Computers, Materials & Continua
DOI: 10.32604/cmc.2022.023516
Article

Tech Science Press

Invariant of Enhanced AES Algorithm Implementations Against Power Analysis Attacks

Nadia Mustaqim Ansari[1,*], Rashid Hussain[2], Sheeraz Arif[3] and Syed Sajjad Hussain[4]

[1]Department of Electronic Engineering, Dawood University of Engineering & Technology, Karachi, Pakistan
[2]Faculty of Engineering Sciences and Technology, Hamdard University, Karachi, Pakistan
[3]Faculty of Information Technology, Salim Habib University, Karachi, Pakistan
[4]Faculty of Computer Sciences, SZABIST, Karachi, Pakistan
*Corresponding Author: Nadia Mustaqim Ansari. Email: nadia.ansari@duet.edu.pk
Received: 11 September 2021; Accepted: 10 January 2022

Abstract: The security of Internet of Things (IoT) is a challenging task for researchers due to plethora of IoT networks. Side Channel Attacks (SCA) are one of the major concerns. The prime objective of SCA is to acquire the information by observing the power consumption, electromagnetic (EM) field, timing analysis, and acoustics of the device. Later, the attackers perform statistical functions to recover the key. Advanced Encryption Standard (AES) algorithm has proved to be a good security solution for constrained IoT devices. This paper implements a simulation model which is used to modify the AES algorithm using logical masking properties. This invariant of the AES algorithm hides the array of bits during substitution byte transformation of AES. This model is used against SCA and particularly Power Analysis Attacks (PAAs). Simulation model is designed on MATLAB simulator. Results will give better solution by hiding power profiles of the IoT devices against PAAs. In future, the lightweight AES algorithm with false key mechanisms and power reduction techniques such as wave dynamic differential logic (WDDL) will be used to safeguard IoT devices against side channel attacks by using Arduino and field programmable gate array (FPGA).

Keywords: Side channel attacks; power analysis attacks; network security; masking; advance encryption standard

1 Introduction

Internet-of-things (IoT) establishes connections between billions of smart devices, performing a diverse range of purposes. Connected devices will grow to almost 31 billion in the world of IoT [1]. These devices embedded with sensors, software to exchange and collect data with each other. In the early era, IoT was used only by specific people which were related to media and researchers. Day by day, most of the people taking interest in IoT. Some research areas in security of IoT devices are predictions and prevention of security issues, protected applications of the web, attacks of IoT devices,

size of devices, performance of devices, power usage of devices, recognition of devices, and confirm availability at high demand. So, in 2008 first international conference was held in Switzerland on the topic of IoT. Twenty-three different countries participated in that conference and gave their input to explore the IoT world [2].

According to a published report in 2013, revenue generation using IoT-based devices, will be more than 300 billion by the end of the 20th century. So, when more devices communicate with each other than network complexity and hardware security will increase. By Statista (a statistical website) the number of devices around the world used for IoT network will noticeably increase from 20.35 billion to 75.44 billion from 2017 to 2025. Now researchers are working to explore the security of constrained devices including integrated circuits, microcontrollers, sensors, and wearable gadgets, among other similar hardware. With the exponential increase of its infrastructure, there are plethora security concerns. Hardware attacks are categorized by hardware trojan, side channel analysis, fault attacks, counterfeit chips, and reverse engineering [3].

Side channel analysis is more considerable attack for the researchers. This attack involves analyzing the external outputs of the hardware and retrieving the information. Side channel attacks (SCA) is most powerful attack against encryption, but this attack is hard to implement. Initially, SCA was implemented at the edge node level. At this level, SCA are usually non-invasive and intentionally leaked information is extracted. Untraceable is the important characteristic of non-invasive attack and the result of this property is the addition of noise to the information which is leaked and hard to secure the whole process. SCAs based on processing time or power consumption of the device rather than plaintext or ciphertext messages. This information is observed during the computation of different security protocols. The process of SCA is to recover the information processed in Advanced Encryption Standard (AES) algorithm encrypted enable device by observing the power consumption, electromagnetic (EM) field, timing analysis, and acoustics of the devices as shown in Fig. 1 [4].

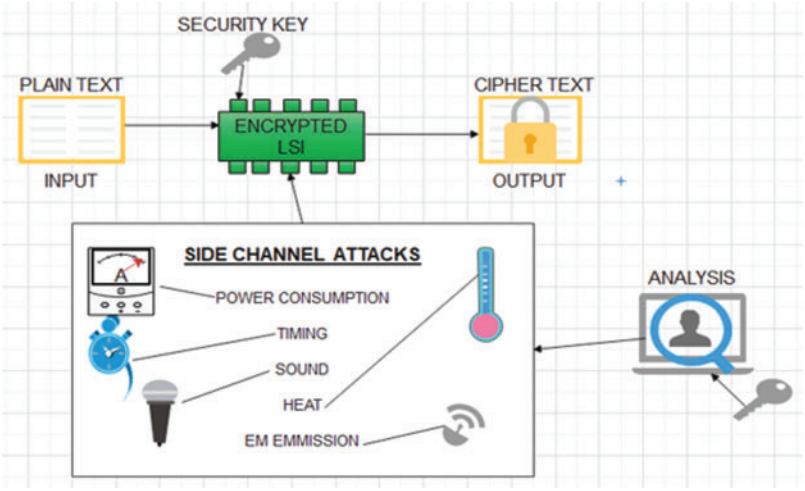

Figure 1: Working of side channel analysis

The most effective type of SCAs is power analysis attacks (PAAs) as they are easy to achieve in exercise and at relatively low cost for attackers. PAAs works on power calculation. Every PAA mechanism needs the usage of a particular power model of the IoT device for the forecast of the real power to be consumed by the device, by the observing specific procedure of the algorithm and choosing the output word for the attack because the power consumption of electronic circuits based on the bit

