A Reliable Low-area Low-power PUF-based Key Generator

Christoph Böhm, Marco Bucci, Maximilian Hofer, Raimondo Luzzi
Infineon Technologies AG
Babenbergerstrasse 10, A-8020 Graz, AUSTRIA

***Abstract*—This paper reports the implementation of a low-area low-power 128-bit PUF-based key generation module which exploits a novel Two-Stage IDentification (TSID) cell showing a higher noise immunity then a standard SRAM cell. In addition, the pre-selection technique introduced in [1] is applied. This results in a stable PUF response in spite of process and environmental variations thus requiring a low cost error correction algorithm in order to generate a reliable key. The adopted PUF cell array includes 1056 cells and shows a power consumption per bit of $4.2\mu W$ at 100MHz with an area per bit of $2.4\mu m^2$. In order to evaluate reliability and unpredictability of the generated key, extensive tests have been performed both on the raw PUF data and on the final key. The raw PUF data after pre-selection show a worst case intra-chip Hamming distance below 0.7%. After a total of more than 5×10^9 key reconstructions, no single fail has been detected.**

I. INTRODUCTION

Physically Unclonable Functions (PUFs) gained attention as a primitive function for identification, especially if no other secured key storage alternative is available.

As a consequence, a large number of different circuital techniques to implement a PUF in a standard silicon process has been investigated. Three basic classes can be distinguished:

1) Delay-based PUFs: the time difference due to local process variations between two nominally identical paths is measured and quantized. Ring oscillator PUFs, Arbiter-based PUFs and Glitch PUFs belong to this class [2], [3].
2) Memory-cell based PUFs: the power-up behavior of memory cells without power on reset (latches or flip-flops) is exploited. Local mismatches in the cell transistors can cause an unpredictable state when the device is powered-up. This category includes SRAM PUFs, Latch PUFs, D Flip-Flop PUFs and Buskeeper PUFs [4], [5], [6].
3) Hybrid PUFs: the two techniques above are combined together in order to improve the randomness of the response and/or the security against attacks [7].

In spite of the wide range of contributions in this field, a complete characterization (under process and environmental variations) of the proposed ideas is not always available. Often too few devices are tested or temperature variations are not taken into account. A first attempt to systematically compare ASIC implementations of the most common PUF types has been reported in [8]: the authors measured about 100 parts and found out bit error rates (BER) between 6 and 15% depending on the PUF type, coming to the conclusion that SRAM PUFs, with an error rate in the order of 7%, show the best performances in terms of reliability and unpredictability of the output. A characterization of ring oscillator PUFs has been reported in [9].

In this work, we focused on the usage of PUFs as key generators and the target was the design of a reliable small footprint PUF module, which can be used if no NVM module is available.

Since area and power consumption are main constraints in a chip-card controller, the focus was on the design of a custom PUF cell which is inherently more reliable than a standard latch or SRAM cell, thus reducing the complexity of the error correction scheme. The proposed two stages identification (TSID) cell operates in two phases behaving as a differential amplifier during a first phase, in order to amplify the local mismatch of two minimum area transistors, and as a latch as soon as a trigger signal is activated. Details about the operating principle and a comparison with a standard latch are reported in Section II. In addition, in order to sort out the few cells that, due to the little mismatch, are more sensitive to noise, temperature and parameter variations, the pre-selection technique introduced in [1] has been adopted. Mask data are generated before the error correction signature during the enrollment and stored in the NVM. During the key reconstruction, the raw data from the PUF cell array (PCA) are first compacted by applying the mask data and then the error correction is performed. The architecture of the proposed key generator is shown in Figure 1: the PCA consists of 1056 TSID cells organized in 22 blocks of 48 cells each. The 48 cells in a block share the same sense amplifier (SA), thus strongly reducing the area of the array. The PCA implementation including the pre-selection is discussed in Section III. The ECC is a standard block code which generates a 128-bit key from the raw data after the masking.

