Microelectronics Journal 44 (2013) 496–503

Contents lists available at SciVerse ScienceDirect

Microelectronics Journal

journal homepage: www.elsevier.com/locate/mejo

Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level

Câncio Monteiro [a,*], Yasuhiro Takahashi [b,**], Toshikazu Sekine [b,**]

[a] Graduate School of Engineering, Gifu University, Japan
[b] Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu-shi 501-1193, Japan

ARTICLE INFO

Article history:
Received 7 September 2012
Received in revised form
4 April 2013
Accepted 5 April 2013
Available online 2 May 2013

Keywords:
SCA
DPA
Adiabatic logic
Bit-parallel cellular array multiplier
AES
Smart card

ABSTRACT

Side-channel attacks by cryptanalysis are becoming a serious threat for cryptographers, who are designing systems that are more robust in terms of hardware and algorithm threats, aiming to thwart violations of the secrecy of securely processed information. As our contribution on a related issue, we propose a new secure logic, called charge-sharing symmetric adiabatic logic (CSSAL), for resistance against differential power analysis (DPA) attacks. We verify the security of the proposed CSSAL by carefully analyzing the individual logic functions corresponding to 16 possible dual-input transitions. Then, we compare the results with those of previous secure logic styles using the same parameters and under the same conditions. The figure of merit to measure the resistance of the logic against DPA attacks has been calculated from the variation in power consumption per input transition. The SPICE simulation results show that our proposed logic balances the peak current traces for all input logic transitions, consuming power uniformly over every cycle, and thus making the input–output data resilient to a DPA attack. Moreover, the ability of the proposed CSSAL in a bit-parallel cellular multiplier over $GF(2^m)$ shows its significant power reduction compared to conventional secure logic styles and its efficient resistance to DPA attacks.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

Side-channel analysis (SCA) attacks have become a special threat for cipher 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. Examples of side-channel attacks are attacks based upon sound, infrared radiation, time delays, simple or differential power analysis (SPA/DPA), and simple or differential electromagnetic analysis (SEMA/DEMA). The timing attacks documented by Kocher in 1996 [1] demonstrated how measuring computation time can reveal vital information about secret keys. The method of a power analysis attack involves probing device for physical measurements of its current consumption with respect to execution time. We consider a power analysis an effective attack for revealing the secret key of a smart card by statistically analyzing power fluctuations that occur while the device encrypts and decrypts large blocks of data [2]. Apart from the side-channel attack techniques described in [1,2], the electromagnetic radiation attacks in [3–7] have been extensively studied. DEMA attacks can reveal secret information because current flow during the switching of the CMOS gates causes a variation of the surrounding electromagnetic field that can be monitored by positioning an inductive probe around the microcontroller chip. Careful analyses for power and electromagnetic leakage at CMOS level have been described in [5]. From a perspective of security, neither the static nor differential logic style is able to avoid information leakage, because an attack based on the Hamming distance model is always possible, since the transitions 0–1 and 1–0 dissipate power, while the transitions 0–0 and 1–1 do not. Moreover, an attack on the dynamic logic style also is always possible based on the Hamming weight model, since the transition 0–1 or 1–1 dissipates power during the pre-charge phase while the transition 1–0 or 0–0 does not.

We emphasize in this paper that the fundamental issue of power analysis attacks on smart cards is closely related to the electrical power consumption of endpoint hardware. Therefore, a logic designed to hide or mask the data being processed should be considered. Numerous studies on hiding intermediate values at cell level have been published, but most of these employed a conventional CMOS logic style, which means the devices are still susceptible to DPA and DEMA attacks because of their energy consumption. Over the last few years, there have been several reports pertaining to cell-level uses of dual-rail (DR) pre-charged logic, such as sense-amplifier-based logic (SABL) and its implementations [8–10], where the input logic structure is designed to balance all internal node capacitances for constant power consumption under all input conditions and for every clock cycle. The simple or wave dynamic differential logic (SDDL/WDDL) [11] was designed, which achieves an important reduction in

[*] Corresponding author. Tel.: + 81 58 293 2692.
[**] Principal corresponding authors.
E-mail addresses: canciotimor@gmail.com (C. Monteiro), yasut@gifu-u.ac.jp (Y. Takahashi), sekine@gifu-u.ac.jp (T. Sekine).

0026-2692/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.mejo.2013.04.003

the power variation for both ASIC and FPGA, but their drawback are the increased area, computation time, and power consumption. An enhanced SABL was developed into the well-known three-phase dual-rail pre-charge logic (TDPL) [12] to unbalance load conditions, thus allowing a semi-custom design flow without any constraint on the routing of the complementary wire. Moreover, an asynchronous dual-rail gate design has been proposed [13] that balances power, requires no capacitance matching of data outputs, and tolerates process variability in the routed interconnect between gates. Additional work on the masking approach [14] was proposed for randomizing intermediate values that are processed by cryptographic devices, but this method is the most widely applied at algorithmic level. Although the existing logic techniques have been successfully implemented, all of the real crypto-devices were designed in the conventional CMOS logic style, which means that they are highly power consuming and have detectable supply current peaks that make the system vulnerable to a practical measurement of power and electromagnetic analysis.

Power management has become a general concern in modern society; consequently, power consumption by cryptographic hardware needs to be addressed for reason of both security and efficiency, especially for battery-powered embedded systems. Adiabatic low-power solutions for digital circuitry were introduced in [15], which is our motivation for designing secure low-power circuits and systems. The secure single-rail (SR) adiabatic logic style was described in [16,17]; however, a thorough analysis accomplished in [18] proved that SR logics are data dependent and vulnerable to DPA attacks. Moreover, a secure low-energy DR logic style called secure adiabatic logic (SAL) [19] and security evaluation of 2N–2N2P adiabatic logic [20] have been reported. However, careful analysis in our work has shown that SAL and 2N–2N2P logic still exhibit supply current dependences that render these vulnerable, since their input logic structures are implemented in the universal DR logic style. Our endeavor in this paper is to design a new secure logic for counteracting side-channel attacks limited to cell level and then investigate that logic in a SPICE simulation. The proposed charge-sharing symmetric adiabatic logic (CSSAL) is implemented with a charge-sharing symmetric input logic structure in symmetric adiabatic logic (SyAL) circuits set against differential power analysis [21].

