Memristor-Based AES Key Generation for Low Power IoT Hardware Security Modules

Hanan Rady[1], Hagar Hossam[2], M.Sameh Saied [3], Hassan Mostafa[4]
[1,3,4] Electronics and Communications Engineering Department, Cairo University., Egypt
[2]Electronics and Communications Engineering Department, Ain-Shams University., Egypt
[4] Nanotechnology Engineering Department, University of Science and Technology at Zewail city, Egypt

Emails: hananrady7716@outlook.com, hagarhossam21@yahoo.com, hmostafa@uwaterloo.ca

***Abstract*— Security of Internet of Things (IoT) needs devices and algorithms that offer ultra-low power consumption and a long lifespan, alongside strong immunity against attacks, lower chip area, and acceptable throughput. Hardware security using nanoelectronic technologies shows promise for the area and energy-efficient implementations in IoT. Owing to the recent advances in Memristor as a potential building block for future hardware, it becomes a vital issue to study the role that Memristor will play in hardware security. This work presents a hardware security module for low power IoT security implementations. The proposed module depends on Memristor-based AES key generation relying mainly on the uniqueness of Memristor devices due to fabrication process variations. In addition to taking into consideration the strength properties and great features of Time-based ADC and AES cryptographic algorithm, the proposed hardware security module could meet the needs of modern technology such as secure communication between IoT embedded devices**.

***Keywords*—** *Hardware security; IoT security; Memristor; Memristor Security; AES; T-ADC.*

I. Introduction

The Internet of Things (IoT) became one of the priorities of research due to the network heterogeneity and the omnipresence of IoT devices [5]. In order to provide robust IoT security with minimal area and power overhead, security solutions are implemented using nanoelectronic security primitives and nano-enabled security protocols. Such nanoscale security primitives are expected to utilize a very small amount of area and consume a negligible amount of power, moreover provide the required levels of security [1], especially for counterfeiting and piracy that are important in that end users need to trust the authenticity of their IoT devices.

Memristor has been recognized as the first practical implementation of the missing fourth circuit element predicted by L. Chua in 1971 [7]. In 2008, R. S. Williams introduced a two-terminal Titanium dioxide ($\mathrm{Ti}O_2$) nano-scale device that follows the memristive characteristics defined by L. Chua in1971[8]. Memristor as an emerging nanoscale technology offers great promise for building small-scale and energy-efficient hardware, including emerging security primitives [2]. Memristor devices offer unique characteristics such as nonlinearity and unpredictable behavior variations. It can be said that what makes memristor a preferable choice in security solutions is the variation in electrical response from each memristor types. Consequently, no mathematical model can predict the response of individual devices. Memristor-based physical unclonable functions (PUFs) has been investigated widely in the last 5 years as memristive security primitives that use the significant resistance variations of the memristive crossbar [1].

Use only one Memristor device rather than a complex crossbar circuitry is presented in the work proposed in [3] that depends on extract master and session keys from two identical Memristor devices. The generation of identical keys for encryption and decryption at the communicating peers is considered a challenge. It is suggested that keys can be extracted from the shared area under the I-V curve of the identical Memristor devices to accomplish a similar encryption and decryption keys, which requires extra computational operations. An alternative work in [4, 5] presented a new postulate depending on the uniqueness of the Memristor device. The suggested technique depends on initiating communications through a third trust party (TTP), each of the different devices and TTP has Memristor devices with unique I–V characteristics and the session keys can be generated by digitizing the I-V curve (rather than the area under the curve) based on the required key size based on the used encryption algorithm.

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 in FPGAs. The AES algorithm is found to be the most suitable algorithm for IoT hardware security applications [6].

In this paper, 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.

The rest of the paper is organized as: Section II presents the proposed module to generate Memristor-based AES Key for IoT hardware security with the detailed explanation of each block and its role in the proposed key generation process. The simulation results from each block are presented in Section III, and conclusion in Section IV.

