# Resistance Against Power Analysis Attacks on Adiabatic Dynamic and Adiabatic Differential Logics for Smart Card

Cancio Monteiro
Graduate School of Engineering
Gifu University, 1-1 Yanagido,
Gifu-shi, 501-1193, Japan
Email: p3124010@edu.gifu-u.ac.jp

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

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

***Abstract*—Numerous articles and patents on the masking of logic gates in CMOS logic styles have been reported, however, less information is available with regards to comparing the single-rail and dual-rail on masking input logic values. This paper investigates single-rail and dual-rail logic families that have been developed by the logic designers for secure logic implementations in cryptographic system. The novelty of this work is that we evaluate the dynamic logic and differential logic for one-phase 2-inputs logic in adiabatic mode in SPICE simulation. We analyze the power consumption of logic circuit along 16 possible transitions of 2-inputs logic during one cycle. The power traces show that adiabatic differential logic families are masking the input logic values, because they consume constant power during pre-charge and evaluation phases that enables the circuit to resist against power analysis attacks. Based on our results, we deduce that adiabatic differential logic families are promising candidates for further development to obtain a far more robust secure logic for countermeasure against power analysis attacks in smart card.**

## I. Introduction

Power analysis attacks have become a special threat for cryptanalysis algorithm designers, software developers and hardware engineers to maintain the security of secret key in cryptographic implementation, such as in smart card. During the past years, a lot of researches have been conducted on simple power analysis (SPA) and differential power analysis (DPA) [1,2] on mathematical algorithm level. The SPA is more focusing on the use of visual inspection techniques to identify relevant power fluctuations during cryptographic operations, hence it is vulnerable for attackers to identify the secret key by calculating the power consumption during cryptographic operations. DPA attacks are more advanced than SPA attacks in which they use the statical methods and digital processing techniques on large number of power consumption signals to reduce noise and strengthen the difference signals, so it will be obvious to distinguish between the logical zero and logical one. There was also an effort of Adi Shamir to protect smart card from two main attacks, such as DPA and SPA attacks by detaching two capacitors to smart card [3]. His work was to detach two capacitors to work as a power isolation element by switch control unit and four power transistors which are added to the smart card chip. To protect the secret keys during encryption and decryption execution of smart card from power analysis attackers, there are a lot of efforts to mask the secret keys on algorithm level and monitoring power consumption signals to withstand side channel attacks (SCA) of cryptographic systems [4]–[7].

The fundamental issues of power analysis attacks on cryptographic systems are closely related to electrical power consumption of hardware implementations. Regarding power consumption in cryptographic implementation such as smart-card, logic design should be highly considered in order to mask the input logic values and also reduce power consumption in digital circuit level. There have been several works done on masking input logic in gate level, such as Power analysis of single-rail storage elements as used in MDPL [8] which is analyzing the leakage of flip-flop designs for various side-channel resistance logic styles, but ignoring the difference between capacitances of complementary wire that affect huge power dissipation. In addition, three phase dual-rail pre-charge logic (TDPL) [9] has proposed to be used in semi-custom design flow without any constraint of the routing of complementary wires, which whose power consumption is insensitive to unbalanced load condition. Furthermore, combination of dynamic and differential logic gates, referred to as Sense Amplifier Based Logic (SABL) has been proposed and implemented in cryptographic implementation by Tiri $et\ al.$ [10]–[13] which is balancing all the internal node capacitances. As a result, SABL consumes a constant power during pre-charge and evaluation phases. To proof the masking input logic values at gates level, Side-Channel Leakage of Masked CMOS Gates [14] and Masked Dual-Rail Pre-charge Logic (MDPL) [15] are proposed. As described in [14], the cryptographic attackers are normally calculate the means of energy and subtract to each other, hence there are leakage of channel information for dynamic normal gates, but channel information is secure for masked gates. It was stated in [15], resistance against DPA attacks at the gate level can not only be achieved by consuming the same amount of energy for all transition, but also by randomizing the logic signals in the circuit.

In this paper, we evaluate two logic types: dynamic logic [16] and differential logic of SABL [13], DCVSL [17], and 2N-2N2P [18]. The aim of this work is to investigate the possibilities of masking input logic in single-rail and dual-rail logic, comparing the current traces and its energy dissipation to be developed in the future work. The remainder of this paper is organized as following: Section II describes the evaluated logics in adiabatic perspective; the simulation results and its calculation of the figure of merit are described in Section III, and finally we conclude this paper in Section IV.

