ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Power Analysis on Boolean and Arithmetic Masking in Randomized Multi-Topology Logic

Ranjani A[1]
Electronic and communication engineering
Parisutham Institute of Technology and Science,
Thanjavur, Tamil Nadu, India

Poornima U[2]
Assistant Professor
Electronic and communication engineering
Parisutham Institute of Technology and Science,
Thanjavur, Tamil Nadu, India

Abstract: In cryptography power analysis is from the side channel attacks to analyze the power by using the Randomized multi-topology logic (RMTL). RMTL family is used for security oriented gates power profile can be predict from exterior observer and each gate having different power profile. DPA attack is obtained while changing the different topology. In this paper randomized multi-topology logic (RMTL) is proposed to enhance immunity to DPA. Each topology consumes different power while using in the system. RMTL reduces input power, area by choosing the suitable logic styles like dynamic domino logic, pass transistor logic, transmission gate logics, dual rail domino logics and identifies the low power gate .In AES, substitution box we are using RMTL logic to prevent the side channel attack and analysis the power.

Keywords: RMTL, Differential power analysis, Advanced encryption standard, substitution box, power consumption.

I. Introduction

RMTL gate is a gate that can be arranged dynamically to operate in one of several topologies. Each topology implemented accurately the same logic function, but different power profile. The RMT Logic gate has more data inputs and single control signals that determine the gate's exact topology. In RMTL, random number generator (RNG), allow real time random switching between different topologies of RMTL gates. Several RMTL gates into the circuit, the power profile become chance. This leads to improved immunity to power attacks.

DPA is aside channel attack which involves statistically power consumption measurement from a cryptosystem. The attack exploit biases varying power consumption of microprocessor or other hardware while performing operation through secret key.DPA attack having signal processing and error correction properties which can extract secret from measurement which can contain too much noise to be analyze using simple power analysis. Using DPA a contestant can contain secret key by analyze the power consumption measurement from multiple cryptographic operation perform by a vulnerable smart card or other device.

In AES, based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is speedy in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a swap of Rijndael which has a fixed block mass of 128 bits, and a key size of 128, 192, or 256 bits. By difference, the Rijndael condition is specified with block and key sizes that may be any multiple of 32 bits, both with a least of 128 and a extreme of 256 bits.AES operates on a 4×4 column-major order matrix of bytes, termed the order although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are completed in a special finite field .The key size used for an AES cipher specify the number of repetitions of transformation rounds that convert the input, called the plaintext, into the concluding output, called the cipher text. The number of cycles of repetition is as follows:

10 cycles of replication for 128-bit keys

12 cycles of replication for 192-bit keys

14 cycles of replication for 256-bit keys

Each round consists of several processing steps, each containing four related but varied stages, including one that depends on the encryption key itself. A set of repeal rounds are applied to transform cipher text back into the original plaintext using the same encryption key .In this paper AES used for the analyze power.

II. Back Ground

[1] Security problem based on ring oscillators is resolved by a new architecture with self-generated true random sequence. A novel low-transition linear feedback shift registers (LFSR) that is based on some new observations about the output sequence of a predictable LFSR. It ensures the safe and secured encryption and decryption method. Security is provided for the AES algorithm by counter measure circuit. This process provides higher security. This method is extended by bit swapping LFSR and it is used in countermeasure circuit and this method reduces the area and power consumption.

[2] AES is a 128 bit Symmetric block cipher which is based on a design principle known as a Substitution permutation network. Power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device (such as a smart card, tamper-resistant "black box", or integrated circuit). The attack cans non-invasively extra cryptographic keys and other secret information from the tool. Differential power analysis (DPA) is a side-channel attack which involves statistically analyzing power consumption from a cryptosystem. Several methods have been proposed in literatures to resist the DPA attack in cryptographic device, but they mainly increase the hardware cost and severely degrade the throughput. In accessible system, the security problem is resolved by a new architecture with self generated true random sequence. DPA countermeasure circuit can successfully reduce the area overhead and throughput degradation.

[3] A novel countermeasure technique against power analysis attacks is proposed which dynamically varies the clock when executing operations (making it difficult to correlate power traces in the time domain) and inserts dummy operations during idling clock cycles (reducing the signal-to-noise ratio of the useful in sequence). Its efficiency is shown by performing a DPA attack on basic, intermediate (random clock) and highly developed (random clock and dummy data) designs for the AES encryption algorithm, implemented on a FPGA-based board. The design among this is resistant to classical DPA attacks and the advanced design reduces the SNR by 79% (increasing area by 70% and reducing performance by 5.33%) when compare to the basic design. It is shown that the design is improved in both metrics than other countermeasure techniques.