II. Proposed module

The proposed module that illustrated in Fig.1 presents a hardware security module based on generating Memristor-based AES key.
The key generation process passes through three stages that are executed by cascading three blocks. The first block is the

Memristor device to get a unique I-V characteristic curve by sweeping the input current. The second block is 3-bit T-ADC that is used to digitize the I-V curve. The third block is a shift register to generate the 128-bit key, which used as AES symmetric key. The following subsections discuss the operation and characteristics of each block.

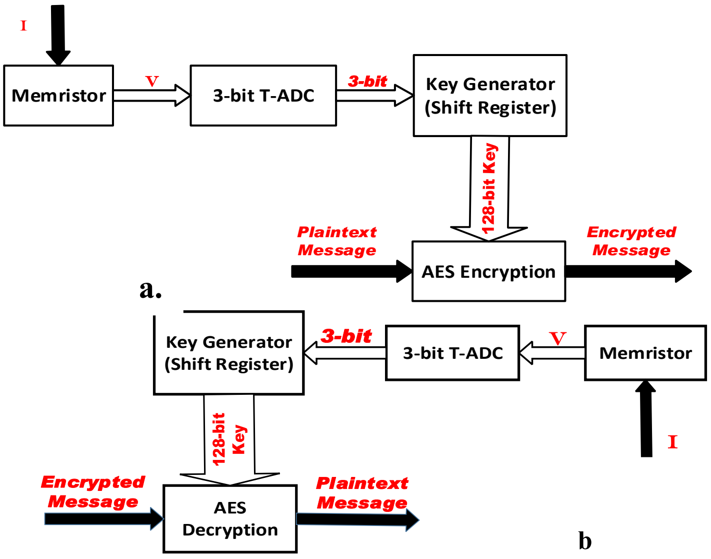

Figure 1.The Proposed Module (a) Encryption process at Device A.

(b) Decryption process at Device B.

A. *Memristor- Based IV Characteristics*

The most important characteristic of a Memristor is the current-voltage characteristic, where it exhibits a pinched hysteresis loop. An important fingerprint of the Memristor is the hysteresis loop. 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 Fig. 2. Due to this unique behavior of Memristor, hardware security has potential application based on Memristor.

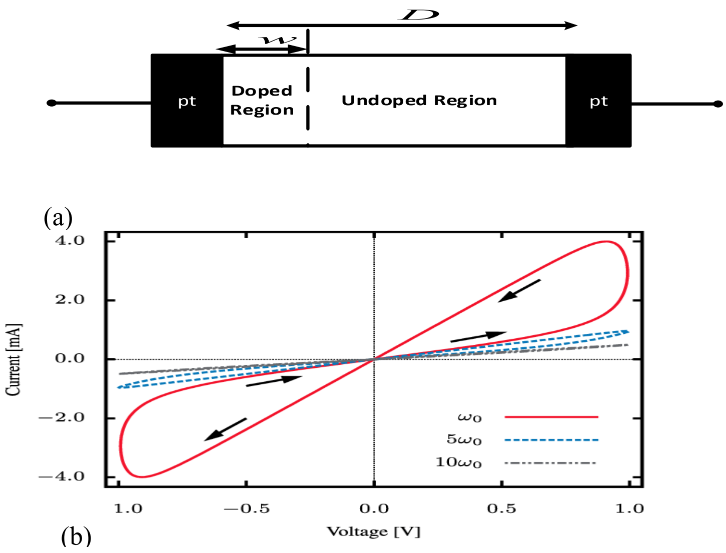

Figure 2: (a) Memristor device structure, (b) Pinched hysteresis loop of the memristor.

The proposed module presents a provision in reliance on the uniqueness of the Memristor device. Therefore, it is supposed that each IoT device has its unique Memristor device as in Fig. 1. When a certain current sweep is applied across a Memristor device, this will result in unique voltages values.

