D3.3 Evaluation report

Project number:	238811
Project acronym:	**UNIQUE**
Project title:	Foundations for Forgery-Resistant Security Hardware
Start date of the project:	01.09.2009
Duration:	33 months

Deliverable type:	Report
Deliverable reference number:	238811/ D3.3 / 2.0
Deliverable title:	Evaluation report
WP contributing to the deliverable:	WP3
Due date:	2012-05-31 (M33)
Actual submission date:	2012-06-22 (M34)

Responsible organisation:	Thales Communications & Security (TCS)
Authors:	TCS (Jérôme Quévremont, Jean-Christophe Courrège, Jérôme Di Battista, Rémy Chau) IID (Vincent van der Leest, Peter Simons) INTEL (Patrick Koeberl) TUD (Christian Wachsmann, Ünal Kocabas) KUL (Roel Maes) SIRRIX (Timm Korte, Wolfgang Meyer zu Bergsten)
Abstract:	This document describes the security functions evaluations of the FPGA and ASIC applications in respect to behavioural validations, side channel and fault attacks.
Keywords:	PUF, tests, security evaluation, attacks

Dissemination level:	Public
Revision:	2.0
Instrument:	STREP
Thematic Priority:	ICT

Table of Contents

1 Introduction 7
1.1 Scope of document 7
1.2 Document overview 7
2 Test environment 8
2.1 Test environment for PUF characterization 8
2.1.1 ASIC board 8
2.1.2 FPGA board 9
2.1.3 Additional components 9
2.2 Test environment for security evaluation 10
2.2.1 ASIC board 10
2.2.2 FPGA board 10
2.2.3 Side Channel Analysis 11
2.2.4 Hamamatsu TriPHEMOS 11
2.2.5 Fault injection / perturbation 11
2.2.6 Additional components 12
3 Low-level functional tests 13
3.1 Low-level functional test description 13
3.1.1 Serial Peripheral Interface 13
3.1.2 Active Core 13
3.1.3 SRAM PUF 14
3.1.4 Latch PUF 15
3.1.5 DFF PUF 16
3.1.6 Buskeeper PUF 17
3.1.7 Ring Oscillator PUF 17
3.1.8 Arbiter PUF 18
3.2 Low-level functional test results 18
3.3 PUF self-test prototype 19
4 PUF characterization 21
4.1 Reliability test description 21
4.2 PUFs aging evaluation 22
4.3 PUFs robustness evaluation 24
4.3.1 Strategy 24
4.3.2 Results 25
4.4 PUFs unpredictability evaluation 27
4.4.1 Strategy 28
4.4.2 Entropy estimation 30
4.4.3 Results 31
4.5 Buskeeper PUF robustness and unpredictability 37
4.5.1 Robustness evaluation 37

4.5.2 Unpredictability evaluation 39
5 Security evaluation 43
5.1 Reverse Engineering 43
5.1.1 Package visual inspection 43
5.1.2 Cross section by FIB 43
5.1.3 Deprocessing 46
5.1.3.1 M8 layer 47
5.1.3.2 M7 layer 49
5.1.3.3 Next metal layers 51
5.1.3.4 Poly and active layers 52
5.1.4 Reverse of SRAM cells 57
5.1.5 Conclusions 59
5.2 PUF tamper evidence 59
5.2.1 Package opening 59
5.2.1.1 Frontside opening 60
5.2.1.2 Backside Opening 60
5.2.1.3 Backside Fib ultimate thinning 64
5.2.1.3.1 FIB ultimate thinning on the RING 64
5.2.1.3.2 FIB ultimate thinning on the SRAM2 67
5.2.1.3.3 FIB ultimate thinning on the LATCH 70
5.2.1.4 Test point deposition on a contact (RING zone) 72
5.3 Side channel analysis 73
5.3.1 General Observation 73
5.3.2 Ring Oscillator based PUF characterization 75
5.4 Light Emission Analysis 77
5.4.1 General activity 77
5.4.2 SRAM PUF activity 78
5.4.3 Ring Oscillator PUF activity 79
5.5 Fault Injection 81
5.5.1 Preliminary test 81
5.5.2 SRAM PUF 81
5.5.3 Ring Oscillator PUF 82
5.6 High temperature testing 83
6 Conclusion 87
7 References 89
8 Glossary 90

List of Tables

Table 1: SRAM PUF test scenario 14
Table 2: Latch PUF architecture and features 15
Table 3: Latch PUF test scenario 15
Table 4: Latch PUF architecture and features 16
Table 5: DFF PUF test scenario 16
Table 6: Buskeeper PUF test scenario 17
Table 7: Ring Oscillator PUF test scenario 17
Table 8: Arbiter PUF test scenario 18
Table 9: Low-level functional test results 19
Table 10: Description of Reliability Tests 21
Table 11: Number of ASICs and PUF types evaluated during each test 22
Table 12: Ageing test results; Min. and Max. FHD compared to reference per PUF for 5 ASICs (incl. results from separate power domain) 23
Table 13: Robustness test cases 24
Table 14: Unpredictability test cases 29
Table 15: CWT compression results 33
Table 16: Results of CTW compression test 40
Table 17: Comparison of PUF reading before and after backside opening and thinning at 25 µm 62
Table 18: Comparison of PUF reading before and after backside opening and thinning at 50 µm 63
Table 19: Comparison of RO PUF reading before and after FIB ultimate thinning 67
Table 20: Comparison of PUF response before and after backside opening and thinning at 50 µm 69
Table 21 : SPA trace of each PUF response during the communication process 74
Table 22: RO PUF light emission activity - RO position 80
Table 23: Comparison of RO PUF at 25°C and 125°C 84
Table 24: Comparison of Latch PUF at 25°C and 125°C 86

List of Figures

Figure 1: PUF self-test sequence 20
Figure 2: Distribution of the bit error rate (BER) over all PUF instances 27
Figure 3: Distribution of Hamming weight over all PUF instances 32
Figure 4: Distribution of the entropy and min-entropy over all PUF instances 35
Figure 5: Distribution of the Hamming distance over all PUF instances 36
Figure 6: Measurement results from Temperature Variation Test 38
Figure 7: Measurement results from Voltage Variation Test at +25°C 39

Figure 8: Hamming Distance distribution of enrollment data Temperature Variation Test 40
Figure 9: Min-entropy development over the number of enrollment files (m) 42
Figure 10: Package top view 43
Figure 11: Package after front side decapsulation. 43
Figure 12: FIB cross-section in SRAM array. 9 Cu layers in this area. 44
Figure 13: Zoom on transistor gates. Gate width is measured around ≈65nm. 45
Figure 14: ASIC general view trough passivation layer (M10 and M9 layers are visible). 46
Figure 15: Pad level (M10 layer in Al) 47
Figure 16: SRAM cells (M9 layer in Cu). Cross-section axis. 47
Figure 17: ASIC general view at M8 level 48
Figure 18:Ring oscillator Power line and some active signal lines (thinner ones) 48
Figure 19:SRAM cells Only power lines and metal filling 48
Figure 20: ASIC general view at M7 level 49
Figure 21:Ring oscillator 49
Figure 22:SRAM cells only metal filling and via for power distribution 49
Figure 23: Ring oscillator. Useful lines at M7 layer. 50
Figure 24: SRAM cells. Metal fills at M7 layer above SRAM cells. 51
Figure 25 : ASIC general view at Poly layer. Functional block identification. 53
Figure 26: Floor plan 53
Figure 27: Latch cell 54
Figure 28: Ring Oscillator. Succession of inverters (one inverter = one PMOS + one NMOS) 54
Figure 29: Flip-Flop cell 55
Figure 30: SRAM cell. Standard 6 transistors cell (see reverse in next paragraph). 55
Figure 31: Bus keeper 56
Figure 32: Arbiter. 12 transistors per cell (6 PMOS + 6 NMOS) 56
Figure 33: Active Core 57
Figure 34: Reverse engineering of SRAM cells. Identification of transistors and active areas 58
Figure 35: Deduced design of SRAM cells 58
Figure 36: Package top view 60
Figure 37: Package after front side decapsulation. (No more Cu wires) 60
Figure 38: RX image for backside opening localisation 61
Figure 39: Package after backside opening. 61
Figure 40: Floor plan ASIC for FIB box localisation 64
Figure 41: Backside laser image for FIB box localisation 64
Figure 42 : FIB image of the 200µm*200µm Si surface on the ring 65

Figure 43 : FIB optical image of same zone: 1000nm filter allows to see by transparency the structure of the ring....65
Figure 44 : FIB image of the 200µm*200µm Si surface of the ring (structure appears)66
Figure 45 : FIB optical image of same zone :500nm filter allows to see by transparency the structure of the ring....66
Figure 46 : FIB image of the ring ultimate thinning after oxide deposition....66
Figure 47 : Optical FIB image of the ring ultimate thinning 66
Figure 48 : Floor plan ASIC for FIB box localisation....68
Figure 49 : Backside laser image for FIB box localisation 68
Figure 50 : FIB image of the 200µm*200µm Si surface of theSRAM2 68
Figure 51 : FIB optical image of same zone: 1000 nm filter allows to see by transparency the structure of the ring....68
Figure 52 : FIB image of the SRAM2 ultimate thinning after oxide deposition 69
Figure 53 : Optical FIB image of the SRAM2 ultimate thinning 69
Figure 54 : Floor plan ASIC for FIB box localisation....70
Figure 55 : Backside laser image for FIB box localisation 70
Figure 56 : FIB image of the 100µm*100µm Si surface of the LATCH....71
Figure 57 : FIB optical image of same zone: 1000 nm filter does not allow the structure of latch to be observed because of the structure size much smaller than used wavelength. 71
Figure 58 : FIB image of the LATCH ultimate thinning after oxide deposition....71
Figure 59 : Optical FIB image of the SRAM2 ultimate thinning 71
Figure 60 : FIB image of the LATCH ultimate thinning after oxide deposition....72
Figure 61 : Si opening on active structures 72
Figure 62 : FIB trench on the RING....72
Figure 63 : Opening trough Si to active structures 72
Figure 64: Ring Oscillator PUF response without Active Core 73
Figure 65: Ring Oscillator PUF response with Active Core....74
Figure 66 : EMA - Ring Oscillator PUF EM emanation (with AC)....76
Figure 67 : EMA - Ring Oscillator PUF EM emanation 76
Figure 68: Backside laser imaging compare to ASIC floor plan (D2.2 – 5.6) 77
Figure 69: Reference light emission activity (AC core ON)....78
Figure 70: SRAM PUF light emission activity (with AC core ON) 79
Figure 71 : Fault injection on SRAM3 81
Figure 72 : Fault injection on SRAM2 during SRAM dump....82
Figure 73 : Fault injection on RO 83
Figure 74 : RO variations over temperature 85

1 Introduction

1.1 Scope of document

This deliverable presents the test scenarios and the test results within the framework of security evaluation of FPGA and ASIC applications with respect to behavioural validations, side channel and fault attacks. The security evaluation is based on the new methodologies introduced in document D3.1.