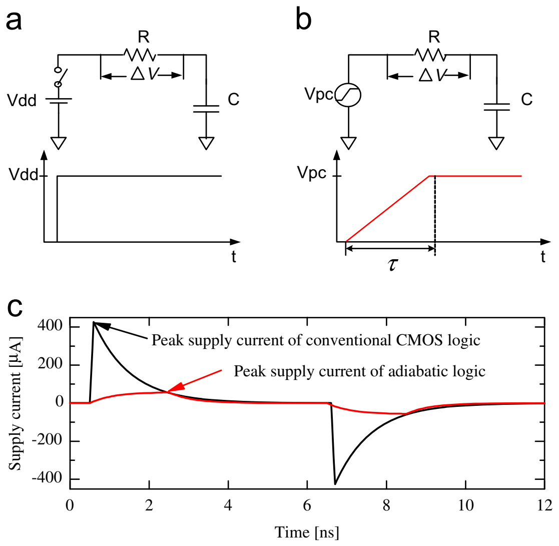

Fig. 1. Comparison of supply currents for equivalent RC models of CMOS logic ((a) step voltage(τ=0)) and adiabatic logic ((b) ramped step voltage). (c) The peak supply current of adiabatic logic is significantly lower than the conventional CMOS logic under the same parameters and conditions.

The rest of this paper is organized as follows. Section 2 compares the conventional CMOS logic with the adiabatic logic technique. Section 3 discusses the proposed logic structures. Section 4 briefly reviews implementation of the proposed logic. Sections 5 and 6, respectively, present and discuss the simulation results. Finally, Section 7 concludes this paper.

2. Adiabatic 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 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

$$E_{charge} = \tfrac{1}{2}CV_{dd}^2. \tag{1}$$

From the perspective of energy conservation, a conventional CMOS logic emits heat and thus wastes energy with every charge–discharge cycle:

$$\begin{aligned} E_{total} &= E_{charge} + E_{discharge} \\ &= \tfrac{1}{2}CV_{dd}^2 + \tfrac{1}{2}CV_{dd}^2 \\ &= CV_{dd}^2. \end{aligned} \tag{2}$$

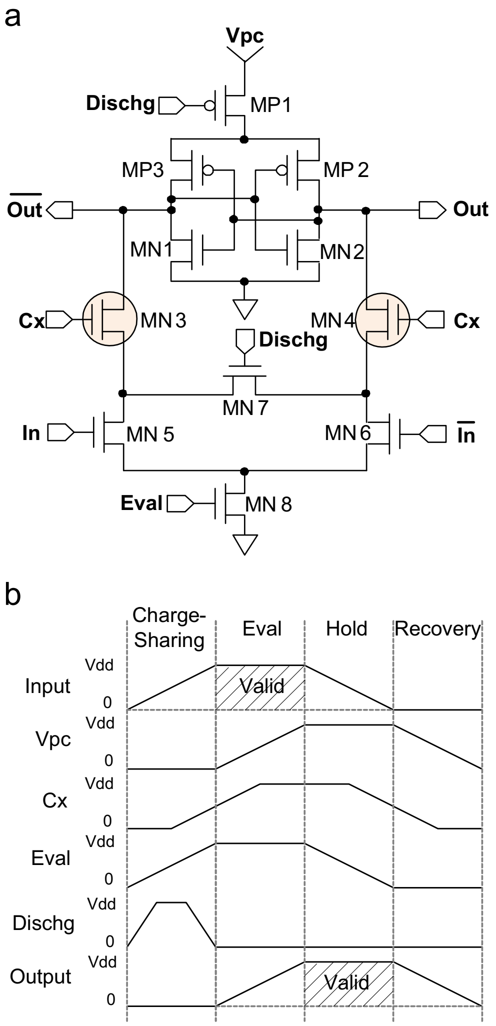

Fig. 2. Proposed CSSAL logic: (a) inverter logic structure and (b) input and output signals of proposed CSSAL inverter logic.

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

$$\begin{aligned} P_{total} &= \frac{E_{total}}{T} \\ &= CV_{dd}^2 f. \end{aligned} \tag{3}$$

Observing that the 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 C.

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

$$\begin{aligned} E_{Adiabatic} &= \xi P\tau = \xi I^2 R\tau \\ &= \xi \left(\frac{CV_{dd}}{\tau}\right)^2 R\tau, \end{aligned} \tag{4}$$

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 [15]. We assume that, if the individual logics, such as AND and XOR are able to consume an uniform and low-peak supply current, regardless of the input logic conditions, then, their implementation in 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). Fig. 1 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.

3. Secure charge-sharing symmetric adiabatic logic

3.1. Logic structure

The proposed CSSAL inverter is depicted in Fig. 2(a), while its input and output signals are shown in Fig. 2(b). As shown in Fig. 2(b), the CSSAL operates in four phases:

1. *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.
2. *Evaluation*: In this *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

