



**HAL**  
open science

## Authentication of Microcontroller Board Using Non-Invasive EM Emission Technique

Mosabbah Mushir Ahmed, David Hely, Etienne Perret, Nicolas Barbot,  
Romain Siragusa, Maxime Bernier, Fredric Garet

► **To cite this version:**

Mosabbah Mushir Ahmed, David Hely, Etienne Perret, Nicolas Barbot, Romain Siragusa, et al.. Authentication of Microcontroller Board Using Non-Invasive EM Emission Technique. 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Jul 2018, Platja d'Aro, Spain. pp.25-30, 10.1109/IVSW.2018.8494883 . hal-02014214

**HAL Id: hal-02014214**

**<https://hal.science/hal-02014214>**

Submitted on 10 Jul 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Authentication of Microcontroller board using non-invasive EM emission technique

Mosabbah Mushir Ahmed<sup>1</sup>, David Hely<sup>1</sup>, Etienne Perret<sup>1</sup>, Nicolas Barbot<sup>1</sup>, Romain Siragusa<sup>1</sup>, Maxime Bernier<sup>2</sup>, Fredric Garet<sup>2</sup>.

<sup>1</sup> LCIS - Laboratoire de Conception et d'Intégration des Systèmes

<sup>2</sup> IMEP-LAHC - Institut de Microélectronique, Electromagnétisme et Photonique - Laboratoire d'Hyperfréquences et Caractérisation

**Abstract**—Counterfeiting of integrated circuits (IC) has become a serious concern for electronics manufacturers, system integrators, and end users. It is necessary to find a robust solution which is both efficient and low cost in terms of implementation in order to detect and avoid the counterfeiting of ICs. To combat the counterfeiting of ICs in this paper we have extended our previous work on utilizing radiated EM emission for authentication of IC on microcontroller boards. Our proposed scheme exploits manufacturing based process variation (PV), which continues to dominate in the nanoscale technologies. We have focused our work on authentication of microcontrollers which are one of the main targets of counterfeiting. The proposed work emphasizes on being non-intrusive and does not require any internal modification of the system on chip, it can be used on already deployed ICs. Generated EM response is treated to different encoding metrics to quantize it as a fingerprint for the IC. To validate our proposed scheme, measurements are carried out over several microcontroller boards.

**Index Terms**—authentication, clocks, counterfeit, EM, fingerprints, microcontrollers, reset.

## I. INTRODUCTION

With an ever-increasing usage of electronics and semiconductor devices in different applications, it is significant to have a reliable and trusted electronic system. In recent years there have been growing number of incidents related to the trust of IC [1]. These trust issues related to the ICs have become a source of major concern in different application areas like telecommunication, medical, space, military and banking. The malicious or counterfeited ICs can cause permanent or temporary damage to the hardware platform reducing the reliability of the system etc[1],[2]. Secondly, with respect to the economics aspect, it has a severe cost issue for IC provider as they lose a lot of money due to counterfeiting. Hence counterfeit ICs causes double fold problem : security and economy.

Microcontrollers (C) is one type of electronics components that are used in broad range of products, ranging from simple single core Cs running in the kilohertz frequency ranges up to complex multi-processor micro controllers running at 300 MHz or faster [3]. They find their applications in various domains such as industrial, automotive, medical, lightings etc. They have the advantages of consuming low power with considerable high speed of operation. With increased usage of Cs in different applications, it is imperative to avoid any kind of counterfeiting of Cs.

Normally manufacturers focus on detection of IC counterfeiting by using classical testing mechanisms. Generally test procedures include two categories: 1) physical inspection and 2) electrical inspection. Physical inspection methods include examination of the components documentation, exterior and

interior inspection with low and high power visual inspection equipment, and material analysis of the device under test (DUT) [4]. The electrical inspection phase of the tests includes AC/DC parametric tests, functional tests, and burn-in tests. While physical inspection methods are effective in detecting poor quality recycled parts, they are expensive, time consuming, and destructive while also being less effective for more sophisticated recycled components. Note that electrical tests can also be very costly [4],[5]. Second method for detecting the counterfeit of IC, is based on traceability approach to find fingerprint for authentication by using process variation (PV). As discussed in [6], using PV approach, physical unclonable function (PUF) is dominantly used. It exploits the inherent variability of an IC, caused due to manufacturing variations of IC itself. Each PUF contains a pair of challenge and response (c-r). For each challenge (c) sent to an IC, there is a unique response (r) to that challenge [3],[4]. Apart from the IC authentication, PUFs are also used for the purpose of secret key generation for cryptographic applications. Bottleneck of the PUF approach is that it requires dedicated on-chip circuitry which may be complex to process and implement.

