IJFANS International Journal of Food and Nutritional Sciences

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

DESIGN AND IMPLEMENTATION OF HIGH PERFORMANCE, LOW POWER MASKED 128-AES USING FPGA

[1]KESANA RAMESH BABU, [2]KAILA SWAROOPA RANI, [3]S. RAVINDRA, [4]S. BABA FARIDDIN

[1,3]Assistant professor, Department of Electronics and Communication Engineering, St. Ann's College of Engineering and Technology, Chirala, Andhra Pradesh, India

[2]Assistant professor, Department of Electronics and Communication Engineering, St. Mary's Women's Engineering College, Guntur, Andhra Pradesh, India

[4]Assistant Professor, Department of Electronics and Communication Engineering, NRI Institute of Technology, Guntur, Andhra Pradesh, India

ABSTRACT: Advanced Encryption Standard (AES) is a specification for electronic data encryption. This standard has become one of the most widely used encryption method and has been implemented in both software and hardware. Field-programmable gate array (FPGA) is growing as a new platform for accelerating heavy computational tasks such as machine learning and cryptography. AES has excellent resistance against linear and differential cryptanalysis. But it can be vulnerable to attackers through side channels. Masking methods are popularly used to defend against power side channel attack (PSCA). This paper presents Design and implementation of High Performance, Low Power Masked 128-AES using FPGA. This masked design is implemented in Xilinx ISE 14.1 Project Navigator for synthesis and simulation. The experimental results show that our proposed design takes up less hardware resources and has the ability to defend against power side channel attack.

KEYWORDS: Advanced Encryption Standard (AES), data masking, side channel analysis, Field Programmable Gate Array (FPGA).

I. INTRODUCTION

Data security is an important aspect in recent wide spectrum of embedded applications. Several cryptographic algorithms are developed for protecting data communication in computer network [1]. Cryptographic-system is an important part of total security. It is used to protect not only the data communicated but also the system itself [2]. Commonly used cryptosystems are secure algorithmically. In general, hardware implementation of encryption for standard security protocols, when implemented correctly, is not only more efficient in energy but also harder to attack than their software counterpart. However, if we are not careful about the implementation of the cipher, it can leak information through side channels attacks compromising the theoretical strength of the security protocol.

The Advanced Encryption Standard (AES) is a computer security standard issued by the National Institute of Standards and Technology (NIST) intended for protecting electronic data [3]. Federal Information Processing Standards (FIPS) Publication 197 defines specification of AES. The AES cryptography algorithm can be used to encrypt or decrypt blocks of 128 bits using cipher keys of 128, 196 or 256 bits wide (AES128, AES196, and AES256)[4]. The Advanced Encryption Standard can be implemented in either software or hardware. Hardware implementation can be used to perform the operation more efficiently than possible in software [5].

Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is called plaintext. AES is symmetric Cipher cryptography algorithm [6]. It requires a single key for both encryption and decryption. The key is independent of the plaintext and the cipher itself. It is not possible to get the plaintext without knowing the encryption key. The encryption key secrecy is of high importance in AES.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

Unfortunately, side channel attacks pose a serious threat to AES, these attacks are based on "side channel information", that is, information that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process. Power analysis attacks are powerful attacks among them. Power analysis attacks include simple power analysis (SPA), differential power analysis (DPA), higher order differential power analysis (HODPA) and glitch attack. DPA is a more advanced form of side channel attack that can allow an attacker to discover the intermediate values within cryptographic computations through statistical analysis of data collected from multiple cryptographic operations [7]. Simple Power Analysis (SPA) is a technique that involves directly interpreting power consumption measurements during cryptographic operations.

Masking is a widely used DPA countermeasure as the intermediate values in the cryptographic algorithm are no longer correlated to the original internal values. By performing a function on the original input with a randomly generated mask, we are able to protect the design against DPA based on Hamming weights. This is because correlation has been scrambled. Simple first order DPA will not be able to infer information on the secret key. According to the function of operations, masking schemes can be divided into Boolean masking, additive masking, multiplicative masking, and mixed masking. According to the application of masking, masking schemes can be divided into gate level and algorithmic level masking.