In order to prove reliability and unpredictability of the generated key, extensive tests have been performed on the raw data by measuring, over temperature, about 100 devices from different lots (including split lots). In a first phase, the masking functionality has been tested, by varying the amount of pre-selection up the the maximum value which still leaves enough cells for the ECC (up to 7 bits in each 22 bit block can be discarded). Afterward, instability (defined as the cumulative number of bits which are not stable over the performed read-outs), inter- and intra-chip Hamming distance (HD), bias, and spatial correlations have been measured, finding out that, over

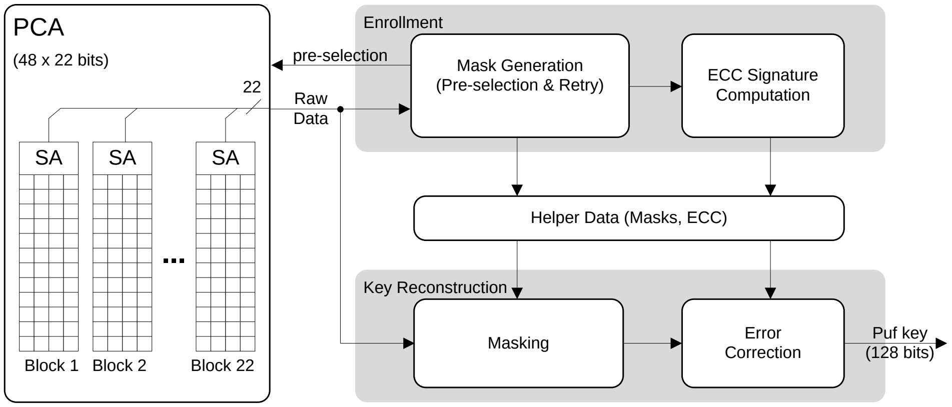

Figure 1. The proposed PUF-based key generator

the temperature range $-40/+110$°C, a worst case instability of about 11% and 2% has to be expected for the proposed PUF before and after pre-selection respectively. The Intra-chip HD (i.e. BER) is below 5% without pre-selection and drops down to maximum 0.7% (at -40°C), if pre-selection is applied. Finally, the stability of the PUF key has been tested by performing the enrollment at 25°C and 10^6 key reconstructions at -40°C and $+110$°C respectively. After testing 3 wafers from different process corners, for a total of about 2000 devices, no single key reconstruction fail has been detected. A summary of the obtained experimental results is reported in Section IV.

II. The TSID cell

The ideal cell in a memory-cell based PUF should generate a stable binary output, dependent on local process variations but immune to electronic noise, disturbances (e.g. from a noisy power supply as in a chip-card controller), global process variations, temperature and aging. Long before the PUF became a topic in the cryptographic community, the problem of generating an ID from local process variations in a chip has been already addressed. In [10], an identification device is patented which is based on an array of identification cells and a circuit for measuring the analog output of each cell and generating a digital data. Each cell includes two equally sized MOS transistors which are biased with the same gate-source voltage. Due to local process variations, the transistor pair shows different threshold voltages and, therefore, the corresponding drain currents are different. The current difference is converted into a voltage difference, amplified and compared using a precise comparator (auto-zeroing comparator) to generate a string of bits. It is unlikely that such a device could be used in a security application (the large analog circuitry could be rather easily probed), but the basic idea was already there: using the unique local process variations to generate on the fly a chip-individual digital information.

