一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
EMCJ2012-100(2012-12)

Survey on Secure Adiabatic Logic for Countermeasure against Side-Channel Attacks

Câncio MONTEIRO†, Yasuhiro TAKAHASHI††, and Toshikazi SEKINE††

† Graduate School of Engineering, Gifu University, Japan
†† Faculty Engineering, Gifu University, Japan

Abstract Side-channel attacks to reveal the secret information on cryptographic device has been extensively studied. One of such side-channel attack is electromagnetic analysis, which is monitoring the current amplitude, its direction, and its position that generated by the CMOS logic operation inside the secure IC-chip. Hence, this survey evaluates the peak-current traces of CMOS logic style using adiabatic logic technique at the secure logic simulation level. The SPICE simulation results show that our previously proposed CSSAL exhibits uniform and low amplitude of supply current compare to the conventional logic styles. Consequently, the logic immunity towards side channel attack is guaranteed.

Key words SCA, DPA, adiabatic logic, S-box, AES, smart card

1. Introduction

In the last century, the modern cryptology has mainly focused on cryptosystems resistant against side-channel analysis (SCA), which has become a special threat for chipper designers, software developers, and hardware engineers working to secure private information stored in cryptographic devices such as smart card, RFID tags, USB token, and wireless sensors. SCA can be used to unveil the secret key of cryptographic devices by analyzing side-channel information, such as power consumption, computing time, and electromagnetic radiation. Among these SCA attack techniques, differential power analysis (DPA) attacks are the most popular type of power analysis attacks to reveal the secret information in cryptosystem. A DPA attack seeks to crack the secret key of a smart card by statistically analyzing power fluctuations that occurs while the device encrypts and decrypts large blocks of data [1]. Apart from DPA attack, timing attack [2], differential electromagnetic radiation attack (DEMA) [3,4] and other side-channel attacks on cryptographic hardware has been extensively studied. Throughout analysis in [2] has described that attacker may able for find the secret key by carefully measuring the amount of operation time of cryptographic hardware. DEMA attack sketches that, current flow during the switching of the CMOS gates causes a variation of the electro-magnetic field surrounding the chip that can be monitored by inductive probes which are particularly sensitive to the related impulse.

The main factors of aforementioned attacks are related to CMOS logic power consumption and required operational time of cryptographic hardware itself. Regarding to this power consumption by secure chip in cryptographic hardware, the CMOS logic design should be highly considered in order to mask or hide the input logic values and also reduce power consumption in digital circuit level. As a countermeasure to the related issue, several method in different ways have been proposed, such as sense amplifier based logic (SABL) [5], wave dynamic differential logic (WDDL) [6], three-phase dual-rail pre-charged logic (TDPL) [7]. Moreover, an asynchronous dual-rail gate design [8] has been proposed that balances power, requires no capacitance matching of data outputs, and tolerates process variability in the routed interconnect between gates.

Although those side-channel countermeasures have been implemented, however, all of them applied conventional charging method (and the major problem in DPA attacks caused by the charging current of the capacitive loads) that causes the extremely high spike current occurrence and huge energy consuming. As a result, the DPA and DEMA attacks are a bit difficult to avoid. Hence, in this survey, we investigate our previously proposed secure charge-sharing symmetric adiabatic logic from the security view-point in comparison with previously published dual-rail adiabatic logic, *i.e.* secure adiabatic logic (SAL) [9], efficient charge recovery logic (ECRL) [10], symmetric adiabatic logic (SyAL) [11], and 2N-2N2P logic [12].

