Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES) – An International Journal
ISSN: 2566-932X, Vol. 6, Issue 2, May 2022

Physical Unclonable Design for Key Generation for AES Encryption Algorithm

Pramila B
Associate Professor, ECE Department, East West Institute of Technology, Bengaluru, India,
bjpramila@gmail.com

Tanmaya M Shetty
Student, ECE Department, East West Institute of Technology, Bengaluru, India,
tanmayamshetty@gmail.com

Bhoomika D
Student, ECE Department, East West Institute of Technology, Bengaluru, India,
bhoomikadevraj725@gmail.com

Pallavi K
Student, ECE Department, East West Institute of Technology, Bengaluru, India,
pallavikpallu03@gmail.com

Abstract: The cryptographic techniques often stored on hardware devices are easy to hack as the keys required for encrypting or decrypting the data must be stored along with the architecture on hardware. This increases a necessity to develop an alternative to key-storing problem. As a solution, a physical unclonable function is proposed. Physical Unclonable Function are circuits which are made up of simple logic devices which are easy to analyse, but it is hard to predict the outputs of such systems. These circuits will be used for key generation for the Advanced Encryption Standard algorithm for data hiding, as part of the proposed project work.

Keywords: Cryptography; Advance Encryption Standard; Physical Unclonable Functions

I. INTRODUCTION

The most widely and popularly adopted and used encryption standard nowadays is Advanced Encryption Standard (AES). Its original name is Rijndael. It was established by the U.S National Institute of Standards and Technology in the year 2001. AES is found to be at least six times faster than triple DES. DES was the first encryption used but the key size was too small, keeping this in mind and to overcome this drawback triple DES was invented. The AES is based on 'substitution-permutation' method. It involves some series of linked operations involving inputs getting substituted by other outputs and shuffling of rows to get the desired output. AES performs on bytes rather than bits.

The AES requires 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. AES can currently encrypt blocks of 16 bytes at a time. The 128 bits or 16 bytes are arranged in rows and columns making it as a 4x4 matrix. In case if the bytes are increased for executing AES does it concurrently. If the plain text is less than 16 bytes then it should be padded.

AES is an iterated block cipher, which means that same operation can be performed many numbers of times on fixed number of bytes. For encryption process these functions can be divided into four steps that is add round key, sub-bytes, shift rows and mix column.

II. AES ENCRYPTION

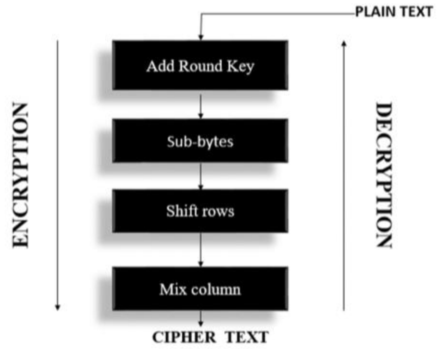

Fig 1. Flow of Encryption and Decryption

In add round key, the data or plain text will be in form of 4x4 matrix this is XORed with the 4x4 keys. The obtained result is now fed to the next step or for further process that is sub-bytes.

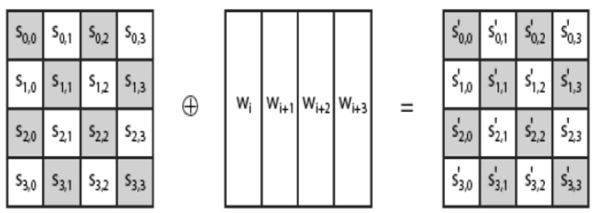

Fig 2. Example of add round key

Sub-bytes means substitution of bytes the 4x4 matrix obtained from add round key is substituted by looking up a fixed table called s-box. For each byte the corresponding rows and columns are checked and is replaced by another value from s-box.

