.1)$$

$$\frac{dw}{dt} = f(w, i) \quad (2.2)$$

Where w is a state variable, R and f are functions of time.

2.2.2 HP Memristor

In 2008, the first basic model of memristor has been preceded in HP labs. This model is governed by Chua's memristive system analytical formulations [6]. This model can be considered the first explicit relation between the practical demonstration of a memristor device and Chua's theory. The memristive behavior is observed by using nanoscale thin-film titanium dioxide (TiO_2) as an insulator layer.

As shown in Figure 2.2, the memristor structure consists of two layers that are chemically different. The first layer is TiO_2 (high impedance) is the undoped layer which is nearer to the top platinum electrode. The second layer is a doped layer that includes oxygen-deficient titanium dioxide TiO_{2-x} in which the titanium dioxide was missing around 2.5% of its oxygen. The vacancies are positively charged. The Memristor is formed as a 3-30 nanometer thickness (D) cube of Titanium dioxide (TiO_2) between two platinum plates [1].

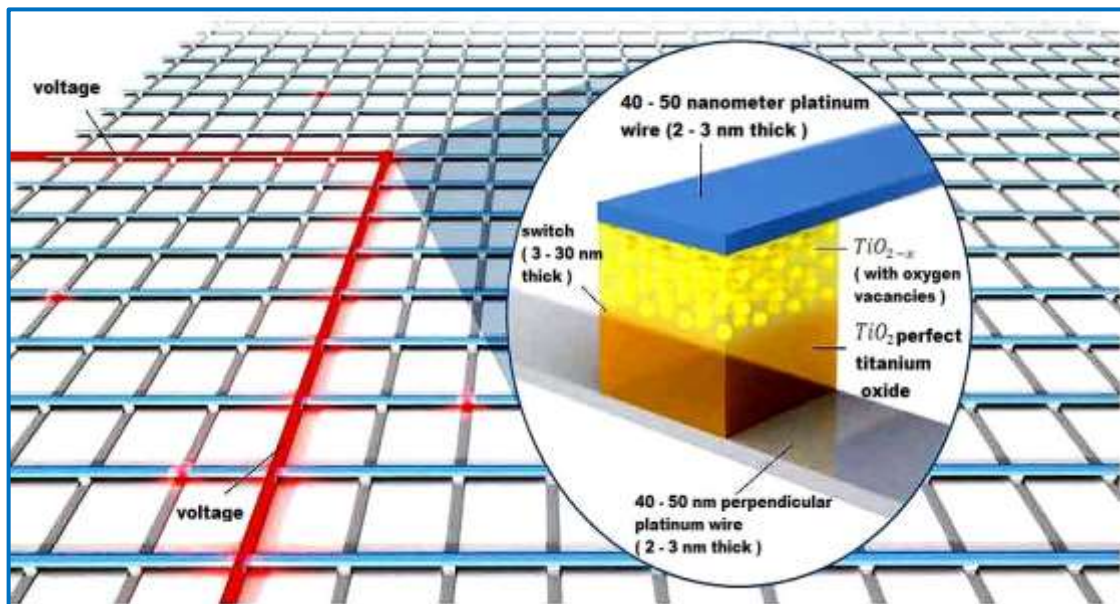


Figure 2.2: Memristor device structure presented by S. Williams and his research group at HP Laboratories. [39]

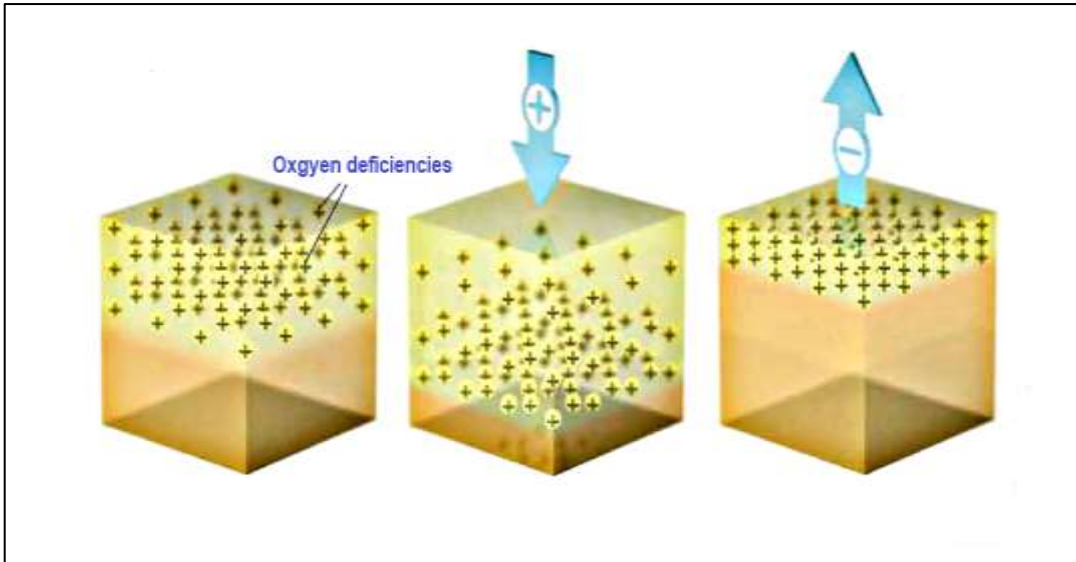


Figure 2.3: The memristor under electrical behavior [39]

As illustrated in Figure 2.3, the applied positive voltage at the top electrode repels the oxygen vacancies in the doped region down to the undoped region. Therefore, the vacancies migrate from the TiO_{2-x} to the TiO_2 region. The migration of the dopants increases the width of the TiO_{2-x} layer while decreases the width of TiO_2 . However, when applying a negative voltage, the vacancies are attracted to the electrode. In this situation, the TiO_{2-x} layer will be narrower than the TiO_2 layer.

As shown in Figure 2.4, The HP Memristor model consists of two series resistors R_{on} that is the doped region resistance and R_{off} is the undoped region resistance. It is supposed that D is the physical device width and w is the doped region. It should be noted that w is the width of the doped region, and it is counted the state variable that changes regard to the amount of charge.

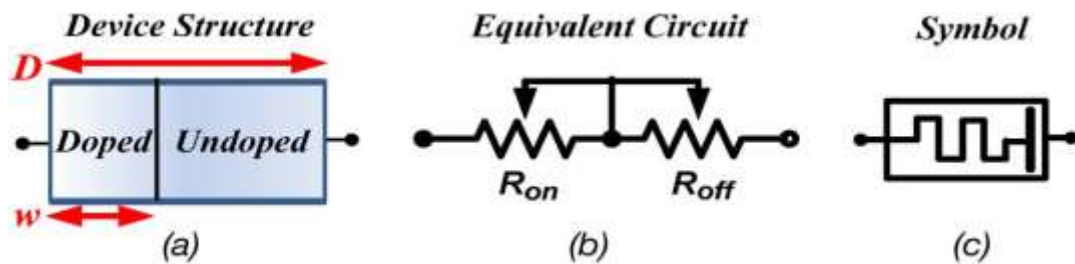


Figure 2.4: (a) Memristor structure, (b) Memristor Equivalent circuit model, and (c) Memristor symbol [10].

As stated by the previous description, the HP team introduced a mathematical model that presents the memristance of their device as a series of two resistances, as shown in Figure 2.4(b) and expressed as:

$$R = \left(R_{on} \frac{w(t)}{D} + R_{off} \left(1 - \frac{w(t)}{D} \right) \right) \quad (2.3)$$

$$\frac{dw}{dt} = \frac{\mu_v R_{on}}{D} i(t) \quad (2.4)$$

Where μ_v is the average ion mobility

The introduced device plays as a switch that introduces a ratio between the OFF resistance and the ON resistance equals 1000 [8].

It should be noted that, the Memristor resistance is governed by the integral of the current at the instantaneous time that is considered the significant difference between the transistor and the Memristor [6].

S. Williams expressed that Memristor can be the alternative to the CMOS transistors however consuming less power, occupying less chip area and providing better performance [10].

2.3 Memristor: Theory, Operation, and Characteristics

2.3.1 Working Principle

According to the previous section, because of the migration of the vacancies through the memristor device under the applied excitation, the resistance of the material stack increases or decreases depending on the applied stimuli polarity. In other words, the device total resistivity changes as illustrated in Figure 2.5.

When the doped region stretches until equals D and $w=D$, the total resistance decreases which signified by R_{on} that is obtained under positive stimuli. Otherwise, under negative stimuli, the undoped region stretched to D and $w = 0$, the total resistance increases which signified by R_{off} .

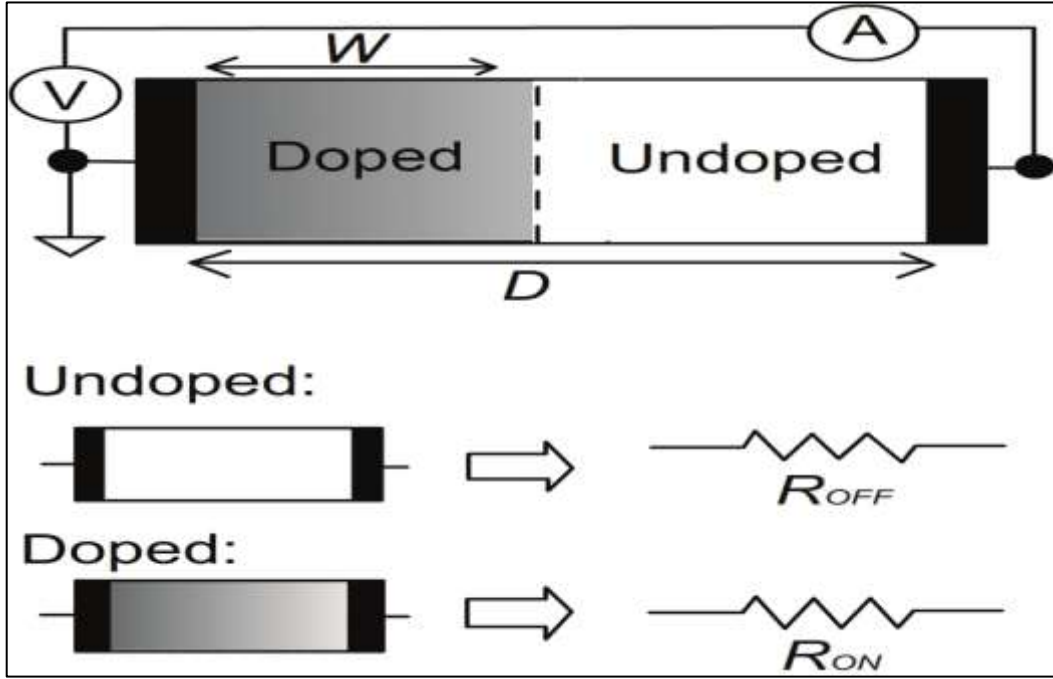


Figure 2.5: Working of a Memristor. [40]

In general, the device can be described by the following expressions:

$$V = R(w) \chi i \quad (2.5)$$

Where

$$R(w) = \left(R_{on} \frac{w(t)}{D} + R_{off} \left(1 - \frac{w(t)}{D} \right) \right) \quad \text{and} \quad 0 \leq \frac{w}{D} \leq 1 \quad (2.6)$$

2.3.2 Theory and Operation

For linear drift in a uniform field with average ion mobility μ_v and the ohmic electronic conduction as the simplest situation, the relation between the voltage and current can be expressed as follow:

$$v(t) = \left(R_{on} \frac{w(t)}{D} + R_{off} \left(1 - \frac{w(t)}{D} \right) \right) i(t) \quad (2.7)$$

and the derivative of the state variable is:

$$\frac{dw}{dt} = \frac{\mu_v R_{on}}{D} i(t) \quad (2.8)$$

Yields the following formula for $w(t)$

$$w(t) = \frac{\mu_v R_{on}}{D} q(t) \quad (2.9)$$

By inserting equation (2.9) into (2.7), we get the memristance that for $R_{on} \ll R_{off}$ will be simplified to:

$$M(q) = R_{off} \left(1 - \frac{\mu_v R_{on}}{D^2} q(t)\right) \quad (2.10)$$

Nonlinear change in the current passing through the Memristor device is noticed even if under a constant voltage because the Memristor integrates the voltage over time that is signified as (\emptyset) so a change of the amount of charge happens.

Memristor has two states, a low resistance state (LRS) and a high resistance state (HRS) [2]. Accordingly, there are two switching operations, a SET operation during it the Memristor is switched from the HRS to the LRS by applying a voltage VSET of the adequate magnitude and polarity. However, during a RESET operation, a device in the LRS could return to the HRS by applying VRESET. Note that, VRESET is lower than VSET. MIM (metal-insulator-metal), Memristor affords several switching styles depending on its material stack.

2.3.3 Characteristics

Memristor devices specifically metal-oxide devices have unique characteristics and properties that will be leveraged for several applications, especially for security approaches. It should be noted that the definite characteristics manifested by a memristor rely on its material stack.

1. Non-volatility: *The device remembers its history.*

The resistance of a memristor depends on the history of current that had previously passed through the device that according to the governing mathematical relations. This means that the current resistance of the device relies on the amount of the electric charge that has passed through it besides the direction of flowing in the past [11]. It can be said that Memristors preserve their memristance value even if the device is powered OFF.

2. Bi-directionality: the bipolar memristors show identical I-V response irrespective of the applied stimuli polarity.

3. Formation process: a forming step (Vf) is required to initialize the memristor to the LRS in the most types of memristors. Before this process, the Memristor acts as a linear resistor.

4. Non-linearity: because of the time-dependent behavior of memristors, their I-V characteristics are highly non-linear.

5. Process variations: the memristance value of a memristor is changed by the fabrication process-variations that result from alterations in both the dimensions and dopant concentration. Moreover, the thickness of the memristor versus the memristance values is highly non-linear due to the effects of variation.

6. Temperature stability: in the case of a TiO₂ memristor, the LRS and HRS values are highly stable because the temperature coefficient of TiO₂ resistance is smaller than $-3.82 \times 10^{-3}/K$. Because of the change in dopant mobility, the switching speed of the memristor changes with the temperature.

7. Memristance drift: the memristance changes when applying a voltage across metal-oxide memristors, because of the movement of dopants that is denominated by memristance drift.

Except for non-volatility property, all of the memristor characteristics have a negative impact during the memory and logic circuits design. Although, these characteristics constitute points of strength in the security applications [2].

2.3.4 Memristor Fingerprints

Memristors should exhibit three characteristic fingerprints: [6], [41-43]

1-Memristors offer a unique signature “fingerprint” differentiated by a pinched hysteresis loop. In general words, the pinched hysteresis loop is a double-valued Lissajous figure of $v(t)$ for all time values, but the loop is pinched once it passes through the origin. As shown in Figure 2.6, the pinched hysteresis loop is restricted in the first and the third quadrants of the current-voltage plane. The pinched loop changes with both the frequency and amplitude of the periodic input “sinewave-like”. The abovementioned refers to what Chua said: “**If it is pinched, it is a Memristor**”.

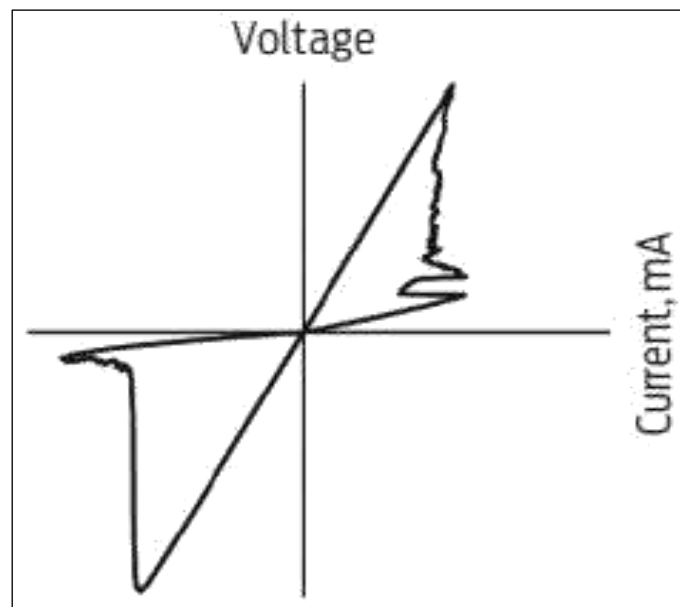


Figure 2.6: Memristor I-V pinched hysteresis loop [7]

2- As shown in Figure 2.7, the area of the hysteresis lobe depends on the applied signal frequency, which is considered the second distinguished signature of the memristor device. This behavior emphasizes that the pinched hysteresis lobe area reduces gradually when the periodic stimuli frequency rises and that occurs above a certain critical frequency. It is not a Memristor, if the hysteresis lobe area does not shrink with increasing frequency.

