A DESIGN METHODOLOGY TO IMPROVE PULL-DOWN LOGIC CONFIGURATION FOR SECURE DIFFERENTIAL GATES

Rooka Sukanya[1], S.Tabasum2
[1]PG Scholar, [2]Assistant Professor,
Dept of ECE, Sri Sai Institute of Technology And Science, Rayachoty, Kadapa, Andhra Pradesh.

Abstract: In the modern world secure data transfer and privacy is becoming a major problem. Smart cards and other embedded devices use an encryption technology for secure data transfer. If a person want to obtain the secret data that is encrypted within these cards he can obtain it by measuring the power supply current of such device while it is performing an encryption and carefully analyzing it mathematically. In this paper a new technology is presented to increase the security by at least two orders of magnitude and with negligible performance degradation. It is accomplished by redistributing the charge stored in internal nodes and thus, removing memory effects that represent a significant threat to security. The first attack on smart cards has been reported in 1999 and since then various researches are going on how to implement a secure data transfer. In this paper a novel complete methodology for removing internal charges in any gate of any differential logic style is discussed. It is proving suitability for secure implementation designing and simulating different digital gates. A method for performing simulation based DPA attacks on the substitution box of the Kasumi algorithm to assess the proposal is also explained. The paper also discussed about the effect of temperature variations on the security of the proposal against DPA attacks.

Keywords: Differential Power Analysis (DPA), Homogeneous Dual-Rail Logic (HDRL), Power Consumption, Side-Channel Attacks

I. INTRODUCTION

Security is an important concern in the present life scenario. Cryptographic cores are used to protect various devices but their physical implementatio can be compromised by observing dynamic circuit emanations in order to derive information about the secrets it conceals. Protection against these attacks, also called side channel attacks are major concern of the cryptographic community.A cryptographic system in operation can be monitored and the traces of measured parameter values can be examined by an attacker to discover the secret key of the system. Such attacks are termed as side channel attacks. Among all forms of side channel attacks, the power monitoring attacks so called Differential Power Attacks (DPA) are the most prominent threat to the cryptographic systems since power traces of operations can be easily obtained.Those power traces can be mathematically analyzed to reveal the secret keys quite easily. In general, power dissipation of a circuit is proportional to its switching activity which, in turn, depends on the data that is being handled. The data dependent power

consumption can be exploited to leak away the secret information, specifically, distribution of 0's and 1's. DPA involves collecting large number of power traces and performing statistical analysis of the power variation with respect to changes in data values to extract the secret key. Thus, an attacker can obtain the secret key by measuring the power supply current of a cryptographic device while it is performing an encryption, and by statistically analyzing of the measured power traces. Nanometric technologies with a drastic increase in leakage power are also vulnerable to similar leakage associated attacks. Since the vulnerability of cryptosystems to DPA was reported in 1999, various power analysis attacks and corresponding counter measures have been studied. The earliest methods of combating DPA, such as the incorporation of random power consuming operations and introduction of random delays, among others, proved generally to be ineffective, since they only slightly increase the number of measurements to disclose (MTDs) required to recover the secret key To maximize DPA attack prevention, numerous methods based on protecting cryptosystems at algorithm level have been presented, with some noteworthy solutions being based on duplication. However, algorithmbased security techniques are very specific and difficult to automate, due to their heavy dependence on specific cryptographic algorithm. On the other hand, circuit-level counter measures are more generic, since they are not constrained to one specific cryptographic algorithm. Once a practical method has been found, designers need worry no more about the security of implementations for a specific algorithm, and this make automatic design feasible. This type of solution falls into two categories: gate level mask circuits and complementary circuits. One example of gate level masking is Random Switching Logic (RSL) in which a random signal is used to equalize output transition probability. The main disadvantage of this procedure is its strict timing concern. The other level called complementary level is also named as hiding techniques, is the implementation of a logic circuit with power consumption theoretically independent of the data being processed. The design of this kind of secure cells has been an ongoing obsession in the crypto community, thus it can be used for the hardware implementation of any kind of cryptographic algorithm for either public-key or private-key cryptosystems, regardless of the specific application. There are several approaches to creating hiding counter measures at circuit level with complementary coding and data-independent power consumption. Those based on adiabatic logic, like for instance , offer relevant low-power security features, but adiabatic designs require precise timing (at

least four supplyclock phases) and still need further development. To maximize hiding effects for security purposes using more conventional logic styles, dual rail with precharge logic (DPL) families have been proposed to ensure one computation performed in every clock cycle showing exactly the same transition probability for every input condition.

