International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A High Performance Data Encryption and Masking Using AES Algorithm

Poornima TN[1], Dr. Somashekar K[2]

[1, 2]Scholar, M. Tech VLSI Design, and Embedded System, SJBIT, India

[1, 2]Professor, Department of Electronics & Communication Engineering, SJBIT, India

Abstract: ***Advanced Encryption Standard is a specification for electronic data encryption (AES). This standard is one of most widely used encryption methods because it has previously been implemented in hardware and software. AES excels at resisting both linear and differential cryptanalysis. Although this design is algorithmically secure, it could be vulnerable to side channel attacks depends on how it will be implemented. For instance, it has been proven that monitoring the implementation's power along with running statistical analyses on the various traces will reveal the secret key that is used. In the study, an effective hardware - based implementations of the 128 - bit and 256 - bit AES architecture is described. It employs a masking technique and side channel attack - resistant picture encryption***

Keywords: Advanced encryption standard, Cryptography

1. Introduction

IoT technology thatis employed which is trustworthy and safe in order for it to be widely used and gain popularity. IOT trust issues may lead to the lack of integrity and confidentiality of both the task for devices and based coordination that are used as supporting systems. A crucial component of the system's overall security, the cryptographic system is employed to safeguard not only the sent data but the system as a whole. Algorithms employed in commonly implemented cryptosystems are secure. Making IOT devices vulnerable to physical assaults is difficult since they are more easily physically accessed than server software systems. The Strong Advanced Encryption Standards is the name of the encryption technique used to protect electronic data (AES). Even though AES has strong protections against algorithmic attacks, side channel threats still can take advantage of it. A common SCA known as Differential Analysis [DPA] allows hackers to learn the possible values utilised in cryptography computation by statistical analysing the data received from the different cryptographic operations. AES implementation has already been demonstrated to DPA. Masking is a commonly used DPA countermeasure since the intermediary parameters in the cryptographic process are no longer connected to the original particular values.

2. Literature Survey

[1] Title: Using Lattice - Based Cryptography to Secure Devices with in Post - Quantum Iot technology
Zhe Liu, Kyung Raymond Woo, and Johann Grobschädl are the authors**.**
Year: 2018

Publication: IEEE Communications Magazine

Any data sent through edge devices, along with all data held on smart objects, must be encrypted in order to enhance the security for edge computing. Only post - quantum cryptography can provide the long - term protection over durations of 10 years or more that may be necessary, especially whenever the transferred nor stored data is given sensitive data. First, a brief introduction to post - quantum public - key cryptographic protocols based on challenging mathematical issues with lattices, hash functions, blunder codes, and multivariate quadratic systems is provided in this article. Secondly, the applicability of matrix cryptosystems for devices with limited resources

[2] Title: Inverse S - box/Combined S - box New Area Records for AES
The authors are Mostafa Taha, DoaaAshmawy, and ArashReyhani - Masoleh.
IEEE Communications Magazine, a publication
Year: 2018

The AES algorithm uses a single architecture, the AES mix S - box/inverse S - box, for both encrypting and decrypting. The AES mix S - box/inverse S - box solution that is now the most compact is Can right's creation, which was initially shown in 2005. Since then, the research community has proposed a variety of optimizations for the S - box alone, however less attention has been paid to the S - box and inverse S - box combo. They propose an innovative AES S - box/inverse S - box architecture in their paper that surpasses Can right's in term of size and speed. In order to achieve this goal, it is advised to employ a tower fields.

[3]Title of this article is A High Information Rate Workflow system Architecture of AES Cryptographic in Network.
PooyaTorkzadeh, MeisamNesaryMoghadam, and Hossein Kouzehgar are the authors.
Year: 2018
26th Iranian Conferences on Electrical And computer engineering publication (ICEE2018)

Amongst the most widely used encryption methods is AES. The complexity of the application including internal blocks was attributed to various ways of implementing the AES algorithm on an FPGA. In this paper, we examined various AES algorithmic building blocks and provided a paradigm

for its encryption and decryption components to be implemented on an FPGA. In order to achieve high throughput and reduced area extent, pipeline structures are used. A combined strategy of memory utilisation and GF (24) is used to achieve the target throughput rate for the AES algorithm in the data storage network. A unique multiplexer - based design is used as the foundation. The AES algorithm's desired throughput rate in the computer storage network. The basis of the proposed scheme is a novel multiplexer - based design.