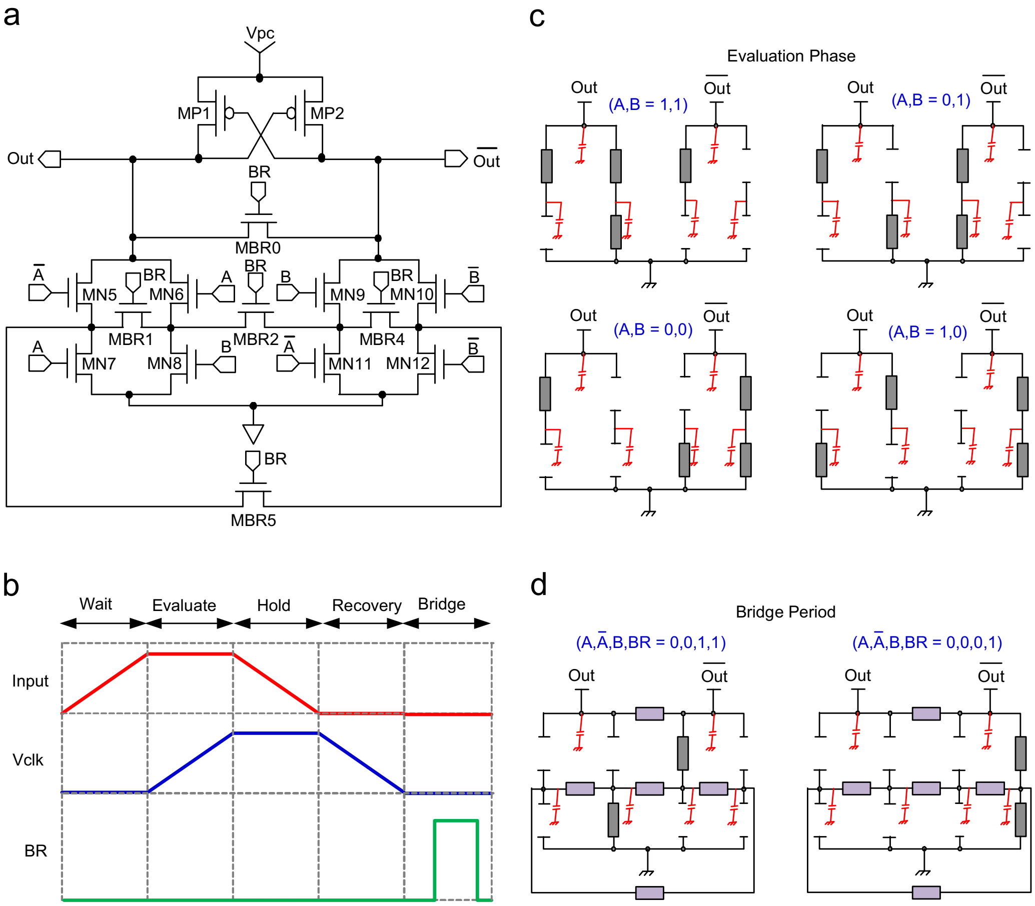

Fig. 3. (a) SyAL NAND/AND logic schematic. (b) Timing diagram of SyAL ver.2 [22]. (c) Equivalent RC models of internal nodes during evaluation phase. (d) Equivalent RC models during bridge period.

through one of the active input cells and *Cx* transistors that are already at a high level.

3. *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.
4. *Recovery*: The power clock voltage (V_{pc}) is 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.

3.2. Analysis of proposed logic

The proposed CSSAL is an enhancement of the SyAL form of the symmetric input logic style. The SyAL is one of the latest secure DR logic styles using adiabatic principles to equalize the voltage between the output nodes and applied charge-sharing techniques to reduce the data dependences. A comparison given in [21] shows that SyAL ver.2 provides a consistent peak current for all input transitions. However, charge-sharing between the internal node capacitances occurs during the bridge phase, in which both the input and its complementary signals are low for the inverter logic, as depicted in Fig. 3(b), and exhibit output node voltage equalization. In the case of a dual-input logic construction, as shown in the schematic diagram of SyAL, ver. 2, unbalanced charging and discharging occur during the evaluation phase and bridge phase. Hence, the input data remain dependent in SyAL ver.2, according to our comparison of results. For a better comparative study, diagrams of the equivalent RC models of the internal node connections of SyAL ver. 2 are shown in Fig. 3(c), where the evaluation phase diagram obtains according to the conditions of inputs *A* and *B* excluding the *BR* signal. Moreover, the bridge phase diagram in Fig. 3(d) obtains when the *BR* signal is in a high condition that coincides with input *B* or its complementary signal.

A transistor schematic of the NAND/AND logic of the CSSAL is depicted in Fig. 4(a). The logic structure of the XNOR/XOR is the same as that of the NAND/AND schematic, except that the positions of the input signals are different. The internal node capacitances during the active charge-sharing phase are shown in Fig. 4(b) for four representative input transitions of the NAND/AND logic function. This RC diagram obtains when the *Disch* signal is high in the charge-sharing phase. In the next evaluation phase, the logic function is evaluated the same as for the RC diagram in Fig. 3(c). However, in contrast with SyAL, our proposed logic starts by setting all internal node capacitances to ground level when the input signal is such that $VIn/V\overline{In} \geqq V_{THN}$ before the power-clock signal arrives. This makes our proposed logic balance low-peak supply current transitions, which is the unique different from SyAL, and is the idea behind the name charge-sharing symmetric adiabatic logic. Additionally, we adopt in our proposed logic the cross-couple latch circuit of the 2N–2N2P [22] that was designed primarily for low power applications, not security. Conversely, SyAL was designed using the simplest DR adiabatic logic, called ECRL [23], with the potential for power efficiency. Essentially, the logic functions of ECRL and 2N–2N2P logic are identical. However, the outputs of ECRL are fully controlled by input rails, whereas the 2N–2N2P logic outputs are controlled by both input rails and grounded cross-coupled CMOS latches. Consequently, during logic evaluation, the 2N–2N2P demonstrated a non-floating data output that remained valid and stable despite unexpected input changes. A report on DPA-resistance of charge recovery logics [20] stated that use of the 2N–2N2P logic style leads to an improvement in DPA-resistance and at the same time reduces the energy consumption, which makes this especially suitable for pervasive devices. However, our analysis at cell level proves that by adopting the universal DR NAND/AND input logic style, in contrast to TDPL style, the information leakage still exists when input states are flipped.

4. Implementation of logic in finite field over $GF(2^m)$

Galois field (GF) arithmetic has an important role in coding theory and cryptographic algorithms. An efficient algorithm for both hardware and software implementations was standardized by the NIST in 2001 as the Advanced Encryption Standard (AES) [24], which operates over $GF(2^8)$ for computational efficiency, high