## II. Adiabatic Logic

Most of previous secure logic styles against power analysis attacks in cryptographic VLSI systems are energy consuming. Our approach in this work is to evaluate dynamic logic and differential logic in adiabatic mode. The principle of adiabatic charging can be understood by contrasting it with conventional method during the charge of a capacitor in an RC circuit, as described in Fig. 1.

In conventional CMOS circuits, the capacitance C is charged from 0→$V_{dd}$, where $V_{dd}$ is DC power supply. During charging period in conventional CMOS, the charged energy in C is:

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

From the energy conservation perspective, a conventional CMOS logic emits heat, hence it wastes energy in every charge-discharge cycle:

$$\begin{aligned} E_{total} &= E_{charge} + E_{discharge} \\ &= \frac{1}{2} C V_{dd}^2 + \frac{1}{2} C V_{dd}^2 \\ &= C V_{dd}^2. \end{aligned} \quad (2)$$

If the logic is driven by certain frequency $f(= 1/T)$, where $T$ is the period of the signal, then the power persecond of CMOS gate is determine as:

$$\begin{aligned} P_{total} &= \frac{E_{total}}{T} \\ &= C V_{dd}^2 f. \end{aligned} \quad (3)$$

Observing the conventional CMOS, power consumption is proportional to $V_{dd}^2$ so, one of the most effective way to reduce its power consumption is to lower the power supply voltage.

Adiabatic switching is commonly used in minimizing energy lost during charging/discharging period. The main idea of adiabatic switching is shown in Fig. 1(b) indicated that transition is considered to be sufficiently slow so that the heat is not emitted significantly. This is made possible by replacing the DC power supply by a resonant LC driver or oscillator. If constant current source delivers the $Q = CV_{dd}$ charge during the time period $\Delta T$, the energy dissipation in channel resistance $R$ is given by:

$$\begin{aligned} E_{diss} &= \xi P \Delta T = \xi I^2 R \Delta T \\ &= \xi \left( \frac{C V_{dd}}{\Delta T} \right)^2 R \Delta T, \end{aligned} \quad (4)$$

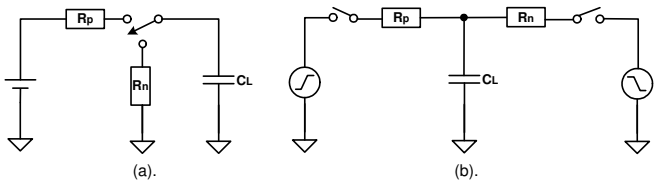


Fig. 1. (a) Conventional CMOS charging, (b) Adiabatic charging circuit

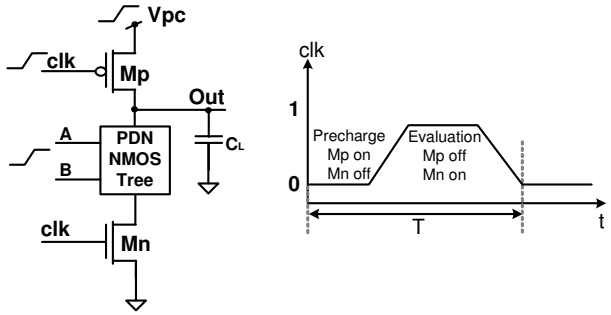


Fig. 2. Generic dynamic logic (left) and its phases (right)

where $I$ is considered as the average of the current flowing to $C$, and $\xi$ is a shape factor which is dependent on the shape of the clock edges. Observing the adiabatic switching equation, the charging period $\Delta T$ is indefinitely long, ideally the energy dissipation is reduced to nearly zero [19].

### A. Adiabatic Dynamic Logic

The basic construction of dynamic logic gate is shown in Fig. 3. Dynamic logics are always driven by clock (clk), which has two phases: Pre-charge phase and Evaluation phase. When clk=0, $M_p$ is $ON$ and $M_n$ is $OFF$, and under this condition, the pre-charge phase occurs, which drives $Out = 1$ and energy is stored in $C_L$. On the other hand, if clk=1, $M_p$ is $OFF$ and $M_n$ is $ON$, this condition is called the evaluation phase. The output is conditionally discharged based on the input values and the pull-down network topology.