II. LITERATURE SURVEY

In 2001, Rakers P et al developed a secure contactless smart card having no batteries. As the device power is extracted from the RF field. The transceiver adheres to the ISO 14443, type B specification. This system-on-a-chip integrates the RF circuitry with a large digital circuit without benefit of external bypass capacitors. A measured bit error rate of 3 -10 is achieved. Security is also improved as the isolation circuit increases the required time for differential power analysis (DPA) attack by a factor of 2^{22}. An additional loop antenna is required for this and an isolation circuit is also an essential part that prevents the coupling of digital noise into the receiver[1].

In 2002, Messerges S T et al investigated on simple power analysis and differential power analysis and reviewed the theory behind DPA attacks. His study examines how power analysis theory attacks an actual smart card [2]. The paper showed how DES algorithm gets attacked by specific multiple bits DPA attack. SNR calculation is also presented and the main drawback of this power analysis study is that it is a very elaborate study process. Since it considers only the stronger attacks and neglect the weaker attacks, this kind of methodology can't be used as a reliable one. In 2006, Monnet Y et al presented hardening techniques against fault attacks and the practical evaluation of their efficiency. The circuit technology investigated to improve the resistance against fault attacks is asynchronous logic. Fault tolerance is measured and all the errors that were actually injected into the SBOXES of the hardened DES are detected. The countermeasures are evaluated using laser beam fault injection. The proposed study has got a very large computational complexity [3].

In 2008, Muresan R et al proposed a circuit that protects smart cards against differential power analysis attacks. The circuit is based on a current flattening technique, is designed using a standard 0:18-micrometer CMOS technology, and can be integrated on the samedie or in the same package with the smart card microcontroller[4].

In 2010, Liu C P et al a DPA countermeasure circuit based on digital controlled ring oscillators is presented to efficiently resist the first-order DPA attack. The implementation of the critical S-box of the advanced encryption standard (AES) algorithm shows that the area overhead of a single S-box is about 19% without any extra delay in the critical path. Moreover, the countermeasure circuit can be mounted onto different S-box implementations based on composite field or look-up table (LUT). Based on our approach, a DPA-resistant AES chip can be proposed to maintain the same throughput with less than 2K extra gates. The main disadvantage of the proposed system is its cost is much higher and the throughput is degraded by at least 50%[5].

In 2011 Zhang Y et al, presented a novel multi-level design method to secure encryption algorithms against DPA attack. Generally, DPA-resistant methods can be mainly divided into two levels: software and hardware. Software-based countermeasures are relatively cheaper to put in place, while hardware-based methods counteract DPA at a lower level and achieve better countermeasure effectiveness. Taking both the cost and the level of security into consideration, the technique of WDDL and dynamic cryptosystem are combined, and propose a comprehensive DPA countermeasure on both the algorithmic and the logic level. Hardware accelerator based higher-order masking is used here. The dynamic cryptosystem considerably increases the attack complexity, and meanwhile we utilize WDDL to balance the leakage of power. In this way, DPA attack can be effectively resisted atacceptable cost. Third-order masking design reduces 8/9 execution cycles of GPP based reference design[6].

In 2012 Tanimura K et al proposed the homogeneous dualrail logic (HDRL) standard. It is a standard cell DPA attack countermeasure that theoretically guarantees fully balanced power consumption and significantly improves DPA attack resistivity. A designer does not have to modify the original circuit at all and HDRL does not require pre-charge step. This paper proved that HDRL is more secure than WDDL for more attack results[7].