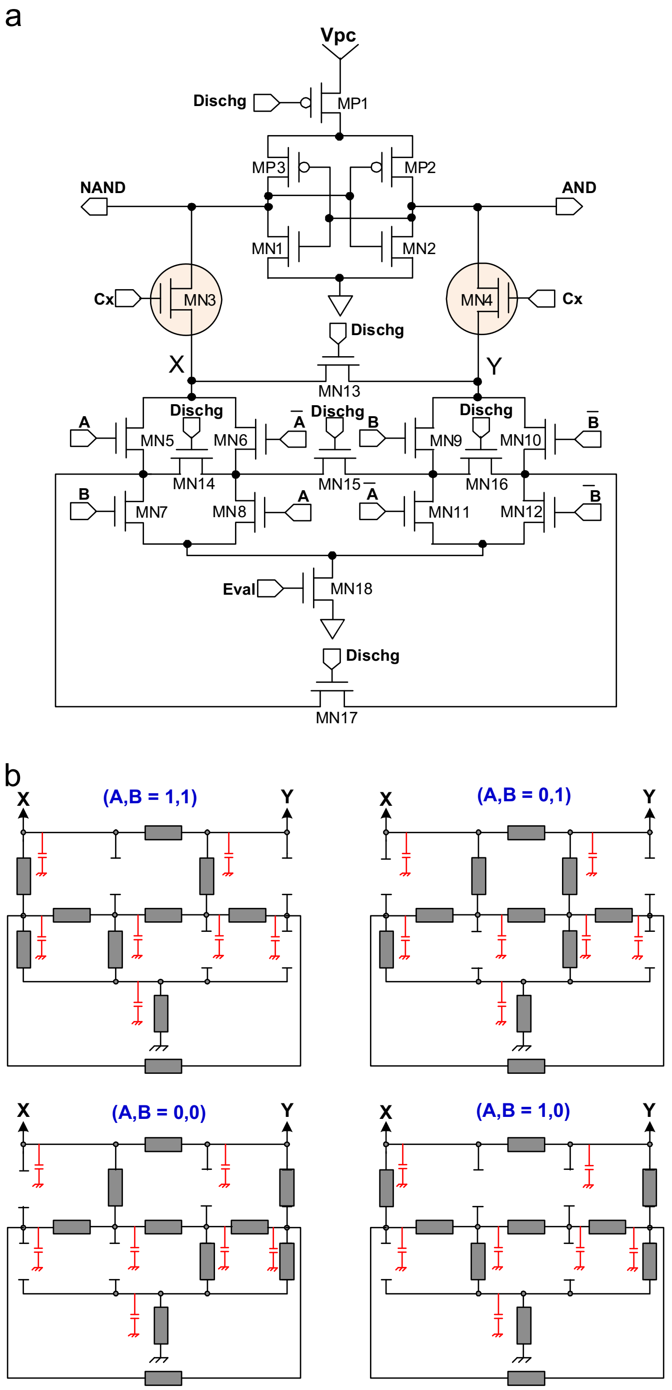

Fig. 4. Logic structure. (a) NAND/AND logic of proposed CSSAL. (b) Equivalent RC models during evaluation phase of NAND/AND logic function of proposed CSSAL.

resistance to cryptanalysis, hardware and software compatibility, and flexibility. Since the new AES standard was announced, much effort has been expanded [25–31] to simplify the finite field over $GF(2^8)$ in S-Box transformation to $GF((2^4)^2)$ and $GF(((2^2)^2)^2)$ for low cost, low power consumption, and low complexity.

In order to verify the capability of our proposed CSSAL for counteracting DPA attacks, we implement the individual logics with the existing bit-parallel cellular multiplier in [32], which analytically explored the inner product multiplication algorithm for calculating AB^2 in a class field $GF(2^m)$ using a cellular architecture that involves low-complexity and less computation time. In the case of $m=4$, arithmetic calculations have been performed to define the cellular array multiplication of $AB^2=\sum_{j=0}^{m} A^{(2j)}[B^2]^{(-j)}$ to calculate the function block of the bit-parallel multiplier over $GF(2^4)$. The inputs and outputs of the inner cell structures are cyclically shifted with respect to one another to construct a low-complexity cellular architecture as depicted in Fig. 5. The cellular architecture in Fig. 5 is such that the configuration of each inner-product multiplication is divided into $m+1$ basic cells, so the complexity includes one dual-input AND gate, one dual-input XOR gate, and $AB+C$ operations. The designed structure of the cellular multiplier includes $(m+1)^2$ cells and each requires computation time $T_{AND}+T_{XOR}$.

5. Simulations and results

5.1. Simulation conditions

To evaluate the power traces of the secure adiabatic logic, the individual logics and the bit-parallel cellular multiplier over $GF(2^4)$ using the A-cell circuit in [32] are evaluated in a SPICE simulation with $0.18-\mu$m, 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. To validate our proposal, we repeat the simulation and compare the SAL, SyAL, and TDPL for NAND/AND gates and XNOR/XOR gates at the same input operating frequencies. In the SPICE simulations, the conditions for the secure adiabatic logic styles are that all power supplies are trapezoidal waveforms and the power-clock frequency varies from 1.25 MHz to 12.5 MHz and 125 MHz for all adiabatic logics investigated. The investigation concentrates on individual AND and XOR logics, because those have been widely deployed in AES hardware architectures and AES algorithms, for addition and multiplication over secure S-box structure designs. We investigate not only the peak supply current transition for 16 possible dual-input transitions but also the energy consumed when input data are flipped.

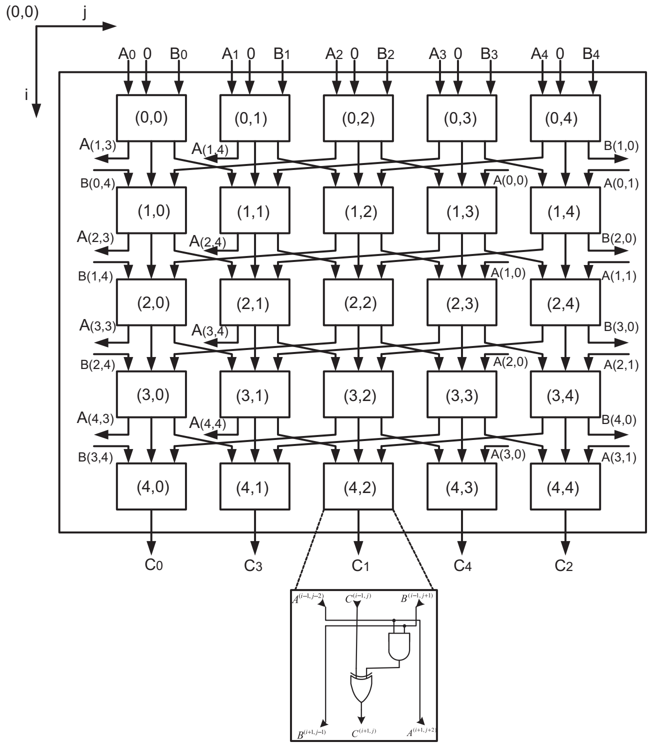

Fig. 5. Bit-parallel cellular multiplier over $GF(2^4)$.