word-processed by themselves. The power model is developed considering the logical characteristics of the data word. After that, consumption of actual power and power model are compared by using different variables. IoT devices operate at low power because they have short storage and complicated process; hence the algorithm may fail, and devices become corrupted. All mentioned reasons are very much helpful for PAA [5–7].

Simple power analysis (SPA), Differential power analysis (DPA) and Correlation power analysis (CPA) are the main types of PAAs. In SPA, a single display shows the power trace of a cryptographic device and tries to establish the secret key based on the electrical levels over time. In DPA, statistical techniques are used to recognize differences in power traces, thus showing data leakage to guess the secret key. Generally, in CPA to identify the correlation between predicted output and the actual power output of an encrypted device by using the hamming weight power model [8].

Researchers use countermeasures for SCA and categorize them into masking techniques, hiding techniques, and code morphing techniques. Hiding relates to the hardware of the system and masking relates to changes in the algorithm through software [9]. When the function of cryptographic devices is performed then attackers perform DPA and apply statistical function on measured power consumption traces to recover the secret key [10]. The security of IoT devices should achieve a certain level without an increase in area and performance overhead by using reconfigurable voltage regulators [11]. Masking is a countermeasure against SCA, since it enhances the security. It can break the dependence between the power consumption and the intermediate values in the cryptographic algorithm. Following are the different types of masking schemes: Boolean masking, additive masking, multiplicative masking, mixed masking, gate level and algorithmic level masking [12].

In this manner, the National Institute of Science and Technology (NIST) endorsed the AES, in 2001. Higher security levels and low complexity are characteristics of AES. This algorithm has proved to be a good security solution for constrained IoT devices [13]. AES requires large memory size because it has 800 bytes of lookup tables, and if system wants more secure then increase the number of lookup tables as well as increase capacity. AES algorithm ensures stronger cloud-based secure storage. AES-128 offers more secure system, faster encryption speed and gives better throughput compared to another encryption algorithm. But still, improvement will further reduce hardware dependency, provide more security, and minimize overheads on the data [14].

AES is the most powerful symmetrical algorithm against SCA and is designed based on a block cipher. It plays a vital role in securing the network from attackers. It is supported for data privacy [15]. AES has four transformations:

1. Add Round Key 2. Substitution Byte 3. Shift Rows 4. Mix Column

Add a round key based on key extension algorithm. This algorithm runs parallel to the AES rounds and provides the key for each round. It has three functions.

1. Rotation Word 2. Substitution Word 3. Round Constant

One round of AES consists of 2 layers:

1. Non-linear Layer: Substitution Byte transformation is only non-linear function in AES.
2. Linear Layer
   a) Shift Rows is a linear part of the AES. b. Mix column is a linear part of the AES.

As above define the substitution byte is the only non-linear function and based on the values of Substitution Box (S-BOX) for encryption and INVERSE S-BOX for the decryption process. The backbone of the cryptographic system is S-BOX because of its non-linear property. It is based on

substitution-permutation networks (SPNs) and built by Galois Field for the AES and Data Encryption Standard (DES) algorithm. Attackers use 'S' boxes for differential attacks [16]. Using a polymorphic variant of the Advanced Encryption Standard (P-AES) increases data safety. The values will change with each new key in P-AES and in basic AES, Substitution Bytes, Shift Rows and Mix Columns transforms have been made dependent on the keys [17].

This research paper adequately investigates the literature on AES and their types in the IoT. Compares different encryption algorithms, then we analyze and explore the characteristics of AES which is used to provide security of different IoT devices. For prevention of SCAs on IoT devices, a proposed model is presented. This paper implements and resurrects a model which is based on enhancement of the AES algorithm using logical masking property and demonstrates hardware attacks with countermeasure algorithms on IoT devices comprehensively. This enhanced AES invariant algorithm masks the bit array by using the masking technique in converting AES substitution bytes effectively. This model is used for SCAs and particularly PAAs. Simulation model is designed on the MATLAB simulator by using a script. Results will validate and provide a better solution by hiding the power profile of IoT devices from the AES [18].

The rest of this research paper is organized as follows: In Section 2 methodology is present. Section 3 defines the implementation environment of the model. Section 4 shows the procedure and results. Section 5 defines the research contributions. Section 6 discusses the results obtained by implementing the proposed model. Section 7 shows the conclusions and future work of the research paper.

