International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 13, December 2016

ISSN: 2394-4404

A New Approach For The Design Of Low Power Dynamic Differential Logic For Secure Integrated Circuits

M. Pavitra

Associate Professor, ECE Dept., PBR VITS,
Kavali, Nellore (Dt.), AP, India

SK.Afrin

PG Scholar, DSCE, ECE Dept., PBR VITS,
Kavali, Nellore (Dt.), AP, India

Abstract: ***Production of cost effective secure integrated chips, such as smart cards, requires hardware designers to consider tradeoffs in size, security, and power consumption. To design successful security-centric designs, the low-level hardware must contain built-in protection mechanisms to supplement cryptographic algorithms, such as advanced encryption standard and triple data encryption standard by preventing side-channel attacks, such as differential power analysis (DPA). Dynamic logic obfuscates the output waveforms and the circuit operation, reducing the effectiveness of the DPA attack. For stronger mitigation of DPA attacks, we propose the implementation of adiabatic dynamic differential logic (ADDL) for applications in secure integrated circuit (IC) design. Such an approach is effective in reducing power consumption, demonstrated using HSPICE simulations with 22-nm predictive technology. Then, a high-performance ADDL is presented for an implementation in high-frequency secure ICs. This method improves the differential power over previous dynamic and differential logic methods by up to 76.41%.***

Index Terms: Adiabatic logic, Differential Power Analysis (DPA) attacks, Forward body biasing, Reversible logic.

I. INTRODUCTION

SMART cards are small integrated circuits (ICs) embedded onto plastic or tokens, and are used for authentication, identification, and personal data storage. They are used by the military, in automatic teller machines, mobile phone subscriber identity module cards, by schools for tracking class attendance, and storing certificates for use in secure web browsing. They are also used internationally as alternatives to credit and debits cards by Euro pay, MasterCard, and Visa. They are application specific, so their size and software overhead may be minimized. In addition, smart cards use tamper-resistant secure file cryptosystems. They are more difficult to forge than Tokens, Money, and Government issued identification cards [1].

They can be programmed to deter theft by preventing immediate reuse, making them more effective than cards with magnetic strips. Due to their emphasis on security at both the software and hardware levels, smart-card technology is emerging as the platform of choice in key vertical markets [10]. Smart-card technology is moving toward multiple applications, higher interoperability, and multiple interfaces, such as TCP/IP, near-field communicators, and contact less chips.

Due to their recent proliferation, smart cards are targets of attacks motivated by identity theft, fraud, and fare evasion. Despite their secure software design, smart cards may still be susceptible to side-channel attacks, which are based on correlations of leaked secondary information and the IC output signals. In smart cards, these include electromagnetic emanations (EM leakage) [2], measuring the amount of time required to perform private-key operations [3], and analysis of noisy power consumption.

One of the most effective attacks is a differential power analysis (DPA) attack [5], where the attacker analyzes the power consumption in the IC and compares it to the ICs output signals. The leaked side-channel information is due to the presence of entropy gain in the system. These attacks are effective, since most modern computing technology is CMOS based, and the power consumption tendencies of these devices are well studied. Reducing the power consumption of the circuit makes a DPA attack more difficult.

Reversible logic is a promising design paradigm for the implementation of ultralow power computing structures with minimal entropy gain [7]. This is because quantum mechanics principles govern the physical limitations of computing devices. These systems dissipate energy due to bit erasure within their interconnected primitive structures, which is an important consideration as transistor density increases. Adiabatic logic is an implementation of reversible logic in CMOS where the current flow through the circuit is controlled such that the energy dissipation due to switching and capacitor dissipation is minimized [13]. This is accomplished by recycling circuit energy rather than dissipating it into the surrounding environment. This is beneficial for CMOS implementations, since the input and output charges are kept separate. Adiabatic logic implementations of CMOS have been used to improve power consumption in comparison to pass transistor logic [9].

In this paper, we propose the use of performance of adiabatic dynamic differential logic (PADDL) for reducing the effectiveness of DPA attacks on CMOS based secure IC devices.

In Section II, we present the motivation and back-ground for low-power secure IC design. First, the methods for implementing a DPA attacks are discussed. Next, we review the previous method of mitigating these attacks, such as secure differential multiplexer logic using pass transistors (SDMLp) [6].