More recently, in [6], the authors proposed an identification device based on an array of latches (Figure 2). Initially, both sides of the latch are pulled down (*reset* is high). As the reset is released, each latch evaluates to a state determined by the switching threshold mismatch of the two inverters in the latch. The main advantage with respect to [10] is the simple (low area) implementation: due to the positive feedback, the same circuit generates the process dependent offset, amplifies it and performs the one bit digitization. However, this brings as drawback a higher sensitivity to electronic noise: when the reset is released, the output nodes (*out_p*, *out_n*) are charged up together. As soon as they are close to the inverter thresholds, the positive feedback forces the outputs to diverge: which output goes in which direction depending on which PMOS is stronger and which NMOS has the lowest threshold. Clearly, around the decision point, the circuit is sensitive to noise: if a noise event (or disturbance) occurs right before the decision instant, the positive feedback can force the outputs in the wrong direction. Once the outputs take one direction, they saturate to VDD/VSS. Of course, as smaller is the mismatch, as higher is the sensitivity to noise and disturbances. The authors report that 5.5% of the bits in a 128-bit identification device are not stable. However, the data could be optimistic since the evaluation has been done on 19 dies only and on a reduced temperature range ($0-80$°C).

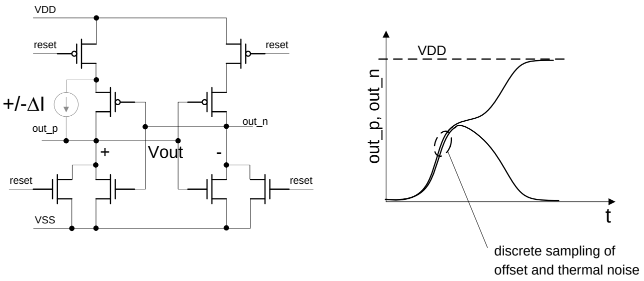

Figure 2. Latch-based ID cell

To show how the noise can lead to a wrong decision, a transient noise Spice simulation of the cell has been performed by forcing an offset current $\Delta I = 50nA$ which simulates a mismatch between the PMOS transistors. The differential output $Vout$ is plotted in Figure 3 over 100 runs (simulating 100 evaluations of the same cell with mismatch ΔI): 9% of the simulated start-ups results in a wrong response.

The TSID cell addresses the noise issue by combining the

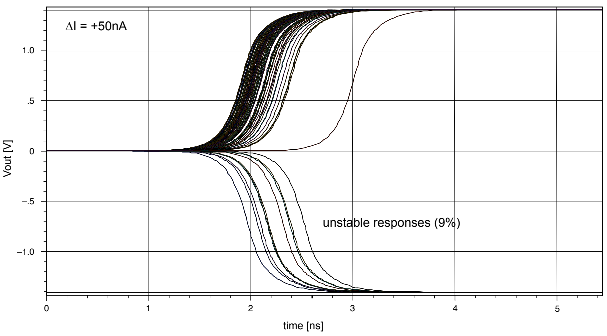

Figure 3. Latch-based ID cell: noise stability

positive feedback with the amplification approach in [10]. A principle scheme is shown in Figure 4: two nominally equal bias currents $I_{bias}$and $I_{bias} \pm \Delta I$ are forced on a positive feedback decision circuit (load) thus generating, when *trigger_n* is low, a differential voltage on *out_p*, *out_n* proportional to the offset ΔI and the differential impedance seen looking into the load (very high, $\gg 1M\Omega$). When the trigger signal is raised (*trigger_n* = 0), the two switches under the diode connected NMOS's are open and the positive feedback pushes the outputs to VDD and VSS respectively. With respect to the cell in Figure 2, in this case there is a phase during which the offset is amplified and only when the trigger is activated, the decision is taken on which direction the outputs saturate. Therefore, offset amplification and decision/digitization are two separate phases. During the first phase the circuit is not sensitive to noise. In the second one, the amplified offset has reached its maximum value thus increasing the signal/noise ratio.