In this paper a high performance, low energy, compact, masked 128-bit AES is implemented. We demonstrate through simulation that its resistance against DPA attack while incurring no performance loss. This design is very efficient in energy and area and is suitable for IoTs. The rest of the paper is organized as follows. In section II Previous works are described, Section III explains described methodology of masked 128-bit AES. Implementation details are represented in Section IV, and finally paper concluded with Section V.

II. LITERATURE SURVEY

C. Equihua et al., [8] a highly compact encryption/decryption architecture, which is implemented in a low-cost FPGA, to efficiently simulate the AES algorithm, is proposed. Specifically, an optimized Galois Field Multiplier, which is the most demanding operation in terms of area consumption and processing speed, involved in Mix-Columns and Inverse Mix-Columns transformations, is presented. The results demonstrate that the proposed digital circuit expends fewer LUTs and fewer registers when compared with the most compact encryption/decryption architectures reported to date.

S. Sawataishi, R. Ueno and N. Homma, et. al. [9] proposed hardware in this brief efficiently unifies the fundamental components to perform a set of AEADs with minimal area and power overheads. we confirm that the proposed hardware can perform the four AEADs with quite smaller area than the sum of the each dedicated AEAD hardware, comparable throughput and power consumption. In addition, we confirmed that the proposed hardware is superior to software implementation on general-purpose processor in terms of both throughput and power consumption.

W. -G. Ho, A. A. Pammu, N. K. Z. Lwin, K. -S. Chong and B. -H. Gwee, et. al. [10] propose an authentication-based matrix-transformation cum parallel-encryption

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

implemented on an asynchronous multicore processor (AMP-MP) to achieve a high throughput and yet secure advanced encryption standard based on counter with chaining mode (AES-CCM). The experimental results show that the throughput of the authentication is 13.54 Gbps while the throughput for both authentication and encryption collectively is 8.32 Gbps, which are 17× and 70× faster than the reported counterparty, respectively.

K. -L. Tsai, F. -Y. Leu, I. You, S. -W. Chang, S. -J. Hu and H. Park, et. al. [11] propose a low power consumed AES encryption architecture, named Low-Power AES Data Encryption Architecture (LPADA), which reduces the power consumed by the AES for data encryption by using low power SBox, power gating technique and power management method. The experimental results show that 62.0% of dynamic power reduction and 88.5% of leakage power lowering have been achieved compared to the power consumed by traditional AES data encryption.

Y. Wang, L. Ni, C. -H. Chang and H. Yu, et. al. [12], a block-level in-memory architecture for advanced encryption standard (AES) is proposed. The proposed technique, called DW-AES, maps all AES operations directly to the domain-wall nanowires. The experimental results show that DW-AES can reduce the leakage power and area by the orders of magnitude compared with existing CMOS ASIC accelerators. It has an energy efficiency of 22 pJ/b, which is 5× and 3× better than the CMOS ASIC and memristive CMOL-based implementations, respectively. Under the same area budget, the proposed DW-AES achieves 4.6× higher throughput than the latest CMOS ASIC AES with similar power consumption. The throughput improvement increases to 11× for pipelined DW-AES at the expense of doubling the power consumption.

M. Xie, S. Li, A. O. Glova, J. Hu and Y. Xie, et. al. [13] propose a fast and efficient AES in-memory (AIM) implementation, to encrypt the whole/part of the memory only when it is necessary. We leverage the benefits (large internal bandwidth and dramatic data movement reduction) offered by the in-memory computing architecture to address the challenges of the bandwidth intensive encryption application. Embracing the massive parallelism inside the memory, AIM outperforms existing mechanisms with higher throughput yet lower energy consumption. The experimental results show that compared with state-of-the-art AES engine running at 2.1 GHz, AIM speeds up the encryption process by 80× for a 1-GB nonvolatile memory (NVM).

III. MASKED 128-AES

The architecture of Design and implementation of High Performance, Low Power Masked 128-AES using FPGA is represented in below Figure 1.

AES encryption consists of both linear and nonlinear transformations. The idea behind masking is that before data enters a function, it must be added to a random mask. By this masking process the actual data values is hidden from any attackers. To unmask, we simply add the masked output to the transformed mask. Transformations such as ShiftRows, MixColumns, and AddRoundKey are linear operations. Masking and unmasking processes are relatively straight forward.