5.2. Results

The simulation result of output voltage is depicted in Fig. 6(a) and (b) for the CSSAL multiplier and the TDPL multiplier, respectively. The TDPL logic was implemented using pre-charged logic style; hence, the pre-charged signals at the complementary L (low) voltage is appeared as H (high); however, in comparing to CSSAL, we consider them as Low level, which is indicated as L and H on the top of the TDPL Out(C0).

The simulation results of the individual logics evaluated (AND, XOR) and their implementations in bit-parallel cellular multipliers over $GF(2^4)$ are summarized in Table 1. In the SPICE simulations 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. We show the transitional supply currents traces of I_{pc} (I_{dd}) in Fig. 7, and below we analyze the peak current traces of each circuit for three different frequencies to scrutinize the merit of the logic in terms of power efficiency, the ability of the logic to resist SCA attacks, and speed for hardware compatibility.

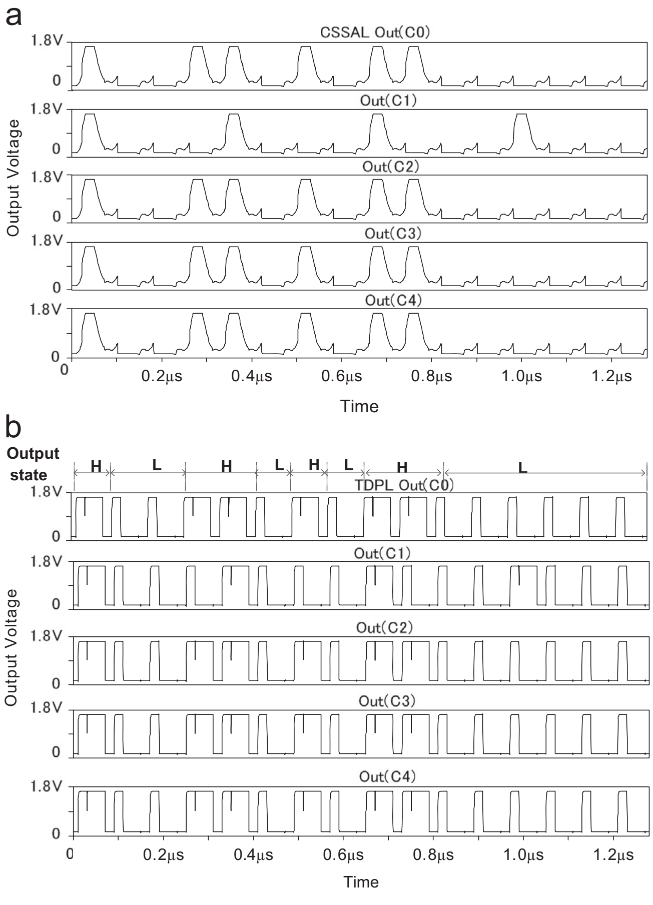

Fig. 6. Output voltage of the bit-parallel cellular multiplier over $GF(2^4)$: (a) CSSAL and (b) TDPL.

Table 1
Simulation and calculation results of AND and XOR individual logics, and their application in bit-parallel cellular multiplier over $GF(2^4)$ at different operating frequencies. Note: There are no data for SAL logic in cellular multiplier over $GF(2^4)$ at 125 MHz power clock frequency, because SAL was not working by using half of original eight-phases at high frequency by our SPICE simulation result.

Freq. (MHz)	SAL			SyAL			Proposed			TDPL		
	1.25	12.5	125	1.25	12.5	125	1.25	12.5	125	1.25	12.5	125
Individual NADN/AND logic												
E_{min} (fJ)	5.23	7.43	15.21	9.03	0.73	13.53	19.79	21.45	16.65	128.08	121.77	119.77
E_{max} (fJ)	12.13	12.09	21.78	20.14	19.66	24.20	20.07	21.70	21.47	134.82	124.39	125.29
$\overline{E}$ (fJ)	6.36	8.60	17.50	12.39	12.78	18.48	19.92	21.59	19.48	130.77	124.39	121.97
σ_E (fJ)	1.55	1.11	1.85	3.83	2.98	3.45	0.08	0.09	1.48	2.17	0.57	1.69
NED (%)	56.99	38.51	30.17	55.18	50.46	44.08	1.39	1.15	22.45	4.99	2.11	4.41
NSD (%)	24.23	12.85	10.56	30.94	23.32	18.68	0.44	0.42	7.59	1.66	0.46	1.39
Individual XNOR/XOR logic												
E_{min} (fJ)	5.38	8.95	21.11	5.32	6.77	12.96	19.80	21.59	16.65	142.86	127.26	132.39
E_{max} (fJ)	8.12	12.22	29.49	12.79	13.27	20.11	20.09	21.79	19.84	143.79	128.14	132.77
$\overline{E}$ (fJ)	6.86	10.74	25.74	9.58	10.20	9.58	19.92	21.68	18.87	143.33	127.74	132.63
σ_E (fJ)	1.07	1.35	3.20	2.75	2.59	2.49	0.10	0.07	1.29	0.33	0.36	0.15
NED (%)	33.78	26.78	28.43	58.39	48.98	35.33	1.38	0.92	16.09	0.65	0.69	0.29
NSD (%)	15.63	12.57	12.43	28.70	25.39	18.37	0.52	0.32	6.86	0.23	0.28	0.11
Cellular multiplier over $GF(2^4)$												
E_{min} (fJ)	228.41	337.15	–	262.85	311.64	526.88	219.73	310.28	583.11	8037.03	3957.84	3411.61
E_{max} (fJ)	361.28	682.92	–	381.05	418.25	645.19	279.37	350.74	766.92	8196.84	4112.35	3549.57
$\overline{E}$ (fJ)	284.31	506.78	–	336.50	382.02	614.79	260.24	333.86	715.62	8118.16	4042.54	3496.50
σ_E (fJ)	37.79	85.42	–	32.07	31.02	32.19	15.42	11.15	43.73	38.73	40.77	38.73
NED (%)	36.78	50.63	–	31.02	25.49	18.34	21.35	11.54	23.97	1.95	3.76	3.89
NSD (%)	13.29	18.83	–	9.53	8.12	5.24	5.92	3.32	7.10	0.48	1.01	1.11

