Process Variation Verification of Low-Power Secure CSSAL AES S-box Circuit

Câncio Monteiro
Graduate School of Engineering, Gifu University
1-1 Yanagido, Gifu-shi, 501-1193, Japan
Email: canciotimor@gmail.com

Yasuhiro Takahashi and Toshikazu Sekine
Faculty of Engineering, Gifu University
1-1 Yanagido, Gifu-shi, 501-1193, Japan
Email: {yasut, sekine}@gifu-u.ac.jp

***Abstract*—In this work, we implement our previously proposed charge-sharing symmetric adiabatic logic (CSSAL) in an 8-bit S-box circuit using a multi-stage positive polarity Reed-Muller (PPRM) representation with a composite field technique. We evaluate the effectiveness of the CSSAL S-box circuit against side-channel attacks towards the variations of the CMOS process technology. The results of this paper are obtained from the SPICE simulation with 0.18-μm and 90-nm standard CMOS technology at an operating frequency band of 125 KHz–70 MHz.**

I. Introduction

The modern cryptology had mainly focused on cryptosystems resistant against side-channel analysis (SCA), which has become a special threat for chip designers, software developers, and hardware engineers working to secure private information stored in cryptographic devices such as smart cards, RFID tags, USB tokens, and wireless sensors. The SCA can be used to unveil the secret key of cryptographic devices by analyzing the side-channel information such as the power consumption, computing time, and electromagnetic radiation. Among these SCA attack techniques, differential power analysis (DPA) attacks are the most threatening type of attacks that reveal the secret information in a cryptosystem. A DPA attack seeks to reveal the secret key of a smart card by statistically analyzing the power fluctuations that occur while the device encrypts and decrypts large blocks of data [1]. Apart from the DPA attacks, the differential electromagnetic radiation attack (DEMA) has been extensively studied [2]. DEMA attacks can reveal secret information because the current flow during the switching of the CMOS gates causes a variation in the surrounding electromagnetic field, which can be monitored by positioning an inductive probe around the microcontroller chip.

On the basis of cryptanalysis knowledge to unveil secure information in the preceding data encryption standard, the Advanced Encryption Standard (AES), an efficient algorithm for both hardware and software implementations, was standardized by the NIST in 2001 [3]; this standard operates over $GF(2^8)$ for computational efficiency and exhibits high resistance to cryptanalysis, hardware and software compatibility, and flexibility. Since the new AES was announced, much efforts have been expended [4], [5] to simplify a finite field over $GF(2^8)$ in the S-box transformation to $GF((2^4)^2)$ and $GF(((2^2)^2)^2)$ for low cost, low power consumption, and low complexity.

A majority of the logic styles implemented in cryptographic hardware applied the conventional CMOS logic operation that causes the occurrence of different high spike current and huge energy consumption. For example, peak current transition of a static complementary CMOS (scCMOS) used for security ICs consumes different peak current for charging and discharging process as shown in Fig. 1(a). Furthermore, a technique to balance the charging and discharging load for uniform peak current trace, the dual-rail CMOS (DR-CMOS) logic in Fig. 1(b) become a solution for secure logic designing. Observing the current transition in Fig. 1(a), (b), generally, transitional power consumption values hold that $(P_{0\to0}{\approx}P_{1\to1}) \ll (P_{0\to1},P_{1\to0})$, which is attackable by using Hamming Distance (HD) model in power analysis attacks. The idea behind HD model is to count the number of $P_{0\to1}$ and $P_{1\to0}$, $P_{0\to0}$ and $P_{1\to1}$ transitions that occur in the digital circuit during a certain time interval with the assumption of $(P_{0\to1} \approx P_{1\to0}) \neq (P_{0\to0} \approx P_{1\to1})$. From the view point of DPA and DEMA attack techniques, the scCMOS and DR-CMOS are vulnerable, because they perform different peak current transition and different large magnitude which cause a sudden variation of the electromagnetic field surrounding the chip as reported in [2]. As a result, the DPA and DEMA attacks are a bit difficult to avoid.

In our approach, we have implemented a logic circuit that exhibits uniform peak current for all possible input transition to avoid HD model by an expression $(P_{0\to1} \approx P_{1\to0}) = (P_{0\to0} \approx P_{1\to1})$ as shown in the right side of Fig 1(c). In this work, our previously proposed CSSAL [8] is implemented in an 8-bit S-box circuit using the PPRM representation [5] for low peak current transition and low energy consumption by exploiting an adiabatic switch principle [9]. We have also implemented several dual-rail adiabatic logic styles, such as SyAL [10], 2N-2N2P [11], and Morioka's circuit [5] in the same S-box circuit and compared the results. All the comparative results described in this work are obtained using the SPICE simulation at the cell level.