### B. Adiabatic Differential Logic

We choose Differential cascode voltage switch Logic (DCVSL), 2N-2N2P and secure logic of SABL as the differential logic families to be investigated in adiabatic mode. In generic differential logic families, the circuits are operated in two outputs conditions: 1) When the input vector $\mathbf{x} = (x_1, ..., x_n)$ is the true vector of the switching function Q($\mathbf{x}$), node Q is disconnected from the ground by the unique path of NMOS Differential Pull Down Network (DPDN) tree. 2) When $\mathbf{x} = (x_1, ..., x_n)$ is false vector of Q($\mathbf{x}$), the reverse holds. The rough analysis of energy dissipation in DCVSL and 2N-2N2P logic families as shown in Fig. 4 are identical, that energy is dissipated when exactly one output node is discharged, but the only important idea is that energy is increasing proportional to the increasing number of gates.

The secure logic of SABL is constructed with combination of dynamic and deferential logic with special differential pull down network (DPDN) that achieves two goals; (1) switching

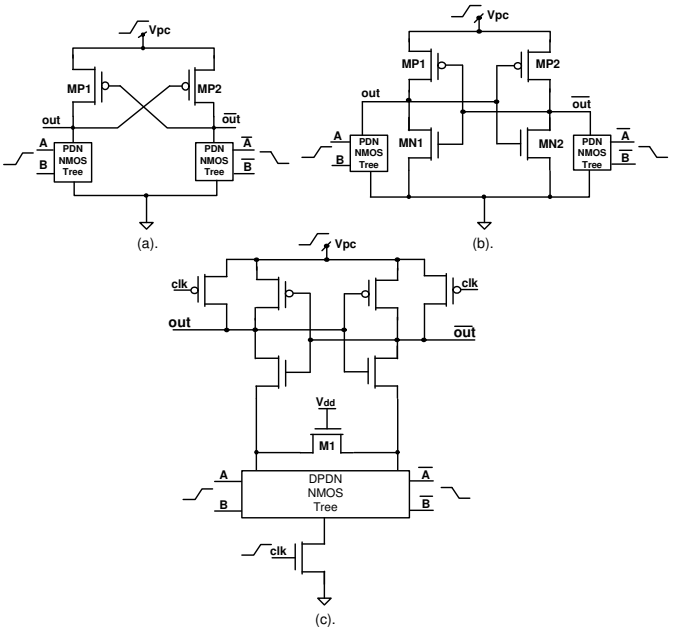


Fig. 3. Differential logics: (a) DCVSL, (b) 2N-2N2P, (c) SABL

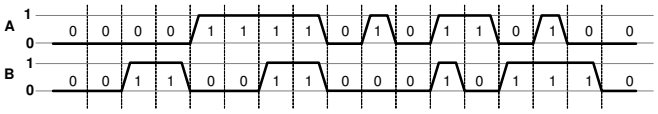


Fig. 4. 16 possible transition of 2-inputs logic

the output independently of the input values and (2) having a constant load capacitance equal to all internal nodes combined with one of the balanced output load. Hence, the SABL is consuming constant energy for every transition.

## III. Simulation and Results

### A. Simulation Conditions

To evaluate the power traces of adiabatic dynamic logic and adiabatic differential logics, the 2-inputs of NAND2, XOR, XNOR in dynamic logic and 2-inputs of NAND/AND, XNOR/XOR in differential logics are simulated in SPICE simulation with an 0.18 $\mu$m, 1.8 V CMOS standard process technology. The transistor size $W/L$ is 0.6 $\mu$m/0.18 $\mu$m for both of PMOS and NMOS transistors.

In SPICE simulation, the condition for adiabatic dynamic logic: all power supplies are trapezoidal signals, $f_{pc}$ = 100 MHz and 1.8 V of $V_{pc}$. The condition for Differential logic: all power supplies are trapezoidal signals, $f_{pc}$ = 50 MHz and 1.8 V of $V_{pc}$.

The merit of this work is that we design timing diagram for 16 possible transactions of 2-inputs logic to investigate the possible masking of input logic values in single-rail and dual-rail logic families. The designed of 2-inputs transitions is depicted in Fig. 4.

