A Low Power S-Box Implementation for AES Using Power-Gated PLA on Altera

Kalaiselvie.C.M
PG Student (VLSI Design), Dept of ECE, Arasu Engineering College, Kumbakonam, Tamil Nadu, India.

kavitha.D
Assistant professor, Dept of ECE, Arasu Engineering College, Kumbakonam, Tamil Nadu, India.

Abstract – This paper present a low power custom hardware implementation of Rijndael S-BOX for Advanced Encryption Standard using power-gating and PLA design techniques to reduce power and area. AES is the private-key cryptography. The proposed S-BOX system is implemented using the multiplexer technique to reduce the area and logical elements. The proposed scheme is used for military applications and governmental ID.

Index Terms – PLA, Power-gating, Multiplexer, S-BOX.

1. INTRODUCTION

The AES algorithm is also known as Rijndael which is a specification for the encryption of electronic data which is established by the National Institute for standards and technology (NIST) in the year 2001. Two Belgian cryptographers, Joan Daemen and Vincent Rijmen, submitted a proposal to NIST for AES selection process. Rijndael algorithm is a combination of security, efficiency, flexibility and easy to implement.

Rijndael is a family of ciphers has the different key and block sizes. The three different key length are 128, 192, 256 bits. AES provide an excellent service to several application using high level protocols. A cryptography system can be simple and easy to implement in software. Hardware can be implemented by pipelining and parallelization concept to provide a secure network.

The AES cipher in which there are certain repetitive round operations used such as, Sub-Bytes, Shift Rows, Mix-Column, and Add round key. These all rounds are combined to call as a Transformation Techniques. In this paper discuss the implementation of S-BOX in efficient way to improve the AES performance. The AES is a symmetric key algorithm (uses same key for both encryption and decryption). The AES working based on the substitution-permutation network and combination of both substitution and permutation and hence it is very fast to implement in both hardware and software.

This proposed paper based on implementation of S-BOX circuit using PLA architecture and power gating method for reduce power leakage during sub-Bytes transformation is not active based on the mode. . In the next section AES algorithm block diagram and explanation stated followed by the proposed PLA and power gating mechanism and then the result is compared with the previous work result in terms of delay and performance, followed by conclusion and summary of the result.

2. CIRCUIT DESIGN AND IMPLEMENTATION

A) S-BOX TRANSFORMATION

AES is a symmetric-key block cipher. AES operates on 128-bit data blocks and accepts 128-, 192-, and 256-bit keys. It is an iterative cipher, which means that both encryption and decryption consist of multiple iterations of the same basic round function as shown in Figure 1. In each round, a different round (or internal) key is being used. In AES, the number of cipher rounds depends on the size of the key. It is equal to 10, 12, or 14 for 128-, 192-, or 256-bit keys, respectively.

The Rijndael S-Box is a matrix used in Rijndael cipher. The sub-Byte also referred to as S-Box. The AES hardware complexity was mainly due to the S-Box. In cryptography S-Box performs substitution though it is a symmetric key algorithm. Many different block ciphers use a special substitution called as S-Box. The sub-Byte is performed by substituting the input byte with the new byte resulted from the non-linear transformation. A non-linear transformation provides higher security services.

The S-Box and inverse S-Box can be implemented in two operations. First, the multiplicative inverse in Galois field is performed and then affine transformation takes place. It has the advantage that low area overhead, but the delay and hardware complexity is more. Another way is to design the S-Box using the combinational logic which is straightly calculated from the Arithmetic properties. But it has more delay and covers large area.

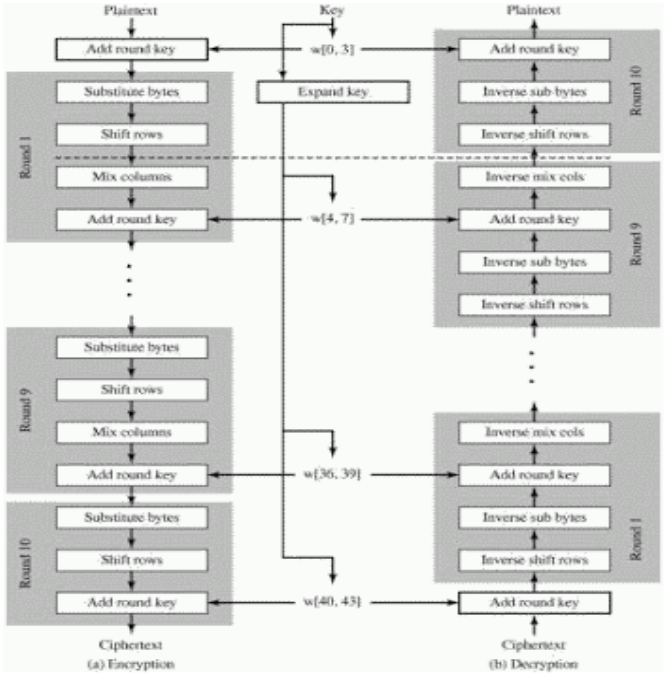


Figure 1: AES Algorithm Encryption and Decryption Structure.

