A Full-custom Design of AES SubByte Module with Signal Independent Power Consumption

Liang Li, Jun Han*, Xiaoyang Zeng, Jia Zhao
State-Key Lab of ASIC and System, Fudan University, Shanghai 201203, China
062052003@fudan.edu.cn

***Abstract*—A full-custom design of AES SubByte module based on Sense Amplifier Based Logic is proposed in this paper. Power consumption of this design is independent of both value and sequence of data. Therefore this design is resistant to power analysis attack. This design is implemented using SMIC 0.18um CMOS technology. Simulation results show that it can work at the frequency of 83.3MHz, and its total area is about 0.85mm^2. This design is suitable for application in the hardware implementation of symmetric-key cryptographic devices that have high security demand.**

I. INTRODUCTION

Security IC which applies to smart cards, e-commence, electronic bank and so on, is becoming more and more important nowadays. But in recent years, attackers can find the security IC's secret key through side-channels information leaked by the switching behavior of digital CMOS gates [5][6][7][8]. Especially differential power analysis (DPA) attack is very effective in finding secret key. This attack is based on the fact that CMOS logic operations have the power characteristics that come from transition of data [7].

The default logic style in standard cell libraries used for security ICs is static complementary CMOS logic (scCMOS), which only consumes energy from power supply when its output has a 0-1 transition [9]. This asymmetric power characteristics provides the information that is useful for DPA attacks. The power consumption of logic gate originates from the value and the sequence of the input data. To avoid DPA attacks, a dynamic and differential CMOS logic style named as Sense Amplifier Based Logic (SABL) is proposed in [1][2], which can operate with constant power consumption. Recently, the design of sense-amplifier based flip-flop (SAFF) [3][4] have been proposed. The high clock frequencies of contemporary circuit are generally gain by using a fine-grain pipeline. Because of high number of pipeline stages in this circuit, the power consumption of the flip-flops is the substantial portion of total power budget. The SAFF provides ratioless design , reduced the short-circuit power dissipation. The design of this paper chooses pipeline structure, and uses the sense-amplifier based flip-flop（SAFF）[3], which can operate with constant power dissipation.

Advanced Encryption Standard (AES) is a secret key cryptography algorithm specified by the National Institute of Standards and Technology (NIST). It is the most commonly accepted private key algorithm currently in use today. In order to fit some portable devices, the low power design of AES is proposed in [10][11]. This paper uses the structure of low power AES proposed in [10]. In AES algorithm, SubByte module is the main target of most DPA attacks, as illustrated in previous papers, for example [12]. Traditional IC design for SubByte is not secure because of the reasons mentioned above.

Consequently, this paper proposes a full-custom design of AES SubByte module using SABL to prevent DPA attacks. This paper is organized as follows. Section 2 describes the implementation of SABL. Section 3 introduces the architecture of AES SubByte module based on SABL. Section 4 describes the experimental results including area, frequency and the feature of anti DPA attack. Section 5 concludes this paper.

II. SENSE AMPLIFIER BASED LOGIC

A. Sense Amplifier Based Logic gate

SABL is based on two principles [1][2] according to K.Tiri's research: (1) the logic style is a Dynamic and Differential Logic (DDL), therefore it has a single switching event per cycle and the switching event is independent of the input signals; and (2) during every switching event, it charges and discharges a constant capacitance, which is the sum of all the internal nodes capacitance together with one of the balance output capacitance.

The corresponding author: email:junhan@fudan.edu.cn

This work supported by the National Natural Science Foundation of China(No. 60576024，60776028)

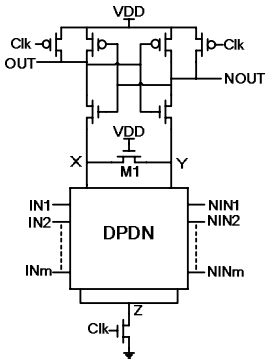

Figure 1. Structure of SABL

Figure 1 shows the structure of SABL[1][2]. The Differential Pull Down Network (DPDN) [2] connects one of the external nodes X and Y to the node Z. In the precharge phase (clk low), node Z is disconnected from GND and the output nodes X and Y are respectively precharged to VDD and VDD-Vth , where Vth is the threshold voltage. During the evaluation phase (clk high), the cross-coupled inverter toggles and provides a stable output as soon as a branch of the DPDN provides a path to GND. In case node X is connected to node Z, node OUT becomes 0, while node NOUT remains at 1. Similarly, in case node Y is connected to node Z, node NOUT becomes 0, while node OUT remains at 1.

