Secure IC Design Using Blur Gate

A.Gokilavani and M.Revathy

***Abstract*—Power analysis is a type of side channel analysis which utilizes the information that leaks from the power dissipation when data are processed. The use of data dependent delays helps in mitigating an attack but also leads to change in power value. The power value is changed by introducing CMOS based blur gate (BG) which helps in increasing the immunity of the cryptographic system. It is used to secure processor and channel attack resistant in IC's.**

***Index Terms*—Side channel analysis (SCA), Data dependent Delay assignment methodology, Blurgate (BG), Itohsuji algorithm**

1. INTRODUCTION

Since, provide the security of confidential data through the electronic way data exchanging process. Vast field of attacks were present in the hardware and software implemention.In cryptographic device analyze the *side channel attack (SCA)*, it will exploits the information through leakage[1]-[2]. In 1998 the *cryptography research* was presented about the *differential power analysis*. A cryptographic hardware the leakage information used by DPA, it is called power consumption [5].A cryptographic research was announced by the simple power analysis (SPA) is less powerful variant[3]. First, Hackers try to measure the power consumption of the circuit. Second the hackers try identify the computation algorithm. Third the hacker requires the plaintext and chiper text keys. The oracle was verified by using the statistical method to identify the peaks in the statistics [8]. *DP A*attacks will be clearly explained in this article. The power model will be created using the different statistical method and these power [6] models were used in the DPA. In DES algorithm are explained and analyzed the DPA attacks. The application of *DPA* on asymmetric cryptosystems was discussed [7].

Power Analysis Foundations

Now a days the digital systems are made with complementary metal oxide semiconductor (CMOS) technology [4]. First to understand the CMOS technology and analyzed the power consumption of the CMOS device. If CMOS gate changes (0 to 1or 1 to 0) the transition state, the power will be measured in VDD (VSS) pin [9]-[11]. If consider the circuit it will change more transition state. The corresponding power will be dissipated at ground or VSS pin. In synchronous design, the gates are clocked that means all gates change their state at the same time. The small resistor R_m will be used to analyzed the dissipated power. The resistor *Rm*in series between *Vdd* and source (or ground). The most essential part of the power consumptions (change of a state) are the dynamic charge and discharge. The dynamic short circuit current is measured approximately 15% [10]. This is observed by the example of an inverter Fig.1.

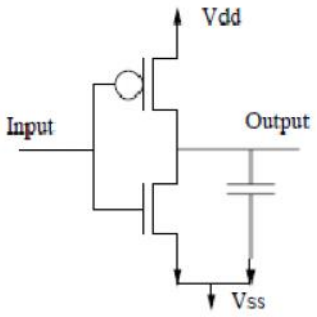

Fig.1. Inverter

An input transition results in an output transition, which discharges or charges this parasitic capacity, causing a current flow to *Vdd* (or *Vss*). This current is the dynamic charge discharge current [6]-[7]. By measuring current flow on *Vdd*. we can identify whether the output changed from 0 to 1 or not. Inherent delay of the logic structure it will reduces the propagation time, power, and area overhead [12].In differential *CMOS* logic, every output appears also in its inverted form, which means a transition always causes charge and discharge on the output and inverted output. Measuring current on *Vdd* or *Vss* (0 to 1or 1to 0), it will be used to detect whether a transition occur or not. By observing the current flow it will detect changes of the output node. Differential or standard *CMOS* logic is lower power consumption when compared precharge logic.

II. RELATED WORKS

A security-oriented delay assignment algorithm for resisting single and multi bit attacks is presented. The algorithm enables a reduction of the correlation between the processed data and the consumed current by utilizing the data-dependent delays as a source of correlated noise. This is done while minimizing the area overhead, propagation time, and power. We show that for the same security level this new algorithm provides X2 and X6 more area efficiency, andX1.5 and X2.25 higher frequencies than a permuted path delay assignment and random embedding of delay elements.

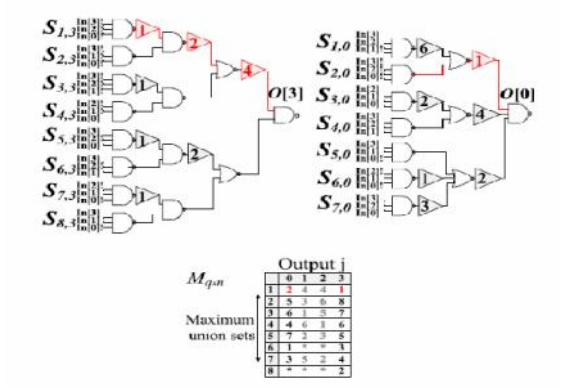

Fig.2. Partial gate level of the SBOX and its corresponding *mates* matrix *M*.

