Analysis Of DPA Resistant Adiabatic Logic Style In Low Power Adder Circuits

Lavanya R, Karpagam M

Abstract: This paper analyzes the ability of adiabatic logic with charge sharing mechanism to implement low power adder circuits. Power consumption comparison with variety of adiabatic logic structures and static CMOS logic is made. Simulation results show that charge sharing adiabatic technique achieves 81% power reduction on the average with reference to 2N-2N2P, ECRL and SyAL logic. Hence charge sharing DPA resistant logic style is evaluated through implementation of adder circuits which are used as secondary elements in cryptographic algorithms.

Index Terms: DPA, adiabatic logic, low power, arithmetic circuits, charge sharing, cryptography.

1 Introduction

The need for the design of digital very low-power integrated circuits is increasing the range of applications in portable and embedded computing. Cryptographic devices such as access cards, RFID tags, pay TV modules etc., leak sensitive information through the time taken and power consumption of the circuit used, which can be used to predict the secret key of that device. The secret key can be used to attack the device. Power analysis is a major attack in tracking the secured key of the cryptographic device by statistically analyzing power variation that occurs when the device decrypts a large amount of data [1]. The main factors of power attacks are due to CMOS logic power consumption. Generally, CMOS devices are dependent on bit change and on the capacitance at the functional block's output. The power consumption will be different for bit '0' and bit '1' transition. If the power consumption of the circuit is found, then it is possible to predict the 0 or 1 data as the amplitude of the power consumption is a function of the capacitances. This problem can be solved by to have a logic that consumes the same amount of power for every kind of bit transition (i.e. 1 →0, 1→1, 0→1, 0→0). To achieve low power consumption different design techniques can be applied. Adiabatic switching is a technique based on reducing the charge transport, and recovering the charge stored in the parasitic capacitors. The adiabatic circuits found in literature can be classified as fully adiabatic circuits or partial adiabatic circuits. Fully adiabatic circuits consume asymptotically zero energy for operation, but it occupies large area and has high design complexity. Whereas partial energy recovery circuits are designed to recover a large portion of the energy stored in the circuit node capacitances. Many circuit level countermeasures for power analysis attacks have been proposed, one of the most widely encountered countermeasures is Sense-Amplifier Based Logic (SABL). SABL is a dynamic logic with differential pull down network for processing the input signals. The pull down network completely charges and discharges the load capacitance sustaining it at a constant value which makes the power consumption independent of the input data. As SABL cells need to be custom designed an alternate style called Wave Dynamic Differential Logic (WDDL) came as a replacement as they were designed using standard cells. This makes implementation on FPGAs easier, reducing the design effort and complexity. With reduced complexity the design was prone to DPA (Differential Power Analysis) attacks as the cells were highly data dependent. Random switching logic (RSL) uses a random switching bit to avoid dual rail logic. It also has a precharge signal that automatically changes states after the inputs are passed to the logic, this operation tends suppresses the glitches [2],[3]. A variety of adiabatic logic structures are seen in literature with the power clock signal controlling the logic functions in pre-charge phase and evaluation phase. Dual rail logic families such as ECRL,2N2P,SyAL show minimized dependence of peak supply current to the input variations, but they are found to consume considerable amount of power[3],[4]. In order to achieve low current correlation and power the symmetry of the dual rail logic with respect to the capacitance that is charged/discharged during the evaluation and recovery phase is equally managed using Charge sharing symmetric adiabatic logic(CSSAL)[5], this logic is employed in the design of an efficient Ultra low power carry look ahead adder. The organization of the paper is as follows. In Section II, the concept of CMOS conventional switching is illustrated. In Section III, Charge recovery adiabatic logic principle is explained. Section IV, discusses the various secure adiabatic logic styles, supply current variations are evaluated to bring about the DPA resistance property of each style and its power consumption and illustrates the implementation of Adder circuits with the efficient charge sharing symmetric adiabatic logic style. Finally section V gives the conclusion of the study undertaken.