2 Methodology

In literature the expansion of demand pushes towards improving information encryption algorithms. Cryptographic algorithms are used to provide security of the IoT devices, and it helps minimize the total implementation cost and covers various parameters such as power consumption, key size, throughput rate, and cycle rate. Symmetric lightweight and asymmetric lightweight ciphers are the types of lightweight cryptography. To cope with attacks, we have different encryption algorithms: As Tab. 1, shows comparison of some encryption algorithm details which are used to secure the hardware of IoT environment. All algorithms have different pros and cons, but all mentioned algorithms, IoT devices support AES algorithm. To secure the data AES and RSA (Rivest-Shamir-Adleman) algorithm are used. DES (Data Encryption Standard) and 3DES (Triple Data Encryption Standard) isn't secure any longer and it can be broken easily. TWOFISH and BLOWFISH are slower than AES in terms of processing time. In RC2 (Rivest Cipher), encryption operation is not equal to decryption operation. RC5 and RC6 are now outdated. CAST (Carlisle Adams and Stafford Tavares) is less secure because it is open access algorithm. IDEA (International Data Encryption Algorithm) has many weak keys by design. DSA (Digital Signature Algorithm) is only used for authentication of data. ECC (Elliptic Curve Cryptography) has less computational power. Speed of ELGAMAL is low because memory size of ciphertext is double as plain text. SPECK specifically used for hardware attacks such as side channel attack and LiCi used to increase efficiency, minimize area, and low energy consumption of the system [19–22].

Table 1: Comparison of cryptographic algorithms [19–22]

S. no.	Algorithm name	Type (symmetrical/ asymmetrical/ hash function)	Published year	Block size	Key size (bits)	structure	Number of rounds	Remarks
1	DES	Symmetric	1975	64	54	Feistel	16	Less secure (brute force search)
2	3DES	Symmetric	1995	64	56/112/168	Feistel	48	Increase the runtime, now deprecated.
3	AES	Symmetric	2001	128	128/192/256	SPN	10/12/14	Extremely effective on equipment.
4	RSA	Asymmetric	1977	86/214	1024	X	1	Slow for big data.
5	TWOFISH	Symmetric	1997	128	128/192/256	Feistel	16	Slower than the ESA.
6	BLOWFISH	Symmetric	1993	64	32–448	Feistel	16	Initialize slowly with each change button.
7	RC2	Symmetric	1987	64	1–128 bytes	Feistel	18	Encryption operation does not equal the decryption operation.
8	RC6	Symmetric	1998	128	128/192/256	Feistel	X	Not generally used as RSA.
9	RC5	Symmetric	1994	16/32/64	0–255	Feistel	0–255	Not on duty.
10	CAST	Symmetric	1996	64	40–128	Feistel	12/16	Royalty-free algorithm, free access for anyone therefore less secure.
11	IDEA	Symmetric	1991	64	128	Lamasery scheme	8.5	The large number of weak keys were found.
12	DSA	Asymmetric	1991	X	X	X	X	DSA data is not encrypted, we can only authenticate the data.
13	ECC	Asymmetric	1985	X	160	Algebraic	X	Less power for calculation.

(Continued)

Table 1: Continued

S. no.	Algorithm name	Type (symmetrical/ asymmetrical/ hash function)	Published year	Block size	Key size (bits)	structure	Number of rounds	Remarks
14	ELGAMAL	Asymmetric	1985	514	32 bytes	X	X	Double-encrypt the text into clear text so that the speed is slow.
15	SPECK	Symmetric	2013	128	128	SPN	32	Specifically used for hardware implementation with a micro-controller.
16	LiCi	Symmetric	2017	64	128	Feistel and SPN	31	Use for to increase efficiency, reduce surface area and energy use.

The idea behind our design is to secure the data by using encryption algorithm. Fig. 2 is the generalized flow chart of the proposed work. So, we will discuss highlighted boxes 1 and 2. First box is "Perform AES for encryption" and the second box is "Perform AES for decryption". In this part all the transformations have different properties and different values like add round key, substitution byte, shift rows, and mix column for encryption. Inverse substitution byte, Inverse shift rows and Inverse mix column for decryption. Attackers mainly observe the power consumption at a non-linear part of the AES, i.e., Substitution Byte and Substitution Word in add round key algorithm. Both of functions based on S-BOX.