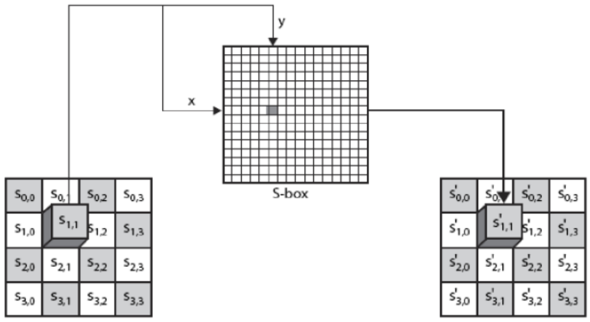

Fig 3. Example of sub-bytes

After substitution of bytes, the 4x4 matrix data undergoes shift row operation, where in the 1st row is not shifted that is kept as it is, 2nd row is shifted one(byte) position to left, 3rd row is shifted two position to left, similarly the 4th row is shifted three position to left.

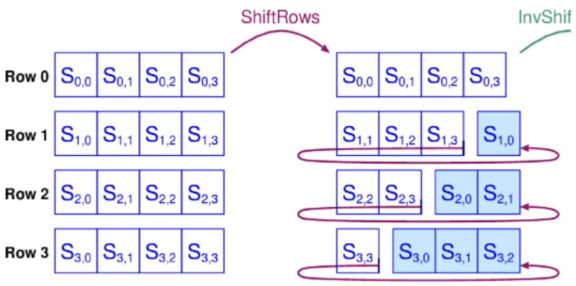

Fig 4. Example of shift rows

Now the mix column step which is the hardest to explain as well as to understand. There are two parts in this step. The first step tells how the two matrix is multiplied and the second one deals with the Galois filed implemented over the multiplied value.

A. Matrix Multiplication

At a single time one column matrix multiplication is done (4 bytes). Every value of the matrix is multiplied against each value in the column matrix. After multiplication of these two values then they are XORed then they become the output for the next state. The multiplication is performed against each value of the column matrix with each row matrix of other one.

$$\begin{matrix} \boxed{2\ 3\ 1\ 1} \\ 1\ 2\ 3\ 1 \\ 1\ 1\ 2\ 3 \\ 3\ 1\ 1\ 2 \end{matrix} \qquad \begin{array}{|c|l} b1 & b5\ b9\ b13 \\ b2 & b6\ b10\ b14 \\ b3 & b7\ b11\ b15 \\ b4 & b8\ b12\ b16 \end{array}$$

The first row of a matrix is multiplied with the first column of other matrix then the obtained result is XORed to produce 1 byte value. For e.g., result1 = (b1 * 2) XOR (b2*3) XOR (b3*1) XOR (b4*1) Similarly this is method is followed for all the rows and columns. It is done until all the columns are completed.

B. Galois Multiplication

The above multiplication is performed over the Galois Field. The concept of this is very difficult to understand. So, this section will instead implement on the two tables known as L and E table which is in HEXA decimal form.

If two HEX values have to be multiplied, we first lookup for L table, the corresponding two HEX values will be taken, then we simply add the number together. After addition if the result is greater than FF, we subtract FF from the addition result. After getting the added value we will look up for E table, again we take the 1st digit to lookup the vertical index and 2nd digit to lookup the horizontal index. The values obtained from E table will be the result of the HEX values taken in the beginning over a Galois Field.

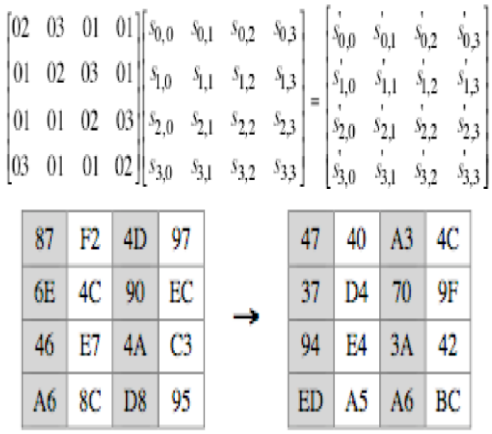

Fig 5. Example of mix column

Similarly, all the steps are performed over all the numbers in matrix and obtained text will be the cipher text.

III. DECRYPTION PROCESS

The conversion of cipher text from the encryption process to the plain text again is called decryption. It is generally the reverse process of encryption. Steps involved in this process are Inverse mix column, Inverse shift rows, Inverse sub-bytes, Inverse add round key. Steps are same as encryption process but in reverse order. The cipher text obtained after encryption process is fed as input to decryption process. In inverse mix column step using L and E table the values are obtained in shift rows 1st row is not shifted, 2nd row is shifted one position to right, 3rd row is shifted two positions to right, 4th row is shifted three positions to right. The obtained shifted matrix now undergoes substitution using Inverse S-box table. Now 128 bits of matrix from sub-bytes is now XORed with the random generated matrix, the output obtained is same as input to encryption process.

