Experimental Evaluation of Physically Unclonable Functions in 65 nm CMOS

Roel Maes, Vladimir Rožić and Ingrid Verbauwhede
KU Leuven: ESAT-COSIC and IBBT
Leuven, Belgium
http://www.esat.kuleuven.be

Patrick Koeberl
Intel Ireland
Leixlip, Ireland
http://www.intel.com

Erik van der Sluis and Vincent van der Leest
Intrinsic-ID
Eindhoven, The Netherlands
http://www.intrinsic-id.com

***Abstract*— We present a silicon characterization vehicle implementing six different constructions of intrinsic Physically Unclonable Functions (PUFs). The design contains four different memory-based PUFs, one of which is a novel buskeeper PUF, and two different delay-based PUFs. Test chips are fabricated in 65 nm Low Power (LP) technology, using a standard cell ASIC design flow for the memory-based PUFs and a full custom flow for the delay-based ones. This test vehicle enables a comprehensive experimental evaluation of individual PUF implementations as well as a comparative analysis across different PUF types for the same silicon technology. PUF responses are obtained from 192 device samples and the uniqueness and reliability of the implemented PUFs are evaluated. In addition, the effects of varying temperature and silicon device ageing on the PUF characteristics are extensively studied.**

I. Introduction

Secure identification of products has become a crucial issue for many industrial sectors. Threats such as device cloning, hardware tampering and theft of service have surfaced in recent years. In order to combat these threats, it is necessary to develop schemes for unique device authentication and secure storage of cryptographic keys. The emerging technology of Physically Unclonable Functions (PUFs) provides an innovative solution for these issues [5]. A PUF is basically a physical challenge-response procedure such that produced responses depend on the challenge and on the intrinsically unique and random physical variations of the implementing device. Particularly for PUFs implemented in silicon, such device-unique randomness arises naturally from uncontrollable process variations which are abundant in modern deep-submicron CMOS manufacturing technologies. Due to their random nature it is technically impossible, even for the genuine device manufacturer, to physically clone a given PUF or to create a PUF with a given challenge-response behavior.

We present a PUF characterization vehicle implemented in 65 nm low-power CMOS. The six different implemented PUF types are divided in two categories based on their operating principles. The PUF behavior of *memory-based PUFs* arises from the influence of process variations on matched bistable cells, and in this work we study SRAM, Latch, D flip-flop and the newly introduced buskeeper PUFs. *Delay-based PUFs* are based on the impact of process variations on digital circuit delay and we implement ring oscillator and arbiter PUFs. Large-scale analysis of the behavior of these six PUF types is carried out using 192 manufactured chips. PUFs are tested for uniqueness and reliability at different temperatures and under the influence of device ageing.

II. ASIC Architecture

The system-level block diagram of the UNIQUE PUF characterization vehicle is shown in Fig. 1. Six different PUF variants are instantiated with external access for data acquisition, control and status functions provided via a Serial Peripheral Interface (SPI). The minimalistic architecture is driven by the need to minimize design risk while maximizing data acquisition across a wide range of PUF implementations. An active core generates on-chip switching activity to simulate a realistic operating environment, in order to test the sensitivity of some PUF variants to power supply noise generated by switching transients. Operation of the active core is optional. In addition to the core 1.2V power domain a gateable second 1.2V power domain is implemented, providing a coarse-grained power gating capability for a subset of the PUFs. This enables investigation into effects related to the power-up behaviour of selected PUF types. The IO voltage is 2.5V.

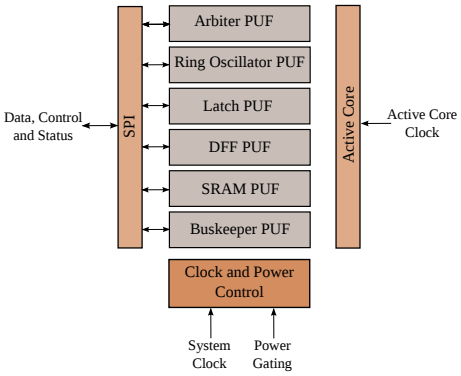

Fig. 1. System block diagram of the test chip.