2 Conventional Switching of CMOS Logic

In static CMOS logic shown in Fig. 1 the major factor that contributes to power consumption is the power required to charge capacitive nodes. The capacitance at the output of logic function has to drive the input of succeeding gates. The PMOS or NMOS is turned on based on the logic value of the input signal. If the input changes from 1 to 0, then the PMOS transfers energy from the source voltage to the output capacitor. The charge taken from the voltage source is

$$Q=CV_{DD} \quad (1)$$

and, the energy given in (2)

$$EV_{DD} = QV_{DD} = C\,V_{DD}^2 \quad (2)$$

- *R.Lavanya, Assistant Professor, ECE, Sri Ramakrishna Institute of Technology, Coimbatore, India. E-mail id: lavanya.ece@srit.org*
- *Dr.M.Karpagam, Associate Professor, EEE, Hindusthan College of Engineering and Technology, Coimbatore, India. E-mail id: karpagam.sathish@gmail.com*

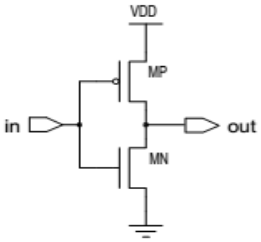

Fig. 1. *CMOS Inverter*

Is drawn from the voltage source. The energy stored on the capacitor is equal to

$$E_c = 1/2\ (C\ V_{DD}^2) \quad (3)$$

The difference between the drawn energy and stored energy is dissipated through PMOS. During 0 to 1input transition, the NMOS turns on and PMOS turns off. Charge stored in the output capacitor is dissipated through the NMOS pull down network. The energy dissipation of the CMOS inverter is given as

$$E_{CMOS} = \alpha(1/2)\ (C\ V_{DD}^2) \quad (4)$$

Where α is the switching probability, when there is no switching activity then the dissipation is zero. Many approaches are used to reduce the energy dissipation in CMOS logic; it involves decreasing the number of transitions for a computation in algorithmic level, structural level and circuit level. The next approach involves reducing the capacitive load, but it is limited by technology. Scaling the supply voltage V_{DD} is an influential method to reduce the energy dissipation, but the performance gets degraded.

3 Adiabatic Logic

Adiabatic logic uses the condition that a single cycle of a clock pulse is much longer than the RC delay and hence the charge can be extended over the entire cycle which in turn reduces the energy dissipation. In order to extend the charging time of the gate the transistor should not be turned on when there exists a potential difference between the source, during on state energy flows in a gradual and controlled way. Due to this charging manner the overall energy dissipated at each transition is reduced to

$$E_{Adiabatic} = \xi\ (RC/T)\ (C\ V_{DD}^2) \quad (5)$$

where T denotes the charging-discharging time, V_{DD} is the supply voltage, and ξ is the shaping factor of power clock waveform. The circuit should not be turned off when there is current flowing through as the transistors are not perfect switches and they gradually change their states with respect to the change in gate voltage. Thus because of this gradual switching the transistor is in a in- between state for a long period of time during which the voltage drop across the transistor increases however the resistance is not sufficient to bring down the power dissipation to zero. This adiabatic logic functionality can be proved practically by adopting the logic equivalent RC models for the conventional CMOS logic[5] is illustrated in Fig. 2.

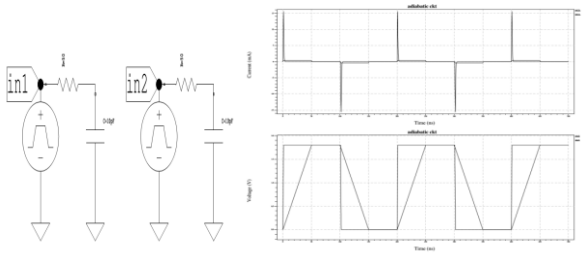

Fig. 2. *RC model with pulse input and power clock input and difference in peak supply current of the RC models*

TABLE 1
POWER COMPARISON OF RC NETWORK

Logic	Average Power Consumption (Watts)	Maximum Power Consumption (Watts)
RC Network with fixed input	1.24e-04	2.80e-02
RC Network with Adiabatic input	3.54e-05	6.48e-04

From Table I the Power consumption of RC network with pulse input and ramp input reveals that adiabatic circuits consume less power. The Adiabatic principle is also verified with a CMOS inverter driven by power clock as shown in Fig. 3.