In software, S-Box design was implemented by simple Look up table (LUT), which stores S-Box predefined 256 bits in ROM (Read only memory). This can offer shorter critical path, but it is not used for high speed design due to the unbreakable delay and larger area. To alleviate these disadvantage, this paper proposes power and area efficient PLA and power gating technique based S-Box design for Soc solution of AES system in CMOS technology.

3. PROPOSED PLA AND POWER-GATING LOGIC

A. Programmable Logic Array

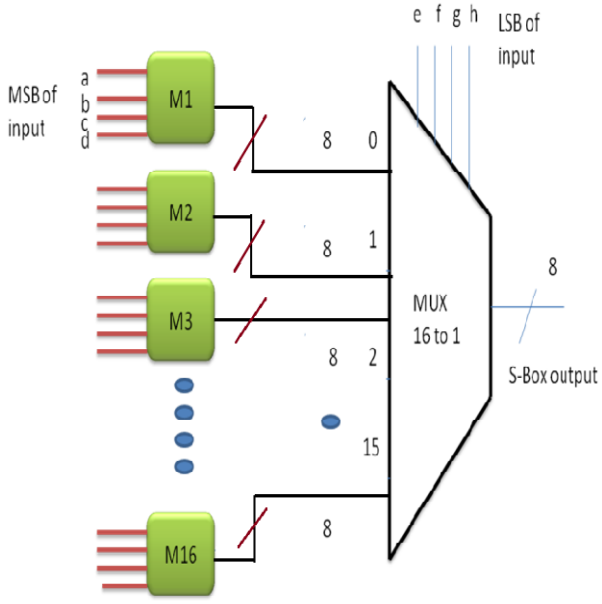
In this section, the S-Box is implemented using the combinational random logic and 16-Bit Mux. This combinational logic is called as time-independent logic implemented by Boolean circuits. In this paper, the S-Box design is based on the PLA and power-gating method to reduce power and reduce delay. A Programmable Logic Array (PLA) is a programmable logic device used to implement combinational logic circuits. The PLA has a set of programmable AND gate planes, which link to a set of programmable OR gate planes, which then be conditionally complemented to produce an output.

The S-Box architecture has 16 module logic functions and each module has AND gate, OR gate and NOT gate.

$$y7 = b\bar{c}\bar{d} + a\bar{b}\bar{c} + a\bar{b}\bar{d} + \bar{a}bcd,$$
$$y6 = \bar{a} + \bar{b}c\bar{d} + b(\bar{c}d),$$
$$y5 = ac + \bar{d} + \bar{a}\bar{c} + \bar{b}c,$$
$$y4 = \bar{a}\bar{b}(c + d) + \bar{c}\bar{d}(a + b) + abd,$$
$$y3 = \bar{a}\bar{c}d + b\bar{c}\bar{d} + \bar{b}cd + abd,$$
$$y2 = a\bar{b}\bar{c} + \bar{b}c\bar{d} + \bar{a}\bar{b}\bar{c}d + \bar{a}bc + abd,$$
$$y1 = b\bar{c} + \bar{b}c + \bar{a}\bar{d} + ab,$$
$$y0 = c\bar{d} + \bar{b}c + \bar{a}\bar{b}\bar{d} + \bar{a}bd + a\bar{c}d,$$

The Boolean expressions are used to calculate the logic 0 or logic 1. The below architecture consists of too many gates and thus the complexity of hardware is high. The conventional approaches to implement S-Box has been FPGA (Field Programmable Gate Array) based design using HDL language. The FPGA design is very simple and cost effective. Because of the two reasons, it has faster" Time-to-market". And main thing is it can be reprogrammed to suit another applications and flexible. But it is relatively slower than the ASIC. Thus the full custom design are used to overcome the disadvantages in both FPGA and ASIC based design in this area as systems-on-chip (SOC) and IP block design are becoming more general approach.

Fig 2: S-Box architecture using combinational logic.

