IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 30 April 2013; revised 6 September 2013; accepted 7 October 2013. Date of publication 27 October 2013;
date of current version 7 May 2014.

Digital Object Identifier 10.1109/TETC.2013.2287182

A PUF Based on a Transient Effect Ring Oscillator and Insensitive to Locking Phenomenon

LILIAN BOSSUET[1] (Member, IEEE), XUAN THUY NGO[2], ZOUHA CHERIF[1,2], AND VIKTOR FISCHER[1]

[1]Laboratoire Hubert Curien, UMR CNRS 5516, University of Lyon, Lyon 69007, France
[2]Laboratoire CNRS LTCI, Institut MINES-TELECOM, TELECOM ParisTech, Paris 75013, France
CORRESPONDING AUTHOR: L. BOSSUET (lilian.bossuet@univ-st-etienne.fr)

The work presented in this paper was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French Agence Nationale de la Recherche.

ABSTRACT This paper presents a new silicon physical unclonable function (PUF) based on a transient effect ring oscillator (TERO). The proposed PUF has state of the art PUF characteristics with a good ratio of PUF response variability to response length. Unlike RO-PUF, it is not sensitive to the locking phenomenon, which challenges the use of ring oscillators for the design of both PUF and TRNG. The novel architecture using differential structures guarantees high stability of the TERO-PUF. The area of the TERO-PUF is relatively high, but is still comparable with other PUF designs. However, since the same piece of hardware can be used for both PUF and random number generation, the proposed principle offers an interesting low area mixed solution.

INDEX TERMS PUF, TRNG, oscillatory metastability.

I. INTRODUCTION

The continuous increase in the number of publications on silicon physical unclonable functions (PUFs) highlights their scientific and practical interest. Numerous silicon PUF structures have already been proposed, although only a few basic principles are known: one can use the race of delays between two symmetrical delay lines (arbiter PUF [1]), frequency mismatch in multiple ring-oscillators (RO-PUF [2], [3]), metastability of a couple of cross-coupled elements (SRAM-PUF [4] and butterfly PUF [5]), and a mixture of a chain of configurable delay lines and a ring oscillator (Loop-PUF [6]).

Recent characterization of PUF architectures showed that RO-PUF was the best candidate for FPGA and ASIC implementation [1], [2]. Indeed, RO-PUF has very good statistical properties (output bias, intra-uniqueness and steadiness) when implemented in both FPGA and ASIC. However, one major constraint must be satisfied: the ring oscillators must be completely independent. Still, it is possible to change the working conditions of the ring oscillators to make them dependent. A phenomenon of locking of the ring oscillators then can occur. This locking phenomenon was highlighted by Bochard et al. in 2010 by manipulating the supply voltage of the RO-based true random number generator (TRNG) [7]. More recently, Bayon et al. used electromagnetic fault injection to change the behavior of ring oscillators embedded in FPGA [8]. They also used an electromagnetic channel to collect information such as oscillator frequency and the physical location of the oscillator inside the chip [9]. Similar results were obtained in [10] when the target was specifically RO-PUF. These works clearly challenge the use of ring oscillators for TRNG and PUF design. Depending on the security requirement [2], first, ring oscillators have to be completely independent. Second, the frequency of the ring oscillator has to be hidden. Because of electromagnetic attacks, these requirements are no longer guaranteed.

In this article, we propose a new PUF structure that exploits the oscillatory metastability of cross-coupled elements. Entropy extraction is based on the mean number of oscillation cycles. This PUF is based on transient effect ring oscillator (TERO) cells and it is called TERO-PUF. It is not sensitive to locking phenomenon because the oscillation frequency is not taken into account during the entropy extrac-

tion process. Oscillator independence is not required for security.

TEROs were originally proposed for TRNG designs [11]. Although TRNGs and PUFs extract randomness from the same piece of hardware, the source of randomness exploited in the two primitives is very different: TRNGs use continuous real-time random phenomena that occur when the device is running, while PUFs use random phenomena that occur only once – during the manufacturing process. As described in [12], combining PUF and TRNG in the same primitive could be cheaper than implementing the two structures independently. Although our experimental results showed that the proposed TERO-PUF structure can also provide a random bitstream, this paper focuses only on TERO-PUF design and characteristics.