978-1-4799-4132-2/14/$31.00 ©2014 IEEE

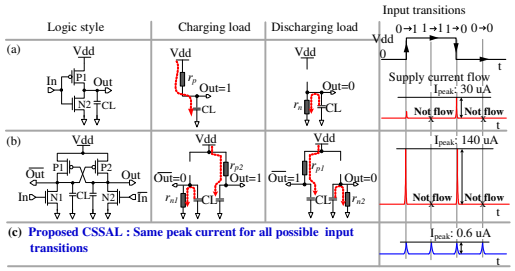

Fig. 1. Logic comparison of the transitional current traces; (a) scCMOS, (b) DR-CMOS, (c) Target supply current trace of the proposed CSSAL.

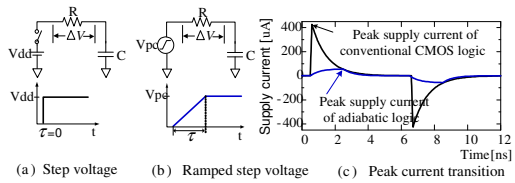

Fig. 2. Comparison of the supply currents for the equivalent RC models: (a) CMOS logic with step voltage; (b) adiabatic logic with ramped step voltage; (c) The peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic under the same parameters and conditions.

II. Low-Power S-Box Circuit using Adiabatic Logic

A. Adiabatic Logic Technique

Adiabatic switching is commonly used for minimizing the energy lost during the charging/discharging period at all nodes of the circuit. The main concept of adiabatic switching is shown in Fig. 2(b); this figure indicates a transition that is considered sufficiently slow such that heat is not significantly emitted. The adiabatic dissipated energy is expressed as $E_{adiabatic} = 2(RC/\tau)CV_{dd}^2$, where R is the effective resistance in the driven device, C is the output node capacitance to be switched, τ is the time over which switching occurs, and V_{dd} is the voltage to be switched across. Ideally, the charging energy $E_{adiabatic}$ tends to zero by increasing the length of τ. Conversely, the conventional CMOS logic operation is shown in Fig. 2(a), with the following equation: $E_{conv.} = CV_{dd}^2/2$; here, it is possible to reduce the charging energy only by reducing V_{dd} or capacitor C. Figure 2(c) shows a comparison of the peak supply current for the equivalent RC models of the conventional CMOS logic and the adiabatic logic. The comparison result in this figure shows that the instantaneous peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic style.

B. Charge-Sharing Symmetric Adiabatic Logic

The proposed charge-sharing symmetric adiabatic logic (CSSAL) operation was described in detail in [8]. We recall the CSSAL inverter logic in this paper for better understanding of the secure logic comparison with Fig. 1, as depicted in Fig. 3(a)–(c). The logic operation is clearly described in Fig. 3(b) that at In, $Eval$, $Dischg \geq V_{th}$ of the MOS transistor in the charge-sharing phase, all internal nodes are

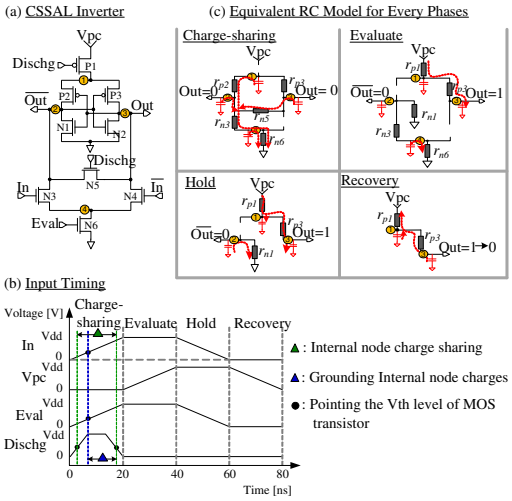

Fig. 3. Proposed CSSAL; (a) inverter logic structure, (b) timing diagram, (c) equivalent RC model for each phase.

discharged to ground level before evaluation, hold and recovery phases take place, as shown by the equivalent RC model in Fig. 3(c).