Time-Based ADC

T-ADC is used to digitize the I-V characteristic curve. T-ADC composed of two stages. The first stage is 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 shown in figure 3, The input voltage at node 'X' controls the delay of the falling edge of the clock signal, Vclk; through the inverter (Transistors M4 and M5), by Controlling the discharging current of transistor M3. Next stage is the (TDC) circuit that converts the output delay produced by the starved inverter into the thermometer code that is encoded into binary code through a time to digital converter using Vernier delay line [9]. This Vernier delay line consisted of two parallel delay chains and sense amplifier based on D-flip flops. The stop signal is the reference signal. The signals (start, stop) travel through these delay chains until they become aligned. The D-flip flops sense amplifier determines which of the two input signals comes first and produces the thermometer code. Fundamentally, the TDC sensing circuit needs only a starved inverter and the numbers of flip-flops are determined according to this formula: 2^n -1; where n: represents the number of bits. A thermometer-to-binary is then used to produce a 3-bit binary output.

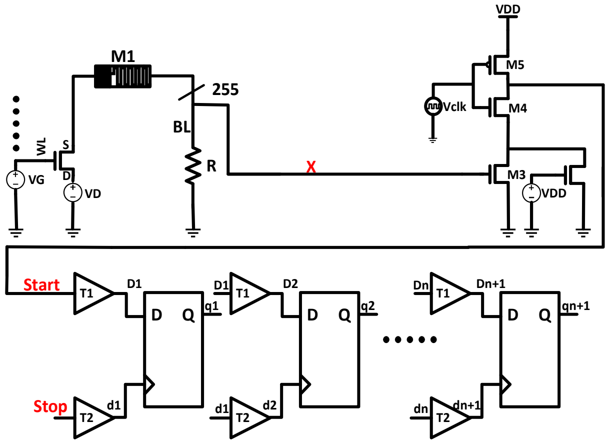

Figure 3: The simplified schematic of T-ADC [9]

B. *Key Generator (SIPO Shift Register)*

To get the 128-bit required key, it is assumed that 128- bit Serial-in to Parallel-out (Right Shift) Shift Register can be used. The T-ADC output is fed serially at the input of the first flip-flop (D1 of FF1). The inputs of all other flip-flops (except the first flip-flop FF1) are driven by the outputs of the preceding ones say, for example, the input of FF2 is driven by the output of FF1. In this kind of shift register, the data stored within the register is obtained as a parallel-output data word (Data out) at the individual output pins of the flip-flops (Q1 to Qn), where n is the length of the output data word. In the right-shift SIPO shift-register, data bits shift from left to right for each clock tick.

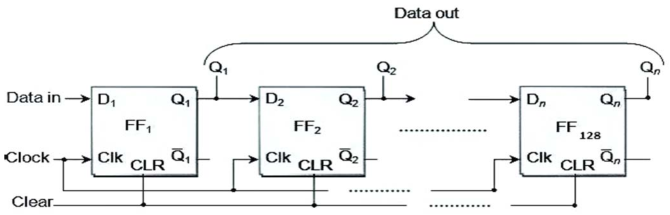

Figure 4: 128-bit Serial-In Parallel-out (Right-shift) Shift Register [10]

B. AES Block Diagram

AES 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 allows a 128-bit data length that is divided into four basic operational blocks. These blocks are treated as an array of bytes and formed as a matrix of the order of 4×4 that is called the state. For full encryption, "number of rounds" = 10, 12, 14 for key length 128,192 and 256 respectively) are used [12].

The AES algorithm consists of three phases [11]. In the first phase, an initial addition (XORing) is performed between the input data (plaintext) and the given key (cipher key). In the second phase, a number of standard rounds ("number of rounds" -1) are performed, which represents the operating kernel of the algorithm. In the proposed module, AES 128-bit key size is used. Each standard round includes four fundamental algebraic function transformations on arrays of bytes as following:

(1) Byte substitution using a substitution table (Sub Bytes).

(2) Shifting rows of the State array by different offsets (ShiftRow).

(3) Mixing the data within each column (MixColumn).

(4) Adding a round key to the State array (AddroundKey).