The device was fabricated in TSMC 65 nm LP CMOS with all 192 samples packaged in LQFP64. Fig. 2 shows the die microphotograph and floorplan of the device with the second, gateable power domain shown as the shaded area. A standard-cell design flow was primarily employed with exceptions for

the arbiter and the ring-oscillator PUFs which partially used a full-custom methodology. Table I lists the area breakdown and PUF composition for each functional unit.

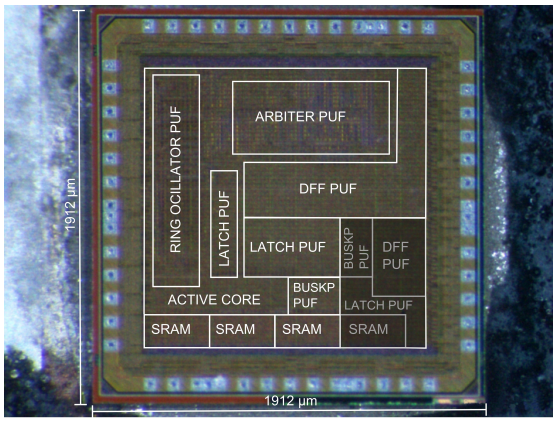

Fig. 2. Die microphotograph of the UNIQUE PUF Characterization Vehicle. The shaded area indicates the separate power domain.

TABLE I
TEST CHIP AREA BREAKDOWN

Functional Unit	Area (mm^2)	PUF Composition
DFF PUF	.392	32768 flip-flops
Active Core	.353	n.a.
Arbiter PUF	.279	256 64-bit arbiters
Latch PUF	.272	32768 latches
Ring Oscillator PUF	.241	4096 inverter chains
SRAM PUF	.213	262144 SRAM cells
Buskeeper PUF	.076	16384 buskeepers

III. MEMORY-BASED PUFS

The device-specific characteristics of memory-based PUFs arise from the positive-feedback loops used to store bits. These loops consist of cross-coupled gates, which ideally are perfectly matched. At power-up the memory state is undetermined; a perfectly balanced loop has an even chance of becoming logic 1 or logic 0. The production process introduces slight variations that unbalance the feedback loops uniquely for each cell. The start-up state therefore becomes device-specific.

A. SRAM PUFs

The characterization vehicle contains four TSMC 2048x32 6T SRAMs, one of which is power gated. By design each SRAM cell contains a feedback loop consisting of two cross-coupled inverters, allowing these SRAMs to produce 262144 PUF bits. Since SRAM includes read-logic and is integrated as a whole, it requires almost no engineering effort. Furthermore SRAM is highly optimized in respect to area and power. The SRAM PUF was introduced by Guajardo et al. in 2007 [2].

B. Buskeeper PUFs

Two groups of buskeepers are incorporated in the design, one of which is power gated. Each group consists of 8192 buskeepers and addressing logic that enables addressing per 32-bit word. The buskeeper or busholder cell is available in standard cell libraries. Like the SRAM cell, the buskeeper contains a feed-back loop of two cross-coupled inverters. Unlike the SRAM cell it does not contain any write logic; this and the low drive strength result in a very area efficient PUF implementation. The buskeeper PUF was introduced by Simons et al. in 2012 [6], the first ever implementation is within this characterization vehicle.

C. Latch PUFs

Four groups of 8192 standard-cell latches are implemented on the experimental chip, of which one is power gated. Latch groups 0 and 1 use MUX-based addressing and groups 2 and 3 are read using scan chains in an attempt to reduce addressing logic. The PUF behavior of a latch is also caused by an internal feedback loop with matched devices. The concept of a latch PUF was introduced by Su et al. in 2007 [7]

D. D Flip-Flop (DFF) PUFs

The characterization vehicle contains four groups of D flip-flops, one of which is power gated. Each group consists of 8192 flip-flops and addressing logic. Each D flip-flop contains two latches, one of which determines the PUF behavior. Flip-flops are available in standard cell libraries. While flip-flops require more area than buskeepers or latches, it is easier to reuse them for other storage purposes. Like for the Latch PUFs, groups 0 and 1 use MUX-based addressing and groups 2 and 3 are read using scan chains. The flip-flop PUF was introduced by Maes et al. in 2008 [4].