In 2013 De P et al, presented the designing of dpa resistant circuits using BDD architecture and bottom pre-charge logic. In this work, a reduced ordered binary decision diagram (ROBDD) based dual rail circuit for a basic DPA resistant cell has been designed. The specialty of this cell is that the overall input current of the cell is invariant to the input combinations of data bits applied to the cell. For the first time, bottom pre-charge logic is used in the design of such a cell[8].

In 2014, Sanchez T E et al proposed a new design methodology for DPA resistant circuits. Here, secure differential gates are developed by redistributing the charge stored in internal nodes and thus, removing memory effects that represent a significant threat to security. The DPA resistance of the gate is improved, with minimum performance degradation through the proposed system. A simulation based DPA attacks on the substitution box of the Kasumi algorithm is performed and verified[9].

III. OPTIMIZATION METHODOLOGY FOR DPDN

To prevent the undesired effect described above, we propose a technique for matching the charge in internal nodes during theprecharge phase. This can be achieved principally in two main different ways: 1) by recycling the charge and equalizing it by its distribution between the internal nodes and 2) by charging/discharging all the internal nodes to the samefinal value. In both cases, it suffices to add specific transistors that are in the ON state only during precharge. Initially, the same depth was considered for both branches of DPDN. If the logic function allows different branch lengths, dummy transistors must be added in the same way as for the AND/NAND gate in Fig. 1(a) in order to improve symmetry.
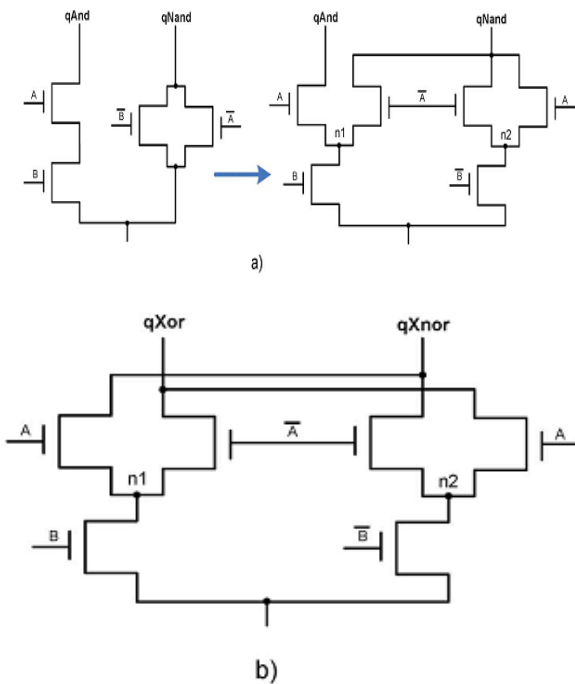
Fig. 1. Implementation of an (a) NMOS AND/NAND and (b) NMOS XOR/XNOR DPDN

Fig. 2. Single-switch generic scheme for N-depth DPDN

Fig. 3. Dual-switch generic scheme for N-depth DPDN.

Single-Switch Solution (P): In any DPDN implementation for a generic differential logic function, the intermediate nodes in the same depth level are tied together through a switch that is ON during the precharge phase , setting an equal value of voltage in nodes in the same level. The overhead associated to this solution is one switch for each transistor level in the DPDN except for thefirst one, which generates the true and the complemented output. In the SABL structure, these are interconnected with the intermediate Vdd-gated NMOS transistor that is always ON. For an N-depth DPDN, therefore, the overhead is N-1 switches. Considering ideal switches, this solution ensures accurate charge distribution during precharge and does not leak any information. From a practical point of view, since a CMOS switch needs one PMOS and oneNMOS transistor, as well as and , the associated overhead is very high, especially in SABL solutions where only a single phase clk is needed. The generation of a global or local becomes unpractical, and so a one-transistor switch represents a good trade-off between complexity and security achievements. A PMOS transistor that is ON in the precharge phase therefore provides the most feasible solution. A generic scheme for a single-switch solution is shown in Fig. 2.