[4] A general model of differential power analysis (DPA) attacks to static logic circuits. Focus on symmetric-key cryptographic algorithms, the proposed analysis provides a deeper insight into the vulnerability of cryptographic circuits. The major parameters that are of interest in practical DPA attacks are derived under suitable approximations, and anew fig of merit to measure the DPA effectiveness is proposed. Most horrible case conditions under which a cryptographic circuit should be tested to evaluate its robustness against DPA attacks are recognized and analyze. Several interesting properties of DPA attacks are also derived from the future model, whose fundamental expressions are compared with the counterparts of correlation power analysis attacks. The model was validated by way of DPA attacks on an FPGA implementation of the advanced encryption standard algorithm. Experimental outcome show that the model has a good accuracy, as its error is always lower than 2%.excellent accuracy and security; it had delay time is more.

[5] The `Boolean to Arithmetic' algorithm is not sufficient to prevent Differential Power Analysis. Two different kinds of masking is used. There is thus a need for a method to alter back and forth between Boolean masking and arithmetic masking.AES algorithm is used for decrease the memory and execution time it had only used in 2bits DPA.

III. Existing System

RMTL approach is used to prevent an undesirable outcome in the process from DPA attacks. RMTL logic gates can minimize the correlation between leakage and the information by randomly changing their topologies. Each gate of this logic can be configd in real time to operate in a different circuit topology, where each topology induces a different power profile.

2.2.1 General concept of RMTL

An RMTL gate is a gate that can be configd dynamically to operate in one of several topologies. Each topology implements exactly the same logic function, but has a different power profile. The RMTL gate has n data inputs and q control signals that determine the gate's specific topology. Sequence generators, such as Random Number Generator (RNG), allow real time random switching between different topologies of RMTL gates. By incorporating several RMTL gates into the circuit, the power profile becomes random. This leads to improved immunity to power attacks.

In general, each one of the RMTL topologies can be implemented using existing static and dynamic logic families, such as CMOS, PTL, differential PTL, dynamic logic, differential dynamic logic, domino, or any other logic family.

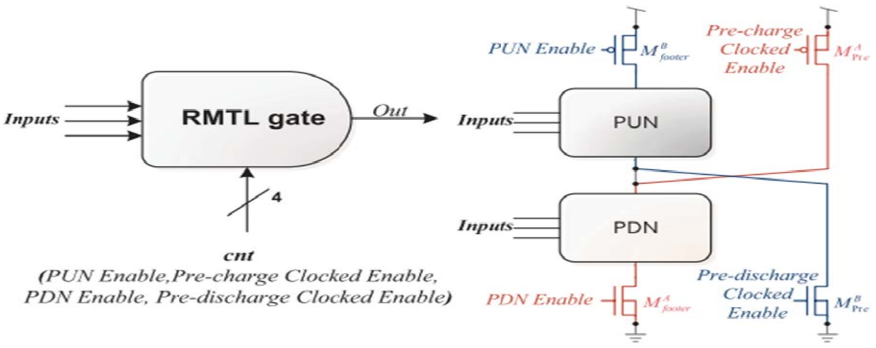


Fig1. Basic RMTL

However, it is important to make sure that the power profile of each topology for the same input sequence is totally different. It is clear that straightforward integration of a number of logic families into a single RMTL gate will not be efficient in most cases, because it will significantly increase the area and power dissipation of the gate.

The gate is based on standard CMOS logic with Pull-Up Network (PUN) and Pull-Down Network (PDN), with the addition of four transistors. As shown in the Fig.2.1. To determine the right topology, a control bus consisting of four control signals, is used.

IV. Proposed System

In this paper RMTL (Randomized Multi-topology logic) gate uses different topologies. Each topology consumes different power attacks. It reduces input power, transistor count and identifies the low power gate. That low power gate will be used in substitution box. S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to difficult to understand the relationship between the key and the cipher text**.**

In general, each one of the RMTL topologies can be implemented using static and dynamic logic families, such as CMOS, PTL, differential PTL, dynamic logic, differential dynamic logic, domino, Pseudo**,** conventional dynamic logics, standard dynamic logics, Cascade Voltage Switch Logic (CVSL). The structure of the gate enables the implementation of five different Topologies A, B, C, D, and E.

Topology A is very similar to a standard static CMOS topology. Topologies B and C are the conventional dynamic logics with precharge and predischarge configurations, respectively. Topologies D and E are nonstandard dynamic logics with precharge and predischarge configurations, which also include complementary PUN and PDN networks, respectively. To operate the gate in Topology A the Precharge Clocked Enable and the Predischarge Clocked Enable signals are permanently set to 1 and 0, respectively, and PDN Enable and the PUN Enable signals are permanently set to 1 and 0 respectively. This way the gate operates similarly to a CMOS gate. For the dynamic topologies (Topologies B, C, D, and E), the Precharge Clocked Enable and Predischarge Clocked Enable signals are assigned an asymmetric clock that activates two distinct phases: Precharge (or Predischarge) and evaluation. During the Precharge (or Predischarge) phase, the output is charged to high/low, depending on the topology of the RMTL gate. In the subsequent evaluation phase, the output is evaluated according to the values at the gate inputs. The operation of the RMTL gate in Topologies B and C are identical to conventional dynamic gates with footers, Topologies D and E are slightly different from standard dynamic logic since both the PUN and PDN networks are active during the evaluation phase. Topology D is the dynamic precharge topology that incorporates the PUN network. Topology E is the dynamic predischarge topology incorporating the PDN network.