B. XOR-NXOR gate based on SABL

The design in this paper uses XOR gate many times. Figure 2(a) shows a two inputs SABL XOR-NXOR gate[2] (XOR2D1). Figure 2(b) illustrates its parasitic capacitances and the current path from output to ground during evaluation phase. Simulation result demonstrates that the XOR2D1 gate works correctly and the transient response of two different cycles is very similar. This indicates that the power consumption is independent of the data.

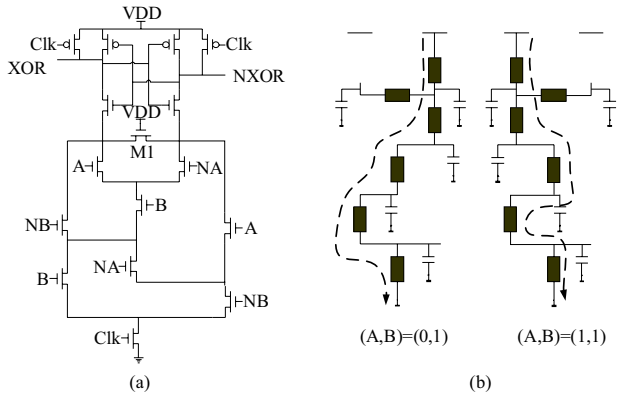

Figure 2. (a) SABL- XOR2D1 Gate, (b) Analysis of two inputs SABL XOR-NXOR Gate for (0,1)-input and (1,1)-input

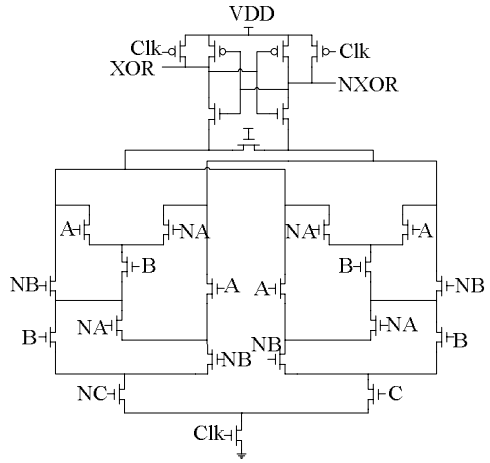

Figure 3. SABL-XOR3D1 Gate

Figure 3 illustrates a three inputs SABL XOR-NXOR gate (XOR3D1) for more complicated logic in AES SubByte module. The working principle of XOR3D1 is similar to that of XOR2D1. Table 1 shows the implementation result of XOR2D1 and XOR3D1 using SMIC 0.18um CMOS technology. There is no obvious capability difference between XOR2D1 and XOR3D1. And they have the nearly same delay when the clock cycle is 12ns.

Table 1. Comparison of the XOR2D1 and the XOR3D1

Gate	Numbers of the transistor	Delay (ns)	Layout area (um^2)
XOR2D1	16	0.109	185.8116
XOR3D1	26	0.128	289.9535

III. AES SUBBYTE MODULE DESIGN BASED ON SABL

A. AES SubByte

SubByte is the most complicated part in the AES algorithm, because it is the only non-linear operation and performs different affine transformation in encryption and decryption phase.

There are two ways to realize the SubByte module in general, look-up table and finite field calculation. This paper employs the finite field calculation method to realize this module so as to reduce its hardware cost. The $GF(2^8)$ inversion calculation is mapped into $GF(2^4)$ because calculations in $GF(2^4)$ are easier to conduct. This approach can accelerate and simplify the $GF(2^8)$ inversion calculation.