The proposed TERO-PUF was tested on nine ALTERA DE1 boards featuring Cyclone-II FPGA. For each FPGA, four placements were used.

The paper is organized as follows. In Section II and III, we describe TERO cell behavior and TERO-PUF architecture and design. In Section IV, we present the experimental results of FPGA implementation of a TERO-PUF. Finally, in Section V, we compare the characteristics of the main known PUF principles and the proposed TERO-PUF. In Section VI, we draw some conclusions.

II. TERO LOOP ARCHITECTURE AND BEHAVIOR

The TERO loop is composed of an SR flip-flop: two AND gates and an even number of inverters (usually two but the loop can be extended by using more inverters in order to extend the oscillations). According to [13], [14], the TERO loop uses an SR-flip-flop with oscillatory metastability by connecting the *S* and *R* inputs of the SR-flip-flop to the *ctrl* signal. Fig. 1 shows the TERO loop architecture.

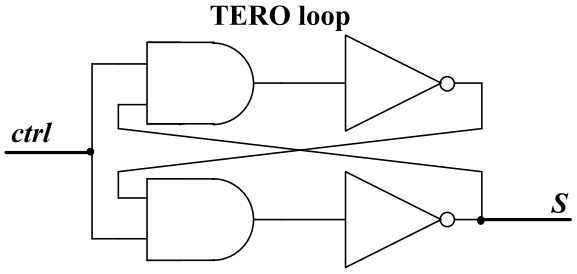

FIGURE 1. **TERO loop structure.**

The rising edge of the *ctrl* signal (the loop stimulation signal) causes transitory oscillations in the loop if the two following conditions are fulfilled [11]: the circuit must have a positive feedback and the *RC* time constant (defined by the parasitic resistance and capacity) must be shorter than the total delay of all logic elements involved in the loop. In theory, if the loop is ideally symmetrical, oscillations never stop. However, the circuit usually only oscillates for a short time after which the oscillations stop due to intrinsic asymmetry *Td* defined in [11]. This behavior is commonly named oscillatory metastability [13], [14] or metastability of oscillations. The *Td* factor represents the time difference between the time delays of both halves of the loop.

The authors in [11] claim that the number of temporary oscillations is inversely proportional to the size of *Td*. They also claim that the average *Td* value of a well balanced TERO loop is related to random contributions to gate delays, which originate in semiconductor intrinsic noise. In this way, the number of oscillations is significantly affected by random circuit noise, so the number of oscillations varies at the end of successive stimulation intervals. On the other hand, general perturbations (e.g. in the power supply) do not significantly affect the *Td* parameter because of the ''differential'' behavior of the loop.

Unlike the structure in [11], which uses XOR and AND gates to control the loop, our architecture uses AND gates and inverters to stimulate the oscillatory metastable state. Accordingly, the loop used is smaller than in [11].

Fig. 2 shows the input signal (*ctrl*) and output signals ($S_{\#1}$, $S_{\#2}$) of two TERO loops implemented in an ALTERA Cyclone-II FPGA. Each TERO loop is implemented in one logic array block (LAB). In Fig. 2, the *ctrl* signal controlling the loop #1 and #2 is forced to '1' for 2.5 μs (its frequency is 200 kHz). As explained above, the rising edge of the *ctrl* signal causes temporary oscillations of the $S_{\#1}$ and $S_{\#2}$ signals. As illustrated in Fig. 2, the number of oscillations is not the same in the two signals. In addition, the final logic levels can also differ, ('0' or '1'), as shown in Fig. 2.