In [7], as a part of earlier work, we have proposed an alternate methodology that exploits the manufacturing induced PV by utilizing the radiated electromagnetic (EM) emission from IC. With the PV from an IC, each IC showed a characteristic EM signature which can be used as its fingerprint for the authentication. Using this methodology, we are able to authenticate FPGAs. In comparison to the existing methods (electrical and physical) our method requires less time, is non-intrusive and there is no risk of damaging the IC. In comparison to PUF approach, our methodology uses very less silicon area. The main point is that for PUF, the processing is done on-chip (inside the IC) whereas in this methodology it is done outside the IC. This is an advantage in terms of design cost. But the limitation of our proposed methodology is that the IC cannot use the authentication information and also requires external measurement equipments.

The objective of this paper is to extend the work done in [7], and use the same methodology of EM emission to authenticate the C boards. We have used new C boards in this work. The idea is to exploit non-intrusively the design, periphery and architecture of C such that a viable fingerprint can be obtained which can be used for authentication purpose. There is major architectural difference between FPGA and C. Understanding from [8], the structure of a C is comparable to a simple computer placed in a single chip with all of

the necessary components like memory and timers embedded inside. It is programmed to do some tasks for other hardware. FPGA on other hand is an integrated circuit that could contain millions of logic gates that can be electrically configured to perform a certain task. The very basic nature of FPGAs allows it to be more flexible than most C. Owing to the flexibility and re-programmability feature of FPGA, in [7] we have programmed FPGA with a variability aware circuit which exploited its underlying PV to create fingerprints for the authentication. However, C already have their own circuitry and instruction set that the programmer must follow in order to write code for that C which restricts it to certain tasks.

The main aspect in this work is that there has not been any extra circuitry (or marker) implemented or programmed in the C as it can be done in FPGAs as in [7]. The non-intrusive nature of the work compels to use only the implemented hardware and peripheral sets of C, and utilize them such a way that they: 1) generate an EM emission and 2) generated EM emission is unique to each C. The first part of this work is focused on studying and utilizing the hardware architecture of the C to get a prominent EM emission. In the later part of this work we have performed post-processing of the EM response from C boards, to get a statistical and qualitative response that can be quantified as fingerprint of the C.

Before going into the details of working principles and how the Cs are authenticated using EM emission technique in this paper, we first highlight in the following section (section II) the description of the methodologies that has been adopted in our previous work to capture EM emission from FPGAs to create fingerprints for authentication. This highlights the different aspects required to be implemented to have an efficient authentication using EM emission technique.

This paper is organized in the following way: In Section II, a brief discussion on EM based authentication techniques along with previous work has been discussed. Section III elaborates the detail about C architectures, different aspects of EM emissions from Cs. In Section IV, we have described about the EM measurement and tests along with their respective post-processed results. Section V elaborates the results and discussions from measurements. And finally, section VI outlines a final conclusion from the paper and gives a brief detail about the future works.

## II. EM BASED AUTHENTICATION SCHEME

This section highlights the methodology used to authenticate an electronic device / IC by using radiated EM emission.

To quantify a fingerprint to any IC, the first step is determining / identifying a unique metric that is related to that particular IC. For ICs, the manufacturing induced PV grants them with unique physical and electrical properties, which cannot be duplicated to other ICs even if they are developed by the same manufacturing process [9]. The second step to characterize a fingerprint to an IC, is to perform a qualitative analysis or post-processing of the data obtained after capturing EM emission to create fingerprints of the IC. Fig. 1 gives

a pictorial representation of the different stages involved in obtaining fingerprints for authentication of IC.

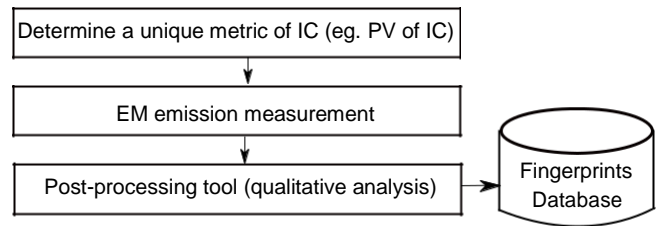


Fig. 1. Illustration of different stages to create fingerprint using radiated EM emission technique.