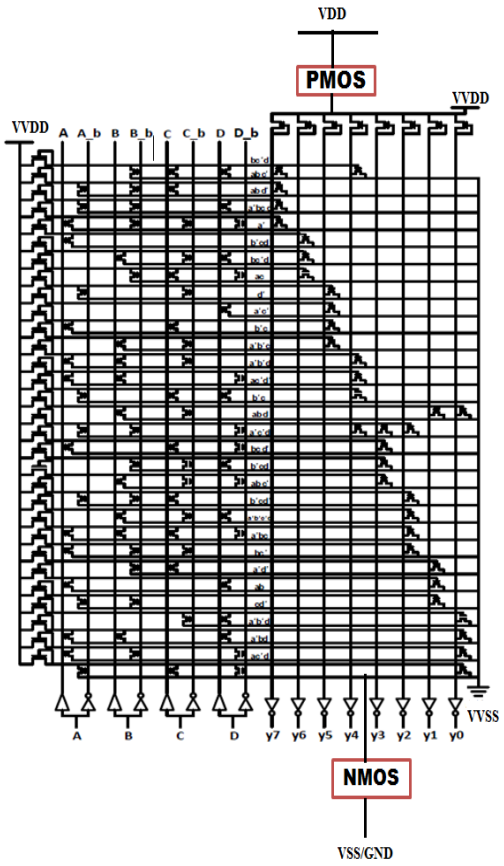


Therefore, a power effective implementation of S-Box architecture is proposed in this paper by using power gating and PLA techniques. A PLA is one way to design a

combinational logic circuits it to get gates and connect them with wires. PLA differ from PAL (programmable array logic) in that both AND, OR gate planes are programmable. The PLA has many min terms. The 16 modules present in the below architecture have a separate Boolean expression that can be converted in to the PLA planes.

The transistor size of the PLA has been optimized by considering the wire load of every signal line and the pre-charge device.

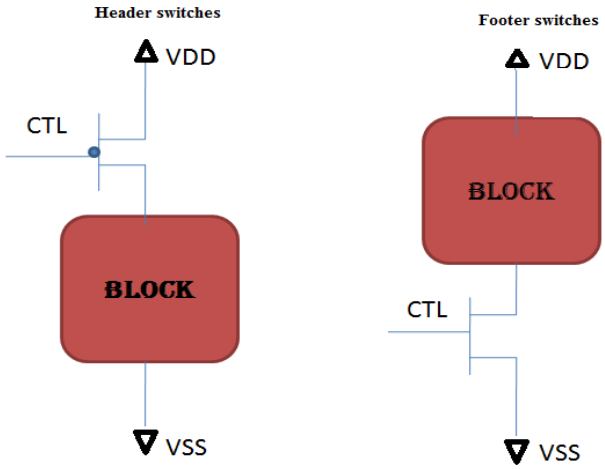
Fig 3: Proposed module (M1) implementation with PLA.



B. Power-gating model

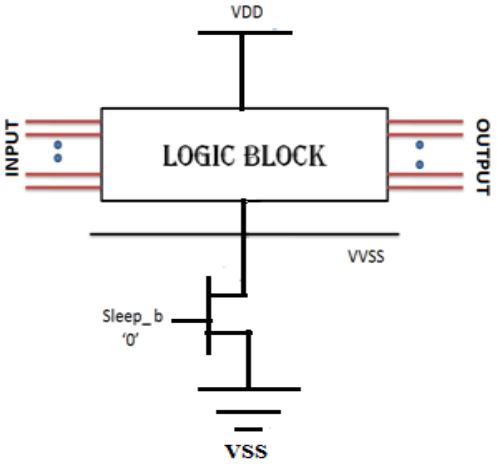
The power reduction is one of the major concerns in this design; power gating technique is applied to the proposed system to reduce leakage current during standby mode. Power gating method is used in integrated circuit design to reduce power consumption, by shutting off the current to blocks of the circuit that are not in use. In AES the S-Box size is large and hence it consumes more power and also causes power dissipations, so power gating method is used in this proposed architecture.

Fig 4: Power gating circuit.



The power gating implementation has additional considerations for timing closure implementation. For the successful implementation the four parameters are important they are: power gate size, slew rate which controlled by gates, switched capacitance, power gate leakage. In this paper, gate leakage and sub-threshold leakage currents are focused since the junction leakage depends on the substrate bias voltage but the substrate bias voltage is typically tied to ground in most logic devices. The NMOS footer device does not reduce gate leakage as much as PMOS header. The NMOS footer transistor size can be half of PMOS header size this can reduce the leakage as much as possible, so the NMOS footer is used as a power gating model in this paper.

