A RING OSCILLATOR BASED PUF IMPLEMENTATION ON FPGA

Giray KÖMÜRCÜ[1], Ali Emre PUSANE[2], Günhan DÜNDAR[2]

National Research Institute of Electronics and Cryptology, TÜBİTAK, 41470, Kocaeli, Turkey[1]
Bogazici University, Dept. of Electrical and Electronics Eng. 34342 Bebek, Istanbul, Turkey[2]
Email: giray.komurcu@tubitak.gov.tr, ali.pusane@boun.edu.tr, dundar@boun.edu.tr

Abstract *Physical Unclonable Functions (PUFs) are circuit primitives that generate chip specific and unique outputs, depending on the uncontrollable variations present in the manufacturing process. These cheap and highly efficient structures have a wide range of application areas, including authentication, key generation, and IP protection. Uniqueness, robustness and unpredictability are other important aspects of PUF circuits beside unclonability. In this work, we first review basic PUF circuit types, including Optical PUFs, Arbiter PUFs, Ring Oscillator (RO) PUFs and, SRAM PUFs. Then, two FPGA implementations of RO-PUFs are presented with their uniqueness and robustness analyses. Finally, new concepts in RO-PUF literature and their limits and performance expectations are discussed.*

Keywords: PUF, Physical Unclonable Functions, Uniqueness, Ring Oscillator, FPGA.

I. INTRODUCTION

Physical Unclonable Function (PUF) is a relatively new concept that is used to address security problems, and it was first introduced in 2001 by Pappu *et al.* [1]. These circuits have the capability of generating robust, unclonable, unpredictable, and chip specific outputs, whenever needed during operation. Manufacturing of integrated circuits is a very uncontrollable process in nanoscale. For instance, it is very unlikely for any two transistors on an integrated circuit (IC) to have exactly the same doping concentration, threshold voltage or oxide thickness. This property results in slight differences between the operation of circuits with the same layout and hence enables utilization of PUF circuits to obtain chip specific signatuers.

PUF circuits have three main usage areas. First, PUFs have the unique advantage of eliminating the need for expensive non-volatile memory for key storage by generating the signature on the fly. Cryptographic operations have become compulsory for many applications performed by ICs. As a result of this, public or private keys are being used, transferred, and stored within the chips. However, many attack methods have been recently developed to capture the key during the transfer or storage phases. PUF structures present a promising solution to this problem with their capability of generating the key on the fly when required. This ensures the safety of the key, since it is not stored on a memory for a long time, and the need for key transfer from the outer world to the device or vice versa is eliminated.

The main advantage of FPGAs over ASICs is their reprogrammability on the field. When power is applied to the system, an FPGA is configured by reading the design from an external memory via a bus between the blocks. This is a very weak point of the intellectual property (IP) developer, since an attacker can easily probe the bus and copy of the design without paying license fees to the IP owner. A possible solution to this problem is encrypting the bit stream stored in external memory and decrypting it on the FPGA, during each load of the design. Here, the main problem is to store a key on the FPGA to decrypt the encrypted bit stream. Two solutions are proposed to this problem. The first solution is adding a non-volatile memory to the FPGA, and the second is to store the key on volatile memory and add a battery to power-up that memory all the time. Both of these solutions have significant amounts of price penalty to the system. At this point, PUF structures provide a cost effective and easy solution by providing key generation schemes depending on the process variations of

the chip. The key is reconstructed every time the FPGA is powered up, eliminating the storage requirement on a memory.

IC identification and authentication can also be achieved using PUF structures. RFID technology provides the capability of identifying each and every circuit uniquely. Many devices can be identified simultaneously, without the requirement of line of sight. The cost of this technology is mainly based on storing the ID on a non-volatile memory. In addition to these, the stored ID can be copied by attackers during a transaction if authentication protocols are not applied properly. PUF structures provide an efficient solution with the capability of ID generation via Challenge-Response Pairs (CRPs), that work on the fly. This scheme reduces the cost of RFID ICs significantly by eliminating the need for non-volatile memory.

With the increasing security concerns related to the operation of ICs, PUF circuits are expected to be used widely in the near future. The rest of the paper is organized as follows. In Section II, PUF properties are defined. Next, types of PUF structures are presented in Section III. Implementation of two RO-PUFs are explained and their results are analyzed in Sections IV and V. New concepts and expectations in RO-PUFs are discussed in Section VI. Section VII concludes the paper.