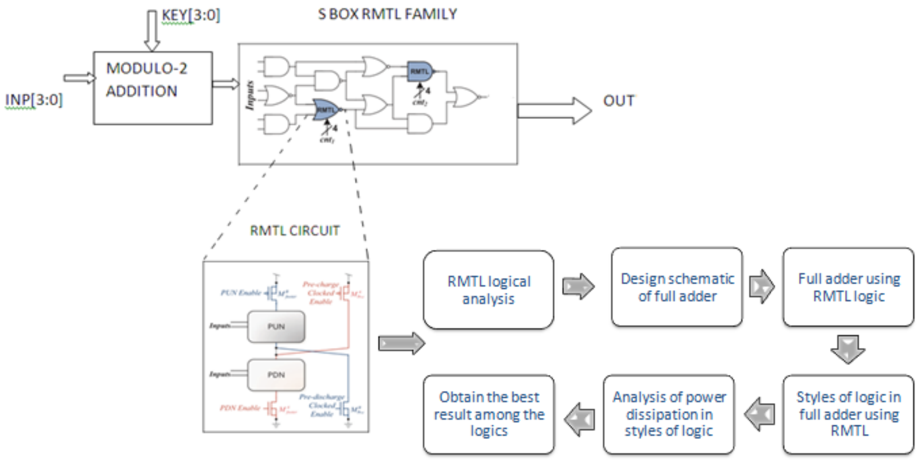

KEY[3:0]
S BOX RMTL FAMILY
INP[3:0]
MODULO-2 ADDITION
Inputs
RMTL
OUT
RMTL CIRCUIT
PUN Enable
Pre-charge Clocked Enable
Inputs
PUN
PDN
PDN Enable
Pre-discharge Clocked Enable
RMTL logical analysis
Design schematic of full adder
Full adder using RMTL logic
Styles of logic in full adder using RMTL
Analysis of power dissipation in styles of logic
Obtain the best result among the logics

Fig2. Architecture Diagram

The signals Precharge Clocked Enable and PDN Enable are identical. Note that the signals Predischarge Clocked Enable and PUN Enable are the same as well. Obviously, the power profile and total energy consumption of each topology differ from each other even for the same data flow.

a) Modulo 2 addition

Modulo 2 addition is performed using an exclusive OR (xor) operation on the corresponding binary digits of each operand. The following table describes the xor operation.

A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Table1. XOR Truth Table

b) Substitution Box

4-bits are used as input for S-box module. The different locations of the RMTL gates are connected in each S-box module. The control buses of the S-box modules are fed from a control generator. Each consists of six control buses. Each control bus will have four control signals. This block is smaller, which enables reduced power and simulation time.

c) RMTL Logic

RMTL gate has n data inputs and q control signals that determine the gate's specific topology. Sequence generators, such as RNG, allow real time random switching between different topologies of RMTL gates. In CMOS designs, two transistor structures one PMOS and one NMOS. Structure of the gate enables the implementation of five different Topologies A, B, C, D, and E.

V. Tools Used

As the technology in electronic circuits is improving, the difficulty in these circuits also increases. The difficulty in the circuits leads to the require of that type of circuits which are portable and rapid circuits. The portability in the electronic circuits are achieved by utilize of battery. So the authors have to develop such type of circuits that consume very less power. The major focal point in designing a high performance digital system such as microprocessors and various digital signal processors is given to low power design. The major part of any digital system is its memory unit. Tanner is use for analysis the power and compares the power in the different topologies.

VI. Result

In this paper tanner software is used for analyzing power. There are five different types of logic has been used and the logic is represented as topology A, topology B, topology C, topology D, topology E. The five topologies have consumed different power and compare the power.