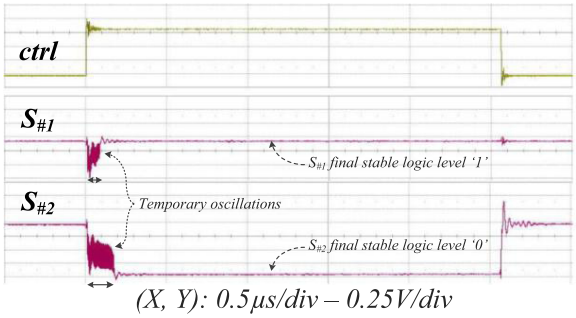

FIGURE 2. **Electrical behavior of the two TERO loops.**

III. TERO-PUF DESIGN

A. EXTRACTION OF THE PROCESS VARIATION ENTROPY

As explained previously, the behavior of the TERO loop depends on variations in the production process in two ways; both the final stable state of the *S* signal (''0'' or ''1'') and the number of temporary oscillations that depend on it. Clearly, both phenomena can be used as a source of entropy to generate a PUF response. The PUF challenge can be generated by the rising edge of the *ctrl* signal.

We first tested the number of stable end levels '0' and '1' of the *S* signal for all possible TERO loop placements in nine ALTERA DE1 boards featuring the EP2C20 device. As each TERO loop uses one Cyclone II LAB, we implemented 1172

TERO loops in each device. For all 10 548 TERO loops tested in the nine cards, we obtained the following results: the output signal S fell to the stable logic level '0' in 40.3% of the cases, to level '1' in 30.7% of the cases, and was unstable (oscillating) in 29.0% of the cases. This oscillating state is a major drawback when using the final state of the output signal S as a PUF response.

We assume that in some cases (roughly a third of the TERO loops implemented) Td is quite small due to random symmetry of process variations, and similar results were reported in [15]. Unlike [15], we thus conclude that final state of the output signal S cannot be used as a source of the entropy from the manufacturing process.

Next, we measured the number of oscillations of the output signal S. We used 8-bit counters to measure the number of temporary oscillations. We chose a low speed *ctrl* signal (390 KHz) to clearly distinguish temporarily oscillating loops from those that were permanently unstable. As before, 10 548 TERO loops were tested. The number of oscillations was measured 2^{18} times for each loop. In all the experiments, temporarily oscillating signals did not oscillate more than 255 periods and an 8-bit counter was consequently sufficient. In 2^{18} measurements, for each temporarily unstable TERO loop, the number of oscillations was normally distributed. According to the central limit theorem, the distribution of the number of oscillations is due to the sum of many independent random variables. Clearly, the mean value of this distribution is related to the characteristics of the chip, which is determined by variations in the manufacturing process and can thus serve as an entropy source for the PUF response. The standard deviation of the distribution is due to electronic noise.

According to our experimental results, the last significant bits (LSBs) of the 8-bit counter are not stable because of the electronic noise in the device (they are used as an entropy source for the TRNG).

The most significant bits (MSBs) varied significantly from one TERO loop to another, and their mean values were pretty stable during the 2^{18} measurements in one TERO loop. Next, the statistical properties of these bits were observed to characterize the proposed TERO-PUF.

In the case of oscillating TERO loops, we observed that the mean number of oscillations of signal S was stable in all PUF cells, but differed in all of them. As a consequence, the same MSBs can be used as a PUF response. By using the mean number of oscillations, the TERO-PUF uses both stable and unstable TERO loops.

B. TERO-PUF ARCHITECTURE

According to the previous section, the TERO-PUF should exploit the mean number of oscillations of the output signal of the TERO loop. The proposed TERO-PUF uses TERO loops and also needs binary counters and the circuitry aimed at computing the mean value of oscillations of each TERO loop. Since the first step of our research was focused on observing PUF statistical parameters, the PUF circuitry was not optimized for area: we decided to use the same counter size (8 bits) and to make 2^{18} measurements of the number of oscillations to ensure the precision of the measurements required for PUF characterization.

Using a differential structure is customary when noise perturbations in electronic systems have to be reduced. However, implementation of differential structures can result in considerable additional costs, especially if large TERO-PUF responses are needed. The differential structure of the proposed TERO-PUF takes this constraint into account. Fig. 3 depicts TERO-PUF architecture. It is based on a set of pairs of elementary TERO loops extended by a binary asynchronous 8-bit counter with a 26-bit accumulator and an 18-bit shift register to measure the mean value of the number of oscillations.