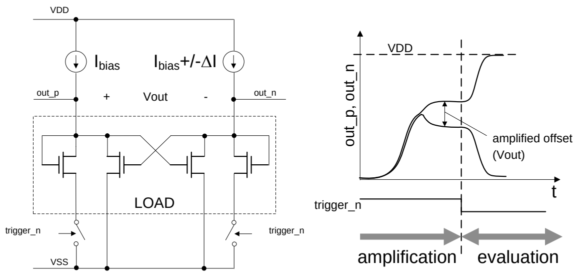

Figure 4. TSID cell: operating principle

The same transient noise simulation as in Figure 3 has been repeated for the TSID cell (with $\Delta I = 50nA$) and in this case none of the 100 runs leads to a wrong decision: after the offset amplification, the electronic noise amplitude is much too small to affect the decision. The distribution of the output voltage V_{out} short before the cell is triggered, simulated over 10^3 Monte Carlo runs at 25°C, is shown in Figure 5 (upper plot): it is interesting noting how the amplification reshapes the mismatch distribution generating a hole around the zero, thus decreasing the number of cells which can be affected by the noise. The same simulation has been performed at -40 and $+120$°C and the distribution of the cells whose response is unstable over temperature (i.e. $(V_{out}$ @-40°C) <> $(V_{out}$@120°C)) is shown in the lower plot: 3.4% of the cells results to be unstable and, as expected, the unstable cells are the ones with the smaller amplified mismatch. As reported in [1], the temperature instability is caused by the mismatch in the temperature coefficient of the MOS threshold voltage V_{th}: two transistors which show a V_{th} mismatch in one direction at low temperature can have a mismatch in the opposite direction at high temperature. Of course, cells with a little mismatch at the reference temperature are more affected by the temperature instability and the solution proposed in [1] consists of sorting out these cells (pre-selection). The authors adopted this technique in this work since, as shown in the followings, it can be applied to the TSID cell with a negligible area overhead and it results to be very effective.

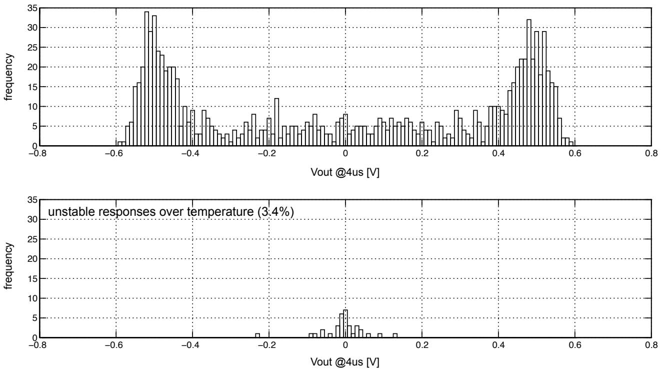

Figure 5. TSID: temperature stability

III. PCA Implementation

A top level description of each block in the PCA is given in Figure 6. The 48 cells in a block share the same sense amplifier and an address decoder allows to select the cell that must be evaluated. A bias generation block provides the biasing signals for the bit cells. The cells are organized in 4 columns of 12 cells each. In contrast with the principle scheme in Figure 4, the TSID cell implementation is reversed: a minimum area NMOS differential pair and two NMOS switches to select one cell inside a row are placed in each bit cell while the load circuit is shared and implemented with PMOS's which are large enough to have a mismatch (i.e. a sensing offset) negligible with respect of the average mismatch of the bit cells. As a result, the response depends almost uniquely on the selected bit cell. In addition, the share sense amplifier provides also some capacitive load that reduces the noise on the bit cell outputs (*sens_p*, *sens_n*) and therefore increases the response stability.

Since the bit cell includes just one type of MOS, the whole cell array is built in a single silicon bulk area thus avoiding the large area loss that follows when two different kinds of bulks must be alternated on the surface. A very compact layout for the cell array can be used and, as a result, the bit cell is much smaller than a typical SRAM cell (Table I).

