An Area Efficient Low Power High Speed S-Box Implementation Using Power-Gated PLA

Ho Joon Lee
Electrical and Computer Engineering
Northeastern University
Boston, MA, USA
hjlee@ece.neu.edu

Yong-Bin Kim
Electrical and Computer Engineering
Northeastern University
Boston, MA, USA
ybk@ece.neu.edu

ABSTRACT
Advanced Encryption Standard (AES) is one of the most common symmetric encryption algorithms. The hardware complexity in AES is dominated by AES substitution box (S-Box), which is considered as one of the most complicated and costly part of the system because it is the only non-linear structure. This paper presents a low power design of Rijndael S-Box for the SubByte transformation using power-gating and PLA design techniques to reduce area and leakage power during stand-by mode. The proposed design is implemented using 110nm standard CMOS process with 1.2V power supply. The proposed design reduces the total leakage power and the total transistor count to 10% and 50% of the conventional design, respectively while improving the speed performance by ten times.

Categories and Subject Descriptors
Cryptography, Power Gate, Low Power

Keywords
AES, PLA, Power Gate, S-Box

1. INTRODUCTION

The AES algorithm that has been used most widely is based on Rijndael algorithm, which was developed by Joan Daemen and Vincent Rijmen. It was announced by National Institute of Standards and Technology (NIST) in 1997 as AES algorithm[3] according to the primary criteria of security, performance, efficiency in software and hardware, flexibility, and implementability.

AES is attractive to embedded systems designers for a variety of reasons. Most importantly, it is a standard that is required in some applications and serves as the basis for several higher level protocols. It is also used in many existing applications where interoperability is desired, such as the wireless standards 802.15.4 and 802.11i and protocols including IPSec and SSH. AES is also relatively simple to implement in software, requiring little program and data memory[4]. It does, unfortunately, require substantial processing capabilities because the non-standard arithmetic is involved. For this reason, cryptographic functions like AES are often implemented in hardware as coprocessors to the main microprocessor.

The AES cipher involves repetitive round operations. Each round operation, SubBytes has been shown to be the performance limiting step, being several times slower than the other three steps (ShiftRows, MixColumns, and round key) required in AES algorithm. In general, SubBytes operation occupies half of the total delay time and 20% of the circuit area[8]. This paper focuses on the way to implement the SubBytes (S Box) operational unit efficiently to improve the overall encryption algorithm performance.

This paper proposes the S-box circuit implementation using PLA architecture and power gating scheme for the leakage reduction at nanoscale technology node to reduce leakage power when the SubBytes transformation is not active based on the mode introduce by [1]. The circuit design of the proposed architecture has been performed with 110 nm standard CMOS technology with post layout performance verification. In the next section, the S-Box algorithm is described briefly, and the proposed PLA and power gated design will be proposed in section 3. Section 4 presents the comparisons of the proposed design with the previous work in terms of power and performance, followed by conclusion and the summary of the results in section 5.

2. SUBBYTE 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[9].

The SubBytes function replaces each byte in the state with an affine transform of that byte. The process is usually called a Substitution Box (S-Box) in cryptography, and it is a fairly common operation[5].
Figure 1: The AES algorithm. (a) Encryption structure. (b) Equivalent decryption structure.

In software, S-Boxes are usually implemented by a simple look-up table (LUT), which store all 256 bit predefined values of S-Box in a ROM. The advantage of using LUT is that it offers a shorter critical path. However, it has a drawback of the unbreakable delay in high speed pipelined designs, and it cannot be used in high speed applications. It also requires a large area to implement AES encryption and decryption system due to different table used for both systems.

Another way is to design S-Box circuit using combinational logic only which is directly calculated from the arithmetic properties. This approach has breakable delay of S-Box transformation. It can achieve a high speed design but suffer from extremely huge area cost.

One of previous proposed design[7] implemented S-Box using a combinational logic without computing the Galois Filed. They proposed two techniques; one is based on logic synthesis using truth table, and the other is direct implementation of the Algebraic Normal Form (ANF) expression for each column. But it creates very many constant path delays compared to designs based on composite field.

Other approach using multiplicative inverse in Galois Filed GF $2^n$ uses composite filed[6]. Although it has an advantage of low area overhead, the critical path delay is increased and hardware complexity is significantly increased. To address the disadvantages that the conventional approach to implement the S-Box, this paper proposes a power efficient and area efficient PLA based S-Box design for SoC solution of the AES system in nanoscale CMOS technology.