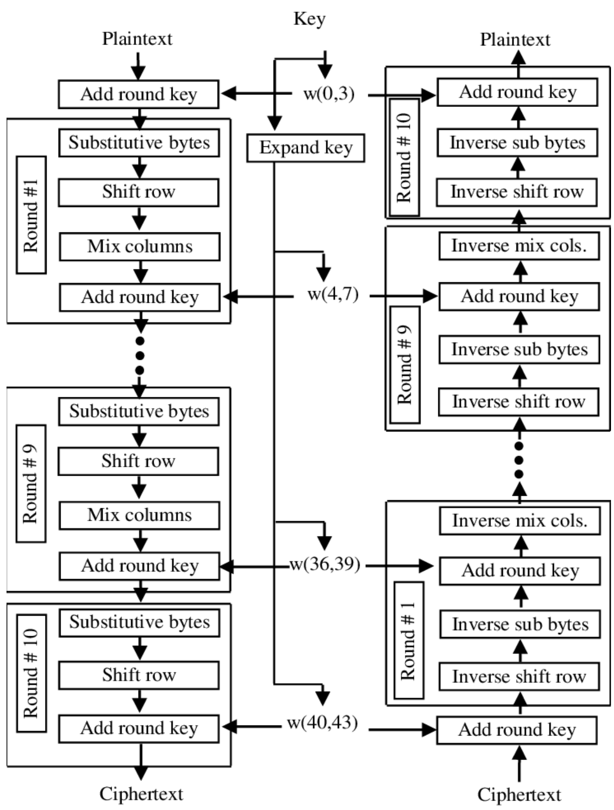

Fig 6. Process of AES Encryption and decryption

IV. PHYSICAL UNCLONABLE FUNCTIONS

Since it is easy to analyze or hack the system which are implemented on hardware devices and even during fabrication wire delays are introduced between the components of circuitry introduces a "surprise" factor to circuit developed, thus making it difficult to predict output at given time and this is the same principle of PUF. Physical unclonable function are circuits which are made up of simple logic devices which are easy to analyze, but it is hard to predict the outputs of such systems.

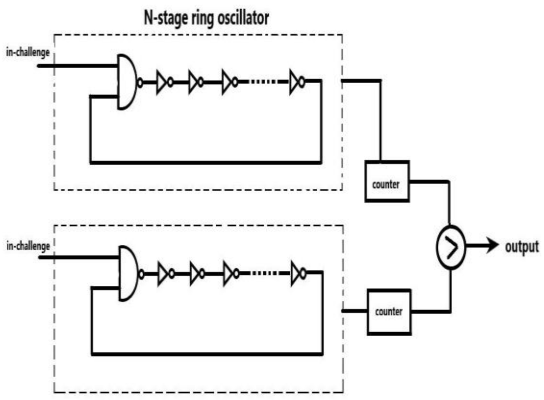

Fig 7. 1-bit ring oscillator based PUF

A 1-bit PUF consists of three major units- 2 N stage ring oscillator, two counters and one comparator. A ring oscillator are a series of inverters connected in series with a negative feedback system. The in-challenges work as enables to the ring oscillators for them to produce single bit values. Every time a "1" bit is generated by the ring oscillator; the counter must increment by 1. To generate 1 bit of result 2 ring oscillators and counters must be working in parallel. Due to varying wiring delays in ring oscillator generated due to fabrication, only one of the counters will reach its maximum limit. If the first counter reaches the maximum limit, the output is "0", otherwise the output is "1". In this manner 128-bits must be generated to obtain the 128-bit key for add round key of AES. Once the data is XORed with the key during add round key step, the remaining steps of AES-shift rows, mix-column and sub-bytes are performed. To verify the working, decryption must also be performed to retrieve the plain text from the cipher/encrypted data.