A bi-directional SubByte block capable of both encryption and decryption function is shown in Figure 4 [8]. In Part1 and Part3, affine (invaffine) is the (inversive) affine transformation, mapping is the transformation from $GF(2^8)$ to $GF(2^4)$ and invmapping is the transformation from $GF(2^4)$ to $GF(2^8)$.

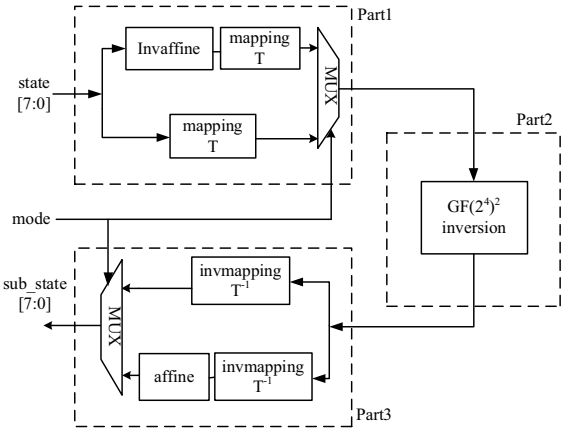

Figure 4. Structure of AES SubByte module

Part1 and Part3 have similar structure, and both can be realized by a sequence of XOR calculations with a multiplex output.

The internal structure of Part2 is shown in Figure 5. Part2 contains such calculations as add, square, multiplication and inverse in GF(2^4). All these calculations are equivalent to combinations of XOR, AND, INV [10].

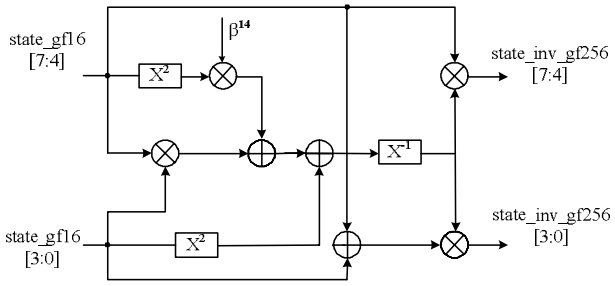

Figure 5. Structure of Part2

B. Implementation of SubByte based on SABL

Consequently, this AES SubByte module can be implemented with the following set of basic cells: INV, AND2D1, AND3D1, XOR2D1 and XOR3D1 based on SABL [11]. Because SABL is differential and dynamic logic, this paper chooses the pipeline structure instead of directly connection. This kind of structure can achieve high speed at the cost of some area. The latch used in this design is also Sense Amplifier Flip-flop (SAFF) [3][4][13][14] whose work frequency is much higher than normal flip-flops. In order to obtain smaller area, some optimizations are performed in choosing XOR2D1 or XOR3D1 when facing a formula with several XOR operations. For example: Y=A^B^C^D^E^F. Figure 6 shows two methods of achieving the equation. Figure 6(a) has 2 XOR3D1 gates, 1 XOR2D1 gate and 3 SAFFs while Figure 6(b) has 1 XOR3D1 gate, 3 XOR2D1 gates and 4 SAFFs. According to Table 1, the layout area of one XOR3D1 gate is smaller than the layout area of two XOR2D1 gates. Obviously, Figure 6(a) has smaller area than that of Figure 6(b).

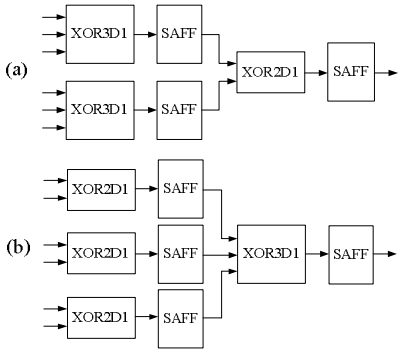

Figure 6. Two methods of achieving the equation Y=A^B^C^D^E^F

And the structure of multiplexer is illustrated in Figure 7. Its basic cell is SABL-AND2D1 which is a two inputs gate [9].