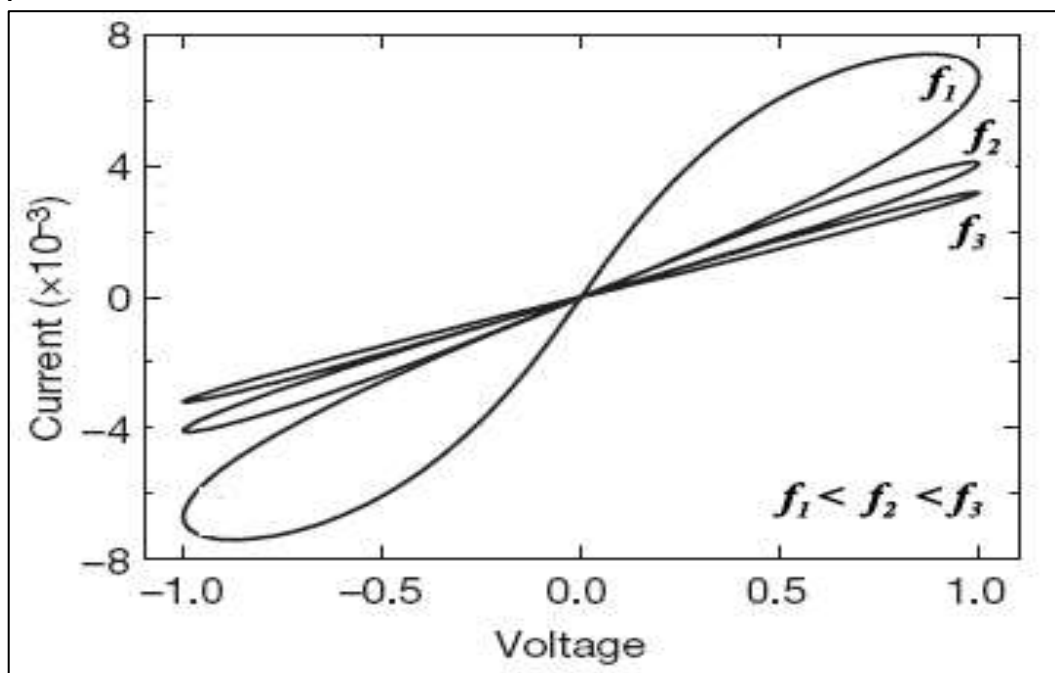


Figure 2.7: The hysteresis loop collapses to a straight line for high frequencies [8].

2.3.5. Switching Mechanism

Regardless of the device material and physical operating mechanisms, **Resistance Switching Memories Are Memristors** [5].

The memristive switching behavior based on the thin film MIM configuration has been described as the high impedance layer is constituted of one or more metal-oxides that have properties of a semiconductor. It can be said radically that, a MIM device should offer a set of internal resistance states to could act as memristor [4]. As illustrated in Figure 2.8, in metal-oxide memristors, resistive switching proven model is that the occurrence of the creation and rupturing of conductive filaments in the oxide layer that make the device to shift from the “OFF” state to the “ON”

state, and vice versa. (HRS) is generated due to the formation of filaments. Figure 2.8, represents a native insulator (HRS) in A, the creation of conductive filament by electroforming process in B, a SET process that is represent the ON state where HRS to LRS transition occurs in C, and the filament ending in a RESET process that is represent OFF state where LRS to HRS transition occurs in D.

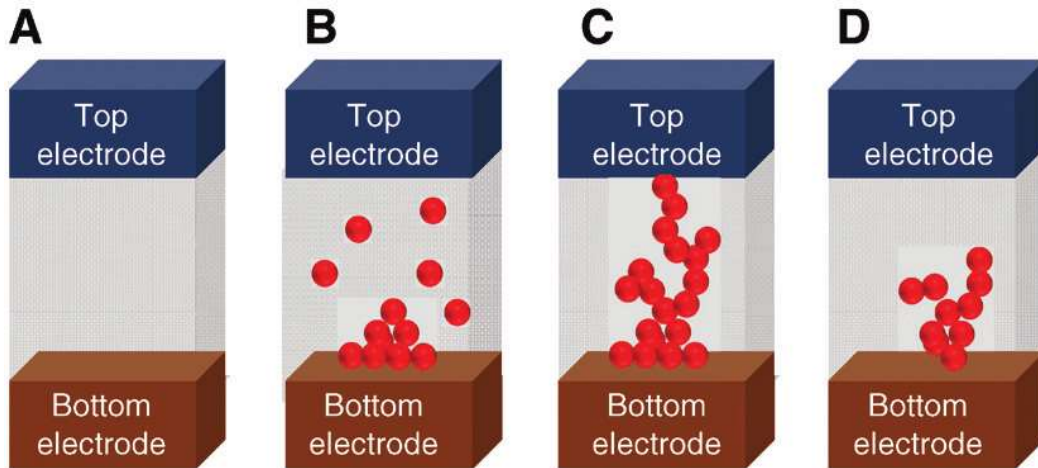


Figure 2.8: Schematic phases of resistive switching as stated by the filamentary conduction model [4].

The instantaneous resistive state of the device can be defined by different factors that play a key role like the compliance current and the applied electric field that can be controlled through the characterization of the device. Another restriction factor, like the gradient of species concentrations, temperature gradient inside the insulator layer, and electron mobility that relay on the semiconducting material solid-state properties. Therefore, the modification of the fabrication process is required for more tuning [4].

2.3.6 Memristor Switching Styles

There are two switching modes, “unipolar model” and “bipolar mode” that are generally recognized for Memristor devices, which are illustrated in Figure 2.9 (a) and (b) respectively [4].

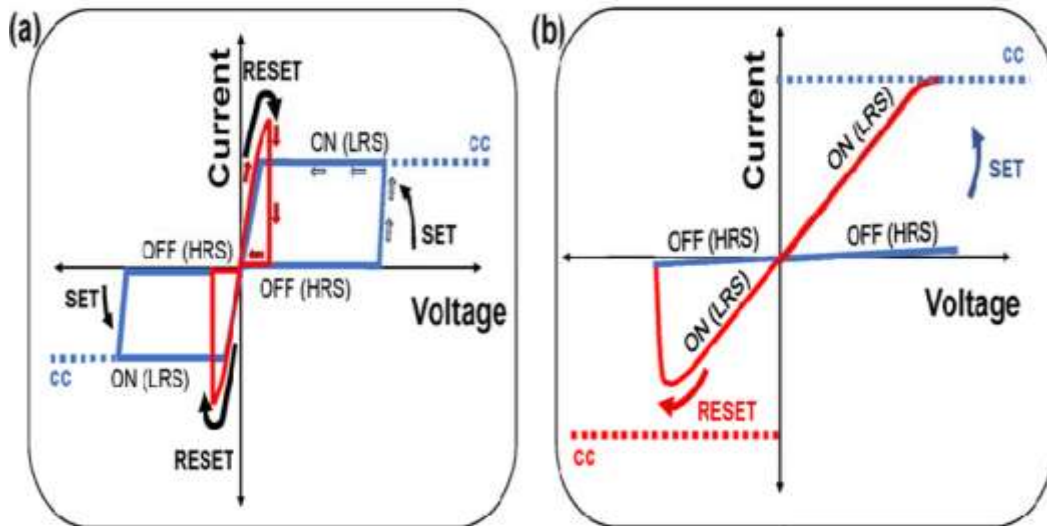


Figure 2.9: Schematic diagram of Memristor switching characteristics for (a) unipolar style ; (b) bipolar style [4]

Unipolar switching style (Figure 2.9. a), the resistance switching state relies only on the magnitude of the biased voltage. The ON state that is the SET process is achieved by applying a voltage that is higher than the magnitude of the voltage that needed to transit to the RESET state. The unipolar switching of metal-oxide memristors is depending on the Ohmic heating effect that is a key driving force. As stated by the sense, the SET and RESET switching is accomplished by the thermally motivated creation and rending of the nano-width conductive filaments over the entire oxide layer.

Bipolar switching style (Figure 2.9 b), the key requirement for switching the devices between ON (SET) and OFF (RESET) states is applying of opposite voltage polarities. Even though the resistance switching is electrically induced in each mode, the main motivation force relaying on the relationship of the Ohmic heating and electric field and on governing the filaments stability and formation. In most metal-oxide devices, bipolar resistive switching is observed.

Noteworthy, several metal-oxide systems including Mixed Unipolar/Bipolar Switching styles based on metal elements that present irregular simultaneous unipolar and bipolar switching modes. TiO_x , MoO_x , HfO_2 , AlO_x , and ZrO_x are examples of these metal-oxides. The current is the critical factor which determines whether the device is going through a bipolar switching regime or a unipolar switching regime that is usually at higher current than required in bipolar switching style [4]. In other words, the device is stated to be bipolar when VSET and VRESET are of opposite polarity. Otherwise, the device is stated to be unipolar when VSET and VRESET are of the same polarity. Nonpolar memristors exhibit bipolar and unipolar switching styles.

2.4 Memristor Modeling

Several models that described the Memristor were presented after the first model in 2008 [6]. These models were presented for simulating the memristive characteristics. The aforementioned models could be classified as in the following sections into Linear ion drift, nonlinear ion drift, Simmons tunnel barrier, and TEAM "ThrEshold Adaptive Memristor model".

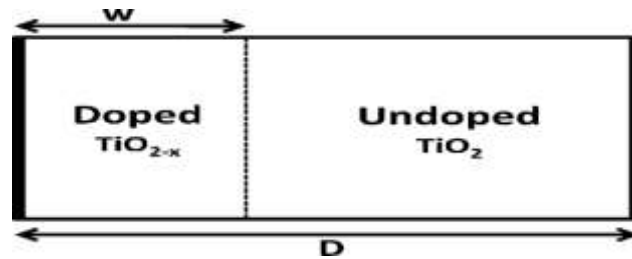


Figure 2.10: Linear ion drift model [9].

2.4.1 Linear Ion Drift Model

Figure 2.10 shows the linear ion drift model for memristive devices that is assumed in [7]. There is one assumption that is the Memristor device consists of two regions, doped and undoped. The first one of width w that works as the state variable. w contains a high concentration of oxygen vacancies dopants of TiO_2 namely TiO_{2-x} other region is an oxide region of originally TiO_2 , and its width formed to $(D-w)$. The sum of the resistance of both regions represents the total resistance of the device. Hence, it is obvious that the device is modeled as two series resistors. The actual memristance relies on the ratio between the state variable $w(t)$ and D , which is the thickness of the device [6]. HP lab Team issued results that characterized the Memristor device as the above-mentioned in equations (2.7), (2.8) that stated the relationship between the current and the voltage as a pinched hysteresis form.

$$v(t) = \left(R_{on} \frac{w(t)}{D} + R_{off} \left(1 - \frac{w(t)}{D} \right) \right) i(t)$$

$$\frac{dw(t)}{dt} = \frac{\mu_v R_{on}}{D} i(t)$$

The w value is within the interval $[0, D]$; this means that w within the boundaries of device dimensions.

In the Linear Ion Drift model, featured assumptions like; ion drift in a uniform field and ohmic conductance are taken into consideration [9]. In addition, the assumption that the vacancies are free through the device length is introduced [6]. At any situation, it is not valid, for the trouble that the vacancies slow down at the boundary. Hence, there will be no vacancies along the device and the doped region length equal to zero, which is meaningless if the dopants move through the whole device. A window function ($f(w)$ or $f(x)$) is raised to overcome this problem. The derivative of w is multiplied by a window function to prevent w from growing beyond the physical device size. Therefore, it can be said that the equation (2.8) forces to be zero when w at boundaries by using the multiplication of (2.8) by a window function that nullifies the derivative.

2.4.2 Nonlinear Ion Drift Model

The behavior of the implemented memristors is highly nonlinear as studies and experiments have proved so the linear ion drift model is not accurate enough [6, 9]. The nonlinear ion drift model suggests that voltage-controlled memristor. Furthermore, unsymmetrical switching is taken into regard. Voltage and state variable derivative relationship is nonlinear. I-V relationship and state variable derivative are expressed as:

$$i(t) = w^n(t) \beta \sinh(\alpha v(t)) + \chi [\exp(\gamma v(t)) - 1] \quad (2.11)$$

Where α , β , γ , χ are fitting parameters, n restricts whereby the current could be affected by the state variable and w is set within the interval $[0, 1]$

$$\frac{dw}{dt} = \alpha \cdot v^m(t) \cdot f(w) \quad (2.12)$$

Where $f(w)$ is a window function, α and m are constants.

2.4.3 Simmons Tunnel Barrier Model

As shown in Figure 2.11, the device consists of a resistor and a tunnel barrier in series connection, in a more accurate physical model that was introduced in [44]. V is the applied voltage; X is the state variable, v is the internal voltage in the device. Note that, the state variable X is referred to as the Simmons tunnel barrier width. Unsymmetrical switching and nonlinear behavior are assumed in this model, due to an exponential movement dependency of the dopants.

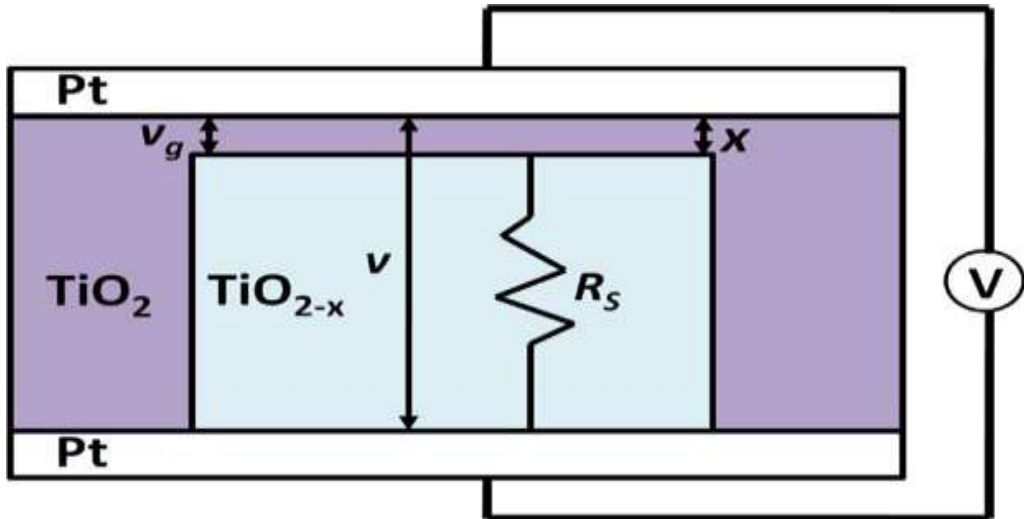


Figure 2.11: Simmons tunnel barrier memristive device Physical model [9].

2.4.4 TEAM "ThrEshold Adaptive Memristor" model.

It is worth mentioning that the Simmons tunnel barrier model is considered the best achievable model of a TiO_2 Memristor. However, the Simmons model is counted as a very complicated model; it fits only a specific type of memristive device and presents an ambiguous relationship between current and voltage. A computationally complex inefficient model of the Simmons model is proposed. Therefore, because of the aforementioned disadvantages, a computationally efficient Memristor device model, based on modification and simplification of the Simmons Tunnel Barrier Model with simpler expressions is proposed. A simplified model represents simpler mathematical functions and the same physical behavior is The TEAM model. For analysis simplification and computational efficiency, this model based on two of assumptions;

- (1) Below a certain threshold, there is no change in the state variable,
- (2) A polynomial dependency between the current and the state derivative instead of exponential dependency.

Change in the resistance is an exponential dependence on the state variable. Under this assumption:

$$v(t) = R_{ON} e^{(\lambda/(x_{off}-x_{on})(x-x_{on}))} \cdot i(t) \quad (2.13)$$

where λ is a fitting parameter, and R_{ON} and R_{OFF} satisfy the following ratio:

$$\frac{R_{OFF}}{R_{ON}} = e^{\lambda} \quad (2.14)$$

It should be noted that The TEAM model is simple, flexible, and general. TEAM model is appropriate for circuit design and has been implemented in Verilog- A. A Verilog-A model is more efficient in terms of computational time than a SPICE macro model while providing similar accuracy.

Table 2.1: A comparison between the four memristor device models submitted in [9]

<i>Model</i>	<i>Linear ion drift</i>	<i>Nonlinear ion drift</i>	<i>Simmons tunneling barrier</i>	<i>TEAM</i>
State variable	$0 \leq w \leq D$	$0 \leq x \leq 1$	$a_{off} \leq x \leq a_{on}$	$x_{on} \leq x \leq x_{off}$
Control mechanism	Current	Voltage	Current	Current
I-V relation	Explicit	Explicit	Ambiguous	Explicit
Memristance relation	Explicit	Ambiguous	Ambiguous	Explicit
Generic	No	No	No	Yes
Accuracy	Lowest	Low accuracy	Highest	Sufficient
Threshold exists	No	No	Yes	Yes

2.5 Memristor-Based Applications

Regarding the memristor characteristics that have been discussed in section 2.3.3, it can be said that due to low-power and ultra-fast switching capabilities, nonlinearity, and unpredictable behavior variations, nanoscale geometry memristors are researched as future alternatives to memory in analog and digital applications.

