Ring Oscillator Based True Random Number Generator

Ajay Kiriti Kapparada[1], P.S.K.Ganesh Kumar[2],

[1]P.G Student, Kakinada Institute of Engineering and technology, korangi , JNTUK , A.P, INDIA

[2]Assistant professor, Kakinada Institute of Engineering and technology, korangi , JNTUK , A.P, INDIA

[1]ajay.4a6@gmail.com, [2]pganesh66@gmail.com

***Abstract*— True random number generators (TRNGs) are ubiquitous in data security as one of basic cryptographic primitives. They are primarily used as generators of con_dential keys, to initialize vectors, to pad values, but also as random masks generators in some side channel attacks countermeasures. As such, they must have good statistical properties, be unpredictable and robust against attacks. This paper presents a contact-less and local active attack on ring oscillators (ROs) based TRNGs using electromagnetic _elds. Experiments show that in a TRNG featuring _fty ROs, the impact of a local electromagnetic emanation on the ROs is so strong, that it is possible to lock them on the injected signal and thus to control the monobit bias of the TRNG output even when low power elec-tromagnetic _elds are exploited. These results con_rm practically that the electromagnetic waves used for harmonic signal injection may rep-resent a serious security threat for secure circuits that embed RO-based TRNG.**

Keywords— **CMOS digital integrated circuits, feedback oscillators, silicon-on-insulator, Active attacks, EM injections, IEMI, Ring oscillators,TRNGs.**

I. INTRODUCTION

True random number generators (TRNGs) are essential in data security hard-ware. They are implemented to generate random streams of bits used in cryp-tographic systems as con_dential keys or random masks, to initialize vectors, or to pad values. If an adversary is able to change the behavior of the generator (for instance if he can change the bias of the generated stream of bits), he can reduce the security of the whole cryptographic system.

Surprisingly, there are not many papers dealing with physical attacks on random number generators. The only practical attack to the best of our knowledge, was published by Markettos and Moore. In their attack, the attacker targets

Integrated Circuit (IC). Markettos and Moore inject a sine wave signal onto the power pad of the device in order to intentionally modify the operating conditions of the two ROs and thus to get a biased output signal. Within this context, our main contribution is an electromagnetic (EM) attack on the RO based TRNG that can be seen as a signi_cant improvement of the attack introduced in. In our attack, the attacker alters the entropy extractor by injecting an EM signal into the device rather than by inducing a harmonic signal on the power pad.

The EM injection is contactless and does not require any access to the power line. The procedure may be applied to ROs operating at higher frequencies than the cut-o_ frequencies of the power pad and the supply/ground network. the proposed attack may work on generators featuring separated power and ground nets for each RO. Note that this technique is used sometimes in order to decouple the ROs and thus to maximize the entropy per bit at the generator's output.

In real cryptographic devices, the embedded TRNG is often built using more than two ROs (a 2-RO TRNG targeted in is rather exceptional). For this reason, the EM attacks presented in this paper are evaluated on a TRNG using as much as 50 ROs. This kind of TRNG was considered to be invulnerable up to now.

II. A RING OSCILLATOR (RO) BASED TRNG IMPLEMENTED

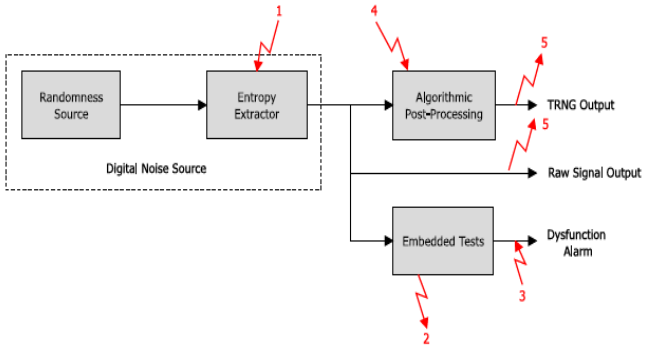
This section discusses the TRNG threats and describes briey the generator adopted as a design under test (DUT) in the rest of the paper.