In Section III, we present design and analysis using high-performance adiabatic dynamic differential logic (PADDL) for mitigating DPA attacks, which is a novel universal cell that performs AND, NAND, OR, NOR, XOR, and XNOR operations. The average power of the PADDL is compared with the SDMLp. The PADDL is used to improve the operating frequency of ultralow power devices.

II. MOTIVATION AND BACKGROUND

A. SECURE INTEGRATED CHIP DESIGN

Smart cards consist of a secure integrated chip, which contains the main processor, arithmetic logic unit, processing registers, random access memory for arithmetic processing, read-only memory (ROM) for storing the operating system, and electrically erasable programmable ROM for data memory. The operating system controls data access and implements the cryptographic security algorithms. The international standard for contact-based smart cards electronic identification cards is the ISO/IEC 7816 [10],

In this standard, smart cards use the triple data encryption standard (DES).

B. DPA ATTACKS

Since the design of smart cards has been standardized, and their development is moving from single issuer models to cooperative private–public sector partnerships, a two-prong approach to smart card security is required: software-systems security and hardware-oriented security. Even though smartcards utilize operating systems with cryptographic kernels, the memory devices used to store them are not isolated in perfectly tamper-proof locations. As a result, analysis of a chip's operation metrics, such as differential power consumption, total execution time, magnetic field values, and radio frequencies allows attackers to gain sensitive user data. The effectiveness of these side-channel attacks was demonstrated in [5]. Kocher demonstrated in [3] that attackers may be able to find fixed Diffie-Hellman exponents, factor Rivest-Shamir-Adleman (RSA) keys, and break other crypto systems by analyzing power consumption and private key execution time.

The use of power consumption to obtain compromising information is known as a DPA attack. The attacker analyzes information gleaned from the practical implementation details of otherwise secure algorithms [4]. Most modern computing systems use CMOS technology, and the dynamic power consumption of a CMOS gate is proportional to its input signals, Analyzing the output power consumption allows the attacker to determine a correlation between the data and the key, since the switching in the CMOS gates is dependent on those inputs.

C. DPA PREVENTION

The primary drawback with addressing DPA attacks at the software level is that the power and current variations being analyzed by attacker occur at the hardware level, and no software algorithm, however effective, can affect the operation of a CMOS gate once it receives an input signal. For example, inserting random process interrupts to prevent sequential operation of an algorithm [11] may be circumvented by resynchronization and integration techniques [4]. In addition, bit masking can be defeated using DPA attacks.

Therefore, the most effective approach to the prevention of DPA attacks is to include security-based logic within the hardware implementation itself to make it difficult for the attacker to ascertain the necessary information to determine the inputs. The three most important metrics to consider while designing CMOS circuits for this purpose are power consumption, area, and operating frequency, since $Ediss = CL * V\ dd\ \hat{}2 * f$, where CL is the load capacitance, Vdd is the supply voltage, and f is the operating frequency.

D. ADIABATIC LOGIC IN CMOS

The adiabatic theorem states that a physical system remains in its instantaneous Eigen state if a given perturbation is acting on it slowly enough and if there is a gap between the Eigen value and the rest of the Hamiltonian's spectrum [16]. Since CMOS circuits operate on clock cycles, adiabatic logic design results in a gauge-invariant Berry phase. Normally, when waves are subjected to variations that are self-retracting, then the initial and final states of the system will differ. To prevent this, adiabatic systems are designed reversibly so that the system may always reach its initial state, regardless of the number of cycles it operates. Therefore, the objective of adiabatic logic design is to use the principles of reversible logic to minimize energy dissipation in CMOS circuits.

There are two issues that must be addressed in any adiabatic circuit. First, the implementation must result in an

energy efficient design of the combined power supply and clock generator. Second, reversible logic functions require greater logical overhead to meet the bijective requirement [14]. Therefore, the energy dissipated by switching of the circuit must be controlled and recycled instead of dissipated into the environment.

III. EXISTING METHODS (SDMLp)

OVERVIEW

Existing method is a new logic style called "Secure Differential Multiplexer Logic (SDMLp) [6]". SDMLp is a dynamic differential logic that is weakly based on complementary pass transistor logic. It is a universal two input cell that can be configured to perform any two input operation. In general there are 16 operations that can be performed on two inputs.

