2018 IEEE Asia Pacific Conference on Circuits and Systems

Enhancing Physical Unclonable Function Robustness Employing Embedded Instruments

Jerrin Pathrose, Ghazanfar Ali and Hans G. Kerkhoff
Testable Design and Test of Integrated Systems Group (TDT)
Centre of Telematics and Information Technology (CTIT)
University of Twente
Enschede, The Netherlands
j.pathrosevareed@utwente.nl

***Abstract*—This paper proposes a methodology to improve the robustness of CMOS physical unclonable functions with regard to environmental parameter variations and thus enhancing the security. The methodology exploits the reuse of embedded instruments which are being deployed for dependability purposes. The approach is hardware and power efficient which is especially important for applications such as IoT. Chip implementation of the embedded instruments in 40nm CMOS technology is presented in addition to simulations and experimental validation on an FPGA.**

***Index Terms*—Embedded Instruments, Physical Unclonable Function, reliability, I_{DDT}, temperature, IJTAG, IEEE 1687.**

I. Introduction

Physical Unclonable Functions (PUFs) have gained popularity in the area of hardware security due to its property of generating a unique signature for each integrated circuit which is difficult to reproduce for an adversary [1], [2]. This is achieved by making use of the inevitable manufacturing process variation between integrated circuits. Each PUF has a set of challenge-response pairs which varies from chip to chip due to inter-die process variations. One of the required characteristics of a PUF is the *reliability* of the responses. However, the responses of the PUF are subject to environmental variations of the integrated circuit which can result in authentication failure.

The noise probability of temperature μ_t and voltage μ_v noise on PUF measurements for an arbiter PUF is up to 20% (for a temperature increase up to 40 degrees) and 16% (voltage variation of $\pm 2\%$) respectively of the inter-chip variation [2]. It has been shown [3] that temperature variations result in the largest BER increase of various PUFs compared to supply voltage and noise (active core). Error Correction Codes (ECC) [4], masking schemes [1], temperature binning for a ring oscillator PUF [5] etc. have been applied to mitigate the environmental impact and improve the security. This is at the expense of additional hardware and computation overhead. The changes in responses caused by temperature and voltage have also been exploited to increase the Hamming distance and hence enhance the PUF security [6]. This has been achieved by applying vectors to the primary inputs to cause voltage and temperature changes and hence increasing the Hamming distance. However, one drawback could be impact of the external environment which can alter the chip working environment in addition to the influence of the input vectors.

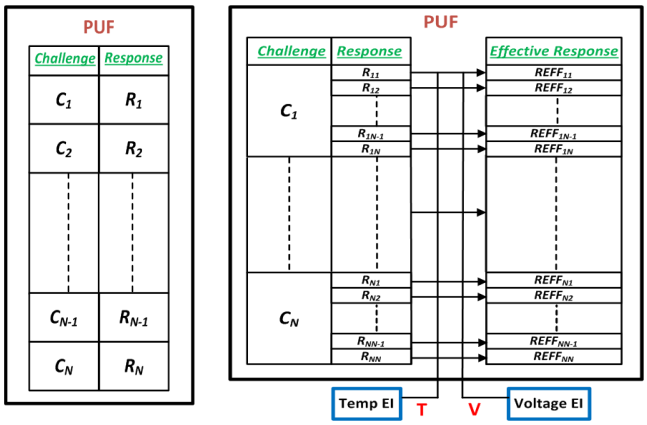
Embedded (on-chip) Instruments (EIs) are ubiquitous in modern day SoCs and have been deployed for various applications such as test, debug, monitoring and recently for reliability [7], [8], [9]. IoT devices remotely deployed in harsh environments suffer from reliability issues such as aging and would require an embedded dependability infrastructure to reduce maintenance costs. EIs such as temperature, voltage, transient power-supply current (I_{DDT}) have been applied for dependability purposes wherein the EIs monitor aging dependent parameters such as temperature, voltage, I_{DDT}, slack-delay to extend the lifetime of SoC [8], [9]. IJTAG (IEEE 1687) [10] which is an extension of the IEEE 1149.1 addresses the access and control of EIs. In addition, IJTAG also standardizes the description of the network as well as the instrument operating procedure employing the Instrument Connectivity Language (ICL) and Procedural Description Language (PDL) respectively.