For more consistency, behavioural validations are described in the deliverable D4.3 Test performance and results.

1.2 Document overview

This document describes in section 2 the test environment used to perform the PUF characterization and the PUF security evaluation. The first tests done on the UNIQUE chips are the low-level functional tests of section 3 which ensure that the basic ASIC functionalities are operational. With fully functional chips, PUF evaluations can start. PUF assessment is composed of two main components which are PUF data analysis and PUF security evaluation. Section 4.2 describes the PUF response behaviour in aging conditions while sections 4.3 and 4.4 describe the robustness and the unpredictability of PUF responses except for Buskeeper PUF. Indeed, as the Buskeeper PUF assessment is issued from an independent study, those results are presented separately in the section 4.5 of this evaluation report. Finally, section 5 describes the security evaluation campaign which is the PUF resistance assessment against different attack types.

2 Test environment

2.1 Test environment for PUF characterization

The test environment for the PUF characterization tests (as described Section 4 PUF characterization) comprises:

- a board with sockets for the UNIQUE ASIC (physical part of the PUF)
- an FPGA board with firmware for reading out PUF data
- additional components (such as host PC, climate chamber, …)

2.1.1 ASIC board

An ASIC board has been designed by the UNIQUE partners in order to facilitate both the PUF characterization tests as well as security testing. This board has been designed by following the requirements as listed in this section.

Geometrical requirements for the security analysis:

Several requirements have been taken into account during the development of the ASIC board in order to facilitate penetration testing.

Form factor requirements:

- Open-top ASIC socket to support front-side analysis
- Several (preferably 5) sockets on board for testing multiple ASICs at once, board should be functional if only a subset of sockets is populated.
- In order to make back side analysis possible, the board is opened behind the central ASIC position so that it is possible to observe the component during operation.
- The central position supports both socket insertion or direct ASIC soldering in order to limit the working distance for optical analysis
- Direct access to ASIC power lines for side channel analysis
- Large clearance (15 cm diameter) on the top of the board for extreme temperature testing (using heater head)

Connectors and Sockets:

- Connection between ASIC and FPGA-board via Ribbon-Cable
- SMA differential sockets for external clocking options
- Test pads and ground connectors at convenient locations

Power Budget:

- Estimated at 52mW @ 33MHz per ASIC
- Factors for temp/clock variations up to x6

Power supply:

- ASIC: VDD=1.2V, VDD_OFF=1.2V, VDD_PST=2.5V should be derived from FPGA supplied voltages (3.3V and 5V)
- Design should support side channel analysis
- Both VDD and VDD_OFF should be controllable by incoming connector signals
- Core supplies should lag IO-supplies by >= 1us

Clock generation:

- ASIC core clock @ 33MHz, ASIC active core clock @ 33 MHz – 65 MHz
- Clocking selectable by jumper (either onboard or supplied externally via differential SMA sockets)

Other:

- ASIC scan chain support, all test signals from at least one socket routed to the board connector
- Board should support operating temperatures from -40°C to +125°C

More details about the ASIC board can be found in UNIQUE deliverable D2.2.

2.1.2 FPGA board

For the PUF characterization tests the following FPGA board has been connected to the UNIQUE ASIC board: **Virtex-5 LX50 Evaluation Board** (Supplier: Avnet).

Additional hardware: Cable from QSE connector (JX1 on LX50 board) to ASIC board connector (P1/P2).

Only the direct access functionality (as described in UNIQUE deliverable D4.2) is used on the Xilinx LX50 board. The demo FPGA functionality of the UNIQUE use cases has been removed to prevent that pins are used that have a different function on the LX50 board compared to the ML501 board used for the UNIQUE prototype (as described in D4.2).

2.1.3 Additional components

In order to perform the PUF characterization tests as described in section **4**, the following additional components have been used:

- Climate chamber (Espec type SH-641), which has been used to perform PUF measurements at different temperatures. The temperature range has been varied from -40°C to +85°C.

- Programmable power supply (Agilent type E3631A), which has been used to apply different supply voltages to the UNIQUE ASIC when performing PUF measurements.
- Programmable function generator (Agilent type 33250A), which has been used to create different voltage ramp-up times when powering the UNIQUE ASIC.
- Amplifier (Philips type EOG20), which has been used to amplify the signal from the function generator in order to provide sufficient current for the UNIQUE ASIC.
- Host PC, which has been connected to FPGA board in order to receive the PUF measurement data. This data has been stored by the PC in binary files (one file per measurement per PUF instance).

2.2 Test environment for security evaluation

The test environment for the security evaluation tests (as described Section 5 security evaluation) comprises:

- a board with sockets for the UNIQUE ASIC (physical part of the PUF).
- an FPGA board with a Microblaze implementation and firmware for reading out PUF data.
- Hamamatsu TriPHEMOS equipment for light emission measurement.
- Power and electromagnetic measurement bench for SPA and EMA analysis.
- Laser test bench for fault injection.
- Additional components for the different step of the evaluation.

2.2.1 ASIC board

An ASIC board has been designed by the UNIQUE partners in order to facilitate both the PUF tests as well as security testing. This board has been designed by following the requirements as listed in section 2.1.1.

More details about the ASIC board can be found in UNIQUE deliverable D2.2.

2.2.2 FPGA board

For the PUF characterization tests the following FPGA board has been connected to the UNIQUE ASIC board: **Virtex-5 LX50 Evaluation Board** (Supplier: Avnet).

The Microblaze implementation (as described on the UNIQUE svn database WP4_Prototype/Microblaze_driver) is used on the Xilinx LX50 board. A specific C code is developed on Xilinx SDK platform (using the library provided by KUL partner as described in Unique_microblaze_driver_manual.pdf) in order to test all PUF functions.

2.2.3 Side Channel Analysis

A Power test bench equipped with a current probe and an acquisition system (oscilloscope+computer) has been used to perform SPA analysis. The power consumption curves analysis was then processed by a specific software.

An Electromagnetic test bench equipped with an electromagnetic sensor and an acquisition system (oscilloscope+computer) has been used to perform EMA analysis. The electromagnetic curves were then processed by a specific software developed by TCS.

These tests will consist in analysing/observing the current consumption and/or electromagnetic emanation of each PUF to see if they present any significant signature.

2.2.4 Hamamatsu TriPHEMOS

A Hamamatsu TriPHEMOS has been used to perform both static and dynamic light emission measurements. This equipment is composed of an InGaAs camera (high infrared sensitivity in the 950 nm to 1400 nm) coupled with a photon counting system. The optical sensor of the InGaAs camera (resolution of 640x480 with a pixel size of 20um x 20um) associated with a Solid Immersion Lens (SIL) supports a resolution of 300nm enabling structures in 65 nm technology to be observed. This equipment is able to capture the light emitted by the transistors during switching events in order to visualize the behavior of a circuit (or a PUF function).

2.2.5 Fault injection / perturbation

A pulse laser test bench injection permits setting or resetting of memory nodes. This technique can permit the retrieval of the initial value of a PUF if an attacker is able to independently set or reset each of the memory cells involved in the PUF. On the other hand fault injection techniques can be used in order to modify/characterize ring oscillator frequencies and as a result change the normal behaviour of RO based PUFs.

The continuous wave laser used is the Meridian 1 acquisition system from DCG Systems, equipped with a laser scanning microscope system (LSM) with two different lasers for induced current and thermal stimulation (1064 nm and 1340 nm). This technique is able to perturb cells in order to observe the effect on PUF functions (SRAM, RO…).

2.2.6 Additional components

In order to perform the PUF security evaluation as described in section 5, the following additional components have been used:

- To perform a partial reverse engineering : chemical products (acid H3PO4 + HF) has been used for delayering, a plasma device has been used to remove the oxide layer interlevel dielectric, a microscope to perform optical observation, and an SEM (scanning electron microscope) to perform a surface topography.
- Sesame acid 770 CU which has been used to perform frontside opening and Ulatratech ASAP for backside opening (plasma for silicon thinning).
- Temperature forcing system (Thermonix T-2500SE), which has been used to perform additional PUF measurements at extreme temperatures. The temperature range has been varied from -90°C to +220°C.
- Host PC, which has been connected to FPGA board in order to receive the PUF measurement data and control the FPGA with the Xilinx SDK platform.