3. PROPOSED PLAS BASED DESIGN

3.1 Programmable Logic Array based Circuit Implementation

[1] implemented the S-Box using the combinational random logic and a 16:1 bit mux as shown in Figure 2. It is a simple gate level translation from Boolean logic expression without power and performance consideration, which requires a power/area optimization as well as PVT(Process, Voltage, and Temperature) variation consideration in nanoscale technology era. Furthermore, leakage current during standby mode needs to be minimized for overall power reduction. In this paper, S-Box design based on the model introduced in [1] is presented using Programmable Logic Array (PLA) and power-gating techniques for power and area efficient solution. The previously proposed S-Box design in [1] is implemented with combinational logic as an effort to solve the unbreakable delay incurred by look-up table(LUT) based architecture and to reduce the critical path delay by using composite filed arithmetic.

The S-Box architecture consists of sixteen module logic functions, and each of the module logic function consists of AND gate, NOT gate, and OR gate. For example, the Boolean expression for Module 1(M1) as follows:

\[
\begin{align*}
    y_7 &= b\overline{cd} + ab\overline{c} + ab\overline{d} + \overline{a}bcd, \\
    y_6 &= \overline{a} + \overline{b}c\overline{d} + b(\overline{c}d), \\
    y_5 &= ac + \overline{d} + \overline{a}c + \overline{b}c, \\
    y_4 &= \overline{a}\overline{b}(c + d) + \overline{a}d(a + b) + abd, \\
    y_3 &= \overline{a}d(c + d) + bc\overline{d} + abd, \\
    y_2 &= ab\overline{c} + b\overline{c}\overline{d} + \overline{b}cd + abd, \\
    y_1 &= \overline{a}c\overline{d} + \overline{b}c + \overline{a}\overline{b}d + ab.
\end{align*}
\]

However, this architecture still suffer from the hardware complexity because too many basic random logic gates are used. The conventional approaches to implement the S-Box has been Field Programmable Gate Array (FPGA) based design using HDL language. Since the FPGA based design is cost and time effective, it is really fast time-to-market solution. However, certainly tradeoffs exist between FPGA and ASIC approaches. Although FPGA offers advantages such as easiness of design/test as well as cost comparing with Application Specific Integrated Circuits (ASICs), it suffers from disadvantages of area, speed, and power. How-
ever, performance of ASIC approach often does not meet the requirements of the systems for high performance and low power applications. Fortunately, the full custom design becomes the choice of design to overcome the disadvantages of FPGA and ASIC based design in this area as Systems-on-Chip (SoC) and IP block design are becoming more general approach.

Therefore, a power and area effective implementation of S-Box architecture is proposed in this paper using power-gating and PLA design techniques. The proposed circuit is highly optimized for performance, area, and power by taking advantages of full custom design approach. Programmable Logic Array (PLA) is kind of programmable logic device used to implemented combinational logic circuits that has many min terms. The PLA has a set of programmable AND gate planes, which link to a set of programmable OR gate planes, they can be conditionally complemented to produce an output. This architecture allows for a large number of logic functions or gates to be synthesized in the sum of products canonical forms. All the 16 modules’ boolean expressions mentioned previous section are converted into PLA planes. The proposed Module 1 (M1) implementation with PLA structure is shown in the Figure 3. The transistor size of the PLA has been optimized considering the wire load of every signal line and the pre-charge device.

3.2 Power Gated modeling

As described in the previous section, the SubByte transformation is considered as a very complex design and it causes high area and power dissipation in AES. Since power reduction is one of the primary concerns in this design, power-gating technique is applied to the proposed architecture to reduce leakage current during standby mode. There are a few leakage components in nanoscale transistor, which are gate leakage, diode leakage (junction leakage), and sub threshold leakage currents. In this paper, gate leakage and subthreshold 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. Although NMOS footer device does not reduce gate leakage as much as PMOS header, NMOS footer transistor size can be only half of PMOS header size and also it reduces other leakage current such as subthreshold current effectively with a half size of PMOS header. That is the reason that the NMOS footer, as shown in the Figure 4, is used as a power gating element in this paper. To minimize the ground bounce at the drain node of the footer device due to rush current at the start of operation, the footer device size is determined with enough width to ensure a solid virtual ground level at the drain node.

3.2.1 Input Control Circuit

Once the current switch (power gating device) is designed based on the method presented in the above, the power consumption of the power-gated circuits needs to be further reduced by controlling the primary inputs. By providing logic 1 to all primary inputs of a power-gated circuit with a footer, input gate leakage currents can be minimized because the input devices of the PLA is NMOS.

Since the extra logic for input control can be an overhead in terms of power consumption, area, and delay, an efficient circuits as shown in Figure 5 is used. In the circuit of the Figure 5, the input is transferred through transmission gate and two buffers in normal operation (i.e., when sleep = 0). When sleep operation, the input signal is de-coupled to the buffers and the gate of the first buffer is driven by logic 1, which almost eliminates the gate current of the buffer.