[4]Title: Article Crypto processing Designed for Resource - Constrained Edge and IoT Devices
HatamehMosanaei - Boorani, SiavashBayat - Sarmadi, and Shahriar Ebrahimi are the authors.
Year: 2019
Journal: IEEE Internet - Of - things PP (99): 1 - 1

More security risks have been introduced as a result of the internet of things' (IoT) exponential growth in applications, including such smart ecosystems or e - health. IoT networks need to develop multiple security protocols among nodes in order to fend against known assaults. IoT devices must therefore perform a number of cryptographic activities, including public key encryption and decryption. Classic public key cryptosystems, including RSA and ECC, are susceptible to quantum attacks and require additional processing complexity to implement effectively on IoT devices. Consequently, these cryptosystems won't be secure once quantum computing is fully.

[5] Title: Small Internet of Things Devices with Low Power Encryption Implementing 8 - Bit and 32 - Bit Message Transfer Optimisation
Authors: MyungHoonSunwoo and HoKeun Kim
Period: 2019
Journal of Signals Processing Applications is a publication.

In this study, a low - power version of the advanced encryption standards (AES) is proposed. This version can be used for smaller applications, such as IoT devices for the internet of things (IoT). The suggested AES complies with low power and compact area constraints by using 8 - bit & 32 - bit data channels. Only the Mix Columns block uses the 32 - bit data path; the Sub Bytes, Byte Possible combination, Add Rounds Key, & Key Expansion blocks all utilize the 8 - bit data path. Additionally, in order to achieve minimal power consumption in a constrained space, we suggest improved Sub Bytes & Mix Columns

3. Methodology

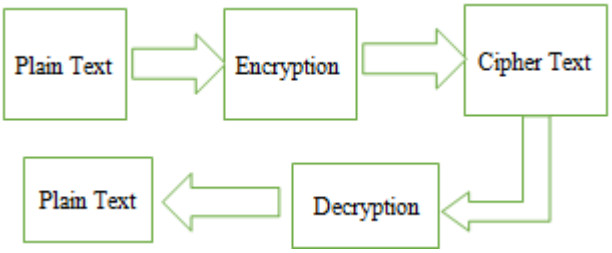

Figure 1: Block Diagram of Encryption and decryption system

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.

Figure 1 shows the general block diagram of the AES encryption and decryption system. The input will be given as the plain text in a readable form. Then the encryption process will be processed and the output which obtained is the Encrypted one which will be in the non - readable form. This cipher text can only be decrypted with the same key which is used for the encryption method. Here, Key plays an vital role in encryption and decryption. If the key is not proper then the accurate will not be delivered.

