International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Enhanced Delay-based Dual-rail Precharge Logic against Leakage Power Analysis Attack

Madishetty Shivani†* and Cheerla Padmini†

†Department of ECE, Vardhaman Engineering College, R.R.Dist,Telangana state, India

Accepted 10 Aug 2015, Available online 15 Aug 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

Information security can be achieved through cryptographic algorithms. Even though they are at most secured. The physical implementation of the encryption algorithm leaks side-channel information that can be used by an attacker to reveal the secret key. Crypto circuits can be attacked by third parties using differential power analysis, which uses power consumption dependence on data being processed to reveal critical information. To protect security devices against this issue, differential logic styles with constant power dissipation are widely used. This project extends the analysis of the effectiveness of Leakage Power Analysis (LPA) attacks to cryptographic VLSI circuits. This project circuit level countermeasure against DPA is adopted. The proposed solutions leak less information than typical DDPL gates, increasing security and with negligible performance degradation.

Keywords: *Cryptography, differential power analysis, leakage power analysis, security, side-channel attack and countermeasures, DDPL.*

1. Introduction

[1]In the current information and communication technology based world, security is a major concern. Privacy is considered an important personal right. Commonly used devices like smart cards and other embedded devices require encryption technology to guarantee security. Encryption security is typically based on mathematically secure algorithms, designed to produce a ciphertext from a plaintext that cannot be mathematically attacked. But even when such theoretical security is achieved, the physical implementation of the encryption algorithm leaks side-channel information that can be used by an attacker to reveal the secret key. The physical implementations of cryptographic devices therefore have to be carefully considered.

Side channel attacks (SCAs) on cryptographic devices use certain physical information such as power consumption, time delay, or electromagnetic radiation to find the secret key. SCAs can be noninvasive and usually require minimal equipment; hence they are easy to carry out. Of all SCAs, differential power analysis (DPA) is one of the most powerful for its simplicity and effectiveness. DPA attacks are based on the well-known fact that dynamic power consumption in a logic circuit is dependent on the data being processed by the device.

*Corresponding author: **Madishetty Shivani; Cheerla Padmini** is working as Associate Professor

Countermeasures have been conceived at the different abstraction levels of the security application (M. Djukanovic *et.al* 2011). It started at the algorithmic level. One example is masking. In this technique, a random "mask" is added to the data prior to the encryption and removed afterwards without changing the result. Algorithmic countermeasures, however, need to be reformulated for each algorithm, and, often, proposed solutions actually appear insecure and/or inefficient afterwards. Instead of concealing or decorrelating the side-channel information, circuit level countermeasures pursue the effect of not creating any side channel information. The goal of these countermeasures is to balance the power consumption of the logic gates. The major advantages are that this approach is correct by construction, is independent of the cryptographic algorithm or arithmetic implemented, and is a distributed measure. The idea is to create digital circuit styles that have a switching behavior independent of the data or sequence of data that they are processing.

First approach, Dual-rail precharge (DRP) logic style (e.g., sense amplifier-based logic (SABL), wave dynamic differential logic (WDDL)) (M. Alioto *et.al* 2010; K. Tiri *et al* 2005), signals are spatially encoded as two complementary wires and power consumption is constant under the assumption that the differential outputs of each gate drive the same capacitive load. DRP logics are not affected by glitches but building two balanced wires requires a full-custom approach thus increasing design and maintenance costs.

Second method is based on a masked dual-rail precharge logic style (MDPL) (T. Popp *et.al* 2005) where, due to the random masking at the gate level, power consumption is randomized. Moreover, since MDPL is DRP logic, glitches are avoided and, at the same time, the complementary wires do not need to be balanced thus removing the main drawback of the dual-rail circuits.

MDPL showed a DPA leakage due to the early propagation of the input data with respect to the masking ones. So the third solution has been proposed i.e., a logic insensitive to unbalanced routing capacitances is obtained by introducing a three-phase dual-rail precharge logic (TDPL) (M. Alioto *et.al* 2010) with an additional discharge phase where the output which is still high after the evaluation phase is discharged as well. The main drawback of this solution is the additional area for the routing of the three control signals.