Steps similar to as discussed above and shown in Fig. 1, were deployed in [7] in order to authenticate FPGAs. The following points summarize the different steps that were used in [7] for FPGA authentication:

- 1) Program all the FPGAs under test with a lightweight marker viz. ring oscillator (RO) in our work. RO is used as a variability aware circuit, which exploits the effects of PV on FPGAs. This is equivalent to determination of a unique metric.
- 2) Perform the EM measurement using a magnetic field probe placed over the ICs horizontally. A non-intrusive method to perform the measurement.
- 3) The output spectrum are captured in oscilloscope (and spectrum analyzer) and the appropriate post-processing is applied to give statistical measures of the result.

Using the above points in [7] we were able to authenticate non-intrusively by using only one RO circuit, several FPGA boards of two different families and technologies i.e. SPAR-TAN 3A (90 nm CMOS technology) and ARTIX-7 (28 nm CMOS technology).

Similar to the steps adopted for FPGA authentication and methodology defined in Fig. 1, in this paper, to authenticate Cs, we have also used a non-intrusive EM emission based approach. Identifying metric is a challenge owing to device constraints of Cs, since any external marker cannot be added in the C, hence we need to focus on finding an inherent marker for C.

In the succeeding sections, an overall description of the C as device under test (DUT) is illustrated, along the different parameters and metrics that can attribute to EM emission and authentication. The same methodology as shown in Fig. 1 has been employed for the C authentication. The next subsection discusses in detail about the procedure, details of C DUT, measurement and results.

## III. MICROCONTROLLER AUTHENTICATION USING EM EMISSION

In this section, a detailed analysis and study of C authentication using EM emission has been discussed. A detailed architecture study has been adopted by using the manufacturer datasheet given in [11]. The discussions in this section is divided into brief understanding of C architecture, determining the unique metric for authentication and then measurement and results.

## A. Description of DUT

In this study, 12 STM32F103 Nucleo-64 C boards from ST Microelectronics have been used as DUT. It has ARM Cortex processor with 128k flash memory. Among the different interesting aspects of Cs, in this paper our focus is mainly on the working and understanding of clock and reset circuit. The clock of C plays an important role when EM radiation technique is explored. The oscillating nature of clocks emit EM radiation on powering up. So it is important to distinguish which frequency harmonic comes from which source in the C. It will be shown later that, reset in our work plays a role to set the metric that can be used to generate fingerprints for each C. In the succeeding sections, we will first discuss about the clock schemes and then, we move to discuss about reset, its exploitation to create fingerprints and results.

## B. Clock scheme of STM32F103C

Three different clock sources can be used to drive the system clock (SYSCLK): i) High speed internal (HSI) clock. The HSI clock signal is generated from an internal 8 MHz RC oscillator. The HSI RC oscillator has the advantage of providing a clock source at low cost (no external components). ii) High speed external (HSE) oscillator clock, generated using HSE ceramic resonator or external user clock. iii) Low speed internal (LSI) clock, generated using on chip RC oscillator. Each clock source can be switched on or off independently when it is not used, to optimize the power consumption. In next subsection, the EM emission from the clock of STM32 is discussed.

1) Clock and EM emissions from C: In this work, HSI clock is selected. It is configured to run at 8 MHz. To program / configure the clock, the STM32CubeMX from ST Microelectronics has been used. STM32CubeMX is a graphical tool that allows an easy configuration of STM32 microcontrollers and generates corresponding initialization C code through a step-by-step process.

To capture the EM emission from the C clock, a magnetic (H-probe) from Langer emv. probe is used. The output is observed in oscilloscope, which has bandwidth of 10 GHz, 75000 number of points, hamming window and spectrum of signal observed from 0 to 100 MHz.

Given the small size of the IC comparable to the H-probe, there is no need to move the probe in horizontal direction to capture the high SNR value of EM emission. The emission power is reasonable in all part over the IC. So the probe is fixed at one particular place for all the measurements steps for all 12 C boards.