Fig.2. shows two different gate-level implementations for outputs *O*[3] and *O*[0] of a4-bit Add Key_SBOX block with embedded delays. In Fig.2.the delay elements (buffers) are denoted by triangles and the number inside each buffer is proportional to its delay. Delay is defined in units of a single minimum sized buffer. Note that the delays are embedded into the original design. The colored paths and the *mates* matrix *M* in Fig.2. will be used in later examples. The correlations between the measured currents and the hypothesized current for a *multibit* hypothesis. The correlations for all the keys are plotted. Fig.2. refers to the original design with embedded delays. The correlation that corresponds to the correct key is marked in black, and the one that corresponds to the best wrong key is marked in dashed line. This property can be intensified to SNR values smaller than 1 with increase in the unit delay value.

III. PROPOSED SYSTEM

In this project, we introduce a new CMOS-based blurring gate (BG) which increases the immunity of a cryptographic system to these attacks. The BG switches randomly between two operational-modes, static and dynamic. When embedded in the crypto-core, the BGs enforce different and unpredictable arrival times (propagation delays) along the logic paths from inputs to outputs. This results in blurred power profiles and random propagation delays, which in turn mitigate power attacks.

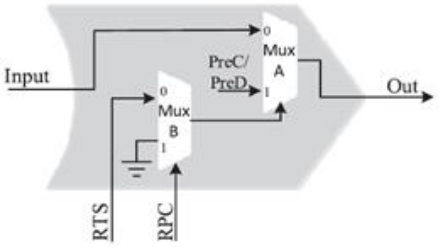

Fig.3. Structure of the BG unit

Simulationresults and security analyses using system with embedded BG units with standard 65-nm technologyclearly show higher immunity to power analysis attacks over other standard-library based randomization technologies. The signal-to-noise ratio (SNR) decreases rapidly below 1.A BG unit consists of two degenerated 2 × 1 mux components. Its structure is shown in Fig.3. An example of cascading a standard CMOS NAND gate to a BG unit is shown in Fig. 4.

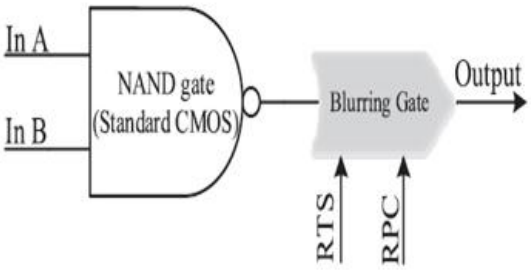

Fig.4. A Standard CMOS NAND gate to BG unit

When the static mode is activated, the BG unit functions as a standard CMOS NAND gate. When the static mode is disabled, the BG unit functions as a (dynamic) precharge or predischarge logic. This flexible configuration of the operational mode allows to randomize the power profile. The two operation modes of a

BG unit, static and dynamic, depend on the internal voltage level in the PreC/PreD signal which is permanently set during the design phase. When the internal PreC/PreD is connected to *V*DD, the BG operates in the static or dynamic precharge (*p*) modes, and when the internal PreC/PreD is connected to GND.It operates in the static or dynamic predischarge (*pd*) modes. A BG unit has two external control signals, *random transitions sequence (RTS)* and *random phase control (RPC)*, which are governed externally. The RPC signal is the random signal fed by a sequence generator, and determines the operation mode of the gate. In the case where RPC is logical "1," the BG is set to a transparent (*t*) mode which implies that the system will propagate signals in a static CMOS-like logic. In the case of logical "0," the BG is set to precharge (*p*) or predischarge mode (*pd*) in which the output operates like in the first precharge/predischarge phases of dynamic logic. The RTS signal impacts the static or dynamic behavior, i.e., it determines whether a precharge/predischarge phase or static-like evaluation (*e*) will take place.

Notice that the duration of the *e* phase can be more than one cycle. The RTS signal arbitrarily toggles between "0" and "1."In order to avoid timing violations due to the RTS signal in a simple way, the designer can block the RTS signal (by using an AND operation) with the system clock.

V. ITOH TSUJI MULTIPLICATIVE ALGORITHM

Elliptic Curve Cryptographic algorithm includes addition, squaring, multiplication and division (or inversion).The security of ECC relies on the difficulty of solving Elliptic Curve Discrete Logarithm Problem or ECDLP. Here introduce a delay assigned BG method to secure multiplicative inversion algorithm in ECC. Given two integers 'a' and 'm', find modular multiplicative inverse of 'a' under modulo 'm'. The modular multiplicative inverse is an integer 'x' such that. a x ≡ 1 (mod m) The value of x should be in {0, 1, 2, … m-1}, i.e., in the ring of integer modulo m. The multiplicative inverse of "a modulo m" exists if and only if a and m are relatively prime (i.e., if gcd (a, m) = 1).