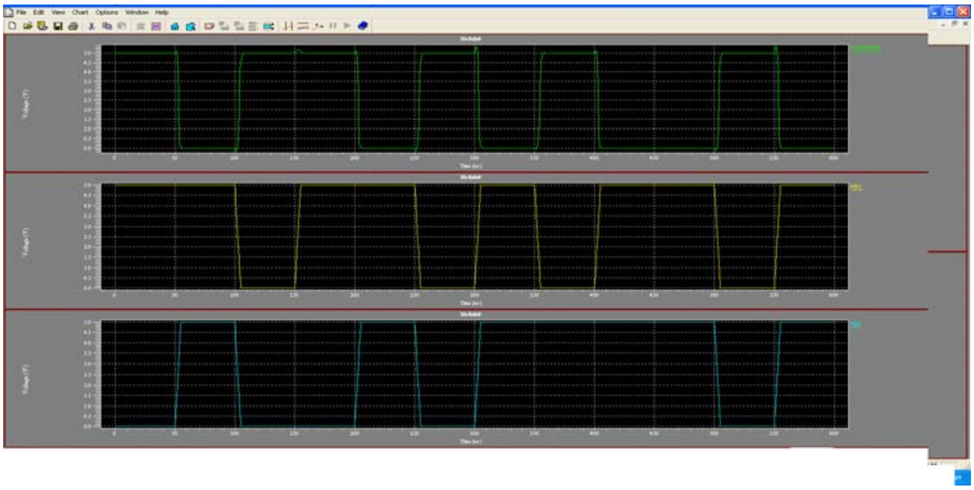
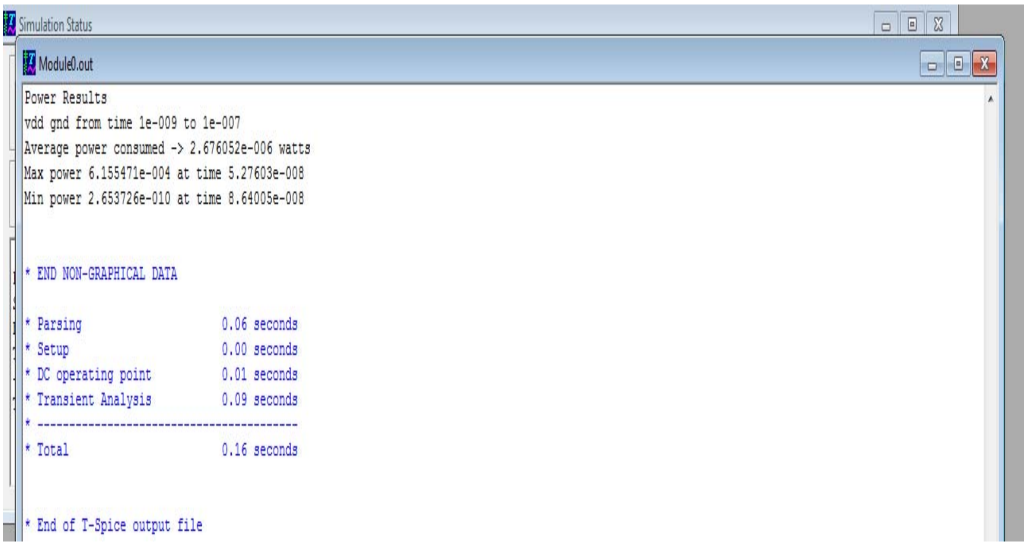


Fig.3 Simulation result for Topology A

Topology A (fig 3.1) is static logic. If the input is high means precharge clock & predischarge clock are disable and pullup transistor & pulldown transistor are enable.



```
Power Results
vdd gnd from time 1e-009 to 1e-007
Average power consumed -> 2.676052e-006 watts
Max power 6.155471e-004 at time 5.27603e-008
Min power 2.653726e-010 at time 8.64005e-008


* END NON-GRAPHICAL DATA

* Parsing                    0.06 seconds
* Setup                      0.00 seconds
* DC operating point         0.01 seconds
* Transient Analysis         0.09 seconds
* -----------------------------------------
* Total                      0.16 seconds


* End of T-Spice output file
```

Fig.4 Power consumption of Topology A

In Fig3 represent the power consumption of static logic. In that we have identified minimum power, maximum power and average power according to the input, power consumption can be change.

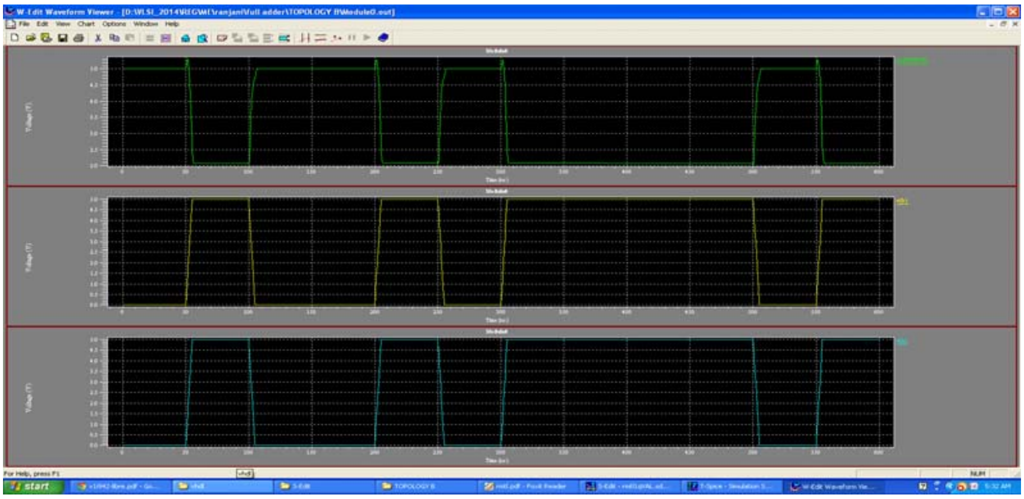
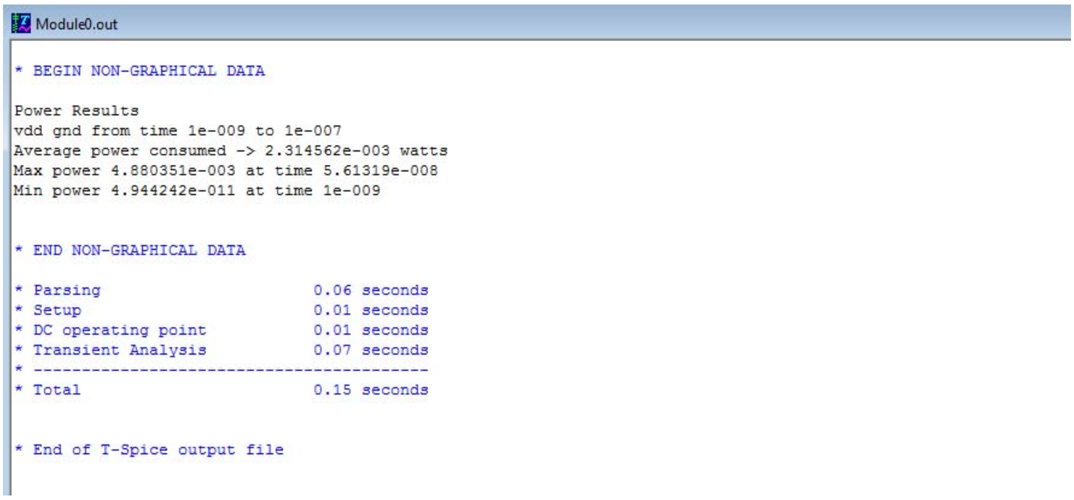