2. Charge Recovery Logic

2.1 Adiabatic Logic vis-à-vis Conventional CMOS Logic

The principle of adiabatic charging can be understood by contrasting it with the charging of a capacitor in an equivalent RC circuit for the conventional CMOS method. In the conventional CMOS circuit, the load capacitance C is charged from 0 to V_{dd}, where V_{dd} is the voltage of the DC power supply, as shown in Fig. 1(a). During the charging period of the conventional CMOS, the energy charged into the capacitor is:

$$E_{charge} = \frac{1}{2}CV_{dd}^2. \quad (1)$$

From the perspective of energy conservation, a conventional CMOS logic emits heat and thus wastes energy with every charge–discharge cycle: $E_{total} = E_{charge} + E_{discharge} = 1/2(CV_{dd}^2) + 1/2(CV_{dd}^2) = CV_{dd}^2$. If the logic is driven with a certain frequency $f(= 1/T)$, where T is the period of the signal, then the power consumption of the CMOS gate is determined as $P_{total} = E_{total}/\mathrm{T} = CV_{dd}^2 f$. Power consumption of conventional CMOS is proportional to V_{dd}^2. One of the most effective ways to reduce its power consumption is to lower the power supply voltage V_{dd} or the load capacitance.

Adiabatic switching is commonly used in minimizing the energy lost during a charging or discharging period. The main idea of adiabatic switching is shown in Fig. 1(b), which indicates a transition that is considered sufficiently slow that heat is not significantly emitted. This is made possible by replacing the DC power supply with a resonant LC driver or a trapezoidal power-clock voltage waveform. If constant current source delivers a charge $Q = CV_{dd}$ during the time period τ, the energy dissipation in the channel resistance R is given by:

$$E_{Adiabatic} = \xi P\tau = \xi I^2 R\tau = \xi \left(\frac{CV_{dd}}{\tau}\right)^2 R\tau, \quad (2)$$

where I is considered as the average of the current flowing to C, and ξ is a shape factor that is dependent on the shape of the clock edges. Observing the adiabatic switching equation, the charging period τ is indefinitely long, and so energy dissipation is ideally reduced to nearly zero [13]. We assume that, if the individual logic consumes a consistent and low-peak supply current, regardless of the input logic conditions, then a more complex digital circuit will be more secure against leakage of processed information to DPA or DEMA attacks. We make this assumption become possible by adopting the adiabatic logic technique as shown in Fig. 1(c). Figure 1(c) shows a comparison of peak supply current for equivalent RC models of the conventional CMOS logic and the adiabatic logic. The instantaneous peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic style.

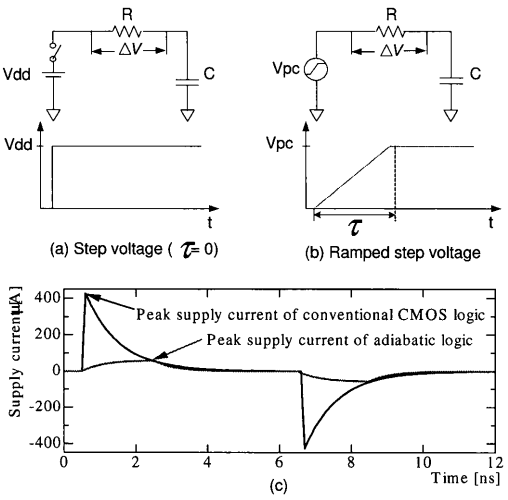

Fig. 1 Comparison of supply currents for equivalent RC models of CMOS logic ((a) step voltage) and adiabatic logic ((b) ramped step voltage). (c) The peak supply current of adiabatic logic is significantly lower than the conventional CMOS logic under the same parameters and conditions.

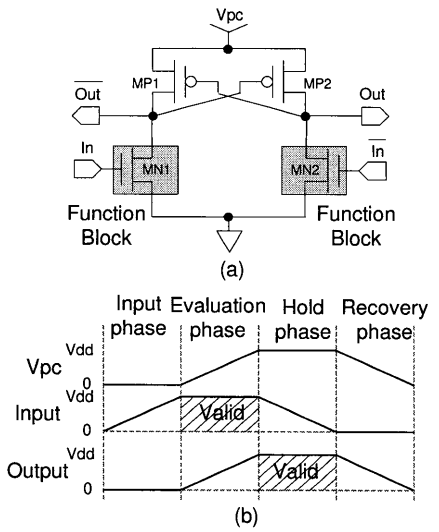

Fig. 2 ECRL; (a) Generic logic structure, (b) Timing diagram.