Figure 5: Proposed power gating circuit.



The power consumption of the power-gated model is further reduced by controlling the primary input. If we apply logic 1 to the primary input of power gated circuit then the input gate

leakage is reduced much then other circuit. The figure 5: stated the proposed power gating method. The power gate method has some disadvantage that the rush current may lead to large fluctuation in power this can be overcome by using the multiple sleep transistors in this paper.

4. RESULTS AND DISCUSSIONS

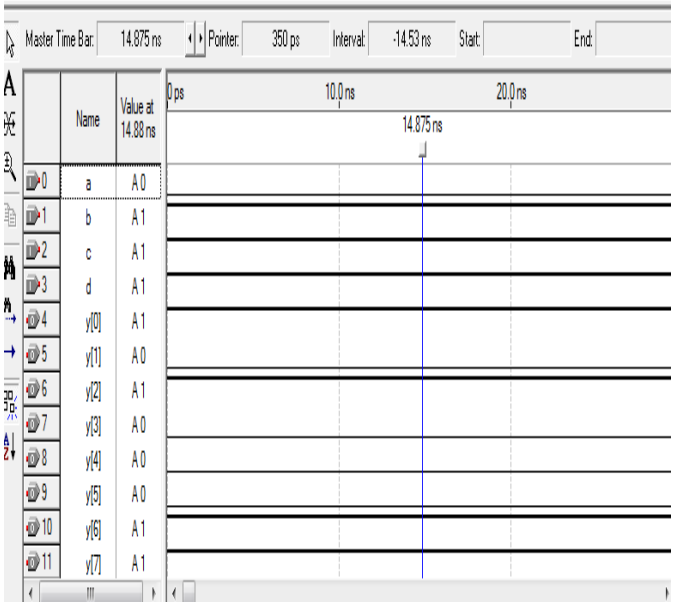
AES S-BOX has been designed and implemented by using the PLA technique to reduce power and area.

Figure 6: proposed Flow summary of S-Box

Flow Status	Successful - Sun May 08 00:12:31 2016
Quartus II Version	9.1 Build 350 03/24/2010 SP 2 SJ Web Edition
Revision Name	SBOXPLA
Top-level Entity Name	SBOXPLA
Family	Cyclone II
Device	EP2C5T144C8
Timing Models	Final
Met timing requirements	Yes
Total logic elements	8 / 4,608 (< 1 %)
Total combinational functions	8 / 4,608 (< 1 %)
Dedicated logic registers	0 / 4,608 (0 %)
Total registers	0
Total pins	12 / 89 (13 %)
Total virtual pins	0
Total memory bits	0 / 119,808 (0 %)
Embedded Multiplier 9-bit elements	0 / 26 (0 %)
Total PLLs	0 / 2 (0 %)

The above mentioned flow summary denotes about the family used in Altera quartus II and the number of logical elements and their status.

Figure 7: simulation result



The above mentioned figure shows the waveform for the input a ,b,c,d as 0,1,1,1. We can change the input values and it can be substitute in the Boolean expression and evaluate the result.

5. CONCLUSIONS

In this paper, The S-Box area and power are reduced using the PLA and power gating techniques. The waveform can be analysed using the ALTERA QUARTUS II. The VHDL language coding is used to provide simulation result and are successfully dumped in Altera kit. This paper not only considers reducing power consumption it also reduce the transistor counts. This can be used for various security applications and for communications.

REFERENCES

[1] P.N. Khose, V.G. Raut. “Implementation of AES algorithm on FPGA for low area consumption”. In International Conference on 2015, Pages 1-4.

[2] T. Good and M. Benaissa. “Very small FPGA application-specific instruction processor for AES”. Circuits and systems l: Regular papers, IEEE Transactions on, 53(7):1477-1486, 2006.

[3] N. Ahmad, R. Hassan, and W. Jubadi. “Design of AES S-Box using combinational logic optimization”. In Industrial Electronics Applications (ISIEA), 2010 IEEE Symposium on, pages 696-699, 2010.

[4] C. Nalini, P. Anandmohan, D. Poomaiah, and V. Kulkarni. “Compact designs of Sub-Bytes and Mix-column for AES”. In Advance Computing Conference, 2009. IACC 2009. IEEE International, Pages 1241-247, 2009.

[5] Mozaffari-kermani, M.; Reyhani-Masoleh, A. “Efficient and High-performance parallel hardware architectures for the AES-GCM “. IEEE Transactions on 2012, volume: 61, pages: 1165-1178.