3 Low-level functional tests

This section defines low-level functional tests which will form the basis of the post-silicon validation plan. The motivation is to verify the basic ASIC functionality as far as possible in order to establish a baseline before moving onto to other aspects of post-silicon validation such as PUF performance evaluation.

Three main areas of testing are addressed:

1. Datapath correctness
2. Post reset register behaviour
3. Control protocol tests where appropriate

Establishing that the datapaths are correct and reliable is a key element of post-silicon validation. For the Unique ASIC in particular, ensuring that the inherently noisy PUF data returned reflects actual PUF behaviour rather than a datapath artefact is of primary importance.

A number of problems can compromise datapath correctness, ranging from pre-silicon verification gaps to implementation issues such as reduced signal integrity. As an example of one verification gap in UNIQUE, the simulation and the implementation database configurations differed, with the former being a scaled down version in terms of the number and aspect ratio of the PUF instantiations. The inability to fully simulate power gating events at RTL and gate-level is another.

In addition to the above manufacturing defects such as stuck-faults can be present on any of the 192 ASIC prototypes. Although a scan-based test methodology was used on the ASIC, appropriate test patterns where not generated or applied. As a result stuck-at faults may be present on any ASIC sample and unless steps are taken to detect these can remain undetected and influence subsequent PUF characterization.

For the initial ASIC bring-up process the intention is to execute these tests at room temperature and at nominal core and IO supply voltages. The tests can also form the foundation for subsequent validation tasks (security, reliability and higher-level functional tests) and also provide low-level chip diagnostics.

3.1 Low-level functional test description

3.1.1 Serial Peripheral Interface

Loopback mode in the SPI interface is enabled and loopback tests performed to validate the interface.

3.1.2 Active Core

The active core clock is applied and active core monitor pin observed to check activity.

3.1.3 SRAM PUF

Four 8 KB SRAM instances are instantiated, SRAM Array 0-3. SRAM Array 0 is placed in a separate power-domain which can be dynamically gated.

The following tests are specified:

Table 1: SRAM PUF test scenario

Test Number	Description
1	Read complete SRAM contents from each instance. Verify that each SRAM instance has a unique signature. Repeat to verify each signature is stable (per ASIC power-up). SRAM PUF signatures will differ across power-up cycles; this test should be designed with this in mind.
2	Verify each addressable SRAM location is read/write with no side-effects on other locations.
3	Perform classic 'checkerboard' SRAM test on each instance.
4	Power gating test. Gate power off and repeat Test 1,2 and 3. SRAM Array 0 should be inaccessible. Gate power on and repeat Test 1, 2 and 3.

3.1.4 Latch PUF

Four latch arrays of 8 Kb are instantiated. These four arrays have different features as shown in the table below. Two read architectures are used, one based on multiplexers, the other serial. The serial architecture has enable isolation employed on one instance. The multiplexer architecture has power gating employed on one instance. Note that the latch PUFs are read-only and that reading Array 2 and 3 will result in subsequent reads being zero.

Table 2: Latch PUF architecture and features

	Architecture	Power Gating	Enable Isolation
Latch Array 0	Multiplexer	Yes	
Latch Array 1	Multiplexer		
Latch Array 2	Serial		
Latch Array 3	Serial		Yes

The following tests are specified:

Table 3: Latch PUF test scenario

Test Number	Description
1	Read complete latch PUF contents from each instance. Verify that each instance has a unique signature. Repeat reads to verify each signature is stable. Verify that the contents of array 2 and 3 are zero after the first read. Latch PUF signatures will differ across power-up cycles, this test should be designed with this in mind.
2	Power gating test. Gate power off and repeat Test 1. Latch Array 0 should be inaccessible. Gate power on and repeat Test 1.

3.1.5 DFF PUF

Four DFF arrays of 8 Kb are instantiated. These four arrays have different features as shown in the table below. Two read architectures are used, one based on multiplexers, the other serial. The serial architecture has enable isolation employed on one instance. The multiplexer architecture has power gating employed on one instance.

Table 4: Latch PUF architecture and features

	Architecture	Power Gating	Enable Isolation
DFF Array 0	Multiplexer	Yes	
DFF Array 1	Multiplexer		
DFF Array 2	Serial		
DFF Array 3	Serial		Yes

The following tests are specified:

Table 5: DFF PUF test scenario

Test Number	Description
1	Read complete DFF PUF contents from each instance. Verify that each instance has a unique signature. Repeat reads to verify each signature is stable. DFF PUF signatures will differ across power-up cycles, this test should be designed with this in mind.
2	Verify each addressable DFF location is read/write with no side-effects on other locations.
3	Perform classic 'checkerboard' test on each instance.
4	Power gating test. Gate power off and repeat Test 1,2 and 3. DFF Array 0 should be inaccessible. Gate power on and repeat Test 1, 2 and 3.

3.1.6 Buskeeper PUF

Two buskeeper arrays of 8 Kb are instantiated. These are read-only. The following tests are specified:

Table 6: Buskeeper PUF test scenario

Test Number	Description
1	Read complete buskeeper PUF contents from each instance. Verify that each instance has a unique signature. Repeat reads to verify each signature is stable. Buskeeper PUF signatures will differ across power-up cycles, this test should be designed with this in mind.

3.1.7 Ring Oscillator PUF

The RO Oscillator PUF instantiates 4096 oscillators. The following tests are specified:

Table 7: Ring Oscillator PUF test scenario

Test Number	Description
1	Verify all control and status registers have expected post-reset values: RO Control RO Status RO Reference Counter RO Select Batch
2	Full data-width read/write test on the following registers: RO Select Batch RO Reference Counter
3	Set reference counter and enable oscillators. Test RO read protocol (issue start / poll for status) on each oscillator in each batch. Verify each RO result is non-zero.

3.1.8 Arbiter PUF

The arbiter PUF instantiates 256 arbiters arranged in 8 groups of 32. The 32-bit read datapath supports reading 32 arbiters in parallel. A 64-bit challenge can be applied on a per-group basis. The following tests are specified:

Table 8: Arbiter PUF test scenario

Test Number	Description
1	Verify all control and status registers have expected post-reset values: Arbiter Control Arbiter Status Arbiter Challenge Arbiter Enable
2	Full data-width read/write test on the following registers: Arbiter Challenge Arbiter Enable
3	Test Arbiter read protocol (issue start / poll for status) on each arbiter. Verify arbiter result is not all-zeros or all-ones.

3.2 Low-level functional test results

Functional testing of the UNIQUE ASICs has resulted in the following bug sightings:

Table 9: Low-level functional test results

Bug Sighting	Description	Workaround
Invalid Arbiter Status	Busy bit in the arbiter status register is set to '0' after a hard reset which indicates busy.	Ensure any software polling the status bit ignores for the first operation after hard reset.
Partial Arbiter Reset	Three flops in a 4-bit arbiter counter (proc_ctrl_cnt) are not connected to the global synchronous reset 'arst_n_net' .	Flops are cleared down by the datapath after the first operation. Ignore results from first arbiter access.
Ring Oscillator Hang	Setting the reference counter to certain values causes a hang (e.g. 0x00001000). Believed to be due to the RO counter implementation (toggle architecture).	Depending on the magnitude of the reference counter value, one or more of the LSBs of this value should always be set to '1': 1) The first most LSB should always be '1' (e.g. 0x00000401) 2) When the reference counter value is larger than 0x00000FFF, the two most LSBs should be '1' (e.g. 0x00002003) 3) When the reference counter value is larger than 0x03FFFFFF, the three most LSBs should be '1' (e.g. 0x10000007).

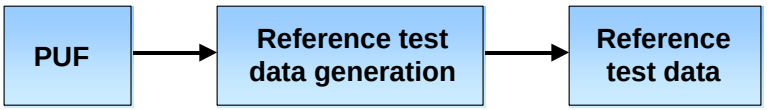
3.3 PUF self-test prototype

In the security domain, chip reliability is a critical requirement. Each physical component can partially or fully deteriorate during the lifecycle due to various causes. This is the reason why high-end cryptographic components shall embed a mechanism assessing the reliability of each function along the lifecycle. The goal is to be able to monitor each failure. An example is the Built-In-Self-Test (BIST) of memories which mainly consists on writing and re-reading patterns in memory cells in order to make sure that the tested memory is still functional. As PUFs are a new technology, no self-test mechanisms have been proposed so far.

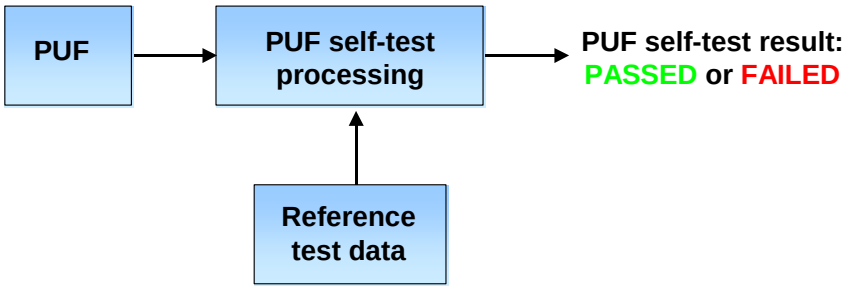
Therefore, a PUF self-test mechanism has been proposed. This mechanism comprises two sequences: measuring the reference data (which will permit to reconcile PUF information) once then checking the next measurements online against the reference data. The result is binary: passed or failed. This sequence is illustrated in Figure 1.

Figure 1: PUF self-test sequence

Phase 1: initial measurement



Phase 2: online PUF self-test



An example of PUF self-test has been implemented in a prototype using the SRAM PUF embedded in the UNIQUE ASIC and the FPGA board.