ALGORITHM 1

```
Input a,m;
Output x;
{
a = a%m;
for (int x=1; x<m; x++)
if ((a*x) % m == 1)
return x;
}
```

IV. EXPERIMENTAL RESULTS

The proposed has been simulated and the synthesis report can be obtained by using Xilinx ISE 12.1i.The power, SNR and current values are analyzed by TINA software The various parameters used for computing existing and proposed systems with Spartan-3 processor are given in the table 5.1.

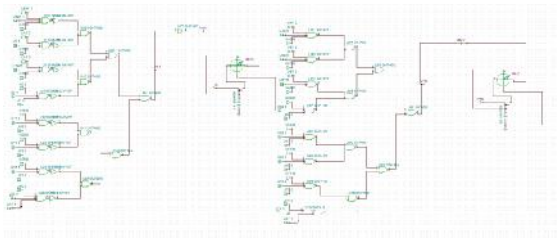

Fig.5.Layout of S-Box without and with delay assignment methodology

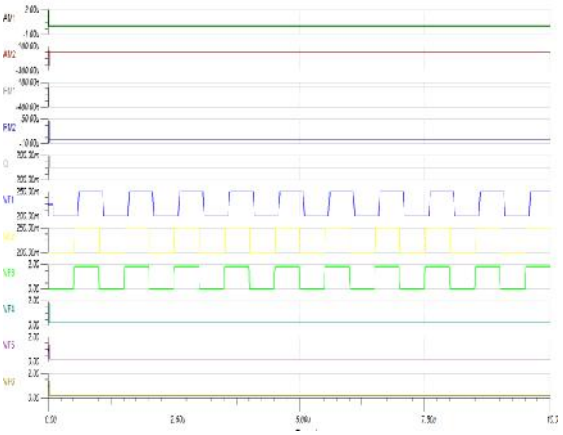

Fig.6. Power and current analysis

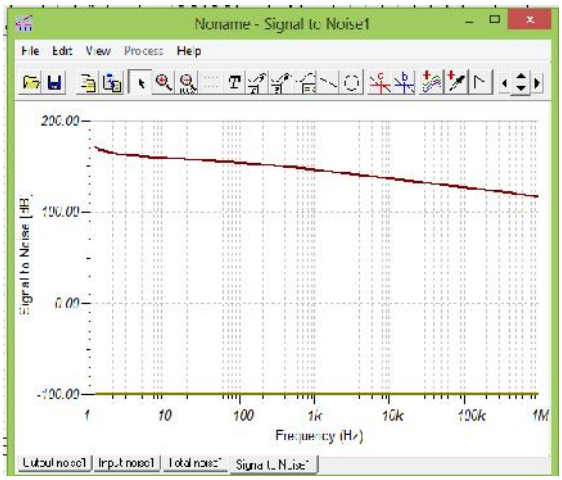

Fig.7.SNR Results For S-Box Structure with and without Delay Assignment Methods

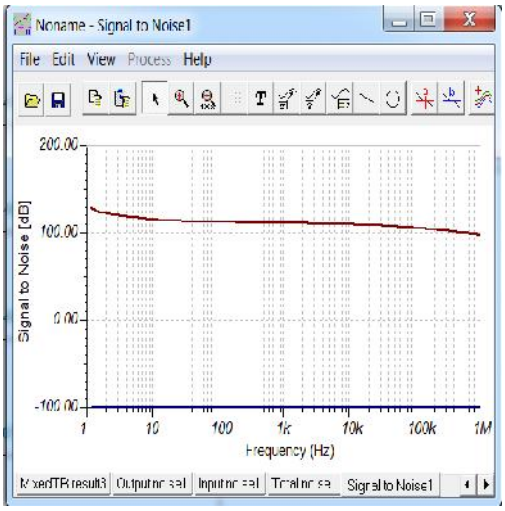

Fig.10. SNR Value for Blur Gate Design

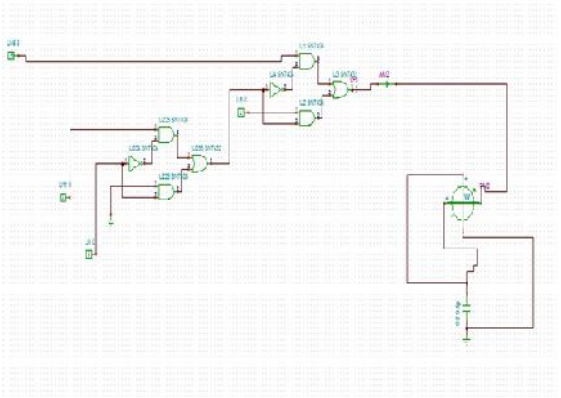

Fig.8. Layout of CMOS Based Blur Gate Design

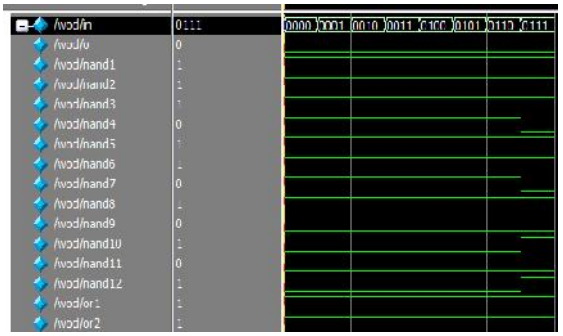

Fig.11. Output For S-Box Structure Without Delay AssignmentMethod

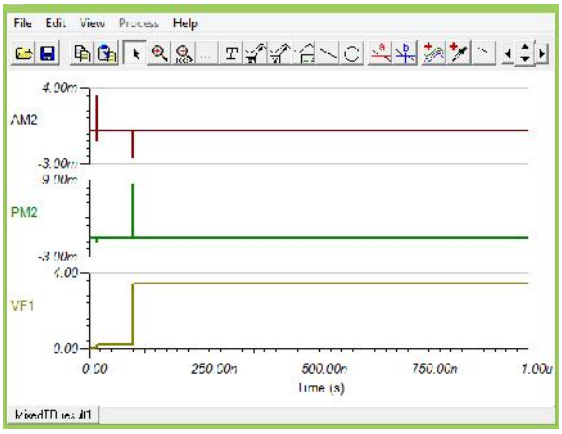

Fig.9. Power Value for Blur Gate Design