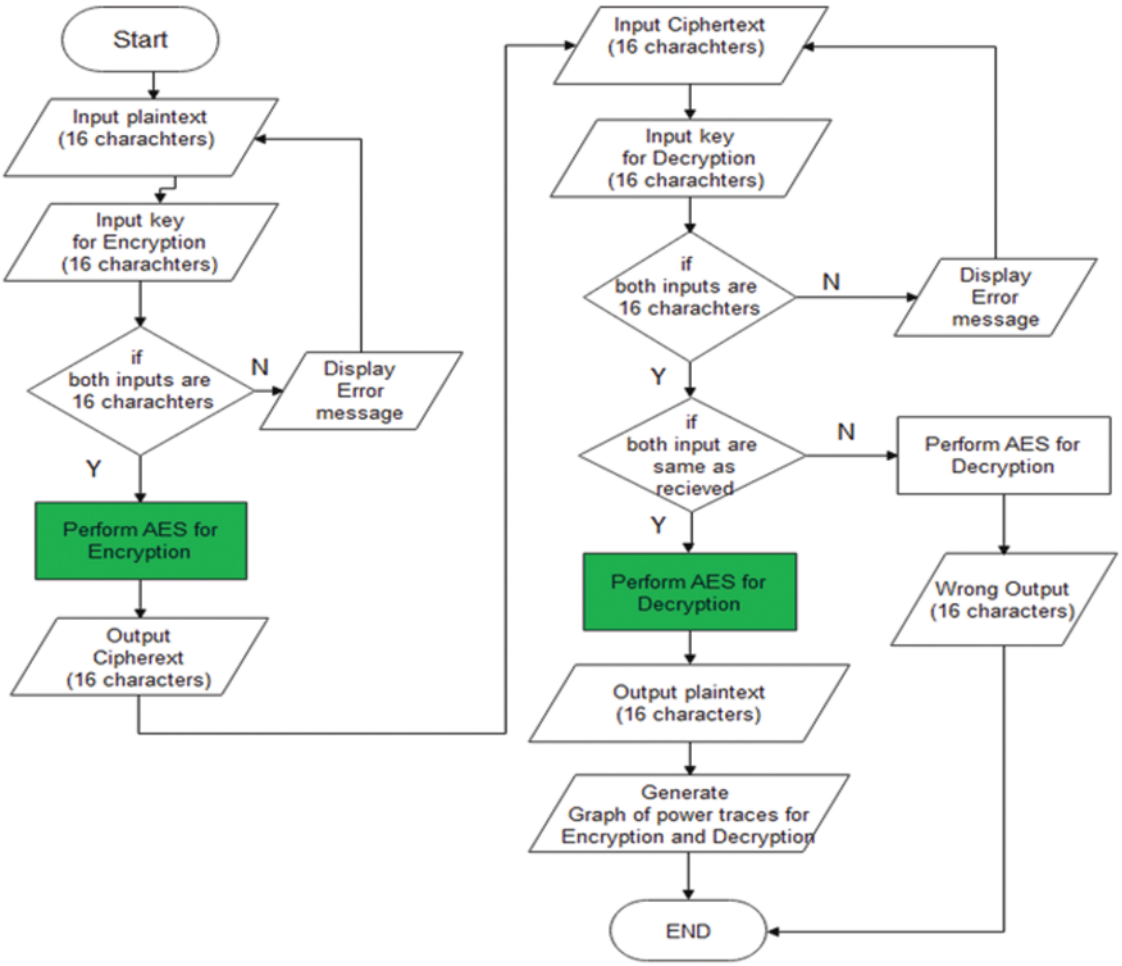

Figure 2: General flow chart of the proposed technique

3 Implementation Environment

Software tools and platform used to implement proposed algorithm is described in Tab. 2.

Table 2: System specification for implants

Name	Specification
IDE	MATLAB
Programming language	C/C++, MATLAB
MATLAB Version	MATLAB 2018a
Operating System	Windows 10 pro 64 bit
Processor	Intel Core Ii7 3rd generation, 2.4 GHz.
RAM	4.00 GB

MATLAB is specially developed for engineers and scientists. It allows the creation or expression of matrices and mathematical tables directly. The use of toolboxes is very important. All toolboxes work together and integrate with parallel computer environments. In MATLAB several algorithms are directly accessible and used in design, interactive applications with immediate visual display with minimal time. Researchers can alter or replicate their work until they get the outcome as they want [23]. AES design on matrix. Plain text and key length, both consist of matrix. Similarly, MATLAB also works on a matrix so, it is easy to manipulate and use by researchers to implement AES in MATLAB and obtain desired results with graphic representation.

4 Procedure and Results

In this section, we have improved the characteristics of the AES algorithm by using a logical masking technique in substitution byte transformation. Here are the steps to redesign and use the AES algorithm in a special way.

i. Enter a plain text as string value from user.
ii. Take an input key as string value from user.
iii. Both inputs have string properties, so, convert them into decimal numbers by using the DOUBLE ( ) function of MATLAB.
iv. By Key Expansion Algorithm generates round keys for every round of AES simultaneously.
v. Then run the XOR operation between the plain text and the 1st round key using the BITXOR ( ) function of MATLAB.
vi. We now have 16 distinct values. These values overwrite the S-BOX values.
vii. We use S-BOX for the encryption process.
viii. S-BOX is 16 x 16 array with decimal values. It means that this box has 16 rows and 16 columns in hexadecimal form start from 0 to F.
ix. The 16 values mentioned in step no. (vi) are replaced by the values of S-BOX.
x. Now shift rows transformation is performed by using circshift( ) function in MATLAB.
xi. Similarly, Mix Column transformation is carried out by the Galois Field array function.
xii. In last the output matrix performed XOR operation with round keys.
xiii. Step no. (xii) is the last step of the 1st round. Likewise, the remaining rounds are conducted one by one and generate a new matrix using loop iterations.
xiv. Finally, after 10th round, we have a ciphertext as shown in Fig. 3.

```
enter plain text,it shuld be 16 charachter with spaces
i m nadia ansari
entr key it should be 16 charachter with spaces
rohaan is my son

****AES Encryption****
Plaintext is:
i m nadia ansari
Key is:
rohaan is my son
    27    79     5    65    15    15    68     0    18     0    12    23    83    18    29     7

   175   118   201   237
   132   118    99   201
   107    27   254   164
   131    99   240   197
```