Finally as an improvement of TDPL, Delay-based Dual-rail Pre-charge Logic Style has been presented (M. Bucci *et.al* 2010). It introduces a new data encoding concept which allows enhancing the benefits of TDPL with fewer constraints.

This paper introduces enhanced DDPL techniques which provides less power consumption (almost 50 %) compared to previous techniques. The review of LPA attack is summarized in section 2. DPA resistant logic styles are presented in section 3. Section 4 contains proposed logic styles. Comparison results are carried out in section 5. Finally conclusion is presented in section 6.

2. Review of LPA attack

The LPA attack aims to recover the secret key *k* of a cryptographic device where the processed data X under attack is a function (or a portion) of *k* through the analysis of the leakage consumption. This attack was rigorously defined along with a clear five-step procedure, (P. C. Kocher *et.al,* 1999; Paul Kocher *et.al,* 2011) which is briefly recalled in the following:

1) Choose an internal m-bit signal X (i.e., the signal under attack) that depends on both the input I and the secret key k;
2) Measure leakage current $I_{leak,i}$ of the cryptographic chip by applying all 2m different input values I_i (with i=1…2m);
3) Estimate the value X_{ij} of the signal under attack X for the i-th input and j-th key guess (we do not know the key, so we have to make all possible guesses);
4) Estimate leakage H_{ij} as a function of the i-th input and j-th key guess. As discussed above, a simple but effective choice of this function is the Hamming weight $H_{ij}=H(X_{ij})$ of the signal under attack X_{ij}.
5) Find the secret key among all key guesses. This is done by evaluating the correlation coefficient $\rho(I_{leak,i},H_{ij})$ and finding the key guess that maximizes $\rho(I_{leak,i},H_{ij})$.

3. DPA resistant logic styles

3.1 SABL

Sense Amplifier Based Logic (SABL) has been one of the first full-custom DPA-resistant logic styles (S. Mangard. *et.al* 2007) SABL data encoding is based on a spatial domain conception for which data are in a complementary logic state for all the duration of the evaluation period. This information is useful to practically implement an LPA analysis because the static power consumption can be measured before the ending of the evaluation phase, obviously waiting for the steady-state condition to be satisfied, according to the settling time of the devices in a given technology and for different inputs. Following these considerations, transient simulations on SABL gates have been performed. The clock frequency has been lowered so that after the ending of the evaluation phase all signals settle to the steady-state value as occurs in a real attack scenario. Finally leakage currents have been measured for each possible input data combination. However a slight dependence between input and leakage can be detected for the AND/NAND gate due to the asymmetry of the cell.

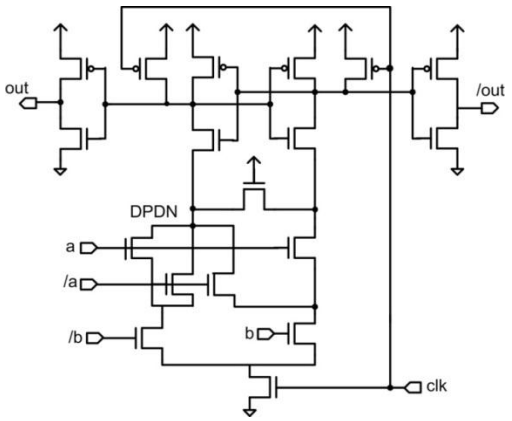

Fig.1 SABL AND/NAND Circuit

3.2 DDPL

DDPL is a DPA resistant logic style which is based on a time domain data encoding technique (M. Bucci *et.al,* 2011). In DDPL the information is represented in the time domain by forcing a positive (logic-1) or negative (logic-0) relative delay between the differential lines. Therefore, both outputs are precharged and discharged inside the operating cycles but, due to the chosen data encoding, a single control signal is sufficient as in standard dual-rail logic. During the precharge phase both differential lines are charged to V_{DD} and, in the evaluation phase those lines are discharged to V_{SS}. The information is encoded in the order with which the lines are discharged. For a logic-1, the negated line is discharged after a delay Δ with respect to the asserted one. Conversely, for a logic-0 the negated line is discharged first.