The general structure of a TRNG is depicted in Figure 1. The generator is composed of:

→ A digital noise source (randomness source and entropy extractor) that should give as much entropy per bit as possible, enable a sucient bit-rate and be robust to environmental (voltage, temperature) variations.

→ An algorithmic post-processing could be added at the output of the TRNG to enhance statistical properties without reducing the entropy.

→ In some cases, the designer could add some embedded tests to evaluate on-chip the quality of the randomness source in real time or to detect online the generator's permanent or temporal failure. However, advanced and complex statistical tests are time and energy consuming. Therefore, the functionality and the quality of a TRNG can only be periodically tested on-chip.



Passive (2, 5) and active (1, 3, 4) attacks on a TRNG general structure

A. TRNG Threat Model

Two types of attacks on TRNGs can be considered: passive and active attacks. Passive attacks collect some information about the generator in order to predict future values with a non negligible probability (attacks 2 and 5 in Figure 1 { see arrow orientation). Active attacks tend to modify the behavior of the generator in order to control somehow its output (attacks 1, 3, and 4 in Above Figure). According to Figure, the adversary may target di_erent parts of the TRNG in di_erent ways. We could expect, that the statistical tests (simple embedded tests or complex external tests) could detect the attack. One could also argue that the algorithmic postprocessing would reduce the force of the attack. However, algorithmic post-processing is missing in some generators or embedded tests are not used, because the generator is "provably secure" . Nevertheless, it is a common practice in applied cryptography that the security of all building elements is evaluated separately. For this reason, evaluation of the robustness of
the generator and all its parts is of great interest.
Many sources of randomness such as thermal noise, 1/f noise, shot noise or metastability can be used in TRNGs. A good source of randomness should not be manipulable (and therefore not attackable) or the manipulation should be prevented. For example, the thermal noise quality can be guaranteed by controlling the temperature. It is thus reasonable to expect that attacks will not target the source of randomness.

B. RO-based TRNG

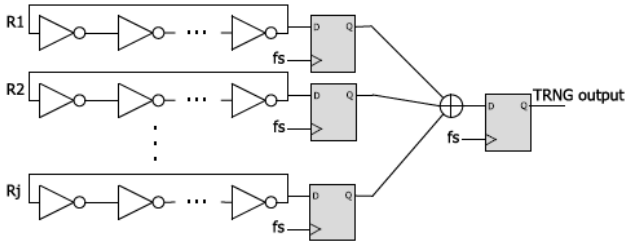
A jittery clock generated by a RO is the most common type of source of random-ness used in TRNGs. ROs are easy to implement in both ASICs and FPGAs. Commonly used TRNG principle employing several ROs was proposed in and enhanced. The resulting architecture shown in Figure below represents one of the simplest TRNG structures that can be implemented in FPGAs. It needs only NOT gates (for implementing ROs), ip-ops (as samplers) and a large XOR gate (entropy collector). A mathematical model of the TRNG that guarantees enough entropy in the output bit and thus the robustness and security. In their model, ROs are assumed to be independent.

The generator has several parameters that can be tuned: number of elements composing ROs, number of ROs and the sampling frequency. Modifying these parameters, the designer can change the statistical properties of the random stream of bit produced by the TRNG. For example, for a sampling frequency of 100 MHz, the generator composed of 25 ROs, each using 3 NOT gates, generates stream of bits passing the NIST and DIEHARD tests even without post-processing .

III. Experimental Setup

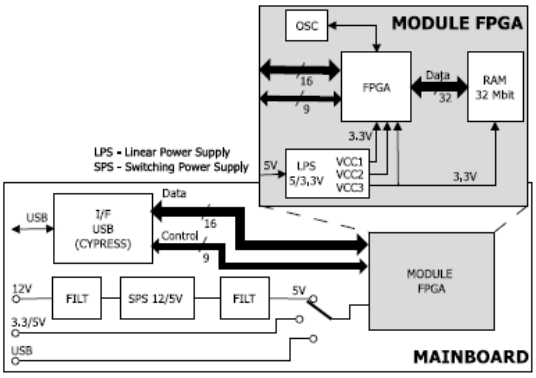
A. TRNG Implementation

The EM attacks were realized on a board featuring ACTEL Fusion FPGA. The board is dedicated to evaluation of TRNGs. Special attention was payed to the power supply design using low noise linear regulators and to the design of power and ground planes. It is important to stress that the board was not specially designed to make the EM fault injection or side-channel attacks easier, as it is



RO-based TRNG.