This paper proposes a methodology to enhance the robustness of PUFs by employing EIs. This is achieved with minimum additional overhead by reusing dependability EIs such as the ones for monitoring temperature, voltage, transient power-supply current (I_{DDT}). In addition, this paper also explores the potential of EIs to eliminate the differential nature of PUFs thus further reducing the cost. Section II explains the proposed concept, whereas sections III and IV present the chip implementation of the EIs and the experimental validation on an FPGA respectively. Finally, conclusions are provided in section V.

II. EI solutions for PUF

In this paper we introduce an environmentally robust PUF design methodology which can be applied to any CMOS PUF. This approach entails the addition of environmental variables such as voltage and temperature which are digitized, to the existing response bits of the PUF. This is enabled by incorporating temperature and voltage EIs which capture these environmental parameters of the PUF circuit during response generation. The implementation of this approach can be achieved with minimal hardware cost by reusing the hardware of existing temperature and voltage EIs which have

978-1-5386-8240-1/18/$31.00 ©2018 IEEE



(a) (b)

Fig. 1. (a) Conventional PUF (b) Proposed PUF employing EIs

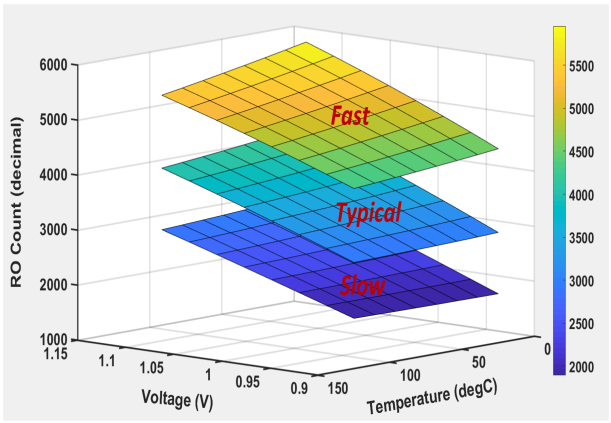


Fig. 2. Response planes of non-differential RO PUF for slow, typical and fast corners

already been deployed for dependability monitoring purposes. In the scenario where temperature and voltage changes are induced by input vectors to increase the Hamming distance, accurately measuring the environmental variables through EIs can also be applied to address the potential issue of errors due to the influence of external environment.

Fig. 1(a) shows the conventional design methodology where a set of challenges $C_1, C_2 \ldots C_N$ are mapped to a set of responses $R_1, R_2 \ldots R_N$ assuming a controlled operating environment. The proposed methodology has been illustrated in Fig. 1(b). For the same challenges $C_1, C_2 \ldots C_N$, we define $\{R_{11}, R_{12} \ldots R_{1N}\}, \{R_{21}, R_{22} \ldots R_{2N}\} \ldots \{R_{N1}, R_{N2} \ldots R_{NN}\}$ to be the corresponding responses of the PUF within the expected environmental variations. The *effective* response according to our proposed technique $\{REFF_{11}, REFF_{12} \ldots REFF_{1N}\}, \{REFF_{21}, REFF_{22} \ldots REFF_{2N}\} \ldots \{REFF_{N1}, REFF_{N2} \ldots REFF_{NN}\}$, would include the temperature (T) and voltage (V) EI bits in addition to the response R as given below:

$$Reff = R + T + V \qquad \begin{matrix} T_{min} \leq T \leq T_{max} \\ V_{min} \leq V \leq V_{max} \end{matrix} \qquad (1)$$

where V_{min} and V_{max}, T_{min} and T_{max} are the minimum and maximum range of the expected voltage and temperature variations respectively. As illustrated in the figure, each challenge is mapped to multiple *effective* responses *each* of which are valid thus resulting in a multi-dimensional *response plane*. This approach eliminates "false negative" scenarios where an authentication failure occurs due to the environmental parameter differences when the response is generated. This technique is valid in both cases, of noise produced by environmental variations or induced environmental variations.