In addition, the memristor is a preferable choice in security solutions due to its unique electrical response from each memristor type. The memristor is well applicable for random number generation and encryption as a nonlinear device. In the following subsections, some of the memristor applications are presented:

2.5.1 Digital Applications

Memory is the most remarkable application of a memristor. The capacitors are reestablished with memristors in DRAM where a single bit of data can be stored [39]. In addition, emerging non-volatile memories such as Memristor-based resistive RAM (ReRAM) provides many advantages such as scalability, energy efficiency, density, CMOS compatibility [19]. Usage of a memristor as a configurable switch in FPGA is considered as one of a famous logic application of memristors, and also use it in connecting the CMOS-logic gates. Logic circuits are another digital application of memristor, where it is used as a standalone logic gate or in hybrid CMOS circuits.

2.5.2 Neuromorphic Circuits

As shown in Figure 2.12, Memristor plays a very important role in synapse simulation with minimal power.

Brain-inspired computing models back to the earliest days of modern computing [18]. Moreover, Carver Mead coined “neuromorphic” in the late 1980s to describe analog CMOS circuits; he was then investigating to model biological neural systems. Neuromorphic computing has been refreshed by the appearance of Memristor, which in many ways naturally behaves as an artificial synapse. The neuromorphic system is a mixed system emulating neural architecture to neurons pattern by emulating, simulation, and computation in real-time.

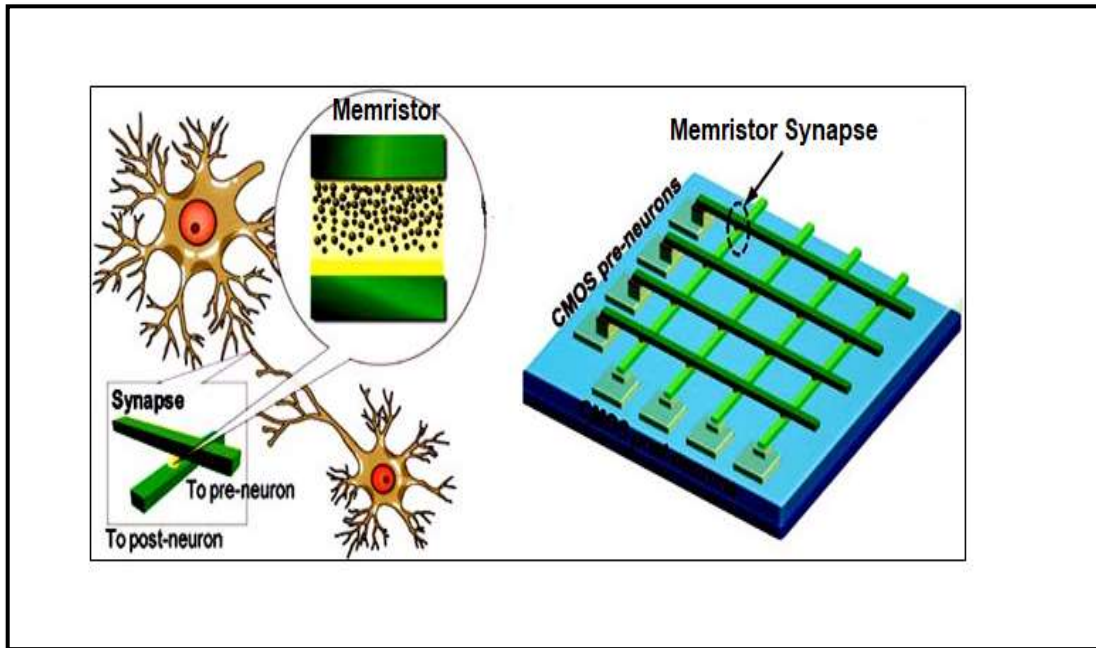


Figure 2.12: Schematic illustration of using memristors as synapses between neurons [6]

2.5.3 Analog Circuits

Analog computation and circuit Applications such as Memristor-Based Sinusoidal Oscillators that are considered the most common oscillator circuits where some or all resistors are replaced with memristors [6]. Besides, Programmable Analog Circuits, Loop Filter of Phase-Locked Loop and Adaptive Filters are Memristor-based analog circuits.

Note that, in the next chapter, Memristor- based hardware security applications will be discussed in detail by presenting the contribution in literature during the last few years

Chapter 3: Memristor-based Hardware Security solutions (contributions in the literature)

3.1 Background

Hardware-related security research is often referred to as hardware implementations of cryptographic algorithms where hardware is utilized to improve the calculation performance and efficiency for cryptographic applications. For quite a while, cybersecurity specialists have confidence in that the integrated circuit (IC) supply chain was well-secured. Due to the increasing in design complexity of modern system-on-chip (SoC) platforms and the high cost of cutting-edge foundries, the IC supply chain, has been spread everywhere that was situated in one country or even in one company [15]. This globalization of the Integrated Circuits (ICs) supply chain has raised security concerns on how to grantee the trustworthiness and the integrity of the fabricated circuits [17]. In light of these rationales, a variety of hardware security primitives have been sophisticated in the last few years, aimed at mitigating issues such as integrated circuit (IC) piracy, counterfeiting, and side-channel Analysis [12].

The core properties of hardware devices that hurt the circuit performance are utilized for security applications [15]. One remarkable example in this field is the Physical-Unclonable Functions (PUFs) that depending on the device process variations in generating chip fingerprints in challenge-response pairs. Researchers are developing the use of memristor and emerging transistors, like the spin-transfer torque (STT) device by leveraging their properties for hardware security applications. As technology scaling down into the nanometer scale, emerging nanoelectronic technologies have become a great value in several technologies of next-generation computing. Emerging non-volatile memory (NVM) technologies, including resistive RAM such as Memristor, RRAM and ReRAM, phase-change memory (PCM), and spin-transfer-torque magnetic RAM (STT-MRAM) are not finite to nonvolatile memory, but also in developing computing-in-memory (CIM) for artificial intelligence (AI) chips, nonvolatile logics (nvLogics) for nonvolatile processors, and in implementing security circuits for the internet of things (IoT) [16]. At the intersection between Nanoelectronics and security, many solutions of nano-based security primitives are proposed [12].

3.2 Rationales for Memristor-based Hardware Security Primitives

CMOS is shrinking periodically according to Moore's Law from 1960s in few micrometers to nowadays in tens of nanometers. In order to continue the miniaturization of circuit elements, several alternatives to building ultra-dense circuitry are investigated. Memristor is one of these nanoelectronic alternatives [12] that can be considered a basic nanoelectronic circuit element that has been approached for several hardware security applications due to several unique characteristics and properties like: bidirectional and the nonlinear input-output response, unique device forming step and inherent non-volatility combined with temporal drift. These unique characteristics lead to the use of these devices in several applications including key exchange, authentication, time stamping and bit commitment [11]. In addition, CMOS -Memristor hybrid circuits have been presented as hardware security primitives due to the intrinsic controlled sensitivity of process-variations [14]. What provides memristors a unique advantage over many other nano-devices is the compatibility with modern CMOS manufacturing technologies. It is important to be noted that every memristor device has unique current-voltage characteristics due to that the memristor behavior is highly influenced by the material stack that is used for fabrication [12]. For instance, (Metal -oxide TiO₂, HfO₂, etc.) substrate (MIM) memristors offer similar behavior, however other memristor types have different internal physics regard to their material stack like magnetic, and spintronic memristors .

Memristor-based designs are predicted to occupy a small area and use a fewer number of transistors than CMOS implementations [12]. To improve these aforementioned features, two-dimension crossbar arrays make use of space is very effective. As shown in Figure 3.1, the crossbar array consists of two-terminal memristor devices at the crosspoints of perpendicular nanowires that improved area efficiency. Hence, it can be said that Memristor is a preferable candidate in security applications due to the unique electrical response from one type of Memristor to another. Consequently, the response of individual devices is difficult to predict by a specified mathematical model. Hence, it is a challenge to predict the memristor response that is integrated into the hardware implementation [25].

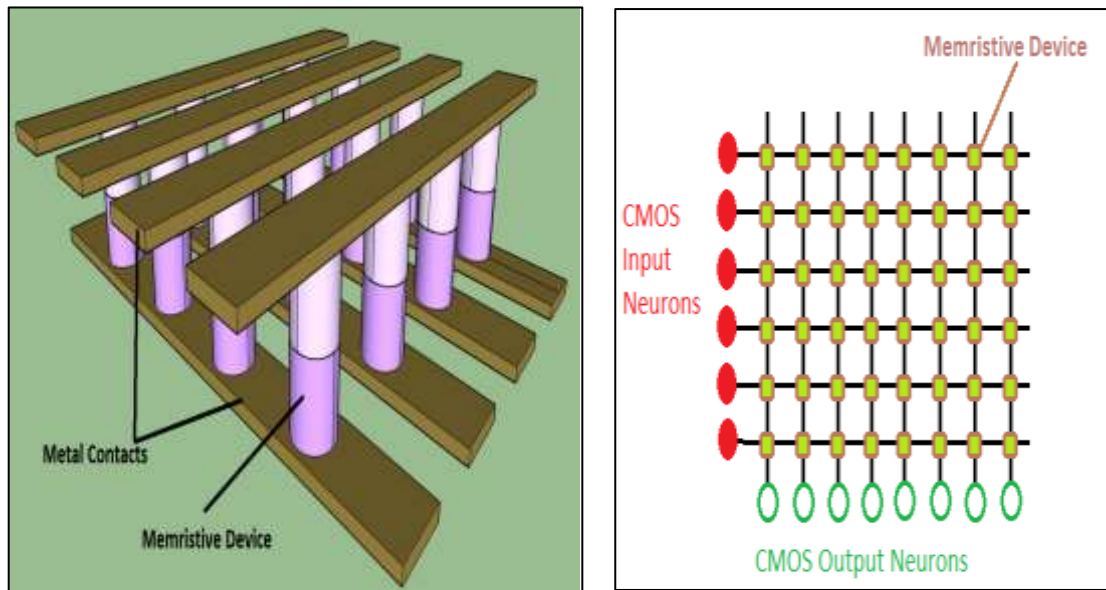


Figure 3.1: Crossbar array of memristors [45]

Memristor has emerged as a Security primitive promising candidate in Physical unclonable function (PUF) implementations [13]. The Memristor technologies provide an excellent opportunity to PUF circuits with desired statistical properties, energy-efficient, and engineer dense. In general, (PUFs) generate fingerprints or unique signatures by exploiting the process variations. These unique signatures can be used for secret key generation or authentication. PUFs provide unique challenge-response pairs that can be used as the authenticating signatures for that chip where the PUFs are implemented on it.

Memristor-based PUFs as hardware security primitives have lower area compared to CMOS-only. Furthermore, since Memristor are bidirectional devices, whereas MOSFET is a unidirectional device, Memristor-based PUFs are predicted to strongly resist the violation models than purely CMOS-based PUF implementation [14]. The common structure of nanoelectronic implementations is XbarPUF where the memristive crossbar is used in its construction [12]. A variety of nanoelectronics security primitives have been developed, like as, nanoelectronic public PUF (NanoPPUF) by the use of memristive crossbars.

3.3 Memristor - based Secret Key Generation (Literature contributions)

By referring to the above mentioned in sections 3.1 and 3.2, Memristor as an emerging nanoscale technology offers great potential for building energy-efficient and small-scale hardware, including emerging security primitives [20]. Memristor devices offer unique characteristics such as nonlinearity and unpredictable behavior variations. As aforementioned in the previous section, the variation in electrical response from each memristor type makes memristor a preferable candidate in security solutions. Memristor-based physical unclonable functions (PUFs) has been investigated widely in the last few years as memristive security primitives that use the significant resistance variations of the memristive crossbar [21].

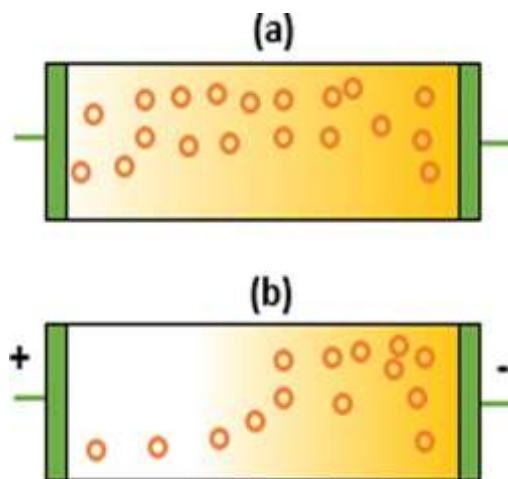


Figure 3.2: Schematic of a memristor device.
(a) Initial oxygen vacancies profile.
(b) The obtained new profile after applying a certain voltage for a certain time. [22]

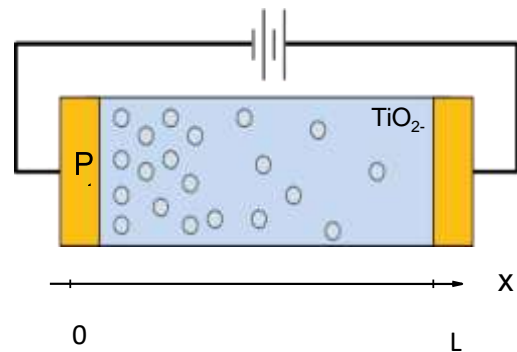


Figure 3.3: Conceptual geometry for an oxide memristor [24]

The work proposed in [22], only one Memristor device has been used instead of a complex crossbar circuitry. This work depends on extract master and session keys from two identical Memristor devices. The key generation techniques can be accomplished by monitoring and tuning the vacancies profile in the device and then the resultant profile could be digitized according to the required key size.

Figure 3.3 represents a schematic of oxide Memristor where the TiO₂ thin-film oxide layer is sandwiched between two metals. Figure 3.2 (a) shows an instance of an initial profile of the oxygen vacancies. It is possible to control the mentioned profile during the fabrication process.

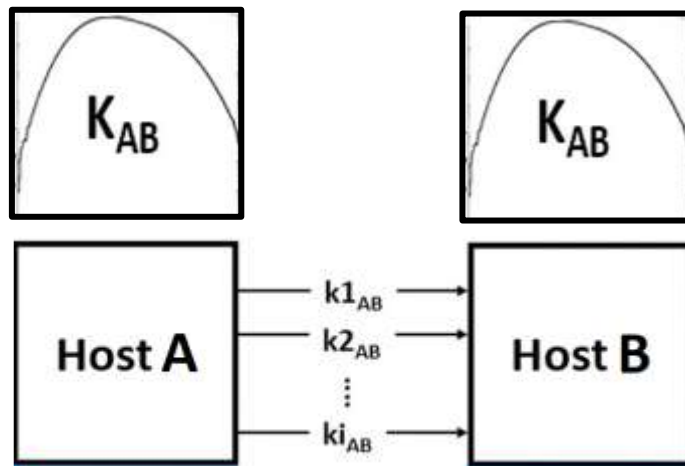


Figure 3.4: Host A and B communication scenario [22]

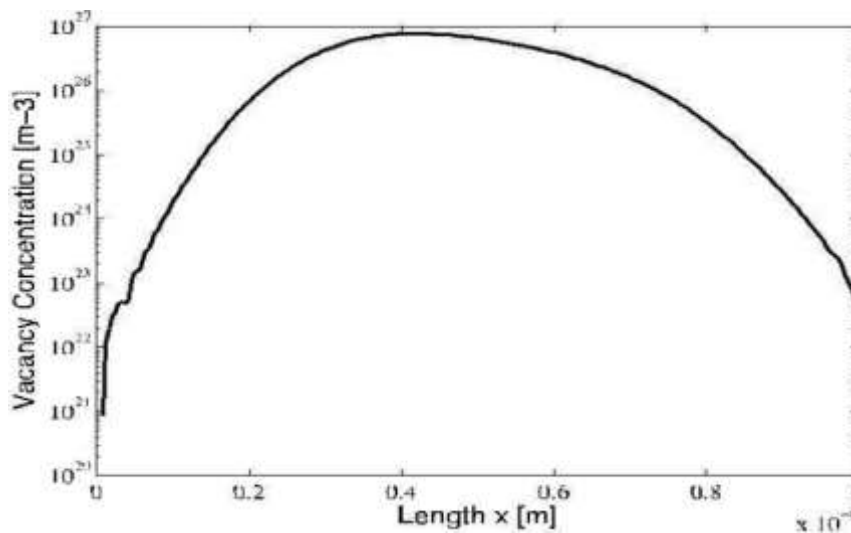


Figure 3.5: initial vacancies profile for TiO₂ [22]

The oxide vacancies will migrate through the device when applying a bias voltage between memristor terminals. And therefore when applying a certain voltage for a certain time duration a new profile can be obtained as shown in Figure 3.2. (b).