IV. DELAY-BASED PUFS

A. Arbiter PUFs

The operation of the arbiter PUF is based on the fact that digital pulses propagating simultaneously through two identical paths will experience different delays due to process variations. The PUF's structure consists of serially connected delay elements forming two delay paths, and an *arbiter circuit* at the end which is used to determine the faster path. Delay elements have two path inputs and two path outputs and a single challenge bit parameter determines its configuration; for a '0' challenge bit, the path inputs are mapped straight to the outputs, and for a '1', the inputs are swapped. The arbiter PUF was initially proposed by Lee et al. in 2004 [3].

The presented arbiter PUF implementation consists of 64 MUX-based chained delay elements, with each 64-bit challenge corresponding to a different configuration of the delay paths. A NAND-latch with symmetrical circuit topology is used as an arbiter to minimize metastability effects and arbiter bias. 256 instances of this 64-bit arbiter PUF are placed on the IC. A full custom layout is used to ensure that circuit delay differences are caused by random process variations rather than by deterministic routing bias or structural circuit asymmetry of standard cells. Delay elements have a symmetrical layout and capacitive loads of the connecting wires are balanced.

B. Ring Oscillator PUFs

Ring oscillator PUFs measure random *frequency* variations on identical ring oscillators. A basic ring oscillator is implemented as a chained loop of an odd number of inverters. One inverter is replaced by a NAND-gate to control the oscillation. Multiple hard-macro copies of a single fixed inverter chain are instantiated to ensure identical nominal frequencies. Each oscillator consists of 40 inverters + 1 NAND-gate.

To evaluate the ring oscillator PUF, two oscillators are enabled simultaneously and fed to two toggle counters which are enabled for a fixed period. The counter values are compared and a single response bit is generated based on the outcome. Since both oscillators have the same nominal frequency, the observed counter value difference results from process variations and noise. The basic concept of a ring oscillator PUF as used in our tests was proposed by Suh et al. in 2007 [8].

Obvious correlations in response bits can occur, e.g. if oscillator A is faster than oscillator B, and B is faster than C, it is apparent that A will also be faster than C and the resulting response bit can be accurately predicted. To avoid predictable responses, only neighbouring oscillators are compared, e.g. oscillators A and C are never compared. The presented ring oscillator PUF implementation contains 4096 instantiations of the hard-macro oscillator, arranged in 256 rows and 16 columns, with one toggle counter per column. Oscillators in the same row are measured simultaneously, hence 256×(16-1) = 3840 response bits are evaluated in this manner.

V. Test Results

This section provides an overview of different tests that have been performed on the PUFs in this IC to evaluate their reliability and uniqueness. PUF responses are susceptible to environmental variations and will change over time due to noise and device ageing. Therefore, it is important to evaluate PUF reliability under different circumstances as well as over time. Besides reliability, it is also important that PUFs are unique. This means that it should be possible to uniquely identify different PUFs without confusing their intrinsic electronic fingerprints. In other words, responses from different PUFs should be significantly different from each other. These PUF properties are studied in the following two tests.

A. Temperature Cycle Test

To test the reliability of different PUFs at varying ambient temperatures, all 192 ICs have been placed in a climate chamber. Measurements of PUF responses are obtained at three different temperatures: -40^{o}C, +25^{o}C, and +85^{o}C (industrial standard for temperature testing of ICs ranges from -40^{o}C to +85^{o}C). For this test all measurements are compared to a reference measurement at +25^{o}C using fractional Hamming Distance (FHD)[1]. Table II shows the results of the Temperature Cycle Test for all included PUF types. When interpreting the results, one must take the following into account:

[1]Hamming Distance (HD) is defined as the number of bits that differ between two bit strings. In case of fractional Hamming Distance (FHD) the HD is divided by the length of the compared strings.