By choosing NMOS transistors as mismatch devices, we can get rid of the negative-bias temperature instability (NBTI) which affects PMOS devices and is the main responsible for aging degradation in a SRAM PUF by causing an increase in

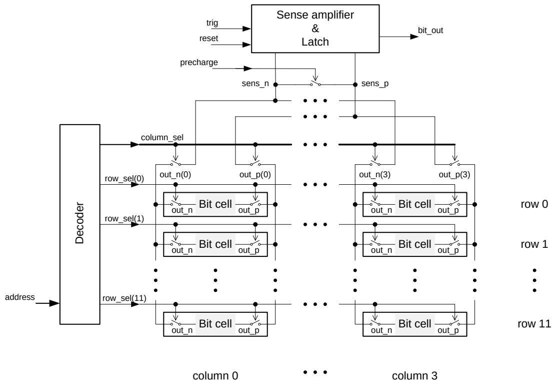

Figure 6. PCA block implementation

the threshold voltage over the time. In addition, the bit cells are powered only when they are addressed thus decreasing power consumption and other aging effects.

The output latch allows to store the previous evaluated response while the next one is evaluated. The sense amplifier is also provided with a precharge (*precharge_n*) and a trigger (*trig*) input. The signal *precharge_n* performs a fast reset of the sensing input before starting the next response evaluation. The signal *trig* changes the behavior of the sense amplifier from high impedance (sensing mode) to negative impedance (latching mode). Since the output is latched by the sense amplifier itself, the input offset of the following latch cannot have any effect on the PUF response. The cell evaluation lasts in total ten clock cycles at 100MHz including one cycle for the precharge, eight cycles for the amplification phase ($80ns$) and a last one to latch the data.

The bit cell structure is shown in 7, where the bias generation is also sketched. The cells are all connected in parallel to the same current source and to the same bias signals *ref_p* and *ref_n*. Two levels of switches allow the selection of the cell. The row switches are inside the cell, while the column ones are shared by the whole column. The pre-selection functionality is implemented in the bias generator by forcing a voltage difference between *ref_p* and *ref_n*. In normal operation, no current flows through R_p and R_n and, therefore, *ref_n* = *ref_p* and each cell delivers an output that depends only on its internal mismatch. When some current is injected in R_p or R_n, a certain offset is forced on the inputs of the bit cell. As a result, the cells whose internal mismatch is not large enough can change their response depending whether or not the forced offset has the opposite direction with respect to the internal mismatch. Hence, by forcing an offset in both direction, it is possible to pinpoint the weak bit cells as the ones that change their response depending on the sign of the pre-selection offset. Of course, the offset level can be adjusted in order to perform a more or less selective pre-selection.

IV. Experimental results

The 1056-bit PCA full-custom macro has an area of about $3250\mu m^2$. The rest of the module has been synthesized. A $1.35V$ power supply and a 100MHz clock are available for the PUF. The average current consumption during the readout of a 22-bit PUF word is about $47\mu A$ at 100MHz, where $25\mu A$ is the current consumption of the bias circuitry. This results in an energy dissipation of 42fJ/bit.

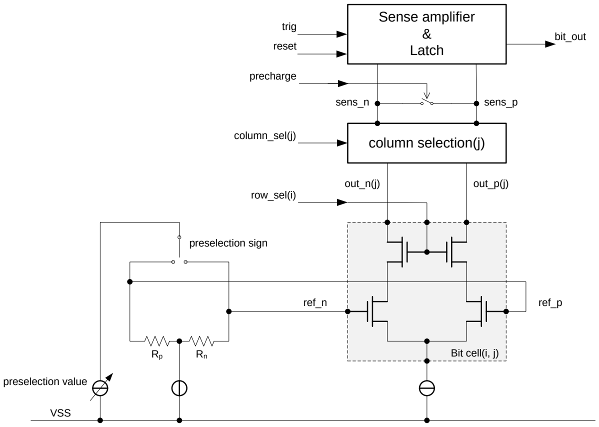

Figure 7. TSID cell with pre-selection

Performance	Value	Unit
Total area	3250	μm^2
Bit-cell area	2.4	μm^2
Cell count	1056	
Energy/bit	42	fJ/bit
Power/bit@100MHz	4.2	μW