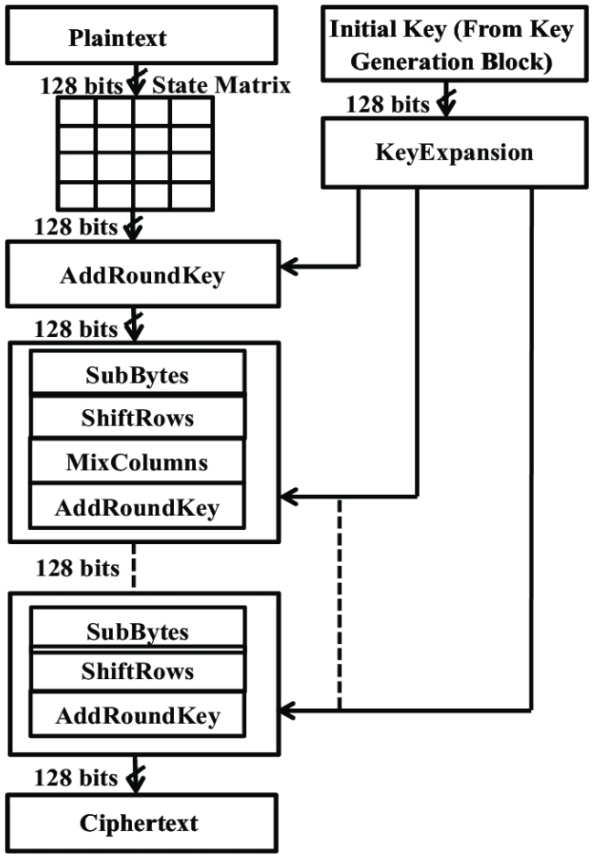

Figure 2: Flow Diagram Data Encryption using Key expansion Technique

Key Expansion – round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128 - bit round key block for each round plus one more.2. Initial round key addition:

1) **Add Round Key** – each byte of the state is combined with a byte of the round key using bitwise xor.3.9, 11 or 13 rounds:
2) **Sub Bytes** – a non - linear substitution step where each byte is replaced with another according to a lookup table.
3) **Shift Rows** – a transposition step where the last three rows of the state are shifted cyclically a certain number

of steps.

4) **Mix Columns** – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
5) **Add Round Key**

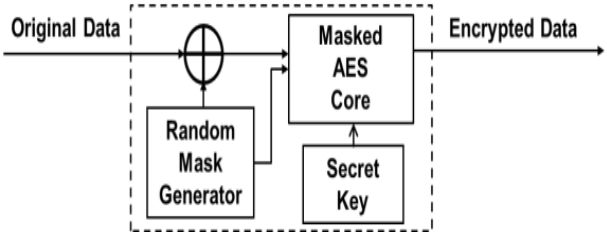

Figure 3: Block diagram of the proposed Masking system

During the encryption process, masked AES constantly adds random intermediate information from the original message in order to conceal side - channel leaking via replacements boxes that handle the secret data. At the end of the encryption, the correct cipher data are segregated from the randomized packet that was produced as aspect of the masking procedure.

4. Results and Discussions

Input: [Without Masking]
Clock: High [1]
Plain text: 00000000111111110000000011111111
Transmitter Key: 00001111000011110000111100001111000011111
Receiver Key: 00001111000011110000111100001111000011111
Output: 00000000111111110000000011111111