TABLE II
Temperature Cycle Test results; min. and max. FHD compared to reference per PUF (incl. uniqueness results)

PUF Type	Meas. Data (instances x nr. of bits)	FHD (noise) -40^{o}C min	-40^{o}C max	+25^{o}C min	+25^{o}C max	+85^{o}C min	+85^{o}C max	BCFHD (uniq.) mean
SRAM	4 x 65536	7.0%	8.0%	5.0%	6.0%	6.5%	8.0%	49.7%
Bus-keeper	2 x 8192	8.0%	11.0%	3.0%	4.5%	15.5%	20.5%	49.1%
Latch	2 x 8192	15.0%	28.0%	2.5%	3.5%	8.0%	18.0%	36.9%
DFF (#0,2,3)	3 x 8192	10.0%	17.0%	3.0%	4.0%	16.0%	21.0%	41.8%
DFF (#1)	1 x 8192	10.0%	33.0%	3.0%	10.0%	12.0%	24.0%	41.8%
Arbiter	1 x 8192	3.0%	4.5%	2.5%	4.0%	2.5%	4.5%	47.3%
Ring Osc.	1 x 3840	1.6%	3.9%	0.6%	2.8%	1.4%	3.9%	49.5%

- The two latch PUF instances with scan chain addressing are not part of these results. The data was not usable due to problems with the implemented read-out circuitry.
- DFF PUF instance 1 (with mux tree addressing) exhibits a significantly reduced reliability. Therefore, we consider this instance separately from the other DFF PUFs in Tables II and III. Finding the reason for this reduced reliability will be future work.

From Table II it is clear that the FHD increases when the temperature deviates from the reference temperature. This is a well-known phenomenon for PUFs. In PUF-based security systems, this is resolved by using error correction techniques in order to reconstruct the reference pattern. This error correction becomes more complex when noise levels get higher, hence a low FHD at extreme temperatures is a valuable asset for a PUF. Based on the results from the table, it can be concluded that the performance of SRAM, arbiter and ring oscillator PUFs are hardly influenced by temperature variations.

The other important property of PUFs that has been evaluated in this test is uniqueness. For this the FHDs between the reference measurements of different PUF instances were calculated. When two PUFs are unique and independent, their "between-class" FHD (BCFHD) should be close to 50%. Collecting all BCFHDs of a PUF type results in a distribution, which can be fitted to a Gaussian. Based on the distribution mean, the correlation between PUFs from different devices can be assessed. For an indication of low correlation (hence unique patterns), the mean should be close to 50%. From the results in Table II it is clear that both the Latch and the D Flip-Flop PUFs perform suboptimally regarding uniqueness. On the other hand, the SRAM and ring oscillators show the highest uniqueness of the evaluated PUF types.

B. Ageing Test

The main failure mechanism that causes memory-based PUF responses to change over time is NBTI (Negative Bias Temperature Instability). This mechanism is accelerated in our

TABLE III

AGEING TEST RESULTS; MIN. AND MAX. FHD COMPARED TO REFERENCE PER PUF FOR 5 ICS (INCL. RESULTS FROM SEPARATE POWER DOMAIN)

PUF Type	Before Ageing		After Ageing ($\sim$ 4.5 years)		After Ageing Separate P.D.	
	min	max	min	max	min	max
SRAM	5.0%	5.5%	7.0%	8.0%	5.5%	5.5%
Bus-keeper	3.5%	5.0%	5.5%	7.0%	3.5%	5.0%
Latch	2.0%	3.0%	5.0%	6.0%	2.5%	3.5%
DFF (#0,2,3)	2.5%	4.0%	4.5%	6.0%	3.5%	4.0%
DFF (#1)	3.5%	7.0%	4.0%	12.0%	n.a.	n.a.
Arbiter	2.5%	3.5%	3.0%	4.5%	n.a.	n.a.
Ring Osc.	0.9%	2.3%	3.4%	4.8%	n.a.	n.a.

ageing test by keeping 5 ICs under high voltage (120% of Vdd = 1.44V) and temperature conditions (+85^{o}C). The total estimated acceleration factor [1] is the product of the Thermal Acceleration Factor (TAF) and the Voltage Acceleration Factor (VAF), which are computed as:

$$\text{TAF} = e^{\frac{E_a}{k}(\frac{1}{T_{op}} - \frac{1}{T_{stress}})} \text{ and } \text{VAF} = e^{\gamma(V_{stress} - V_{op})}$$

With E_a (0.5 eV) the activation energy, k (8,62$\cdot 10^{-5}$ eV/^{o}K) Boltzmann's constant, T_{op} (313^{o}K (+40^{o}C)) the nominal operating temperature, T_{stress} (358^{o}K (+85^{o}C)) the stressed temperature, γ (2.6) the voltage exponent factor, V_{op} (1.2V) the nominal core voltage and V_{stress} (1.44V) the stressed core voltage. This results in a total estimated acceleration factor of TAF$\times$VAF = 10.27$\times$1.77 = 18.2.