GATE ARCHITECTURE

The novel cell design, as shown in Figure 1, the circuit shown has two main functions, the first is to realize any two input function, this is achieved with implementing two Multiplexers using transistors m1, m2, m7, and m8 and applying the appropriate gate. Secondly, the cell is capable of generation and transmission of a pre-discharge wave using the four PMOS transistors m3, m4, m9, and m10. It is important to note that the gate terminal connection of all the pass transistors is either connected to S or Sbar irrespective of the function implemented by the circuit. Furthermore, the series PMOS pass transistors. Responsible for the pre-discharge wave are connected to Vdd.

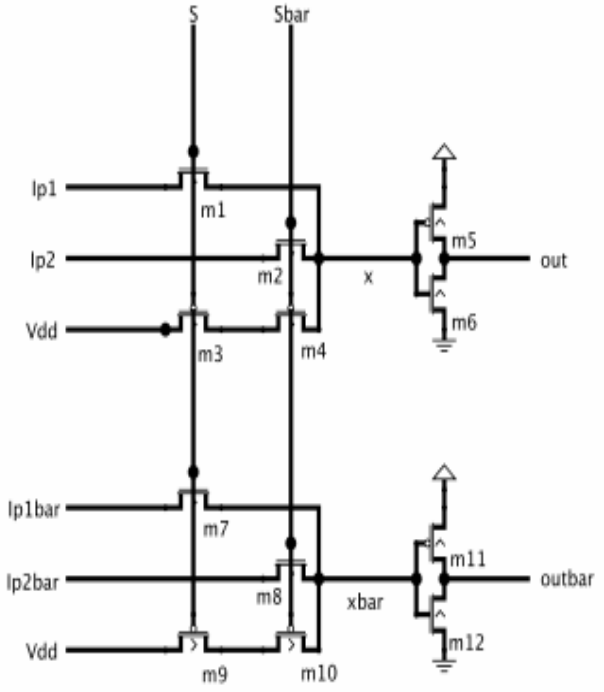


Figure 1: SDMLp Gate Structure

This gate is different from typical Complementary / Differential pass transistor logic (CPL). In CPL, the outputs are complementary to each other at every instant of time. Whenever out switches to a value (0 or 1), Outbar switches to the opposite value (1 or 0). In out logic (SDMLp), the outputs are not always complementary to each other. During pre-discharge phase both outputs are forced 0 and on evaluation only, one of these signal switches to the value 1 while the other remains at 0. In this way, we have exactly one transition (Out or Outbar). Additionally, when there is no activity, CPL retains its complementary output value, unlike SDMLp in which there is a transition in every clock cycle making it's a dynamic differential logic.

It is interesting to observe that the implementation of a circuit using complementary logic degrades the power invariance while the implementation of the circuit using differential logic improves it. The above statement can be supported by the following argument.

CASES 1: In a complementary logic when a signal in uncomplementary logic switches, the signal in complementary logic also switches consuming huge power (i.e, dual switching during transition of uncomplementary logic).

CASE 2: When there is no transition in uncomplementary logic, there is no transition in complementary logic as well thus no power is consumed. Thus there is a huge difference between the two cases clearly indicating whether or not there was a transition in the gate thus worsening power invariance.

In a differential logic only one of the signal (either complementary or uncomplementary) switches. If there is a switching in uncomplementary logic there is no switching in complementary logic and vice versa. So this insures that there is always one transition in the circuit whether or not the circuit or gate changes state in reality. This highly improves power invariance thus making the circuit robust against differential power analysis attacks.

OPERATION PRE-DISCHARGE AND EVALUATION PHASES

During every clock cycle, a SDMLp cell will go through two phases of operation namely a pre-discharge phase and an evaluation phase as discussed below.

PRE-DISCHARGE PHASE: The pre-discharge wave generation circuit used in our logical style is basic and straight forward the interested reader can refer to as fundamental principles in both designs are similar. During the pre-discharge phase of operation the pass transistors gate control inputs, S and Sbar, are both held at logic zero. This forces the NMOS transistors (m1, m2, m7and m8) to stop conducting and the PMOS transistors (m3, m4, m9 and m10) conduct thus forcing both the outputs Out and Outbar to zero.