The masked AES core performs 128 bit encryption. The process is done in 10 cycles, computing 1 round per cycle, with the hardware of each round being reused to save area verses a fully unrolled implementation.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

The original data (plaintext) is first masked by a random mask. The mask used in each encryption round should be different to avoid the risk of being counteracted. A proper design should include a physical random number generator. For the demonstration purpose (without loss of generality) we used a 128 bit linear feedback shift register (LFSR) with taps at bits 128, 127, 126, 121 to generate fresh random mask at each round. To find the transformed mask for linear operations, it is simply done by passing the original mask that the data is masked with, through the same transformation. The only nonlinear transformation in AES encryption is the S-box, and the root of the nonlinearity comes from the usage of AND operations mainly found in multipliers.

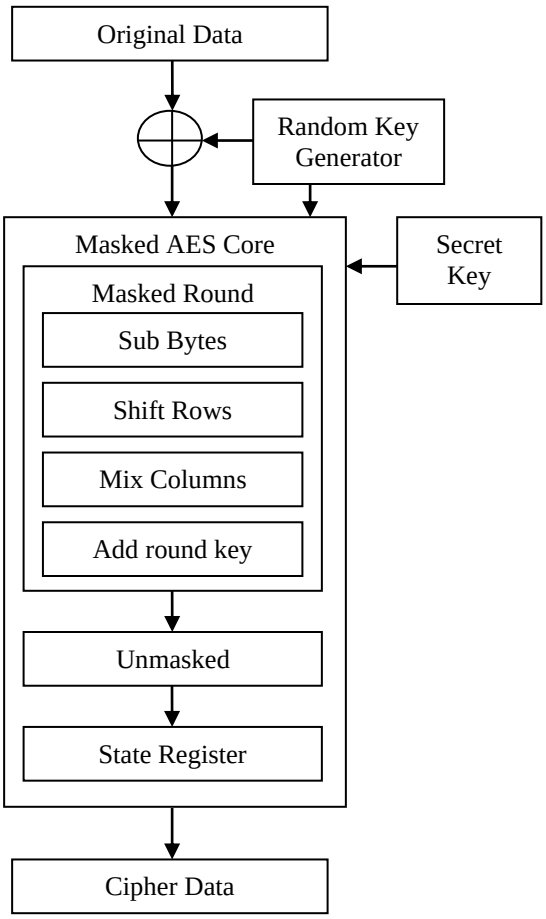

Figure 1: Architecture of Masked AES

Each Masked round consists of 4 steps (layers): SubBytes, ShiftRows, MixColumns, and AddRoundKey. SubBytes involves replacing each byte of the state with a 8-bit substitution box called the S-box which is a non-linear transformation. ShiftRows cyclically shifts the each row of the state matrix by a certain offset. In MixColumns, the four bytes of each column is combined with an invertible linear transformation. Lastly, AddRoundKey simply adds or XORs the current state with the RoundKey. In the final round, the MixColumns step is omitted and the cipher text is obtained after completing the AddRoundKey step in the final round.

The masked plaintext and the mask are, then, fed through the "masked AES core" which encrypts the masked data with the secret key. Result masked cipher-text is input into the unmasking module to arrive at the intended cipher-text.

IV. RESULT ANALYSIS

In this section, we have implemented the proposed design. This masked design is implemented in Xilinx ISE 14.1 Project Navigator for synthesis and simulation. The comparative performance of the design is evaluated in terms of power dissipation, Delay, Area and Security for described Masked AES and Unmasked AES. Below Table 1 shows the Performance comparison analysis for Masked AES and Unmasked AES.

Table 1: PERFORMANCE COMPARISON TABLE

Parameters	Masked AES	Unmasked AES
Delay (ns)	3.35	5.87
Power (mW)	18	57

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

Area (Slice)	356	412
Security (%)	99	90

The graphical representation of delay parameter for described Masked AES and Unmasked AES is represented in below Figure 2.