Fig.12.Output For S-Box Structure With DelayAssignment Method

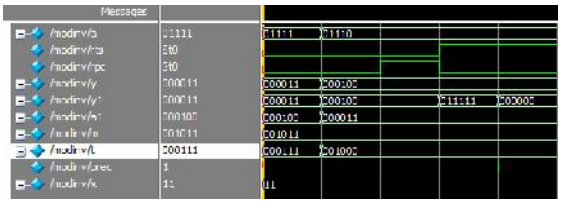

Fig.13. Output for BG in Itoh and Tsujii Multiplicative Inverse algorithm

Table I

Comparison between the delay assignment and blur gate

S.No	Parameter	With Delay Assignment	Without Delay assignment	Blur gate
1	Slice	4	3	2
2	LUT	6	5	4

The delay assignment and blur gate has been simulated and the synthesis report can be obtained by using Xilinx ISE 12.1.

Table II

Comparison between Power, SNR, Current Variation Of Delay Assignment and Blur gate

S. No	Parameter	Without delay	With delay	Blur gate
1	Power(w)	50u	80m	9m
2	Current(A)	100u	20m	4m
3	SNR(dB)	160dB	130dB	120dB

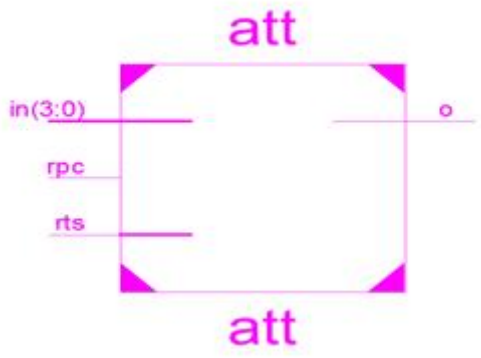

Fig.14. RTL Schematic of Blur gate (BG)

VI. PERFORMANCE ANALYSIS

The Figure given below shows that there is a considerable reduction in time and area based on the implementation results which have been done by using Spartan-3 processor. The proposed algorithm significantly reduces area consumption when compared to the existing system.