It can be said that it is possible to obtain a number large of vacancies redistribution under different values of an electric field for different periods [23].

If it is assumed that L is the length of the memristor device as in Figure 3.3 and the vacancies migration can be considered in a 1-D direction where no lateral of vacancy migration or concentration [23]. The nonlinear physics-based mathematical model presented in [23-24] describes the behavior of memristive devices. The infinite number of possible initial vacancy profiles of the initial profile are obtained as shown in Figure 3.5. The initial profile suggested being digitized to generate the master key that will be extracted. A new profile can be achieved by changing the voltage and time, which is assumed to be used to generate a session key. Memristor's initial profile as master key K_{AB} is proposed as an encryption process base [22]. As an example that is shown in Figure 3.3, It is assumed that when the two hosts A and B want to communicate securely, A and B should share a secret initial profile that is used as a master key which its size can be controlled and determined by the hosts. With every different value of voltage and time, it is possible to generate a new unique profile due to the characteristics of the Memristor. As illustrated in Figure 3.4, session keys $K1_{AB}, K2_{AB}, \dots, Ki_{AB}$, can be generated In the security approach that is supposed in [22]. The presented approach depends on the extraction of the master and session keys and it is supposed that hosts have identical devices but due to the fabrication process variations is considered a challenging process. Therefore, the generation of identical keys for encryption and decryption at the communicating peers is considered a challenge.

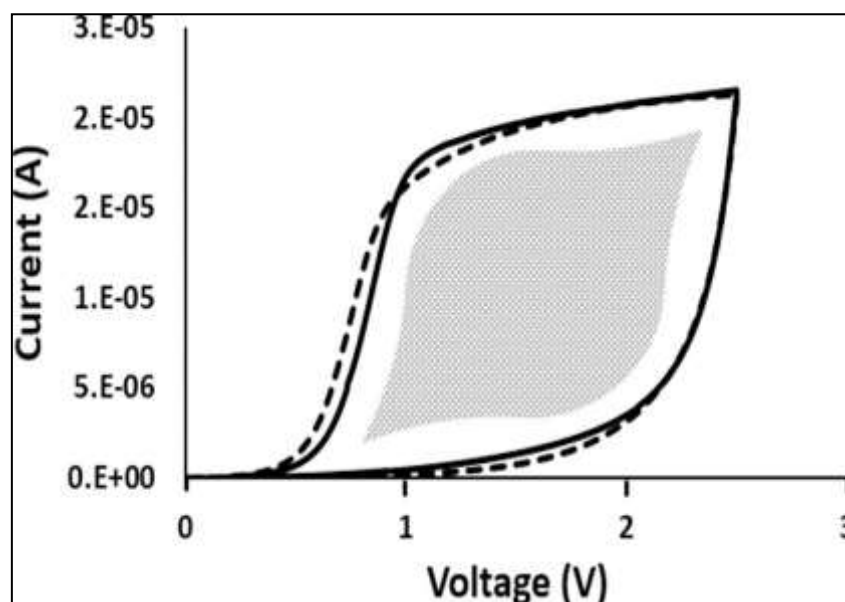


Figure 3.6: Initial profiles (master keys) generated using identical Memristor devices [22]

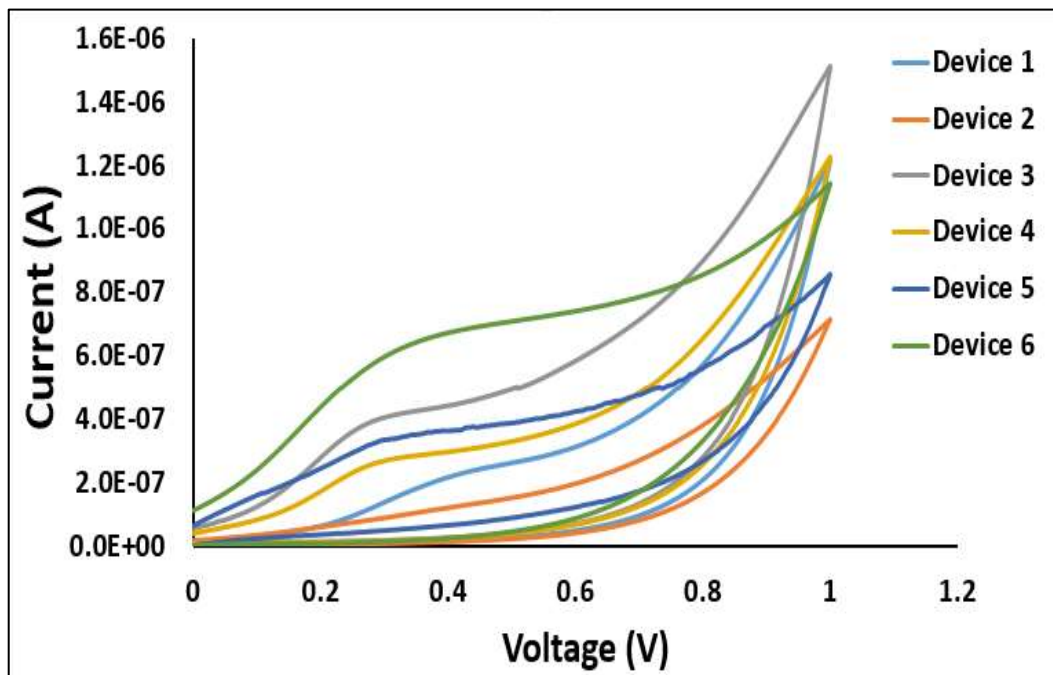


Figure 3.7: Electrical characteristics of different fabricated Memristor devices. [25]

It is postulated that the keys are extracted in the shared area under the I-V curve of the identical Memristor devices, to overcome this issue as shown in Figure 3.6 to accomplish a similar encryption and decryption keys, which requires extra computational operations.

An alternative work in [25, 26] presented a new postulate depending on the uniqueness of the Memristor device. In this approach, a secure technique for two different communication peers based on generating unique keys is proposed by exploiting the advantage of the fabrication process variations.

It can be said that, by using similar starting material and processing conditions for different memristor devices through the same process, unique I-V characteristics can be generated as shown in Figure 3.7, that can be exploited to generate unique keys based on the required key size, by digitizing the I-V curve. The key can be generated, depending on the encryption algorithm used. It is worth noting that, a powerful feature is that I-V characteristic previous states cannot be retrieved that is used to generate session keys in this communication technique securely.

The suggested technique relies on initiating communications between the communicating peers through a third trust party (TTP). As a general definition, TTP in cryptography is a component that manages the interactions between two other parties, TTP revises all critical communications operations between these parties. As an example, the TTP authentication protocols used to implement Mobile Agent System (MAS), which can migrate between platforms, executes its code autonomously and hold consumers' requests. To make the owner right decisions, the agent is required to return results to its owner [27].

In the proposed Memristor – based security approach that is presented in [25-26], each device and Third Trusted Party (TTP) has its memristor that will result in unique I-V characteristics for each device, as shown in Figure 3.8. Furthermore, to communicate with the TTP, A and B have an initial secret Key (K_{AT} and K_{BT}). As previously mentioned, the presented technique benefits from the uniqueness property of the Memristor devices to generate session keys [4]. To describe the proposed technique when a device A would like to share messages secretly with B, the following steps should be executed:

- 1- At the start, host A communicates with the TTP to inform it with the address of the peer who wants to initiate a communication with it. A generates a timestamp T_A . By using K_{AT} , T_A , A, B, and TTP are encrypted.
- 2- TTP checks the message that is received from A, then session key K_{AB} will be generated by TTP memristor. To send the session key K_{AB} , TTP uses K_{AT} and K_{BT} .
- 3- After A receives session key K_{AB} , a new secure session key K_{ABnew} will be generated after the creation of t_{AB} and V_{AB} using its memristor. After that A sends B a message to share the newly generated K_{ABnew} and to verify the used session key.
- 4- At the last step, B returns another message to inform A about the awareness of the future session key.

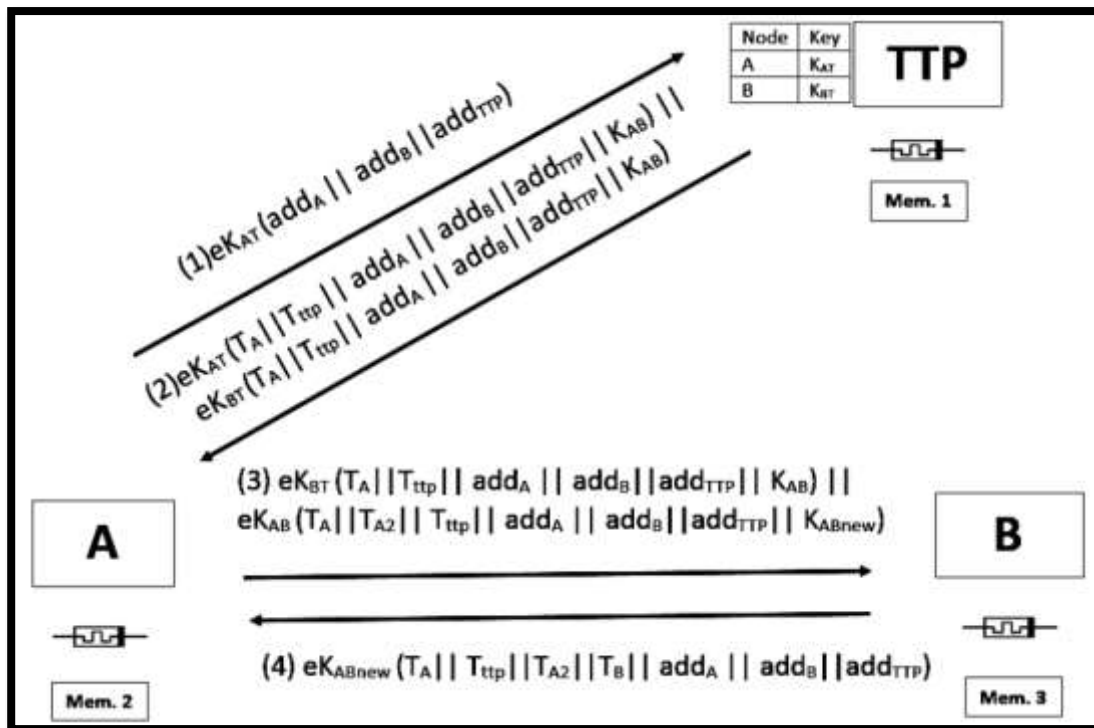


Figure 3.8: Memristor- based security approach, Host A and B can initiate communication through TTP.[25]

Table 3.1: the acronyms and definitions used for the proposed security technique that submitted in [25].

Acronyms	Definition
KAB	Unique secret key generated by TTP to share information between node A and B
KABnew	Unique secret key generated by A to share information between node A and B
KAT	Secret Key between TTP and node A
KBT	Secret Key between TTP and node B
vAB	Voltage generated at TTP to initiate key between node A and B
tAB	Time generated at TTP to initiate key between node A and B
Addi	Address of node i
Ti	Timestamp generated at node i
eK	Encrypted with key K

Chapter 4: Memristor-Based AES Key Generation for Low Power IoT Hardware Security Modules. (Proposed Module)

4.1 Introduction

In the last years, lightweight symmetric ciphers have acquired importance because of rising the need for security services in constrained computing environments, for instance in the Internet of Things [28]. Internet of Things (IoT) is a wireless network of interconnected devices such as wearable devices, transportation, and appliances that enable these objects to exchange information [29]. In addition, IoT always includes ordinary devices such as thermostats and kitchen appliances developed with computational power to allow communication through the internet [21] as shown in Figure 4.1. Privacy and security concerns are two main challenges on the designer's road especially for low power IoT devices because of the growth of IoT systems [29].

The encryption used to secure confidential information by performing effective schemes depending on complex cryptographic mathematics [29]. Generally, IoT devices are wireless; operate using limited battery supply. Specifically, it can be said that the resource limits of the IoT devices direct to the demand for security techniques that depend on the area-efficient hardware security primitives and consume little power as possible [21]. Security solutions are implemented using nanoelectronic security primitives and nano-enabled security protocols, to obtain robust IoT security with minimal power overhead and small area. The emerging nanoscale technologies like Memristor, Carbon nanotubes, graphene presents the capability for constructing energy-efficient and small-scale security techniques.

As an affirmation of what was mentioned previously, Memristor as an emerging nanoscale technology offers an excellent candidate for small-scale and energy-efficient hardware implementations and emerging security primitives [20]. Memristor devices offer unique characteristics such as nonlinearity and unpredictable behavior variations. In addition, Memristors are CMOS compatible, offer high retention time, and multilevel resistances. The response of individual memristors devices is difficult to predict by a specified mathematical model due to unique electrical responses from one type of memristor to another.

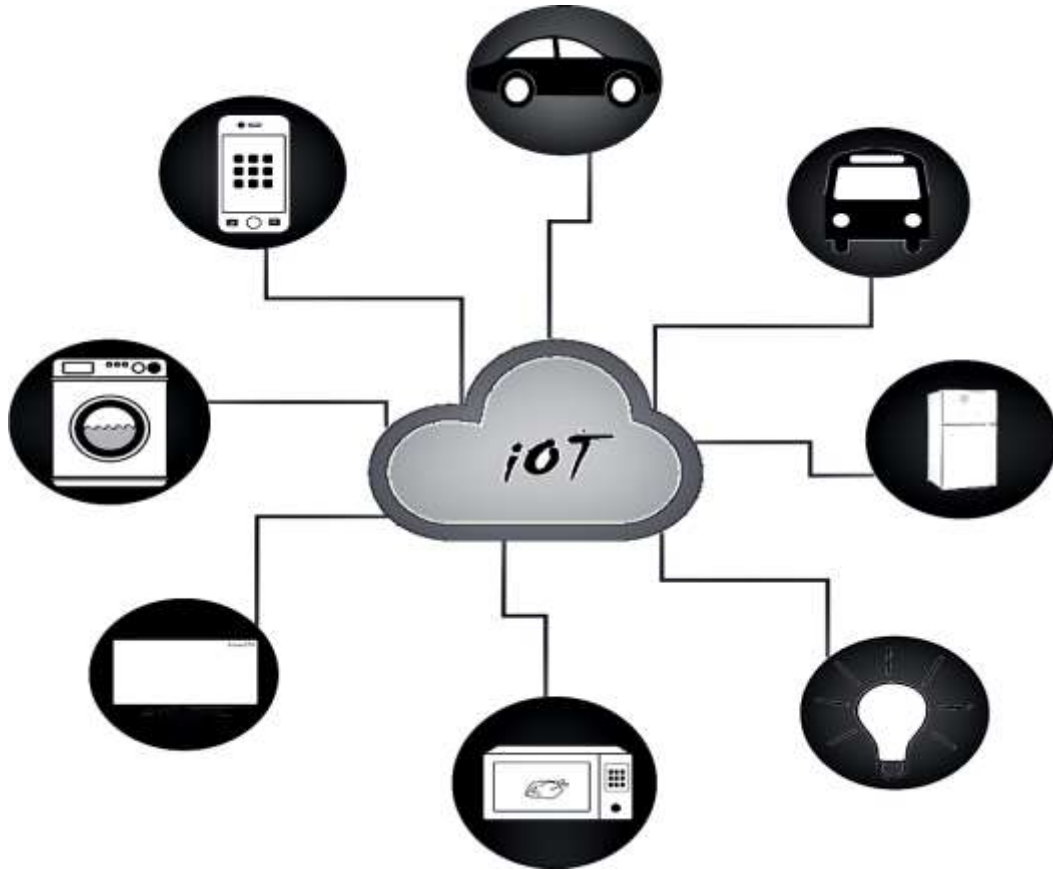


Figure 4.1 Internet-of-things (IoT) paradigm [18]

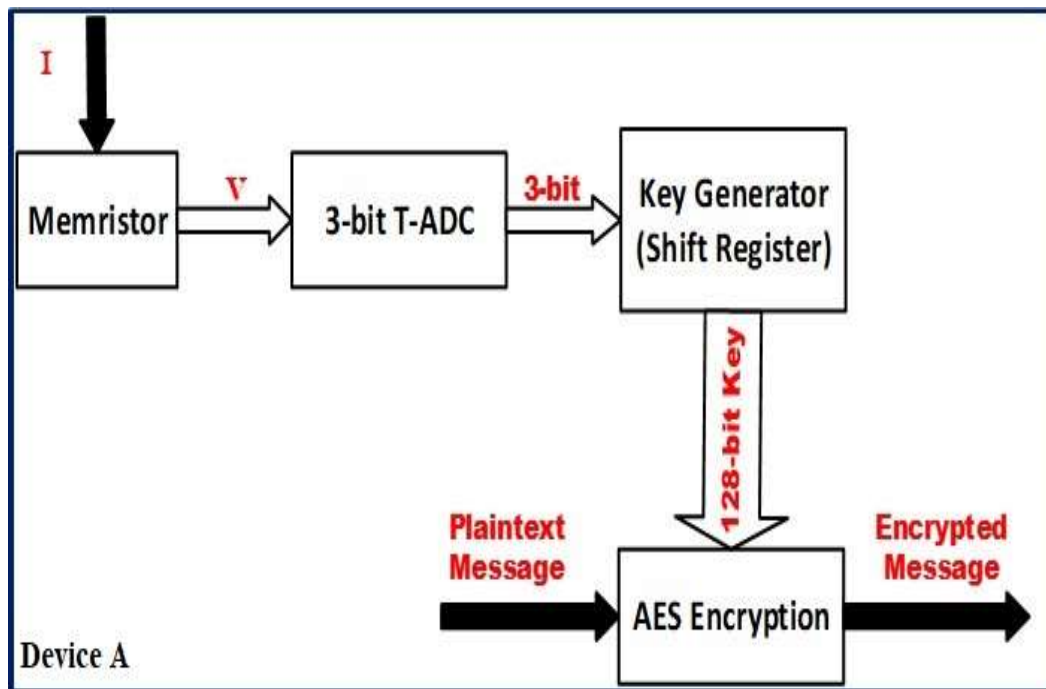
Based on the above-mentioned unique characteristics of the Memristor device, a hardware security module (HSM) based on the memristive key generation scheme is presented. This scheme depends mainly on the uniqueness property of the electrical characteristics of the Memristor devices. The generated Memristor-based key is used through AES encryption and decryption processes.