The HSI clock configured at 8 MHz emits EM emission at harmonics of 8 MHz as shown in the Fig. 3. The HSI clock is generated using RC oscillator, which do get effected by PV, but on observing Fig. 3, it is evident that the distinction in peaks due to HSI clock for the 12 C is not very clear or noticeable (all peaks superimpose on each other). Hence it cannot be very efficient to use only HSI clock as an inherent marker for authenticating C.

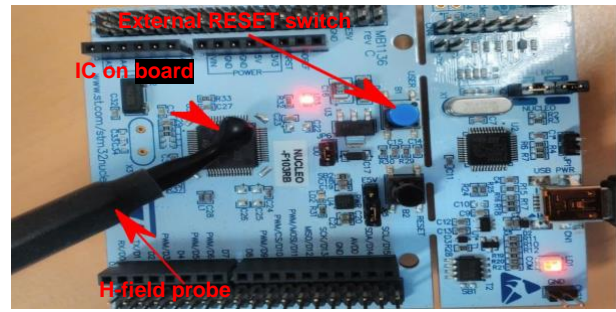


Fig. 2. Measurement step : Localized EM probe horizontally placed over the IC of C board.

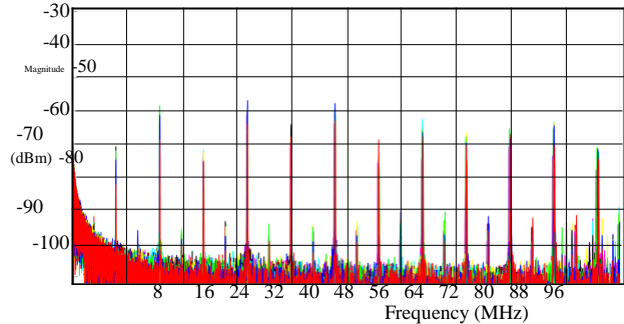


Fig. 3. EM emission due to HSI clock from the 12 C DUTs in bandwidth range up to 100 MHz. clock Harmonics observed at 8 MHz. The term MC and C are interchangeable.

To obtain a fingerprint from the Cs, a more precise and characteristic feature of C has to be exploited so that it can generate a prudent and conclusive fingerprint for each C. In next section an elaborated description of the metric and feature of C that has been exploited in this work to achieve authentication of Cs.

## C. System reset overview

In this paper, we have explored and utilized external reset as a mean to produce EM emission from C (apart from clock) and characterize it as a metric to obtain fingerprint for each Cs. Before illustrating the measurement steps and results using external reset as metric, we first discuss about the different aspects of the overall system reset of this STM32 C family.

A system reset sets all registers to their reset values. The STM32 C can be reset in several ways. The different ways to generate systems reset for STM32 is : 1) low level on the NRST pin or external reset, 2) window watchdog end-of-count condition (WWDG reset), 3) independent watchdog end-of-count condition (IWDG reset), 4) software reset (SW reset) and 5) low-power management reset. An illustrated diagram of the system reset circuit is shown in Fig. 4.

Fig. 4 description divides the reset circuit into two parts. One part consisting of Rpu, NMOS transistor, filters and Schmitt trigger are inside the ARM Cortex IC and other part consisting of capacitor, NRST and external switch outside the P on the C board. Although we have limited information owing to constraints from the manufacturers.

The system reset signal provided to the device is output on the NRST pin. The pulse generator guarantees a minimum

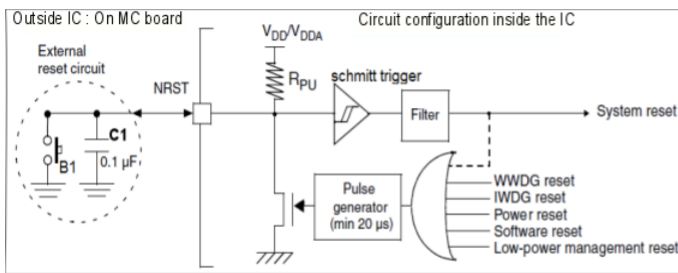


Fig. 4. Illustration of reset circuit for STM32F103RB.

reset pulse duration of 20 s for each internal reset source. In the case of an external reset, the reset pulse is generated while the NRST pin is asserted low. The Cs are typically specified with a minimum reset pulse width  $t(rst)$ ; for a general C, if the pulse applied do not meet the specification, the reset action may become invalid. However, the STM32 enforces proper reset by holding the reset signal universally for 20 s. This means that if a reset is ever initiated, it is always going to do its work. Additionally, there is a Schmitt trigger attached to the input, which allows the signal to have a rather long rise/fall time.