The parameters in Table 1 provide an alternative method for comparing DPA resistance without a full DES/AES implementation. They describe 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 parameter of 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) proposed by Bucci et al. [12] indicates how much the energy consumption varies based on the inputs and is calculated as $\sigma_E/\overline{E}$. The quantity $\overline{E}$ is the average of energy dissipation for the 16 possible input transitions, and the standard deviation that indicates variation of energy dissipation is defined as $\sigma_E=\sqrt{\sum_{i=E_1}^{E_n}(E_i-\overline{E})^2/n}$. The calculated 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 NED and NSD results indicate that the individual logics and the bit-parallel cellular multiplier over $GF(2^4)$ using the proposed CSSAL circuit are better able to balance the energy consumption in comparison with the SAL and SyAL. Moreover, in comparison with the well-known conventional TDPL, the proposed individual logics exhibit a similar ability to thwart the DPA attack technique; however, the proposed CSSAL consumes significantly less power in the low-frequency band.

Apart from the logic ability for resistance against SCA attacks, the power reduction is also one of the research targets. It is obviously described by the graphical information in Fig. 8 that our proposed CSSAL multiplier has significant energy reduction about a 12 times lower than that of the TDPL logic.

6. Discussion

We have employed several techniques in our work, such as (1) adiabatic logic technique to achieve low power consumption and low peak current, (2) dual-rail logic style to establish uniform transitional supply peak current, and (3) symmetric pull-down network transistors with charge-sharing technique which construct a constant internal equivalent RC model for all input condition to reduce current-to-data dependency.

Accordingly, we affirm that the most important part in our logic designing is the construction of the input logic cells in the CSSAL logic structure. The structure of the input transistors in the CSSAL determine independence of the power consumption with respect to input data that are being processed. Moreover, extra complementary signals in secure logic designs also help to achieve concealment of input data at cell level. Therefore, we insert control signal (C_x) pass transistors into the CSSAL structure as indicated in Fig. 2(a) or Fig. 4(a). The main role of the C_x pass transistors is to maintain the stability of the output during the charge-sharing phase, as explained in the previous section. They also enable our proposed logic to consume the same amount of energy for all possible transitions. However, the disadvantage of these pass transistors is high-energy consumption. For example, the CSSAL $GF(2^4)$ at 12.5-MHz power-clock frequency with C_x transistors has $E_{diss}=13.02$ pJ/cycle. However, without the C_x pass transistors the CSSAL has $E_{diss}=5.36$ pJ/cycle, which is about 12% less than for SyAL (E_{diss}=6.11 pJ/cycle), 44.13% less than for SAL (E_{diss}=7.74 pJ/cycle), and 12 times less than for TDPL logic (E_{diss}=64.71 pJ/cycle).

It is important to note that applying extra pass transistors in the logic construction of a more complex digital circuit (e.g., a multiplier) may affect the electric hazard (glitch)[1] of a spike voltage occurrence when the logic state is stable at a low or high level, as has been extensively analyzed in [33–35]. Careful analysis of simulations and physical measurements [34] has shown that both unmasked and masked implementations leak side-channel information due to glitches at the outputs of logic gates. Furthermore, we found out that this glitch current phenomenon in our SPICE simulation results when C_x transistors were inserted

[1] Glitches are logic gate switching operations that are caused by timing properties of gates and by interconnection delays. Glitches occur in every CMOS circuit. Consequently, the existing schemes for masking CMOS gates do not prevent DPA attacks [34].

