ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

A Novel Implementation of secure VLSI logic design

[1] Kusuma B T, [2] A.R.Priyarenjini
[1] Student, [2]Asst. Professor
[1][2] ECE, MSRIT

***Abstract* - Crypto circuits can be attacked by third parties using differential power analysis (DPA), which uses power consumption dependence on data being processed to reveal critical information. To protect security devices against this issue, differential logic styles with (almost) constant power dissipation are widely used. However, to use such circuits effectively for secure applications it is necessary to eliminate any energy-secure flaw in security in the shape of memory effects that could leak information. This paper proposes a design methodology to improve pull-down logic configuration for secure differential gates by redistributing the charge stored in internal nodes and thus, removing memory effects that represent a significant threat to security. To evaluate the methodology, it was applied to the design of AND/NAND and XOR/XNOR gates in a 90 nm technology, adopting the Sense amplifier based logic (SABL) style for the pull-up network. Sbox 8 can be implemented using these circuits for the security purpose.**

Index Terms—Complementary metal oxide semiconductor (CMOS) digital circuits, differential power analysis (DPA), side-channel attacks(SCA), and very large scale integration (VLSI) design of cryptographic circuits.

I.INTRODUCTION

In today's information and technology based world, everyone has come in contact with another by using some form of embedded systems. These embedded systems can contain large amount of personal information, some time these information, if stolen by an attacker, they can be used against us. So the security is a major concern for these types of devices. However it is possible to provide a level of security so that the information within these stolen devices is not accessible by an attacker. All these devices need encryption technology to guarantee security. Encryption is based on mathematically secure algorithm, designed to get a cipher text from a plain text by using secrete key, that secrete key cannot be attacked mathematically [1].

The physical Implementation of these encryption algorithm leaks side channel information, this information can be used by an attacker to know the secrete key [2]-[6]. This project mainly deals with protection against this type of leakages. Power consumption plays a major role in present day VLSI design technology. The demand for low power consuming devices is increasing rapidly and the adiabatic logic style is said to be an attractive solution. Adiabatic Logic is the low-power electronic circuits that implement reversible logic. The term adiabatic process is one in which the total heat or energy in the system remains constant [7]. The power consumption of the electronic devices can be reduced by adopting different design styles. Adiabatic computation has been widely studied as a low power design technique. In the recent years, several adiabatic or energy recovery logic architectures have been proposed. They have achieved significant power savings compared to conventional CMOS circuits [8]. After providing great protection against the intruder using mathematical

algorithm, it is necessary to make a physical implementation of these algorithms, this physical implementation leaks secrete key i.e., called as a side channel information, by using this information attacker can reveal the secrete key. So that the physical implementation of cryptographic devices therefore have to be carefully considered [9].

The motivation of this project is to provide new low power solutions for Very Large Scale Integration (VLSI) designs for portable devices. Security is a main concern so all data is encrypted hence dedicated encryption/decryption modules required. In this encryption and decryption module security attackers, should not reveal key in side channel attacks [10]. A portable device uses no constant power supply, where as encryption/decryption is continuous and hence Power consumption should be low.

Different types of adiabatic logics are ECRL, PFAL, CAL, DFAL, and SABL. An efficient charge recovery logic (ECRL) circuit adopts a new method that performs pre-charge and evaluation simultaneously[11]-[14]. It eliminates the pre-charge diode and dissipates less energy than other adiabatic

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

circuits. Positive feedback adiabatic logic circuit (PFAL), it is quasi adiabatic logic i.e., only a part of energy is recovered. The core of PFAL consists of two PMOS and two NMOS transistors which forms latch. The latch helps in avoiding logic level degradation at output node.

Sense amplifier based logic (SABL) circuit, which introduced the concept of Dynamic and Differential Logic (DDL), DDL enables one switching per cycle by having both true and complementary signals which generate the differential outputs. Wave dynamic differential logic (WDDL) circuit uses a differential and pre-charge technique which is used for cryptographic devices to make the power consumption of the logic cell is constant in each clock cycle.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key[15].

