

Review on Various Methods Used for Secure Data Transfer

Anagha A¹, Gnana Sheela K²

^{1,2}Department of Electronics and Communication Engineering, Toc H Institute of Science and Technology, CUSAT, Kerala, India

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

1. 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. 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, 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 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 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.

2. 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 same die 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 at acceptable 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 dual-rail 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].

3. Comparative Analysis

Table 1: Comparative analysis of different methodologies used for developing DPA Resistant Circuits

Author	Year	Algorithm	Advantages	Disadvantages	Results
Snchez T E et al	2014	Eliminating stored charges in internal nodes and avoiding harmful memory effects.	1. Two new mechanisms were presented to remove charge in the pull-down of a differential gate. 2. Improved security for DPA circuit. 3. The DPA-resistance of the gate is improved, with minimum performance degradation.	1. Increased area. 2. Increased power consumption during the pre-charge phase. 3. Delay in the evaluation phase.	1.A novel complete methodology for removing Internal charges in any gate of any differential logic style. 2.Performed simulation-based DPA attacks on the substitution box of the Kasumi algorithm. 3.Analysed the effect of temperature variation in the security of the proposal.
De P et al	2013	BDD Architecture and Bottom Pre-charge Logic.	1. For the first time, bottom pre-charge logic is used in the design of such a cell. 2. The ROBDD based design minimizes both area and early	1. Additional circuits are needed. 2. High noise effect.	1.DPA resistance of the circuits (for example an adder) developed using this cell. 2.Out-performing other competing design with respect to peak power variance.
Tanimura K et al	2012	Homogeneous Dual-Rail Logic (HDRL).	1. Successfully repelled DPA attacks. 2. HDRL has no delay overhead. 3. HDRL requires only 100% energy overhead. 4. Does not require pre-charge 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.HDRL circuit has a differential power at a level that is resistive to DPA attacks. 2.One can implement HDRL using the same cells for primary and complementary cells.
Zhang Y et al	2011	Hardware accelerator based higher-order masking.	1. Area-efficient. 2. Dramatically reduces execution cycles from 197 – 470 K to only 3.3 K comparing with the state-of-the-art software implementations.	1.Unable to meet requirements of the performance. 2.More and more modern embedded system. 3.An extensive comparison method.	1.Third-order masking design reduces around 8/9 execution cycles of GPP based reference design. 2. Reduces 70.5% area of hardware accelerator based reference design.
Liu C.P. et al	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 the 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.
Muresan R et al	2008	Current flattening technique.	1.An effective protection circuit against DPA attacks for smart cards. 2.Simplicity of integration. 3.It has a simple interfacing. 4.It is algorithm independent. 5.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 a resistance against DPA attacks increased up to 30 times with respect to a system without protection.
Monnet Y et al	2006	Asynchronous logic.	1.Significant fault tolerance improvement. 2.All the errors that were actually injected into the SBOXES of the hardened DES are detected. 3.The robustness of the circuit	1.Complex computations. 2.Sensitiveness of the muller gate.	1.Delay-insensitive property makes them inherently robust against some categories of faults such as delay faults. Thus, QDI circuits are attractive for designing fault-tolerant/ resistant systems.

Messerges S.T. et al	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 problem and has to be addressed. 2.Noise analysis.
Rakers P et al	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. 3.Security is improved .	1.Addition of an 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.

Table 1 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.

4. 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 operating 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 Resistant 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 Pre-charge 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, June 2014.

Author Profile



Anagha A received her B-Tech degree in Electronics and Communication Engineering from University of Kerala, Kerala, India in 2014. Currently she is pursuing her M-Tech Degree in Electronics and Communication Engineering with specialization in VLSI and Embedded System in Cochin University of Science and Technology (CUSAT), Kerala, India.



Dr. Gnana Sheela K: She received her Ph D in Electronics & Communication from Anna University, Chennai. Presently she is working as an Associate Professor in TIST, Kerala. She has published 14 international journal papers. She is a life member of ISTE.