Blur Gate Based Data Leakage Reduction Technique

P.Kanmani, Mr.SP.Senthil Kumar M.E.,
Pg Scholar, Assistant Professor
Department of ECE
Shanmuganathan Engineering College, Arasampatti

Abstract

Globalization of microchip fabrication opens the possibility for an attacker to insert hardware Trojans into a chip during the manufacturing process. While most defensive methods focus on detection or prevention, a recent method, called Randomized Encoding of Combinational Logic for resistance to Data Leakage (RECORD),uses data randomization to prevent hardware Trojans from leaking meaningful information even when the entire design is known to the attacker.Both RECORD and its sequential variant require significant area and power overhead.In this paper, a Time-Division Multiplexed version of the RECORD design process is proposed which reduces area overhead by 63% and power by 56%. This time-division multiplexing (TDM) concept is further refined to allow commercial off the shelf (COTS) products and IP cores to be safely operated from a separate chip. We also Propose a novel Boolean functional properties of the cube stripping function and logic restoration to improve a security of logic circuitsThese new methods tradeoff latency and energy use to accomplish area and power savings and achieve greater security than the original RECORD process.

I. INTRODUCTION

Since increasingly confidential data are being exchanged on electronic way an ever greater importance is attached to the protection of the data. Where cryptosystems are being used in real applications not only mathematical attacks have to be taken into account. Hard and software implementations themselves presents a vast field of attacks. Side-Channel-Attacks exploit information that leaks from a cryptographic device. Especially one of these new attacks has attracted much attention since it has been announced. This method is called Differential Power Analysis (DPA) and was presented in 1998 by Cryptography Research. DPA uses the information that naturally leaks from a cryptographic hardware device, namely the power consumption. A less powerful variant, the Simple Power Analysis (SPA) was also announced by Cryptography Research. What does a DPA attack require? First, an attacker must be able to precisely measure the power consumption. Second, the attacker needs to know what algorithm is computed, and third an attacker needs the plain- or cipher texts. The strategy of the attacker is to make a lot of measurements, and then divide them with the aid of some oracle into two or more different sets. Then, statistical methods are used to verify the oracle. If and only if the oracle was right, one can see noticeable peaks in the statistics. This vague description of a DPA attack should be clarified in this article. In section 2, a power model is developed and related to the statistical methods used in DPA .Thereafter, a DPA attack is explained on the grounds of the DES. In the third section, a concrete implementation of the DPA is discussed. The section begins with a C++-model which will turn out to be useful to verify some countermeasures against DPA attacks

II. LITERATURE SURVEY

Basel Halak et al evaluates the security of cryptographic circuits designed with this technology against the newly developed LPA. Two forms of LPA are investigated, one is based on differential power analysis (LDPA) and the other based on Hamming weight analysis (LHPA).

Rohit Lorenzo et al propose a new design data retention scheme which consist PMOS helper transistors which reduces leakage current while saving exact logic state.

Bin Chen et , a mal proposed method of observability analysis and state estimation for PMU-measured power system, and an index of measurement redundancy degree considering critical measurements is designed

Cecilia Garcia Martin et al introduced new low-power methodology in order to reduce the leakage current while maintaining the speed advantages of the data driven dynamic logic. A sleep switch transistor is used in the data driven dynamic circuits in order to force a sleep mode asynchronously.

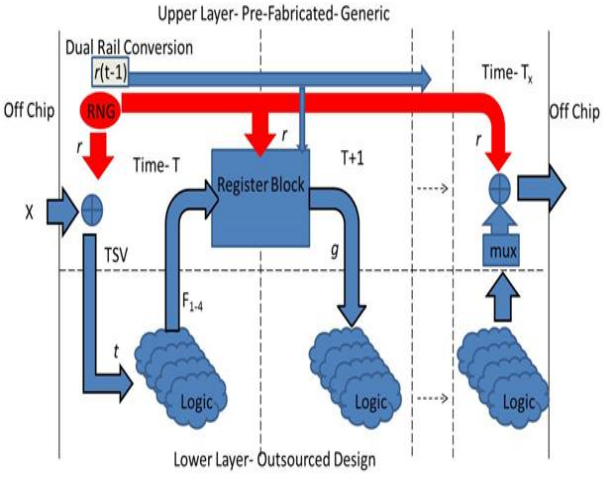
B.M. Damian investigates its efficiency, having different FPGAs under test. The main characteristics of

a suitable test environment are highlighted. Additionally, this paper proposes a countermeasure against this type of attack.

Trey Reece et al examines the impact of 18 hardware Trojans inserted into an AES (Advanced Encryption Standard) cryptographic circuit in terms of area, leakage power, and dynamic power.