Rijndael was designed to have the following characteristics: Resistance against all known attacks, Speed and code compactness on a wide range of platforms and Design Simplicity.

Substitute Bytes known as Sub-Bytes is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16 × 16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables. In below fig 1. shows the Rijndael Sbox lookup table.

right (low-order) nibble

left (high-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig 1. Rijndael Sbox

II. DPA RESISTANT DIFFERENTIAL LOGIC GATES

Fig.2 shows a Differential logic style. Such logic styles consists of differential pull down network (DPDN) performing the logic function and SABL logic style is used as differential pull up network (DPUN) working in alternate pre-charge and evaluation phases. They provide both true and complemented output in every clock cycle, with only one charging event.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

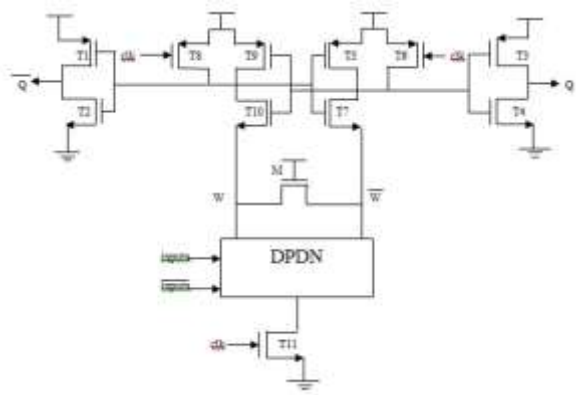

Fig 2.Logic circuit of an SABL

SABL operates as follows, the PMOS transistors with a gated clock (T6 and T8) in the DPUN are ON in the pre-charge phase i.e., clk = 0,setting WW = 11(QQ = 00). In the evaluation phase i.e., clk = 1,the sources of NMOS transistors T7 and T10 are grounded through a discharge path in the DPDN and the switching action of transistor M, which is always ON, making the logic function at the output dependent on input values. 1) the presence of the clocked bottom transistor T11, 2) full symmetry in DPUN, and 3) outputs of DPDN not connected to the gate of output inverters (T1/T2 and T3/T4), these specific features make SABL resistant to DPA. Even using the appropriate logic style such as SABL in the DPUN, the DPDN must be symmetrical when implementing the logic regardless of the inputs. Symmetry means that all the paths from WW to ground must have the same number of transistors.

Even with a fully symmetric DPDN, information could be leaked if the evaluation of specific data leaves some memory that can be exploited by an attacker. To guarantee maximum DPA protection, therefore, any kind of memory effect should be removed. In SABL AND/NAND logic style is shown in fig 3. for every input condition, the charge stored in the internal nodes (n1 and n2) should be equalized, because these nodes may store information about the previous state. Waveforms in fig 4. can be obtained from a simulation of a AND/NAND SABL gate implemented in a 90nm technology. Let us consider the implementation of the XOR/XNOR DPDN shown in Fig. 5 and SABL XOR/XNOR logic style is shown in fig 6. The values stored in internal nodes n1 and n2 in the pre-charge phase depend on the value of input B in the previous evaluation.