2.2 Secure Adiabatic Logic Styles

2.2.1 Efficient Charge Recovery Logic

Efficient charge recovery logic is the simplest DR adiabatic logic since ever been proposed. The generic logic structure of ECRL and its input and output waveform are shown in Fig. 2. The ECRL is basically operated in four phases; input phase where the input signal slowly goes high from $0 \rightarrow V_{dd}$, while the power clock signal is low. At the end of this phase, inputs have taken their own valid values. Suppose that In=HI and $\overline{In}$=LO; therefore MN2 is closed and MN1 is open. In other words, the function block which pre-

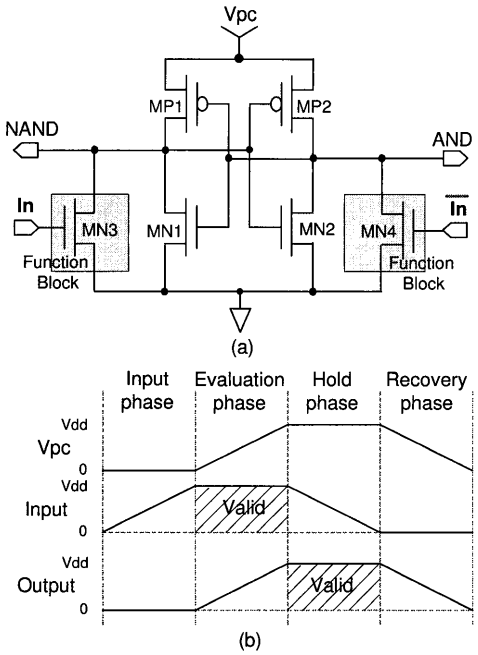

Fig. 3 2N-2N2P; (a) Generic logic structure, (b) Timing diagram.

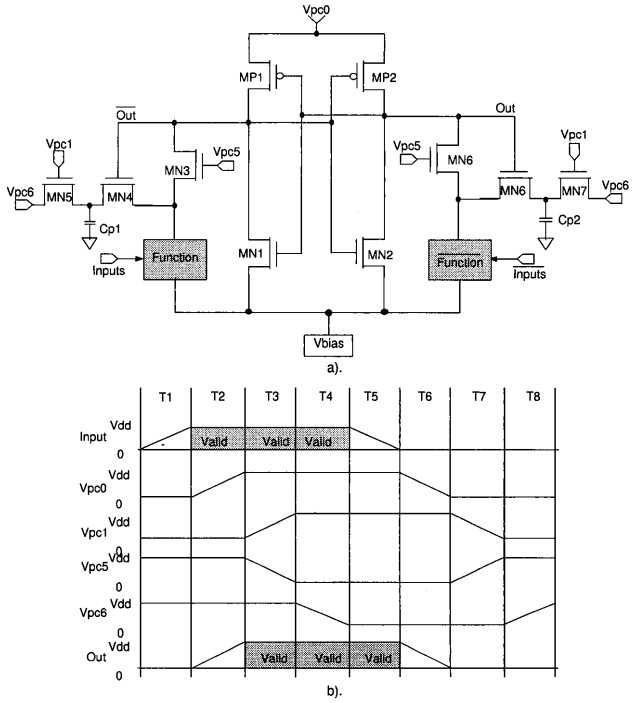

Fig. 4 SAL; (a) Generic logic structure, (b) Timing diagram.