II. PUF PROPERTIES

A. Uniqueness

Uniqueness, which is also known as Inter-PUF variation, is the variation of the responses or a PUF circuit design to the same set of challenges on different ICs. Ideally, the responses of two PUF instances to the same challenge should differ 50% on the average, meaning that no correlation exists between them. If the uniqueness property of a PUF is weak, it will not be possible to generate enough number of IDs or signatures to identify the required number of circuits. As a result, in practice, more than one circuit will have the same ID.

B. Unclonability

Unclonability is a very fundamental behavior of a PUF and it indicates that it is a very hard and time consuming task to build two identical PUF circuits, that respond similarly to the same challenges. In addition to this, unclonability indicates that, it is very hard and practically nearly impossible to build an accurate mathematical model of a PUF, that will compute the responses to the chosen challenges without using the PUF circuit itself. Since process variations are uncontrollable, they are the core of a PUF's unclonability property.

C. Unpredictability

Unpredictability is another key concept of PUF circuits. According to the unpredictability principle, responses of a PUF to a challenge should be unpredictable, even if the environmental variations, structure and layout of the PUF is known. In addition to this, the system should maintain that even infinitely many CRPs are known, response to a new challenge should be still unpredictable.

D. Robustness

Robustness, which is also called the intra-PUF variation, is the number of bits in a response, that change value between repeatedly applied challenges. In a perfect PUF, response to a certain challenge should always be the same under all environmental conditions. But, in practice a number of bits are not determined reliably and they change their values according to environmental conditions such as temperature, voltage, humidity, aging, etc. General PUF structures depend on small variations in the manufacturing process. Therefore, changes in the environment affect the responses inevitably. This problem is called intra-chip noise. Since PUF outputs are used for security related applications, such as key generation, ID generation, or signature generation, this noise should be somehow removed from the system. The most common approach is to apply post processing to the data. For instance, error correction codes can be used to generate robust outputs from noisy PUF responses. However, using error correction codes increases the cost of the system as well as the time required to generate the output. These overheads are also very dependent on the amount of noise on the data. Therefore, increasing the quality of PUF responses and hence minimize the post processing cost is another aim of the designer.

In addition to these properties, PUFs should be easy to use, meaning that applying the challenge and getting the response should be easy and fast. Moreover, it should require small area and low power, and convenient for integrating on an IC.

III. PUF STRUCTURES

A. Optical PUF

Optical PUFs are the first structures presented in the name of physical one-way functions in [1], [2]. Bubble filled transparent epoxy is applied on top of the wafer and laser is shined on the sample to lead a speckle pattern. Since this pattern is dependent on the wavelength and the angle of the laser, material of the wafer, thickness of the wafer, and the property of the epoxy, different chips will have different patterns, hence producing unique IDs or signatures. Even though a high number of CRPs can be generated via Optical PUFs, they are not very practical to use in the field, since measurement devices are quite complicated. Reconfigurability is an advantage of an Optical PUF, which enables changing the signature or key when needed [3]. This is achieved via a high energy laser beam, which changes the optical properties of the epoxy.

B. Ring-Oscillator PUF

Ring Oscillator (RO) type PUF, which depends on the delay differences of identical structures, was first presented by

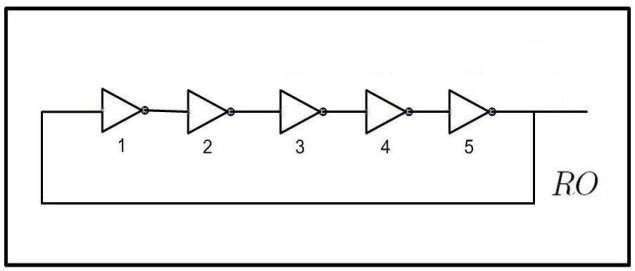

Fig. 1: 5-stage RO schematic

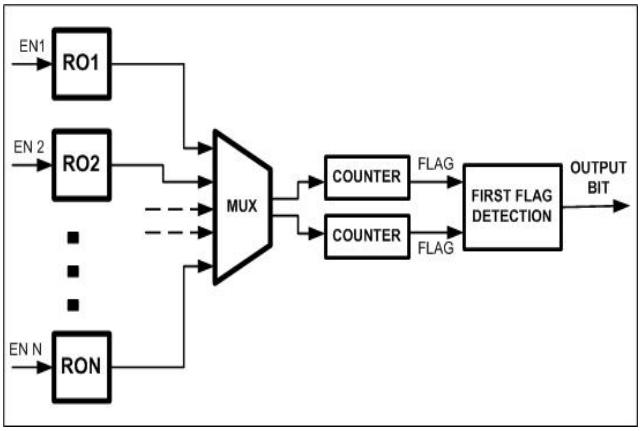

Fig. 2: PUF output bit generation by conventional system.