After comprehending the overview of system reset that is deployed in our DUT, in the following section we focus on the working of external reset and different current switching which results in EM emission.

#### D. External reset and EM emission : metric for authentication

The goal in this section of the paper is to highlight the hardware (circuit) description of each part of the external resets. This description is essential as it describes how different circuits of external reset can be utilized to generate EM emission. Owing to the PV, the generated EM emission from each DUT is unique but this is described in detail in the next section of measurements and results. External reset is activated by turning on the switch B1 shown in Fig. 4. Switching on the B1 pushes NRST pin to low. EM emission occurs when there is a sudden switching of the current.

Fig. 5 and the following points outline a brief summary of the mechanisms and effects of charging / discharging of capacitor (C1) and electrical phenomenons of other circuits on activating external reset switch B1.

When B1 is pressed, the capacitor C1 discharges through path B1.

The Schmitt trigger uses the hysteresis and produces a pulse at the output.

Pulse generated from the Schmitt trigger is fed back to NMOS transistor through the pulse generator.

The NMOS transistor when high, pulls the current down through it.

Consecutively there is a switching of current between  $R_{pu}$  - NMOS and  $R_{pu}$  - C1.

It is complicated to get the complete architectural detail on circuit / transistor level of the DUT (constrains from the manufacturer). But there could be some other effects from other parts of C circuits on getting reset pulse, which could

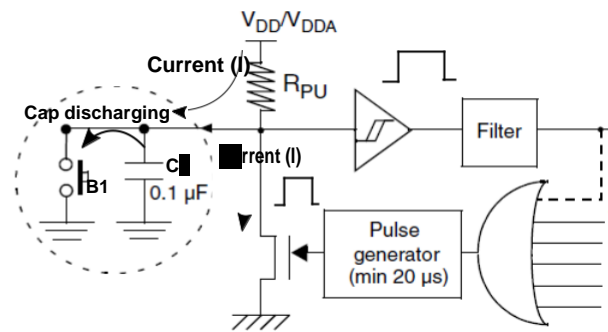


Fig. 5. Effects of switch B1 (external reset) on current switching in the different circuit elements of reset circuit (viz charging discharging of capacitor).

also play a role in the EM emission, like clearing out of the registers which could result in sudden voltage drop and hence causing sudden switching of current.

The next subsection focuses on measurements steps, which makes it clear if it is possible to use external reset as a metric to generate considerable EM emission that could be used as a prudent metric for authentication.

#### IV. EM EMISSION FROM Cs :MEASUREMENTS AND RESULTS

This section details the EM emission from the 12 Cs. All the Cs are of same manufacturer, same series and of same age. Before going into details of the EM emissions and results first we discuss about the procedure to generate and capture the EM emission.

The test and measurement is carried out by locally placing the H-probe on Cs and following same measurement pro-protocols as is done when capturing the emission from clock in section III (B1). The other procedures focused on using external rest while doing the measurement is discussed in steps below:

Program the C boards under test (or DUT) to run with only HSI clock.

Measure the peaks (or clock harmonics) using EM probe.

Press the external reset button. Once the reset button is pressed, it results in extra peak (harmonics) generation.

Measure the harmonics coming due to reset, and find out if these harmonics are unique for each C.

Following the above points measurement is carried out on 12 Cs and the emission due to the external reset is shown in the Fig. 6 for all 12 Cs. From Fig. 6, it is clear that on pressing the reset due to switching of currents as also discussed in previous section, there is considerable EM emission and for each C. The measurement is repeated five times to account for the measurement and systematic errors.

