ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

Implementation of a Novel Algorithm in the Design of DPA Resistant Circuits for Improved Security

V. Snigdha, P. Ravi Babu
Department of Electronics and Communication Engineering, ACE Engineering College, Hyderabad, India

Abstract-In this 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 wants to obtain the secret data that is encrypted within these cards he/she 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 algorithm 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. It is thereby considered to be a novel technology, unseen in the literature. A complete methodology for removing internal charges in any gate of any differential logic style is discussed. It proves 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.

***Index Terms*-Differential Power Analysis (DPA), Differential Pull Down Network (DPDN), 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 implementation 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. Nano metric 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, algorithm based 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 not worry more about the security of implementations for a specific algorithm, and this makes 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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

adiabatic designs require precise timing (at least four supply clock 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 [1], a secure contactless smart card having no batteries was developed. 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 3e-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. Investigations on simple power analysis and differential power analysis and review on the theory behind DPA attacks is presented in [2]. The paper delivers the power analysis theory attacks an actual smart card. It also presented results on DES algorithm being attacked by specific multiple bits DPA attack along with SNR calculation. But, 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 [3], hardening techniques against fault attacks and the practical evaluation of their efficiency is presented. The circuit technology investigated to improve the resistance against fault attacks is an 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. Nevertheless, the proposed study has got a very large computational complexity. A circuit that protects smart cards against differential power analysis attacks can be seen in [4]. 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 same die or in the same package with the smart card microcontroller. Whereas, a DPA countermeasure circuit based on digital controlled ring oscillators is presented to efficiently resist the first-order DPA attack [5]. 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 this approach, a DPA-resistant AES chip can be proposed to maintain the same throughput with less than 2K extra gates. The main disadvantage of this kind of system is its cost and the throughput is degraded by at least 50%. A novel multi-level design method to secure encryption algorithms against DPA attack is shown as a research in [6]. 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 Wave Dynamic Differential Logic (WDDL) and dynamic cryptosystem are combined, and a comprehensive DPA countermeasure on both the algorithmic and the logic level was proposed. WDDL is used to balance the leakage of power. In this way, DPA attack can be effectively resisted at acceptable cost. But, usage of hardware accelerator based higher-order masking and dynamic cryptosystem have considerably increased the attack complexity. In [7], the homogeneous dual rail logic (HDRL) standard was proposed. 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. In [8], the designing of DPA resistant circuits using Binary Decision Diagram (BDD) architecture and bottom pre-charge logic was presented for the first time. Reduced ordered binary decision diagram (ROBDD) based dual rail circuit for a basic DPA resistant cell has been designed as an extension. 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. A new design methodology [9] for DPA resistant circuits where secure differential gates are developed by redistributing the charge stored in internal nodes lead to the removal of 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, but failed to regulate the delay in the evaluation phase of the transistor.

III. DESIGN METHODOLOGY: IMPLEMENTATION OF DPDN

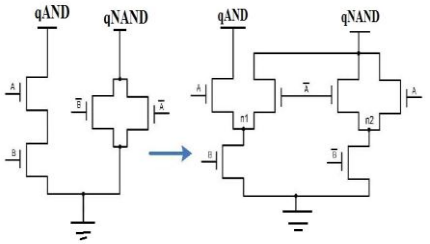
To prevent the undesired effects observed in the literature, we propose a technique for matching the charge in internal nodes during the recharge phase. This can be achieved principally in two main different ways.

Method 1: By recycling the charge and equalizing it by its distribution between the internal node.

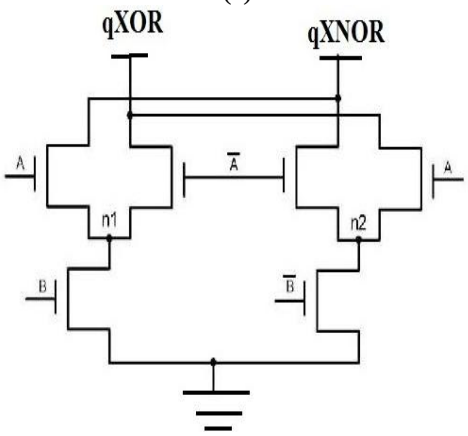
Method 2: By charging/discharging all the internal nodes to the same final value. In both cases, it suffices to add specific transistors that are in the ON state only during precharge. Initially, the same depth was considered for both branches of DPDN. If the logic function allows different branch lengths, dummy transistors must be added in the same

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

way as for the AND/NAND gate in Fig. 1(a) in order to improve symmetry.