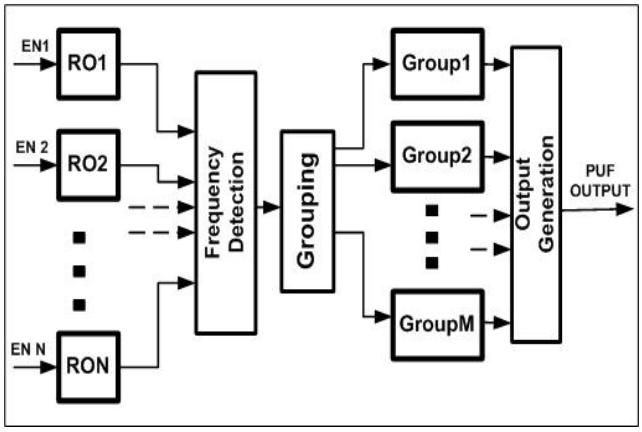

Fig. 3: PUF output generation by ordering based systems.

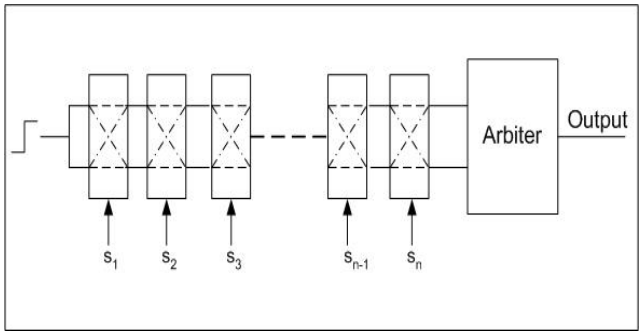

Fig. 4: Arbiter Based PUF Circuit [11]

Gassend *et al.* in 2002 [4], [5]. The structure presented in [4], [5] can be considered as a self oscillating loop and it has led to the ring oscillator PUF structures proposed afterwards. In this approach, a variable delay circuit that continuously oscillates is built. According to the applied inputs, the delay of the circuit changes, as well as the oscillation frequency. The frequencies of the variable delay circuit are then used to generate the PUF output.

In regular RO-PUFs, ROs are composed of an odd number of inverting stages connected serially, to maintain continuous oscillation as shown in Figure 1. In these systems, frequencies of two ROs are compared to generate 1 bit output. In order to generate a number of output bits, a certain number of ROs are built and two of them are selected and their frequencies are compared with identical counters for each bit generation. This RO-PUF output generation mechanism is presented in Figure 2.

In addition to the regular RO-PUFs, grouping based RO-PUFs are proposed recently, which offer much higher rate of entropy extraction and error-free outputs [6], [7]. The output generation mechanism of these systems mainly depend on the frequency ordering of ROs, in a group of more than 2 elements. The schematic of grouping based RO-PUFs are presented in Figure 3.

C. Arbiter PUF

The first arbiter type PUF structure was presented by Gassend *et al.* [8]–[11] based on the differing timing behavior of elements on chips [12]. In arbiter PUFs, a number of delay elements that construct two parallel paths are connected serially, and a rising signal is applied to these paths as in Figure 4. At the end of these lines, an arbiter decides which signal passed the lines faster and outputs one bit response. This delay element is chosen to be composed of two multiplexers, which carry two input signals to the outputs. According to the value of the select signal that controls both of the multiplexers, one input passes through first gate and the other input passes through the second gate or vice versa. In arbiter PUFs, a significant number of delay elements are connected serially and input signals race within these parallel lines. Challenge to the PUF determines the path that the signals will pass and the response will be one bit logic 0 or logic 1, based on the arrival times of two input signals. Arbiter PUF generates 2^n possible delay paths if n elements are used. To generate an m bit response, this structure can be duplicated m times or m consecutive measurements can be done by applying m different challenges.