### B. Results

The simulation results of evaluated circuits are shown in Figs. 5–7. By using the same 16 patterns of 2-inputs transition, we draw the power consumption of each circuit as: $E_{diss} = \int_0^T V_{pc}(t) I_{pc}(t) dt$, which is adopted as figure of merit to measure the resistance against power analysis attacks. We show the currents traces of $I_{pc}$ to be observed, and from here we analyze the peak currents of each circuit to decide which logic family should be developed in future work for robust

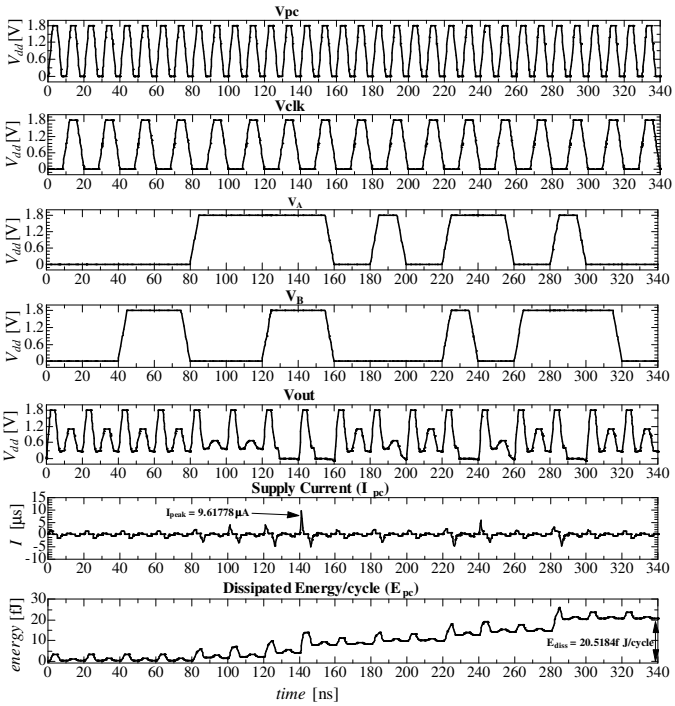


Fig. 5. Inputs and Outputs Signals of adiabatic dynamic NAND2

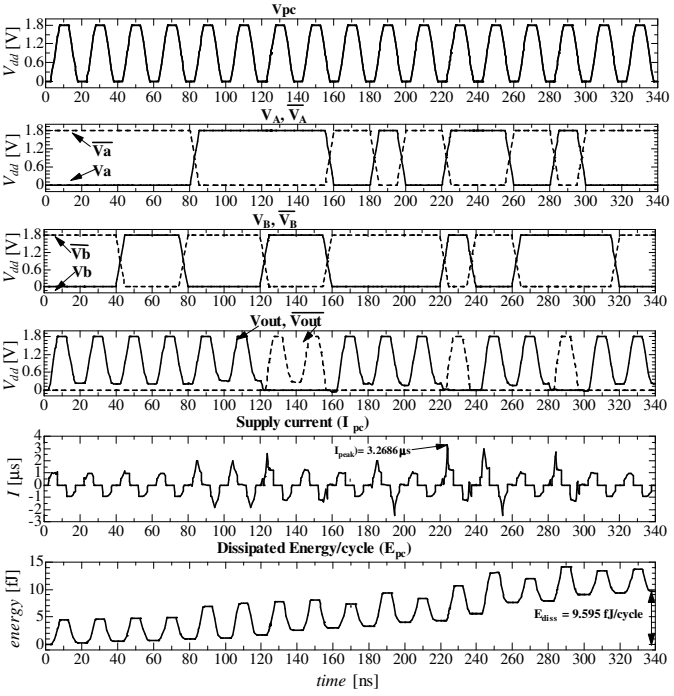


Fig. 6. Inputs and outputs signals of adiabatic DCVSL NAND/AND

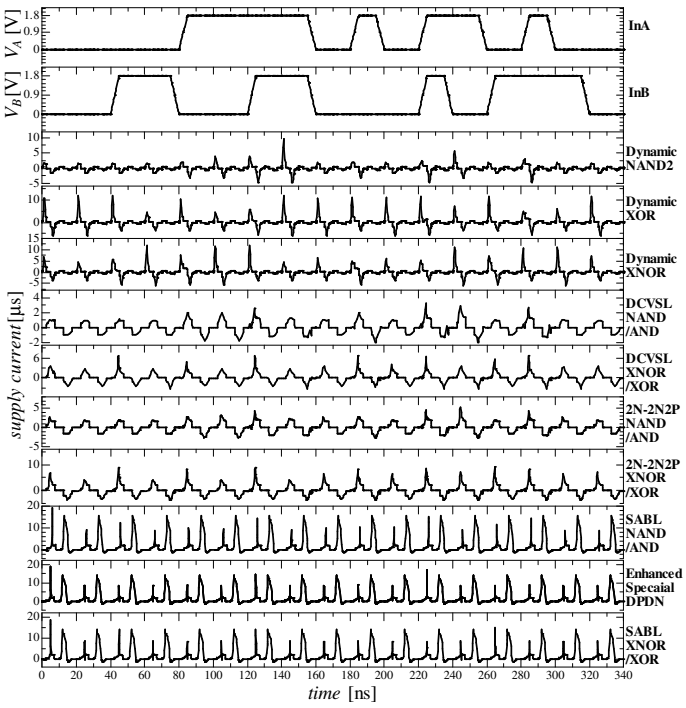


Fig. 7. Current traces of evaluated circuits

TABLE I
SIMULATION AND CALCULATION RESULTS FOR INPUT NAND/AND

| | NAND/AND | | | | |
|---|---|---|---|---|---|
| | D.NAND2 | DCVSL | 2N-2N2P | SABL | E.S.SABL |
| $E_{min}$[fJ] | 0.017 | 0.166 | 0.307 | 54.038 | 52.099 |
| $E_{max}$[fJ] | 5.687 | 2.105 | 2.705 | 54.663 | 52.611 |
| NED[%] | 99.71 | 92.13 | 88.65 | 1.14 | 0.97 |
| $\bar{E}$ [fJ] | 1.21 | 0.59 | 0.9 | 54.28 | 52.23 |
| $\sigma_E$[fJ] | 1.6 | 0.51 | 0.7 | 0.201 | 0.189 |
| NSD[%] | 132.8 | 86.77 | 4.1 | 0.369 | 0.363 |

D.NAND2: Dynamic 2-inputs NAND logic
E.S.SABL: Enhanced Special DPDN of SABL

TABLE II
SIMULATION AND CALCULATION RESULTS FOR INPUT XNOR/XOR

| | XNOR/XOR | | | | |
|---|---|---|---|---|---|
| | D.XNOR | D.XOR | DCVSL | 2N-2N2P | SABL |
| $E_{min}$[fJ] | 0.807 | 0.809 | 0.959 | 1.415 | 52.126 |
| $E_{max}$[fJ] | 9.189 | 9.214 | 3.291 | 4.063 | 52.541 |