(a)



(b)

Fig.1. Implementation of an (a) NMOS AND/NAND (b) NMOS XOR/XNOR DPDN

A. 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 the first one, which generates the true and the complemented output. In the Sense Amplifier Based Logic (SABL) structure, these are interconnected with the intermediate V_{DD}-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 one NMOS transistor, as well as an inverter, the associated overhead is very high, especially in SABL solutions where only a single phase clock 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.

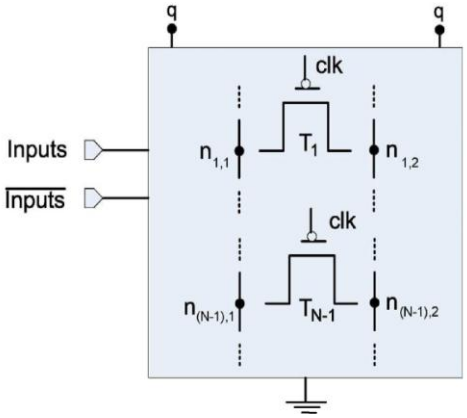


Fig.2 Single-switch generic scheme for N-depth DPDN

B. 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 V_{DD}-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 V_{DD}. 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.

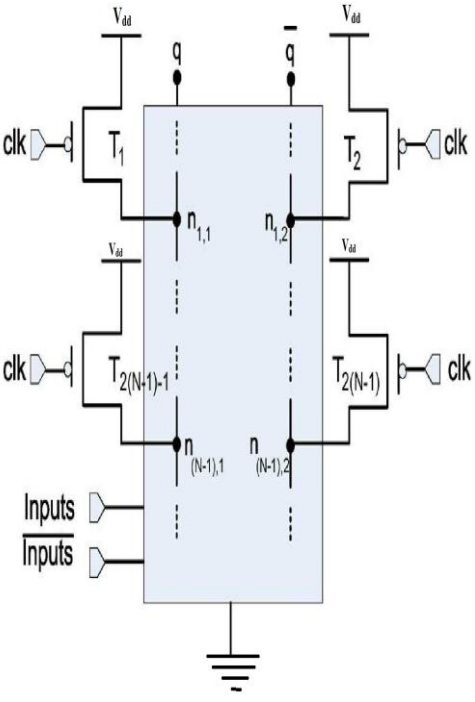


Fig.3 Dual-switch generic scheme for N-depth DPDN

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

TABLE I: Comparative Analysis of the different algorithms used in the literature to improve security against attacks.