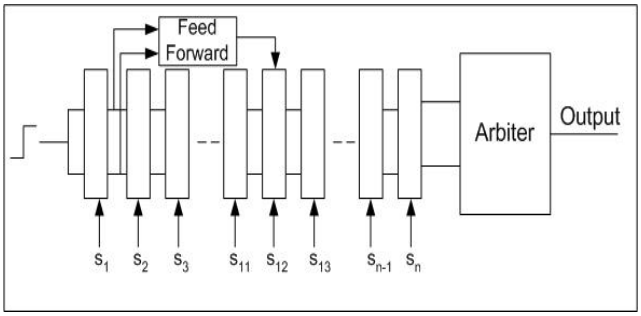

Fig. 5: Feed-Forward arbiter based PUF circuit [11]

The main problem of arbiter based structures is their vulnerability against modeling attacks. The attacker may model the behavior of an arbiter PUF, after collecting a certain number of challenge-response pairs. To overcome this problem, a feed forward arbiter structure was presented by Lim *et al.* [8]. With this scheme, nonlinearities are added to the PUF in order tol harden modeling attacks. This structure is presented in Figure 5.

D. SRAM PUF

CMOS SRAM is a circuit with six transistors [13], as shown in Figure 6. Four of the transistors are used as two cross-coupled inverters that will hold the value at their outputs. Two transistors are used as the load transistors to drive the value applied from outside to the cross coupled inverters. During write operation, the value stored in the SRAM may change. Otherwise, stable operation is maintained. However, during power up, external signal is not applied to the inverters. Therefore the value of SRAM will tend to be 0 or 1, depending on the minor voltage differences and mismatches between the two inverters, caused by internal parasitics of the IC. Since internal parasitics are mostly stable within the IC, SRAM output will be stable during power up with high probability. However, internal parasitics are different among ICs and hence the initial condition of SRAM value will differ. These properties maintain the uniqueness and robustness of PUF structures, hence SRAM can be used as a PUF.

The main advantage of an SRAM PUF is its convenient structure for FPGA implementations [14]. Most of the FPGAs that are in use today includes built-in SRAM memory blocks that can be used to store data. However, some of the SRAMs in these products have initial conditions, which prevent them from having random values during the startup phase. These types of FPGAs do not allow SRAM PUF implementations.

Another advantage of an SRAM PUF is its ease of use, since no evaluation circuitry is needed. Since SRAM bits get their value during power up immediately, just the read operation is performed on FPGA to get the output. Then, error correction is applied and the required key or

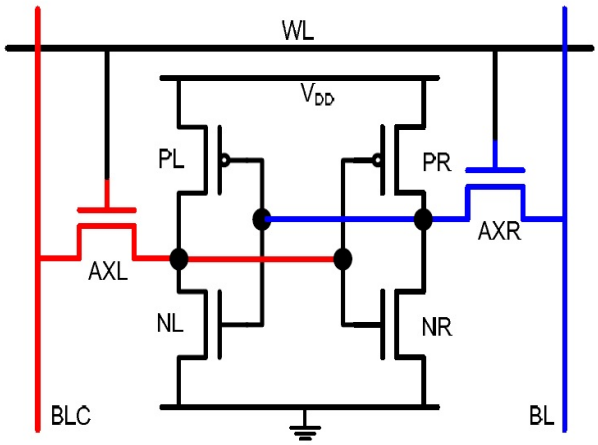

Fig. 6: Six transistor SRAM cell [14]

signature is generated in a short time, compared to other PUF structures such as RO-PUF or Arbiter PUF.

In addition to the PUF types discussed above, there are quite a number of other structures proposed in the literature. Coating PUF [15], Glitch PUF [16], Butterfly PUF [17], Reconfigurable PUF [18], and Reset PUF [19] are some of the structures that should be mentioned for a complete analysis.

IV. IMPLEMENTATION OF AN RO-PUF STRUCTURE

Among various PUF types discussed in the previous section, RO-PUFs seem to be the most convenient type for FPGA implementation. Optical PUFs are not practical and high end equipment is needed, whereas Arbiter PUFs require perfect symmetry among delay lines, (not possible on FPGAs) and SRAM PUFs present low entropy and they are not available in certain FPGA families. In order to realize a PUF circuit in FPGA and evaluate its performance according to the metrics discussed, two versions of the RO-PUF structure proposed by Gassend *et al.* [5] are implemented. For both versions, a five stage RO is built, composed of four inverter stages and a NAND gate as shown in Figure 7. The functionality of the NAND gate is to enable optional oscillation. RO is built as hard macro and mapped into designs to maintain equal wire loads, which is a must for proper PUF operation. Two counters are then used to compare the frequencies of two ROs for one bit PUF output generation. A limit is set for counters and a flag is raised by the counter to determine which reaches the limit first. The measurement time is determined via trial and error, based on the robustness of the outputs. With this approach, 82μs per bit seemed to be the optimum measurement time, in terms of error rate and speed.