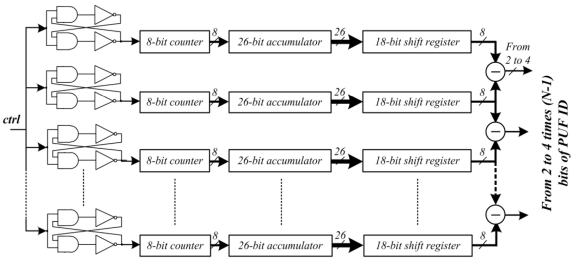

FIGURE 3. TERO-PUF architecture.

To end the design of TERO-PUF, selection of some of final bits (subtraction results) has to be made by statistical characterization. Following section presents characterization metrics used for PUF.

C. PUF CHARACTERIZATION METRICS

Three metrics are used for the PUF intra- and inter-device characterization [2], [16]: bias, intra-device variation and inter-device variation.

Bias is evaluated by measuring the bit bias of the PUF ID. This parameter is equal to the percentage of '0' in the PUF ID.

Intra-device variation (also called **reliability** [2] or **steadiness** [16]) quantifies changes at the output of a PUF function over many measurements. Since we did not have enough chips at our disposal for well founded statistical evaluation, we considered four PUF implementations in the same chip as four realizations of the same PUF in different devices. An n-bit reference response $\bar{R}_i^{PL}$ was estimated from chip i and placement PL in normal operating conditions, usually by averaging samples $R_{i,y}^{PL}$ (where y is the y-th sample of measurement of R_i^{PL}). The intra-device variation X_i^{PL} was estimated as the average intra-chip Hamming distance (HD) over 1 samples defined for the chip i as

$$X_i^{PL} = \frac{1}{x}\sum_{y=1}^{x}\frac{HD\left(R_{i,y}^{PL}, \bar{R}_i^{PL}\right)}{n} \times 100\%. \qquad (1)$$

The compared responses were produced from the same PUF implementation (one of four PUF placements or one of nine

devices) and this Hamming distance is consequently called the intra-device *HD*. A lower intra-device *HD* (close to 0%) results in a more stable PUF response.

Inter-device variation (also called **uniqueness** [2], [16]) shows to what extent IDs generated by the PUF in different devices are unique. Average between-device *HD* of the PUF ID is an estimate of the uniqueness property. With two different chips u and v, and responses $R^{PL}_{u,y}$ and $R^{PL}_{v,y}$ respectively, the average between-device variation U^{PL} for a set of m chips is defined as (2)

$$U^{PL} = \frac{1}{m\,(m-1)\,x} \sum_{u=1}^{m} \sum_{\substack{v=1 \\ v \neq u}}^{m} \sum_{y=1}^{x} \frac{HD\left(R^{PL}_{u,y}, \bar{R}^{PL}_{v}\right)}{n} \times 100\% \quad (2)$$

where $\bar{R}^{PL}_{v}$ is an estimated reference ID of chip v with PUF placement PL. In normal operating conditions, it is estimated by averaging samples $R^{PL}_{v,y}$.

Expression (2) includes all possible pair-wise *HDs* among m distinct chips tested. For a truly random PUF output, the between-device variation should be close to 50%.

D. SELECTION OF OUTPUT BITS IN TERO-PUF

We evaluated the bias and intra-device variation in each of the 8-bit results of subtraction with the following experimental setup: 64 TERO loops, 63 subtractions, 4 placements, 9 boards, and 128 samples by measurement. Table 1 lists the average values for all subtraction results.

TABLE 1. Evaluation of bias and intra-device variation of subtraction 8-bit outputs for TERO-PUF.

	Bias (%)	Intra-device variation (%)	Used in TERO-PUF response
Bit #7	54.2	1.7	yes
Bit #6	54.2	1.7	yes
Bit #5	52.3	2.7	may be
Bit #4	51.7	4.8	may be
Bit #3	51.6	9.1	no
Bit #2	51.8	17.2	no
Bit #1	52.7	30.1	no
Bit #0	50.3	39.5	no

The two most significant bits of the shift register output are always selected as a TERO-PUF response, since they have a very low intra-device variation (less than 2%). However, according to Table 1, instead of using only two bits, the three or four most significant bits could be used and still give acceptable results. In this case, a stronger error correcting system has to be used.