Fig.5 Simulation result for Topology B

Topology B (fig.5) is conventional dynamic logics with precharge. If the input is high means precharge clock & pulldown transistor are disable and pull up transistor & predischarge are enable.



```
* BEGIN NON-GRAPHICAL DATA

Power Results
vdd gnd from time 1e-009 to 1e-007
Average power consumed -> 2.314562e-003 watts
Max power 4.880351e-003 at time 5.61319e-008
Min power 4.944242e-011 at time 1e-009


* END NON-GRAPHICAL DATA

* Parsing                    0.06 seconds
* Setup                      0.01 seconds
* DC operating point         0.01 seconds
* Transient Analysis         0.07 seconds
* -----------------------------------------
* Total                      0.15 seconds


* End of T-Spice output file
```

Fig.6 Power consumption of Topology B

In Fig.6 represent the power consumption of conventional dynamic logics with precharge. In that we have identified minimum power, maximum power and average power according to the input, power consumption can be changed.

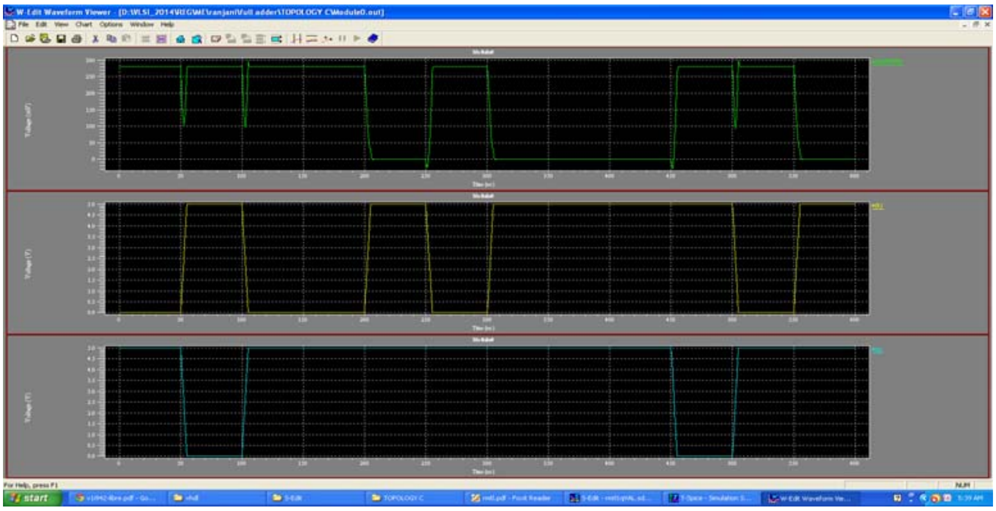
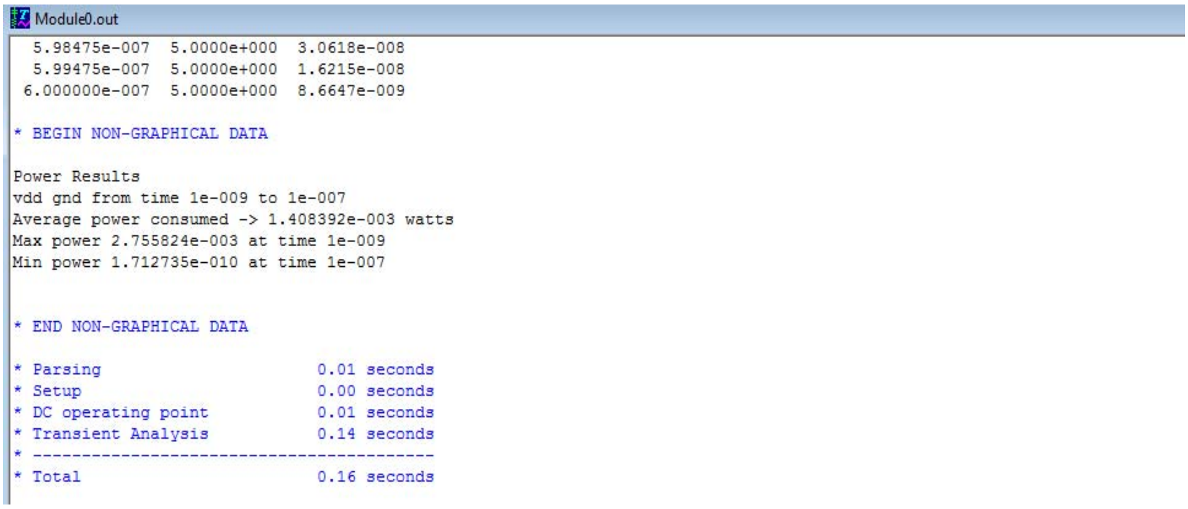