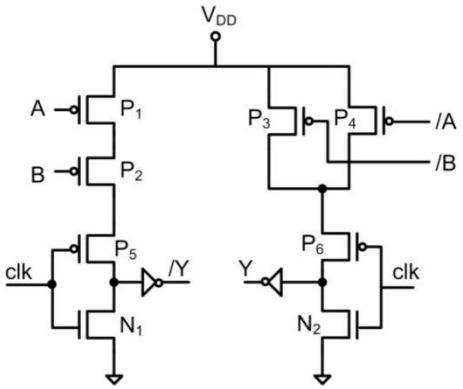

Fig.2 DDPL NAND/AND

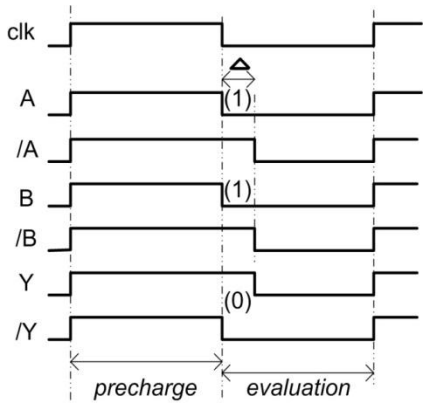

Fig.3 Timing Diagram of DDPL NAND

4. Proposed Method

In order to reduce the power consumption and to improve the performance of the circuit sleep transistors (P. S. Aswale *et.al,* 2012; R. Udaiyakumar *et.al,* 2012) were introduced in the circuit of DDPL. This makes the circuit more data independent power consumption which makes the circuit more resistive to DPA attacks.

4.1 DDPL with Sleep transistors

The below figure shows the DDPL with sleep transistors NAND/AND circuit. When circuit is idle these sleep transistors will off. So alternatively the power consumption will be reduced.

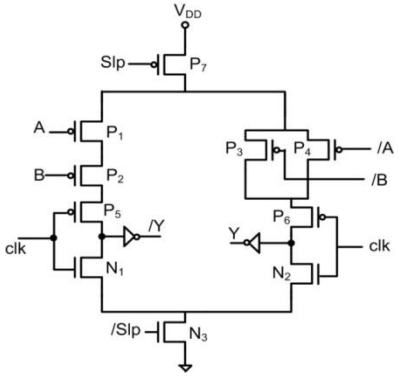

Fig.5 DDPL with Sleep transistors

4.2 Enhanced DDPL

In enhanced DDPL the logic is implemented in pull down network. This is also time domain data encoding in which precharge phase both differential lines are charged to V_{DD} and, in the evaluation phase those lines are discharged to V_{SS} as shown in below figure 6.

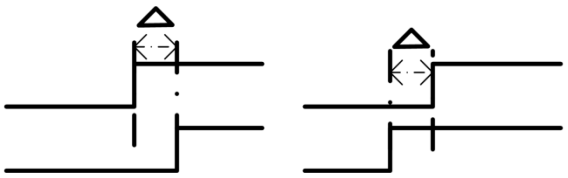

Fig.6 Data encoding in enhanced DDPL (a) Logic-1 (b) Logic-0

The information is encoded in the order with which the lines are charged. For a logic-1, the negated line is charged after a delay Δ with respect to the asserted one. Conversely, for a logic-0, the negated line is charged first. Since over the operating cycles both lines are charged and discharged once, the total power consumption is data-independent.

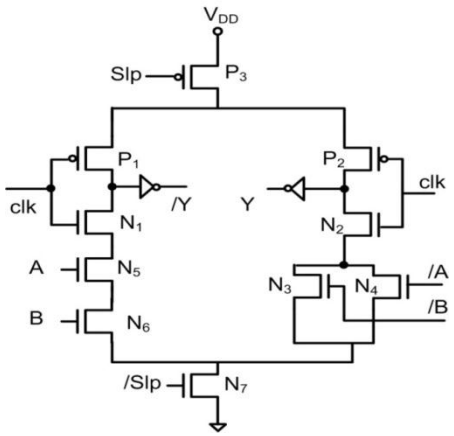

Fig.7 Enhanced DDPL

The timing diagram of enhanced DDPL NAND is shown below.