As a consequence, TERO architecture is fully scalable; using 64 elementary TERO loops, the TERO-PUF can generate a response of 126 bit, 189 bit or 252-bit ID, when using 2, 3 or 4 bits of the subtraction result. In the following section we present some hardware implementation results of a 64-Loop TERO-PUF with an ID size ranging from 126 bits to 252 bits.

IV. TERO-PUF HARDWARE IMPLEMENTATION AND CHARACTERIZATION

To characterize intra- and inter-device variation in the TERO-PUF response, we placed four identical 64-Loop TERO-PUFs (126-bit, 189-bit or 252-bit IP in size) described in the previous section in all available FPGAs. Fig. 4 depicts the architecture of the design implemented in nine ALTERA Cyclone II FPGA devices.

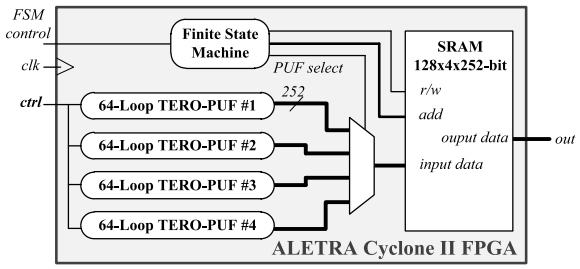

FIGURE 4. FPGA Implementation of four 64-loop TERO-PUFs.

Each TERO-PUF was tested for four placements ($PL = 4$), nine chips ($i = 9$) and 128 samples ($y = 128$). We tested PUF responses in normal operating conditions (Ta = 28 °C and nominal $V_{core} = 1.5V$). The frequency of the *ctrl* signal was 50 MHz.

- The mean value of intra-device variation in the implemented TERO-PUF with 126-bit ID was equal to 1.73%, meaning that the average intra-device Hamming distance was less than 2.2 bits from a 126-bit ID.
- The mean value of intra-device variation in the implemented TERO-PUF with 189-bit ID was equal to 2.07%, meaning that the average intra-device Hamming distance was less than 3.9 bits from a 189-bit ID.
- The mean value of intra-device variation in the implemented TERO-PUF with 252-bit ID was equal to 2.75%, meaning that the average intra-device Hamming distance was less than 7.0 bits from a 252-bit ID.

Fig. 5 shows the histograms of TERO-PUF intra-device variation obtained experimentally with 126-bit (Fig. 5-a), 189-bit (Fig. 5-b) and 252-bit (Fig. 5-c) IDs. The results show the good stability of the TERO-PUF response over time. Nevertheless, it is clear that an additional error-correcting algorithm will be required if bit errors are to be completely avoided.

The mean values of inter-device variation in the implemented TERO-PUF were respectively 48.07%, 48.99% and 49.27% for 126-bit, 189-bit and 252-bit IDs. This is close enough to the ideal value (50%) and is thus suitable for most applications where device authentication is needed. Fig. 6 shows histograms of inter- and intra-device ID variation in TERO-PUF for the three ID sizes (126-bit ID: Fig. 6-a, 189-bit ID: Fig. 6-b, 252-bit ID: Fig. 6-c). For each case, the two histograms are clearly separated.

Fig. 6 shows that the bigger the ID, the better the inter-device variation. The same result can be found in Table 2