The third phase of the AES algorithm represents the final round of the algorithm, which is similar to the standard round, except that it does not have a MixColumn step as shown in figure 5.

Decryption process involves reversing all the steps taken in encryption using inverse functions as shown in Figure 5 [13].

C. Mutual Authentication of the generated key at the encryption and decryption processes

The suggested communication algorithm in [4, 5], depends on initiating communications between the two communicating devices through a third trust party (TTP). In general, TTP in cryptography is defined as an element that facilitates interactions between two parties who both trust the third party. As an example, the TTP authentication protocols used to implement Mobile Agent System (MAS), which is able to control consumers' requests, migrates between platforms [14].

The proposed module illustrated in Fig.1, based on taking into consideration the advantage of the uniqueness property of the 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.

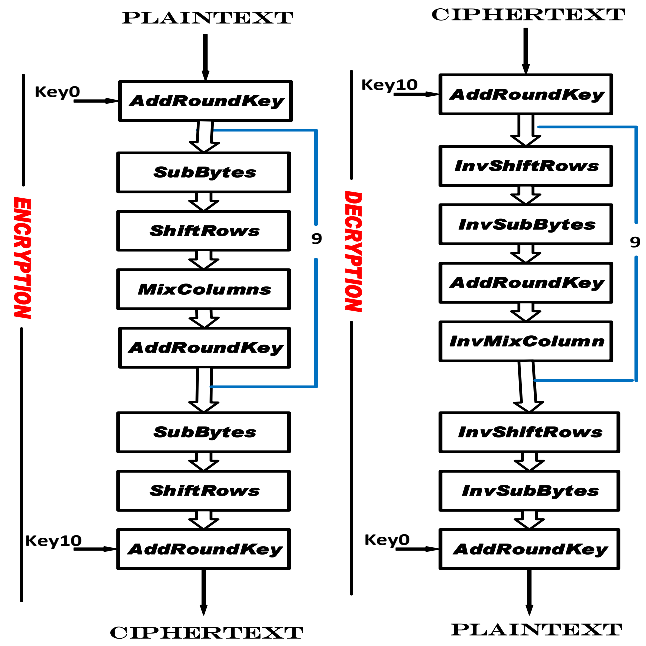

Figure.5 AES Block Diagram for a 128-bit key size.

III. SIMULATION RESULTS

The Memristor and 3-bit T-ADC circuits are verified using Cadence Spectra simulation tool and the TSMC 130nm CMOS technology. The ThrEshold Adaptive Memristor Model (TEAM Model) for the Memristor is used with the proposed circuit. For more information on the TEAM model; please refer to [15].

A. Memristor IV characteristic curve

Fig.6 represents the Memristor I-V characteristics that result from applying the input sin waveform current from (-80µA to 80µA) and at initial state = zero.

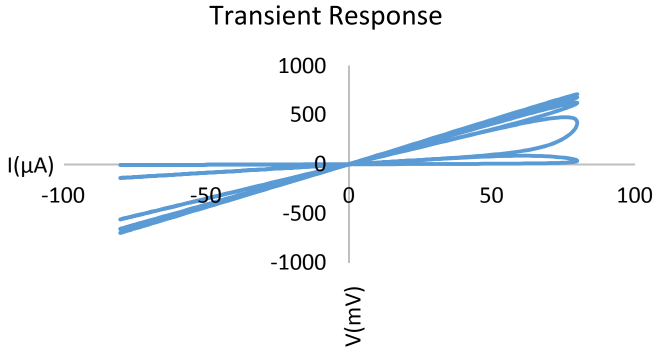

Figure. 6. Memristor I-V Characteristics by sweeping the input current from (-80µA to +80µA) at frequency=100 MHz at initial state= zero.

B. 3-bit T-ADC output and Key generation

Table 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 Fig.6 or Fig.7 are digitized through the 3-bit T-ADC. Note that, the resolution of the proposed 3-bit T-ADC =200mV/ 8=25 mV, where 200mV is the T-ADC dynamic range. This means that every 25 consecutive values give the same digital output.