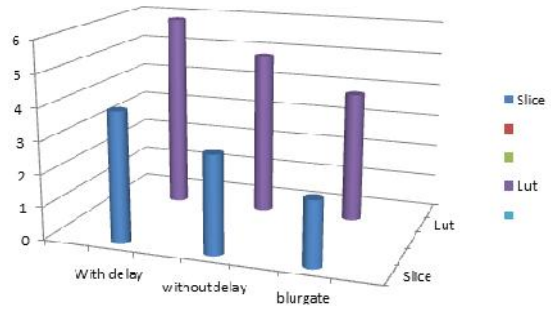

Fig.15. Comparison of Slice And LUT Between Delay Assignment And Blur Gate

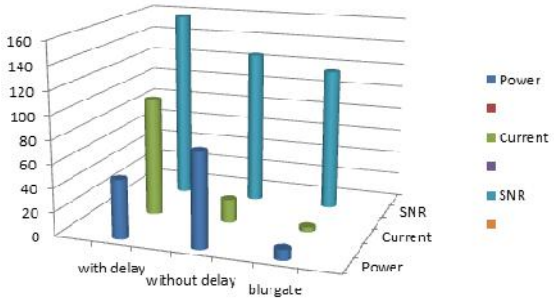

Fig.16. Comparison of Power, SNR and Current variation Between Delay Assignment and Blur Gate

VII. CONCLUSION

Power analysis attacks are considered to be powerful side channel attacks on cryptographic circuits. Power analysis countermeasures rely on the fact that the consumed energy per cycle is data-dependent. The attack procedure is based on the power-supply instantaneous power rather than the energy per cycle .In this project, presented and analyzed a new CMOS-based blurring gate (BG) which can be embedded in any digital design to increase the immunity of the system to power analysis attacks. The BG switches randomly and independently between two operational modes static and dynamic (precharge or pre discharge). Compared the efficiency of the proposed BG technique to the efficiency of the RPL and RDI technology analysis and simulation results indicate that the proposed approach is a very efficient technique to counteract power attacks.

Blur Gate can be implemented in Kastruba multiplier which is a fast multiplication algorithm. Thus output of the Kastruba multiplier is protected by using the blur gate. To introduce the blur gate in Kastruba multiplier, it will reduces the multiplication steps of two n digit number.

A.Gokilavani, PG Scholar, Dept. of ECE, PSNA CET
M.Revathy, Assistant Professor , Dept. of ECE,PSNA CET.,
Dindigul, India. (kokiilavaani@gmail.com)

REFERENCES

[1] Itamar Levi, Alexander Fish, and OsnatKeren, "CPA Secured Data- Dependent Delay-Assignment Methodology," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 25, no. 8, pp. 608–620, Feb.2017, doi: 10.1109/TVLSI.2016.2592967.

[2] S.Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked AES hardware implementations," in Cryptographic Hardwareand Embedded Systems, J. R. Rao and B. Sunar, Eds. Heidelberg,Germany: Springer, 2005, pp. 157–171.

[3] M.Alioto, S.Bongiovanni,M. Djukanovic, G.Scotti, and A. Trifiletti,"Effectiveness of leakage power analysis attacks on DPA- resistant logic styles under process variations," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 61, no. 2, pp. 429–442, Feb. 2014.

[4] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18-µm CMOS with resistance to differential power analysis side channel attacks," IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[5] S. Hajra and D. Mukhopadhyay, "Reaching the limit of nonprofiling DPA," IEEE Trans. Comput.-Aided DesignIntegr.,vol.34,no.6,pp.915927,Jun.2015,doi:10.1109/TCAD.2014.2387830.

[6] C.Clavier ,J.-S. Coron, andN.Dabbous, "Differential power analysisthepresence of hardware countermeasures," in Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst. Berlin, Germany: Springer, 2000,pp. 252–263.

[7] M.Avital,H. Dagan, O. Keren, and A. Fish, "Randomized multitopology logic against differential power analysis," IEEETrans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 4, pp. 702–711, Apr. 2015.

[8] M.Bucci ,M.Guglielmo, R. Luzzi, and A. Trifiletti, "A power consumption randomization countermeasure for DPA-resistant cryptographic processors," in Integrated Circuit and System Design. Power and Timing Modelling, Optimization and Simulation, E. Macii, V. Paliouras, and O.Koufopavlou, Eds. Heidelberg, Germany: Springer, 2004,pp. 481–490.

[9] I. Levi, O. Keren, and A. Fish, "Data-dependent delays as a barrier against power attacks," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 62,no. 8, pp. 2069–2078, Aug. 2015, doi: 10.1109/TCSI.2015.2452371.

[10] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smartcard security under the threat of power analysis attacks,"IEEETrans.Comput., vol. 51, no. 5, pp. 541–552, May 2002.

[11] G.Goodwill,B.Jun,J.Jaffe,andP.Rohatgi, "A testing methodology for side-channel resistance validation," in NIST Non-Invasive Attack Test.Workshop, 2011.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advancesin Cryptology, M. Wiener, Ed. Heidelberg, Germany: Springer, 1999,pp. 388–397.