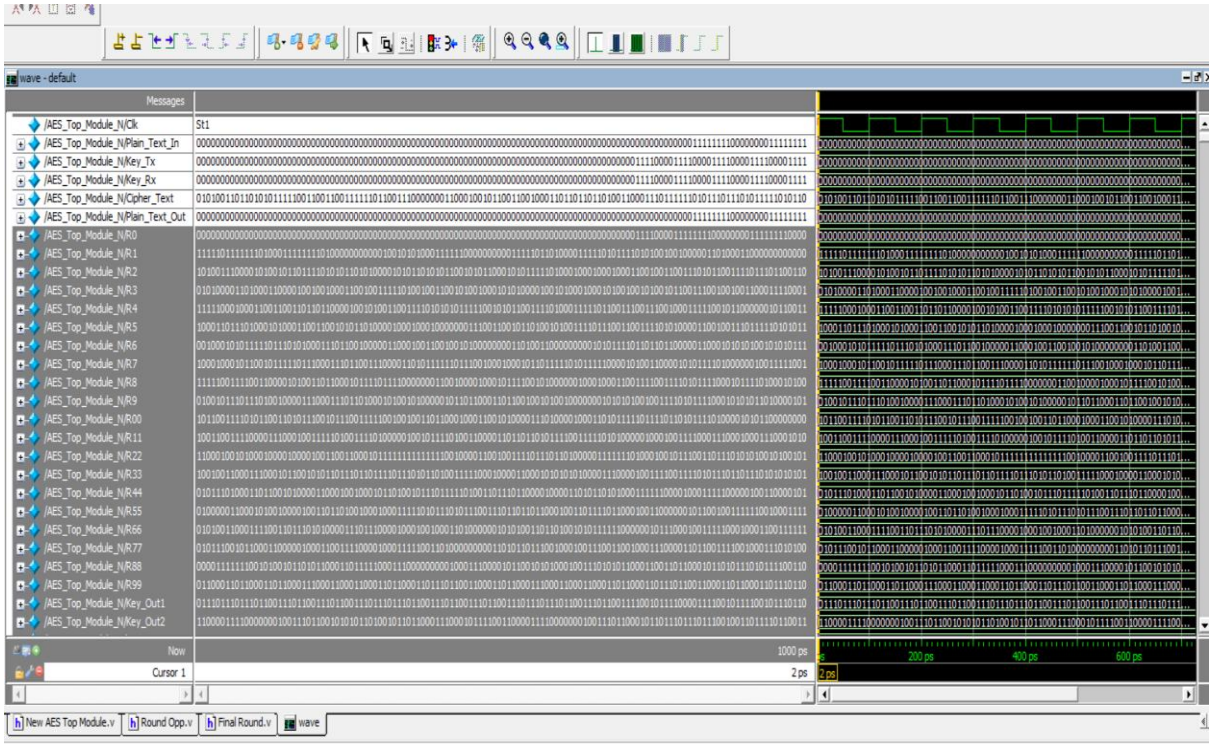

Figure 4.1: Encryption and decryption for binary data

Input: [Masking]
Clock: High [1]
Reset: High [1]
Plain text: 0000000011111111000000000111111110000000011111111000000000111111111
Transmitter Key: 0101000001011111010100000101111101010000001011111
Receiver Key: 0101000001011111010100000101111101010000001011111
Output:: 0000000011111111000000000111111110000000011111111000000000111111111