C. Multi-Stage PPRM Architecture

The targeting S-box circuit of the multi-stage PPRM architecture has been proposed by Morioka *et al.* in [5]. In our proposed CSSAL S-box circuit, we apply three power clock supplies for each stage as shown in Fig. 5, which completely avoid the glitch current, consume uniform transitional energy and ensure significant energy reduction in our comparative results, even though the transistor counts much higher than other adiabatic logics investigated, as shown in Table II. Triple power clock Vpc0, Vpc1 and Vpc2 signals are depicted in Fig. 4. The primary input signal and Vpc2 shown in Fig. 4 and the input signal and Vpc signal shown in Fig. 3(b) are identical. The S-box circuit structure presented in the appendix of [5] describes that variables $x_7 - x_0$ denote the primary inputs of an S-box and $y_7 - y_0$ denote primary outputs. The other variables such as a, b, c, and d denote the internal wires. Therefore, in Fig. 4, we apply Vpc0 and Vpc1 as the power supplies for the internal wires of the circuit architecture shown in Fig. 5(b) in order to eliminate the unwanted electric hazard voltage at the output signals. Moreover, we utilize a logic sharing method instead of a multiple logic recurrence method that uses the same input signals; hence, the dual-input logic complexity is reduced to approximately 17% that of Morioka's design in [5], as an example is shown in Table I for internal wires "$a_0 - a_3$". In addition, the transistor complexity of the proposed CSSAL is higher than the other adiabatic logic styles; thus, the proposed CSSAL individual logics are an area consuming by our full custom layout design as shown in Table II. Furthermore, the proposed CSSAL S-box timing diagram in Fig. 4 shows that the phase delay time of Vpc2 is 20 ns from primary input signal; therefore, the logic speed is slow in comparing to the other adiabatic logic styles as

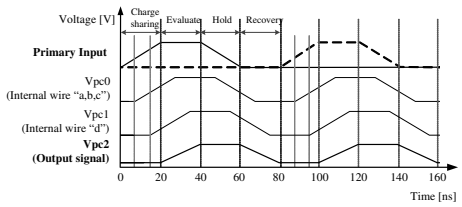

Fig. 4. Triple power clock signals for CSSAL S-box circuit shown in Fig. refFig7(b).

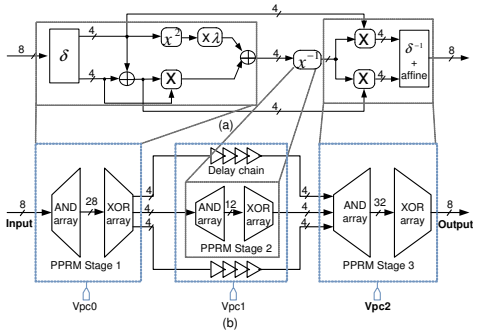

Fig. 5. (a) Conventional composite field AES S-box architecture; (b) multi-stage PPRM representation with the implementation of the proposed triple V_{pcs} signals in the CSSAL 8-bit S-box circuit.

summarized in Table II. Definitions of adiabatic delay time is derived as Td$_{Adiabatic}$ = Phase delay time + Propagation delay time. Although, the proposed circuit has disadvantages in term of overhead area and latency, but it consumes more uniform power than other benchmark methods; thus, the input-output data analysis using peak supply current differences by DPA technique are difficult.

III. Simulation and Result

A. Condition

The typical result provided in this paper was obtained using SPICE simulation with 0.18-μm and 90-nm standard CMOS technology. To validate the results in this proposal, we have simulated and compared our proposed CSSAL with SyAL, 2N-2N2P and Morioka ' s circuit [5] using the same parameters. We attach 10-fF load capacitors to all the output nodes of the buffer, NAND/AND, and XNOR/XOR gates in our simulation as an optimal design for future chip measurement comparison. The range of the power clock frequency for the proposed CSSAL S-box circuit is from 125 KHz–70 MHz using 0.18-μm, and 1.25–70 MHz using 90-nm. Moreover, to investigate the effectiveness of the logic immunity in a presence of process variations, we then conduct the calculations at 12.5 MHz for both 0.18-μm and 90-nm CMOS process variation in Monte Carlo simulation. In these cases, there are 256–transitional energy dissipation data of each S-box circuit for calculation samples.