Every week the ambient temperature and supply voltage were lowered to +25^{o}C and 1.2V respectively to measure the PUF responses. After these measurements, the temperature and voltage were increased again to stress levels. Prior to starting the ageing test one reference measurement per PUF at +25^{o}C and 1.2V was taken to which all other measurements are compared based on the FHD. The ageing test has run for 2150 hours. With the estimated acceleration factor of 18.2, this simulates an effective ageing of around 53.5 months, or almost 4.5 years. The results in Table III show that within this time frame the ageing for all PUF types is quite limited. Furthermore, the last column of this table displays the results for the memory-based PUFs that are located in the separate power domain of the IC. This domain was not powered during the stress conditions and was therefore only used when performing PUF measurements at +25^{o}C. The results from this column clearly show that the (minimal) ageing effect occurring on the memory-based PUFs can be diminished by powering down memories when not using them for PUF purposes. Keep in mind that this ageing test was designed specifically for memory-based PUFs, which might explain the relatively minor impact on the delay-based PUFs.

VI. CONCLUSIONS

In this work, six different types of intrinsic PUFs are characterized through an extensive experimental study on 192 test chip samples in 65 nm CMOS. The following memory-based PUF types were implemented on every test chip: four 64 kbit SRAM PUFs, four 8 kbit Latch PUFs, four 8 kbit D flip-flop PUFs and two 8 kbit Buskeeper PUFs. In addition each test chip contains two different types of delay-based PUFs: 256 Arbiter PUFs with 64-bit challenges and a Ring Oscillator PUF containing 4096 inverter rings. Extensive measurements from all PUF instances on all test chips were obtained at different temperatures: -40^{o}C, +25^{o}C and +85^{o}C. Moreover, five chips were exposed to an accelerated ageing process ($\sim$ 4.5 years) to study the effect of silicon ageing (NBTI) on the PUFs.

Our test results show that SRAM PUFs and both delay-based PUFs show good PUF behavior, with high reliability (less than 10% noise at corner cases and after ageing) and high uniqueness (very close to 50%). To fully assess the practical value of each PUF type, other parameters such as area efficiency and unpredictability need to be taken into account. This will form the subject of future work.

ACKNOWLEDGMENT

This work has been supported by the E.C. through the FP7 programme under contract 238811 "UNIQUE". The authors thank all project partners who have contributed to the design and production of the ASICs and test boards. Besides partners from the UNIQUE project, the authors would also like to thank IMEC and Europractice. IMEC design services has performed the back-end design for the described ASIC and Europractice has been responsible for facilitating the ASIC production.

REFERENCES

[1] Altera. Reliability report 52 q3 2011. http://www.altera.com/literature/rr/rr.pdf.

[2] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls. FPGA intrinsic PUFs and their use for IP protection. In *Workshop on Cryptographic Hardware and Embedded Systems*, pages 63–80, 2007.

[3] Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh, Marten van Dijk, and Srinivas Devadas. A technique to build a secret key in integrated circuits for identification and authentication application. In *Symposium on VLSI Circuits*, pages 176–159, 2004.

[4] Roel Maes, Pim Tuyls, and Ingrid Verbauwhede. Intrinsic PUFs from flip-flops on reconfigurable devices. In *Workshop on Information and System Security*, 2008.

[5] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security*, Information Security and Cryptography, pages 3–37. Springer, Heidelberg, 2010.

[6] Peter Simons, Erik van der Sluis, and Vincent van der Leest. Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs. In *IEEE Int. Symposium on Hardware-Oriented Security and Trust*, 2012.

[7] Y. Su, J. Holleman, and B. Otis. A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations. In *IEEE Int. Solid-State Circuits Conference*, pages 406–611, Feb. 2007.

[8] G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Design Automation Conference*, pages 9–14, 2007.