Dual-Switch Solution (2P):The intermediate nodes in the DPDN implementation are tied to supply/ground rails with independent switches during precharge, 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. Thus, for an
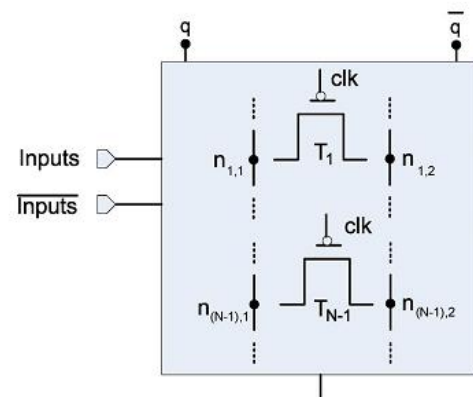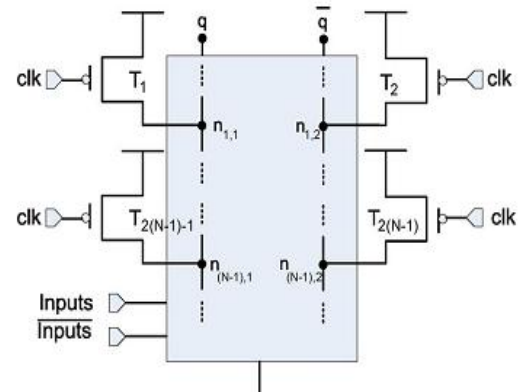
N-depth DPDN, the overhead is switches. As with the single-switch configuration, the only feasible solution uses PMOS switches that are ON during precharge, connected to Vdd. Any other solution has important drawbacks: NMOS switches need to be controlled by unavailable signal, PMOS switches are not suitable for GND connection because of their limited conduction of "0" and CMOS switches are too expensive to implement. A generic scheme for a dual-switch solution is shown in Fig.3
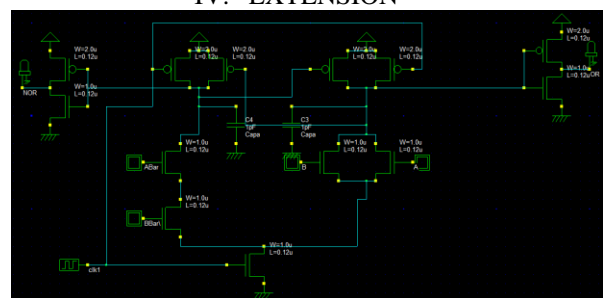
IV. EXTENSION

Fig.4 OR/NOR Schematic

Fig. 4 shows the schematic for the dual-switch solution applied to the OR/NOR DPDN implemented in the same 90 nm technology. Here, two PMOS transistors T1 and T2 connected to internal nodes n1 and n2 are gated by the clock signal. In each precharge phase, when , the PMOS transistors T1 and T2 are turned ON, setting an equal voltage value (Vdd) in nodes n1 and n2. These two feasible solutions prevent the above-mentioned memory effect and ensure that

all evaluations start in the same DPDN with dual-switch proposal. initial conditions. A priori, the main drawbacks would be slight increases in 1) area, 2) power consumption during the precharge phase, and 3) delay in the evaluation phase. Moreover, a significant improvement in security of the gate is expected, since closer power consumption and delay values can be achieved for different input data.
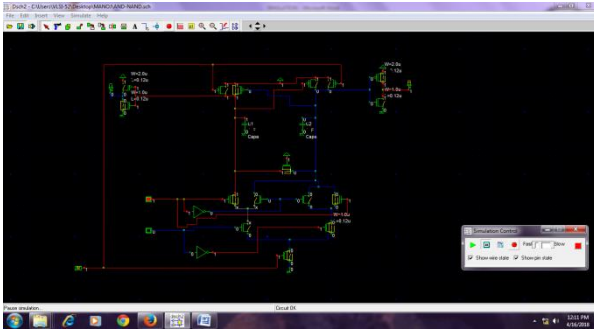
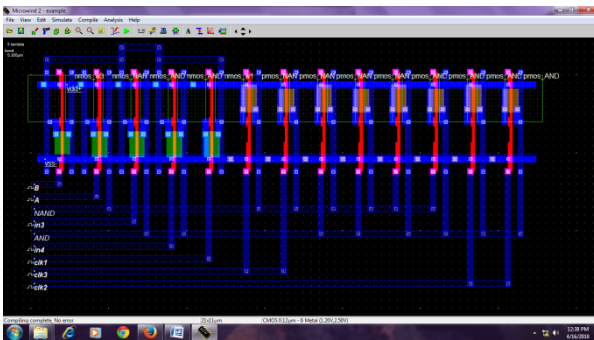## V. RESULTS