The spectral responses in Fig. 6 is shown over a bandwidth spreading from 0 to 25 MHz. Although the total spectral response of the measurement (measurement steps discussed in section III) is up to 100 MHz, Fig. 6 highlights the spectral response only up to 25 MHz to show the clarity of the spectrum. In this bandwidth range, first harmonics are

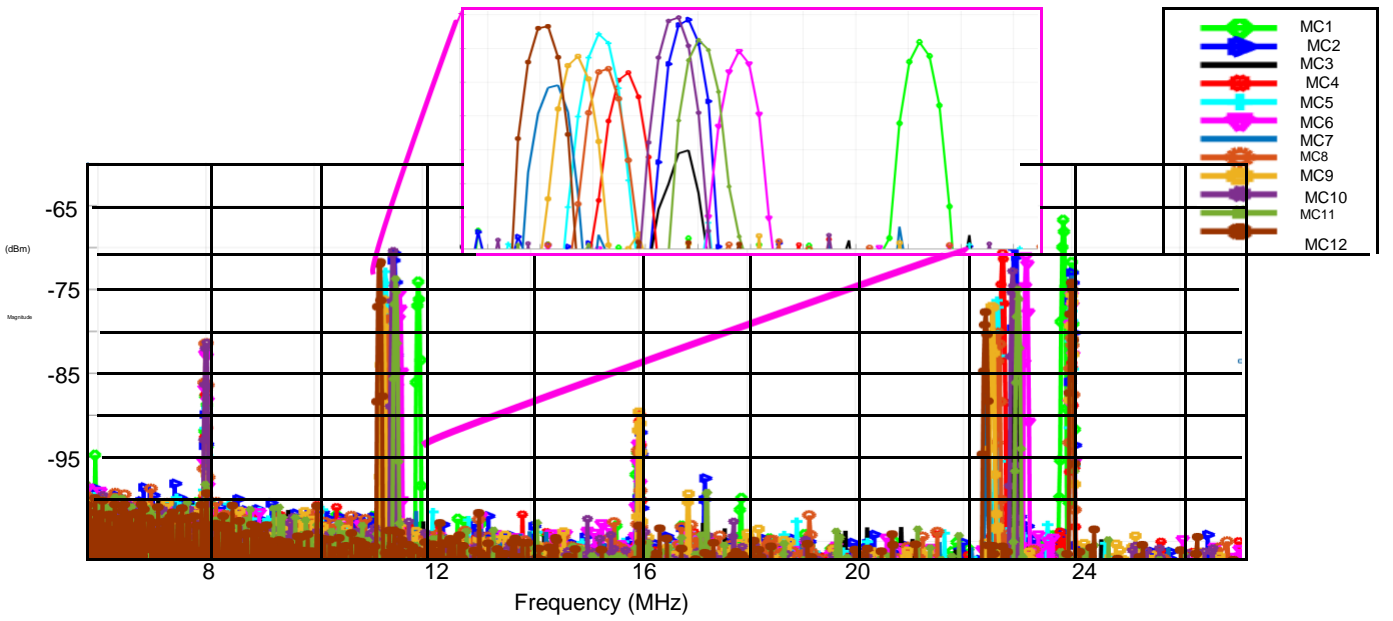


Fig. 6. EM emitted by 12 different Cs due to external reset depicted in the bandwidth up to 25 MHz and (inset) a zoomed-in view around the fundamental frequency peak. Terms MC (in legends of figure) and C are interchangeable

observed along the fundamental frequencies of each DUTs. The post-processing (discussed in subsection) of the signal is done around the fundamental frequency of the spectrum.

From the spectral responses of different DUTs in Fig. 6, it is evident that the frequency peaks are clearly different for 12 Cs. Each frequency peak corresponds to the C which emits it. The spectral responses for each DUT is unique owing to the PV effects on different circuit elements of external reset. Owing to non-deterministic behavior of the PV, some Cs like C1, C7 and C12 vary too much while some of them have overlapping response.

The variation in the frequency response of the 12 Cs, even if they are of same manufacturer, same family and same age justifies that utilizing only external reset, an inherent feature of C, PV can be exploited for Cs which can be applied for purpose of their authentication. Even though it may be unclear to point out which part of C board contributes to maximum EM emission, but this does not deter the objective of this study. As even if the large share of EM emission is outside the IC, we are still able to exploit the PV of the circuit elements of the board and use it to authenticate the whole C board rather than only the IC.

Now, we move to the next subsection where we highlight our work on post-processing of the EM emission response.

### A. Post-processing techniques

After the observation of the difference in frequency spectrum of each Cs in Fig. 6, the notion is to use a qualitative approach that performs a post-processing of the obtained EM response from different Cs. In this paper we have adopted cosine similarity as our post-processing technique as we have done in our previous study [7].