AES (Advanced Encryption Standard) cryptographic algorithm has proved its immunity against attacks. AES has become the perfect choice for various applications, including not only wireless standards such as Wi-Fi, ZigBee, and WiMAX but also, the security of smart cards and bit-stream security applications [30].

The following section presents the proposed module to generate Memristor-based AES Key for IoT hardware security with a detailed explanation of each block and its role in the proposed key generation process.

4.2 The Proposed Module

(a)



(b)

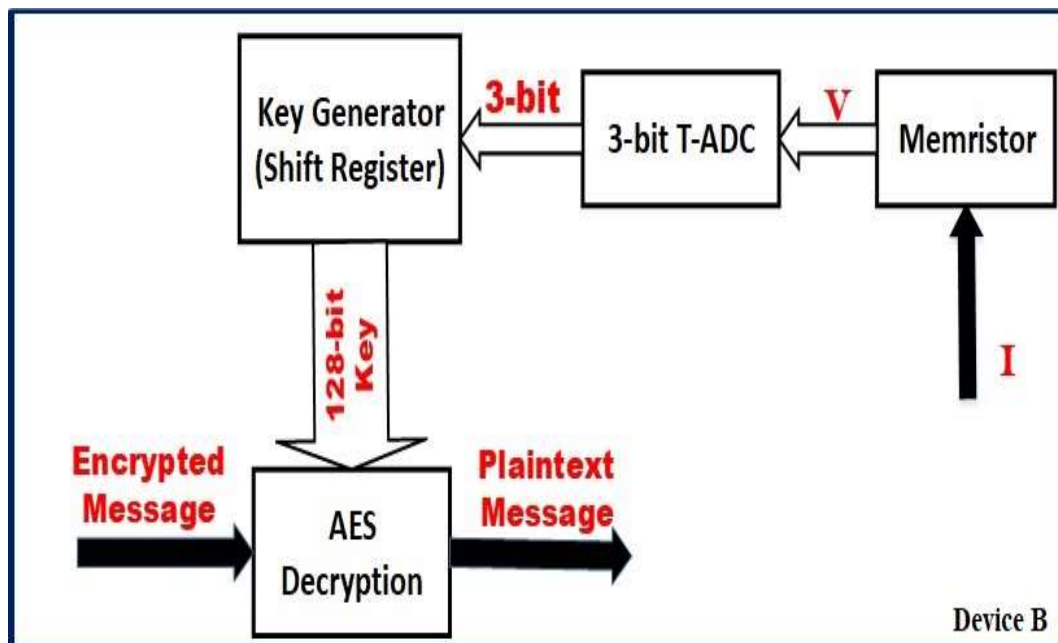


Figure 4.2: The Proposed Module (a) Encryption process at Device A.
(b) Decryption process at Device B.

The proposed module illustrated in Figure 4.2, presents a hardware security module based on generating a Memristor-based AES key. The key generation process passes through three stages that are executed by cascading three blocks:

- 1-Memristor to get a unique I-V characteristic curve by sweeping the input current.
- 2-The second block is 3-bit T-ADC that is used to digitize the I-V curve.
- 3-The third block is a shift register to generate the 128-bit key, which is used as AES symmetric key.

The following subsections discuss the operation and characteristics of each block:

4.2.1 Memristor- Based I-V Characteristics

The most important characteristic of a Memristor is the current-voltage characteristic, where it exhibits a pinched hysteresis loop as discussed in chapter 2. It is said to be pinched at the origin if it always passes through the origin at all-time instants when the input signal waveform (current or voltage) is zero regardless of the internal state variables w . Due to this unique behavior of Memristor, hardware security has a potential application based on Memristor.

4.2.2 Time-Based ADC

A 3-bit T-ADC is used to digitize the Memristor I-V characteristic curve. Figure 4.3 shows that the Time-based ADC (T-ADC) composed of two phases, as shown in Figure 4.3, a Voltage-to-Time Converter (VTC) and a Time-to-Digital Converter (TDC). The time- based ADC converts the analog signal to a time-represented delay signal through a (VTC) and then the time-represented signal is converted to digital thermometer code through a Time-to-Digital Converter (TDC). A thermometer-to-binary conversion is then performed to produce the binary output.

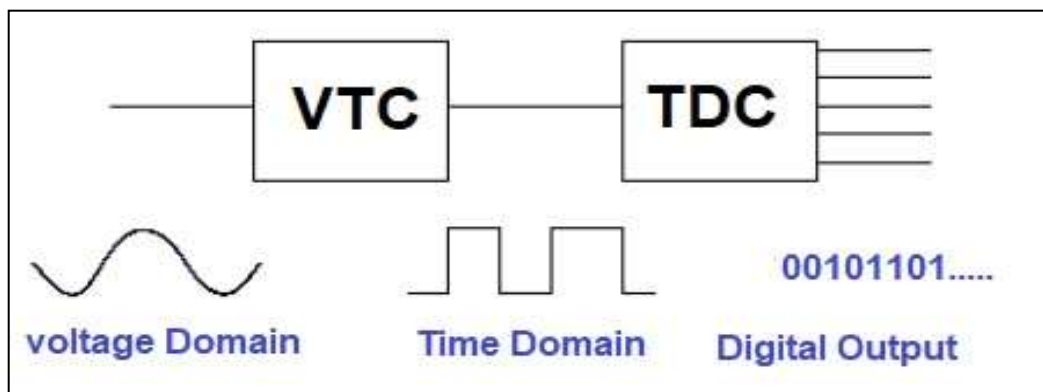


Figure 4.3: T- ADC architecture [31]

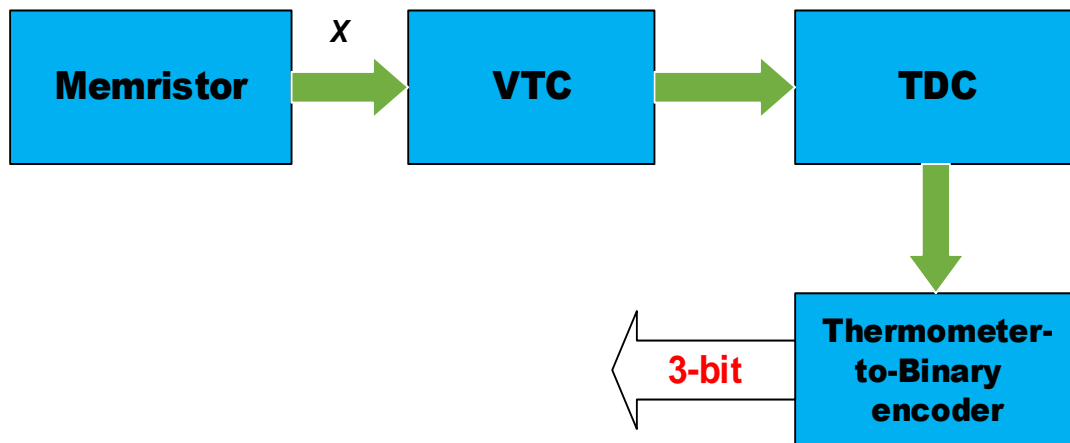


Figure 4.4: Block diagram of digitizing Memristor I-V curve.

The first stage is VTC to convert the analog voltages as a result of sweeping the Memristor input current to pulse delay through a voltage to time converter (VTC). The basic circuit that can be used to implement this function is the starved inverter as illustrated in Figure 4.5, the memristor output voltage at 'X' is the input voltage that controls the delay of the falling edge of Vclk; through the inverter that consists of two transistors M4 and M5, by Controlling the discharging current of transistor M3 [31].

The second stage is the TDC (Vernier delay line) circuit, which is responsible for the conversion of the output delay from the starved inverter into the thermometer code through time to digital converter using the Vernier delay line [32]. This Vernier delay line consists of two parallel delay chains and a sense amplifier based on the D-flip flops as shown in Figure 4.6. The start and stop signals transfer through the two delay lines until they aligned. If the start signal comes first the produced output is "1" and the output is "0" otherwise. Hence, the D-flip flops sense amplifier is used to determine which of the two signals comes first to generate the thermometer code. Principally, the numbers of flip-flops are calculated by the formula: $2^n - 1$; where n: the number of bits of T-ADC, thus for 3-bit T-ADC, 7 D-flip flops are used to generate a thermometer code for values from '0' to '7'. A thermometer-to-binary encoder is then used to produce a 3-bit binary output.

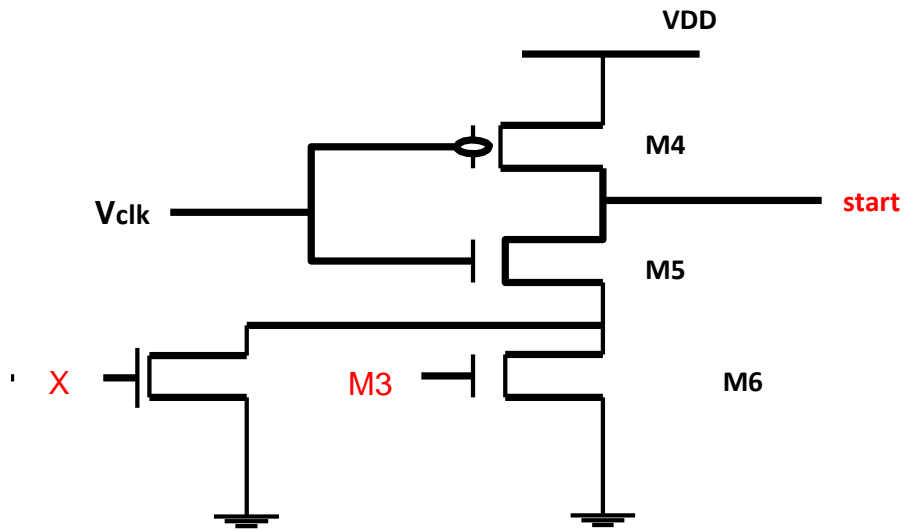


Figure 4.5: The starved inverter

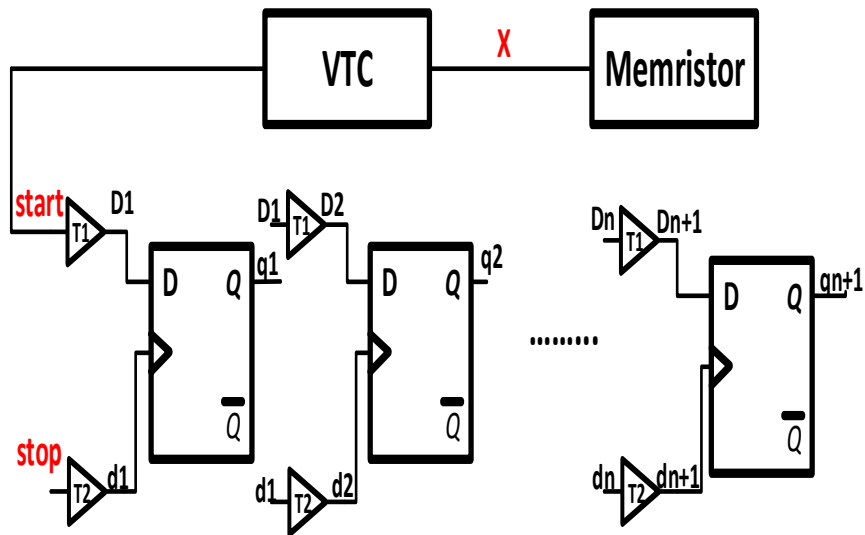


Figure 4.6: Implementation of the Memristor I-V characteristic curve digitization process by using the two stages of T-ADC, VTC, and TDC.

4.2.3 Key Generator (SIPO Shift Register)

To generate the 128-bit required key, every 3-bit from T-ADC could be applied serially to 128-bit Serial-in to Parallel-out (Right Shift) Shift Register through a multiplexer as illustrated in Figure 4.7.

The T-ADC output is fed serially through a Multiplexer to the shift register inputs as in Figure 4.8. The inputs of all flip-flops except the first flip-flop FF1 are driven by the outputs of the prior ones. For instance, the input of FF2 is motivated by the output of FF1. In the right-shift SIPO shift-register, data bits shift from left to right for each clock tick as illustrated in Figure 4.9 where $n = 128$. This type of shift register has stored data within the register that is provided as a parallel-output data word (Data out) at the individual output pins of the flip-flops (Q1 to Q128)