B. Results

The simulation results of this comparison study are show in Figs. 6, 7 for all the logics investigated in the 8-bit S-box circuit. The data of power consumption of each circuit

TABLE I
Example of the logic sharing method of S-box stage-1 of internal wires a_0–a_3

[5]	This work
$a_3 = x_7 \oplus x_5$	$\mathbf{x_a} = x_7 \oplus x_5$; $\mathbf{x_b} = x_3 \oplus x_2$;
$a_2 = x_7 \oplus x_6 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1$	$\mathbf{x_c} = x_a \oplus x_b$; $\mathbf{x_d} = x_6 \oplus x_4$
$a_1 = x_7 \oplus x_5 \oplus x_3 \oplus x_2$	$a_3 = x_a$
$a_0 = x_7 \oplus x_5 \oplus x_3 \oplus x_2 \oplus x_1$	$a_2 = \mathbf{x_d} \oplus x_7 \oplus \mathbf{x_b} \oplus x_1$
	$a_1 = \mathbf{x_c}$
	$a_0 = \mathbf{x_c} \oplus x_1$
Sub-total: 13 XORs	Sub-total: 8 XORs

TABLE II
Gate size, transistor counts, layout area and delay of an 8-bit S-box circuit (0.18-μm 1.8-V CMOS standard cell @ 12.5 MHz)

Gate Counts			
Circuit	Buffer	AND	XOR
Figure 7(b)	148	141	216

Transistor Counts and Delay					
Circuit	Buffer	AND	XOR	S-box	Delay (ns)
CSSAL	9×148	19×141	19×216	8,115	22.41
SyAL	5×148	15×141	15×216	6,095	12.29
2N-2N2P	6×148	8×141	10×216	4,176	15
[5]	–	8×203	16×228	5,272	3

Individual Logic and S-box Layout Area (μm^2)				
Circuit	Buffer	AND	XOR	CSSAL S-Box Area
CSSAL	83.82	185.82	142.73	795×614
SyAL	48.36	122.22	108.87	–
2N-2N2P	51.99	55.54	98.4	–

Note: CSSAL Buffer: 9T; CSSAL AND: 19T; CSSAL XOR: 19T; (T = Transistors)
Example of CSSAL S-box: (9×148) + (19×141) + (19×216) = 8,115T
Where, 148, 141, 216 are the gate counts of Buffer, AND and XOR respectively

are obtained as: $E_{diss} = \int_0^T V_{pc}(t) I_{pc}(t) dt$, which is adopted as the figure of merit to measure the resistance against power analysis attacks. The calculation for the normalized standard deviation (NSD) is given as $\sigma_E / \overline{E}$ [7]; where, $\overline{E}$ = $(\sum_{i=E_1}^{E_n} E_i)/n$ is the average of the energy dissipation over each respective transition, and the standard deviation is defined as $\sigma_E = \sqrt{\sum_{i=E_1}^{E_n} (E_i - \bar{E})^2 / n}$.

We measure NSD which indicate the ability of the logic against a power analysis attack. This parameter indicates how the consumed energy is more constant for different input transitions, only for small values of these parameters. Observing the NSD results in Figs. 6, 7 histograms, the CSSAL S-box has always smallest percentage than others for both CMOS process variations; thus, we can assure that the proposed CSSAL S-box has a unique ability to withstand the DPA attack.

In addition, it has been recognized that the conventional CMOS logic styles such as TDPL [7] and SABL [6] logics are well known and stronger to DPA attacks in secure logic implementation; however, comparative data are not available in this work because we have found out in our thoroughly SPICE simulation results that they are not suitable to operate in the 8-bit S-box using the PPRM representation.

Apart from the logic's ability for resistance against SCA attacks, power reduction is also one of the research targets. The graphical information in Fig. 8, evidently shows that the proposed logic has the lowest energy at all investigating operating frequencies using 0.18-μm BSIM3 model, 1.8-V

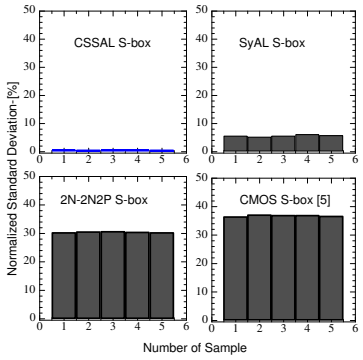

Fig. 6. Simulation and calculation results of NSD using 0.18-μm CMOS process variation for five samples of each circuit.

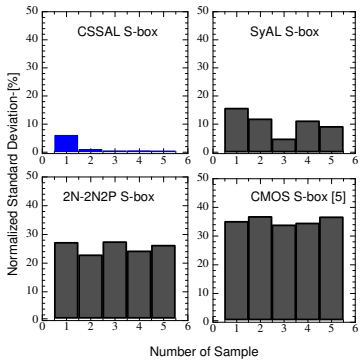

Fig. 7. Simulation and calculation results of NSD using 90-nm CMOS process variation for five samples of each circuit.