A. Literature Review

Jeeson Kim, Taimur Ahmed, Hussein Nili, Jiawei Yang, Doo Seok Jeong, Paul Beckett, Sharath Sriram, Damith C. Ranasinghe, and Omid Kavehei, "A Physical Unclonable Function with Redox-based Nanoionic Resistive Memory" - Redox-based(reduction oxidation) based resistive memory, it acts like switch and for ReRAM's memories, it has nano-fabrication process. PUF with Redox-based device then analyze the cyber-physical Security Application and performance, observe the characteristics. Redox based resistive memories is one of the most promising devices for information processing and memory application. Various PUF performance metrics have been analyzed. Redox based provide low-cost, low power, and secure unclonable function. ReRAM have disadvantage of using a combination of novel architectural and peripheral circuity.

Erik Sargent and Weston Jensen, "Authentication using a physically unclonable function" - In this project PUF was development on a FPGA board to implement a form of authentication project will discuss how the PUF was designed tested and how well it worked. Using PUF's function on FPGA, are really efficient at minimizing and matching signal propagation delays. They use arbiter PUF's, but generally do not work well on FPGA devices because they have function variations in signal propagation delay.

Sangjae Lee, Mi-Kyung Oh, Yousung Kang, and Dooho Choi, "Implementing a phase detection ring oscillator PUF on FPGA" - PUF protects the IOT devices and hardware and software technologies because IOT devices had a proliferation issue it is affected to key management and generation of digital identifier PUF helps to generate the device specific IDs to protect the hardware cloning and RO PUF uses phase detection scheme to generate a random output of PUF. For implementing the phase detection two block of RO devices are used for comparison of phase, light and images. More circuit complexity and distortion occur while detecting any signals.

Likhithashree R and Divya Kiran, "Design of Power-Efficient Ring Oscillator based Physically Unclonable Functions for FPGA" - For data transfer and communication purpose people used reconfiguration devices means rearrange the settings of systems or elements or applications of the devices so this is easy for the attackers of the devices have sensitive property. Because of this condition they design "Ring oscillator based Physically Unclonable Function". FPGA it provides security for the devices and avoid the hacking process. Existing approaches are power exhaustive due to computation complexity, produce power overhead issues. Number of circuit stages are required to implement the design of RO on FPGA.

V. CONCLUSION

The PUF can be simulated to generate different fabrication delays to obtain 128-bit key. This key must be used to encrypt/decrypt a 128-bit data. This PUF will be added to AES add round key step to generate cryptic keys to make the hacking 'nearly' impossible.

REFERENCES

[1] Mahin Anil Kumar and Ramesh Bhakthavatchalu, "FPGA based delay PUF Implementation for security applications", Department of electronics and communication engineering, Amritha Vishwa vidhyapeetam, Amritapuri, kerala, India, 2017 IEEE International Conference on Technological Advancements in power and Energy(TAP Energy), 978-1-5386-4021-0/17/$31.00 (c)2017 IEEE.

[2] Likhithashree R and Divya Kiran , "Area – Efficient Physically Unclonable Functions for FPGA using ring oscillator", Department of ECE, Ramaiah University of Applied Sciences, Bengaluru, India, Proceedings of the Second International conference on Innovative Mechanisms for Industry Applications(ICIMIA 2020), 978-7281-4167-1.

[3] Erik sargent and Weston Jensen," Authentication using a Physically Unclonable Function", Utah state University Department of electrical and Computer Engineering.

[4] Likhithashree R and Diva Kiran, "Design of Power-Efficient Ring Oscillator based Physically Unclonable Functions for FPGA", Ramaiah University of Applied Sciences, Bengaluru, India, 2019 4th international conference on Electrical, Electronics, Communication, Computer technologies and Optimization Techniques (ICEECCOT), 978-1-7281-3261-7/19/$31.00 (c)2019 IEEE.

[5] Tatsumi Tanamoto, Shinich Yasuda, Satoshi Takaya and Shinobu Fujita,"Physically Unclonable Function using Initial Waveform of Ring Oscillators", Corporate R & D center, Toshiba corporation, Saiwai-Ku, Kawasaki 212-8582,Japan, 1549-7747 (c)2016 IEEE.

[6] Alexander spenke, Ralph Breithaupt and Rainer plaga,"An arbiter PUF secured by remote random reconfigurations of an FPGA", Hochschule Bonn-Rhein-Sieg,53757 Sankt Augustin, Germany, federal Office for information Security(BSI), 53175 Bonn, Germany, 12 Oct 2016.