Figure 3: Output from the AES algorithm

Furthermore, the algorithm converts all values into hexadecimal values as 27 is a decimal number and 1B is a hexadecimal conversion of this number. Thus, 1 and B convert addresses of row and column. This means that 1 row and B column contain the value 175 and replaced by 27. Simultaneously, all the values replaced by their specific row and column. In the decryption process, we use inverse SBOX table in substitution bytes and key expansion algorithm process of AES by using reverse key mechanism. Therefore, starting with SBOX, value of 8th row and 8th column is C4 in hexadecimal and 196 in decimal, this value is generated by the mentioned steps. All input values are replaced by specific SBOX values, and the collective data are sent to the next transformations of AES, which is shift rows and mix column. To process S-box transformations, we propose to use a new SBOX lookup table which is recalculated each time when AES is performed.

Algorithm 1:

1. For i = 1 to 10 do
2. For j = 1 to 16 do
3. $T(i, j) \leftarrow A(i, j) * B(j) \oplus C$
4. Return R

The variable i and j are used for the loop structure and R is the return value after process the equation. When we apply MATLAB code for the above flow diagram, then the output is given below:

Algorithm 2:

1. For j = 1 to 10 do
2. Ciphertext = AES output $\oplus$ Round keys (j)
3. For i = 1 to 16 do
4. If (output values) >0 && (output values < = 128)
5. Then apply logical mask for 5
6. Else apply logical mask for 0

When we apply the proposed algorithm in the above code the result is given below:

In Fig. 4, graph shows the output values of 1^{st} to 10^{th} round of AES algorithm without implementation of masking property as define in algorithm 1. The graph has 16 different values with a different power level, so attackers execute statistical functions on a set of measured energy consumption tracks to retrieve the secret key. Likewise, the graph shows in Fig. 5, the output of 10 rounds of the AES algorithm with the implementation of the proposed masking property as defined in Algorithm 2, in the code section of the script in MATLAB. We select two levels, i.e., 0 and 5. Level 0 shows low level of power and 5 shows high level of power in algorithm 2, the masking logic is applied so that the result displayed in Fig. 5. The graph shows the output values from the 1^{st} to 10^{th} rounds of AES. The chart has 16 different values with the same power level as the previous one, so attackers face the challenge of observing different energy consumption values. The unit of y-axis is power in watt and x-axis labels are number of rounds of AES i.e., 1, 2, 3, ...16.