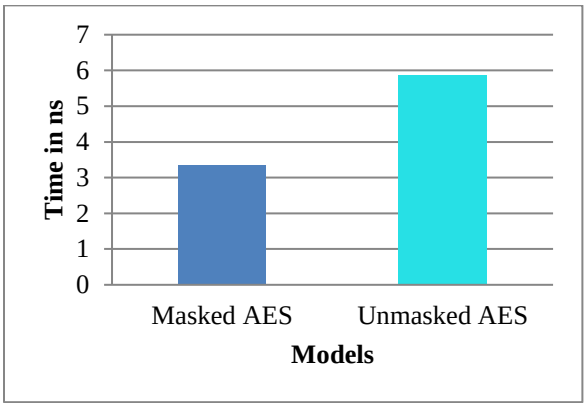

Figure 2: Delay comparison

Below Figure 3 shows the graphical representation of power comparison for two models and it states that power for masked AES model is less compared to Unmasked AES.

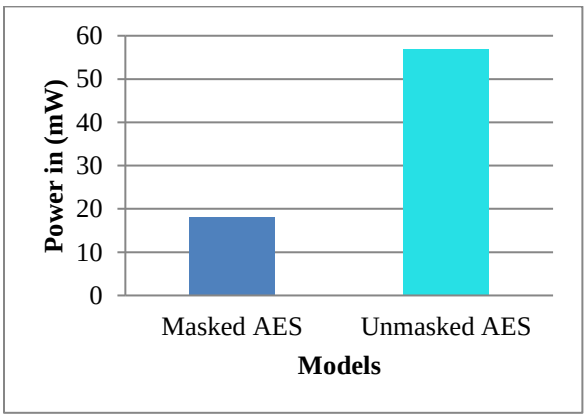

Figure 3: Power comparison

Area comparison graphical representation of described Masked AES and Unmasked AES is represented in below Figure 4 and it states that area of described model is less compared to other model.

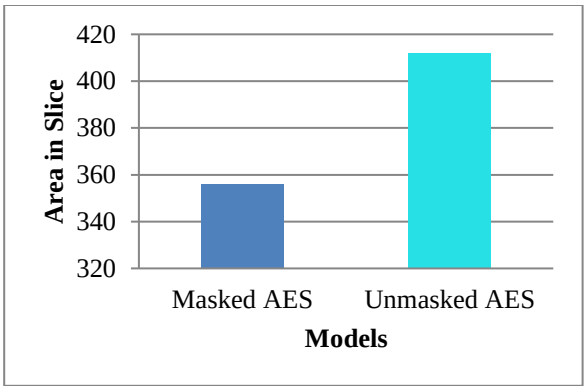

Figure 4: Area comparison

Finally Security of the Masked AES and Unmasked model is graphically represented in below Figure 5 and it states that security of Masked AES model is higher than Unmasked AES.

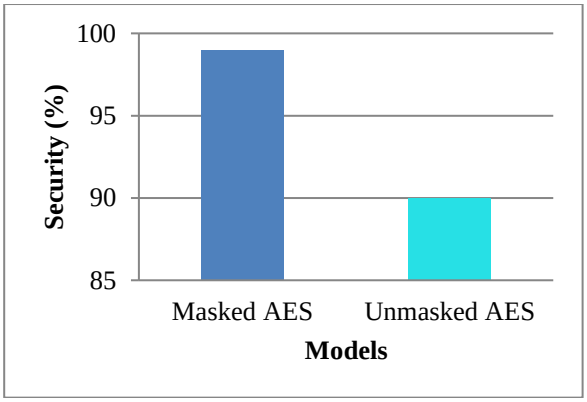

Figure 5: Security comparison

From overall results, it is clear that described Masked AES model is efficient in terms of power dissipation, Delay, Area and Security parameters. Achieved parameters for described model are Security as 99%, Delay as 3.35ns, Area as 356 slice and finally Power as 18mW.

V. CONCLUSION

In this paper, Design and implementation of High Performance, Low Power Masked 128-AES using FPGA is described. Cryptologic circuits such as Advanced Encryption Standard (AES) are susceptible to power based side channel analysis (PSCA) attacks. The idea behind masking is that before data

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

enters a function, it must be added to a random mask. By this masking process the actual data values is hidden from any attackers. This masked design is implemented in Xilinx ISE 14.1 Project Navigator for synthesis and simulation. The comparative performance of the design is evaluated in terms of power dissipation, Delay, Area and Security for described Masked AES and Unmasked AES. From overall results, it is clear that described Masked AES model is efficient in terms of power dissipation, Delay, Area and Security parameters. Achieved parameters for described model are Security as 99%, Delay as 3.35ns, Area as 356 slice and finally Power as 18mW.