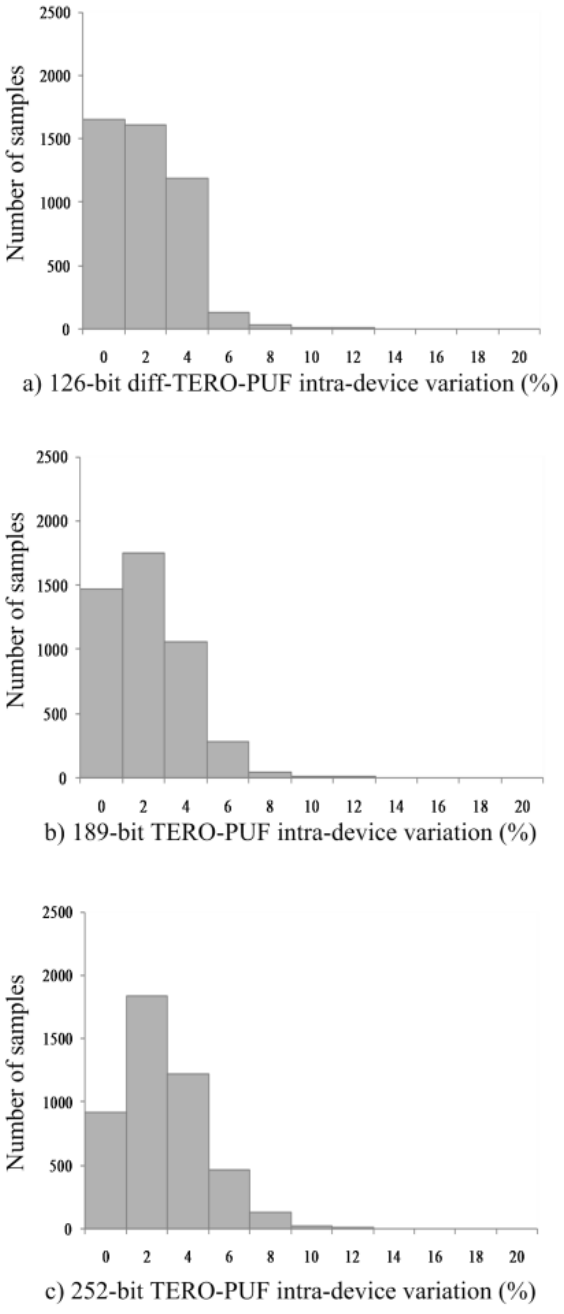

FIGURE 5. **TERO-PUF intra-device variation.**

which gives a summary of the 64-loop TERO-PUF statistical characterization.

V. DISCUSSION

In this section, we compare the proposed TERO-PUF with the silicon PUF described in previous works. Table 3 lists the intra-device variation, inter-device variation and ID-size of published and new PUFs. It is not possible to compare the area and hardware resources needed by different designs, because most published designs use different technologies and optimization strategies.

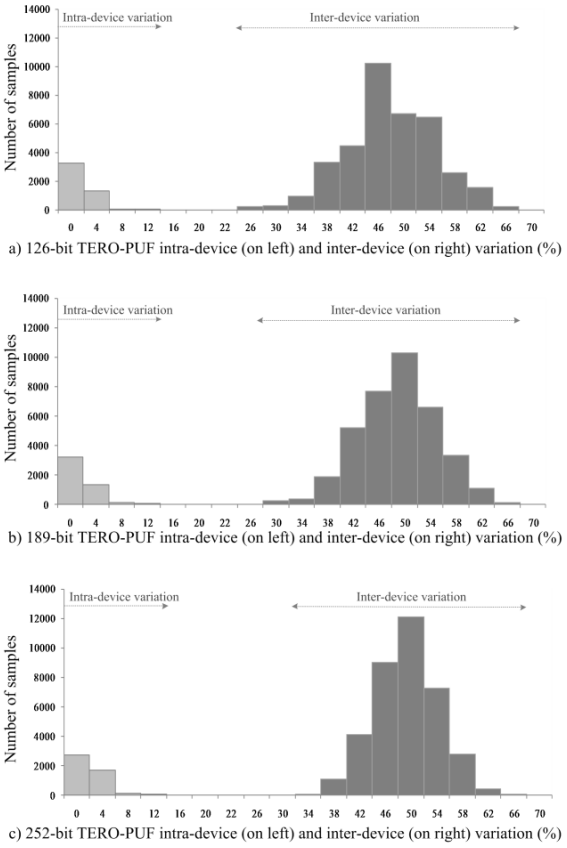

FIGURE 6. **TERO-PUF intra- (left) and inter-device (right) variation.**

TABLE 2. **Characteristics of 64-loop TERO-PUF.**

PUF ID size (bits)	Intra-device variation (%)	Inter-device variation (%)	Cyclone-II LABs
126	1.73	48.07	416
189	2.07	48.99	
252	2.75	49.27	