| NED[%] | 91.21 | 91.22 | 70.84 | 65.178 | 0.79 |
| $\bar{E}$ [fJ] | 4.92 | 5.07 | 2.31 | 3.13 | 52.24 |
| $\sigma_E$[fJ] | 2.88 | 2.37 | 0.71 | 0.93 | 0.17 |
| NSD[%] | 58.4 | 46.8 | 30.9 | 29.8 | 0.329 |

D.XOR: Dynamic 2-inputs XOR logic
D.XNOR: Dynamic 2-inputs XNOR logic

secure logic against power analysis attacks on smart cards.

Results of evaluated gates are summarized in table I and table II for 2-inputs NAND/AND and XNOR/XOR separately. The calculation for normalized energy deviation (NED) is defined as $(E_{max} - E_{min})/E_{max}$ and normalized standard deviation (NSD) is $\sigma_E/\bar{E}$ [9]. The $\bar{E}$ is average of energy dissipation of every transition during 16 transitions of two input logics that shows in Fig. 4. Figure 5 and 6 are simulation graphs of adiabatic dynamic NAND2 and DCVSL NAND/AND logics respectively. These figures show that dynamic logic dissipates more energy dependent on frequency of clock signal. By comparing the peak of supply currents, the DCVSL has lower peak current than that of dynamic NAND2, making it possible to mask the input values from side channel attacks. Detailed data is shown in Fig. 7, demonstrating all the supply currents of evaluated circuit.

From table I and table II, the calculation of NED and NSD are to measure the ability of logic circuit for resistance against power analysis attacks. The results indicate that adiabatic differential logic has been our choice to develop for secure logic application, however the energy dissipation of dual-rail logics is higher than that of single-rail logic. Therefore, we will present a new low pawer secure dual-rail adiabatic logic in our future work.