Popular PUF implementations such as an arbiter and RO PUF have a differential characteristic to reduce the effect of environmental variables. This differential nature leads to extra hardware and power consumption which is often critical in IoT applications. Differential versions of the PUF can be avoided if the environmental variables are part of the response as illustrated in (1). In this scenario, the absolute frequency in case of a ring oscillator or absolute delay in case of a delay PUF would be sufficient. For a typical RO PUF, a pair of ROs only produce one bit of response. In the case of a non-differential approach each RO can produce multiple bits provided the environmental variables are taken into account. To increase the inter-chip variation, multiple ROs could be selected for responses, whereas the challenge would be the combination of ROs selected for the response.

Fig. 2 shows the *response plane* of a non-differential version of an RO as a PUF obtained by simulations in TSMC 40nm CMOS technology. To illustrate the worst-case inter-chip variation scenario the simulations have been carried out for typical, slow and fast corners. As discussed before, by virtue of having a multi-dimensional response plane including temperature and voltage, each PUF can be authenticated reliably. From the simulation data as well as close observation of the figure, we infer that there is an overlap of counts/responses between the typical and slow as well as between typical and fast corners. Therefore, there is a probability for "false positives" even in the worst-case inter-chip variation scenarios. However, by adding temperature, voltage into the *response plane* one obtains a worst-case minimum Hamming distance which is dependent on the number of bits generated by the temperature and voltage EIs.

In addition to temperature and voltage, PUF circuits are also influenced by aging which is especially significant in nanometer CMOS technologies. However, due to the intermittent operation of the PUF, aging of the PUF is significantly less as compared to the aging of a processor core. Nevertheless, the parameters such as temperature [11], I_{DDT} [12] have a strong correlation to aging. A preliminary work on the correlation of I_{DDT} parameter to aging and its potential for aging prediction has been presented in [9]. A similar approach to the one presented in this paper could be a potential solution wherein an aging EI or a virtual aging EI [9] formed by fusing multiple EIs could enhance aging robustness. Aging related effects are still under investigation.

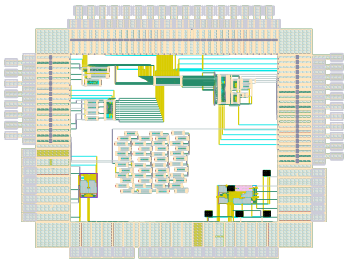


Fig. 3. Layout of the test chip with various EIs along with RO PUF

III. Embedded Instrument Chip Implementation

This section gives a description of the embedded instruments such as temperature, voltage, I_{DDT}. All the EIs have been designed to be accessed using an IJTAG network infrastructure.

A. Temperature EI

Our temperature EI design [8] is based on the bandgap principle. The front-end of the EI consists of sensing devices which generate a temperature-dependent voltage and a bandgap reference (BGR) which generates a temperature-independent reference voltage for digitization. The sensing devices are pdiff-nwell diodes which are distributed at various locations of the processor core for dependability purposes. Due to the non-critical nature of PUF locations, the PUFs could be located in accordance with the dependability requirements of the temperature EI locations and hence there is zero additional cost. The temperature-dependent voltage generated by the diodes has a complementary to absolute temperature (CTAT) characteristic with a sensitivity of -2mV/°C. The sensing devices occupy an area of 0.0012mm^2 and sense the local temperature of the PUFs at the same instance when the responses are generated.

B. Voltage EI

A voltage monitor to monitor the power supply line is presented in [9]. The basic principle of operation is the dependency of the propagation delay through a delay line as a function of the supply voltage. The design is using the 40nm standard cell library which reduces the design effort for its layout and system integration. The resolution of the voltage EI is 10mV which is suitable for our dependability application as well for PUF. From the system level point of view, the acquisition time is 0.32µs which can capture relatively fast transients in voltage. The EI occupies an area of 0.0013mm^2. The proposed design is fully digital and IJTAG compatible and therefore it does not require any ad-hoc methodologies for its configuration.

C. I_{DDT} EI

The I_{DDT} EI working principle is based on sensing the current through the parasitic resistance of the power-supply line via an unbalanced current mirror [8]. As a result, there is a minimum influence of the EI on the normal operation of the circuit. The front-end of the EI generates a current-independent reference and a current-dependent linear voltage which can be subsequently digitized by an ADC. Both the current-independent reference and the current-dependent linear voltage are synthesized from the same circuit which makes the design hardware efficient. The details of the design have been presented in [8].

