Improving Security Using Modified S-Box for AES Cryptographic Primitives

S. Sudhakar ^{a,1}, A. Akashwar ^b, M. Ajay Someshwar ^b, T. Dhaneshguru ^b, M. Prem Kumar

^a*Assistant Professor, Department of Electronics and Communication Engineering*

^b*UG Student, Department of Electronics and Communication Engineering*

Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

Abstract. The growing network traffic rate in wireless communication demands extended network capacity. Current crypto core methodologies are already reaching the maximum achievable network capacity limits. The combination of AES with other crypto cores and inventing new optimization models have emerged. In this paper, some of the prominent issues related to the existing AES core system, namely, lack of data rate, design complexity, reliability, and discriminative properties. In addition to that, this work also proposes a biometric key generation for AES core that constitutes simpler arithmetic such as substitution, modulo operation, and cyclic shifting for diffusion and confusion metrics which explore cipher transformation level. It is proved that in AES as compared to all other functions S-Box component directly influences the overall system performance both in terms of power consumption overhead, security measures, and path delay, etc.

Keywords. Cryptography, AES algorithm, Security, cipher

1. Introduction

In recent decades the emergence of social media and the invention of several digitalized transmissions – data security is becoming most important than ever and also a difficult task to accomplish. The need for each individual to identify themselves digitally has spawned a wide variety of challenges, such as, for example, how to avoid fraud. Biometric data as fingerprint or iris scan is one way of identification, however, to use the data that is reliable for identification purposes the data must stay confidential, for that reason information security is important. The security measures inadequacies inherent in existing cryptosystems have driven the development of a new security model. With the development of several cipher models, the methodologies to explore the unique properties of each transformation model which can extract the information from cipher are also increased steadily. By using some combined approaches to provide solutions to the highly robust cryptosystem as well as other key issues are motivated by the research community.

¹ S.Sudhakar, Department of Electronics and Communication Engineering, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, Tamilnadu, India; E-mail: sudhakars106@gmail.com.

To ensure the cryptosystems are economically viable, all intermediate functions should be comprised with minimal resources and simplified computation which makes traditional security methodologies out of choice for them. The inherent data aggregation and information sharing properties render all existing public key cryptographic algorithms impractical. The major objective of a high-performance crypto core is to evaluate, develop, and analyze transformation models used in each stage of cipher conversion to achieve higher throughput efficiency with improved security. Among many crypto models, AES is the most promising method used for secured transmission in communication systems and has proven to be an optimal technique well suited for reliable data transmission over unsecured channels. It can be able to support high bit rate data transmission and also robust to all kinds of attacks.

2. Related Works

This section includes the advantages of the existing AES core and its implications on security measures in detail. In general working principle and its parametric measures of any crypto, the core system is largely dependent on key length, the number of rounds, and various physical transformation functions involved during cipher conversion efficiency. In most cases, a trade-off is made among these measures. Implementation of AES core is related IoT applications are applicable only with some optimization models due to its parametric constraints...

In [1] introduced energy-efficient S-Box model for AES which is formulated using multi-stage Positive Polarity Reed-Muller form (PPRM) of composite fields. It includes hazard-transparent XOR gates that are located and replaced all other gates to block the hazards. In [2] developed FPGA technology mapping-based hardware optimization over AES core instead of logic optimization. As a result, both the linear and non-linear functional blocks of AES are considerably reduced, without causing any significant performance losses. In [3] optimized the AES core for lightweight applications and reduce hardware complexity effectiveness and energy consumption. To narrow down the computational burden various S-box architectures are analyzed based on FPGA design-specific hardware analysis for AES core. It includes pre-coded LUT-based S-box, the pure combinatorial gate-level logic implementation-based S-box using Galois field, and the path-optimized pipelined version of S-Box. Finally, optimal S-box using dynamic computation and Linear Feedback Shift Register (LFSR) random pattern generator-based S-Box is implemented for optimized AES core.

In [4] developed high-throughput bit sliced AES implementation based on novel data representation which exploits parallelization over many-core platforms. The building blocks used on each stage of AES utilized a bit sliced approach for parallelization. This improved parallelization offers a significant throughput rate. In this new AES model, the ShiftRows stage implicitly handled simple data rearrangement and neglects the complex computing process. Moreover, byte-wise operations are accomplished using the shift and swapping process.

Novel cipher model invented in [5] used self-inverse-permutation and Golden S-Boxes computations. By introducing a new mapping measure which comprises of self-inverse and arithmetic model ring of integers modulo $2n$, the properties of this mapping function offer several key contributions to cipher structures by activating hard-core multipliers.

Figure 1. Proposed modified AES crypto model

3. Advanced Encryption Standard (AES)

Among various methodologies investigated for security, AES is considered as a prominent methodology that is useful for next-generation IoT and proved to be a potential alternative to exiting all other existing crypto core system [6]. In this real-time application 128 block size is preferred as AES standard due to its optimal tradeoff between security and computational complexity overhead as shown in Figure 1. During cipher conversion input text is arranged as a 4x4 matrix which is known as a state matrix or state array.

Add Round Key: This function involves key-based transformation and using bitwise Exclusive-OR operation between input cipher key and a state array.

Shift Rows: This is a physical transformation that operates on each row of a state array. Here only bytes of each state are shifted cyclically from left to right except the first row. The second, third, and fourth rows are shifted linearly.

Substitute transformation: As compared to all other functions S Box is nonlinear. During S Box computation byte-by-byte substitution is performed which generates a new byte value for each element in the state array. In general S Box is implemented in two ways namely Galois Field-based dynamic computation, Look-Up Table-based approach.