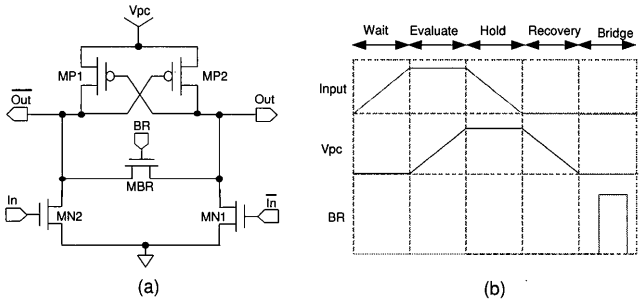

Fig. 5 SyAL; (a) Inverter logic structure, (b) Timing diagram.

pares *Out* signal is closed, and the complementary function block which prepares $\overline{Out}$ signal is open. Then, the evaluation phase, power clock signal slowly goes HI; thus, $\overline{Out}$ is charged through MP2. In contrast, *Out* node remains LO since it is connected to ground through the function block. During the hold phase, the present condition of valid output remains stable at HI level. Finally, the recovery phase, power clock steadily decreases to LO. By falling power clock, $\overline{Out}$ goes LO via MP2. Note that, the are floating charges at *Out* and $\overline{Out}$ nodes when *In* signal falls down to V_{tn} and V_{pc} signal reaches the V_{tp}. The remaining charge at output nodes are dissipated non-adiabatically at the next cycle if new inputs causes the complementary function block to switch on.

2. 2. 2 2N-2N2P Logic

The operational function of 2N-2N2P gate is similar to ECRL logic operation, they have same phases. Generic logic of the 2N-2N2P and its waveform are shown in Figs. 3. Observing Fig. 3(a), 2N-2N2P gate consists of two main parts: (i)two functional block whose duty is to construct the gate outputs *Out* and $\overline{Out}$, and (ii) a latch which is made by two cross-couple NMOS transistor to avoid floating charges at output nodes.

2. 2. 3 Secure Adiabatic Logic

The generic cell construction of SAL and its waveform are depicted in Fig. 4. A SAL consists of three main parts: (i) two function blocks construct the outputs. These functions are implemented by NMOS transistors, (ii) a latch which is made by two cross-coupled PMOS transistors, i.e., MP1 and MP2 to keep the output stable in respect to input condition, and (iii) extra pass transistors, i.e., MN3 to MN8, that are responsible to discharge internal capacitances of the function blocks adiabatically. The function blocks and the two cross-coupled NMOS transistors are connected to a DC bias voltage equal to Vtp instead of GND in order to avoids the non-adiabatic energy dissipation due to incomplete discharge of C_{load}. There are eight phases in original paper [9], however, we use four phases only in our simulation, as shown in Fig. 4(b).

2. 2. 4 Symmetric Adiabatic Logic

Symmetric adiabatic logic (SyAL) [11] employs a symmetric pull-down transistor that was proposed in symmetric discharge logic [15] to minimize differences in power traces for resistances to DPA attacks. The principal idea of the SyAL circuit is assigned to the discharge paths such that on–and off-transistors are configured equally for all cases. As it describes in the logic operation of ECRL that the output nodes of adiabatic logic are not fully discharge to ground level; therefore, SyAL is designed to share all internal parasitic ca-

pacitors by inserting the BR transistors that operate when power clock and both inverter input signals are at low level. As the result, the supply current is not affected by the previous input data. The inverter logic structure and its waveform are shown in Fig. 5.

2. 2. 5 Charge-Sharing Symmetric Adiabatic Logic

The detailed proposed CSSAL logic can be seen in [14]. We present here the CSSAL inverter in Fig. 6(a), and its input and output signals in Fig. 6(b) in order to summarize how the logic is operated. As shown in Fig. 6(b), the CSSAL operates in four phases as described following:

(a) **Charge sharing:** The discharge (*Dischg*) signal increases with a rate twice that of the input signal. In this phase, the power-clock voltage (V_{pc}) is stable at a low level, and the evaluation path signal which is established by In or $\overline{In}$ (MN5 or MN6) and *Eval* (MN8) cells simultaneously also slowly increases. All the internal node capacitances are discharged to ground before the logic function is evaluated, in order to prevent the circuit from depending on the previous input data.