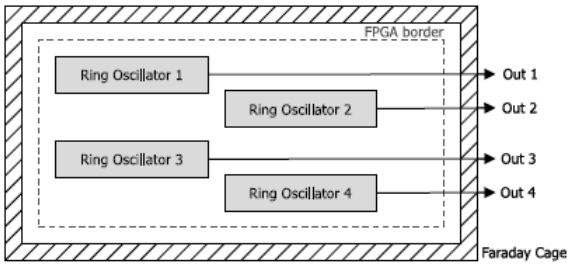
the case of the SASEBO board . It can be seen in Figure below, that the FPGA module was plugged into the motherboard containing power regulator and USB interface.



Block diagram of the board dedicated to TRNG testing

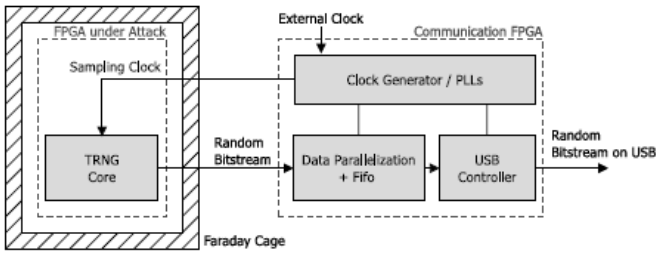
In order to demonstrate that the EM injection can disturb both RO and TRNG behavior, we performed attacks on two kinds of implementations:
→The _rst one was composed of four 3-element ROs. It was aimed at the measurement of the phase di_erence between four generated clocks.This implementation will be called Target#1.

→ In the second implementation depicted in below Figure , the TRNG core was implemented in an FPGA board under attack. Another board that was protected from EM emanations, generated reference clock signals, read data from TRNG and communicated with computer. We decided to separate the communication from random data generation in order to be sure that it was the TRNG that was faulty, not the communication. The communication module is composed of a serial to parallel converter, a FIFO and a USB controller. USB interface throughput (up to 20 MB/s) was sucient to handle
the bit rate of the TRNG. The FIFO guarantees that no data are lost during



Implementation for the measurement on ROs - Target#1

the transfer. Two signals were exchanged between the boards: a clock signal coming from the communication board and the random bitstream produced by the TRNG inside the FPGA under attack. These two signals were monitored with an oscilloscope during the attack in order to ensure that their integrities were untouched. This implementation is called Target#2.



TRNG testing architecture - Target#2

In both cases, ROs were composed of three inverters (NOT gates), giving the working frequencies of about 330 MHz. For Target#2, the TRNG was composed of 50 ROs. A sampling clock of 24 KHz was generated in an embedded PLL. This sampling frequency was chosen in order to make a 2-RO TRNG pass the NIST statistical tests. In general, decreasing the speed of the sampling clock will improve the behavior of the TRNG (the jitter accumulation time will be longer). Moreover, we used more ROs than Wold and Tan in (50 versus 25). We stress that the TRNG featuring 50 ROs should pass FIPS, and NIST statistical tests under normal conditions without any problems.