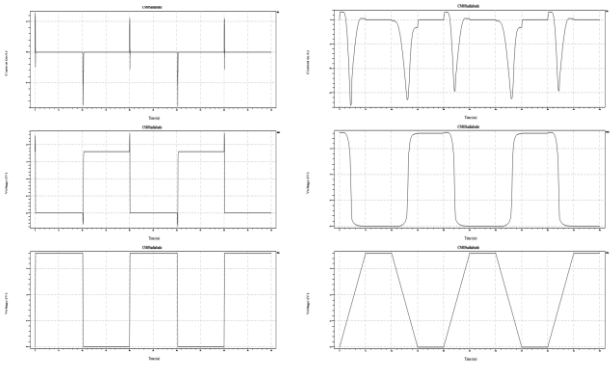

Fig. 3. *Peak supply current conventional CMOS inverter and Inverter with adiabatic principle*

4 Secure Adiabatic Logic Styles

4.1 Efficient Charge Recovery Logic (ECRL)

The Efficient Charge Recovery Logic (ECRL) shown in Fig. 4 has a simple structure, but it has asymmetric discharge paths thus the current from the supply power clock (Vpc) change with respect to the change in the input data. For example, when the input to INR is '0,' transistor MN1 is off, then the supply current charges the capacitance at node OUTB. When the input is '1' the node OUTR is charged. This circuit displays dependency of the output current on the input data. This relation between the current and data has to be removed to make the adiabatic logic effective against DPA [6].

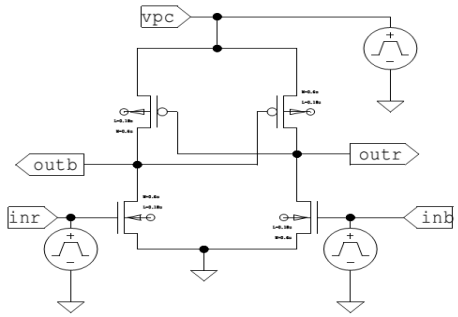

Fig. 4. *Structure of Efficient Charge Recovery Logic (ECRL) Inverter*

4.2 2N2P Logic

A 2N-2N2P charge recovery logic is shown in Fig. 5 has complementary symmetrical structure constructed using NMOS pull down network to realize the logic functionality. The pull down network is triggered with complementary inputs. Two cross coupled PMOS transistors are used to hold the output values constant after the evaluation phase.

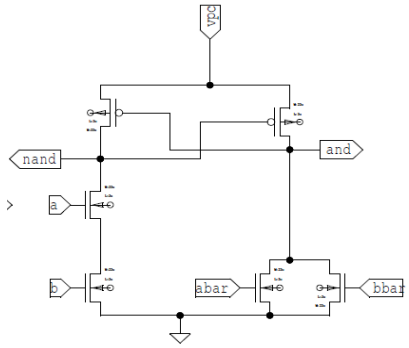

Fig. 5. *Logic structure of 2N2P Inverter*

4.3 Symmetric Adiabatic Logic (SyAL)

Symmetric adiabatic logic (SyAL) shown in Fig. 6 makes use of symmetric pull-down transistor proposed in symmetric discharge logic to reduce difference in power traces in the logic function realized by ECRL by inserting BR transistors to develop resistance to DPA attacks. SyAL is designed to provide equal discharge paths for both on and off transistors in the logic for all cases of input combinations. The BR transistors operate when power clock and both inverter inputs are low level. Thus the supply current is not affected by input data[7].

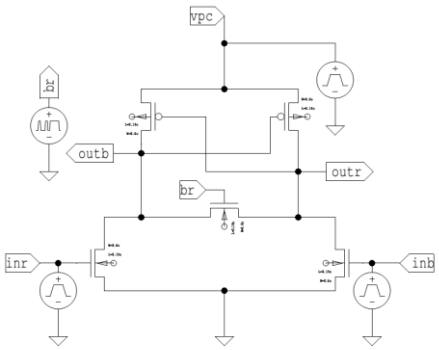

Fig. 6. *Logic structure of Symmetric Adiabatic Logic (SyAL)*

4.4 Charge Sharing Symmetric Adiabatic Logic (CSSAL)

Charge-sharing symmetric adiabatic logic (CSSAL) shown in Fig.7 is a modified form of symmetric adiabatic logic(SyAL) with a charge-sharing mechanism that distributes the charge equally among the inputs. Charge sharing is established by using a discharge (Dischg) signal initially to increase with a rate twice that of power-clock voltage (Vpc) and the evaluation path signal also increases gradually, this discharges all the internal node capacitances before evaluation. This prevents the circuit from depending on the previous input data. In the evaluation phase discharge signal becomes low, MP1 turns on and the supply current flows into the logic circuit, thus the output gets evaluated through one of the active input cells. During the hold phase, Eval signal slowly becomes low, but the output remains stable due to the cross-coupled NMOS transistors MN1 and MN2. During the recovery phase the Vpc steadily decreases, and the output is discharged through the transistors MP2 or MP3. An additional control transistor Cx equalizes the discharge paths during the evaluation phase[8],[9].