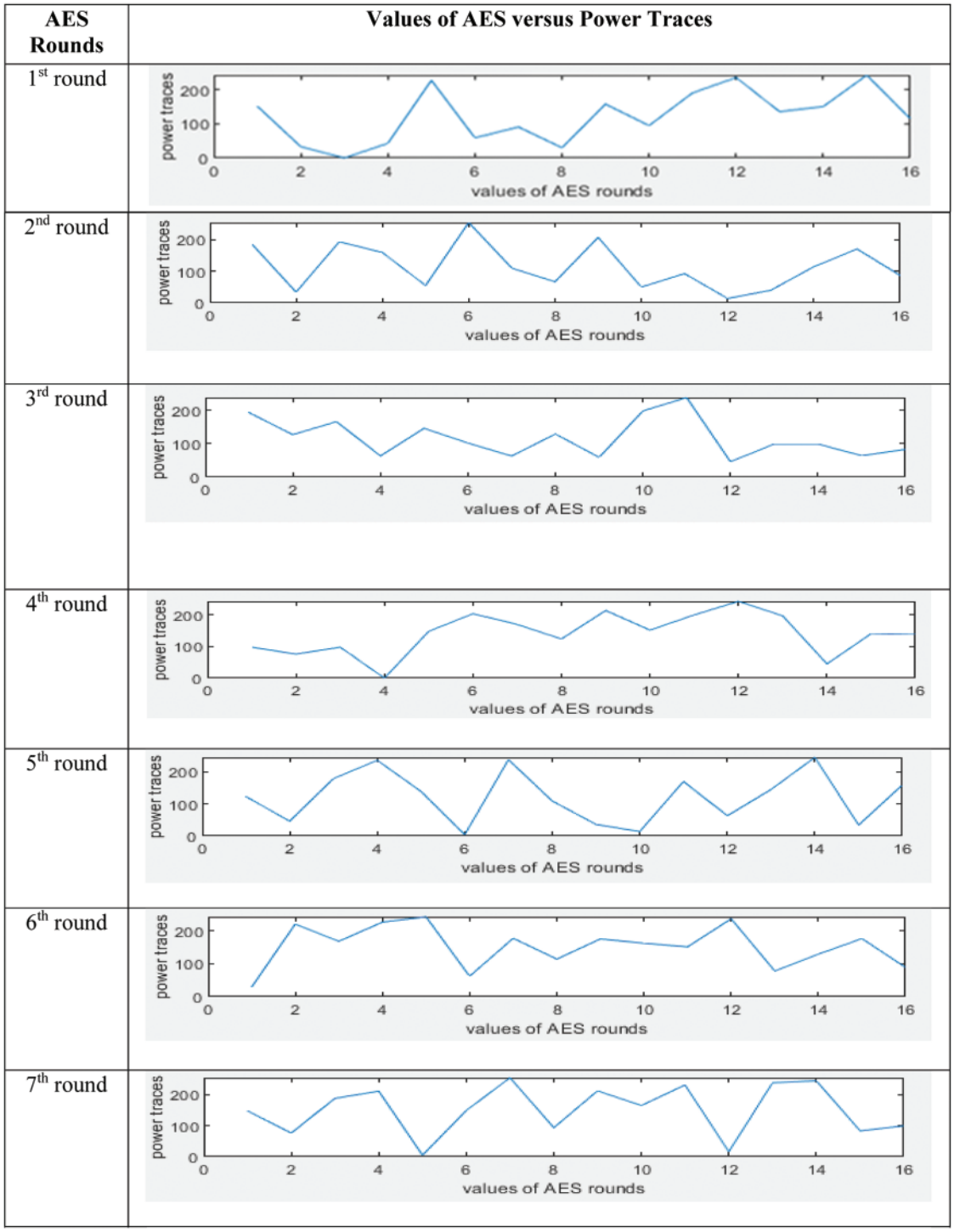

Figure 4: (Continued)

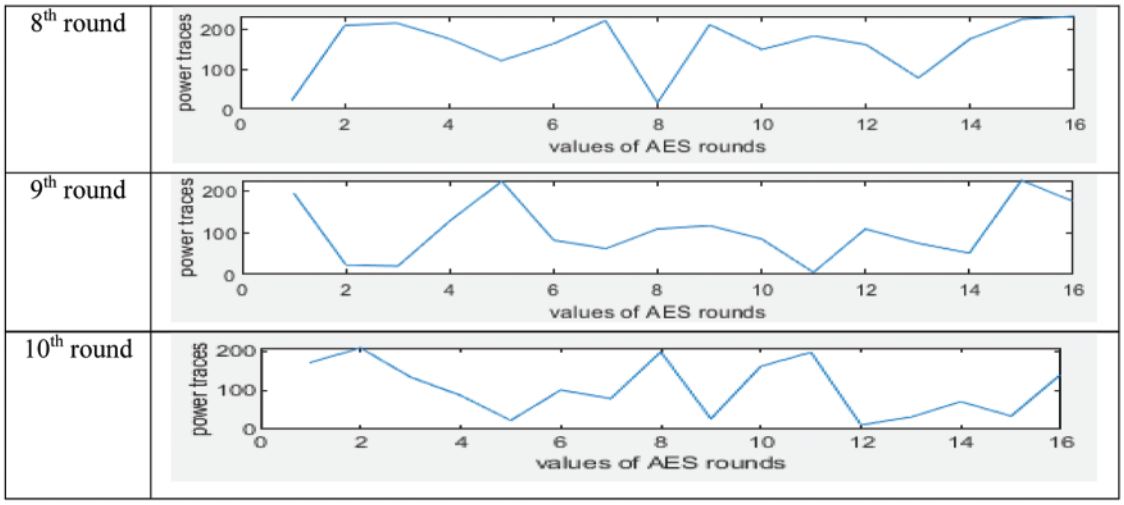

Figure 4: Result of Algorithm 1

Figure 5: (Continued)