Fig.7 Simulation result for Topology C

Topology C (fig.7) is conventional dynamic logics with predischarge. If the input is high means predischarge clock & pullup transistor are disable and pulldown transistor & precharge are enable.



Module0.out

```
  5.98475e-007  5.0000e+000  3.0618e-008
  5.99475e-007  5.0000e+000  1.6215e-008
 6.000000e-007  5.0000e+000  8.6647e-009

* BEGIN NON-GRAPHICAL DATA

Power Results
vdd gnd from time 1e-009 to 1e-007
Average power consumed -> 1.408392e-003 watts
Max power 2.755824e-003 at time 1e-009
Min power 1.712735e-010 at time 1e-007


* END NON-GRAPHICAL DATA

* Parsing                        0.01 seconds
* Setup                          0.00 seconds
* DC operating point             0.01 seconds
* Transient Analysis             0.14 seconds
* -----------------------------------------
* Total                          0.16 seconds
```

Fig.8 power consumption of Topology C

In Fig.8 represent the power consumption of conventional dynamic logics with predischarge. In that we have identified minimum power, maximum power and average power according to the input, power consumption can be change.

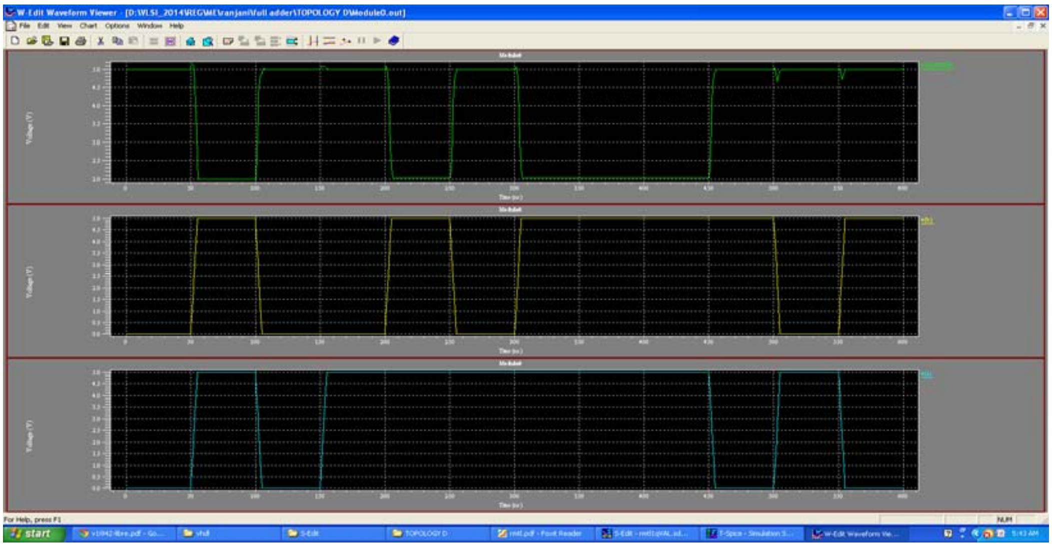
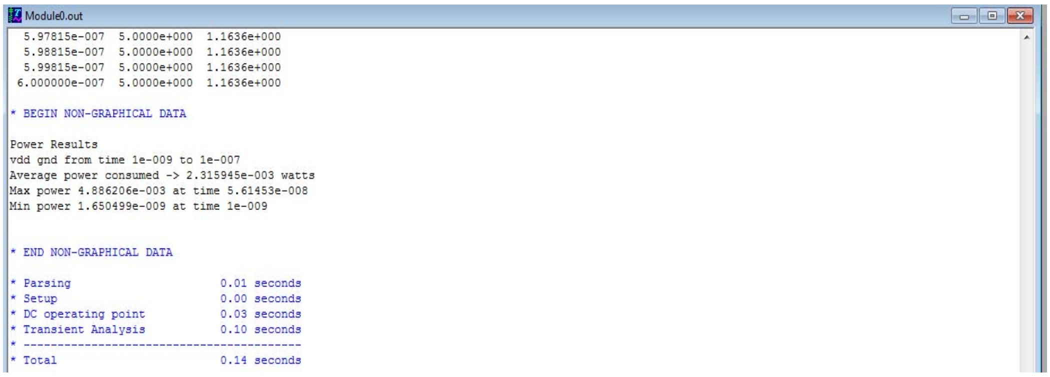