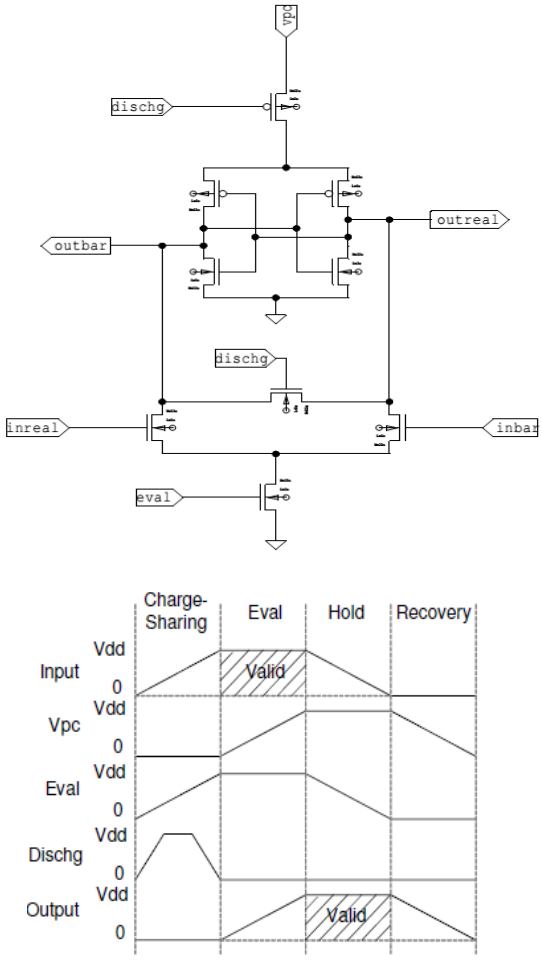

Fig. 7. *Logic structure structure of Charge Sharing Symmetric Adiabatic Logic (CSSAL) and timing waveform of CSSAL*

CSSAL logic initially sets all the internal node capacitances to zero before the onset of power-clock signal and when the input signal Vin/Vin bar≥VTHN. This makes CSSAL logic shown in Fig. 8 balance peak supply current variations, and a cross-coupled latch in the 2N–2N2P logic is introduced for employing the logic low power applications. The NAND/AND

logic is shown in Fig. 9. Fig. 10, Fig. 11 respectively are all implemented in the pull-down function block with the charge sharing mechanism which effectively balances the supply current variations with minimized energy consumption.

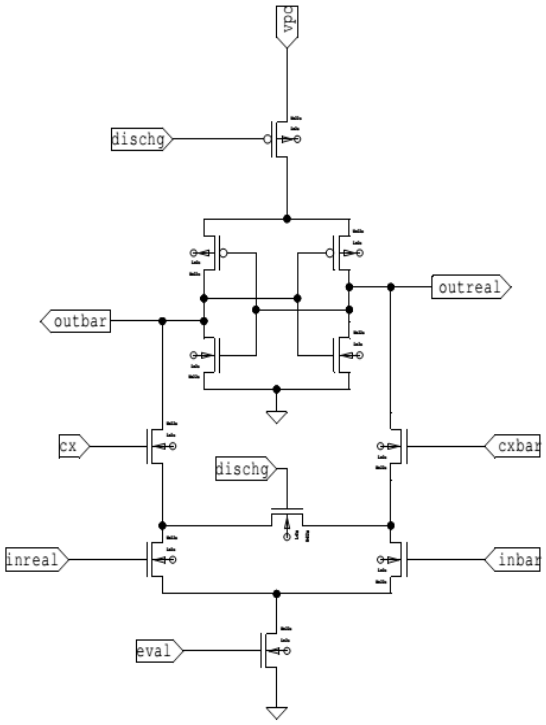

Fig. 8. *Structure of Charge Sharing Symmetric Adiabatic Logic (CSSAL) Inverter with Control transistor Cx*