TABLE 1.

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 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

C. AES processes

TABLE.2

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 3a
66 20 74 68 69 73 20 41 44 43 20 3d 32 30 30 6d	a2 e6 44 lc 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 lf cd 51 67 70 09 8c ef 18 14 20 e8 e4 06
65 64 20 52 61 64 79 43 61 69 72 6f 20 55 6e 69	44 39 52 e9 ee 05 fd fl 6a 98 de d5 ld d6 8f 8d
76 65 72 73 69 74 79 20 6e 61 6e 6f 20 70 72 6f	41 df 4a 44 ae fl b9 88 27 6d cc a4 a9 c2 2e 05

Table 2 shows 5 Plaintext messages after converted from Text to Hexadecimal. These messages are encrypted by using the generated 128-bit key through AES algorithm as in the following steps: Convert the 128-bit key and one plaintext message to Hex.by binary to Hex., Text to Hex respectively, by Converter online tools. Select 32 Hex. (128-bit) from the converted message and insert it into (RTL code) to get the encrypted message. The resultant encrypted message has been taken to (AES online Domain Tools) for Decryption and verify the trustworthiness of the encryption process.

IV. CONCLUSION

In this paper, Memristor-based AES 128-bit key generation is proposed. The work is relying on the uniqueness property of each Memristor devices. Memristor as a nanoscale candidate is preferred over others due to its highly nonlinear characteristics that exhibits 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. In future work, AES-192 or AES-256 can be used for highly strong and robust security. Also 6-bit or 8-bit T-ADC for faster digitizing process. Through an experiment, the mutual authentication of the generated key can be verified by tuning the input current of the Memristor at the decryption side.

ACKNOWLEDGEMENT

This work is partially funded by ONE Lab at Zewail City of Science and Technology and CAIRO University, NTRA, ITIDA, ASRT, Mentor Graphics, NSERC.

REFERENCES

.

[1] Rose, Garrett S. "Security meets nanoelectronics for Internet of things applications." *,Proceedings of the 26th edition on Great Lakes Symposium on VLSI, pp. 181-183. ACM, 2016.*

[2] M. Uddin, B. Majumder, and Garrett S. Rose. "Nanoelectronic Security Designs for Resource-Constrained Internet of Things Devices: Finding Security Solutions with Nanoelectronic Hardwares.*" IEEE Consumer Electronics Magazine 7, pp.15-22, 2018.*

[3] 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).*

[4] 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.*

[5] Hossam, H., M. Dessouki, and H. Mostafa, "Time-Based Read Circuit for Multi-Bit Memristor Memories", *IEEE International Conference on Modern Circuits and Systems Technologies (MOCAST'18)*, Thessaloniki, Greece, pp. 1-4, 2018.

[6] M. Bahnasawi, A., K. Ibrahim, A. Mohamed, M. Khalifa, A. Moustafa, K. Abelmonim, 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.

[7] L. O. Chua, " Memristor - the missing circuit element," *IEEE trans. on Circuit Theory*, vol. 18, no. 5, pp. 507-519, September 1971.

[8] D. B. Strukov, G. S. Snider, D. R. Stewart and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80-83, May 2008.

[9] Hossam, H., 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*

[10] https://www.electrical4u.com/serial-in-parallel-out-sipo-shift-register/

[11] 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.*

[12] M. Prerna, and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security.*", Global Journal of Computer Science and Technology (2013).*

[13] S. Kvatinsky, E. G. Friedman, A. Kolodny, and U. C. Weiser, "TEAMThrEshold Adaptive Memristor Model", *IEEE Transactions on. Circuits and Systems.* I: Regular Papers, vol. 60, no. 1, pp. 211-221, January 2013.

[14] H. Mostafa and Y. Ismail, "Statistical Yield Improvement Under Process Variation of Multi-valued Memristor-Based Memories,"*Microelectrons. Journal*, vol. 51, pp. 46–57, May 2016.