Reference	Year	Algorithm	Advantages	Disadvantages	Results
[1]	2001	Rectifier network and tuning	1. No batteries are required as device power is extracted from the RF field. 2. Integrates the RF circuitry with a large digital circuit without benefit of external bypass capacitors.	1. Addition of inductive loop antenna. 2. An isolation circuit is needed.	1. A secure contactless smartcard is presented. 2. A measured bit error rate of 3-10 is achieved.
[2]	2002	Multiple bit attack algorithm	1. Simple power analysis and differential power analysis are investigated. 2. Develop an approach to calculate signal to noise ratio.	1. Very elaborate method. 2. Considers only stronger attacks and neglects weaker attacks.	1. Power attack is very important and has to be addressed. 2. Noise analysis.
[3]	2006	Asynchronous logic.	1. Significant fault tolerance improvement. 2. All the errors that were actually injected in to SBOXES of the hardened DES are detected. 3. The robustness of the circuit.	1. Complex computations. 2. Sensitiveness of the Miller gate.	1. Delay-insensitive property makes them inherently robust against some categories of faults such as delay faults. Thus, QDI circuits attractive for designing fault-tolerant/ resistant systems.
[4]	2008	Current flattening technique.	1. An effective protection circuit against DPA attacks for smartcards. 2. It has a simple interfacing. 3. It is algorithm independent. 4. It can be applied to different microcontrollers.	1. Increase the complexity of the circuit. 2. A shunt to shunt feedback loop is there hence the overall gain is decreased.	1. A system with current flattening circuit would have resistance against DPA attacks increased up to 30 times with respect to a system without protection.
[5]	2010	Digital controlled ring oscillators.	1. The countermeasure circuit can be mounted onto different S-box implementations. 2. DPA-resistant AES chip can be proposed to maintain same throughput with less than 2k extra gates.	1. The hardware cost is at least two times larger. 2. The throughput is degraded by at least 50%	1. The area overhead to a single S-Box is increased to 53.13% without lengthening the critical path delay. 2. This algorithm independent method can be directly applied to any encryption algorithm counteracting DPA attacks.
[6]	2011	Hardware accelerator based higher-order masking.	1. Area efficient. 2. Dramatically reduces execution cycles from 197-470k to only 3.3k.	1. Unable to meet the requirements of the performance. 2. An extensive comparison method.	1. Third order masking design reduces around 8/9 execution cycles of GPP based reference design. 2. Reduces 705 % area of hardware accelerator based reference circuit.
[7]	2012	Homogeneous dual-rail logic (HRDL).	1. Successfully repelled DPA attacks. 2. HRDL has no delay overhead. 3. HRDL requires only 100% energy overhead. 4. Does not require precharge step. 5. A designer does not have to modify the original circuit at all.	1. Do not have evenly distributed conditions. 2. Increased complexity of the circuit.	1. HRDL circuit has a differential power at a level that is resistive to DPA attacks. 2. One can implement HRDL using the same cells for primary and complementary cells.
[8]	2013	BDD architecture and Bottom precharge logic.	1. Bottom precharge logic is used in the design of such cell. 2. The ROBDD based	1. Additional circuits are needed. 2. High noise effect.	1. DPA resistance of circuits (for example an adder) developed using this cell. 2. Out-performing other competing

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

			design minimizes both the area and early.		design with respect to peak power variance.
[9]	2014	Eliminating stored charges in internal nodes and avoiding harmful memory effects.	1. Two new mechanisms were presented to remove charge in pull down of a differential gate. 2. Improved security for DPA circuit.	1. Increased area. 2. Increased power consumption during the precharge phase. 3. Delay in evaluation phase.	1. A novel complete methodology for removing internal charges in any gate of differential logic style. 2. Performed stimulation based DPA attacks on the substitution box of the kasumi algorithm.
This work	2015	Elimination of stored internal charges at nodes.	1. A significant improvement in security of the gate. 2. Closer power consumption and delay values can be achieved for different data.	1. Area occupied by the board is high.	1. A novel algorithm to secure differential gates is applied to basic digital logic gates. 2. The key is secured by using kasumi algorithm on S-Box9.

Table I shows the comparative analysis of various methodologies which are used for designing and developing efficient DPA resistant circuits. Many methodologies are available for making anti-DPA circuits. But among all these, the proposed system seems to be much efficient and more advantageous.

IV. CONCLUSION AND FUTURE ENHANCEMENT

A novel algorithm to secure differential gates was proposed in this paper and initially the model is applied to basic digital logic gates. The proposed technique produces a high security than typical SABL gates. Also, studies were investigated and examples were illustrated, assuming DPA attacks on Sbox9 cryptographic module. The algorithm used in this work, is Kasumi algorithm and it is found that the time taken to decipher the key is significantly reduced when compared to the other works in the literature and the key is secured using the Kasumi algorithm on S-Box9 for the various differential gates such as AND/NAND, XOR/XNOR, OR/NOR. 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. Crypto circuit's preparing at temperatures lower than 10 degree Celsius is 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 analysis attacks", 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 Euro micro 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.

AUTHOR'S PROFILE

V.Snigdha is a post graduate student pursuing her M.Tech in ACE Engineering College. Her research interests include digital logic circuits, network systems design. Presently, she is engaged in the design of high performance systems for improved security in DPA resistant circuits.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 1, July 2015

P.Ravi Babu is currently working as an Associate Professor in the Department of Electronics and Communication Engineering, ACE Engineering College. He has a vast experience of 8 years in the academic field and has served the telecommunication and optical networking industry for 2 years. He has published two international conference papers in reputed proceedings. His research mainly lies in the design of embedded systems and in the development of image processing algorithms. He is a life member of ISTE.