B. EM Injection Platform

The EM injection platform is presented in above Figure. The platform embeds a power injection chain supplying the micro-antenna, but also two other chains:
one for controlling the whole platform and the other one for data acquisition and storage.
The main element of both control and data acquisition chains is a personal computer (PC), which:
→controls the amplitude and the frequency of the sine waveform signal provided by the signal generator to the input of the 50 W power ampli_er,
→ positions the micro-antenna above the IC surface thanks to the XYZ motorized stages,
→collects data provided by the power meter, connected to a bi-directional coupler, in order to monitor the forward ($P_{forward}$) and reected ($P_{reected}$) powers,
→ sends con_guration data to the ACTEL Fusion FPGA and supplies target boards via USB,
→stores the time domain traces of all signals of interest acquired using the oscilloscope; in our case, the outputs of the four ROs (Target #1 - Out_1 to Out_4) and the TRNG output (Target #2).

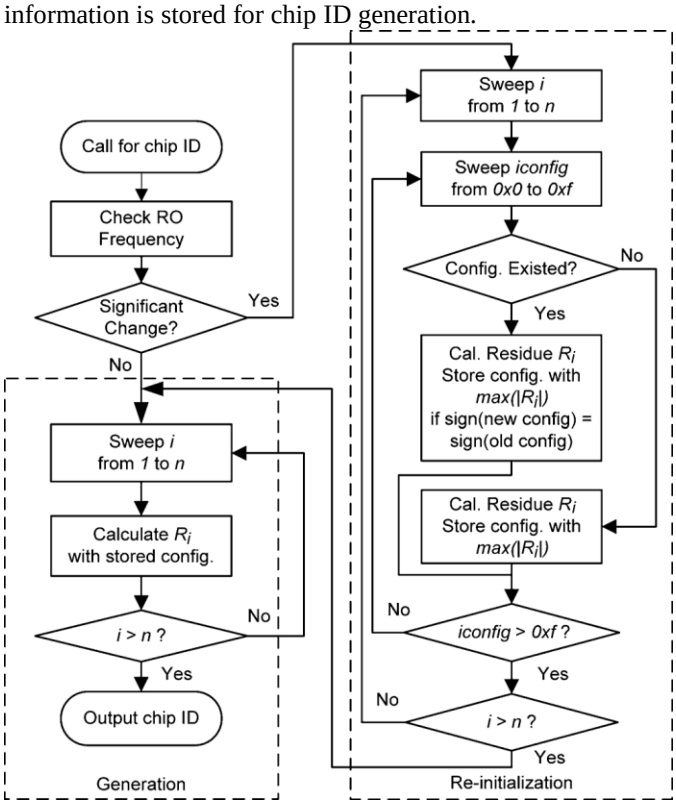
C .Attack Description

Inside the EMC table top test enclosure, the probe was located in the close vicinity of the FPGA plastic seal (the FPGA packaging was left intact), i.e. at a distance of roughly 100 _m from the DUT packaging. In order to maximize the impact of EM injections, the tip of the probe was placed near ROs implemented inside the FPGA.
→The _rst set of experiments, realized on Target#1, was aimed at analyzing the inuence of EM injections on the ROs. The EM signals power level Pforward was set successively to [34 nW ; 340 _W ; 1 mW ; 3 mW], in a frequency range [300 MHz { 325 MHz]. With a sampling rate of 20 MS/s, we acquired 10 traces on each of the four oscilloscope channels, in order to record:
a)Out1, the signal provided by the RO#1 used as a trigger to synchronize the oscilloscope.
b)Out2 to Out4, the signals provided by RO#2, RO#3 and RO#4.
Finally, all acquired data were analyzed o_ line according to several criteria. Among them, one is the mutual information. The phase di_erence between the oscillating signals Out1 and Out3 with EM injection.
→The second set of experiments aimed at studying the behavior of a complete TRNG (Target#2) under EM emanation attacks. For each con_guration, the TRNG output bitstream was stored and analyzed with and without EM injections. This latter set of experiments was conducted with a periodic signal of 309.7 MHz. This frequency corresponded to the value maximizing the coupling between the probe and the IC. It was found by analyzing the results of a Discrete Fourier Transform applied on the SPA signal that was obtained at

di_erent EM emanation frequencies. This point is further explained in the next section.

D. Flow of Chip ID Generation

After power-up initialization, the overall process of the proposed chip IDgeneration can be represented as shown in Fig. It is divided into two phases, *generation* and *re-initialization*. During re-initialization, the configurations of all cells are swept to determine which one generates the largest of the same polarity as the previous best configuration. The information is stored for chip ID generation.