As can be seen in Table 3, the proposed TERO-PUF significantly enhances the PUF design space. Like RO-PUF, TERO-

TABLE 3. **Comparison of PUF characteristics.**

	Intra-device variation (%)	Inter-device variation (%)	PUF ID size (bits)
Arbiter PUF [1]	3.7-12.5	38	1
RO-PUF [2]	1.0	40	1
SRAM-PUF [4]	3.7-10.5	50	*data size*
Butterfly PUF [5]	6.0	45	1
Loop-PUF [6]	1.3	~50	3
TERO-PUF	**1.7**	**48**	**126**

PUF is appropriate for FPGA implementation. Moreover, TERO-PUF is fully scalable. It has low intra-device variation and large size of the response. The main drawback of TERO-PUF is the amount of hardware resources occupied. Nevertheless, the hardware resources presented in Table 2 are obtained without any optimization effort. We assume that it would be possible to significantly decrease the number of resources used by the TERO-PUF by optimizing area during design. Moreover, with the same number of TERO loops, more independent pairs could be selected, with the aim of extracting more entropy from the same hardware. Optimization of the entropy extraction will be one of our future objectives.

Unlike RO-PUF, the main advantage of the proposed TERO-PUF is that it is not sensitive to locking phenomenon. Indeed, the oscillation frequency in not taken into account. TERO-PUF uses the number of oscillations as an entropy extractor that does not depend on the locking phenomenon. An electromagnetic attack, which allows the attacker to discover the oscillation frequency, provides no information on the number of oscillations.

To test the TERO-PUF as a TRNG, we tested the three least significant bits (bits#0, bit#1 and bit#2) of the output of the 8-bit counter (see Fig. 3). These three bits passed the FIPS tests (140-1 and 140-2 [17]) successfully. Nevertheless, according to AIS-31 [18] this result is not sufficient to guarantee TRNG security today. We need to provide an entropy extraction model for both TRNG and PUF services. This will be a part of our future work.

VI. CONCLUSION

In this article, we presented a novel PUF structure based on the TERO loop. By using the average number of oscillations as entropy extractor, the proposed TERO-PUF is not sensitive to the locking phenomenon. This phenomenon challenges the use of ring oscillators in both PUF and TRNG. As a consequence, TERO-PUF is a new candidate for FPGA-dedicated PUF.

Compared with other state-of-the-art PUFs, the proposed TERO-PUF is very attractive thanks to its low intra-device variation and large response (1.73% for 126 bits). Future work will concern optimization of the area and the use of the least significant bits of the TERO-Loop counter to generate random numbers. The proposed TERO-PUF cell will thus simultaneously serve as TRNG and as a PUF functional block.

REFERENCES

[1] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 58–64.

[2] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. HOST*, Jun. 2010, pp. 94–99.

[3] S. Katzenbeisser, U. Kocabas, V. Rožic, A. R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, fact or busted? A security evaluation of physically unclonalble functions cast in silicon," in *Proc. Int. Conf. CHES*, 2012, pp. 283–301.

[4] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tulys, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Int. Conf. CHES*, 2010, pp. 63–80.

[5] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tulys, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. Int. Symp. HOST*, 2008, pp. 67–70

[6] Z. Cherif, J. L. Danger, and L. Bossuet, "An easy-to-design PUF based on a single oscillator: The loop PUF," in *Proc. Int. Conf. DSD*, 2012, pp. 1–7.

[7] N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov, "True-randomness and pseudo-randomness in ring oscillator-based true random number generators," *Int. J. Reconfigurable Comput., Hindawi*, vol. 2010, pp. 1–13, Dec. 2010.

[8] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson. *et al.*, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *Proc. Int. Work. COSADE*, 2010, pp. 151–166.