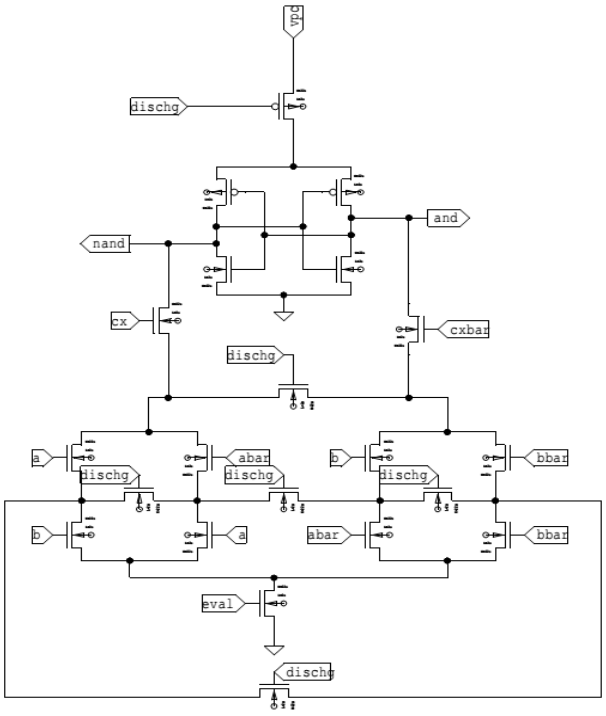

Fig. 9. *CSSAL AND/NAND Structure*

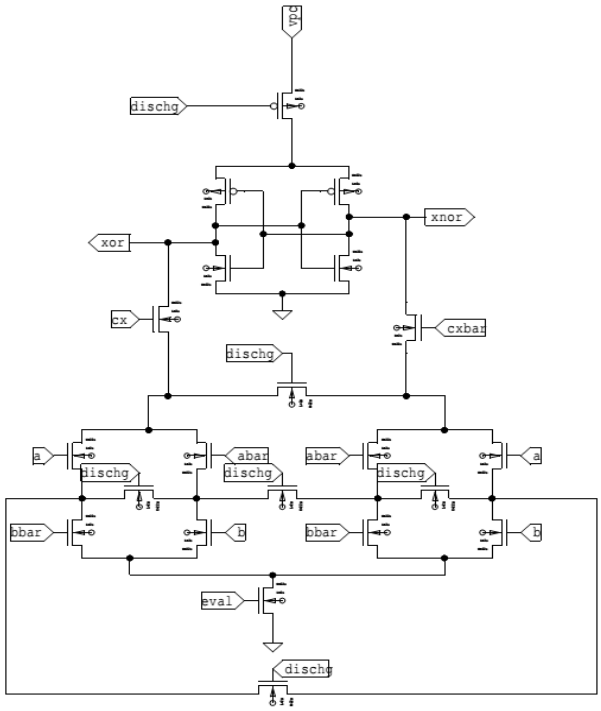

Fig. 10. *CSSAL XOR/XNOR Structure*

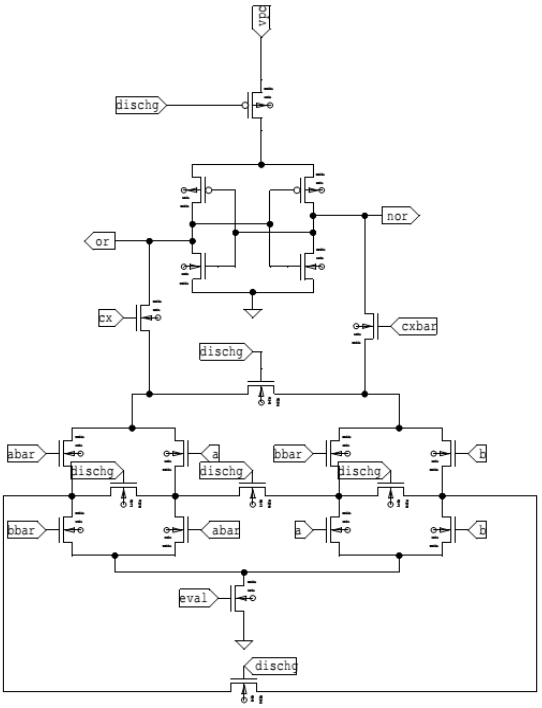

Fig. 11. *CSSAL OR/NOR Structure*

5 Comparison and Evaluation of Secure Adiabatic Logic Styles

To estimate current differences and power consumption of the adiabatic logic circuits HSPICE with 0.18um, 1.8V CMOS standard process technology was used with transistor size W/L is 0.6 um/0.18 um for both PMOS and NMOS transistors with operating frequency of 12.5MHz. The most important part for secure logic designing is input cell construction of the logic