In the first structure, 129 ROs are implemented to generate 128 bit output. Each output bit is generated by comparing the two adjent ROs, placed next to each other. In the second

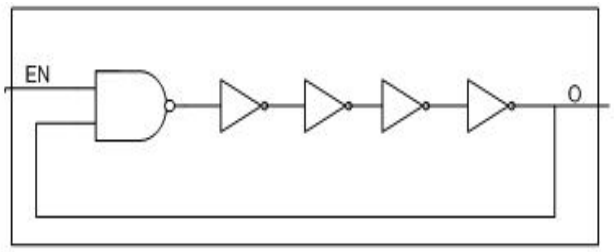

Fig. 7: 5-stage RO schematic

TABLE I: Uniqueness and Robustness results of RO_PUF1 and RO_PUF2.

Uniqueness Analysis	**Time per bit μs**	**# of Meas.**	**Ham. Dis.**	
RO_PUF1	81,92	25	49,05	
RO_PUF2	81,92	25	49,55	
Robustness Analysis	**Time per bit μs**	**# of Meas.**	**Err. R. (NOC)**	**Err. R. Var. Tem.**
RO_PUF1	81,92	1000	0,89	2,63
RO_PUF2	81,92	1000	1,31	3,65

structure, 256 ROs are implemented to generate 128 bit output. Each RO is used only once in this structure. In both designs, output bits are generated one by one and unused ROs are disabled to reduce power consumption and prevent oscillation coupling.

V. ANALYSIS OF EXPERIMENTAL DATA

In the experiments given in this section, FPGAs are used and their outputs are collected through RS-232 serial port, via Matlab. In order to present reliable results, we have adopted the confidence interval approach to PUF output measurements. For robustness, 1000 outputs are collected from each implementation, providing 99.9% confidence within a confidence interval of 0.1%. In addition to the measurements done under normal operating conditions (NOC), a varying temperature analysis is also done by 1000 measurements taken each at 0, 20, 40, 60, 80, and 100 C^o. For uniqueness, the same design is mapped to different sites on a single FPGA. For this purpose, the FPGA is divided into 25 distinct sites and measurements are collected by mapping the design to each site. 95% confidence is achieved within a confidence interval of 2% by 25 measurements.

Robustness and uniqueness results of two RO-PUF implementations are presented in Table I. For robustness, an acceptable rate of erroneous output bits is encountered as expected. Under NOC, the error rate is below 1.5% for both structures and for varying temperature, the error rate increases up to 3.5%, which can be corrected easily by adding error correction codes to the system. For uniqueness, it is observed that the measurement results are very close to the ideal Hamming distance of 50%. The second structure seems to perform a little better in terms of uniqueness. This may be the result of double usage of each RO in the first structure, which lowers the entropy in the system, but increases the area efficiency as well.

VI. NEW CONCEPTS IN RO-PUFs AND THEIR LIMITS

In conventional RO-PUF circuits, two ROs are compared to generate 1 bit output. Entropy utilization is low in such structures, increasing the area cost of the system. In order to increase the entropy extraction from the system, a comparison of more than two ROs is required. With this approach, ROs are grouped and frequency ordering of the group is used to generate output bit streams. In this system, for a group of *N* ROs, *N!* different orderings may occur with equal probability. By mapping each different ordering to an output bit stream, $\lfloor \log_2(N!) \rfloor$ bits can be generated from each group [20]. It should be noted that, not all ROs can be grouped together, due to noise and environmental fluctuations present in the system. One possible solution to the problem is to form more than one group and the ROs, whose frequencies are adequately apart from each other are grouped together. Even though this will make the theoretical upper bound unreachable, robust and highly area efficient RO-PUFs seems to be possible.

VII. CONCLUSION

Physical unclonable functions offer cheap and secure solutions in the areas of IP protection, key generation, ID generation and authentication. They can be implemented using several techniques for both ASICs and FPGAs. In this work, we have implemented two RO-PUF structures on Xilinx FPGAs, and analyzed their performance in terms of robustness and uniqueness. Lastly, new concepts in RO-PUFs are discussed.

References

[1] R. S. Pappu, "Physical one-way functions." Ph.D. dissertation, Massachusetts Institute of Technology, Massachusetts, 2001.

[2] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 6, pp. 2026–2030, 2002.

[3] K. Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, "Reconfigurable physical unclonable functions - enabling technology for tamper-resistant storage," in *IEEE International Workshop on Hardware Oriented Security and Trust (HOST)*, 2009, pp. 22–29.