To check the gate leakage power reduction efficiency of the circuit in Figure 5, the entire PLA circuits including glue logic and power gating circuits are simulated and the total leakage currents are measured. The result is compared
with the case that does not use the power-gating technology. As shown in Table 2, the power gating technique reduces the stand-by currents to one tenth of the circuits without power-gating option. Since timing requirement of the sleep signal should meet the setup time in reference to the input, the transistor size is determined for the optimum setup time.

### 3.2.2 Rush Current Analysis

However, several critical issues should be resolved for PG structure design. The Power Gating structure has the disadvantage that an instantaneous charge current rushes through the sleep transistor operating in its saturation region while switching back to the active mode from the sleep mode[2]. If the sleep mode is long enough, the virtual ground will be charged close to $V_{DD}$. When the footer is fully turned on during the mode transition by a sharp control signal, the virtual ground will sharply be discharged, causing a large transient current. This large current leads to a great fluctuation in the power/ground grid due to the parasite inductance and capacitance in the power and ground pins.

![Figure 6: Rush current analysis of the proposed PG structure.](image)

As an attempt to overcome these problems, multiple sleep transistors are used in this paper as shown in Figure 6. Thanks to the distributed sleep transistors, the large current can be dispersed and it is possible to reduce the rush current as shown in Figure 7.

### 3.2.3 Ground-Bounce Due to Power Gating

From the sleep mode to active mode, it causes voltage fluctuations in the on-chip power distribution network due to the bonding wire and on-chip parasitic inductance. This voltage fluctuation - also known as ground bounce, which is associated with the switching of I/O buffers and internal digital circuitry, and clock gating, is one of the growing concerns for the reliability of power deliver in nanoscale systems. The voltage fluctuation is also reduced by the multiple power-gating switches used to reduce the rush currents. In order to further reduce the ground bounce, the metal connected to the footer device is designed with 3X minimum width to reduce the wire resistance. Then additional power gating path is provided for the leakage reduction and allowable reliability tolerance. Because of the leakage reduction, the magnitude of power supply voltage fluctuations during the active mode transition is reduced. Figure 8 shows the ground bounce using multiple switch/path and it is compared with the ground bounce with a single sleep switch and a single path case. It is very obvious that using multiple switch/path shows better performance compared to the single switch/path case.

![Figure 7: Spice simulation results of rush current.](image)

![Figure 8: Ground bounce analysis of the PG structure.](image)

### 4. EXPERIMENTAL RESULTS

AES S-Box has been designed and implemented using power-gating and PLA design techniques to reduce power...
Table 1: Performance and transistor count comparison

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Delay(ns)</th>
<th>Total no. of transistors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed</td>
<td>0.963</td>
<td>2977</td>
</tr>
<tr>
<td>Prev 1[7]</td>
<td>10.802</td>
<td>7270</td>
</tr>
<tr>
<td>Prev 2[6]</td>
<td>14.653</td>
<td>-</td>
</tr>
<tr>
<td>Prev 3[1]</td>
<td>7.745</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1 compares the previous S-Box design and our proposed PLAS architecture in terms of delay and transistor count. It is observed that our proposed PLA based S-Box design has efficient area compared to other three approaches. It also shows that the delay of our proposed S-Box is at least seven times faster than previous architecture.

Transistor size of the PLA circuit and footer device are highly optimized for area, power, and performance as well as rush current and ground bouncing. The functionality and the performance of the proposed implementation has been verified using 110nm standard CMOS technology with 1.2V power supply considering with wire loading and parasitic elements extracted from layout. The leakage reduction using the proposed implementation approach is significant as shown in Table 2.

Table 2: Standby and leakage current comparison

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Standby power</th>
<th>Leakage current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed(Non PG)</td>
<td>7.548mW</td>
<td>6.28mA</td>
</tr>
<tr>
<td>Proposed(PG)</td>
<td>0.658nW</td>
<td>0.541nA</td>
</tr>
</tbody>
</table>

Table 2 shows the power gating simulation results. As shown in the Table 2, the proposed power-gated PLA based S-Box architecture saves a huge power during standby mode. Since significant amount of leakage power and area are saved in the design, the proposed design approach can be a viable solution for low power AES design.

5. DISCUSSION & CONCLUSION

In this paper, a new design approach for S-Box design is presented using PLA and power-gated techniques, and its performance was analyzed and compared with the conventional S-Box designs. The proposed S-Box architecture demonstrates advantages in terms of area, speed, and power consumption. The proposed design reduces the complexities of hardware by avoiding the use of multiplicative inverse in Galois filed. As the proposed approach saves a significant transistor count and leakage power during stand-by mode, it will be a viable solution for low power SoC integration based on AES.

6. REFERENCES