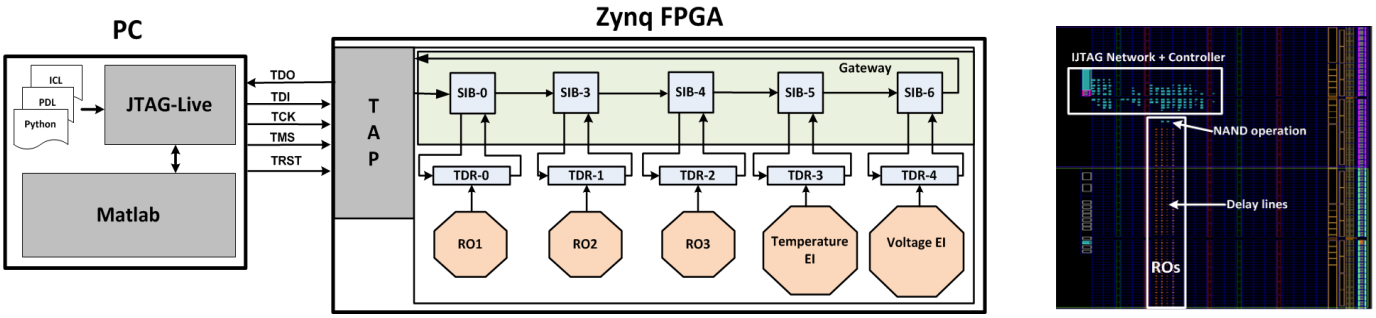
D. EI Layout

Fig. 3 shows the layout of the test chip which contains the various EIs such as temperature, voltage, delay, I_{DDT} along with the RO PUF. Post-layout simulation for the various EIs has been conducted to validate the performance. The test chip is being implemented in TSMC 40nm technology.

IV. FPGA Validation

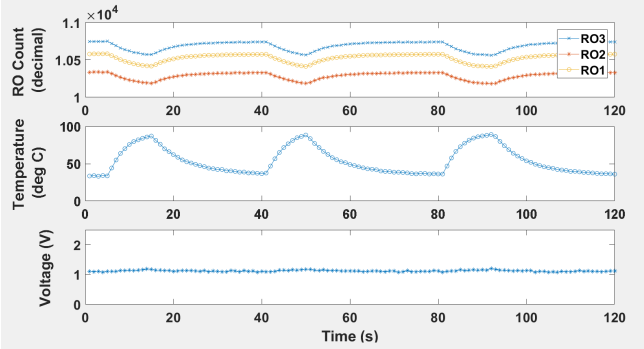
An experiment was conducted using the ZC706 evaluation board for the Zynq-7000 AP SoC. The TAP port available on the evaluation board is used to access the EIs via the IJTAG network we implemented on the FPGA. The temperature and voltage EIs are realized using the on-chip temperature and voltage sensors available on the FPGA and are interfaced as EIs with our IJTAG network. The RO PUFs are also implemented as IJTAG interfaced EIs for the ease of validation. The schematic of the experimental set-up is shown in Fig. 4(a). To build identical ring oscillators, delay lines of the same lengths are implemented in a precise manner. To emulate the change in oscillation frequency due to process variation as present in an integrated circuit, NAND gates present in each of the ROs are implemented at random locations. This changes the wire length for each RO, resulting in frequency differences and hence providing distinguishable counts for RO PUF. Fig. 4(b) shows the layout of the implementation which depicts the location of the ROs consisting of delay lines and the NAND gate along with the IJTAG network. Spatial variations of temperature are minimized by placing the ROs close to each other. To acquire and plot data in real-time, JTAG Live Studio software [13] is used together with MATLAB.

Fig. 5 shows the experimental results. A hot air blower is used to ramp up the FPGA temperature. The experiment is run for three temperature cycles to simulate temperature environmental variations. The top part of Fig. 5(a) shows the RO PUF count, whereas the middle and bottom plots show the temperature, voltage data from the EIs captured at the same instant as the PUF response. Fig. 5(b) shows the response of the RO PUF obtained from Fig. 5(a) plotted against temperature for the three temperature cycles overlaid on top of each other. We have a linear CTAT response which shows the dominant effect of temperature due to the relatively stable voltage. As observed from the figure, we have an overlap of the responses for the three temperature cycles which proves the repeatability of the responses of the non-differential RO PUF which is a key characteristic for any PUF implementation. The repeatability is achieved by the temperature and voltage EIs and hence our methodology can effectively eliminate environmental variations.