(b) **Evaluation:** In this evaluation(*Eval*) phase, the *Dischg* signal is already stable at a low level, which turns on the MP1 for supply current to flow into the logic circuit. The output wires are evaluated through one of the active input cells.

(c) **Hold:** During the hold phase, the presently active input and Eval signals slowly decrease to become low, but the outputs remain stable because those are controlled by cross-coupled NMOSs MN1 and MN2.

(d) **Recovery:** The power clock voltage (V_{pc}) steadily decreases to a low level, and the presently active output is discharged to low via the active MP2 or MP3 and MP1 since the Disch signal is still low. Consequently, charge recovery concept occurs for every power-clock cycle to minimize the energy lost through charging or discharging.

2. 3 Investigation and Comparison of Individual Logic Implementation

The most important part for secure logic designing is input cell construction in CMOS logic functions. Inputs logic structure determines the dependence or independence of power consumption corresponding to inputs data that being processed. The comparison of supply current consumption by each adiabatic logic in this survey is shown in Fig. 7. The internal equivalent RC model of NAND/AND gate are shown in the top of Fig. 7; 2N-2N2P, ECRL and SAL employ universal pull-down network that remain some internal floating capacitors, consequently, they exhibit varying supply current traces for every power clock cycle. On the other hand, the SyAL and proposed CSSAL adopt charge sharing symmetric input logic style which enabling the circuits to consume constant and uniform supply current for all possible input transitions. The bottom of the Fig. 7 explains the representative input transition (A, B) from (0→1, 0→0) that at any input condition, our proposed CSSAL always shows same peak current as indicated in Fig. 7. The proposed CSSAL logic structure in [14] included control signal Cx pass-transistors, however in this survey, the Cx transistors are excluded because pass-transistors are energy consuming and trigger high glitch current in complex digital circuit, such as AES S-Box implementation.

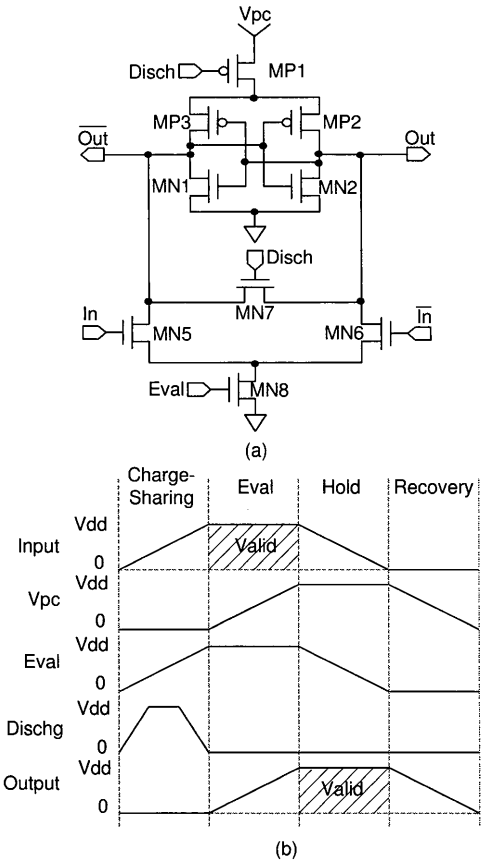

Fig. 6 Proposed CSSAL; (a) Inverter logic structure, (b) Timing diagram.

In order to demonstrate the features of CSSAL with other adiabatic logics, the bit parallel cellular multiplier over $GF(2^4)$ [15] as shown in Fig. 8, and the composite field $GF(((2^2)^2)^2)$ proposed by Satoh *et.al* [17] for AES S-box implementation in Fig. 9 are targeted.