functions. Input logic structure determines the dependence or independence of power consumption corresponding to data that is being processed. The comparison of supply current consumption by each adiabatic logic is analyzed in this survey. 2N2P and ECRL employ universal pull-down network that retain some internal floating capacitance, consequently, they exhibit varying supply current traces for every power clock cycle Fig. 12 (a),(b). On the other hand, the SyAL and CSSAL adopt charge sharing symmetric input logic style which enables the circuits to consume constant and uniform supply current for all the possible input transitions Fig.12 (c),(d).

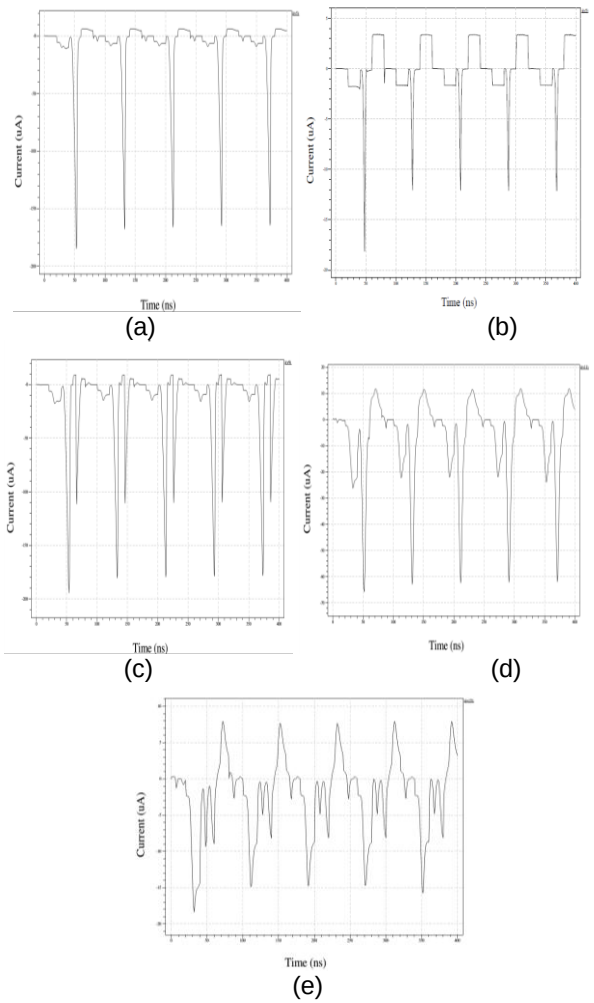

Fig. 12. *CSSAL Supply current variations of (a) 2N2P Inverter,(b) ECRL Inverter, (c) SyAL Inverter, (d) CSSAL Inverter without Cx, (e) CSSAL Inverter with Cx.*

The simulation results show for any input condition, CSSAL always shows lower peak current and identical peak currents for all input combinations as indicated in Fig. 12(d). Further an additive control signal to evaluate the logic function helps in further reduction of the peak current from 60uA to 15uA.CSSAL is found to have about 91% reduction in the maximum power consumed with reference to CMOS logic and about 79.9% lesser power compared with ECRL logic as shown in Table 2. The advantage of CSSAL for use in low power applications is demonstrated through using the logic to implement digital circuits such as adders.

TABLE 2
POWER CONSUMPTION OF SECURE ADIABATIC LOGIC STYLES

Logic	Average Power Consumption (Watts)	Maximum Power Consumption (Watts)
CMOS inverter using Adiabatic input	3.07e-03	3.19e-04
2N-2N2P inverter	1.77e-05	3.37e-04
SYAL inverter	2.80e-05	3.54e-04
ECRL inverter	1.77e-05	3.37e-04
CSSAL WOCX Inverter	1.22e-05	1.18e-04
CSSAL inverter	3.55e-06	2.60e-05

6 ARITHMETIC CIRCUITS WITH CSSAL

A For demonstration arithmetic circuits such as Full adder, Ripple carry adder and Carry look ahead adder are simulated using the power efficient DPA resistant CSSAL design. The design of adder circuits requires basically XOR gate, AND gate and OR gate which are designed using the CSSAL style. Simulation of these gates also verify the charge sharing mechanism works satisfactory with lower supply current variation and lower power as shown in Fig. 13 and Table III. The three adders taken for study show that even when the number of inputs is increased, the supply current variations remain identical for the circuits for all the patterns applied with a slight increase in the current as shown in Fig. 13.