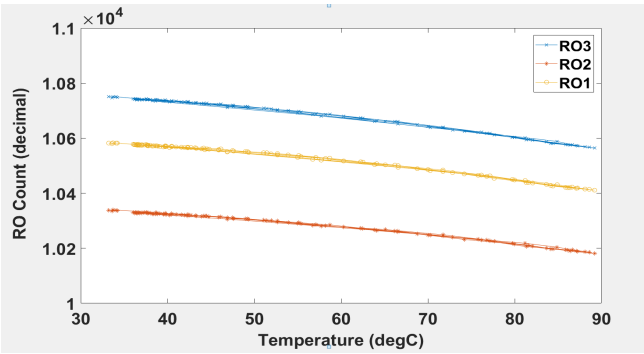


(a) (b)

Fig. 4. (a) Schematic of the experimental set-up (b) PUF implementation on FPGA together with EIs and IJTAG network



(a)



(b)

Fig. 5. (a) RO PUF response along with temperature and voltage EI data for three temperature cycles (b) RO PUF response vs. temperature obtained from (a) for the three cycles

V. Conclusions

In this paper, we have proposed a unified design methodology towards dependability and security by reusing dependability embedded instruments to enhance PUF robustness and hence security. This approach is especially relevant for IoT applications where the IoT devices are remotely deployed and operate in harsh environments in which case dependability is critical. The chip implementation of various EIs in TSMC 40nm in addition to experimental results utilizing EIs available on the FPGA have been presented. The potential of EIs to eliminate the differential nature of typical PUFs and thus reduce the PUF hardware has also been explored.

Acknowledgments

This research was carried out within the ECSEL project HADES (16003) financed by the European Committee & Netherlands Enterprise Agency (RVO). The authors would also like to thank JTAG Technologies and Hassan Ebrahimi for their support.

References

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, June 2007, pp. 9–14.

[2] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers*, June 2004, pp. 176–179.

[3] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," in *Cryptographic Hardware and Embedded Systems – CHES 2012*, 2012, pp. 283–301.

[4] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, June 2011, pp. 128–133.

[5] C.-E. Yin and G. Qu, "Temperature-aware cooperative ring oscillator PUF," in *Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2009, pp. 36–42.

[6] X. Wang and M. Tehranipoor, "Novel physical unclonable function with process and environmental variations," in *2010 Design, Automation Test in Europe Conference Exhibition (DATE 2010)*, March 2010, pp. 1065–1070.

[7] J. Keane, T. Kim, X. Wang, and C. H. Kim, "On-chip reliability monitors for measuring circuit degradation," *Microelectronics Reliability*, vol. 50, no. 8, pp. 1039 – 1053, 2010.

[8] J. Pathrose, G. Ali, and H. G. Kerkhoff, "IJTAG compatible analogue embedded instruments for MPSoC life-time prediction," in *2018 IEEE 19th Latin-American Test Symposium (LATS)*, March 2018, pp. 1–4.

[9] G. Ali, J. Pathrose, and H. G. Kerkhoff, "On-chip lifetime prediction for dependable many-processor SoCs based on slack-delay and IDDX data fusion," in *IEEE 12th International Symposium on Embedded Multicore/Many-core Systems-on-Chip*, September 2018, pp. 1–8.

[10] "IEEE standard for access and control of instrumentation embedded within a semiconductor device," *IEEE Std 1687-2014*, pp. 1–283, Dec 2014.

[11] W. Wang, S. Yang, S. Bhardwaj, S. Vrudhula, F. Liu, and Y. Cao, "The impact of NBTI effect on combinational circuit: Modeling, simulation, and analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 2, pp. 173–183, Feb 2010.

[12] Y. Zhao and H. G. Kerkhoff, "Unit-based functional IDDT testing for aging degradation monitoring in a VLIW processor," in *2015 Euromicro Conference on Digital System Design*, Aug 2015, pp. 353–358.

[13] JTAG Technologies, "JTAG Live Studio." [Online]. Available: https://www.jtaglive.com/