III. EXISTING SCHEMES

Travis presents a Time-Division Multiplexed version of the RECORD design process which reduces area overhead and power. This time-division multiplexing (TDM) concept is further refined to allow commercial off the shelf (COTS) products and IP cores to be safely operated from a separate chip. These new methods tradeoff latency (5.3× for TDM and 3.9× for COTS) and energy use to accomplish area and power savings and achieve greater security than the original RECORD process.



A design prepared using the sequential RECORD method resists data leakage effectively, however, there are a small percentage of cases in which an attacker could decode the design with a Trojan placed on the insecure lower tier if random assembly options are not taken during the assembly process, as discussed later. Table I shows the possible combinations of outputs from the lower tier (F1, F2, F3, and F4) and the returning input to the lower tier, g, which would allow the attacker to infer the random bit, provided they knew which signal was associated with F1–4. Note that these five signals are the only signals an attacker would have access to on the lower tier. In 25% of cases, the random bit could be inferred. To be successful, however, the attacker must know which physical logic block is which, i.e., which is F1, F2, F3, and F4. As can be seen from Table I, the order matters. The attacker must also know which bit the intermediate outputs are being referenced to prior to being stored in the registers. This can be either r1 or r2, and is easily changed by rewiring the select signals on the multiplexers. Finally, the attacker must know to which bit the returning signal g(t + 1) is referenced.

IV. PROPOSED SCHEME

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. Simulation results and security analyses using system with embedded BG units with standard 65-nm technology, clearly show higher immunity to power analysis attacks over other standard-library based randomization technologies. The signal-to-noise ratio (SNR) decreases rapidly below 1 for a relatively small amount of BGs even with a large number of power traces in the worst case test environment.

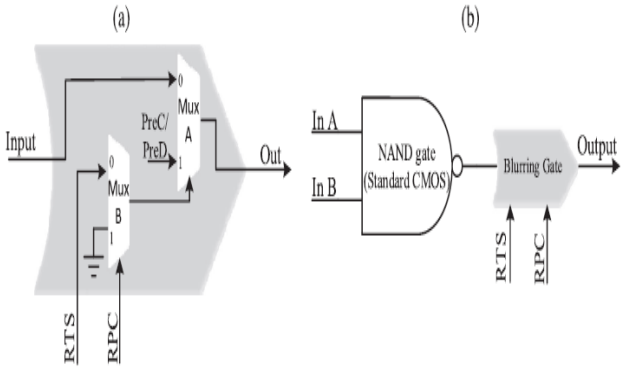


Fig.4.1: Blur Gate

A BG unit consists of two degenerated 2 × 1 mux components. Its structure is shown in Fig. 2(a). An example of cascading a standard CMOS NAND gate to a BG unit is shown inFig. 2(b). When the static mode is activated, the BG unit functionsas 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 operation 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. The precharge and predischarge BG unit truth tables are presented in Tables I and II, respectively.

As shown in Fig. 2, when the internal PreC/PreD is connected to VDD, 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/predischargephases of dynamic logic. The RTS signal impacts the staticor 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. By doing so, it ensures the BG evaluation (e) mode operations at the falling edge of the clock, which certainly complies with the worst timing path. Notice that it implies that p/pd phases can occur only in the first half of the clock cycle whereas the e phase is forced in the second half. In general, if the RTS signal is not blocked by an AND with the clock, the RPC signal has a limited time interval in which it can remain in logic "0." It is important to note that the designer must ensure that along the critical path, the BG units are set to transparent (t) or evaluation (e) modes for a sufficient time (larger than the minimum time, tmin) before the next rising edge of the clock. The time tmin is defined as the total of setup time, tsu, and clock jitter of all different clock phases; meaning, tminΔ=tsu + tJ−L, where tJ−L is the jitter time induced by the clock phases which are incorporated with the combinatorial logic.

We also Propose a novel Boolean functional properties of the cube stripping function and logic restoration to improve a security of logic circuits