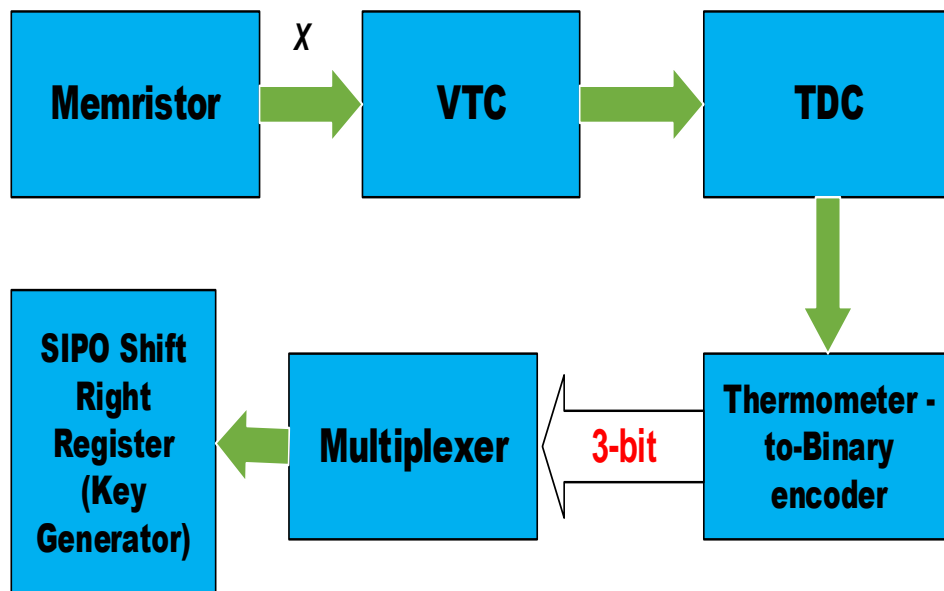


Figure 4.7: 128-bit key generation Block Diagram

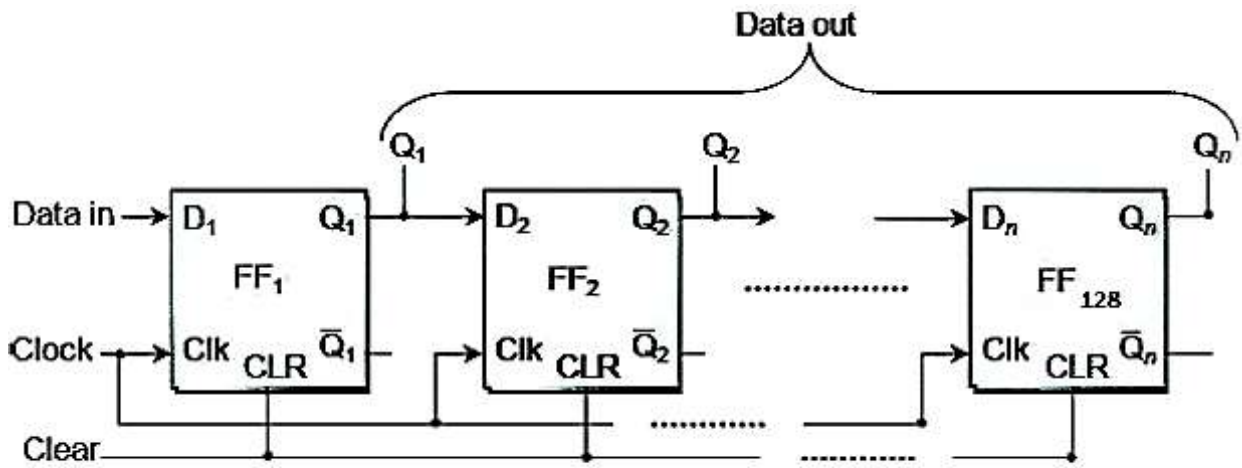


Figure 4.8: 128-bit Serial-In Parallel-out (Right-shift) Shift Register

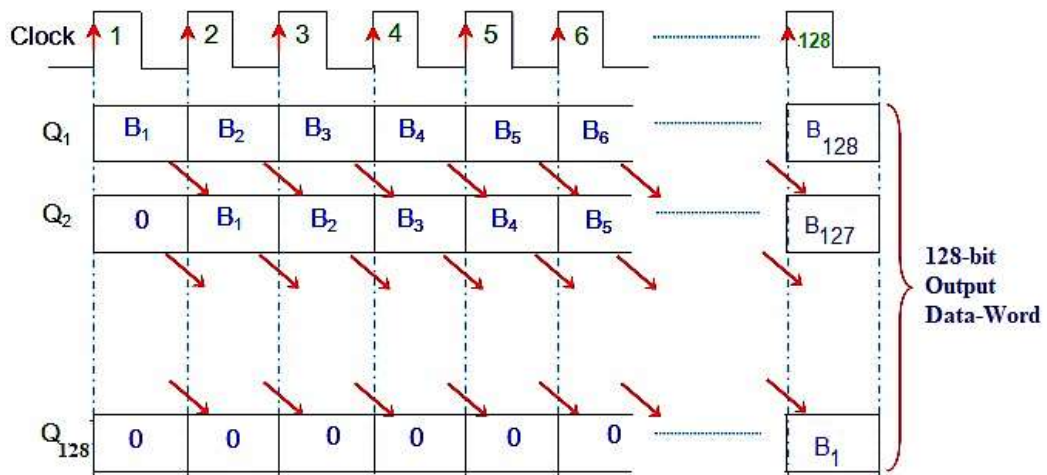


Figure 4.9: Output Waveform of 128-bit Right-Shift SIPO Shift Register

4.2.4 AES Algorithm (Encryption and Decryption processes)

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher, which converts data to an obscure format through the encryption process and converts the data back into its original format through the decryption process [34].

Rijndael algorithm is chosen by (NIST) in 2001, as the Advanced Encryption Standard (AES) as a replacement for the Data Encryption Standard (DES). AES is counted as one of the best symmetric security algorithms for data security. AES has been widely utilized in various applications, such as RFID tags, digital video/audio recorders, military applications, secure communication systems, smart cards, ATM, high-security portable communication equipment and high-performance database servers.

AES has the merit that is applicable in both hardware and software implementations [38]. AES offers strong security and high flexibility because it has a fixed block size of 128 bits and three key sizes to choose from 128, 192 and 256. Therefore, AES permits a 128-bit data length divided into four basic operational blocks that are treated as an array of bytes as a 4×4 matrix that is called the state array as a two-dimensional (2-D) where operations are executed. The State array is four rows of bytes, including "Nb" bytes, where "Nb" is the word size whereas the block length divided by 32. For full encryption process, "number of rounds" equal 10, 12, 14 for key length 128, 192 and 256 respectively [35].

The AES algorithm operations including three phases [34]:

- In the first phase, (XORing) that is an initial addition is executed between the input data (plaintext) and the key (cipher key). Initialization of the state array and addition of the initial round key to the starting state array (Key Expansion) are executed in this phase. In this process the four-column words of the key matrix are expanded into a schedule of 44 words ($44 \times 4 = 176$). The number of round keys = $N_r + 1$, where N_r is the number of rounds, which is 10 in case of 128 bits key size so in our case, the round keys = 11 [36].

The given 128- bits cipher key is stored in $[4] \times [4]$ bytes matrix ($16 \times 8 = 128$ bits)

- In the second phase, a number of standard rounds which represents the operating kernel of the algorithm that is determined by ("number of rounds" -1) are performed. Figure 4.10 presents the full block diagram of AES encryption and decryption processes.

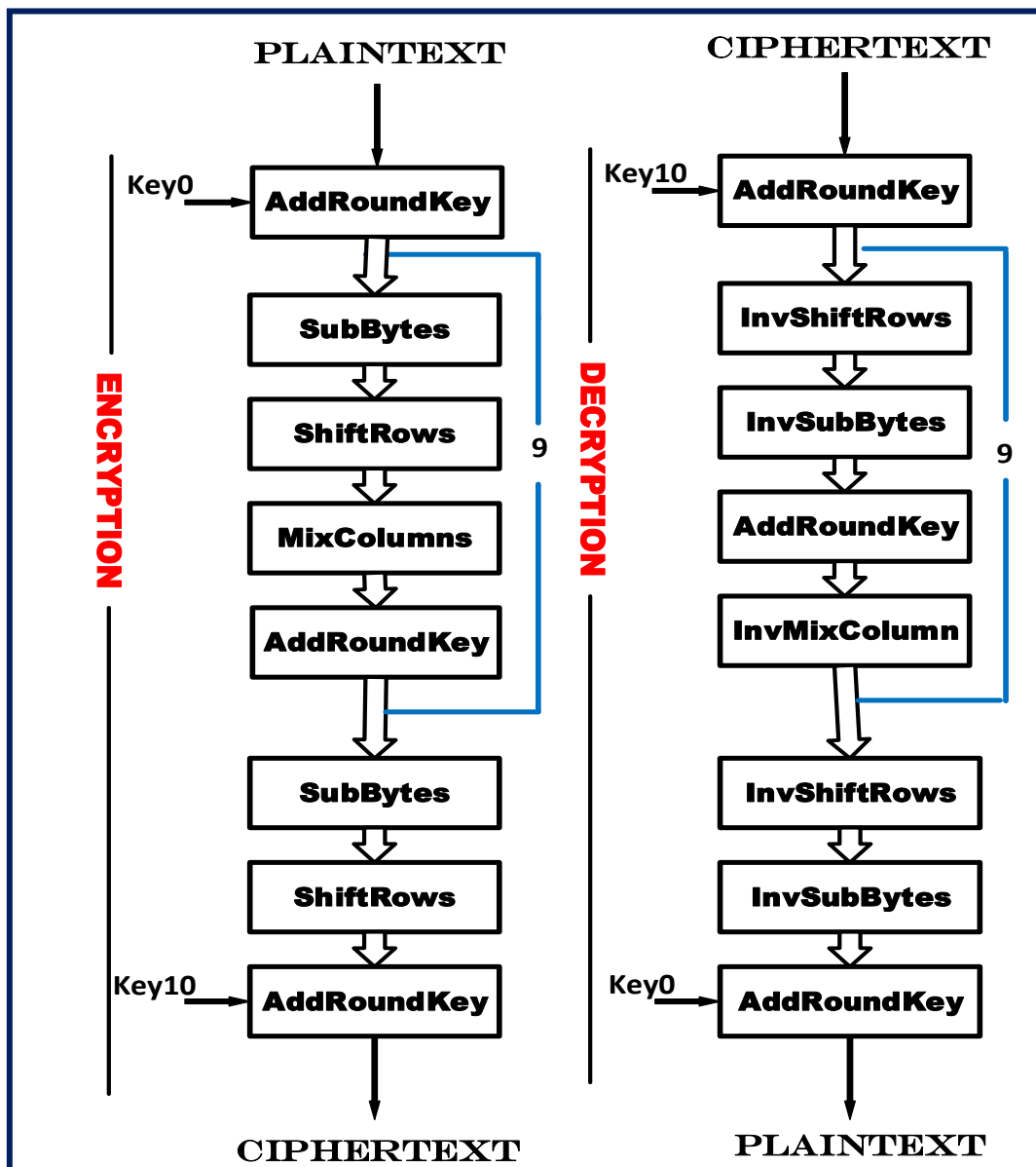


Figure 4.10: AES Block Diagram for a 128-bit key size.

In the proposed module, AES 128-bit key size is used. Every standard round comprises four fundamental algebraic function transformations on the state array as the following steps:

I. Sub Bytes,

Each byte from the input state is replaced by another byte according to the substitution box, this substitution box is called the S-box which is a special lookup table and is constructed by Galois fields. The elements of the S-box are in the hexadecimal system [38]. Each element of the state matrix is substituted by an element of the s-box matrix as in Figure 4.11.

II. Shift Rows, during this step, the rows of the block are cylindrically shifted in the left direction. During the process, the first row of the state array kept as it is and the bytes in the second, third, and fourth rows are cyclically shifted by one, two, and three bytes to the left, respectively as shown in Figure 4.12. The resulting matrix after shift operation as in Fig 4.13

III. Mix Columns is considered the most important process of the algorithm because it results in the flip of bits to spread all over the block. The block is multiplied by a fixed matrix as in Figure 4.14. There are 12 XORs, a 4-byte output and 16 multiplications for each row.

IV. AddroundKey, during this transformation each byte is XOR-ed with the corresponding element of the key's matrix as presented in Figure 4.15. Once this step is done the keys are no longer available for this step.

The third phase is the last round of the algorithm, which is identical to the standard round, but it does not have a MixColumn step as shown in Figure 4.10. Therefore, in the last round, Sub Bytes, Shift Rows, and AddroundKey are the processes that will be implemented during this step.

The decryption process involves reversing all the steps taken in encryption using inverse functions as shown in Figure 4.10 [37].

Based on what has been presented above, it can be said that the simplicity is counted as one of the most important features of AES that is obtained by repeatedly combining substitution and exchanging computations [38].

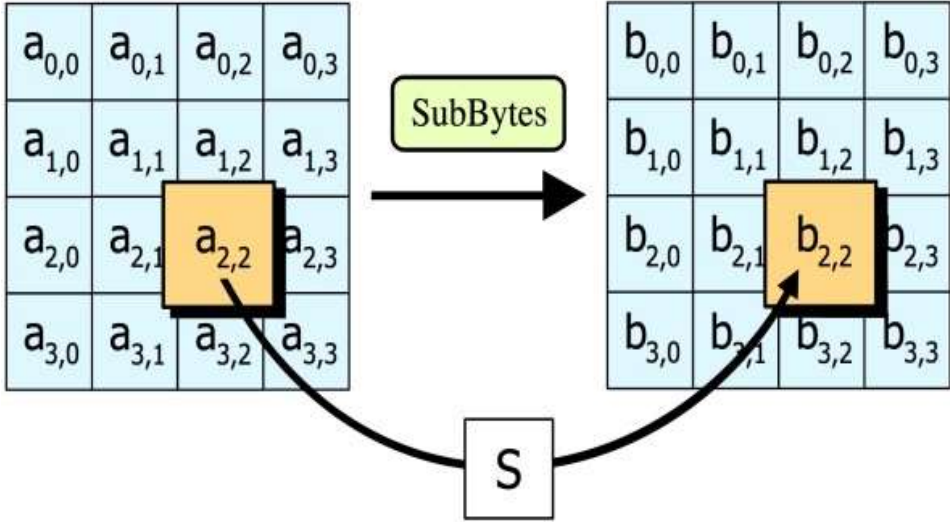


Figure 4.11: Sub Bytes step [36]

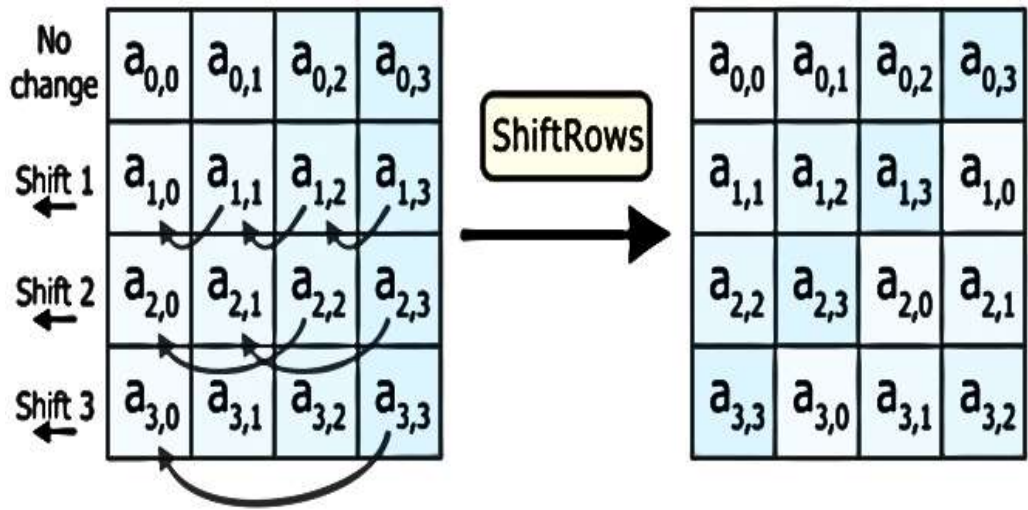


Figure 4.12: Shift Rows step [36]

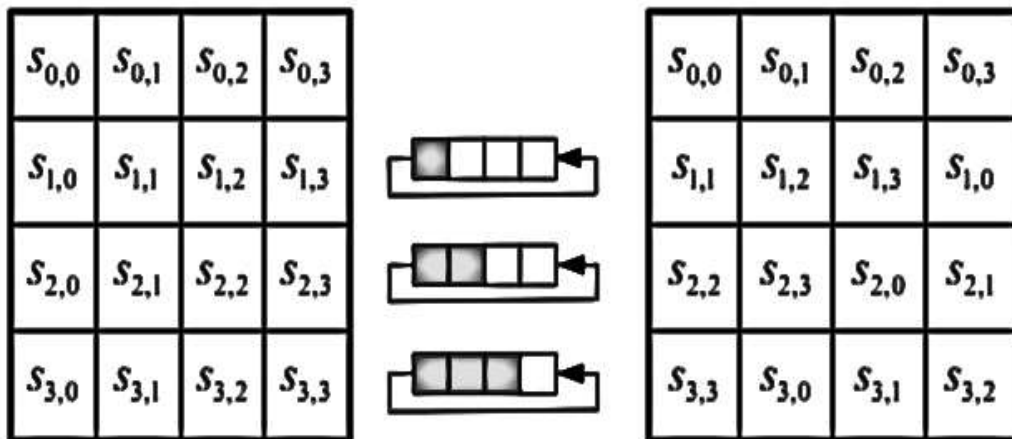


Figure 4.13: The resulting matrix after shift operation [36]

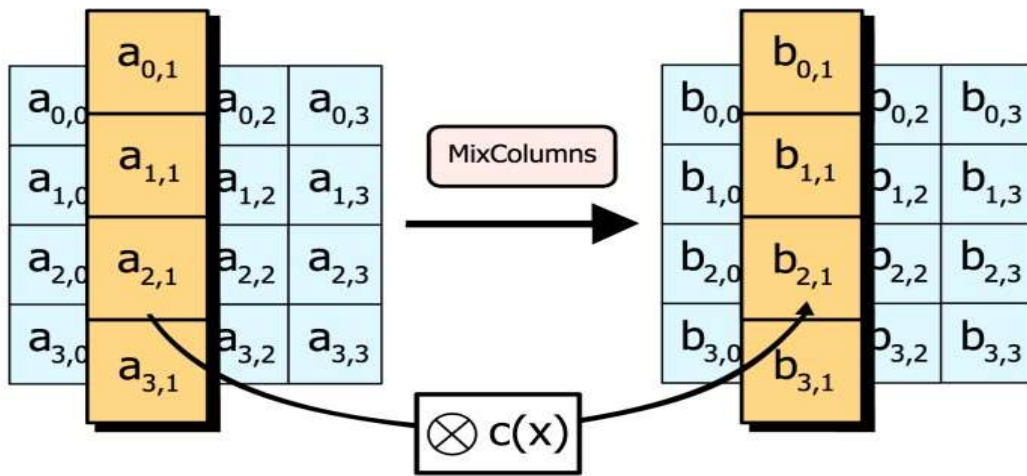


Figure 4.14: Mix Columns step [36]

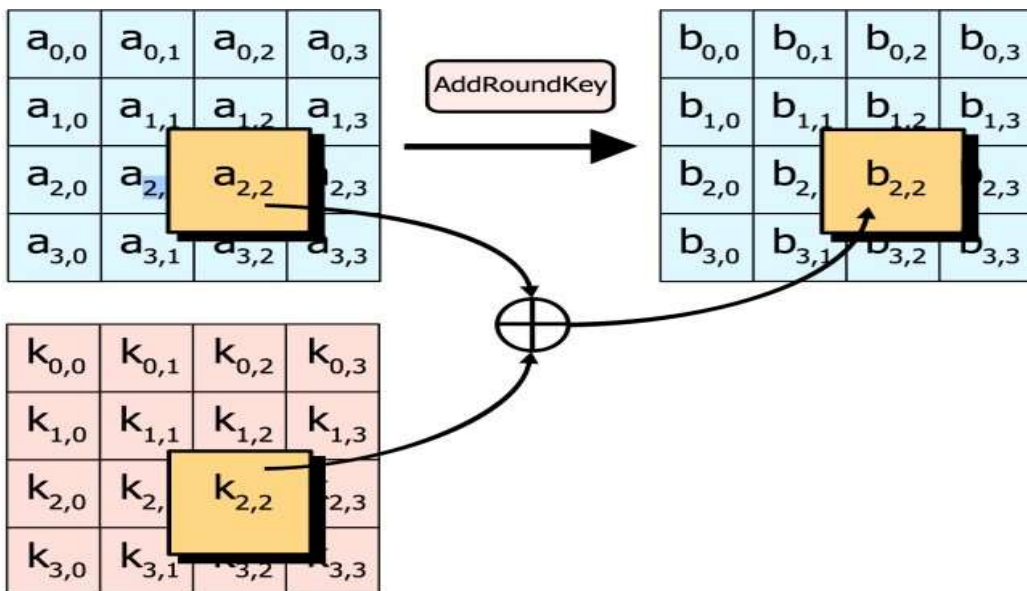


Figure 4.15: AddRoundKey step [36]

4.2.5 Mutual Authentication of the generated key at the encryption and decryption processes

The proposed module illustrated in Figure 4.2, based on taking into consideration the advantage of the uniqueness of each memristor device. Therefore, each device will generate a unique key. The mutual key authentication between the encryption and decryption sides can be achieved experimentally by tuning the input current of the Memristor device at the decryption side until the decryption of the encrypted message is verified successfully as illustrated in Figure 4.16.