3. Simulation Results of Adiabatic Logic Implementation

The results in this work are done in a SPICE simulation with 0.18-μm, 1.8-V standard CMOS process technology. The widths and the lengths of the transistors are 0.6 μm and 0.18 μm, respectively, for both the PMOS and NMOS transistors. We inversitagte all the adiabatic logics from the view-point of power fluctuation of individual logics, the logic

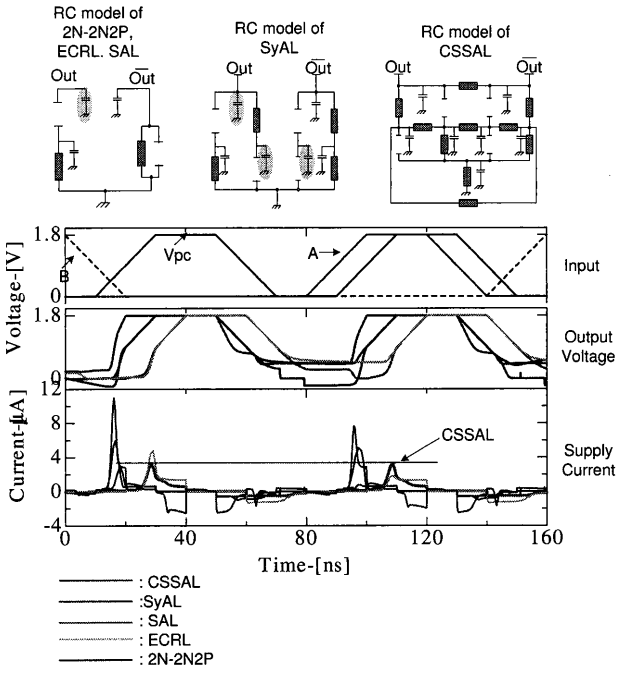

Fig. 7 Simulated transient response of AND/AND gate for input (A,B) transition from (0→1, 0→0) at 12.5 MHz clock frequency. The equivalent RC model in the top of this figure describes the floating capacitors during the input transition which is indicated by gray color in the background.

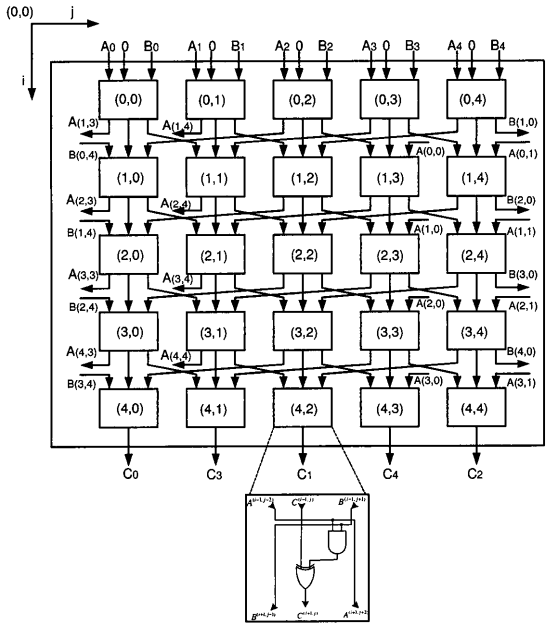

Fig. 8 Bit parallel cellular multiplier over $GF(2^4)$.

implementation in multiplier over $GF(2^4)$, and the AES S-Box under the same power clock frequency operation (12.5 MHz).

In the SPICE simulation, we derive the transitional power dissipation 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 simulation and calculation results are summarized in Table 1. The parameters in Table 1 describe

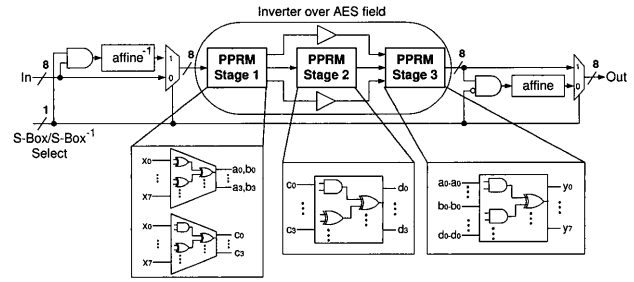

Fig. 9 AES S-Box under the multistage PPRM architecture.