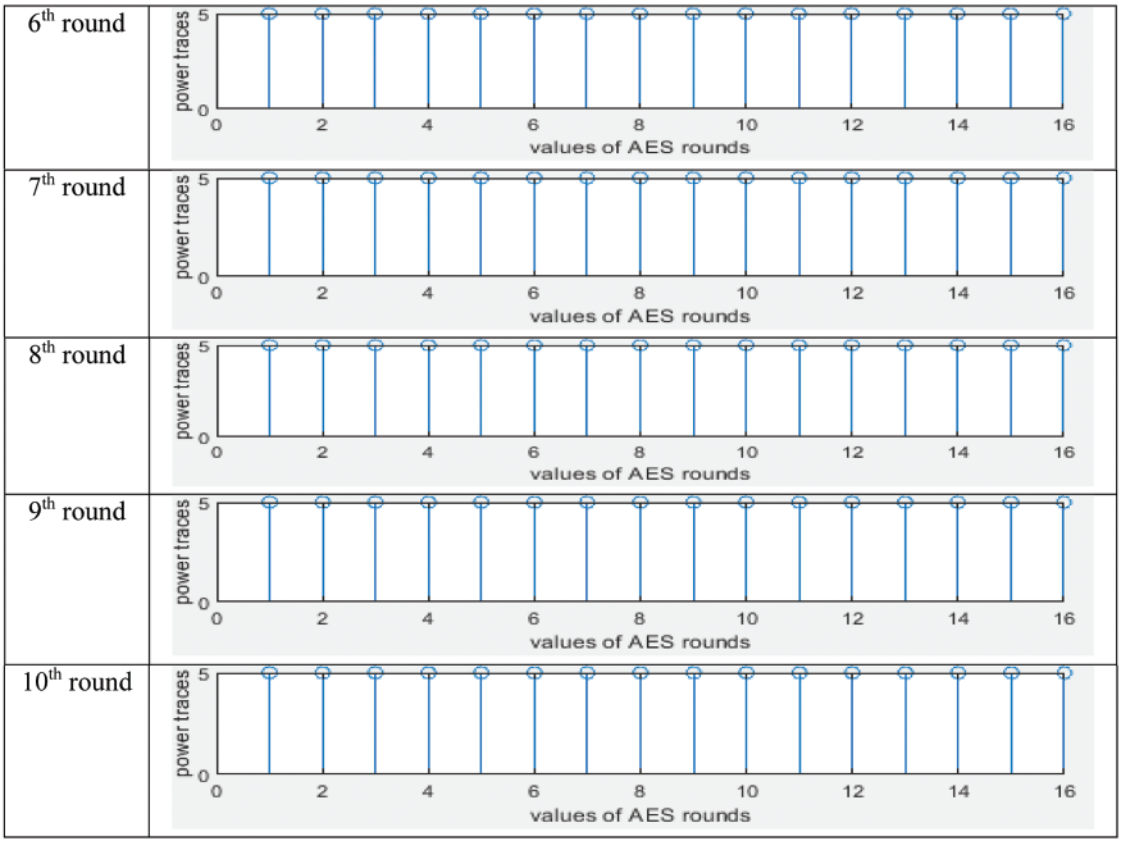

Figure 5: Result of Algorithm 2

5 Research Contributions

This paper is extended version of "Invariant of AES algorithm implementations against side channel attacks in IoT devices", which was presented in ICCOINS 2021 conference and published in IEEE Xplore. In this paper, we work on hiding the power traces of encrypted text using masking technique and get result from the simulation model design on MATLAB. The basic design of simulation was performed in published paper. This paper was based on proposal of generalize AES implementation on MATLAB.

6 Discussion

Attackers analyze different values per differential power analysis (DPA) and retrieve the key. Moreover, this process takes a long time. Thousands of patterns are analyzed by DPA, but attackers perform this activity. Thus, with the help of the proposed algorithm attackers cannot analyze the power and fail to retrieve the key. Also, many researchers provide better solutions against PAAs with different masking techniques like Boolean masking. Results will provide a better solution than that available in the literature to protect IoT device infrastructure against side channel attacks. Temperature and humidity data from the DHT11 and DHT22 sensors will be used as a preliminary experimental configuration. During the attack scenario stages, we will consider clock sampling, which is the vulnerable parameter of the sensor through the correlation analysis. During the counter-measures

phase, the data from DHT11 and DHT22 sensors will go through industry standard for encrypting and decrypting hex strings using AES-128.This analysis will be used as a benchmark for the proposed method.

7 Conclusions and Future Work

This paper implements and resurrects a model which is based on the enhancement of the AES algorithm using logical masking property and demonstrates hardware attacks with countermeasure algorithms on IoT devices comprehensively. This enhanced AES invariant algorithm masks the bit array by using the masking technique in converting AES substitution bytes effectively. The model is used for SCAs and PAAs. The simulation model is designed on the MATLAB simulator by using a script. All the results of AES rounds shows that different values occur in each round. These values can be easily analyzed by the attacker with the help of PAA attack. When we apply algorithm 2 on MATLAB, all the different values give an equal power level and hide the different power level. The results will validate and provide a better solution by masking the power profile of IoT devices with respect to SCA.

When we apply algorithm 2 in MATLAB, all the different values have the same value and hide the different power. This analysis will provide a reference point for the proposed method. In the future, the lightweight AES algorithm with the proposed false key mechanism and power reduction technique such as wave dynamic differential logic (WDDL) will be used to safeguard IoT devices against side channel attacks by using Arduino and field programmable field array (FPGA).

The results have been implemented using 128-bit AES codes available on GitHub Community Forum and the MATLAB function and codes available online for the initial implementation [24].

Acknowledgement: This paper is an extended version of "Invariant of AES algorithm implementations against side channel attacks in IoT devices", which was presented at ICCOINS 2021 conference and published in IEEE Xplore. This work was carried out with the support of Y. Weize and S. Kose, "A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks," IEEE Transactions on Circuits and System, vol. 64, no. 11, pp. 2934–2944, 2017. This work is an extension of author's PhD. Research proposal from Hamdard University. The results have been implemented using Advanced Encryption Standard (AES) 128-Bit codes available GitHub Community Forum and MATLAB Function and codes available online for the purpose of initial implementation.

Funding Statement: This work partially supported by the Research Committee of Hamdard University, Karachi Pakistan (www.hamdard.edu.pk) and partially supported by the Office of Research Innovation & Commercialization (ORIC) of the Dawood University of Engineering & Technology Karachi Pakistan (www.duet.edu.pk).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the recent study.

References

[1] K. Dutta, B. Ghosh and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *Computing and Communication Workshop and Conf., 9th Annual Conf., CCWC 2019. Proc.: Institute of Electrical and Electronics Engineers (IEEE)*, Las Vegas, NV, USA, pp. 0475–0481, 2019.