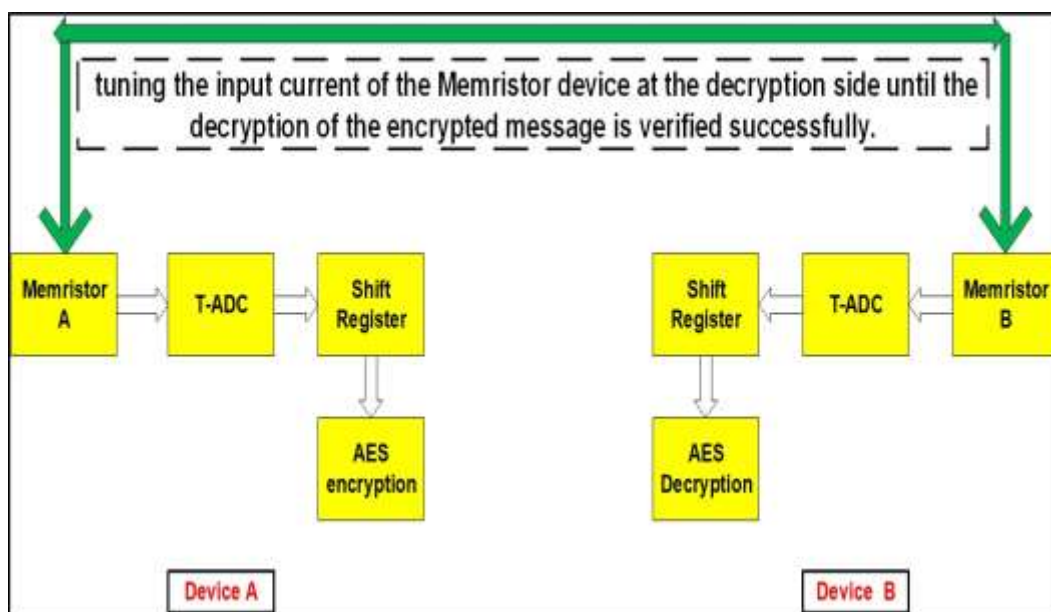



Figure 4.16: Mutual Authentication of the generated key between the encryption and decryption processes. 

4.3 Simulation Results

What should be noted, the Memristor and 3-bit T-ADC circuits are validated by Cadence Spectre simulation tool and the TSMC 130nm CMOS technology. The ThrEshold Adaptive Memristor Model (TEAM Model) [9] is used for the Memristor simulation. In this work, the AES (Advanced Encryption Standard) encryption process is carried out on Xilinx Vivado project navigator alongside online AES tools for decryption and encryption verification.

I - Memristor IV characteristic curve

Cadence Spectra simulation tool and the TSMC 130nm CMOS technology are used to validate the Memristor. The steps that have been followed to get the Memristor I-V Characteristics are:

- 1-Create library.
- 2-Insert Verilog A models.
- 3-Draw the desired Memristor symbol.
- 4- Create the Memristor circuit schematic by using Virtuoso Schematic Editor.
- 5-Use ADE L to simulate the circuit.

Figure 4.17 represents the Memristor I-V characteristics that result from applying the input sinusoidal waveform current from $(-35\mu\text{A}$ to $35\mu\text{A})$ and frequency $=100\text{MHz}$ at initial state = zero, stop time = 15ns and time step parameters (dt in TEAM model) = $1e-9$ seconds.

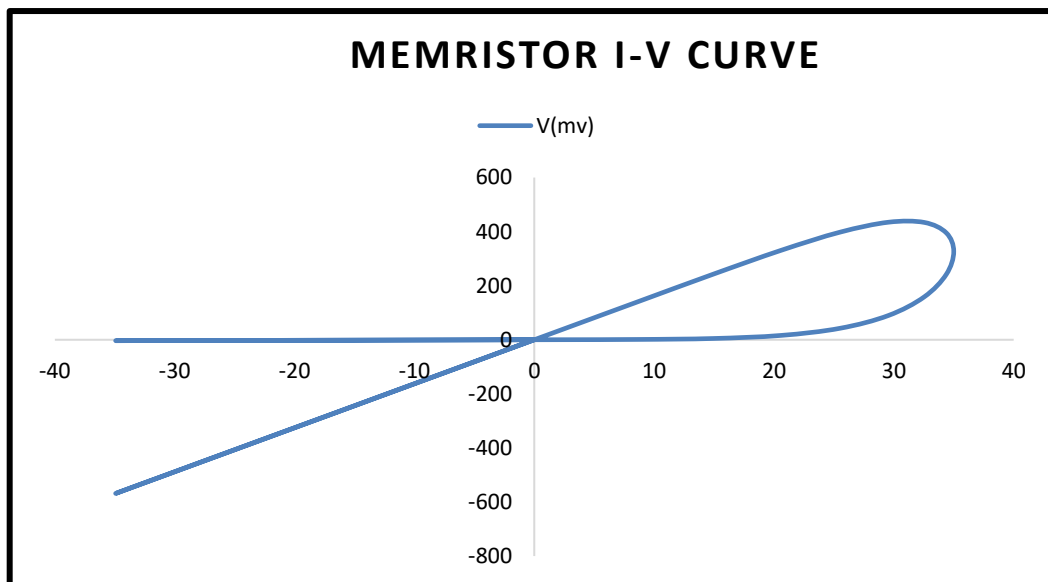


Figure 4.17: Memristor I-V Characteristics by sweeping the input current from $(-35\mu\text{A}$ to $+35\mu\text{A})$ at frequency $=100\text{MHz}$, stop time = 15ns and initial state = zero.

It is noticed that to get the positive lobe only, the stop time could be decreased to 10ns as shown in Figure 4.18 which represents the Memristor I-V characteristics curve that results from applying the input sin waveform current from $(-35\mu\text{A}$ to $+35\mu\text{A})$ at frequency $=100\text{MHz}$, and time step parameters $=1e-9$ seconds.

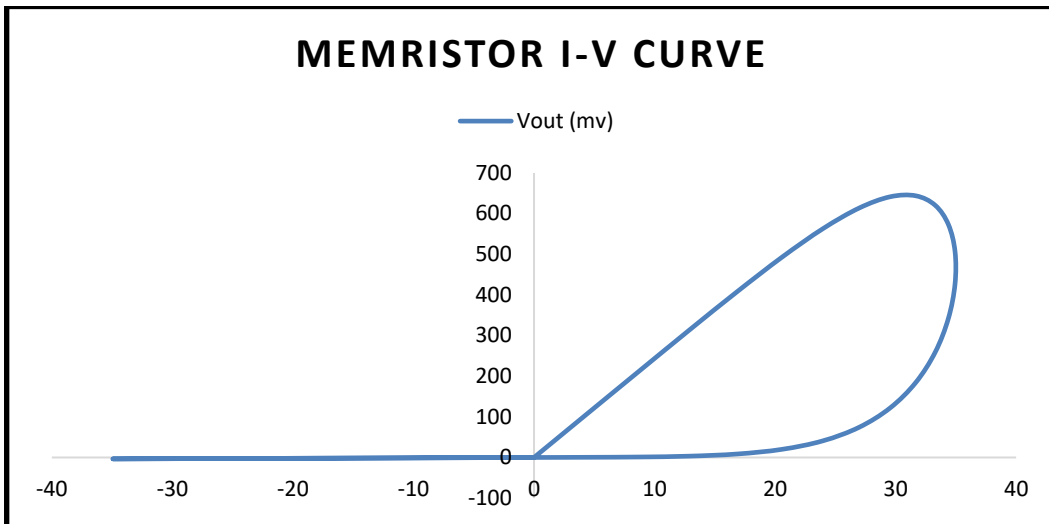


Figure 4.18: Memristor I-V Characteristics by sweeping the input current from (-35 μA to + 35 μA) at frequency =100MHz, stop time= 10ns and initial state = zero.

II - 3-bit T-ADC output and Key generation

Table 4.1 represents the corresponding 3-bit T-ADC binary states with respect to the Memristor output voltage values at 'X'. To get a 128-bit key, 43 points on the curve that is shown in Figure 4.17 or Figure 4.18 are digitized through the 3-bit T-ADC. The resolution of the proposed 3-bit T-ADC = $200\text{mV} / 8 = 25 \text{ mV}$, where 200mV is the T-ADC dynamic range. This means that every 25 consecutive values give the same digital output.

Table 4.1 represents the corresponding 3-bit T-ADC binary states with respect to the Memristor output voltage values at 'X'

State	Voltage range of T-ADC	Volt at node 'X'
000	385 m V – 409 m V	407 m V
001	410 m V – 434 m V	425 m V
010	434 m V – 460 m V	445 m V
011	460 m V – 485 m V	467 m V
100	485 m V – 510 m V	491 m V
101	510 m V – 535 m V	517 m V
110	535 m V – 560 m V	547 m V
111	560 m V – 585 m V	580 m V

An Example of 128-bit key after digitizing 43 points on Memristor I-V characteristic curve:

**Binary: 1111 1111 1111 1111 1111 1110 1011 0110 0100 1000 1101 1011
0110 1001 0010 0010 0100 0000 0000 0000 0000 0000 0000 0000
1101 1101 1111 1111 1010 0010 1001.**

Hex: FF FF FE B6 48 DB 69 22 40 00 00 00 0D DF FA 29

III - AES Encryption and Decryption processes

The AES encryption process is simulated by RTL project navigator through Xilinx Vivado 2015., Figure 4.20 presents AES Encryption Process flow through Vivado. As illustrated in Figure 4.20, the process flow is started by add AES design sources as VHDL files. The synthesis process should be completed successfully to run the implementation process. Then, the generated 128-bits key that is mentioned in the previous section has been inserted in AES.vhd file alongside a text message in a Hexadecimal format as shown in Figure 4.19.

The last step is to run the behavioral simulation. The resultant encrypted message has been taken to (AES online Domain Tools) for Decryption and verify the trustworthiness of the encryption process.

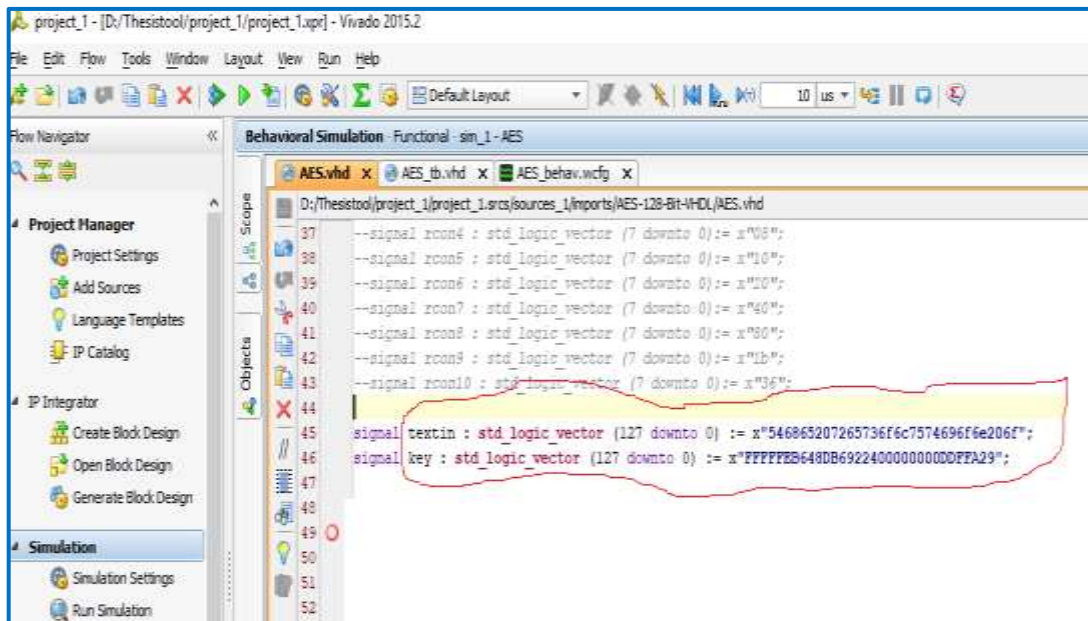


Figure 4.19: Inserting the 128-bits generated key and a Text message into AES.vhd

Five messages have been encrypted by following the aforementioned steps. The plaintext messages in Hexadecimal format and their corresponding encrypted messages are listed in Table 4.2.

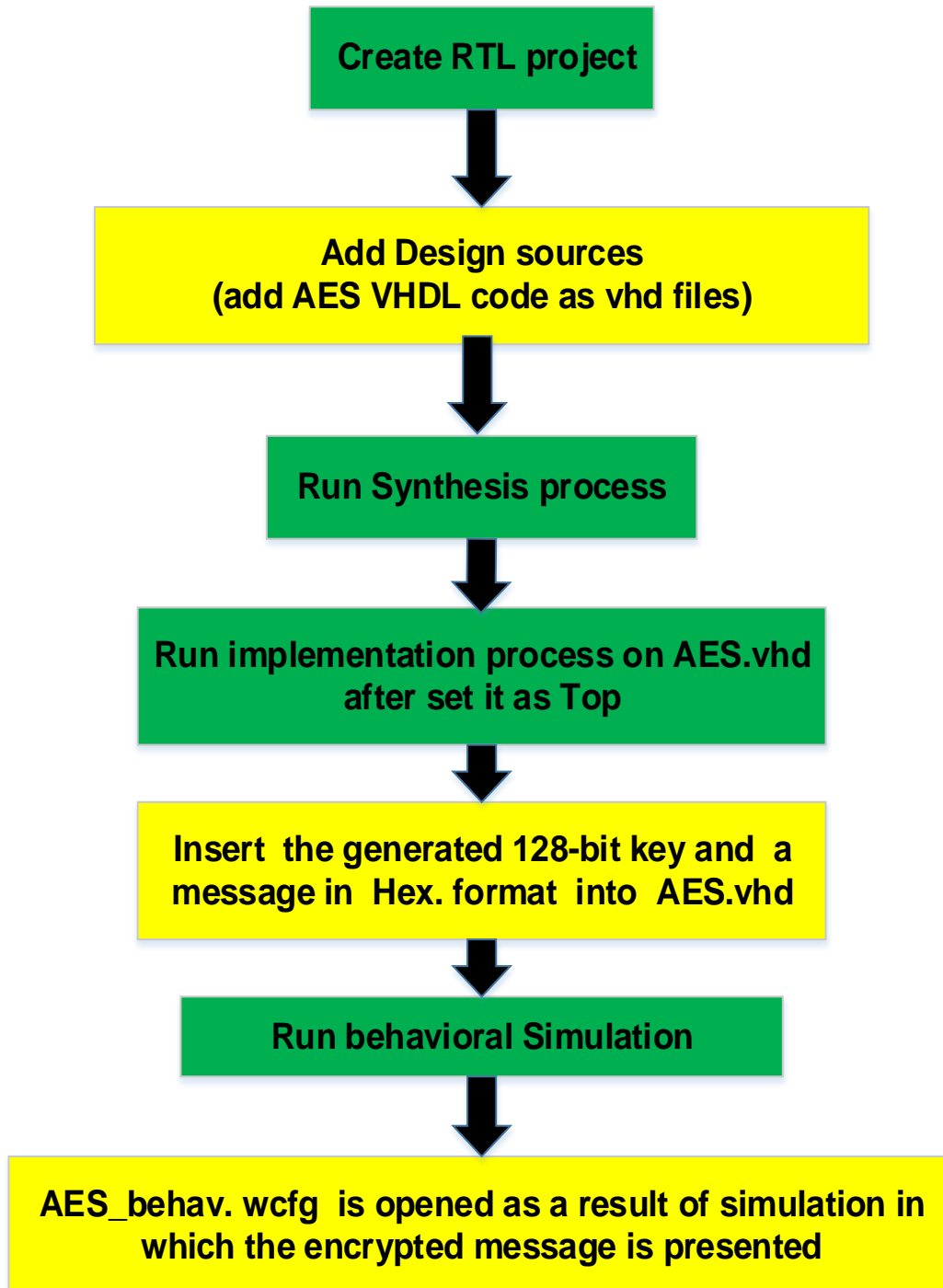


Figure 4.20: Flowchart of the Sequencing steps of AES encryption process which simulated through Xilinx Vivado.