Table I
Analog characteristics

A first set of measurements has been performed to evaluate functionality and performance of the pre-selection circuit. In Table II, the average (over 10^2 readouts) of the first 10 bits in a PCA with different values of pre-selection are reported. Most of the bits are stable (average 0 or 1) and they can be toggled only if a strong pre-selection is applied. The 7-th bit results to be unstable and it can be easily sort out by applying even the smallest pre-selection amplitude (bit @pre-selection = -1 $\neq$ bit@pre-selection = +1).

The total number of unstable bits has been evaluated by reading the PUF raw data 10^3 times at -40, 25 and 110°C over 96 dies extracted from 3 wafers from different process corners. The obtained results are shown in Figure 8 before and after pre-selection is applied. The percentage of masked bits is also shown. For the pre-selection, the largest value which still leaves enough bits (up to 7 bits in a 22-bit word can be masked) is used. In addition, the readout of the PUF is repeated 16 (for both pre-selection directions) during the mask generation accumulating the results. Of course, the mask generation is performed only once at 25°C. After pre-selection, the instability is below 2% and a maximum of about 25% of the cells are masked. It is worth noting that, since the pre-selection strength is chip-individual adjusted in discrete steps to the maximum which still allows a key generation, two clusters are visible in the lower plot: most of the dies are adjusted for the smallest pre-selection (0 - 15% masked bits), for the others the next step is used (20-25% masked bits). Process dependencies are not observable.

In Figure 9, the effect of temperature variations on the intra-chip HD without masking is shown: one device has been read

	Pre-selection steps														
Bit #	-7	-6	-5	-4	-3	-2	-1	*0*	+1	+2	+3	+4	+5	+6	+7
1	0	0	0	0	1	1	1	*1*	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	*1*	1	1	1	1	1	1	1
3	0	0	0	0	0	0	0	*0*	0	1	1	1	1	1	1
4	0	0	0	0	0	0	1	*1*	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	*1*	1	1	1	1	1	1	1
6	0	0	1	1	1	1	1	*1*	1	1	1	1	1	1	1
7	0	0	0	0	0	0	0	*0.14*	1	1	1	1	1	1	1
8	0	0	0	0	0	0	0	*0*	0	0.99	1	1	1	1	1
9	0	0	0	0	1	1	1	*1*	1	1	1	1	1	1	1
10	0	0	0	0	0	0	0	*0*	0	0	0	0	0	1	1

Table II
BASIC PRE-SELECTION TEST

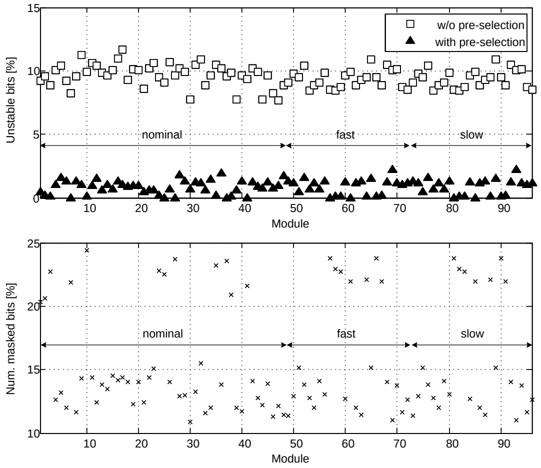

Figure 8. Instability and number of masked bits

out 10^3 times at 3 temperatures, taking one PUF response at 25°C as reference. As expected, the temperature contribution is predominant with respect to the noise.