[9] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, "EM leakage analysis on true random number generator: Frequency and localization retrieval method," in *Proc. APEMC*, 2013, pp. 20–24.

[10] D. Merli, D. Schuster, and G. Sigl, "Semi-invasive EM attack on FPGA RO PUFs and countermeasures," in *Proc. WESS*. 2011, pp. 1–9.

[11] M. Varchola and M. Drutarovsky, "New high entropy element for FPGA based true random number generator," in *Proc. Int. Conf. CHES*, 2010, pp. 351–365.

[12] A. Maiti, R. Nagesh, A. Reddy, and P. Schaumont, "Physical unclonable function and true random number generator: A compact and scalable implementation," in *Proc. 19th GLVLSI*, 2009, pp. 425–428.

[13] T. Kacprzak, "Analysis of oscillatory metastable operation of an R-S flip-flop," *IEEE J. Solid-State Circuits*, vol. 23, no. 1, pp. 260–266, Feb. 1988.

[14] L. M. Reyneri, D. Del Conso, and B. Sacco, "Oscillatory metastability in homogeneous and inhomogeneous flip-flops," *IEEE J. Solid-State Circuits*, vol. 25, no. 1, pp. 254–264, Feb. 1990.

[15] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, M. T. Ochiai, and K. Itoh, "Uniqueness enhancement of PUF responses based on the location of random outputting RS latches," in *Proc. Int. Conf. CHES*, 2011, pp. 390–406.

[16] Y. Hori, T. Yoshida, T. Katashitaand, and A. Satoh, "Quantitative and statistical performance evaluation of Arbiter physical unclonable functions on FPGAs," in *Proc. Int. Conf. FPGAs*, 2010, pp. 298–303.

[17] *Security Requirements for Cryptographic Modules*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, May 2001.

[18] "Functionaly classes and evaluation methodology for deterministic random number generators," Bundersamt für Sicherneit in der Informationstechnik., Germany, Tech. Rep., 2001.

LILIAN BOSSUET was a student of the prestigious Ecole Normale Supérieure de Cachan, France. He received the M.S. degree in electrical engineering from Institut National des Siences Appliquées, Rennes, France, in 2001, and the Ph.D. degree in electrical engineering and computer sciences from the University of South Britanny, Lorient, France, in 2004. From 2005 to 2010, he has been an Associate Professor and the Head of the Embedded System Department, Bordeaux Institute of Technologies. Since 2010, he has been an Associate Professor with the University of Lyon/Saint-Etienne and he is a member of the Hubert Curien Laboratory. He holds the special Centre National de la Recherche Scientifique Chair of applied cryptography and embedded system security. His main research activities focus on embedded systems hardware security, IC security, side channel attacks of cryptographic circuits, CryptoProcessor design, and reconfigurable architecture for security. He is a senior member of the CryptArchi Club.

XUAN THUY NGO is a Ph.D. student at Telecom ParisTech, France. He is involved in research on hardware Trojan design and detection. His work is funded by the French project Homere. In 2012, he received the M.S degree in VLSI from Institut National des Sciences Appliquées de Lyon, France.

ZOUHA CHERIF is a Ph.D. student at Telecom ParisTech and Telecom Saint-Etienne, University of Lyon, France. She is involved in research on sources of randomness and authentication for cryptography. Her work is funded by the French Institut of Telecom. In 2010, she received the B.S. and M.S. degrees in telecommunication engineering from Ecole Superieur des Communications de Tunis, Tunisia.

VIKTOR FISCHER received the M.S. and Ph.D. degrees in electrical engineering from the Technical University of Kosice, Slovakia. From 1981 to 1991, he held an Assistant Professor position at the Department of Electronics, Technical University of Kosice. From 1991 to 2006, he was a part-time Invited Professor at the University of Saint-Etienne, France. From 1999 to 2006, he was a consultant with Micronic Slovakia, oriented in hardware data security systems. Since 2006, he has been a full-time Professor at the University of Saint-Etienne. His research interests include cryptographic engineering, secure embedded systems, cryptographic processors and especially true random number generators embedded in logic devices. He is the co-founder and senior member of the CryptArchi club.