[4] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon pysical random functions," in *ACM Conference on Computer and Communications Security (CCS)*, 2002, pp. 148–160.

[5] B. Gassend, D. Clarke, M. Dijk, and S. Devadas, "Controlled physical random functions," in *18th Annual Computer Security Applications Conference (ACSAC)*, 2002.

[6] C. Yin and G. Qu, "LISA: Maximizing RO-PUF's secret extraction," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2010, pp. 100–105.

[7] G. Komurcu, A. E. Pusane, and G. Dundar, "Dynamic programming based grouping method for RO-PUFs," in *9th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*, 2013, accepted for publication.

[8] D. Lim, J. Lee, B. Gasend, G.E.Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on VLSI Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[9] B. Gassend, D. Clarke, M. V. Dijk, S. Devadas, and D. Lim, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, pp. 1077–1098, 2004.
[10] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Delay-based circuit authentication and applications," in *ACM Symposium on Applied Computing*, 2003, pp. 294–301.
[11] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symposium On VLSl Circuits Digest of Technical Papers*, 2004.
[12] B. Gassend, "Physical random functions," M.S. Thesis, Massachusetts Institute of Technology, Massachusetts, 2003.
[13] A. Bellaouar and M. Elmasry, *Low-Power Digital VLSI Design. Circuits and Systems, 1st edn*. Kluwer Academic Publishers, 1995.
[14] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4727, 2007, pp. 63–80.
[15] P. Tuyls, G. J. Shrijen, B. Skoric, J. V. Geloven, N. Verhaegh, and R. Walters, "Read proof hardware from protective coatings," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4249, 2006, pp. 369–383.
[16] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2010, pp. 366–382.
[17] J. Guajardo, S. Kumar, R. Maes, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Hardware-Oriented Security and Trust (HOST)*, 2008, pp. 67–70.
[18] S. Goren, H. Ugurdag, A. Yildiz, and O. OÌĹzkurt, "FPGA design security with time division multiplexed pufs," in *International Conference on High Performance Computing and Simulation (HPCS)*, 2010, pp. 608–614.
[19] J. Anderson, "A puf design for secure FPGA-based embedded systems," in *Design Automation Conference (ASP-DAC), 2010 15th Asia and South Pacific*, 2010, pp. 1–6.
[20] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference (DAC)*, 2007, pp. 9–14.

Note :

G. Komurcu received his BS degree from Sabanci University, Istanbul, Turkey in 2005 on Microelectronics and his MS degree from Bogazici University, Istanbul, Turkey in 2008 on Electrical Engineering. His PhD is still continuing at Bogazici University. He is currently working at TUBITAK since 2005 as a chief design engineer on VLSI design. His research interests include digital design and mixed-signal design.

A. E. Pusane received the B.Sc. and M.Sc. degrees in electronics and communications engineering from Istanbul Technical University, Istanbul, Turkey, in 1999 and 2002, respectively, and the M.Sc. degree in electrical engineering, the M.Sc. degree in applied mathematics, and the Ph.D. degree in electrical engineering from the University of Notre Dame, Notre Dame, IN, in 2004, 2006, and 2008, respectively. He was a Visiting Assistant Professor at the Department of Electrical Engineering, University of Notre Dame, during 2008-2009, after which he joined the Department of Electrical and Electronics Engineering, Bogazici University, Istanbul, Turkey, as an Assistant Professor. His research is in coding theory.

G. Dündar was born in Istanbul in 1969. He obtained his BS and MS degrees from Bogazici University, Istanbul, Turkey in 1989 and 1991, respectively, and his PhD from Rensselaer Polytechnic Institute, NY in 1993, all in Electrical Engineering. He has been lecturing at Bogazici University since Spring 1994, teaching courses on Electronics, Electronics Lab, IC Design, Electronic Design Automation, and Semiconductor Devices. He has also given lectures at the Turkish Air Force Academy in Spring 1994 on Computer Networks. During the period August 1994 - November 1995, he was with the Turkish Navy and taught courses on Electronics, Electronics Lab, and Signals and Systems at the Turkish Naval Academy. He was with EPFL, Switzerland between September 2002 and June 2003, and with Technical University of Munich in the Spring of 2010, on sabbatical leave from Bogazici University. He has been holding the professor title since March 2002. He has received several awards, including the nationwide research encouragement award from TUBITAK. He is the author/co-author of more than 100 technical papers in international journals and conferences. Research interests: Analog IC design and electronic design automation.