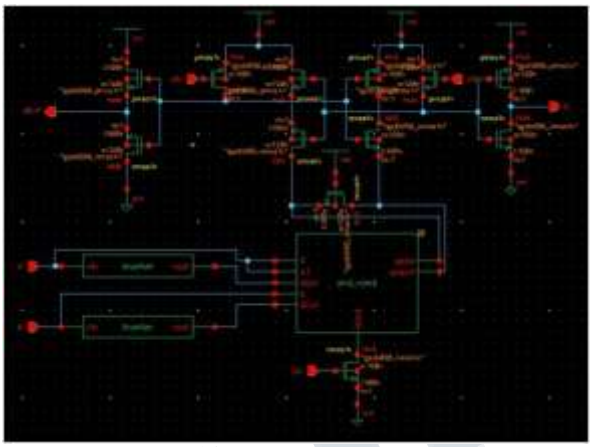

Fig 3. AND/NAND DPDN for SABL

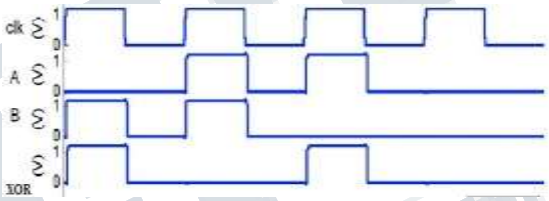

Fig 4.Waveform of SABL and/nand gate

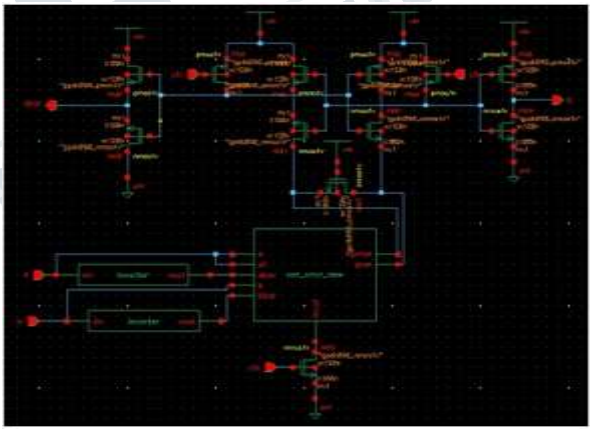

Fig 5. XOR/XNOR DPDN for SABL

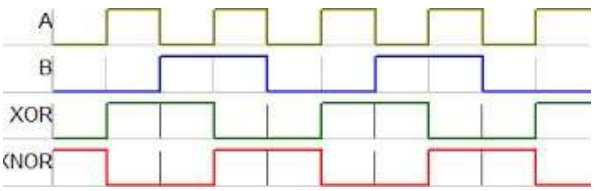

Fig 6.Waveform of SABL xor/xnor gate

To prevent the undesired memory effect, the new technique is proposes for matching the charges in the internal nodes during pre-charge phase. So it is

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

necessary to add specific transistors that are on only in the pre-charge phase it is called as dual switch solution, the intermediate nodes in the DPDN implementation are tied to supply/ground rails with independent switches during pre-charge, forcing exactly the same voltage in all nodes. Each DPDN level except for the first one, which generates the true and the complemented output, needs exactly one pair of switches. In the SABL structure, these are interconnected with the intermediate Vdd gated NMOS transistor that is always ON. A generic scheme for a dual-switch solution is shown in Fig.7 and Fig.8. and in fig 9 shows the output waveform of Dual switch solution for DPDN.