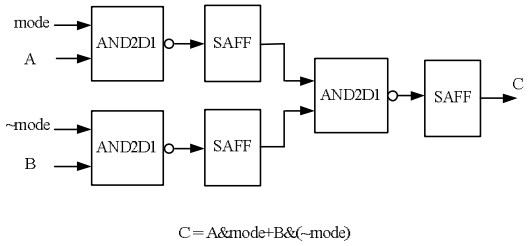

Figure 7. Structure of multiplexer

IV. EXPERIMENTAL VERIFICATION OF SUBBYTE

The circuit is implemented using SMIC 0.18um, 1.8V CMOS technology. The area of this layout is 0.85mm^2. Back-end simulation shows that the circuit can work at the frequency of 83.3MHz. Figure 8, a superposition of simulation power supply current for successive cycles of the transient response, illustrates that the instantaneous current of the scCMOS implementation is various. However during both precharge and evaluation phases, the SABL-SubByte performs the very similar instantaneous current. That means the power consumption is independent of the value and the sequence of the data.

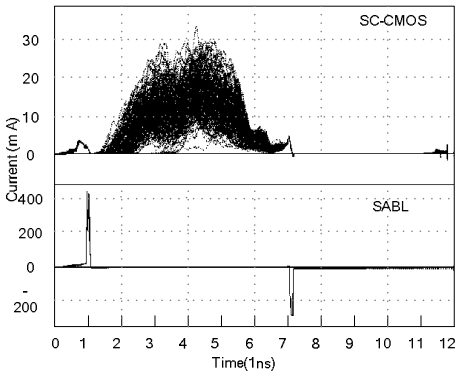

Figure 8. SubByte module : superposition of the instantaneous power supply current for 600 clk cycles of simulated transient response

Simulation results demonstrate that this AES SubByte module is effective against Differential Power Analysis compared to scCMOS implementations. Using Hspice netlist, the same DPA is applied to both scCMOS SubByte module and SABL-SubByte module for comparison. Figure 9 and Figure 10 illustrate the correlation between the number of changed bits from hypothetical model and the power consumption simulated by Hspice in every time point of all 256 possible keys (according to the method suggested in [12]). This attack is based on correlation analysis, which changes the input data and analyzes the correlation between the real power consumption and the result of analyzing hypothetical model [12]. 200 randomly selected plaintexts are executed to generate power consumption information. As shown in Figure 9, DPA on scCMOS SubByte module is successful because a peak corresponding to the correct key occurs. Figure 10 shows the same attack on SABL-SubByte module fails because correlation coefficients are all below 0.4, that shows no clear correlation.