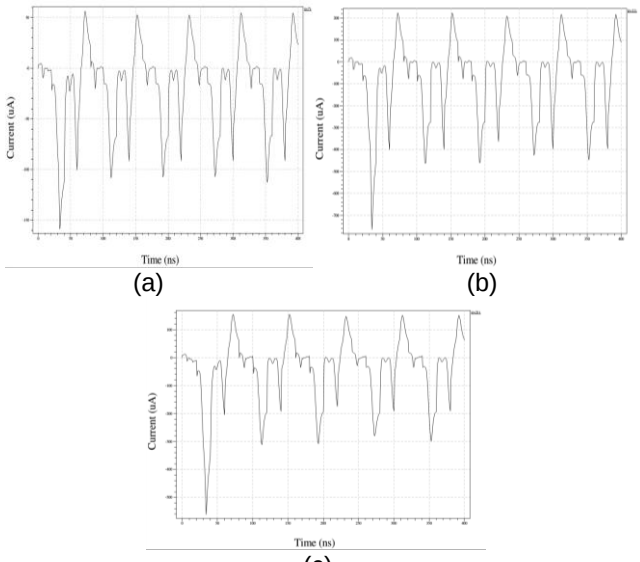

Fig. 13. *Supply current variations of CSSAL (a) Full adder, (b) Ripple Carry adder, (c) Carry look ahead adder.*

TABLE 3
POWER CONSUMPTION OF SECURE ADIABATIC LOGIC STYLES

Logic	Average Power Consumption (Watts)	Maximum Power Consumption (Watts)
CSSAL NAND gate	3.74e-06	5.77e-05

Logic	Average Power Consumption (Watts)	Maximum Power Consumption (Watts)
CSSAL XOR gate	3.51e-06	2.96e-05
CSSAL OR gate	4.10e-06	2.95e-05
CSSAL Full adder	2.97e-05	2.02e-04
CSSAL Ripple Carry Adder	1.19e-04	9.95e-04
CSSAL Carry Look Ahead Adder	6.93e-05	7.22e-04

7 Conclusion

A comparative study on the ability of charge sharing DPA resistant logic as a low power design technique to construct arithmetic circuits shows that the average power consumed is 81% lesser on the average with reference to 2N-2N2P, ECRL and SyAL and the current waveforms show a uniform energy over every input transition and reduced level of peak supply current traces. Previous work on logic level countermeasures against DPA attacks mainly focused on reducing the peak supply current traces, this paper has analyzed the charge sharing adiabatic logic as a countermeasure against DPA as well as applying the logic to design low power arithmetic circuits. The average power consumption of the adder circuits show that DPA resistant charge sharing mechanism is a suitable logic style for low-power applications.

References

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

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

[3] Cancio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine, “Survey on Secure Adiabatic Logic for Countermeasure against Side-Channel Attacks”, IEICE technical report. Electromagnetic compatibility 112(361), 2012.

[4] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, “Three-phase dual-rail pre-charge logic,” Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES ’06), Yokohama, Japan, Oct. 10–13, pp. 232–234.

[5] M. Khatir, and A. Moradi, “Secure adiabatic logic: A low-energy DPA-resistant logic style,” Cryptology ePrint Archive, Report 2008/123, 2008.

[6] Yomg Moon, and Deong-Kyon Jeong, “An Efficient Charge recovery logic circuit,” IEEE Journal of solid state circuits, vol. 31, no.4, Apr. 1996, pp. 514-522.

[7] Byong-Deok Choi, Kyung Eun Kim, Ki-Seok Chung, and Dong Kyue Kim, “Symmetric Adiabatic Logic Circuits against Differential Power Analysis,” ETRI Journal, vol. 32, no. 1, Feb. 2010, pp.166-168.

[8] Câncio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine, “Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level,” Microelectronics Journal, vol. 44, no. 6, June 2013, pp. 496-503

[9] C. Monteiro, Y. Takahashi, and T. Sekine, “A comparison of cellular multiplier cell using secure adiabatic logics,” Proc. Int. Conf. Circuit System, Computers and Communications (ITC-CSCC ’12), Sapporo, Japan, July 15-18, 2012.