the variation of energy dissipation and indicate how well the proposed logic and existing secure logics are able to consume power uniformly for every cycle. The normalized energy deviation (NED), defined as $(E_{max} - E_{min})/E_{max}$, is used to calculate the percentage difference between minimum and maximum energy consumption over all possible input transitions. The normalized standard deviation (NSD) indicates how much the energy consumption varies based on the input transitions, and is calculated as $\sigma_E/\overline{E}$. The quantity $\overline{E} = \sum_{i=1}^{n} E_i$ is the average of energy dissipation of 4-bit and 8-bit for $GF(2^4)$ and AES S-Box respectively. The standard deviation essentially reflects the variation of power consumption is defined as $\sigma_E = \sqrt{\sum_{i=E_1}^{E_n} (E_i - \overline{E})^2/n}$. The values of NED and NSD listed in Table 1 are to measure the ability of the logic circuit to resist against power analysis attacks. The smaller results of σ_E, NED and NSD, the high resistant of the logic towards SCA attacks are guaranteed. From this perspective, the results in Table 1 indicate that the CSSAL implementation in bit-parallel cellular multiplier over $GF(2^4)$ is better able to balance the energy consumption in comparison with the four other adiabatic logic. It has been documented in [14] that the individual logic security performance of proposed CSSAL increased about 98% compare to the SyAL. However, the logic implementation in more complex AES S-Box, the proposed CSSAL has a drawback in producing high glitch current because of the mismatching input arrival time. Therefore, the suitable input timing for 8-bit S-Box architecture need to be carefully revised in further work. Additional information provided in Table 1 that the SAL logic is not fully operated in S-Box using four phases in our investigation.

4. Conclusion

The investigation and comparison of secure adiabatic logic style for countermeasure against SCA attacks at cell level have been thoroughly carried out in this survey. DPA and DEMA attacks reveal the secret information by statistically analyzing the power fluctuations and the current amplitude of attacked hardware, such as smart card. The alternative solution for these challenges, the adiabatic logic technique

Table 1 Simulation and calculation results of the bit-parallel cellular multiplier over $GF(2^4)$ and S-box under multi-stage PPRM architecture at 12.5 MHz power clock frequency.

Power variation of cellular multiplier over $GF(2^4)$ and 8-bit S-Box

	Proposed		SyAL		SAL		2N-2N2P		ECRL	
	$GF(2^4)$	S-Box	$GF(2^4)$	S-Box	$GF(2^4)$	S-Box	$GF(2^4)$	S-Box	$GF(2^4)$	S-Box
E_{min} [fJ]	0.68	17.47	0.62	11.12	0.55	NA	0.21	3.73	0.19	2.87
E_{max} [fJ]	0.71	44.22	0.74	22.82	2.32	NA	1.24	33.97	0.97	24.19
$\overline{E}$ [fJ]	0.69	33.95	0.72	13.08	1.46	NA	0.78	19.47	0.62	13.82
σ_E [fJ]	0.007	6.92	0.031	0.92	0.55	NA	0.30	5.88	0.23	4.28
NED [%]	4.23	60.49	16.22	51.27	78.29	NA	83.06	89.02	80.41	88.14
NSD [%]	1.01	20.38	4.31	7.03	37.67	NA	38.46	30.20	37.10	30.96

is an interesting approach for reducing the information leakage caused by dynamic power, and high dynamic current in CMOS logic operation. The investigation results of low-power adiabatic logic styles have shown that the proposed CSSAL improves the security performance to withstand DPA attacks, and it is applicable for low power, low frequency band, such as contactless smart cards (13.56 MHz), RFID tags, and wireless sensors. We want to highlight in this conclusion that the suitable input timing for adiabatic logic implementation in large area of digital circuit need to be highly considered in order to avoid unnecessary electrical hazard or glitch current, which we put in account for further research work in respect to secure AES S-Box architecture implementation using proposed CSSAL logic.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Int. Advances in Cryptology Conference* (CRYPTO '99), Santa Barbara, CA, Aug. 15–19, 1999, pp. 388–397.