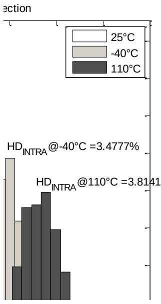

Figure 9. Intra-chip HD without pre-selection vs. temperature

The intra-chip HD evaluated over the complete set of tested modules at 3 temperatures after pre-selection is shown in Figure 10: a worst case value of 0.7% at -40°C has been obtained. Such a low error rate can be easily handled with a low cost error correction code.

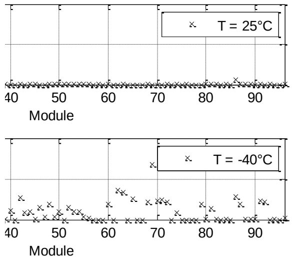

Figure 10. Intra-chip HD after pre-selection

In order to verify the unpredictability of the generated key, inter-chip HD, bias and the correlation between two neighboring bits have been evaluated. The inter-chip HD has been measured over 1080 modules and its average value $HD_{INTER} = 49.986\%$ is almost ideal (Figure 11). The average of the PUF raw data before pre-selection (1056 bits) calculated over 1080 modules is 49.995% showing that the data have no relevant bias (Figure 12). The same average performed on the bit position (Figure 13), gives almost the same distribution thus excluding dependencies with the position of a bit in the array (Figure 13).

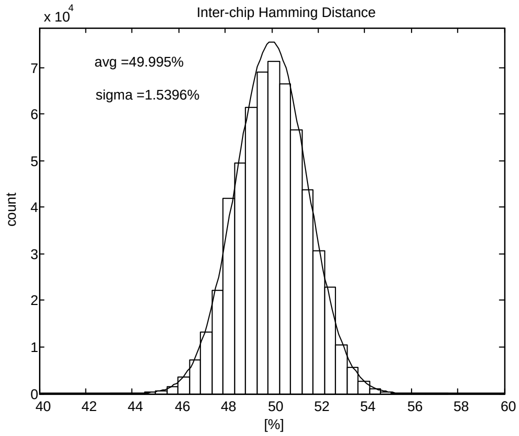

Figure 11. Inter-chip HD

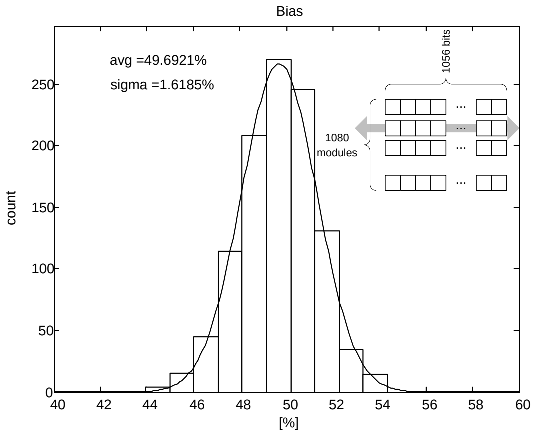

Figure 12. Bias

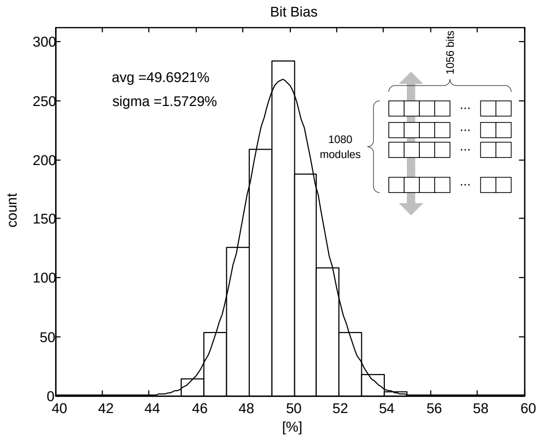

Figure 13. Bit-bias

V. Conclusions

A 128-bit PUF-based key generator which exploits an improved identification cell and the masking of weak bits is described. The module is extremely compact, requiring only 1056 PUF cells to generate a reliable and unpredictable key. The total PUF cell array needs $3250\mu m^2$ and shows an energy consumption per bit of $42fJ/bit$. The bit cell area ($2.4\mu m^2$) results to be even smaller than that of a standard SRAM cell. It is also worth noting that in a SRAM which is not designed to be used as PUF, the cell layout is not necessary perfectly symmetric. This means that the bits can be biased and thus, in order to extract enough entropy, a larger number of cells is necessary than in the proposed generator.