This simultaneous zero output from both the Out and Outbar can be used as S and Sbar control signals for the next level of cells. And thus the pre-discharge wave propagates. The pre-discharge wave signal generation is ensured at primary inputs and outputs of intermediate registers alone, and is generated using a periodic clock at considerably high frequency.

EVALUATION PHASE: Since the basis of our logic is a pair of complementary multiplexers, shown in Figure 1, a total of 16 two-input functions can be realized. The combination of signals A, B, Abar and Bbar given to the four input terminals,

ISSN: 2394-4404

as well as the two select lines S and Sbar, determines the operation or function implemented by the cell. It is made sure that the inputs to the cell are differential in nature.

Usually the inputs to the gate are from the output of another SDMLp gate or from the differential signal generating gates at the output of registers. For all functions the pre-discharge logic remains the same with the PMOS transistors connected to S and Sbar respectively.

The advantage of this universal cell based design is that every cell in the library will have the same characteristics. This means every two input gates or function (AND, OR, XOR, NOR, NAND, XNOR, MUX) has an identical power profile. They have the same delay and have almost equal current variance values. While this particular feature may not be interesting or important in general IC design, when it comes to secure IC design this fundamental property in the SDMLp library may be helpful for building efficient and power invariant architectures based on power hiding.

F	F bar	IP1	IP2	S	Out	Outbar
AND	NAND	A’	B’	B	A.B	(A.B)’
OR	NOR	B’	A’	B	A+B	(A+B)’
XOR	XNOR	A	A’	B	A.B’+A’ B	(A.B’+A’ B)’
INHIBITION	IMPLICATION	A	B’	B	A’.B	A+B’
IMPLICATION	INHIBITION	B’	A	B	A’+B	A.B’
BUFFER	INVERSION	A’	A’	A	A	A’
ONE	ZERO	GND	GND	VDD	VDD	GND

Table 1: Configuring SDMLp cell to implement various logic

Table I. shows the input configuration that needs to be applied for the six input terminals for implementing a particular type of gate or function. The table explains configuration only for the uncomplementary section. The inputs for the complementary section are exactly inverted signal of the uncomplementary section. The input A and B can be completely interchanged and the gate would still implement the same logic.

IV. PROPOSED PADDL CELL

The Proposed method for the implementation of performance of adiabatic dynamic differential logic (PADDL) design methodology for mitigating DPA attacks in high performance applications. The data presented in this section was obtained using HPSICE simulations using the 22-nm predictive technology model presented in [15].

The objective of PADDL is to design as a universal cell capable of dynamically performing all of the fundamental two-input logical calculations (AND, NAND, OR, NOR, XOR, and XOR) with the minimal differential power for each logical calculation. The device is both logically and physically bijective. This means that the input may be uniquely determined by reading the output, a necessity in implementation of low-power reversible and adiabatic designs.

The logical cell calculations of the outputs signals of PADDL cell

P = A’,
P’ = A,
Q = ((A + B) ⊕C)’,
Q’ = (A + B) ⊕C,
R = (AB ⊕C)’, and
R’=AB⊕C

A	A’	B	B’	C	C’	P	P’	Q	Q’	R	R’
0	1	0	1	0	1	1	0	1	0	1	0
0	1	0	1	1	0	1	0	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0
0	1	1	0	1	0	1	0	1	0	0	1
1	0	0	1	0	1	0	1	0	1	1	0
1	0	0	1	1	0	0	1	1	0	0	1
1	0	1	0	0	1	0	1	0	1	0	1
1	0	1	0	1	0	0	1	1	0	1	0

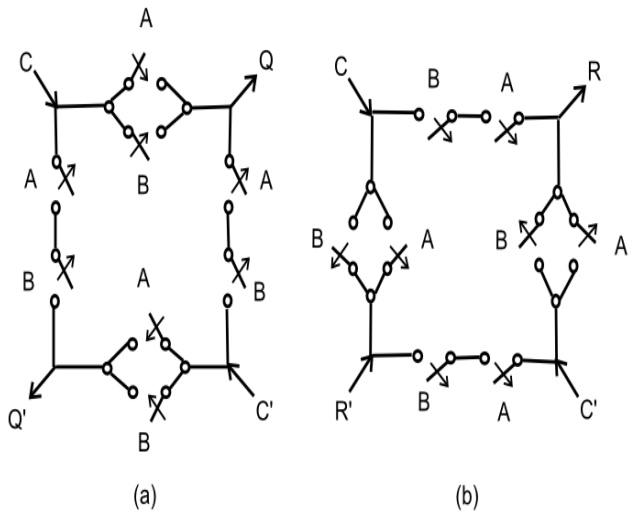
Table 2: Truth Table for Proposed PADDL Cell:

Control Signal	P	P’	Q	Q’	R	R’
A=0	A'	A	$\overline{B \oplus C}$	$B \oplus C$	C'	C
A=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
B=0	A'	A	$\overline{A \oplus C}$	$A \oplus C$	C'	C
B=1	A'	A	C'	C	$\overline{B \oplus C}$	$B \oplus C$
C=0	A'	A	$\overline{A+B}$	$A+B$	$\overline{AB}$	AB
C=1	A'	A	$A+B$	$\overline{A+B}$	AB	$\overline{AB}$

Table 3: PADDL Cell Logic Output:

The truth table of the proposed PADDL cell as shown in Table II, and the logic outputs of PADDL are presented in Table III. Figure 2 shows the design process of the PADDL cell. The objective of the basic square circuit diagram is to determine the switches required for an input signal to flow from an input to an output.

Consider Figure 2(a) in order for the output Q to be 1 when input C is a 1, either A or B must be a 1, which would close the switch. The circuit diagram shows whether the switch will open or close when the appropriate input signal is a 1. The output Q is determined in figure 2(a) and the output R is determined in figure 2(b).



(a) Logical calculations for the Q and Q’outputs based on the A, B, and C inputs.

(b) Logical calculations for the R and R'outputs.

Figure 2: Basic square circuit diagram for the proposed PADDL cell

The PADDL circuit does not require any overhead for maintaining evaluation and discharge phases, making it the better cell for larger implementations, such as DES circuits. However, improving the area of the PADDL device is important.

In addition, PADDL does not require additional evaluation and discharge signals to generate the results further in the cascade. Every cell in the other methods requires a unique evaluation and discharge signal. This means that the overhead required to manage the input and output signals is significantly reduced.

This is beneficial, since DPA mitigation methods have difficulty propagating the signal though the circuit due to signal degradation. The PADDL approach uses the existing signals for evaluation and discharge, which is advantageous over SDMLp. Therefore, even though the transistor count is higher in PADDL, the added power required to generate the evaluation and discharge signals in the other methods makes a DPA attack easier.

Figure 3 shows the gate level design of the PADDL cell derived from the basic square circuit diagram. The device as 32 transistors, each of which have their gate, drain, and source tied to an input or output signal. The pMOS transistors are biased to the nominal supply voltage, which is 0.8 V in the 22-nm model in [15], and the nMOS transistors are biased to ground. The advantage of this approach is that evaluation and discharge signals are not required, meaning that less power is consumed by the circuit, even though the device has more transistors.

The arrows in the basic square diagram indicate what will occur if the signal shown is a logic 1. For example, in Figure 2(a), if A is a logic1, then there exists a path from C to Q, meaning that the logical values of C and Q will be equivalent. This is because the pMOS / nMOS pair will have the nMOS with 1 and the pMOS with 0 and the path will be activated. In Figure 2(b), the path from C to R will be switched OFF if A or B is 1. This is because the pMOS / nMOS pair will have the nMOS with 0 and the pMOS with 1. Therefore, to have C equal to R, then A must be 0, and B must be 0.

The operation of the PADDL logic output as shown in figure 6,The average power of the PADDL device is 1.2456*10−5 W. The Total memory of the PADDL cell is used 317000 bytes. The PADDL cell 32 transistors required for universal. The PADDL cell an improvement of 76.41%. In figure 6 is the output PADDL cells in different combinational logic outputs, show the different inputs A and A', B and B', and C and C' are input logics, for different outputs Q and Q', R and R' output logics respectively .