The prototype has been validated at ambient temperature on 10 different ASIC samples and both phase 1 and phase 2 of the self-test sequence are functional. The next steps would be to perform these measurements over the whole operational range (temperature, voltage, ASIC from different corner cases…)

4 PUF characterization

4.1 Reliability test description

This section describes the Reliability tests that have been performed within the UNIQUE project. These Reliability tests are intended to investigate the reproducibility of PUF responses of all different PUFs in the UNIQUE ASIC under varying external conditions. In the table below an overview of the different Reliability tests that will be performed can be found.

Table 10: Description of Reliability Tests

Repeated Start-up Test	Repeatedly measure PUF responses at room temperature to evaluate noise between measurements
Temperature Cycle Test	Measure PUF responses at different ambient temperatures
Temperature Ramp Test	Measure PUF responses while ambient temperature is increasing/decreasing with approximately 1ºC/minute
Voltage Variation Test	Measure PUF responses at different core voltages
Voltage Ramp Up Test	For memory based PUFs: Measure start-up values when the memory is powered up with different power-up times (ramps)
Voltage Dip Test	For memory based PUFs: Store all ones (0xFF bytes) into the memory and read the values in the memory after it has been subjected to short power dips of varying lengths
Data Retention Test	For memory based PUFs: Store all ones (0xFF bytes) into the memory, temporarily lower the core voltage and then measure the PUF response at the normal voltage level
Ageing Test	Measure PUF responses on a weekly basis on ICs that are kept at high temperature and increased voltage for a long period

Not all PUFs are suitable for use in each of the tests above. In the table below it can be found which PUFs are evaluated during which tests. As can be seen here some tests are only suitable for memory-based PUFs. Furthermore, the Latch and Buskeeper PUFs do not have write functionality. Therefore, they cannot be used in the Voltage Dip and Data Retention Test. Since it was not possible to perform all tests with the complete set of 192 UNIQUE ASICs, some tests have been performed on a subset of devices. In the table below can also be found how many ASICs have been used during each of the individual tests.

Table 11: Number of ASICs and PUF types evaluated during each test

	Number of ASICs	Arbiter	Ring Oscillator	SRAM	D Flip-Flop	Latch	Bus-keeper
Repeated Startup Test	96	X	X	X	X	X	X
Temperature Cycle Test	192	X	X	X	X	X	X
Temperature Ramp Test	192	X	X	X	X	X	X
Voltage Variation Test	192	X	X	X	X	X	X
Voltage Ramp Up Test	50			X	X	X	X
Voltage Dip Test	50			X	X		
Data Re-tention Test	50			X	X		
Ageing Test	5	X	X	X	X	X	X

4.2 PUFs aging evaluation

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 ageing test by keeping 5 ICs under high voltage (120% of Vdd = 1.44V) and temperature conditions (+85°C). The total estimated acceleration factor [14] is the product of the Thermal Acceleration Factor (TAF) and the Voltage Acceleration Factor (VAF), which are computed as:

$$TAF = e^{\frac{E_a}{k}\left(\frac{1}{T_{op}} - \frac{1}{T_{stress}}\right)}$$

$$VAF = e^{\gamma\left(V_{stress} - V_{op}\right)}$$

With E_a (0.5 eV) the activation energy, k ($8{,}62 \cdot 10^{-5}$ eV/°K) Boltzmann's constant, T_{op} (313°K (+40°C)) the nominal operating temperature, T_{stress} (358°K (+85°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 · VAF = 10.27 · 1.77 = 18.2.

Every week the ambient temperature and supply voltage were lowered to +25°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°C and 1.2V was taken to which all other measurements are compared based on the Fractional Hamming Distance (FHD)[1]. 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 12: Ageing test results; Min. and Max. FHD compared to reference per PUF for 5 ASICs (incl. results from separate power domain) 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°C. The results from this column clearly show that the (minimal) ageing effect occurring on the memory-based PUFs can be reduced 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.

Table 12: Ageing test results; Min. and Max. FHD compared to reference per PUF for 5 ASICs (incl. results from separate power domain)

PUF type	Nr of PUF bits	Before Ageing		After Ageing		After Ageing (separate PD)	
		Min	Max	Min	Max	Min	Max
SRAM	65536	5.0%	5.5%	7.0%	8.0%	5.5%	5.5%
Buskeeper	8192	3.5%	5.0%	5.5%	7.0%	3.5%	5.0%
Latch	8192	2.0%	3.0%	5.0%	6.0%	2.5%	3.5%
DFF (#0, 2, 3)	8192	2.5%	4.0%	4.5%	6.0%	3.5%	4.0%
DFF (#1)	8192	3.5%	7.0%	4.0%	12.0%	n.a.	n.a.
Arbiter	8192	2.5%	3.5%	3.0%	4.5%	n.a.	n.a.
Ring Oscillator	3840	1.0%	2.5%	3.5%	5.0%	n.a.	n.a.

[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.

When interpreting the results from this table, one must take the following into account:

- 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 the table above.

4.3 PUFs robustness evaluation

Robustness means the property that, for the same challenge, a PUF always generates responses that are similar to the response generated during the enrolment of the PUF. This is an essential requirement in PUF-based applications that must rely on the availability of data generated by or bound to the PUF. Note that PUFs should be robust under different operating conditions such as different temperature, voltage and noise levels. An overview of all test cases considered for robustness is given in Table 13: Robustness test cases.

Table 13: Robustness test cases

Test Case	Active Core		Ambient Temperature			Supply Voltage			Iter.
	Off	On	−40 °C	+25 °C	+85 °C	1.08 V	1.2 V	1.32 V	k
E_1	×		×			×			20
E_2	×		×				×		40
E_3	×		×					×	20
E_4	×			×		×			30
E_5	×			×			×		60
E_6	×			×				×	30
E_7	×				×	×			20
E_8	×				×		×		40
E_9	×				×			×	20
E_{11}		×		×			×		60

4.3.1 Strategy

The similarity of PUF responses and thus the robustness of the PUF can be quantified with the bit error rate (BER), i.e., the number of bits of a PUF response that are different from the response observed during enrolment divided by the total number of bits of the PUF response.

We determine the average and maximum BER of all PUF instances in the ASICs by collecting challenge/response pairs at different ambient temperatures (-40°C to +85°C), supply voltages (±10% of the nominal 1.2V) and noise levels (active core enabled and disabled) which correspond to corner values that are tested for consumer grade IT products. This shows the impact of the most common environmental factors on the bit error rate of each PUF type.

We estimate the BER of all PUFs in all ASICs using the following strategy:

Step 1: Sample Challenge Set Generation

A sample challenge set C' is generated for each PUF type (arbiter, ring oscillator, SRAM, flip-flop and latch PUFs) which is used in all subsequent steps. For all but the arbiter PUF, the complete challenge space is used as a sample set. Since the arbiter PUF has an exponential challenge space, we tested it only for 13,000 randomly chosen challenges.

Step 2: Enrolment

For each PUF instance, the response ri to each ci ϵ C' is obtained under nominal operating conditions (test case E5 in Table 13: Robustness test cases) and stored in a database DB0.

Step 3: Data Acquisition

For all robustness test cases Ep, each PUF instance are evaluated k times on each ci ϵ C' and stored in a database DBp.

Step 4: Analysis

For each PUF instance the average and maximum bit error rate between responses of PUFj in DB0 and responses of PUFj in DB1,…, DB10 is computed.

4.3.2 Results

We demonstrate our results using bean plots that allow an intuitive visualization of empirical probability distributions. Each bean shows two distributions, smoothed by a Gaussian kernel to give the impression of a continuous distribution, together with their means indicated by black bars. The distribution in black on the left side typically corresponds to data collected under normal PUF operating conditions, while the one in gray on the right side corresponds to some other test case in Table 13. This allows an easy visualization of PUF behaviour under changing environmental conditions. Each plot contains several beans, which correspond to the different PUF types available on the ASICs, which allows an easy comparison of the results for different PUF types.