CMOS process. Furthermore, energy comparison data in Fig. 9 that using 90-nm BSIM4 model, 1.2-V CMOS process, the optimum operating frequency of the CSSAL S-box regards to energy dissipation is at 12.5 MHz, which is power efficiently applicable to low speed cryptographic devices, such as smart card (13.56 MHz, the carrier frequency of contact less IC Card).

IV. Conclusion

The investigation and comparison of secure adiabatic logic in a partial 8-bit AES S-box using PPRM representation for countermeasure against SCA attacks have been thoroughly carried out in this work. The investigation results of low-power adiabatic logic styles have shown that the proposed CSSAL S-box has significant energy reduction, improves the security performance to withstand DPA attacks, consumes less power, and can be operated in low frequency bands, such as contactless IC cards, RFID tags, and wireless sensors.

Acknowledgment

The custom circuits discussed in this paper have been simulated with 0.18-μm Cadence and Synopsys tools through the chip fabrication program of the VLSI Design and Education Centre (VDEC) at the University of Tokyo in collaboration with ROHM Corporation. Further 90-nm CMOS process simulation was implemented using Predictive Technology Model (PTM).

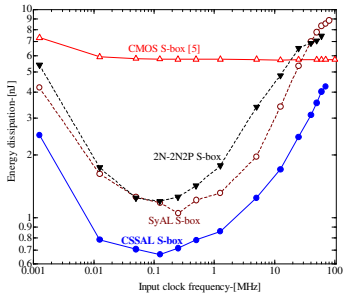

Fig. 8. Simulated energy dissipation comparison of all the investigated adiabatic logics: CSSAL, SyAL, 2N-2N2P, and Morioka [5] in the multi-stage PPRM 8-bit S-box circuit at each operating frequency ranges using 0.18-μm CMOS process.

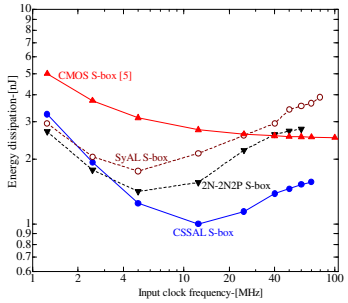

Fig. 9. Simulated energy dissipation comparison of all the investigated adiabatic logics: CSSAL, SyAL, 2N-2N2P, and Morioka [5] in the multi-stage PPRM 8-bit S-box circuit at each operating frequency range using 90-nm CMOS process.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Int. Adv. in Cryptol. Conf.* (CRYPTO), Aug. 1999, pp. 388–397.

[2] E. De Mulder, S. B. Ors, B. Preneel, and I. Verbauwhede, "Differential electromagnetic attack on an FPGA implementation of elliptic curve cryptosystems," in *Proc. WAC*, Jul. 2006, pp. 1–6.

[3] National Institute of Standards and Technology (NIST), "The Advanced Encryption Standard (AES)," FIPS Publication 197 (2001). [Online] Available URL: (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf).

[4] P. V. S. Shastry, A. Agnihotri, D. Kachhwaha, and J. Singh, "A Combinational Logic Implementation of S-box of AES", in *Proc. IEEE 54th MWSCAS*, Aug. 2011, pp. 1–4.

[5] S. Morioka and A. Satoh, "An Optimized S-box circuit architecture for low power AES design", in *Proc. 4th Int. Workshop on CHES 2002*, LNCS vol. 2523, pp. 172–186, 2003.

[6] 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," in *Proc. ESSCIRC*, Sept. 2002, pp. 403–406.

[7] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. CHES'06*, Oct. 2006, pp. 232–241.

[8] C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level," *Microelectronics Journal*, vol.44, no.6, pp.496-503, Jun. 2013.

[9] W. C. Athas, L. J. Svesson, J. G. Koller, N. Traztzanis, and E. Y.-C. Chuo, "Low power digital system based on adiabatic-switching principles," *IEEE Trans. VLSI System*, vol. 2, no. 4, pp. 398–406, Dec. 1994.

[10] B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," *ETRI Journal*, vol. 32, no. 1, pp. 166–168, Feb. 2010.

[11] A. Kramer, J.S. Denker, B. Flower, and J. Moroney, "2nd Order Adiabatic Computation 2N-2P and 2N-2N2P Logic Circuits," in *Proc. of the IEEE International Symposium on Low Power Design*, Apr. 1995, pp. 191–196.