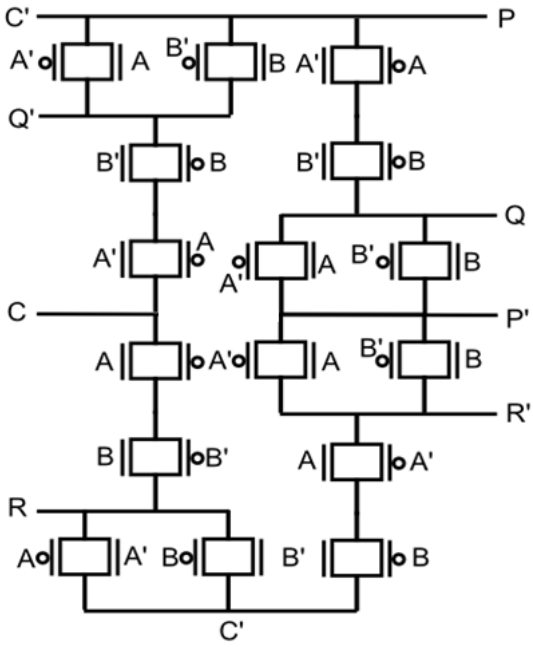


Figure 3: CMOS schematic diagram for proposed PADDL cell

A. NOTE ON BIJECTIVITY IN SECURE IC DESIGN

The PADDL cell is bijective, so the input signals maybe uniquely determined by studying the output signals. In this Case, the functionality of the cell can be easily determined by studying the output. This circuit is a 3*3 dual-rail device, so the function may easily be determined by reading 2^3 input signals. However, since the PADDL cell is universal, it may be combined with other PADDL cells to generate larger circuits, complicating the effectiveness of this strategy. For example, a three-input NAND gate would require seven inputs, since it requires two cascaded PADDL cells, as shown in figure 4. Therefore, instead of only needing to read eight outputs, an attacker would have to consider 512 inputs to properly ascertain the circuit's functionality. Furthermore, the triple DES uses a cipher key size of 56 bits, meaning that an attacker would have to analyze 7.2057*10^16 output signals to properly reverse engineer the circuit.

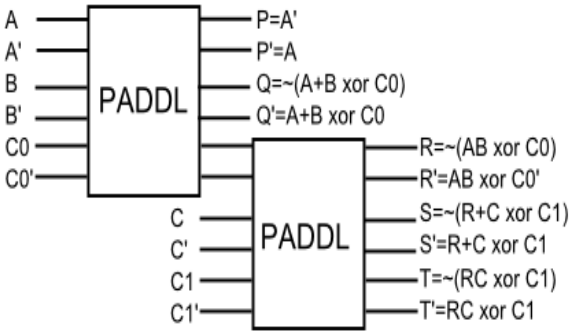


Figure 4: Cascaded PADDL cells with logic outputs show

V. SIMULATION RESULTS

The Proposed method has been demonstrated by using HSPICE simulated with 22 nm predictive technology. Results

are very much evident that, proposed method has yielded better results compared to existing method even under the more number of transistors required. Proposed method performance of Adiabatic Dynamic Differential Logic (PADDL) cell compared with Secure Differential Multiplixer Logic using pass transistors (SDMLp) the average power is reduced.

The presented PADDL design is advantageous to the previous design in average power for each of the fundamental calculations AND, NAND, OR, NOR, XOR, and XNOR. PADDL improves upon SDMLp by 76.41%. The implementation of SDMLp is the previously best implementation, since it uses evaluate and discharge phases. Figure 5 consists of SDMLp logic gate output, observed at the different logic gates. Figure 6 consists of PADDL for logic gate output, observed at the different logic gates.

SDMLp is advantageous in terms of required transistors, since implementation of SDMLp requires 16 transistors as opposed to the 32 transistors needed in our proposed implementation. However, this advantage is erased when cascading the cells together. The hardware overhead required ensuring proper timing of evaluation and discharge stages of each cell increases exponentially as the length of the critical path of the device increases.

Figure 5: SDMLp Logic Cell Output

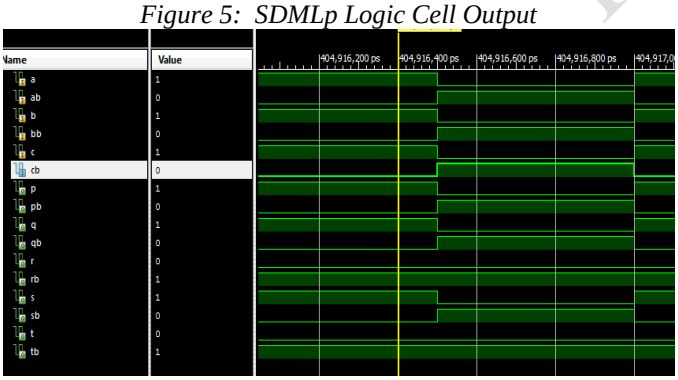


Figure 6: PADDL Logic Cell Output.