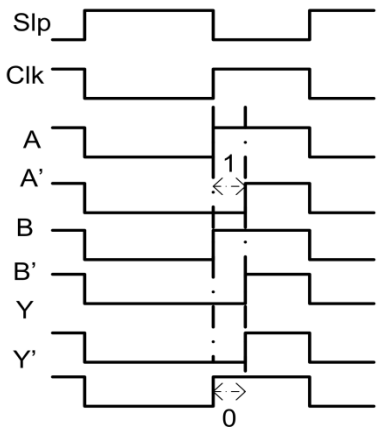

Fig.8 Timing diagram of enhanced DDPL

5. Results

This work is done by using Cadence 45-nm tool. With this enhanced DDPL the power consumption is reduced by 50% and also the delay is reduced compared to DDPL. In enhanced DDPL the power consumption is more data independent.

Table 1: Simulation results for Power and Delay

	Power (nW)	Delay (ps)
DDPL	45.15	12.34
DDPL with sleep transistors	32.47	12.21
Enhanced DDPL	25.27	10.4

Conclusion

This paper has presented a DPA resistant logic style for making the circuit used in cryptographic applications more resistible to DPA attacks. Two new logic styles were presented to improve the DPA resistance of the circuit by making data independent power consumption. Using our configuration, the DPA-resistance of the gate was improved, without any performance degradation.

References

Massimo Alioto, Simone Bongiovanni, (2014) Effectiveness of leakage power analysis attacks under process variations, *IEEE Trans. Circuits and System*

M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti,(2010) Leakage power analysis attacks: A Novel class of attacks to nanometer cryptographic circuits, *IEEE Trans. Circuits Syste*

M. Djukanovic, L. Giancane, G. Scotti, (2011) Leakage power analysis attacks: Effectiveness on DPA resistant logic styles under process variations, in *Proc. ISCA*

P. C. Kocher, J. Jaffe, and B. Jun, (1999) Differential power analysis, *Proc.CRYPTO*

Paul Kocher, Joshua Jaffe, et al: (2011) Introduction to differential power analysis, *Springer regular paper*

T. Popp and S. Mangard, (2005) Masked Dual-Rail Pre-charge logic: DPA resistance without routing constraints , in *Proc. CHES'05, Scotland,*UK, Se

M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti,(2010) Delay-based Dual-Rail Pre-Charge logic, *IEEE Trans. VLSI S*

K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, (2005) Prototype IC with WDDL and differential Routing—DPA resistance assessment, in *Proc. CHES '05, ser. LNCS Springer, U*

S. Mangard, E. Oswald, and T. Popp, (2007) Power Analysis Attacks: Revealing the Secrets of Smart Cards, *New York, NY, USA: Springer- Verlag*.

M. Djukanovic, L. Giancane, G. Scotti, A. Trifiletti, and M. Alioto, (2011) Leakage power analysis attacks: Effectiveness on DPA resistant logic styles under process variations, in *Proc. ISCAS*.

P. S. Aswale, S. S. Chopade, (2012) A low power 90nm technology based CMOS digital gates with dual threshold transistor stacking technique, *International Journal of Computer Applications*, Vol. 59, No.11,PP 47-51.

R. Udaiyakumar, K. Sankaranarayanan, (2012) Dual Threshold Transistor Stacking (DTTS) - A Novel Technique for Static Power Reduction in Nanoscale Cmos Circuits, *European Journal of Scientific Research, ISSN 1450-216X* Vol.72 No.2, pp. 184-194.

J. M. Rabaey, A. Chandrakasan, and B. Nikolic, (2002) Digital Integrated Circuits—A design perspective 2 ed. *Englewood Cliffs NJ, USA, Prentice Hall*.

T. S. Messerges, E. A. Dabbish, and R. H. Sloan, (2002) Examining smartcard security under the threat of power analysis attacks, *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552.

K. Tiri and I. Verbauwhede, (2004) A Logic Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation, in *Proc. Design, Automation and Test in Europe Conference and Exposition (DATE)*, pp. 246-251.

Ms.M.Shivani is working towards a Master of Technology in Digital Electronics and Communication Systems in prestigious Vardhaman College of Engineering, R.R.Dist, India.

Ms.C.Padmini is presently working as an Associate Professor of Electronics Comm. Engineering in prestigious Vardhaman College of Engineering ,R.R.Dist,India.