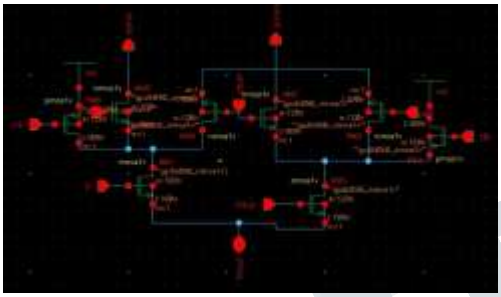

Fig 7.and/nand Dual switch solution for DPDN

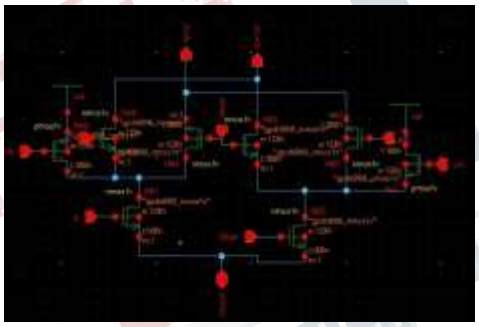

Fig 8.xor/xnor dual switch solution for DPDN

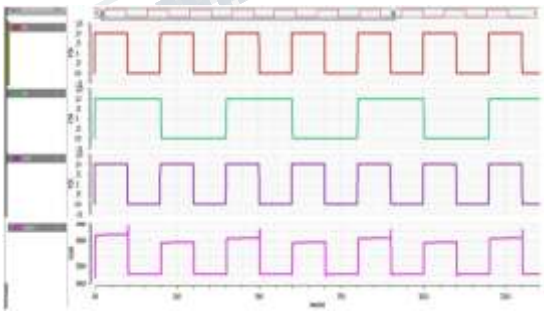

Fig 9.waveform of dual switch AND/NAND

Implementation of above circuits is carried out using Cadence virtuoso at 90 nm technology with a applied voltage of 1V i.e., Vdd = 1V. The required output parameters for both classic and Dual switch SABL solution is listed below TableI.

Table I. Output parameter Comparison

	Evaluation Eavg (fJ)	**Pre-charge** Eavg (fJ)	**Eavg_Total** (fJ)	**Delay** (ps)
Classic AND/NAND	8.44	12.24	208	18
Dual switch solution	8.22	16.08	246	20
Classic XOR/XNOR	12.00	21.72	33.72	173
Dual switch solution	12.24	30.96	43.20	198

III. PROPOSED DESIGN

In previous section I explained about the Dual switch solution of SABL circuits for both AND/NAND and XOR/XNOR, by using these circuits Sbox8 can be implemented in this section. A substitution box or S-box is one of the basic components of symmetric key cryptography. In general, an S-box takes m input bits and transforms them into n output bits. This is called an mXn S-box and is often implemented as a lookup table. These S-boxes are carefully chosen to resist linear and differential cryptanalysis. The generation of S-box involves operation in a Galois Field GF, specially GF(28). Polynomials are either represented in the algebraic form, hexadecimal or decimal notation.

According to the Rijndael proposal, an S-box should have the following characteristics: Invertibility, Minimization of the largest of the non-trivial correlation between linear combinations of input bits and linear combination of output bits, Minimization of the largest non-trivial value in the XOR table, Complexity of its algebraic expression in GF(28), Simplicity of description.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 8, August 2017

All the above criteria are fulfilled by taking the inverse over the finite field GF(28) and the Affine transformation S-box used in AES algorithm consists of 16 X 16 entries, they are the bytes from 00h to ffh and all the entries are unique. Designing of an Sbox includes: Galois field, Affine Transformation, Multiplier and inverse multiplier, Square, Delta, Lambda, and Constant phi

we can reduce delay for implementing the Sbox by using some assumptions, they are

Galois Field, $GF(22) = x2 + x + 1$

$$GF((22)2) = x2 + x + \phi$$

$$GF((22)2)2) = x2 + x + \lambda$$

where ϕ (constant phi) & λ(lambda) is the two polynomial

δ is the isomorphic function used for multiplicative inverse.

The implementation of Sbox in cadence virtuoso at 90nm using SABL XOR/XNOR gate, one of the circuit in designing Sbox8 is shown in below fig 10.

Fig 10. Implementation of Sbox8

By combining the above circuits we come across the final Sbox8 output, its shown in fig 10.

Fig 11. Output waveform of Sbox8.

IV. IMPLEMENTATION AND SIMULATION RESULTS

To evaluate the effectiveness of the two techniques, the proposed methodology was applied to the design of two-input AND/NAND and XOR/XNOR SABL gates in a 90 nm technology. Although simple gates, they are the most commonly used in current crypto hardware implementations. However, the proposals can be easily applied and their effectiveness verified with more complex gates and other differential structures. Classic and proposed AND/NAND (XOR/XNOR) SABL gates were designed in CADENCE using TSMC 90nm and used to design Sbox 8 to provide security against information leakage.