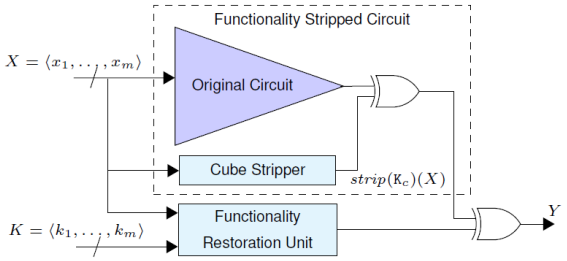


Figure cube stripper

V. SIMULATION RESULTS

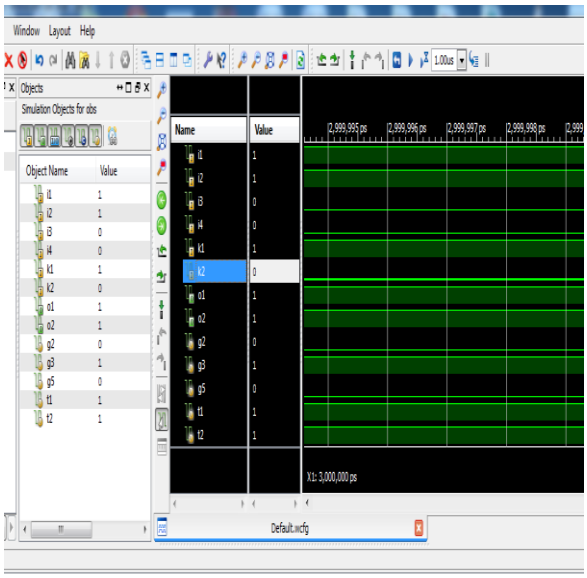


Fig. Simulation result graph

VI. PERFORMANCE ANALYSIS

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

Benchmark		slices	LUT	IOB	delay(ns)
c432	conventional	61	108	43	24.813
	modified	61	108	49	24.018
	Stripper	63	108	44	24.813
C880	conventional	63	108	86	19.503
	modified	67	115	92	18.27
	Stripper	63	109	87	19.503
C1355	conventional	45	78	73	12.499
	modified	47	84	79	12.703
	Stripper	44	79	74	12.950
C2670	conventional	84	160	373	15.094
	modified	85	162	373	21.938
	Stripper	85	162	374	21.938

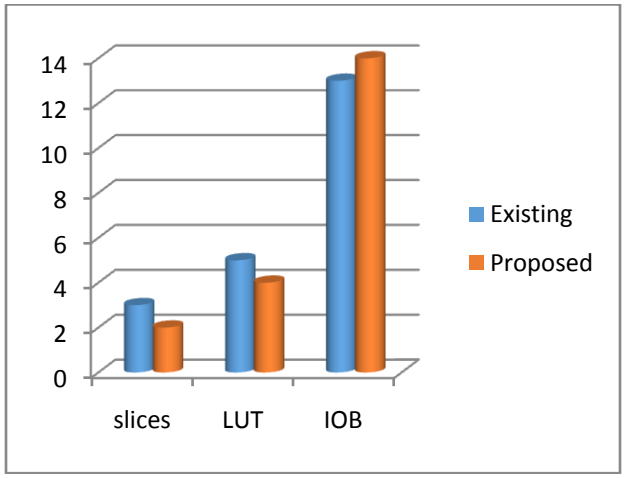


Fig. performance measure

VII. CONCLUSION

In this project, we presented and analyzed a new CMOS-based blurring gate (BG) which can be embedded in any digital design to increases the immunity of the system to power analysis attacks. The BG switches randomly and independently between two operational modes—static and dynamic (precharge or predischarge). We compared the efficiency of the proposed BG technique to the efficiency of the RPL and RDI technologies. As opposed to RPL, which employs random precharge, in a BG based implementation the embedded BG units provide randomand non-correlative operation (as precharge/predischarge, or static logic) at different places in the logic cone. As compared to RDI, which changes the input delays, in a BG based implementation the delays are due to the special allocation of the BGs, or due to the phased clock signal. We showed that the impact of a BG based implementation of a crypto-module on power analysis is three-fold: blurred power profiles, random propagation delays and random initial conditions. Analysis and simulation results indicate that the proposed approach is a very efficient technique to counteract power attacks.

REFERENCES

[1] T.S.Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, May 2002.

[2] 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.

[3] M.Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 2, pp. 355–367, Feb. 2010.

[4] A.Wang, M. Chen, Z.Wang, and X.Wang, "Fault rate analysis: Breaking masked AES hardware implementations efficiently," IEEE Trans. Circuits Syst. II, Express Briefs, vol. 60, no. 8, pp. 517–521, Aug. 2013.

[5] P.Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology—CRYPTO, M. Wiener, Ed. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.

[6] S.Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. New York, NY, USA: Springer-Verlag, 2008.

[7] K.Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in Proc. Conf. Design, Autom., Test Eur.—Vol. 1, Washington, DC, USA, 2004, p. 10246.

[8] M.Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 7, pp. 1147–1153, Jul. 2011.

[9] K.Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in Proc. 28th Eur. Solid-State Circuits Conf. (ESSCIRC) 2002, 2002, pp. 403–406.

[10] C.Monteiro, Y. Takahashi, and T. Sekine, "DPA resistance of chargesharing symmetric adiabatic logic," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), 2013, pp. 2581–2584.