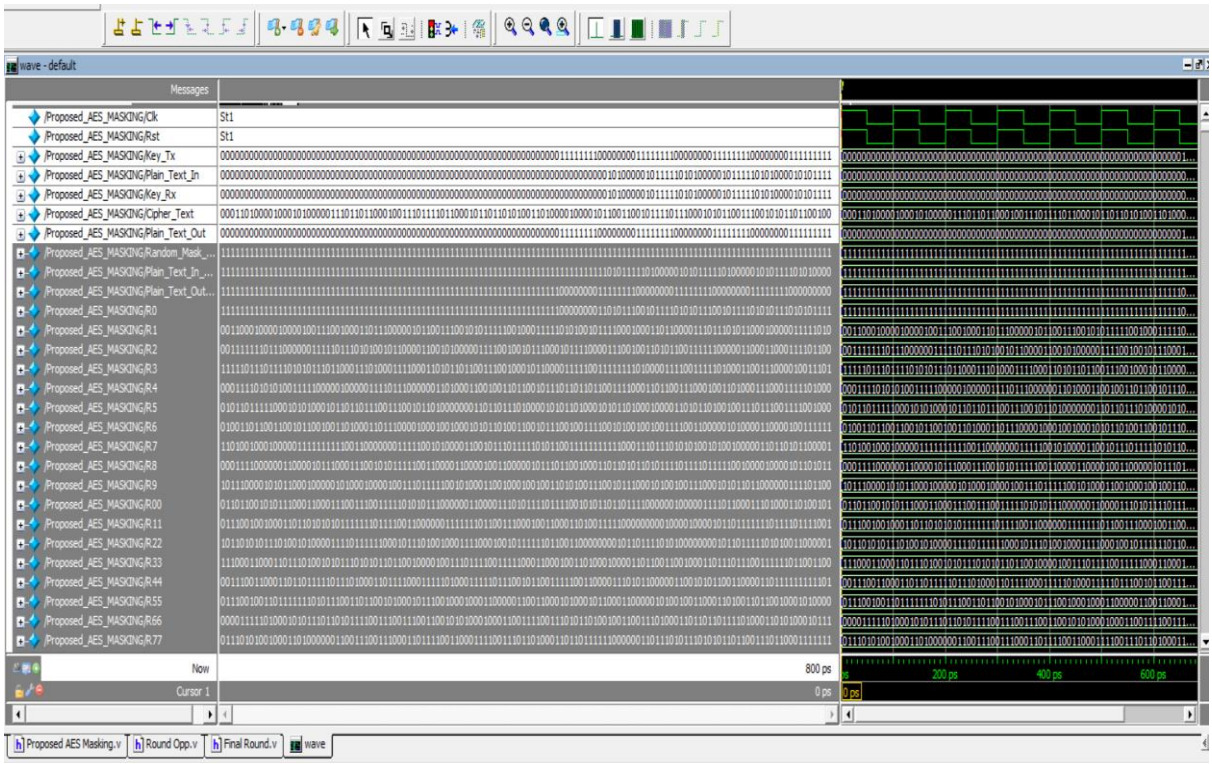

Figure 4.2: Proposed AES Masking [128 bit]

Input: [Masking]
Clock: High [1]
Reset: High [1]
Plain text: 11111111000000001111111110000000011111111100000000111111111
Transmitter Key: 01010000010111110101000001011111010100000010111111
Receiver Key: 0101000001011111010100000101111101010000001011111
Output: 11111111000000001111111110000000011111111100000000111111111