Cosine similarity (CS) gives a degree of similarity among two datasets. The scores are bounded between 0 and 1, where

0 is no similarity among the datasets and 1 having higher most similarity between the data sets. CS can be seen as a method of normalizing document length during comparison [13]. Suppose  $X=[x_1, x_2, \dots, x_n]$  are the representation of the EM data of one C and  $Y=[y_1, y_2, \dots, y_n]$  is the dataset of the EM response of another C, CS yields a score calculated by (1)

$$C:S(X; Y) = \frac{X \cdot Y}{\|X\| \|Y\|} \quad (1)$$

CS based computation uses the comparison between data sets obtained after repetitive measurements on same C and between two different Cs. The term auto-correlation (AC), is used here to compute the correlation between datasets obtained from the repeated measurements of one particular C. And for the comparison among different Cs over repetitive measurements, cross-correlation (CC) is used. Using (1), the equation for the computation of AC and CC respectively is derived in (2) and (3).

$$C:S(AC) = \frac{[M(n)] \cdot [M(n+1)]}{\|M(n)\| \|M(n+1)\|} \quad (2)$$

$$C:S(CC) = \frac{[M_C(n)] \cdot [M_C(n+1)]}{\|M_C(n)\| \|M_C(n+1)\|} \quad (3)$$

where

$M(n)$  represents datasets from nth measurement of same C.

$MC(n)$  represents datasets of nth C under test.

To perform the post-processing on data sets (spectral response of Cs), the signal is compared in complex frequency domain where both the magnitude and phase of signal is taken into account. CS is performed in the particular range of fundamental frequency of the reset signal (approximately in the window of 1 MHz centered around fundamental frequency (11-12 MHz range)). Fig. 7 shows the CS score distribution, illustrating a histogram with normal distribution fit (qualitative

analysis) of AC and CC for all 12 DUTs over repeated measurements. The statistical values for AC and CC are discussed in Table I. The values from Table I shows that the 3 value of AC is up to 0.076 and for CC is 0.57. The overlap of curves of AC-CC from Fig. 7 is beyond 3 values of AC and CC values.

Despite having some overlap in the frequency responses among few Cs viz. C3 and C4, but from Fig. 8 the overall probability of error between false positive and false negative is observed around 1%. The high quality factor (Q-factor) of the signal is one of the major factor resulting in low rate of error probability.

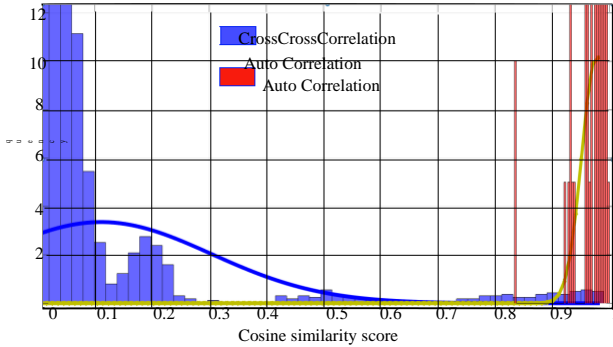


Fig. 7. Histogram of cosine similarity score distribution with a normal distribution fit of auto and cross-correlation for all measurements of 12 DUTs.

TABLE I

TABLE DETAILING MEAN AND 3 OF THE AC AND CC FOR 12 DUTS.

	Mean	3 sigma
AC	0.977	0.076
CC	0.11	0.57

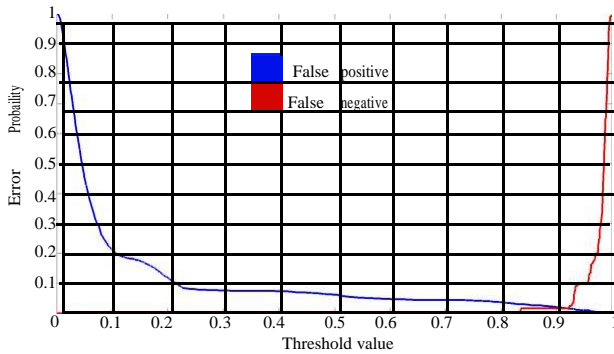


Fig. 8. Error probability curves for the AC and CC distribution for 12 DUTs.