[2] P. Kocher, "Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other system," in *Proc. Advances in Cryptology* (Crypto'96), LNCS, vol. 1109, pp. 104–113, 1996.

[3] E. De Mulder, S B. Ors, B. Preneel, and I. Verbauwhede, "Differential electromagnetic attack on an FPGA implementation of elliptic curve cryptosystems," in *Proc. World Automation Congress* (WAC '06), Budapest, Hungary, July 24–26, 2006, pp. 1–6.

[4] A. Dehbaoui, S. Ordas, L. Torres, M. Robert, P. Maurine, "Implementation and efficiency evaluation of construction-based countermeasures against electromagnetic analysis," in *Proc. of Int. Conf. Design and Tech. of Integrated Systems in Nanoscale Era* (DTIS '11), Athens, Greece, April 4–8, pp. 1–6.

[5] 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. European Conf. Solid-State Circuits* (ESSCIRC '02), Firenze, Italy, 2002, Sept. 24–26, pp. 403–406.

[6] K. Tiri, I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Automation and Test in Europe Conf. and Exhibition*, pp. 246–251, 16-20 Feb. 2004.

[7] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. Workchop on Cryptographic Hardware and Embedded Systems* (CHES '06), Yokohama, Japan, Oct. 10–13, pp. 232–24.

[8] K.J. Kulikowski, V. Venkataraman, Z. Wang, A. Taubin, and M. Karpovsky, "Asynchronous balanced gates tolerant to interconnect variability," in *Proc. of Int. SympĊircuits and Syst.* (ISCAS '08), Seattle, WA, May 18–21, pp. 3190–3193.

[9] M. Khatir, and A. Moradi, "Secure adiabatic logic: A low-energy DPA-resistant logic style," *Cryptology ePrint Archive*, Report 2008/123, 2008. [Online] Available URL: http://eprint.iacr.org/2008/123

[10] Y. Moon and D.-K.Joeng, "An efficient charge recovery logic circuit", IEEE Journal on Solid-State Circuit, Vol.31, pp. 415-522, 1996

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

[12] A. Kramer, J. S. Denker, B. Flower and J. Moroney, "2nd order adiabatic computation 2N-2P and 2N-2N2P logic circuits," in *Proc. of Int. Symp. on Low Power Design*, pp. 191–196, New York, USA, 1995.

[13] 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 Syst.*, vol. 2, no. 4, pp. 398–406, Dec. 1994.

[14] C. Monteiro, Y. Takahashi, and T. Sekine, "A comparison of cellular multiplier cell using secure adiabatic logics," in *Proc. of Int. Conf. Circuit/System, Computers and Communications* (ITC-CSCC '12), 4pages (CD-ROM, ISBN: 978-4-88552-273–4), Sapporo, Japan, July 14–18, 2012.

[15] J. S. Lee, J. W. Lee, and Y. H. Kim, " Symmetric discharge logic against differetial power analysis", *IEACE Trans. Fundamentals*, vol.E90-A, no.1, Jan. 2007.

[16] C. -H. Liu, N. -F. Huang, and C. -Y. Lee, "Computation of AB^2 multiplier in $GF(2^m)$ using an efficient low-complexity cellular architecture," in *IEICE Trans. Fundamentals* vol. E83-A, no. 12, pp. 2657–2663, Dec. 2000.

[17] S. Morioka, A. Satoh, "An Optimized S-Box circuit architecture for low power AES design", in *Proc. of 4th Int'L Workshop on CHES'02* (LNCS), pp.172-186, Redwood Shores, CA, USA, Aug. 13-15, 2002.