Fig.5.Simulation

Fig.6.Layout

VI. CONCLUSION

In this survey paper, a literature review on various designing methodologies used for developing secure differential logic gates has been presented. Many counter measures are available for security enhancement in encrypted circuits. It mainly concentrated on designing secure DPA resistant circuit by redistributing the charge stored in internal nodes and thus, removing memory effects that represent a significant threat to security. It has presented a methodology for improving the DPDN of differential logic gates used in cryptographic applications. Two new mechanisms were presented to remove charge in the pull-down of a differential gate and eliminate the memory effect. Both of them the single switch solution and the double switch solution can be used in any differential structure for security applications. Using the proposed configuration, the DPA-resistance of the gate was improved, with minimum performance degradation. To detect the   security flaws caused by temperature variations, DPA attacks at different temperatures were simulated for Sbox9 CMOS, SABL classic and also for the proposed one. The results obtained indicated that CMOS circuits were vulnerable regardless of temperature, but in the case of classic SABL Sbox9, crypto circuits perating at temperatures lower than 10 degree Celsius are extremely

more secure. Cooling the circuit intentionally can therefore help to protect the circuit against DPA attacks. As future work, the implementation of different Sboxes and block- or stream-cipher is considered to apply the proposed methodology.

REFERENCES

[1] Patrick Rakers,Larry Connell, Tim Collins and Dan Russell, "Secure Contactless Smartcard ASIC with DPA Protection" IEEE J. Solid State Circuits, vol. 36, no. 3, pp. 203- 215, Mar. 2001.

[2] Thomas S . Messerges, Ezzat A. Dabbish and Robert H. Sloan, "Examining smart card security under the threat of power analysisattacks",IEEETrans.Computers,vol.51, no.4, pp.541-552, April 2002.

[3] Yannick Monnet, Marc Renaudin and Regis Leveugle, "Designing Resistant Circuits against Malicious Faults Injection Using Asynchronous Logic", IEEE Trans. Computers, vol.55, no.9, pp. 1104 - 1115, Sept. 2006.

[4] Radu Muresan and Stefano Gregori ,"Protection Circuit against Differential Power Analysis Attacks for Smart Cards", IEEE Trans. Computers,vol.55, no.9, pp. 1540 – 1549,Nov. 2008.

[5] Po-Chun Liu, Hsie-Chia Chang and Chen-Yi Lee, "A Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators", IEEE Trans. VLSI, vol.57, no.7, pp.546 - 550, July 2010.

[6] Yuyu Zhang, Guoxi Wang, Yufeng Ma, Jingwen Li, "A Comprehensive Design Method Based on WDDL and Dynamic Cryptosystem to Resist DPA Attack" ,IEEE Conf. ISIE,vol.18, no.5, pp. 333 - 336,Aug 2011.

[7] Kazuyuki Tanimura and Nikil D. Dutt,"HDRL: Homogeneous Dual-Rail Logic for DPA Attack Resistive Secure Circuit Design", IEEE Embedded System Letters,vol.4, no.3, pp. 57-60,Sept 2012.

[8] Partha De, Kunal Banerjee, Chittaranjan Mandal and Debdeep Mukhopadhyay ,"Designing DPA Resistant Circuits Using BDD Architecture and Bottom Precharge Logic",IEEE DSD Euromicro Conf., no.5, pp.641-644,Sept 2013.

[9] Erica Tena-Sanchez, Javier Castro, and Antonio J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits",IEEE Trans.VLSI,vol.18, no.5, pp. 203- 215, June2014.