VI. CONCLUSION

In this paper, a new approach is proposed an ADDL design methodology for mitigation of DPA attacks on secure integrated chips. To consider the tradeoff in performance and average power consumption. Simulation results clearly shows that the proposed method is much better in reducing the average power when compared with the existing method. As shown in table IV for comparison between SDMLP and PADDL cell.

Logic	SDMLp	PADDL
Avg. Power (10-5 w)	4.2952	1.2456
Transistors required for Universal	16	32
Total Memory cell (Byte)	166000	317000

Table 4: Comparison between SDMLp and PADDL cell

REFERENCES

[1] N.O.Attoh-Okine and L.D.Shen "Security issues Of emerging smart cards fare collection applic-ation in mass transit, "in Proc. Veh. Navigat. Inf. Syst. Conf., jul./Aug. 1995, pp. 523-526.

[2] D.Agrawal, B.Archambeault, J.R.Rao, and P.Ro-hatgi, "The EMside-Channel(s),"in Cryptographic, Hardware and Embedded Systems. London U.K: Springer-Verlag, 2003, pp. 29–45.

[3] P.C. Kocher, "Timing attacks on implementations Of Diffie-Hellman, RSA, DS, and other systems, "in Advances in Cryptology. London, U.K.: Spri- nger Verilag, Aug. 1996, pp. 104–113.

[4] C.Clavier,J.-S.Coron,andN.Dabbous,"Differential power analysis in the presence of hardware coun-ter measures," in Cryptographic Hardware and Embedded Systems. London, U.K.: Springer-Ver-lag, Aug. 2000, pp. 252–263.

[5] P.Kocher,"Differential power analysis,"Advancesin Cryptology (Lecture Notes in Computer Scien-ce), vol 1666.Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.

[6] L.N.Ramakrishnan, M.Chakkaravarthy, A.S.Man-chanda, M.Borowczak, and R.Vemuri, "SDMLp: On the use of complementary pass transistor logic for design of DPA resistant circuit," in proc. IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST), Jun. 2012, pp. 31–36.

[7] C.H.Bennett, "Logicalreversibilityof computation" IBM J.Res.Develop., vol. 17, no.6, pp. 525–532, 1973.

[8] T. Toffoli, "Reversible computing," Lab. Comput. Sci., Massa chusetts Inst. Technol, Cambridge, MA, USA, Tech. Rep.TM-151, 1980.

[9] T.Hisakado, H. Iketo, and K. Okumura, "Logically reversible arithmetic circuit using pass- transistor," in Proc. ISCAS, vol. 2. May 2004, pp. 853–856. Internation Standard Organization, document ISO-IES 7816.

[10] J. Daemen and V. Rijmen, "Resistance against implementation attacks: A comparative study of the AES proposals," in Proc. 2nd Adv. Encrypt-ion Standard (AES) Candidate Conf., Mar.1999.

[11] S.Chari, C.S.Jutla, J.R.Rao, and P.Rohatgi "To-wards sound approaches to counteract power-an alysis attacks," in Proc. 19th Annu. Int. Cryptol. Conf., vol. 1666, Aug. 1999, pp. 398–412.

[12] S. G. Younis, "Asymptotically Zero Energy Com-puting using Split-Level Charge Recovery Logic", D.dissertation, Dept.Electr. Eng.Comput. sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Jun. 1994.

ISSN: 2394-4404

[13] W.C.Athas and L.J.Svensson, "Reversible logic issues in adiabatic CMOS," in Proc. Workshop Phys. Comput., Nov. 1994, pp. 111–118.
[14] PTM 22 nm HSPICE Model. [Online]. Available: http://ptm.asu.edu/modelcard/HP/22nm_HP.pm, accessed Jul. 15, 2013.
[15] M. Born and V. A. Fock, "Beweie Adiabatensatzes" Zeitschriftfür Phys.A, vol. 51, nos. 3–4, pp.165–180, 1928.