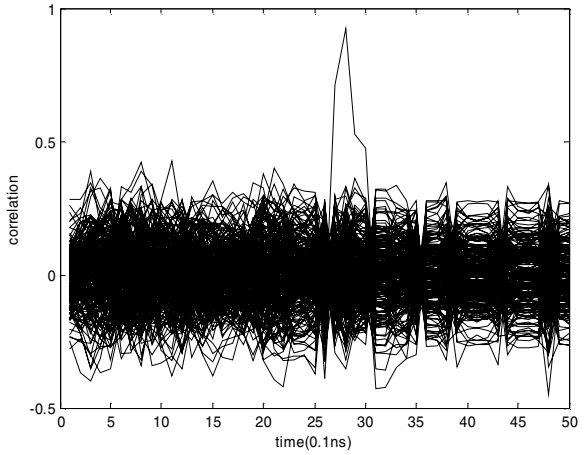

Figure 9. Correlation based DPA on scCMOS SubByte module

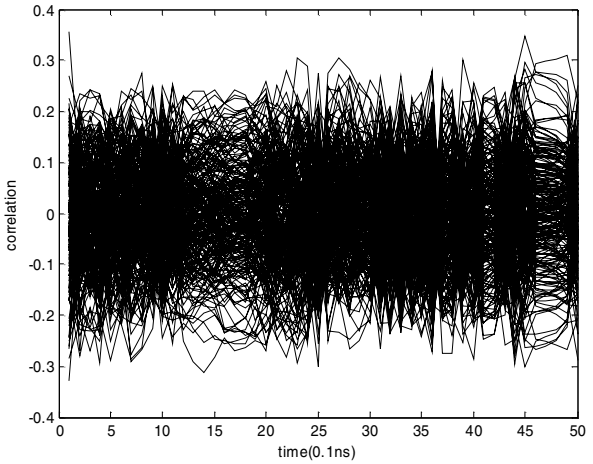

Figure 10. Correlation based DPA on SABL-SubByte module

V. CONCLUSION

This paper proposes a full-custom design of AES SubByte module with signal independent power consumption. Simulation results demonstrate that this AES SubByte module is effective against Differential Power Analysis compared to Static Complementary CMOS implementations. Therefore, this design is suitable for AES hardware application that needs high security.

REFERENCE

[1] K.Tiri, M.Akmal and I.Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards",28th European Solid-State Circuits Conference (ESSCIRC 2002), pp.403-406, September 2002.

[2] Tiri,Kris J V, "Design for side-channel attack resistant security ICs", Ph.D, University of California, Los Angeles, 2005, 141 pages; AAT 3169203.

[3] A.G.M.Strollo, D.De Caro, E.Napoli and N.Petra, "A novel high-speed sense-amplifer-based flip-flop", IEEE.VLSI systems, vol. 13, pp. 1266-1274, Nov. 2005.

[4] B.Nikolic,V.G.Oklobzija,V.Stojanovic,W.Jia,J.K.Chiu and M.M.Leung, "Improved Sense-Amplifier-Based flip-flop : design and measurements", IEEE J. Solid-State Circuits, vol. 35, pp. 876-883, June 2000.

[5] E.Hess, N.Janssen, B.Meyer, and T.Schuetze, " Information Leakage Attacks Against Smart Card Implementations of Cryptographic Algorithms and Countermeasures-a Survey", Eurosmart Security Conference, pp. 55-64, 2000.

[6] P.Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Advances in Cryptology (CRYPTO 1996), Lecture Notes in Computer Science, vol. 1109, pp. 104-113,August 1996.

[7] P.Kocher, J.Jaffe and B.Jun, "Differential Power Analysis", Advances in Cryptology (CRYPTO 1999), Lecture Notes in Computer Science, vol. 1666, pp.388-397, August 1999.

[8] J.Quisquater and D.Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards", Smart Card Programming and Security (E-smart 2001), Lecture Notes in Computer Science, vol.2140,pp.200-210,2001.

[9] J.Rabaey, Digital Integrated Circuits: A design perspective, Prentice Hall, 1996.

[10] Jia Zhao, Xiaoyang Zeng, Jun Han, Jun Chen, "Very Low-cost VLSI Implementation of AES Algorithm" Solid-State Circuits Conference, 2006.IEEE, pp. 223-226, Nov.2006.

[11] S.Morioka and A.Satoh, "An Optimized S-box Circuit Architecture for Low Power AES Design," Proc. CHES 2002, LNCS Vol. 2523, pp. 172-186, 2003.

[12] S.B.Ors, F.Gurkaynak, E.Oswald, B.Preneel, "Power-analysis attack on an ASIC AES implementation", IEEE. Digital Object Identifier, vol. 2, pp. 546-552, 2004.

[13] J. Tschanz, S. Narendra, C. Zhanping, S. Borkar, M.Sachdev, and V. De, "Comparative delay and energy of single edge-triggered and dual edge-triggered pulsed flip-flops for high-performace microprocessors," in Proc. Int. Symp. Low Power Electronics and Design, Aug. 2001, pp. 147-152.

[14] B. Nikolic, V. G. Oklobdzija, V. Stajanovic, W. Jia, J. K. Chiu, and M. M. Leung, "Improved sense-amplifier based flip-flop: Design and measurements," IEEE J. Solid-State Circuit, vol. 3, no.6, pp. 876-883, Jun. 2000.