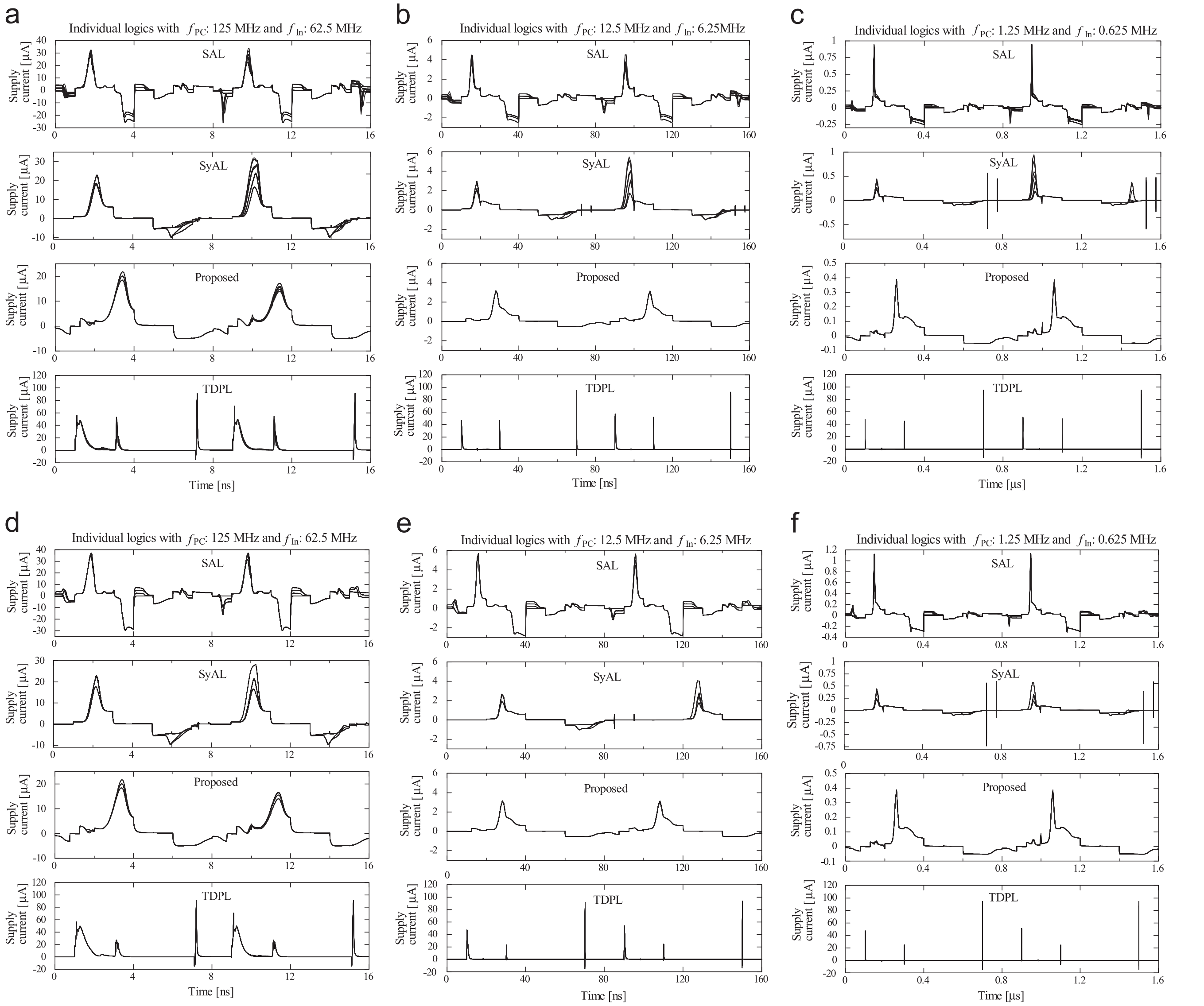

Fig. 7. Supply current transitions of individual logics at different frequencies. (a) 125 MHz AND gate. (b) 12.5 MHz AND gate. (c) 1.25 MHz AND gate. (d) 125 MHz XOR gate. (e) 12.5 MHz XOR gate. (f) 1.25 MHz XOR gate.

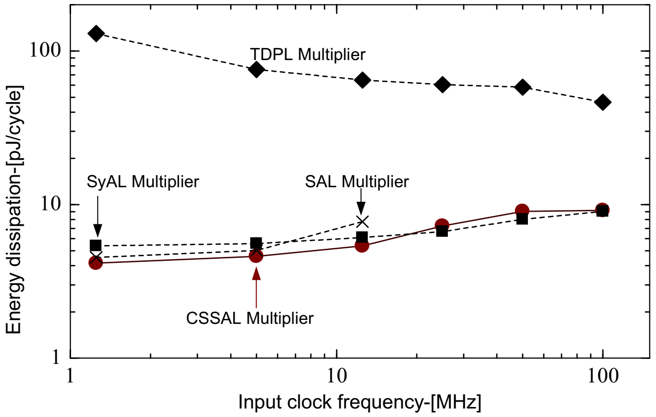

Fig. 8. Simulated energy dissipation comparison of the bit-parallel cellular multiplier over $GF(2^4)$ in respect to the different input clock frequencies.

into the CSSAL in a bit-parallel cellular multiplier over $GF(2^4)$. Therefore, the application of the CSSAL to further work on implementations of the AES hardware architecture, the control signal C_x pass transistors in Fig. 4(a) is considered as conditional transistors. In addition, it is important to acknowledge that the drawback of our proposed CSSAL logic is in increasing the gate numbers, which will be an area consuming for further full-custom layout design.

Fig. 7 shows current trances of all 16 possible dual-input transitions for AND (Fig. 7(a)–(c)) and XOR (Fig. 7(d)–(f)) at operating frequencies of 1.25 MHz, 12.5 MHz, and 125 MHz for all logics investigated. As clearly indicated in Fig. 7, the proposed individual logics yield only a single plot for all 16 data, and the peak supply current is lower than those of the other logic styles in the low-frequency band (i.e. at 12.5 MHz or 1.25 MHz).

An important parameters of NED and NSD explain that the consumed energy is more constant for different transition if we achieve more small values. These properties somehow, not very accurate comparative data, if the variance of mean ($\overline{E}$) are extremely different, such as the one of the CSSAL and TDPL in Table 1. Therefore, an additional evidence in Table 1 proves that the variation of the energy dissipation of the proposed logic has low values of σ_E at low frequencies (1.25 MHz or 12.5 MHz), which assures us that our proposed CSSAL is suitable for low-power and low-frequency applications, such as contactless smart cards (13.56 MHz), RFID tags, and wireless sensors.

7. Conclusion

We have proposed a new secure logic style that is based on the adiabatic switching principle. A comparative study on the ability of this logic as one alternative method to thwart a power analysis attack at cell level has been thoroughly carried out in a SPICE simulation. The optimum results of the individual logics and their implementation in the inner-cell bit-parallel multiplier over $GF(2^4)$ show that the proposed logic consumes energy uniformly over every input transition, lowers peak supply current traces, and significantly reduces power consumption in the bit-parallel cellular multiplier over $GF(2^4)$. Based on these typical results, we deduce that our proposed CSSAL is a suitable candidate for secure hardware in low-power and low-frequency applications, such as contactless smart cards (13.56 MHz), RFID tags, and wireless sensors.

Acknowledgment

The custom circuits discussed in this paper have been simulated with 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.

References

[1] P. Kocher, Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other system, in: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, 1996, pp. 104–113.

[2] P.C. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Proceedings of 19th International Advances in Cryptology Conference (CRYPTO'99), 1999, pp. 388–397.

[3] E. De Mulder, S.B. Ors, B. Preneel, I. Verbauwhede, Differential electromagnetic attack on an FPGA implementation of elliptic curve cryptosystems, in: Proceedings of World Automation Congress (WAC'06), 2006, pp. 1–6.

[4] H. Li, A.T. Markettos, S. Moore, Security evaluation against electromagnetic analysis at design time, in: Proceedings of 10th IEEE International on High-Level Design Validation and Test Workshop, 2005, pp. 211–218.

[5] A. Dehbaoui, S. Ordas, L. Torres, M. Robert, P. Maurine, Implementation and efficiency evaluation of construction-based countermeasures against electromagnetic analysis, in: Proceedings of 6th IEEE International Conference on Design and Technology of Integrated Systems in Nanoscale Era, 2011, pp. 1–6.

[6] V. Lomná, A. Dehbaoui, T. Ordas, P. Maurine, L. Torres, M. Robert, R. Soares, N. Calazans, F. Moraes, Secure triple track logic robustness against differential power and electromagnetic analyses, J. Integr. Circuits Syst. 4 (1) (2009) 20–28.