[7] Jeeson Kim, Taimur Ahmed, Hussein Nili, Jiawei Yang, Doo Seok Jeong, Paul Beckett, Sharath Sriram, Damith C.Ranasinghe, and Omid Kavehei, "A Physical unclonable Function with Redox-based Nanoionic Resistive Memory", RMIT University, 15 NOV 2016.

[8] Muthumeenakshi.N, Hari Prasath Sharma.S, farjanaaameera.M, Rajaprabha.R," VLSI Design of Low Cost(PUF) Physical unclonable Function Using FPGA and Highly Secured Clock Network", IOSR Journal of VLSI and signal Processing (IOSR-JVSP), Jan 2014.

[9] ye wang, Xiaodan Xi, and Michael Orshansky,"Lattice PUF: A Strong Physical unclonable Function Provably Secure against Machine learning attacks", Department of Electrical and Computer engineering, The University of Texas at Austin, USA, 16 Jun 2020.

[10] Sangjae Lee, M-Kyung Oh, Yousung Kang, and Dooho Choi, "Implementing a phase detection ring oscillator PUF on FPGA", Information Security Research Division, Electronics and Telecommunication Research Institute, Daejeon, Korea, 978-1-5386-5041-7/18/$31.00 (c)2018 IEEE.

[11] Seda arslan Tuncer," Real-Time Random Number Generation with Ring Oscillator Based Double Physically Unclonable Function", Firat University, Department of Software Engineering, Elazig, Turkey, 2018.

[12] Armin Babaei and Gregor Schiele,"Physical Unclonable Functions in the internet of Things: State of the Art and Open Challenges", Embedded Systems Group, Faculty of Engineering, University of Duisburg-Essen,47048 Duisburg, Germany, 2019.

[13] N. Sivasankari and A.Muthukumar,"Implementation of a Hybrid Ring Oscillator Physical Unclonable Function", Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, India and Kalasalingam university, India ICTACT Journal on Microelectronics, July 2018.

[14] A.Poorna chander Reddy, Dr.M. Siva Kumar, B. Murali Krishna, Syed Inthiyaz and Sk. Hasane Ahammad," Physical Unclonable function based Design for Customized Digital Logic circuit", Department of ECE, Koneru Lakshmaiah education foundation, Vaddeswaram(A.p), India, (c)2019 IJAST.

[15] Wenjie Xiong, Andre Schaller, Stefan Katzenbeisser, and Jakub Szefer,"Dynamic Physically Unclonable functions", Yale University, New Haven, CT, USA and Technische Universitat Darmstadt, Darmstadt, Germany, 2019

[16] Jiliang Zhang ,Gang Qu,"Physical Unclonable Function – based key Sharing via Machine Learning for IoT Security",IEEE Transactions on Industrial Electronics,21 Aug 2019.

[17] Yi Zhang, Min Zhu, Bohan Yang, Leibo Liu," A Highly Reliable Strong Physical Unclonable Function Design Based on FPGA", Institution of Microelectronics, Tsinghua University, Beijing, China,13th International conference on Computer and Electrical Engineering, 2020.

[18] Teng Xu and Miodrag Potkonjak,"Robust and Flexible FPGA-based Digital PUF", Computer Science Department ,University of California, Los Angeles , 2014.

[19] Chongyan Gu, Weiqiang Liu, Yijun Cui, Neil Hanley, maire O'Neill, Fabrizio Lombardi,"A Flip-Flop Based Arbiter Physical Unclonable Function (APUF) Design with High Entropy and Uniqueness for FPGA implementation" centre for Secure information technologies(CSIT), Institute of electronics, communications & information technology(ECIT),2019.

[20] Cedric Marchand, Lilian Bossuet, Ugo Mureddu, Nathalie Bochard, Abdelkarim Cherkaoui, Viktor Fischer, "Implementation and characterization of a physical unclonable function for Iot: a case study with the TERO-PUF", Hubert Curien Laboratory, Prof.Lauras, St-Etienne, France, TIMA Laboratory, Avenue Felix viallet, Grenoble, FRANCE (c)2017 IEEE.