VI. REFERENCES

[1] S. Chen, Z. You and X. Ruan, "Privacy and Energy Co-Aware Data Aggregation Computation Offloading for Fog-Assisted IoT Networks," in IEEE Access, vol. 8, pp. 72424-72434, 2020, doi: 10.1109/ACCESS.2020.2987749.

[2] B. Lee, I. -G. Lee and M. Kim, "Design and Implementation of Secure Cryptographic System on Chip for Internet of Things," in IEEE Access, vol. 10, pp. 18730-18742, 2022, doi: 10.1109/ACCESS.2022.3151430.

[3] S. Ghandali, S. Ghandali and S. Tehranipoor, "Deep K-TSVM: A Novel Profiled Power Side-Channel Attack on AES-128," in IEEE Access, vol. 9, pp. 136448-136458, 2021, doi: 10.1109/ACCESS.2021.3117761.

[4] D. Reis, H. Geng, M. Niemier and X. S. Hu, "IMCRYPTO: An In-Memory Computing Fabric for AES Encryption and Decryption," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 5, pp. 553-565, May 2022, doi: 10.1109/TVLSI.2022.3157270.

[5] P. Qiu, Y. Lyu, J. Zhang, D. Wang and G. Qu, "Control Flow Integrity Based on Lightweight Encryption Architecture," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 7, pp. 1358-1369, July 2018, doi: 10.1109/TCAD.2017.2748000

[6] C. -H. Lin, "Intelligent Symmetric Cryptography With Chaotic Map and Quantum Based Key Generator for Medical Images Infosecurity," in IEEE Access, vol. 9, pp. 118624-118639, 2021, doi: 10.1109/ACCESS.2021.3107608.

[7] P. -C. Liu, H. -C. Chang and C. -Y. Lee, "A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 59, no. 2, pp. 103-107, Feb. 2012, doi: 10.1109/TCSII.2011.2180094

[8] C. Equihua, "A low-cost and highly compact FPGA-based encryption/decryption architecture for AES algorithm," in IEEE Latin America Transactions, vol. 19, no. 9, pp. 1443-1450, Sept. 2021, doi: 10.1109/TLA.2021.9468436.

[9] S. Sawataishi, R. Ueno and N. Homma, "Unified Hardware for High-Throughput AES-Based Authenticated Encryptions," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 9, pp. 1604-1608, Sept. 2020, doi: 10.1109/TCSII.2020.3013415

[10] W. -G. Ho, A. A. Pammu, N. K. Z. Lwin, K. -S. Chong and B. -H. Gwee, "High Throughput and Secure Authentication-Encryption on Asynchronous Multicore Processor for Edge Computing IoT Applications," 2020 International SoC Design Conference (ISOCC), Yeosu, Korea (South), 2020, pp. 173-174, doi: 10.1109/ISOCC50952.2020.9333008.

[11] K. -L. Tsai, F. -Y. Leu, I. You, S. -W. Chang, S. -J. Hu and H. Park, "Low-Power AES Data Encryption Architecture for a LoRaWAN," in IEEE Access, vol. 7, pp. 146348-146357, 2019, doi: 10.1109/ACCESS.2019.2941972.

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 11, Issu 11, 2022

[12] Y. Wang, L. Ni, C. -H. Chang and H. Yu, "DW-AES: A Domain-Wall Nanowire-Based AES for High Throughput and Energy-Efficient Data Encryption in Non-Volatile Memory," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2426-2440, Nov. 2016, doi: 10.1109/TIFS.2016.2576903.

[13] M. Xie, S. Li, A. O. Glova, J. Hu and Y. Xie, "Securing Emerging Nonvolatile Main Memory With Fast and Energy-Efficient AES In-Memory Implementation," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 11, pp. 2443-2455, Nov. 2018, doi: 10.1109/TVLSI.2018.2865133