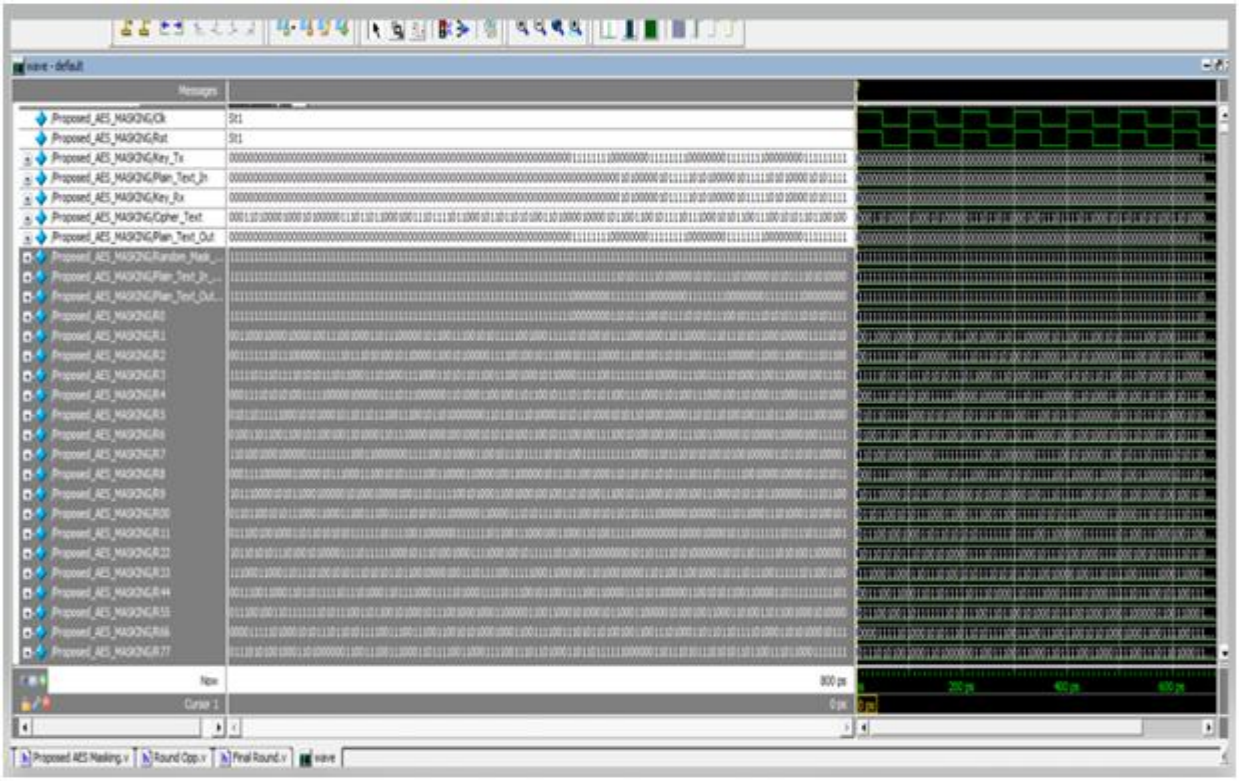

Figure 4.3: Proposed AES Masking [256 bit]

The Proposed system with the masking has been observed that the security level for the data is high compared to the existing system. This made the hacking almost impossible for the third person to access the data.

From the above figures [Fig 4.1, 4.2, 4.3] it can be clearly observed that the data [plain text] which is encrypted using the key expansion uses the same key foe both encryption and decryption as it is a symmetric type of encryption.

5. Applications

Data encryption and decryption
Security system
Digital information security and Computer/network security

6. Conclusion

A high performance masked 128 - bit and 256 bit AES engine has been implemented using Key Expansion technique. . The masked design is verified by simulating the post APR design with Custom Model Sim Simulator and using Correlation Power Analysis (CPA). The results show that the masking scheme effectively hides the secret key. The security for the 128 bit key is more when compared with the existing system. By this technique, it is observed that the are occupied, delay and then the dynamic power consumption will be reduced. As AES Algorithm gives a high security for the data by providing more number of keys, it is suitable for encrypting the Image.

7. Future Scope

The masked design has an area which is around 1.7 times more than the unmasked design. One way to reduce the area, it would be able to reuse the hardware in each round to compute the mask transformation. Since majority of the AES transformation are linear, the hardware which is used for the transformation in each round is same. By passing the masking data in each round depending upon the throughput, the latency cycles can be reduced which in turn reduces the chip area.

References

[1] "Announcing the ADVANCED ENCRYPTION STANDARD (AES) " Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001
[2] Paul Kocher, "Timing attacks on implementations of DiffieHellman, RSA, DSS, and other systems". Advances in Cryptology—CRYPTO'96. Lecture Notes in Computer Science.1109: 104–113
[3] Paul Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis, " Crypto 99 Proceedings, Lecture Notes in Computer Science Vol.1666, M. Wiener, ed., Springer - Verlag, 1999.
[4] Blömer J., Guajardo J., Krummel V. (2004) Provably Secure Masking of AES. In: Handschuh H., Hasan M. A. (eds) Selected Areas in Cryptography. SAC 2004. Lecture Notes in Computer Science, vol 3357. Springer, Berlin, Heidelberg
[5] W. Wei et al., "A compact implementation of masked AES S - box, " 2012 IEEE 11th International Conference on Solid - State and Integrated Circuit Technology, Xi'an, 2012
[6] Edwin NC Mui "Practical Implementation of Rijndael S - Box Using Combinational Logic" 2017
[7] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched - capacitor current equalizer, " 2009 IEEE International Solid - State Circuits Conference - Digest of Technical Papers, San Francisco, CA, 2009, pp.64 - 65
[8] Y. Peng, H. Zhao, X. Sun and C. Sun, "A Side - Channel Attack Resistant AES with 500Mbps, 1.92pJ/Bit PVT Variation Tolerant True Random Number Generator, " 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, 2017, pp.249 - 254
[9] S. Lu, Z. Zhang and M. Papaefthymiou, "1.32GHz highthroughput charge - recovery AES core with resistance to DPA attacks, " 2015 Symposium on VLSI Circuits (VLSI Circuits), Kyoto, 2018, pp. C246 - C247
[12] Henrik Fegran, "DPA - Resistant ASIC Implementation of AES, " MS Thesis, Norwegian University of Science and Technology, June 2018