IV. CONCLUSIONS

In this paper, an active EM attack on RO-based TRNG is presented. The experiment setup is _rst described, and details about the EM harmonic platform and the DUTs are provided. The _rst study of the behavior of the source of entropy in the TRNG, i.e. of the set of ROs, showed the e_ciency of the EM emanations in controlling the behavior of ROs by their locking on the injected signal, depending on the power of the injected signal and its frequency. In a second experiment, realized on a 50-RO Wold's TRNG implemented in an FPGA, we demonstrated that it was possible dynamically control the bias of the TRNG output.

ACKNOWLEDGMENT

I am very thankfully to KIET College for providing a good lab facility. We simulate the Result on ***TANNER TOOLS V 13.0, Xilinx***

REFERENCES

[1] K. Wold and C. H. Tan, "Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings", International Conference on Recon_gurable Computing and FPGAs (ReConFig'08), 2008, pp. 385-390.

[2] B. Sunar, W.J. Martin, and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks", IEEE Transactions On Computers, 2007, vol. 56, no. 1, pp. 109-119.

[3] AIST, Side-channel Attack Standard Evaluation Board (SASEBO) http://sta_.aist.go.jp/akashi.satoh/SASEBO/en/index.html.

[4] T. Dubois, S. Jarrix, A. Penarier, P. Nouvel, D. Gasquet, L. Chusseau and B.Azais, " Near-_eld electromagnetic characterization and perturbation of logic circuits", Proc. 3rd Intern. Conf. on Near-Field Characterization and Imaging (ICONIC'07), 2007, pp. 308-313.

[5] F. Poucheret, K. Tobich, M. Lisart, B. Robisson, L. Chusseau and P. Maurine, "Local and Direct EM Injection of Power into CMOS Integrated Circuits", Fault Diagnosis and Tolerance in Cryptography (FDTC 2011).

[6] F. Poucheret, B. Robisson, L. Chusseau and P. Maurine, "Local ElectroMagnetic Coupling with CMOS Integrated Circuits", International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMC COMPO 2011).

[7]http://edaboard.com

[8] L. Batina, B. Gierlichs, E. Prou_, M. Rivain ,F.X. Standaert and N. VeyratCharvillon, "Mutual Information Analysis: A Comprehensive Study", Journal of Cryptology pp. 1-23 (2010).

[9] H. Yu, P. Leong, H. Hinkelmann, L. Moller, M. Glesner, and P. Zipf, "Towards a unique FPGA-based identification circuit using process variations," in *Proc. Int. Conf. Field Program. Logic Appl. (FPL)* , 2009, pp. 397–402.

[10] R. Pappu, "Physical one-way functions" Ph.D. dissertation, Program in Media Arts Sci., Sch. Arch. Planning, Massachusetts Inst. Technol., Cambridge, 2001. [Online]. Available: http://pubs.media.mit.edu/pubs/papers/01.03.pappuphd.powf.pdf

Authors Profile:

Ajay Kiriti Kapparada *is a final year student of M.Tech VLSI System Design in Kakinada Institute of Engineering and Technology, Korangi, Andhra Pradesh, India. He obtained his Bachelor Degree in Engineering (Electronics and Communication) from Kakinada Institute of Engineering and Technology, Korangi, Andhra Pradesh, India, in 2010. His area of research includes designing of low power memories at micrometer regime, low power VLSI design, analog & digital integrated circuit design.*

P.S.K.Ganesh Kumar *completed his M.Sc in Electronics from P.V.Siddhartha arts and science college, Vijayawada, India in 2005.And M.Tech in VLSI Design from Sathyabama University, Chennai, India in 2008. Currently he is working as a Assistant Professor in Kakinada Institute of Engineering and Technology from four years. His research areas include low power VLSI, LAYOUT design, leakage reduction, sensor networks, energy-efficient circuits, memory design, and sub-threshold operation.*