V. CONCLUSION AND FUTURE WORK

This paper presented a methodology for improving the DPDN of differential logic gates used in cryptographic applications. Two new mechanisms were presented to remove the charge in the pull down of a differential gate and eliminate the memory effect, By using dual switch solution circuit we can design Sbox8, it can be used in any differential structure for security application using this configuration, The DPA resistance of the gate was improved with minimum performance degradation.

Designing another logic circuit by combining the low power features of adiabatic logic with other DPA resistant circuits which has less power difference between transitions. Creating a library of basic cells of low power DPA resistant logic, by using this logic circuits we can Implement S-box .

REFERENCES

[1] S.Chen Erica, Tena-Sánchez, Javier Castro, and Antonio J. Acosta, “A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits,” IEEE journal on emerging and selected topics in circuits and systems, vol. 4, no. 2, June 2014.

[2] Nianhao Zhu, Yujie Zhou and Hongming Liu, “A Novel Way to Implement WDDL Logic to Resist Power Analysis Attack in Algorithm Level,” School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China 2014.

[3]LakshmiNarasimhan,Ramakrishnan,Manoj,andChakkaravarthy "SDMLp: On the Use of Complementary Pass Transistor Logic for Design of DPA Resistant Circuits," IEEE International Symposium on Hardware-Oriented Security and Trust 2012.

[4] Sarathkumar .S, Ravibabu .B, "Design and implementation of multiplexer using positive Feedback adiabatic logic," International Journal of Innovations in Scientific and Engineering Research(IJISER). Vol 1 Issue 11 DEC 2014.

[5] Atul Kumar Maurya, Gagnesh Kumar, "Adiabatic Logic: Energy Efficient Technique for VLSI Applications," International Conference on Computer & Communication Technology (ICCCT)-2011.

[6] Priyanka Sheokand, Garima Bhargave, Saumya Pandey, Jasdeep Kaur, "A New Energy Efficient Two Phase Adiabatic Logic for low power VLSI Applications," 2015 International Conference on Signal Processing, Computing and Control (2015 ISPCC).

[7] Yong Moon and Deog-Kyoon Jeong, "An Efficient Charge Recovery Logic Circuit," IEEE journal of solid-state circuits. vol. 31. no.4. april 1996.

[8] Ashwak alabaichi "Enhance security of advance encryption standard algorithm based on key dependent Sbox," ISBN: 978-1-4673-6832-2©2015 IEEE.

[9] M. Alam S. Ghosh M.J. Mohan D. Mukhopadhyay D.R. Chowdhury I.S. Gupta "Effect of glitches against masked AES S-box implementation and countermeasure," Published in IET Information Security-2008

[10] Massimo Alioto, Luca Giancane, "Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits," IEEE Transactions on circuits and systems papers, vol. 57, no. 2, February 2010.

[11] Massimo Alioto, Massimo PoliA "General Power Model of Differential Power Analysis Attacks to Static Logic Circuits," IEEE transactions on very large scale integration (VLSI) systems, vol. 18, no. 5, may 2010.

[12] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki "Differential Power Analysis of AES ASIC Implementations with Various S-box Circuits," 978-1-4244-3896-9/09/$25.00 ©2009 IEEE.

[13] Sylvain Guilley, Laurent Sauvage "Evaluation of Power Constant Dual-Rail Logics Countermeasures against DPA with Design Time Security Metrics," IEEE Transactions on computers, vol. 59, no. 9, september 2010.

[14] Po-Chun Liu, Hsie-Chia Chang, "A Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators," IEEE Transactions on circuits and systems vol. 57, no. 7, july 2010.

[15] Milena Djukanovic, Luca Giancane, Giuseppe Scotti, "Leakage Power Analysis Attacks: Effectiveness on DPA Resistant Logic Styles under Process Variations," 978-1-4244-9474-3/11/$26.00 ©2011 IEEE.

[16] Yu-ichiHayashi, NaofumiHomma, "Analysis of Electromagnetic Information LeakageFrom Cryptographic Devices With Different Physical Structures," IEEE Transactions on electromagnetic compatibility, vol. 55, no. 3, june 2013.