[7] S. Guilley, L. Sauvage, J.-L. Danger, N. Selmane, R. Pacalet, Silicon-level solution to counteract passive and active attacks, in: Proceedings of Fifth Workshop on Fault Diagnosis and Tolerance in Cryptography, 2008, pp. 3–17.

[8] K. Tiri, M. Akmal, I. Verbauwhede, A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards, in: Proceedings of 28th European Conference on Solid-State Circuits (ESSCIRC'02), 2002, pp. 403–406.

[9] K. Tiri, I. Verbauwhede, Securing encryption algorithms against DPA at the logic level: next generation smart card technology, in: Proceedings of Cryptographic Hardware and Embedded Systems (CHES), 2003, pp. 125–136.

[10] K. Tiri, I. Verbauwhede, Charge recycling sense amplifier based logic: securing low power security IC's against DPA, in: Proceedings of ESSCIRC'04, 2004, pp. 179–182.

[11] K. Tiri, I. Verbauwhede, A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation, in: Proceedings of Design, Automation and Test in Europe Conference and Exhibition, 2004, pp. 246–251.

[12] M. Bucci, L. Giancane, R. Luzzi, A. Trifiletti, Three-phase dual-rail pre-charge logic, in: Proceedings of CHES'06, 2006, pp. 232–241.

[13] K.J. Kulikowski, V. Venkataraman, Z. Wang, A. Taubin, M. Karpovsky, Asyncronous balanced gates tolerant to interconnet variability, in: Proceedings of International Symposium on Circuits and Systems (ISCAS), 2008, pp. 3190–3193.

[14] T. Popp, S. Mangard, Masked dual-rail pre-charge logic: DPA-resistance without routing constraints, in: Proceedings of CHES'05, 2005, pp. 172–186.

[15] W.C. Athas, L.J. Svesson, J.G. Koller, N. Traztzanis, E.Y.-C. Chuo, Low power digital system based on adiabatic-switching principles, IEEE Trans. VLSI Syst. 2 (4) (1994) 398–406.

[16] K.-K. Mok, et al., Adiabatic smart card, in: Proceedings of IEEE Asia Pacific Conference on Circuit and Systems (APCCAS), 2006, pp. 287–290.

[17] K.-K. Mok, C.-F. Chan, A 13.56 MHz adiabatic smart card/RFID, in: Proceedings of IEEE ASICON'07, 2007, pp. 874–877.

[18] C. Monteiro, Y. Takahashi, T. Sekine, Resistance against power analysis attacks on adiabatic dynamic and adiabatic differential logics for smart card, in: Proceedings of the IEEE Intelligent Signal Processing and Communication System (ISPACS'11), 2011, pp. 1–5.

[19] M. Khatir, A. Moradi, Secure adiabatic logic: a low-energy DPA-resistant logic style, in: IACR Cryptology ePrint Archive, Report 2008/123. Available from: (〈http://eprint.iacr.org/2008/123〉).

[20] A. Moradi, M. Khatir, M. Salmasizadeh, M.T.M. Shalmani, Investigating the DPA-resistance property of charge recovery logics, in: IACR ePrint Archive, 2008, pp. 192–192. Available from: (〈http://eprint.iacr.org/2008/192.pdf〉).

[21] B.-D. Choi, K.E. Kim, K-S. Chung, D.K. Kim, Symmetric adiabatic logic circuits against differential power analysis, ETRI J. 32 (1) (2010) 166–168.

[22] A. Kramer, J.S. Denker, B. Flower, J. Moroney, 2nd order adiabatic computation 2N-2P and 2N-2N2P logic circuits, in: Proceedings of the IEEE International Symposium on Low Power Design, 1995, pp. 191–196.

[23] Y. Moon, D.K. Jeong, An efficient charge recovery logic circuit, IEEE J. Solid-State Circuits 31 (4) (1996) 514–522.

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

[25] A. Satoh, S. Morioka, K. Takano, S. Munetoh, A compact Rijndael Hardware architecture with S-Box optimization, in: Proceedings of the Advances in Cryptology—ASIACRYPT'01, 2001, pp. 239–254.

[26] S. Morioka, A. Satoh, An optimized S-Box circuit architecture for low power AES design, in: Proceedings of 4th International Workshop on CHES'03, 2003, pp. 172–186.

[27] H.-S. Kim, K.-Y. Yoo, Multiplier for public-key cryptosystem based on cellular automata, in: Computer Network Security, Lecture Notes in Computer Science, vol. 2776/2003, 2003, pp. 436–439.

[28] J.-H. Chen, S.-J. Huang, W.-C. Lin, Y.-K. Lu, M.-D. Shieh, Exploration of low-cost configurable S-Box designs for AES applications, in: Proceedings of International Conference on Embedded Software and Systems (ICESS), 2008, pp. 422–428.

[29] P.V.S. Shastry, A. Agnihotri, D. Kachhwaha, J. Singh, A combinational logic implementation of S-box of AES, in: Proceedings of IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), 2011, pp. 1–4.

[30] S. Talapatra, H. Rahaman, J. Mathew, Low complexity digit serial systolic montgomery multipliers for special class of GF(2^m), IEEE Trans. VLSI Syst. 18 (5) (2010) 847–852.

[31] W. Yi, J. Li, R. Li, W. Zhao, FPGA based optimization for masked AES implementation, in: IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS), 2011, pp. 1–4.

[32] C.-H. Liu, N.-F. Huang, C.-Y. Lee, Computation of AB^2 multiplier in $GF(2^m)$ using an efficient low-complexity cellular architecture, IEICE Trans. Fundam. E-83A (12) (2000) 2657–2663.

[33] S. Mangard, N. Pramstaller, E. Oswald, Successfully attacking masked AES hardware implementations, in: Proceedings of CHES, 2005, pp. 157–171.

[34] S. Mangard, T. Popp, B.M. Gammel, Side-channel leakage of masked CMOS gates, in: International Conference on Topics in Cryptology–CT-RSA, Lecture Notes in Computer Science, 2005, pp. 351–365.

[35] S. Nikova, V. Rijmen, M. Schlaffer, Secure hardware implementation of non-linear functions in the presence of glitches, J. Cryptol. 24 (2) (2011) 292–321.