Table 4.2: Five Plaintext messages in Hexadecimal and the corresponding encrypted messages as a result of using the generated 128-bit key through the AES encryption algorithm.

Plaintext message in Hex.	Encrypted message in Hex.
54 68 65 20 72 65 73 6f 6c 75 74 69 6f 6e 20 6f	5d e1 b8 86 69 ec 12 57 7c c6 7e 3a 7d de 7f 3e
66 20 74 68 69 73 20 41 44 43 20 3d 32 30 30 6d	a2 e6 44 1c 8b b9 67 14 d9 eb 58 43 aa c0 76 ac
48 61 6e 61 6e 20 41 62 64 20 45 6c 48 61 6d 69	4c df 1f cd 51 67 70 09 8c ef 18 14 20 e8 e4 06
48 61 6e 61 6e 41 62 64 65 6c 68 61 6d 69 64 52	e1 dd 4a 7f 50 46 f9 b5 83 c7 81 50 3d 35 9d f8
76 65 72 73 69 74 79 20 6e 61 6e 6f 20 70 72 6f	41 df 4a 44 ae f1 b9 88 27 6d cc a4 a9 c2 2e 05

Chapter 5: Discussion and Conclusions

5.1 Contributions

In this thesis, an overview of the advantages of Nanoelectronics-based hardware security primitives specifically the Memristor-based security solutions for more robust security techniques are discussed in the light of the current state of art. The currently published Memristor-based hardware security approaches were reviewed showing the importance of using Memristor as an emerging nanoscale technology that offers great promise for building small-scale and energy-efficient hardware, including emerging security primitives in security applications.

This thesis presents a hardware security module that relies on Memristor-based AES 128-bit key generation. The work is relying on the uniqueness property of each Memristor devices. Memristor is a nanoscale candidate is preferred over others due to its highly nonlinear characteristics that exhibit the pinched hysteresis loop, which is considered as the fingerprint for memristive devices. 3-bit T-ADC is used to digitize the I-V characteristic curve of the Memristor devices. SIPO (shift right) shift register is supposed to be used for generating the 128-bit key at its parallel output pins. AES-128 is used as a cryptographic algorithm. The generated key can be used as secret key in any cryptographic algorithms rather than AES.

5.2 Published/Submitted Paper

H. Rady, H. Hossam, M. Sameh Saied, and Hassan Mostafa, "Memristor-Based AES Key Generation for Low Power IoT Hardware Security Modules." *IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS 2019)*, Dallas, Texas, USA, pp. 231-234, 2019.

5.3 Recommendations for Future Work

This thesis contributes to the foundation for future work in the area of Memristor-based hardware security modules.

The extension of this work with regards to the proposed module design aspects is related to the use of the following alternatives:

- AES-192 or AES-256 can be used for highly strong and robust security.
- 6-bit or 8-bit T-ADC for the faster digitizing process.
- The mutual authentication of the generated key can be verified experimentally by tuning the input current of the Memristor at the decryption side.

References

- [1] Rajendran, Jeyavijayan, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki. "Nano meets security: Exploring nanoelectronic devices for security applications." *Proceedings of the IEEE* 103, no. 5, pp. 829-849, 2015.
- [2] Rajendran, Jeyavijayan, R. Karri, J. B. Wendt, M. Potkonjak, N. R. McDonald, Garrett S. Rose, and B.T.Wysocki. "Nanoelectronic Solutions for Hardware Security." *IACR Cryptology ePrint Archive* 2012.
- [3] Chua, Leon, "If it's pinched it's a memristor." *Semiconductor Science and Technology* 29, no. 10, 2014.
- [4] H. Abunahla, and Baker Mohammad, "Memristor technology: synthesis and modeling for sensing and security applications." *New York: Springer International Publishing, 2018. (Book)*
- [5] Adamatzky, Andrew, and Leon Chua, "Memristor networks." *Springer Science & Business Media, 2013. (Book)*
- [6] A. G. Radwan, and M. E. Fouda. "Memristor: Models, types, and applications." *In On the Mathematical Modeling of Memristor, Memcapacitor, and Meminductor,* pp. 13-49. Springer, Cham, 2015.
- [7] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, pp. 80–83, May 2008.
- [8] M. Elshamy, H. Mostafa, and M. Sameh Said. "Design considerations/insights for Memristor-based memory arrays." *IEEE International Conference on Engineering and Technology (ICET)*, pp. 1-6, 2014.
- [9] S. Kvatinsky, E. G. Friedman, A. Kolodny, and U. C. Weiser, "TEAM Threshold Adaptive Memristor Model", *IEEE Transactions on. Circuits and Systems. I: Regular Papers*, vol. 60, no. 1, pp. 211-221, January 2013.
- [10] M. Elshamy, H. Mostafa, and M. Sameh Said. "New non-destructive Read/Write circuit for Memristor-based memories." *International Conference on Engineering and Technology (ICET)*, pp. 1-5, 2014.
- [11] Arafin, Md Tanvir, Carson Dunbar, Gang Qu, N. McDonald, and L. Yan. "A survey on memristor modeling and security applications." *In 16th International Symposium on Quality Electronic Design*, pp. 440-447, 2015.

- [12] G.S. Rose, M. Uddin, and M. B. Majumder. "A designer's rationale for nanoelectronic hardware security primitives." *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 194-199, 2016.
- [13] M. Uddin, M. B. Majumder, and G. S. Rose. "Robustness analysis of a memristive crossbar PUF against modeling attacks." *IEEE Transactions on Nanotechnology* 16, pp. 396-405. 2017.
- [14] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan. "A novel memristor-based hardware security primitive." *ACM Transactions on Embedded Computing Systems (TECS)*, 2015.
- [15] Jin, Yier. "Introduction to hardware security." *Electronics* 4, no. 4: pp 763-784, 2015.
- [16] Dou, Chunmeng, Wei-Hao Chen, Yi-Ju Chen, Huan-Ting Lin, Wei-Yu Lin, Mon-Shu Ho, and Meng-Fan Chang. "Challenges of emerging memory and memristor-based circuits: Nonvolatile logics, IoT security, deep learning, and neuromorphic computing." *IEEE 12th International Conference on ASIC (ASICON)*, pp. 140-143, 2017.
- [17] Shamsi, Kaveh, Wujie Wen, and Yier Jin. "Hardware security challenges beyond CMOS: Attacks and remedies." *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 200-205, 2016.
- [18] M. Tehranipoor, D.Forte, G. S. Rose, and S. Bhunia. "Security Opportunities in Nano Devices and Emerging Technologies." *CRC Press, 2017. (Book)*
- [19] Vourkas, Ioannis, and Georgios Ch Sirakoulis. "Memristive crossbar-based nonvolatile memory." *In Memristor-Based Nanoelectronic Computing Circuits and Architectures*, pp. 101-147. Springer, Cham, 2016.
- [20] M. Uddin, B. Majumder, and Garrett S. Rose. "Nanoelectronic Security Designs for Resource-Constrained Internet of Things Devices: Finding Security Solutions with Nanoelectronic Hardware." *IEEE Consumer Electronics Magazine* 7, pp.15-22, 2018.
- [21] G. S. Rose "Security meets nanoelectronics for the Internet of things applications." *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*, pp. 181-183. ACM, 2016.
- [22] H. Abunahla, D. Shehada, C. Y. Yeun, B. Mohammad, and M. A. Jaoude, "Novel secret key generation techniques using memristor devices." *AIP Advances* 6, no. 2, 2016.

- [23] M. Noman, W. Jiang, P. A. Salvador, M. Skowronski, and J. A. Bain, "Computational investigations into the operating window for memristive devices based on homogeneous ionic motion," *Applied Physics A* 102, pp.877–883, 2011.
- [24] N. Hashem and S. Das, "Switching-time analysis of binary-oxide memristors via a nonlinear model," *Applied Physics Letters* 100, 2012.
- [25] H. Abunahla, D. Shehada, C. Y. Yeun, C. J. OKelly, M. A. Jaoude, and B. Mohammad, "Novel microscale memristor with uniqueness property for securing communications." *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2016), Dubai, United Arab Emirates, pp. 1-4, October 2016.*
- [26] H. Abunahla, D. Shehada, C.Y. Yeun, B. Mohammad, and T. Stouraitis, "A novel secure conference communication in IoT devices based on memristors.", *IEEE International Conference on Electronics, Circuits, and Systems (ICECS 2017), pp. 58-61, 2017.*
- [27] H. M. N. Al-Hamadi, C. Y. Yeun, M. J. Zemerly, and M. Al-Qutayri, "Distributed lightweight Kerberos protocol for mobile agent systems", *IEEE GCC Conference and Exhibition (GCC 2011), Dubai, United Arab Emirates, pp. 233-236., February 2011.*
- [28] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M "Lightweight Hardware Architectures for the Present Cipher in FPGA." *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(9), pp.2544–2555, 2017.
- [29] N. Samir, Y. Gamal, A. N. El-Zeiny, O. Mahmoud, A. Shawky, A. Saeed, and Hassan Mostafa. "Energy-Adaptive Lightweight Hardware Security Module using Partial Dynamic Reconfiguration for Energy Limited Internet of Things Applications.", *IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-4, 2019.*
- [30] M. Bahnasawi, A., K. Ibrahim, A. Mohamed, M. Khalifa, A. Moustafa, K. Abdelmonim, Y. Ismail, and H. Mostafa, "ASIC-Oriented Comparative Review of Hardware Security Algorithms for the Internet of Things Applications", *IEEE International Conference on Microelectronics (ICM 2016), Cairo, Egypt, pp. 285-288, 2016.*
- [31] H. Mostafa, and Y. Ismail, "Highly-Linear Voltage-to-Time Converter (VTC) Circuit for Time-Based Analog-to-Digital Converters (TADCs)," *IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS), pp. 149–152, 2013.*
- [32] H. Hossam, G. Mamdouh, H. H. Hussein, M. El-Dessouky, and H. Mostafa, "A New Read Circuit for Multi-Bit Memristor-Based Memories Based on Time to Digital Sensing Circuit", *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2018), Windsor, Ontario, Canada, pp. 1114-1117, 2018.*

- [33] <https://www.electrical4u.com/serial-in-parallel-out-sipo-shift-register/>, Aug. 2019
- [34] G. F. El Kabbany, H. K. Aslan, and M. N. Rasslan, "A design of a fast parallel-pipelined implementation of AES: Advanced Encryption Standard," *International Journal of Computer Science & Information Technology*, vol. 6, no. 6, pp: 39-45, Dec. 2014.
- [35] Mandal, Akash Kumar, Chandra Parakash, and Archana Tiwari. "Performance evaluation of cryptographic algorithms: DES and AES", *IEEE Students' Conference Electrical, Electronics and Computer Science (SCEECS 2012)*, pp. 1-5, March 2012.
- [36] <https://www.slideshare.net/atheistprince/aesadvanced-encryption-standard>, Sep. 2019.
- [37] M. Prerna, and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security." *Global Journal of Computer Science and Technology*, 2013.
- [38] R.D. Bajaj, and U. M. Gokhal. "AES Algorithm for Encryption." *International Journal of Latest Research in Engineering and Technology* 2, pp.63-68, 2016.
- [39] Stanley Williams, R. "How we found the missing memristor." *In Chaos, CNN, Memristors and Beyond: A Festschrift for Leon Chua with DVD-ROM, composed by Eleonora Bilotta*, pp. 483-489. 2013.
- [40] A. P. James. "Memristor Threshold Logic FFT Circuits." *Fourier Transforms: High-tech Application and Current Trends*, 2017.
- [41] S. P. Adhikari, M. P. Sah, H. Kim, and Leon O. Chua. "Three fingerprints of memristor." *IEEE Transactions on Circuits and Systems I: Regular Papers* 60, pp. 3008-3021, 2013.
- [42] D. Biolek, Z. Biolek, V. Biolková, and Z. Kolka. "Some fingerprints of ideal memristors." *IEEE international symposium on circuits and systems (ISCAS2013)*, pp. 201-204., 2013.
- [43] Leon Chua. "Resistance switching memories are memristors." *Applied Physics A* 102, no. 4, pp. 765-783, 2011.
- [44] M. D. Pickett, D. B. Strukov, J. L. Borghetti, J. J. Yang, G. S. Snider, D. R. Stewart, and R. S. Williams. "Switching dynamics in titanium dioxide memristive devices." *Journal of Applied Physics* 106, no. 7, 2009.
- [45] M.V. Nair "Memristive Crossbar Arrays for Machine Learning Systems." *Ph.D. diss., the University of Manchester (United Kingdom)*, 2015.

المخلص

برز أمان الأجهزة كحقل مهم للغاية يهدف إلى التخفيف من المشكلات مثل التزوير وهجمات القنوات الجانبية والهندسة العكسية. بدائل أمان الأجهزة المستخدمة في ضمان سلامة ومصداقية الدوائر المتكاملة لتوفير أمان قوي مع الحد الأدنى من المساحة والطاقة ، يتم استخدام حلول أمان الأجهزة المستندة إلى إلكترونيات النانو، والتي تحافظ على المزايا المذكورة أعلاه مع توفير تقنيات أمان جديدة. علاوة على ذلك ، تعد حلول الأمان القائمة على بدائل النانو أكثر قوة من حلول الأمان CMOS النموذجية فيما يتعلق بأن تعقيد انتهاك أمن بدائل النانو يقابل حل مجموعة من المعادلات غير الخطية لنظام كبير ومعقد .

وحدات الممريستور تعتبر المرشح المفضل في تطبيقات الأمن بسبب الاستجابة الكهربائية الفريدة والتي تختلف من نوع إلى آخر. وبالتالي ، من الصعب التنبؤ باستجابة الأجهزة الفردية بواسطة نموذج رياضي محدد فيصبح من الصعب التنبؤ باستجابة وحدة الممريستور المدمجة في الأجهزة. علاوة على ذلك ، فإن ما يميز الممريستور على العديد من أجهزة النانو الأخرى هو التوافق مع تقنيات تصنيع CMOS الحديثة.

في هذا العمل ، يتم تقديم نموذج أمان الأجهزة المستندة إلى مخطط توليد مفاتيح session keys المستندة إلى الممريستور حيث يعتمد المخطط على السلوك الفريد لخصائص V-I لأجهزة الممريستور حيث يتم استخدام مفتاح الممريستور الذي تم إنشاؤه خلال عمليات التشفير وفك التشفير لخوارزمية التشفير AES. تُقترح وحدة أمان الأجهزة هذه لتطبيقات أمان إنترنت الأشياء IoT منخفضة الطاقة. وتعتمد الوحدة المقدمه في هذا العمل على توليد مفاتيح AES المستندة إلى الممريستور والتي تعتمد بشكل أساسي على تفرد أجهزة الممريستور بسبب اختلافات عملية التصنيع.

بالإضافة أن مع الأخذ في الإعتبار ما سبق ذكره عن الخصائص والمميزات لخوارزمية تشفير AES المستندة إلى الوقت و المحولات الرقمية المستندة الى الوقت T-ADC، يمكن لوحدة أمان الأجهزة المقدمه من خلال هذا العمل تلبية احتياجات التكنولوجيا الحديثة مثل الاتصالات الآمنة بين الأجهزة المدمجة في إنترنت الأشياء.