# CMOS Logic Using Multi-Topology For Power Analysis

Ranjani. A,
PG student,
Department of Electronics and Communication Engineering
Parisutham Institute of Technology and Science,
Thanjavur, Tamil Nadu, India

Poornima. U
Assistant Professor
Department of Electronics 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 outside viewer 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 and identifies the low power gate. In AES, substitution box we are using RMTL logic to avoid the side channel attack and analysis the power.**

***Key word- RMTL, Differential power analysis, Advanced encryption standard.***

## 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 signaled processing and error correction properties which can extract secret from measurement which can contain too much noise to be analyze using simple power analyze. Using DPA an 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. 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. BACKGROUND

### *A. True Random Based Differential Power Analysis Countermeasure Circuit For An AES Engine*

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.

### B. *A Low Power Countermeasure Circuit For Highly Secure AES Algorithm Against DPA Attack*

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.

### C. *Random Clock against Differential Power Analysis*

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 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.

### D. *A General Model For Differential Power Analysis Attacks To Static Logic Circuits*

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 a new figure 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.

### E. *On Boolean And Arithmetic Masking Against Differential Power Analysis*

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. ARCHITECTURE SYSTEM

In this paper RMTL (Randomized multi-topology logic) gate uses different topologies .Each topology consumes different power. RMTL logic had CMOS logic which contain pull up and pulldown with addition four transistors. The two transistor consider as precharge clocked and predischarge clocked ,other tow transistor are consider as PUN and PDN. There are five type of topologies A,B,C,D,E is used static logic, conventional dynamic logics with precharge, conventional dynamic logics with evaluation, standard dynamic logics with precharge, standard dynamic logics with evaluation respectively.

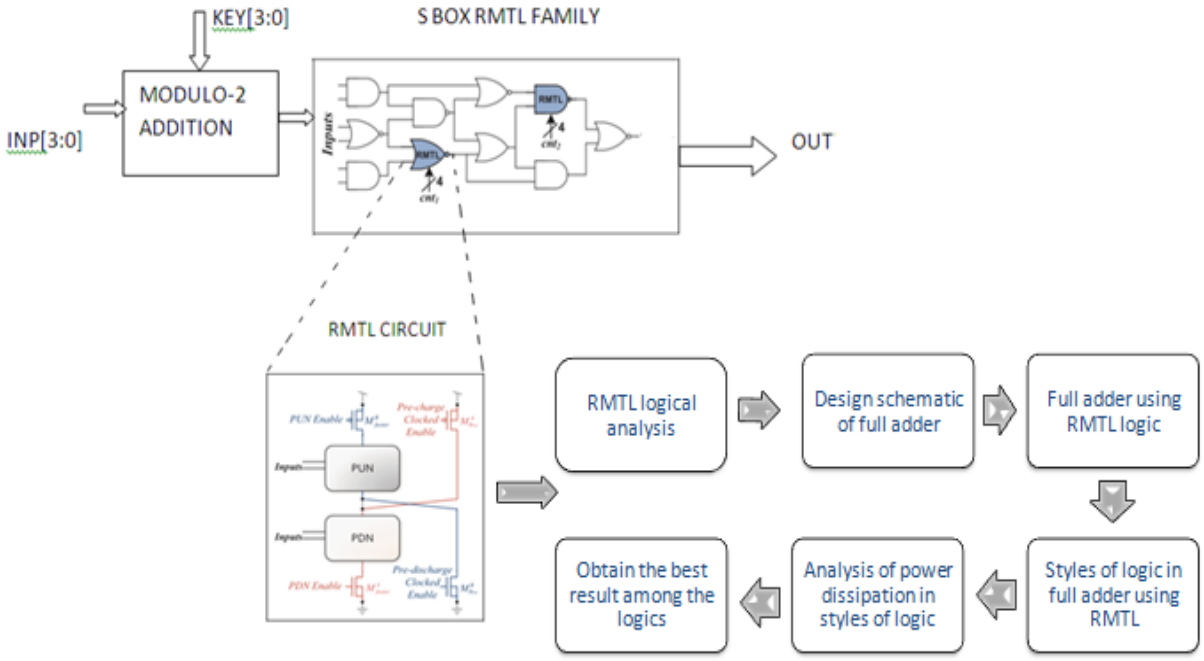


Fig.2 Block diagram of power analysis using RMTL

Design the ordinary full adder gate by using PMOS and NMOS transistor. In that full adder apply different topologies to analysis the power and compare the power. In the comparison, identify the gate consume less power. That Full adder gate has been placed in the substitution box it can be used for transfer data.

## V. TOOLS USED

As the technology in electronic circuits is improving, the difficulty in these circuits also increases. So the authors have to develop such type of circuits that consume very less power. The major focal point in designing a various digital signal processors is given to low power design. Tanner is use for analysis the power and compares the power in the different topologies.

## VI. CONCLUSION

All the five topologies have been compared with the parameter of power and time. The power requirement in terms of minimum, maximum & average has also listed and compared in Table.1 Based on this comparison only the suitable logic can be identified to use inside the substitution box.

TABLE.1 COMPARISON OF FIVE TOPOLOGIES

| PARAMETER | TOPOLOGY A | TOPOLOGY B | TOPOLOGY C | TOPOLOGY D | TOPOLOGY E |
|---|---|---|---|---|---|
| MAX | 6.155471e-003 W | 4.880351e-003W | 2.755824e-003 W | 4.886206e - 003W | 2.055824e-003 W |
| MINI | 2.653726e-010 W | 4.944242e-011W | 1.712735e-010 W | 1.650499e-009 W | 3.445649e-011 W |
| AVG | 2.676052e-003W | 2.314562e-003W | 1.408392e-003 W | 2.315945e-003W | 1.408325e-003 W |
| TIME | 0.16s | 0.15s | 0.16s | 0.14s | 0.12 s |

## REFERENCES

[1] S.Saravanakumar "True Random Based Differential Power Analysis Countermeasure Circuit for an AES Engine" IJARCSMS,FEB 2014 ISSN: 2321-7782

[2] V.S.Subarsana1,C.K.Gobu"A Countermeasure Circuit for Secure AES Engine against Differential PowerAnalysis"2014

[3] M. AliotoK. 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. Crypto. 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. Prams taller, and E. Oswald, "Successfully attacking masked AES hardware implementations, "in Proc.7thInt.WorkshopCHES, vol.3659. Edinburgh, U.K., Aug. /Sep. 2005, pp. 157–171.