## IV. CONCLUSION

We have evaluated single-rail and dual-rail logics to analyze their power consumption and supply current traces, as our preliminary study to design more robust secure logic application, for counteracting power analysis attacks at the cell level in cryptographic implementation. Analysis for the power consumption of logic circuits along 16 possible transitions of 2-inputs logic during one cycle has showed that adiabatic differential logic families are masking the input logic values, since they consume constant power during pre-charge and evaluation phases that enables the circuit to resist against power analysis attacks. Based on the results of this study, dual-rail logic has been our choice to develop for a more stringent robust secure logic against power analysis attacks in cryptographic systems, such as application specific integrated circuit (ASIC) in smart card. To design a more secure logic as a resistance against side channel attacks, we will attempt to combine two important considerations; (1) consuming constant power for every transitions by balancing all internal node capacitances, (2) randomizing the input logic values, which will become our basis for any future work in designing low power secure dual-rail adiabatic logic, for utilization in cryptographic implementation.

## ACKNOWLEDGMENT

The custom circuits in this paper have been simulated with Cadence/Synopsys tools through the chip fabrication program of VLSI Design and Education Centre (VDEC), the University of Tokyo in collaboration with Rohm Corporation.

## REFERENCES

[1] P. C. Kocher, J. Jaffe, and B. Jun,"Differential power analysis," in *Proc. CRYPTO'99*, 1999, Lecture Notes in Computer Science (LNCS), vol. 1666, pp. 388–397.

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," avaliable URL: http://www.cryptography.com/dpa/technical

[3] A. Shamir, "Protecting smart card from passive power analysis with detached supplies," in *Proc. Criptographic Hardware and Embedded System* (CHES'00), 2000, LNCS, vol. 1956, pp. 71–77.

[4] P. Kocher, “Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other system,” in *Proc. Advances in Cryptology* (Crypto’96), 1996, LNCS, vol. 1109, pp. 104–113.
[5] T. S. Messerges, E. A. Dabbish and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” in *IEEE Trans. Computers*, vol. 51, no. 4, pp. 541–552, Apr. 2002.
[6] J. S. Coron and L. Goubin, “On Boolean and arithmetic masking against differential power analysis,” in *Proc. CHES’00*, 2000, LNCS, vol. 1956, pp. 231–237.
[7] S. Chari, C.S. Jutla, J.R. Rao and P. Rohatgi, “Towards sound approaches to couteract power-analysis attacks,” in *Proc. CRYPTO’99*, LNCS, vol. 1666, pp. 398–412.
[8] A. Moradi, T. Eisenbarth, A. Poschmann and C. Paar, “Power analysis of single-rail storage elements as used in MDPL,” in *Proc. of 12th Int. Conf. Information and Cryptology* (ICICC’09), 2010, LNCS, vol. 5984, pp. 146–160.
[9] M. Bucci, L. Giancane, R. Luzzi and A. Trifiletti, “Three-phase dual-rail pre-charge logic,” in *Proc. CHES’06*, 2006, LNCS, vol. 4249, pp. 232–241.
[10] K. Tiri, and I. Verbauwhede, “Securing encryption algorithms against DPA at the logic level: Next generation smart card technology,” in *Proc. CHES’03*, pp. 125–136.
[11] K. Tiri, and I. Verbauwhede, “A logic level design methodology for a secure DPA resistance ASIC or FPGA implementation,” in *Proc. Europe Conference and Exhibition* 2004, vol. 1, pp. 245–251.
[12] K. Tiri, and I. Verbauwhede, “Charge recycling sense amplifier based logic: securing low power security IC’s against DPA,” in *Proc. European Solid-State Circuits Conf.* (ESSCIRC 2004), pp. 179–182.
[13] K. Tiri, M. Akmal, and I. Verbauwhede, “A dynamic and differential CMOS logic with signal independent power consumption to withstand differensial power analysis on smart cards,” in *Proc. ESSCIRC2002*, pp. 403–406.
[14] S. Mangrad, T. Popp and B.M. Gammel “Side channel leakage of masked CMOS gates,” in *Proc. Conf. CT–RSA’05*, 2005, pp. 351–356.
[15] T. Popp and S. Mangard, “Masked dual-rail pre-charge logic: DPA-Resistance Without Routing Constraints,” in *Proc. CHES”05*, 2005, pp. 172–186.
[16] D. J. Tran and M. J. Acuff, “Dynamic logic circuit,” *Unated States Patent* 5,859,547, Jan. 1999.
[17] L. G. Heller, W. R. Griffin, J. W. Davis, and N. G. Thomas, “Cascode voltage switch logic: A differential CMOS logic family,” in *ISSCC Dig. Tech. Papers*, Feb. 1984, vol. 27, pp. 16–17.
[18] 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*, 1995, pp. 191–196.
[19] 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.