W-Edit Waveform Viewer - [D:\VLSI_2014\REG\ME\ranjani\full adder\TOPOLOGY D\Module0.out]
File
Edit
View
Chart
Options
Window
Help
Voltage (V)
Time (ns)
For Help, press F1
start

Fig.9 Simulation result for Topology D

Topology D (fig.9) is standard dynamic logics with precharge. If the input is high means predischarge clock is disable and pullup, pulldown transistor & precharge clock are enable.



Module0.out

```
  5.97815e-007  5.0000e+000  1.1636e+000
  5.98815e-007  5.0000e+000  1.1636e+000
  5.99815e-007  5.0000e+000  1.1636e+000
 6.000000e-007  5.0000e+000  1.1636e+000

* BEGIN NON-GRAPHICAL DATA

Power Results
vdd gnd from time 1e-009 to 1e-007
Average power consumed -> 2.315945e-003 watts
Max power 4.886206e-003 at time 5.61453e-008
Min power 1.650499e-009 at time 1e-009


* END NON-GRAPHICAL DATA

* Parsing                        0.01 seconds
* Setup                          0.00 seconds
* DC operating point             0.03 seconds
* Transient Analysis             0.10 seconds
* -----------------------------------------
* Total                          0.14 seconds
```

Fig.10 Power consumption of Topology D

In Fig.10 represent the power consumption of standard dynamic logics with precharge. In that we have identified minimum power, maximum power and average power according to the input, power consumption can be change.

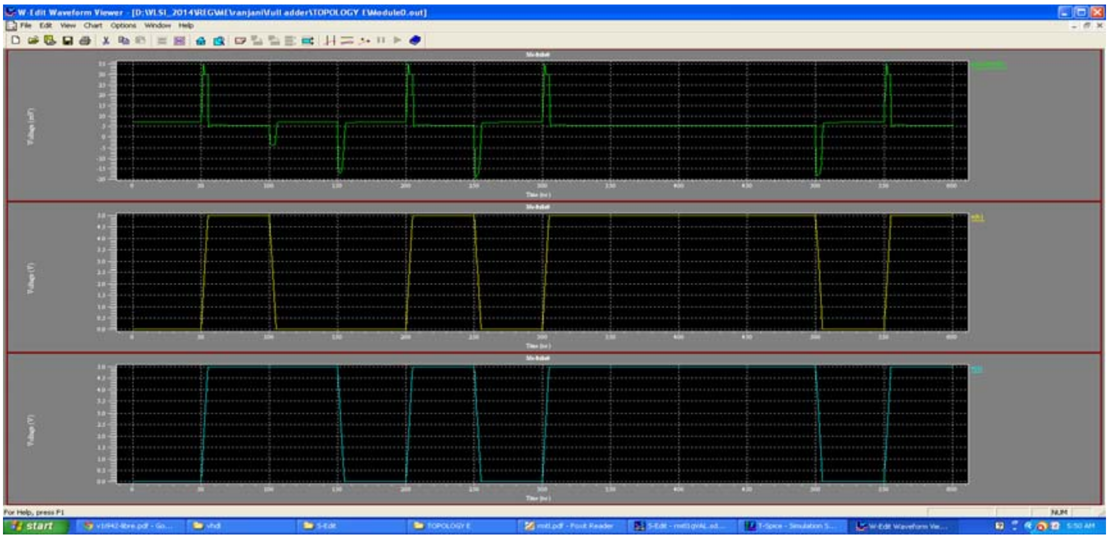
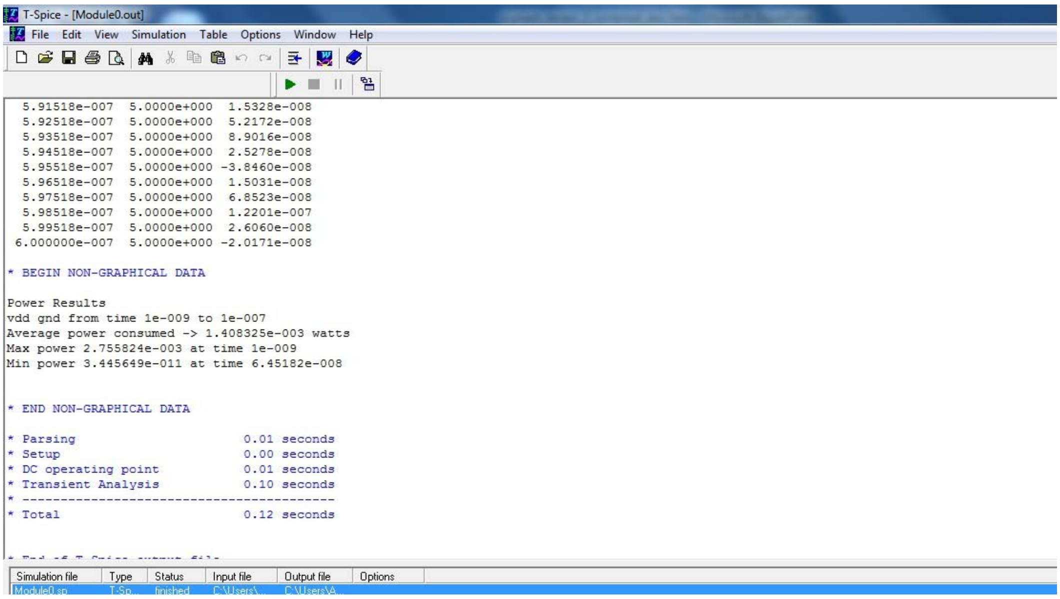