## V. RESULTS AND DISCUSSIONS

From the qualitative analysis of the EM emission results, it is obvious that using the external reset only, which is an inherent feature of C, the PV of each Cs can be exploited. Secondly, statistical distribution of CC and AC does show that with a very less error probability, it is possible to authenticate Cs without any external intrusion or modification to the IC / boards.

Combining the work done in [7] with the present work, we can conclude that by using EM emission technique, we have been effectively able to authenticate two different semiconductor families (FPGAs and microcontrollers) without the need of

additional circuit. In both of our work, our focus has been to remain non-invasive and cost efficient. This can prove to be significant for authentication purpose by using non-invasive and low cost methods for other semiconductor products eg. Analog ICs and other ASICs.

## VI. CONCLUSION

In this case-study we have exploited PV to create EM based fingerprint for Cs of same family and same manufacturer. The proposed technique does not require any extensive programming or addition of any external markers. The low error probability as seen from the Fig. 9 proves that it is possible to authenticate Cs by using only external reset circuit of C. It is a non-invasive, cost-effective and time efficient process to authenticate C. As part of future work we will extend this approach to find out the robustness and stability of this methodology against the aging effects.

## REFERENCES

- [1] A. Maiti, L. McDougall and P. Schaumont, "The Impact of Aging on an FPGA-Based Physical Unclonable Function," 2011 21st International Conference on Field Programmable Logic and Applications, Chania, 2011, pp. 151-156.
- [2] Kai He, Xin Huang and Sheldon X.-D Tan, "EM Based on-Chip Aging Sensor for Detection and Prevention of Counterfeit and Recycled ICs" 015 IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD), Austin, TX, 2015, pp. 146-151.
- [3] T. Jew, "Embedded Microcontroller Memories: Application Memory Usage," 2015 IEEE International Memory Workshop (IMW), Monterey, CA, 2015, pp. 1-4.
- [4] H. Dogan, D. Forte and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," 2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Amsterdam, 2014, pp. 171-176.
- [5] P. Song, F. Stellari and A. Weger, "Counterfeit IC detection using light emission," 2014 International Test Conference, Seattle, WA, 2014, pp. 1-8.
- [6] Charles Herder, Meng-Day (Mandel) Yu, Farinaz Koushanfar, and Srinivas Devadas, "Physical Unclonable Functions and Applications: A Tutorial in Proceedings of IEEE, vol. 102, no. 8, pp. 1126-1141, Aug.2014 2014
- [7] M. M. Ahmed et al., "Radiated Electromagnetic Emission for Integrated Circuit Authentication," in IEEE Microwave and Wireless Components Letters, vol. 27, no. 11, pp. 1028-1030, Nov. 2017.
- [8] R. M. Sweeney, C. Spagnol and E. Popovici, "Comparative study of software vs. hardware implementations of shortened Reed-Solomon code for Wireless Body Area Networks," 2010 27th International Conference on Microelectronics Proceedings, Nis, 2010, pp. 223-226.
- [9] Swaroop Ghosh and Kaushik Roy, "Parameter Variation Tolerance and Error Resiliency: New Design Paradigm for the Nanoscale Era", in Proceedings of the IEEE, vol. 98, no. 10, pp. 1718-1751, Oct. 2010.
- [10] STM32F103x8/STM32F103xB datasheet [Online]. Available: <http://www.st.com/content/ccc/resource/technical/document/datasheet/33/d4/6f/1d/df/0b/4c/6d/CD00161566.pdf/files/CD00161566.pdf/jcr:content/translations/en.CD00161566.pdf>
- [11] Application Note AN2586 datasheet [Online]. Available: [http://www.st.com/content/ccc/resource/technical/document/application\\_note/6c/a3/24/49/a5/d4/4a/db/CD00164185.pdf/files/CD00164185.pdf/jcr:content/translations/en.CD00164185.pdf](http://www.st.com/content/ccc/resource/technical/document/application_note/6c/a3/24/49/a5/d4/4a/db/CD00164185.pdf/files/CD00164185.pdf/jcr:content/translations/en.CD00164185.pdf)
- [12] Chouchang Yang, Alanson P. Sample, "EM-ID: Tag-less Identification of Electrical Devices via Electromagnetic Emission", 2016 IEEE International Conference on RFID (RFID), Orlando, FL, 2016, pp. 1-8.