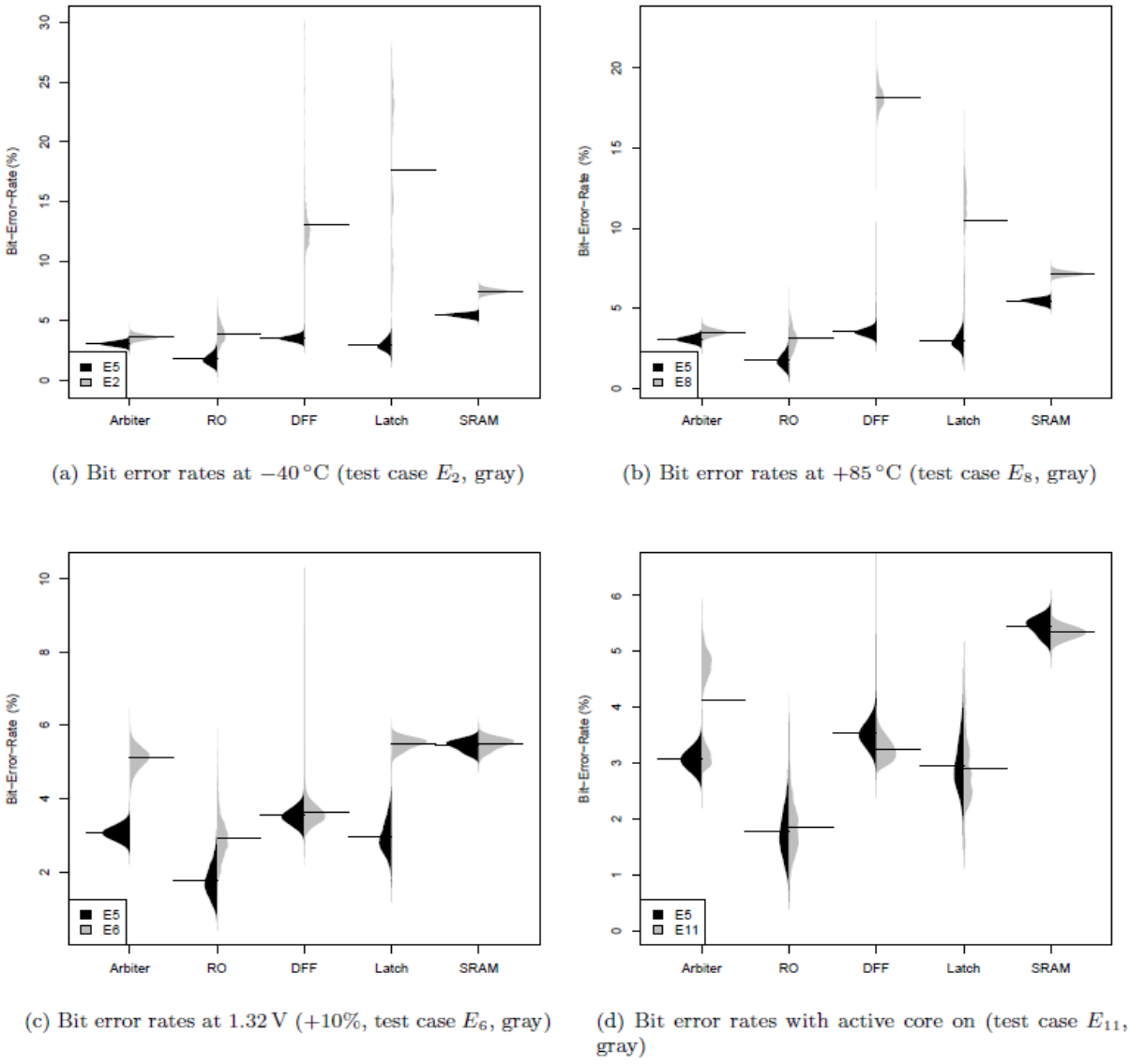
First we computed the bit error rates under varying environmental conditions. Figure 1 illustrates the results: The vertical axis displays the bit error rate (BER) in percent. Our results show that all arbiter, ring oscillator and SRAM PUF instances have a very similar BER (since the distributions are rather narrow), while there is a big variability in the BERs of the flip-flop and latch PUF instances. Further, the BER of the arbiter, ring oscillator and SRAM PUF instances is below 10% for all test cases, which can be handled by extractors based on common error correction schemes [1].

The bit error rate of most PUFs depends on the operating temperature. We observed that at 40°C (test case E2, illustrated by the gray distribution in Figure 2a) the BER significantly increases for the flip-flop and latch PUF, while it only slightly increases for the ring oscillator and SRAM PUF. The BER of the arbiter PUF hardly changes at 40°C. A similar behaviour of the BERs can be observed at +85°C (test case E8, see the gray distributions in Figure 2b).

All PUFs in all ASICs turned out to be robust against variations in their supply voltages. Compared to nominal operating conditions (test case E5), the distributions of the BERs only slightly increase when varying the supply voltage by 10% (test case E4 and E6). Test case E6 is illustrated in Figure 2c for exemplary purposes.

The arbiter PUF exhibits a significantly increased BER when operated in a noisy working environment (test case E11), while there is no significant change of the BER of all other PUFs. This test case is illustrated in Figure 2d. The two peaks of the BER distribution of the arbiter PUF shown in Figure 2d are due to the fact that in the ASIC layout some of the arbiter-PUFs adjoin the active core while others are farther away and not directly affected.

Figure 2: Distribution of the bit error rate (BER) over all PUF instances



(a) Bit error rates at −40 °C (test case E_2, gray)

(b) Bit error rates at +85 °C (test case E_8, gray)

(c) Bit error rates at 1.32 V (+10%, test case E_6, gray)

(d) Bit error rates with active core on (test case E_{11}, gray)

The Hamming distance of the responses of the latch PUFs are always biased towards zero and invariant for different supply voltages.

4.4 PUFs unpredictability evaluation

Unpredictability ensures that the adversary cannot efficiently compute the response of a PUF to an unknown challenge, even if he can adaptively obtain a certain number of other challenge/response pairs from the same and other PUF instances [3]. This is important in most PUF-based applications, such as authentication protocols, where the adversary could forge the authentication if he could predict the PUF response. Note that unpredictability should be independent of the operating conditions of the PUF, which could be exploited by an adversary.

The unpredictability of a PUF instance can be empirically estimated by applying statistical tests to its responses and/or based on the complexity of the best

known attack against the PUF [2,3]. Statistical tests, such as the DIEHARD [4] or NIST [5] test suites, can be leveraged to assess the unpredictability of PUF responses. However, since these test suites are typically based on a series of stochastic tests, they can only give an indication about whether responses are random or not. Moreover, they typically require more input data than the memory-based PUFs and ring oscillator PUFs in the ASIC provide. Another approach to empirically assess the unpredictability of PUFs is estimating the entropy of their responses based on experimental data. In particular, min-entropy indicates how many bits of a PUF response are uniformly random. The entropy of PUFs can be approximated using the context-tree weighting (CTW) method [6], which is an algorithm related to data compression that allows estimating the redundancy of bit-strings [7,8,9,10]. Similar as in symmetric cryptography, the unpredictability of a PUF can be estimated based on the complexity of the best known attack against the unpredictability property. There are attacks [11] against delay-based PUFs that emulate the PUF in software and allow predicting PUF responses to arbitrary challenges. These attacks are based on machine learning techniques that exploit statistical deviations and/or dependencies of PUF responses. However, emulation attacks have been shown only for simulated PUF data and it is currently unknown how these attacks perform against real PUFs. Furthermore, these attacks require a large amount of challenge/response pairs that may be hard to collect in most practical applications [11].

4.4.1 Strategy

We estimated unpredictability of all PUF types and instances implemented in the ASICs by approximating their entropy and min-entropy using different statistical tests. Furthermore, we estimate unpredictability at different ambient temperatures and supply voltage levels to determine the effects of environmental conditions on the unpredictability of the PUF. An overview of all test cases considered for unpredictability is given in Table 14.

Notation: Let E be some event, then Pr[E] denotes the probability that E occurs. We denote with HW(x) the Hamming weight of a bit-string x, i.e., the number of non-zero bits of x. With dist(x, y) we denote the Hamming distance between bit string x and y, i.e., the number of bits that are different in x and y.

We assess the unpredictability of all PUFs in the ASICs using the following strategy:

Table 14: Unpredictability test cases

Test Case	Active Core		Ambient Temperature			Supply Voltage		
	Off	On	−40 °C	+25 °C	+85 °C	1.08 V	1.2 V	1.32 V
E_{13}	×		×				×	
E_{14}	×			×			×	
E_{15}	×				×		×	
E_{16}	×			×		×		
E_{17}	×			×				×

Step 1: Sample Challenge Set Generation

For each PUF type, a sample challenge set C' is generated that is used in all subsequent steps. For all but the arbiter PUF, the complete challenge space is used as a sample challenge set. Since the arbiter PUF has an exponential challenge space, we again test it only for 13,000 challenges that should be representative for the whole challenge set of the arbiter PUF.

The subsequent analysis steps require X' = {x' ϵ X'', dist(x,x') ≤ k}, which includes a set X'' of randomly chosen challenges (representing the challenges to be guessed by the adversary) and all challenges that differ in at most k bits from the challenges in X'' (that in the worst case might be known to the adversary).

Step 2: Data Acquisition

For all unpredictability test case Ep, each PUF instance PUFj is evaluated on each ci ϵ C' and its responses r are stored in a database DBp.

Step 3: Analysis

For each unpredictability test case Ep, the responses in DBp are analyzed as detailed in the following paragraphs:

Step 3a: Hamming Weight

For each PUF instance PUFj , the average Hamming weight of all responses in DBp is computed, which indicates whether the PUF responses are biased towards 0 or 1.

Step 3b: CTW Compression

For each PUF instance PUFj, a binary file containing all responses in DBp is generated and compressed using the context-tree weighting (CTW) algorithm [12]. The resulting compression rate is an estimate of the upper bound of the entropy of the PUF responses.

Step 3c: Entropy Estimation

For each PUF instance PUFj , the entropy and min-entropy of all responses in DBp is estimated as described in the next paragraph.

Step 3d: Hamming Distance

For each physical function type, the Hamming distance dist(y,y') between all pairs of responses in DBp of pairwise different PUF instances to the same challenge is computed. While all previous analysis methods consider only responses of the same PUF instance, the Hamming distances indicate whether responses of different PUF instances are independent, which is important since otherwise the adversary could predict PUF responses using another PUF instance with a similar challenge/response behavior.

4.4.2 Entropy estimation

Let *Y(x)* be the random variable representing PUF response *y to challenge x.* Moreover, let *x* be the challenge for which the adversary should predict *y.*

Further, let *W(x)* be the random variable representing the set of all responses of PUF except response *y* to challenge *x*, i.e., *W(x) = {y': y'← PUF(x'); x' ϵ X\{x}}*.