Fig.11 Simulation result for Topology E

Topology E (fig.11) is standard dynamic logics with predischarge. If the input is high means precharge clock is disable and pullup, pulldown transistor & predischarge clock are enable.



```
  5.91518e-007  5.0000e+000  1.5328e-008
  5.92518e-007  5.0000e+000  5.2172e-008
  5.93518e-007  5.0000e+000  8.9016e-008
  5.94518e-007  5.0000e+000  2.5278e-008
  5.95518e-007  5.0000e+000 -3.8460e-008
  5.96518e-007  5.0000e+000  1.5031e-008
  5.97518e-007  5.0000e+000  6.8523e-008
  5.98518e-007  5.0000e+000  1.2201e-007
  5.99518e-007  5.0000e+000  2.6060e-008
 6.000000e-007  5.0000e+000 -2.0171e-008

* BEGIN NON-GRAPHICAL DATA

Power Results
vdd gnd from time 1e-009 to 1e-007
Average power consumed -> 1.408325e-003 watts
Max power 2.755824e-003 at time 1e-009
Min power 3.445649e-011 at time 6.45182e-008


* END NON-GRAPHICAL DATA

* Parsing                        0.01 seconds
* Setup                          0.00 seconds
* DC operating point             0.01 seconds
* Transient Analysis             0.10 seconds
* -----------------------------------------
* Total                          0.12 seconds


* End of T-Spice output file
```

Simulation file	Type	Status	Input file	Output file	Options
Module0.sp	T-Sp...	finished	C:\Users\...	C:\Users\A...	

Fig.12 Power consumption of Topology E

In Fig.12 represent the power consumption of standard dynamic logics with predischarge. In that we have identified minimum power, maximum power and average power according to the input, power consumption can be change.

VII. Conclusion

This thesis deals with secure logic circuits. It is well established that security lapses are operated in the RMTL logic using different topologies with different logic that compare the power to analyze the low power consumption logic and that logic had been used in the s-box. This approach tries to maintain power consumption patterns independent of the signals that are handled. Therefore there is a need for developing strategies to reduce the power consumption and at the same time meeting the security concerns.

References

1. ”True Random Based Differential Power Analysis Countermeasure Circuit for an AES Engine”S.Saravanakumar2014.
2. V.S.Subarsana1,C.K.Gobu“A Countermeasure Circuit for Secure AES Engine against Differential Power Analysis”2014
3. M. Alioto, H. Boey, Y. Lu, M. O’Neill, and R.Woods,“Random clock against differential power analysis,” in Proc. IEEE APCCAS, Dec. 2010,pp. 756–759.,

4. M. Poli and S. Rocchi, "A general model for differential power analysis attacks to static logic circuits," in Proc. IEEE ISCAS, May 2008, pp. 3346–3349.

5. J.-S. Coron and L. Goubin, "On Boolean and arithmetic masking against differential power analysis," in Proc. 2nd Int. Workshop CHES, 2000, pp. 231–237.

6. K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3rd ed. New York, NY, USA: Wiley, 2010.

7. D. Stinson, Cryptography: Theory and Practice, 3rd ed. Cleveland, OH, USA: CRC Press, 2006.

8. P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Proc. 19th Annu . Int. Cryptol . Conf. Adv. Cryptol ., 1999, pp. 388–397.

9. P.C. Kocher, Timing Attacks on Implementations of Differential-Hellman, RSA, DSS, and Other Systems. New York, NY, USA: Springer-Verlag, 1996,pp. 104–113.

10. M. Alioto, M. Poli, and S. Rocchi, "A general model for differential power analysis attacks to static logic circuits," in Proc. IEEE ISCAS, May 2008, pp. 3346–3349.

11. S.Mangard,N.Pramstaller,andE.Oswald,"Successfully attacking masked AES hardware implementations,"inProc.7thInt.Workshop CHES, vol. 3659. Edinburgh, U.K., Aug./Sep. 2005, pp. 157–171.

AUTHOR(S) PROFILE

Ranjani A , M.E Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu, India.

Poornima U, Assistant Professor, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu, India.