Extensive tests have been performed on the PUF raw data on about 100 dies from different wafers covering process variations, over the temperature range -40 to 110°C. A maximum intra-chip HD of 0.7% have been measured. An analysis of the bias and correlation did not highlight any relevant statistical defect. The stability of the generated key has been tested by performing the enrollment at 25°C and 10^6 key reconstructions at -40°C and $+110$°C. After testing about 2000 devices from different wafers, for a total of more than 5×10^9 key reconstructions, no single fail has been detected.

References

[1] M. Hofer, C. Böhm, An Alternative to Error Correction for SRAM-Like PUFs, Proc. Workshop on Cryptographic Hardware and Embedded Systems, CHES 2010, LNCS, vol. 6225, pp. 335-350, Springer, Heidelberg (2010).

[2] G. E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, Proc. ACM/IEEE Design Automation Conference, DAC 2007, pp. 9-14, (2007).

[3] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas. A technique to build secret key in integrated circuits for identification and authentication application, Proc. Symposium on VLSI Circuits, pp. 176-159, (2004).

[4] J. Guajardo, S. Kumar, G. Schrijen, P. Tuyls, FPGA intrinsic PUFs and their use for IP protection, Proc. on Cryptographic Hardware and Embedded System, CHES 2007, LNCS, vol. 4727, pp. 63-80, Springer, Heidelberg (2007).

[5] S. Okumura, S. Yoshimoto, H. Kawaguchi, M. Yoshimoto, A 128-bit chip identification generating scheme exploiting SRAM bitcells with failure rate of 4.45×10^{-19}, IEEE Proc. European Solid State Circuits Conference (ESSCIRC 2011), pp. 527-530, (2011).

[6] Y. Su, J. Holleman, B. P. Otis, A Digital 1.6pJ/bit Chip Identification Circuit Using Process Variations, IEEE J. Solid-State Circuits, vol. 43, no. 1, Jan. 2008.

[7] S. Satpathy, S. Mathew, L. Jiangtao, P. Koeberl, M. Anders, H. Kaul, G. Chen, A. Agarwal, S. Hsu, R. Krishnamurthy, 13fJ/bit probing-resilient 250K PUF array with soft darkbit masking for 1.94% bit-error in 22nm tri-gate CMOS, IEEE Proc. European Solid State Circuits Conference (ESSCIRC 2014), pp. 239-242, (2014).

[8] S. Katzenbeisser, Ü. Kocabas, V. Rozic, A. Sadeghi, I. Verbauwhede, C. Wachsmann, PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon, Proc. Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, LNCS, vol. 67428, pp. 283-301, Springer, Heidelberg (2012).

[9] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, A large-scale characterization of RO-PUF, Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2010), Anaheim, CA, (2010).

[10] K. Lofstrom, System for providing an integrated circuit with a unique identification, US Patent no. 6,161,213, Dec. 2000.

[11] D. Nedospasov, J.P. Seifert, C. Helfmeier, C. Boit, Invasive PUF Analysis, Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2013, pp. 30-38, (2013).

[12] M. Hiller, M. Weiner, L.R. Lima, M. Birkner and G. Sigl, Breaking through fixed PUF block limitations with differential sequence coding and convolutional codes, Int. Workshop on Trustworthy Embedded Devices, TrustED 2013, pp. 43-54, (2013).

[13] J. Delvaux, D. Gu, D. Schellekens and I. Verbauwhede, Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis, IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol., no. 99, pp. 1-14, 2014.