We are interested in the conditional entropy

$$\mathbf{H}(Y|W) = -\sum_{x\in\mathcal{X}} \Pr\left[Y(x), W(x)\right] \cdot \log_2 \Pr\left[Y(x)|W(x)\right] \quad (1)$$

and the conditional min-entropy

$$\mathbf{H}_\infty(Y|W) = -\log_2 \left(\max_{x\in\mathcal{X}} \left\{ \Pr\left[Y(x)|W(x)\right] \right\} \right), \quad (2)$$

which quantify the average and minimal number, respectively, of bits of a PUF response to some challenge *x* that cannot be predicted by the adversary, even in case all other responses *W(x)* are known. Hence, $2^{-H_\infty(Y|W)}$ is an information-theoretic upper bound for the probability that an unbounded adversary can guess PUF response *x*.

However, computing Equation 1 and 2 for W(x) is difficult in practice since (1) the number of observations required to estimate the underlying probability distributions grows exponentially in the response space size, and (2) the complexity of the computation of *H(Y|W)* grows exponentially with the challenge space size of the PUF to be analyzed. Note that memory-based PUFs typically generate responses that consist of many bits, ranging from the size of a memory word up to the size of the entire memory. Further, delay-based PUFs typically have a very large to exponential challenge space size. This means that for all PUFs to be analyzed, Equation 1 and 2 cannot be computed for *W(x)* and can at most be estimated by making assumptions on the physical properties of the PUF. In the following, we explain how we estimated these entropies for each PUF type and discuss the underlying assumptions.

Memory-based PUFs:

A common assumption on memory-based PUFs is that spatially distant memory cells are independent [2,3]. A similar assumption has been used by Holcomb et al. [13], who estimate the entropy of SRAM PUF responses based on the assumption that individual bytes of SRAM are independent. However, physically neighbouring memory cells can strongly influence each other, in particular when they are physically connected to each other. Hence, our entropy estimation considers only dependencies between neighbouring memory cells (which could be exploited by an adversary) while assuming that spatially distant memory cells are independent. More specifically, we compute the entropy of all bits $Y_{i,j}$ of the response of a memory-based PUF under the worst case assumption that the values of all neighbouring memory cells $W'(x) = (Y_{i-1,j}, Y_{i,j+1}, Y_{i+1,j}, Y_{i,j-1})$ are known, i.e., we compute Equation 1 and 2 for $W'(x)$.

Ring Oscillator PUFs:

The ring oscillator PUF on the ASIC compares the oscillation frequency of two ring oscillators O_i and O_j selected by the PUF challenge $x = (i,j)$ and returns a response $Y(i,j)$, depending on which of them is faster. Since neighbouring ring oscillators are subject to the same manufacturing process variations, it is very likely that their oscillating frequencies are very similar. Therefore, our entropy estimation considers only the potential dependency between neighbouring ring oscillators, while assuming that spatially separated ring oscillators have different oscillating frequencies. Thus, we compute Equation 1 and 2 for W'(i,j) = (Y(i-2,j),Y(i-1,j),Y(i+1,j),Y(i+2)).

Arbiter PUFs:

Arbiter PUFs measure the delay difference of two delay lines that are configured by the PUF challenge. The individual delays caused by the switches and their connections are additive, which implies that the response y to a challenge x can be computed if a sufficient number of responses to challenges that are close to x are known. Hence, we compute Equation 1 for:

$$W'(x) = \{y' \leftarrow PUF(x');\ x' \in X',\ dist(x,x') \leq k\}$$

This corresponds to the worst case where the adversary know responses to challenges that differ in at most k bits from the challenge to the response to be guessed. In our analysis we use X consisting of 200 randomly chosen challenges and k = 1.

4.4.3 Results

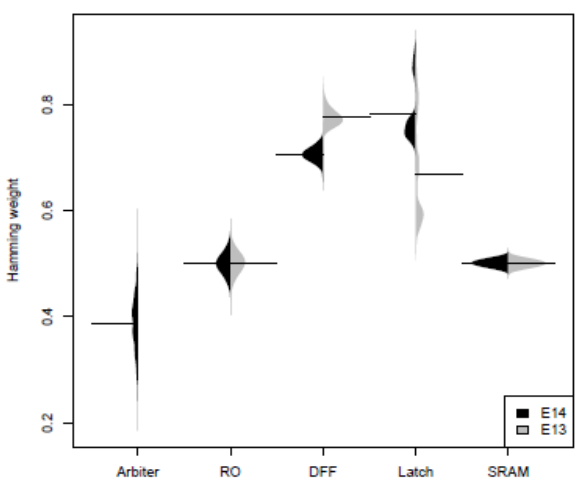
In this section, we present the results of the unpredictability analysis. Due to the time-limited access to the climate chamber the data required to analyze the unpredictability property of the arbiter PUF at −40°C and at +85°C is not

available. However, we show the results for normal operating conditions and different supply voltages.

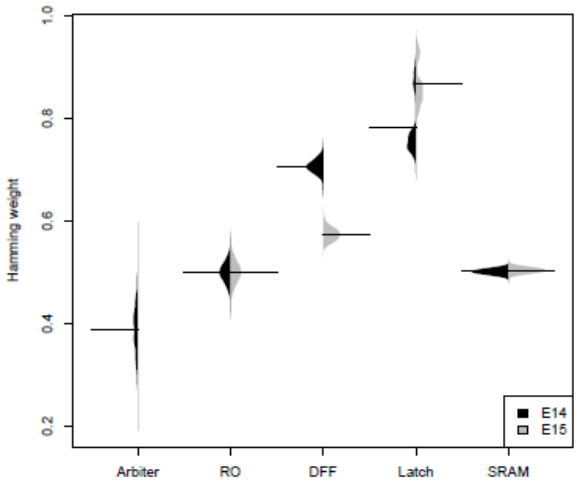
To get a first indication of the randomness of the responses generated by the different PUF instances in the ASIC, we computed the Hamming Weight of the responses as described in section 4.4.1.

Note that a uniformly random string should have a Hamming weight close to 0.5. Our results illustrated in Figure 3 show that ring oscillator and SRAM PUF responses are close to a Hamming weight of 0.5, independent of the operating conditions. This indicates that these PUFs may generate random responses, while the responses of the flip-flop and latch PUFs are clearly biased.

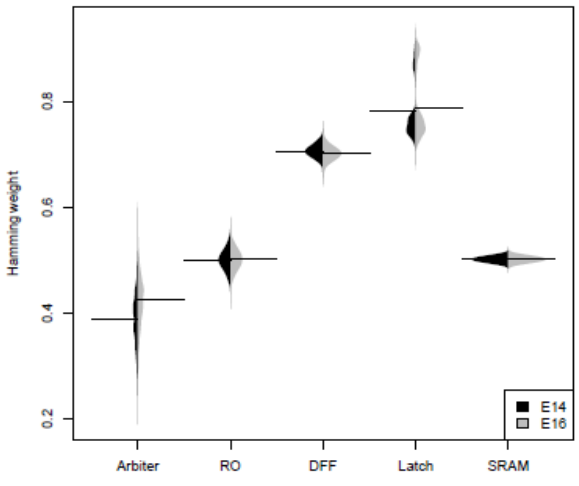
Figure 3: Distribution of Hamming weight over all PUF instances



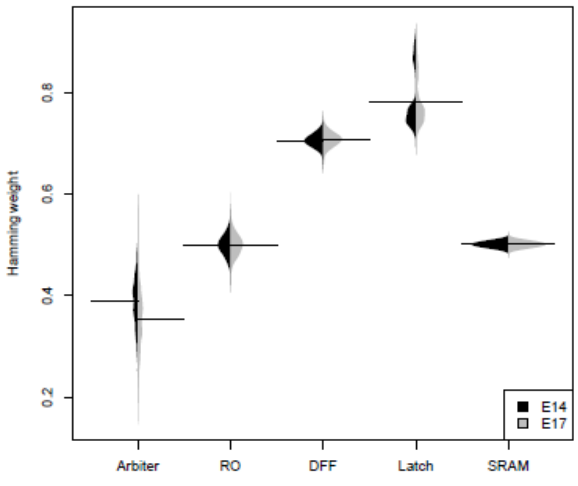
(a) Hamming weight at $-40\,^{\circ}\mathrm{C}$ (test case E_{13}, gray)



(b) Hamming weight at $+85\,^{\circ}\mathrm{C}$ (test case E_{15}, gray)



(c) Hamming weight at $1.08\,\mathrm{V}$ (-10%, test case E_{16}, gray)



(d) Hamming weight at $1.32\,\mathrm{V}$ ($+10\%$, test case E_{17}, gray)

Temperature variations (test case E13 and E15) do not affect the Hamming weight of the ring oscillator and SRAM PUF responses, while the Hamming weight of the flip-flop PUF and latch PUF responses strongly depends on the temperature the PUF is operated at, which can be clearly seen by comparing Figure 3a and Figure 3b. Note that the two peaks of the Hamming weight distribution of the latch PUF come from the fact that, for some unknown reason, one of the four instances on each ASIC behaves differently.

Supply voltage variations (test cases E16 and E17) do not significantly change the Hamming weight of the responses of any of the PUF instances in the ASIC. We show the exemplary graph for E16 in Figure 3c. Results for test case E17 are very similar to E16.

CTW Compression Rates. The second test for unpredictability is the context-tree weighting (CTW) compression test, which compresses the responses of the PUF. As discussed in section 4.4.1, the compression rate achieved by the CTW algorithm gives a good indication of the upper bound of the entropy of the PUF responses. The higher the compression rate, the lower the entropy of the PUF.

The results of the compression test for the different test cases (Table 14: Unpredictability test cases) are summarized in Table 15: CWT compression results, which shows the size of the PUF responses after compression in percent.