Mix Columns: The function is also involved physical transformation performing matrix multiplication with some fixed compound values. Though AES is a technically advanced crypto core significant performance tradeoff is always occurs in many real-time applications due to its complex computations. Optimization is essential for AES to implement in IoT and embedded systems.

3.1 Performance security Measures

The attainable security of any cryptography algorithm largely depends on the key size and associated element of operations involved in the key generation process [7]. However, security enhancements through cipher key come with some significant computational time and hardware complexity overhead. Different algorithms used the different levels of complexity trade-off to meet desired security levels. Biclique Cryptanalysis widely used hash function for cryptanalysis measures over block cipher algorithms. In this type of cryptanalysis, the worst-case reference is used which is formulated from brute force and provides to a new benchmark.

3.2 Biometric Key Sequence Extraction Approaches

Biometric traits are always used to describe some unique discrimination model to explore the unique characteristics of different individuals. The generic biometric model extracts some invariant features from input biometric to incorporate the basic characteristics and all other relevant information useful for security measures. In real-time environments, the features are not stable in nature, and the method proposed should accommodate all nonlinear dynamics of image processing like interferences, rotational variations, and scale changes etc.

4. Experimental Results

4.1 Simulation Results

In order to validate the importance of the biometric key sequence generation process and to verify its impact in AES cryptosystem during cipher conversion process, AES cryptosystem is simulated using appropriate test inputs in various stages of data propagation as shown in Figure 2 and 3. The potential benefits of bio signal in key sequence generation and its efficiency over AES crypto design is also proved through simulation results

Figure 2. AES simulated cipher output for ASCII character input

Figure 3. Bio metric digital image

4.2 Hardware synthesis results

In this chapter, we compare the performance metrics of proposed modified s box AES over conventional LUT based model and validated the metrics both in terms high performance and complexity trade off measures. The proposed AES core is modeled using the Verilog HDL and synthesized using FPGA QUARTUS II EDA synthesizer for state-of-the-art comparison. The resultant S-Box is capable of achieving a flexible tradeoff with least possible design complexity and tolerable error protection in Figure 4. Moreover, by exploiting the benefits of dynamic computation side which can minimize memory space requirements and can able to support the path delay optimization using the sub pipelining model. In this pipelined composite s box can able to jointly optimize the computational complexity and energy from beneficiary GF enabled computation.

Table 1. Performance comparisons between modified dynamic nonlinear S box models using FPGA hardware synthesis results

S-Box model	Area (LE's used)	Fmax (MHz)
LUT model	216	228.21 MHz
Sub pipelined composite model	80	509.16 MHz

Figure 4. Dynamic non Linear S box RTL view

4.3 Performance comparison report

The FPGA hardware synthesizer tool has been used to measure the power utilization report and its experimental results are listed in Table 1. From the logical element's utilization summary, it is proved that the proposed modified S Box using composite field arithmetic model offers 6% area efficiency over conventional LUT based S- Box approach and achieves 14% hardware complexity reduction. The energy efficiency of optimized sub byte transformation is also proved to be the significant one as shown in Figure 5 through FPGA hardware synthesis results.

PowerPlay Power Analyzer Summary	
PowerPlay Power Analyzer Status	Successful - Sun Mar 07 04:36:05 2021
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	TGP
Top-level Entity Name	sbox
Family	Cyclone II
Device	EP2C35F672C6
Power Models	Final
Total Thermal Power Dissipation	148.05 mW
Core Dynamic Thermal Power Dissipation	7.08 mW
Core Static Thermal Power Dissipation	90.05 mW
I/O Thermal Power Dissipation	60.92 mW
Power Estimation Confidence	Low: user provided insufficient toggle rate data

Figure 5. Power dissipation report.

5. Conclusion

Here in this work FPGA implementation of modified dynamic s box driven AES cryptographic algorithms with all forms of nonlinear transformation and analyzed its crypto core futures. It is also demonstrated that LUT based s box introduced for AES hardware open a back door to potential attacks. Here, we propose a nonlinear multiple instance S BOX along with biometric key sequence extraction model as a scan-protection scheme that provides security both at production time and over the course of the circuit's life. Compared to regular mode, this technique has no impact on the quality of the test or the model-based fault diagnosis. Here we proved that modified S BOX based AES will give better hardware complexity and power optimization with considerable delay enhancement.

References

- [1] Good, T., & Benaissa, M. (2005). AES on FPGA from the Fastest to the Smallest (pp. 427–440). https://doi.org/10.1007/11545262_31
- [2] Hafsa, A., Gafsi, M., Malek, J., & Machhout, M. (2021). FPGA Implementation of Improved Security Approach for Medical Image Encryption and Decryption. *Scientific Programming*, 2021, 1–20. <https://doi.org/10.1155/2021/6610655>
- [3] Soltani, A., & Sharifian, S. (2015). An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA. *Microprocessors and Microsystems*, 39(7), 480–493. <https://doi.org/10.1016/j.micpro.2015.07.005>
- [4] Swierczynski, P., Fyrbiak, M., Koppe, P., & Paar, C. (2015). FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(8), 1236–1249. <https://doi.org/10.1109/TCAD.2015.2399455>
- [5] Yang, C.-H., & Chien, Y.-S. (2020). FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. *Symmetry*, 12(2), 189. <https://doi.org/10.3390/sym12020189>
- [6] Hafsa, A., Sghaier, A., Machhout, M., & Malek, J. (2019). A New security Approach to Support the operations of ECC and AES Algorithms on FPGA. 2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 95–100. <https://doi.org/10.1109/STA.2019.8717302>
- [7] Wegener, F., De Meyer, L., & Moradi, A. (2020). Spin Me Right Round Rotational Symmetry for FPGA-Specific AES: Extended Version. *Journal of Cryptology*, 33(3), 1114–1155. <https://doi.org/10.1007/s00145-019-09342-y>