[2] M. Bansal, M. Nanda and M. N. Husain, "Security and privacy aspects for internet of things," in *Inventive Computation Technologies, 6th Int. Conf., ICICT 2021. Proc.: Institute of Electrical and Electronics Engineers (IEEE)*, Coimbatore, India, pp. 199–204, 2021.
[3] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019.
[4] H. A. A. Ghani, D. Konstantas and M. Mahyoub, "A comprehensive it attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.
[5] D. Bellizia, G. Scotti and A. Trifiletti, "On-chip analog current equalizer as a countermeasure against side-channel attacks in CMOS nanometer technology," in *Mixed Design of Integrated Circuits and Systems, 23rd Int. Conf., MIXDES 2016. Proc.: Institute of Electrical and Electronics Engineers (IEEE)*, Lodz, Poland, pp. 229–234, 2016.
[6] D. Bellizia, S. Bongiovanni, P. Monsurro, G. Scotti, A. Trifiletti *et al.,* "Secure double rate registers as an RTL countermeasure against power analysis attacks," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 26, no. 7, pp. 1368–1376, 2018.
[7] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454–1464, 2017.
[8] O. Lo, W. J. Buchanan and D. Carson, "Power analysis attacks on the AES-128s-box using differential power analysis (DPA) and correlation power analysis (CPA)," *Journal of Cyber Security Technology*, vol. 1, no. 2, pp. 88–107, 2017.
[9] K. S. Chong, J. S. Ng, J. Chen, N. K. Z. Lwin, N. A. Kyaw *et al.,* "Dual-hiding side-channel-attack resistant FPGA-based asynchronous-logic AES: Design, countermeasures and evaluation," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3357, no. 2, pp. 343–356, 2021.
[10] R. Gurunath, M. Agarwal, A. Nandi and D. Samanta, "An overview: Security issue in IoT network," in *IoT in Social, Mobile, Analytics and Cloud, 2nd Int. Conf., I-SMAC 2018. Proc.: Institute of Electrical and Electronics Engineers (IEEE)*, Palladam, India, pp. 104–107, 2019.
[11] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019.
[12] B. A. Dao, T. T. Hoang, A. T. Le, A. Tsukamoto, K. Suzaki *et al.,* "Exploiting the back-gate biasing technique as a countermeasure against power analysis attacks," *IEEE Accessing*, vol. 9, pp. 24768–24786, 2021.
[13] S. Kose, "Efficient and secure on-chip reconfigurable voltage regulation for IoT devices," in *Great Lakes Symposium on VLSI, GLSVLSI 2017*, Banff, Alberta, Canada, pp. 369–374, 2017.
[14] Z. Yuan, Y. Wang, J. Li, R. Li and W. Zhao, "FPGA based optimization for masked AES implementation," in *Circuits and Systems, 54th Int. Midwest Symposium, MWSCAS 2011. Proc.: Institute of Electrical and Electronics Engineers (IEEE)*, Seoul, Korea (South), pp. 1–4, 2011.
[15] S. Ray, Y. Jin and A. Raychowdhury, "The changing computing paradigm with internet of things: A tutorial introduction," *IEEE Design & Test*, vol. 33, no. 2, pp. 76–96, 2016.
[16] Y. Weize and S. Kose, "A lightweight masked AES implementation for securing IoT against CPA attacks," *IEEE Transactions on Circuits and Systems*, vol. 64, no. 11, pp. 2934–2944, 2017.
[17] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig *et al.,* "A polymorphic advanced encryption standard-a novel approach," *IEEE Access*, vol. 9, pp. 20191–20207, 2021.
[18] N. M. Ansari, R. Hussain, S. S. Hussain and S. Arif, "Invariant of AES algorithm implementations against attacks in IoT devices," in *Computer & Information Sciences, Int. Conf. ICCOINS 2021. Proc.: Institute of Electrical and Electronics Engineer (IEEE)*, Kuching, Malaysia, pp. 84–89, 2021.
[19] S. Singh, P. K. Sharma, S. Y. Moon and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *Journal of Ambient Intelligence Humanized Computng*, pp. 1–18, 2017. http://dx.doi.org/10.1007/s12652-017-0494-4.

[20] K. P. Choudhury and S. Kakoty, "Comparative analysis of different modified advanced encryption standard algorithms over conventional advanced encryption standard algorithm," *International Journal of Current Research and Review*, vol. 9, no. 22, pp. 31–34, 2017.

[21] J. Tang, K. Lokibe, T. Kusaka and Y. Nogami, "An approach for attacking speck on microcontroller with correlation power analysis," in *Computing and Networking Workshops, 8th Int. Symposium, CANDARW 2020. Proc.: Institute of Electrical and Electronics Engineer (IEEE)*, Naha, Japan, pp. 368–372, 2020.

[22] A. C. C. Torreno, M. T. G. D. Leon, M. D. Rosales and A. B. Alvarez, "Power and area oriented implementations of lightweight cryptographic algorithms for wireless sensor networks," in *Region 10, Conf., TENCON 2020. Proc.: Institute of Electrical and Electronics Engineer (IEEE)*, Osaka, Japan, pp. 473–477, 2020.

[23] N. Siddiqui, H. Khalid, F. Murtaza, M. E. Haq and M. A. Azam, "A novel algebraic technique for the design of computational substitution-boxes using the action of matrices on Galois field," *IEEE Access*, vol. 8, pp. 197630–197643, 2020.

[24] P. Madhu, https://github.com/autoMAD/MATLAB_PROJECTS/tree/master/Advanced%20Encryption%20Standard%20(AES)%20128-Bit, 2013.