The compression rates confirm the Hamming weight test results:

The compression rate of the ring oscillator and SRAM PUF responses is invariant for all test cases. The compression rates of the flip-flop and latch PUF responses do not change for different supply voltages (test case E16 and E17), but vary with the ambient temperature of the PUF (test cases E13, E14 and E15).

Furthermore, the compression rate of SRAM PUF responses gives a strong indication that these responses are uniformly random, while there seem to be some dependencies in the responses generated by all other PUFs.

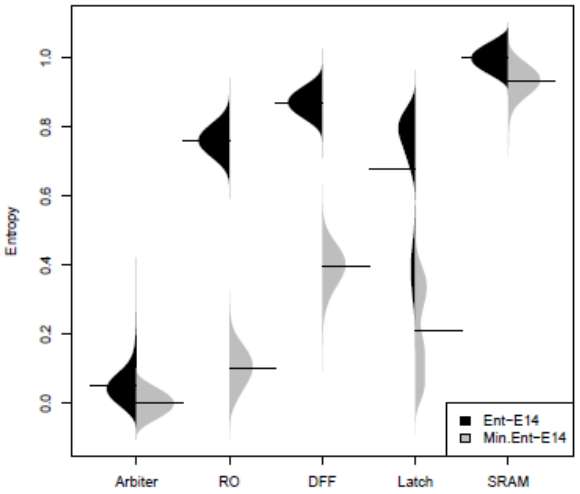
Table 15: CWT compression results

Test Case	CTW Compression Results				
	Arbiter	RO	FF	Latch	SRAM
E_{13}	—	0.77	0.77	0.84	1.00
E_{14}	0.51	0.77	0.87	0.70	1.00
E_{15}	—	0.77	0.98	0.53	1.00
E_{16}	0.53	0.77	0.88	0.69	1.00
E_{17}	0.49	0.77	0.87	0.71	1.00

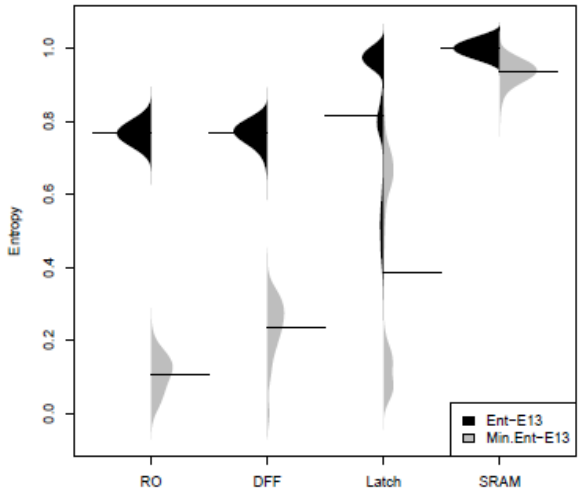
Entropy Estimation. The results of the entropy estimation according to section 4.4.1, illustrated in Figure 4, confirm all previous analysis results and provide more insights into the entropy and min-entropy of the PUF responses. This time, the bean plots allow comparing the entropy (in black on the left side) with the min-entropy (in gray on the right side) for the different test cases.

The entropy of responses corresponding to neighbouring arbiter PUF challenges is remarkably low, which confirms the high prediction rate of emulation attacks against arbiter PUFs reported in literature [11]. In accordance to our previous unpredictability analysis results, the entropy and min-entropy distributions of the ring oscillator and SRAM PUF responses do not change for different ambient temperatures (test cases E13, E14 and E15) and supply voltages (test case E16 and E17). Moreover, the distribution of the entropy and min-entropy of flip-flop and latch PUFs vary with the operating temperature (test cases E13, E14 and E15) and are constant for different supply voltages (test case E16 and E17). Furthermore, the mean of the entropy distributions approximately matches the result of the compression test results. Figure 4 illustrates test cases E13, E14 and E15. The entropy distributions for different supply voltage levels (test case E16 and E17) are similar to the graphs for nominal operating conditions (test case E14) in Figure 4a).

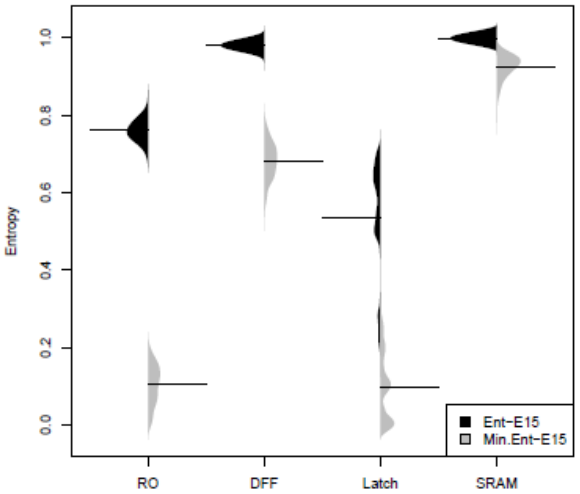
Figure 4: Distribution of the entropy and min-entropy over all PUF instances



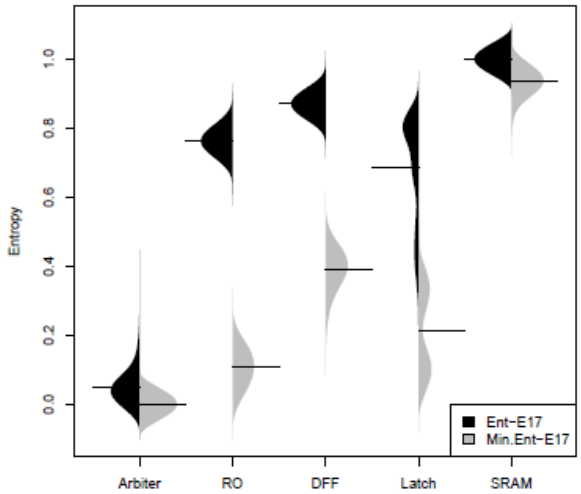
(a) Entropy (black) and min-entropy (gray) at +25 °C (test case E_{14})



(b) Entropy (black) and min-entropy (gray) at −40 °C (test case E_{13})



(c) Entropy (black) and min-entropy (gray) at +85 °C (test case E_{15})



(d) Entropy (black) and min-entropy (gray) at 1.32 V (+10%, test case E_{17})

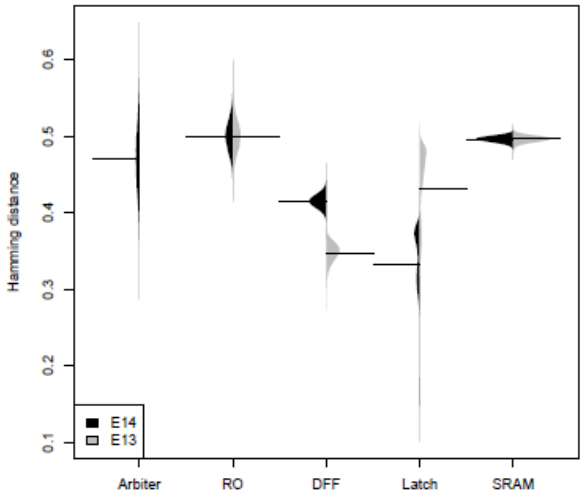
Hamming Distances. The Hamming distance test (section 4.4.1) gives an indication of whether the responses generated by different PUF instances to the same challenge are independent. In case individual PUF responses are independent, their Hamming distance should be about 0.5.

Our results illustrated in Figure 4 show that, independent of the ambient temperature (test cases E13, E14 and E15) and supply voltage (test case E16 and E17), the responses of different ring oscillator and SRAM PUF instances have the ideal Hamming distance of 0.5. The distribution of Hamming distances for the arbiter PUF is again remarkably widespread; indicating that there may be dependencies between the responses generated by different PUF instances to the same challenge.

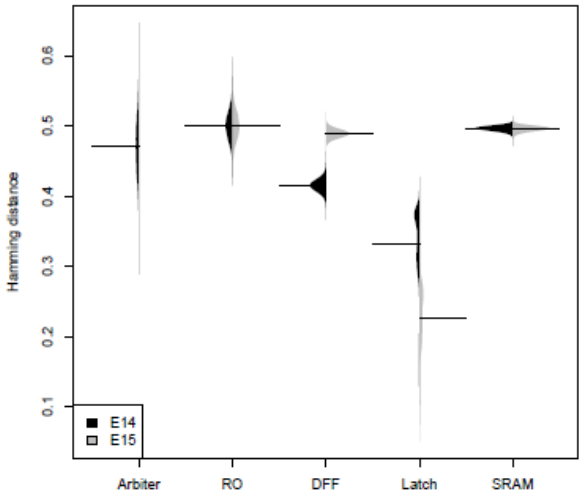
The Hamming distance of the responses of the flip-flop PUFs changes for different temperatures and supply voltages. At +85°C (test case E15, see gray distribution in Figure 5c) the Hamming distance of the flip-flop PUF is ideal, while it is biased towards zero at –40°C (test case E13 in Figure 5b). Moreover, at 1.08V (-10%, test case E16) we observed a bias of the Hamming distance towards one, while the Hamming distance distribution at 1.32V (+10%, test case E17) is similar to the distribution at nominal operating conditions (test case E14).

The Hamming distance of the responses of the latch PUFs are always biased towards zero and invariant for different supply voltages.

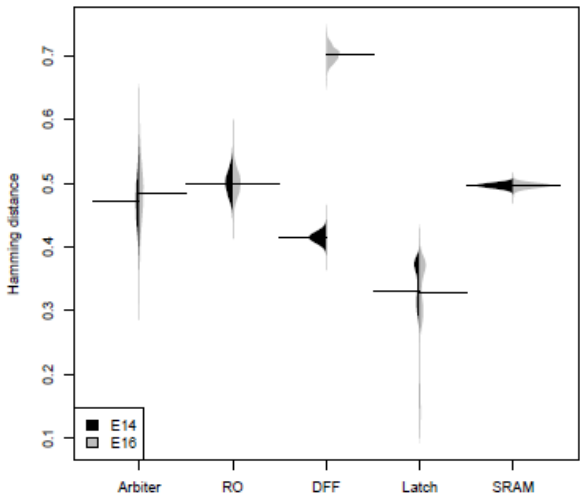
Figure 5: Distribution of the Hamming distance over all PUF instances



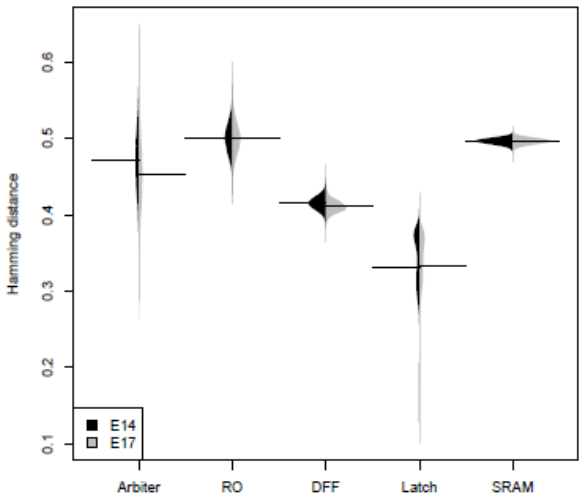
(a) Hamming distance at $-40\,^{\circ}\mathrm{C}$ (test case E_{13}, gray)



(b) Hamming distance distance at $+85\,^{\circ}\mathrm{C}$ (test case E_{15}, gray)



(c) Hamming distance at $1.08\,\mathrm{V}$ (-10%, test case E_{16}, gray)



(d) Hamming distance at $1.32\,\mathrm{V}$ ($+10\%$, test case E_{17}, gray)

4.5 Buskeeper PUF robustness and unpredictability

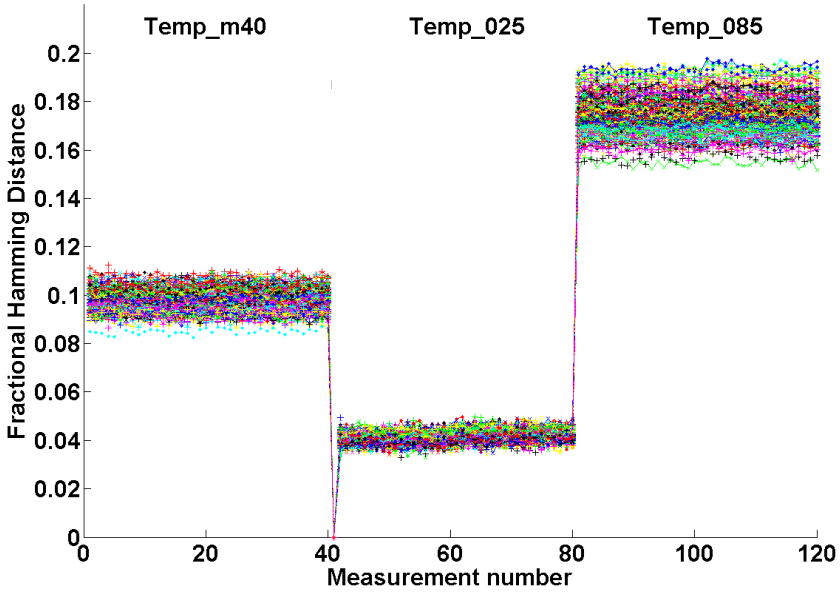
Buskeeper PUF assessment is issued from an independent study. Therefore, the results are not presented in section 4.3 nor 4.4 but in this separate section.

4.5.1 Robustness evaluation

Temperature Variation Test To test the robustness of Buskeeper PUFs under temperature variations 96 ICs (with two Buskeeper PUFs of 1kB) have been placed in the climate chamber. This way a set of 192 Buskeepers can be evaluated. Measurements of PUF start-up patterns have been taken at three different temperatures: -40°C, +25°C, and +85°C (industrial standard for temperature testing of ICs ranges from -40°C to +85°C). In this case +25°C is the enrollment temperature of the PUFs, while the other two temperatures are the most extreme deviations from enrollment available for this test. At each temperature the Buskeeper PUFs have been measured 40 times. These measurements are all compared to one enrollment pattern for each PUF at +25°C using fractional Hamming Distance (FHD)[2]. The results of this test can be found in Figure 6. The number of measurements per device is set to the horizontal axis, while the vertical axis presents the FHD between start-up patterns and enrollment of the chip. At the top of the graph the different conditions, in this case temperatures (Temp_m40 = -40°C, Temp_025 = +25°C, Temp_085 = +85°C), are specified. Each line in the Figure represents a different Buskeeper PUF. The spike to FHD = 0 represents the enrollment measurement of each Buskeeper (since FHD to itself is 0). A similar representation is used in this section for all the other test results.

[2] 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.

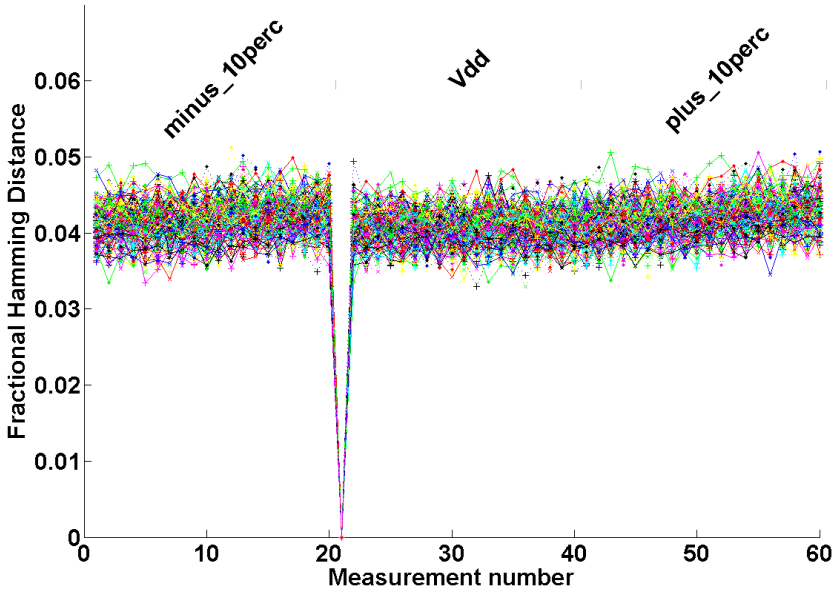
Figure 6: Measurement results from Temperature Variation Test



It can be seen in this Figure that the FHD increases when the temperature deviates from the enrollment temperature. The Buskeeper PUF appears to be more sensitive for high temperatures than low temperatures. Furthermore, it can be concluded that the noise on Buskeeper PUFs due to these temperature variations remains below 20% (FHD = 0.2). This is well within the boundaries, as specified earlier, for error correction using a Fuzzy Extractor.

Voltage Variation Test To investigate the influence of varying supply voltage levels on the robustness of Buskeeper PUFs, the 96 ICs (192 Buskeepers) have been placed in a set-up suitable for varying the supply voltage from 90% of Vdd to 110% of Vdd. An enrollment measurement for each Buskeeper has been taken with supply voltage Vdd. At each voltage level the Buskeeper PUFs have been measured 20 times. The results of performing this test at +25°C can be found in Figure 7 (minus_10perc = 90% of Vdd and plus_10perc = 110% of Vdd). This test has also been performed at +85°C and -40°C for which the results were similar to those at +25°C.

Figure 7: Measurement results from Voltage Variation Test at +25°C

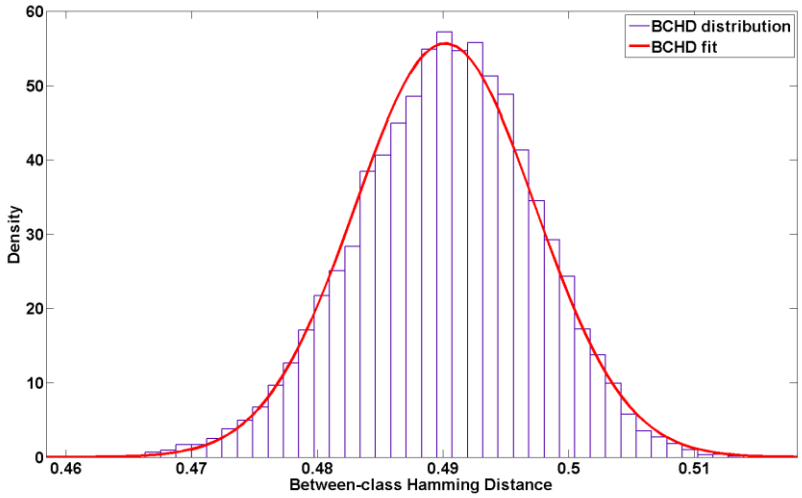


It becomes clear from these results that varying the supply voltage of Buskeeper PUFs does not influence the robustness of their start-up patterns (at any ambient temperature). With a noise level below 5% the Buskeeper PUFs are very stable at different supply voltages.

4.5.2 Unpredictability evaluation

Hamming Distance Test When performing unpredictability tests, we are interested in finding out whether it is possible to distinguish between different devices given their PUF responses. This is required to make sure that unique keys can be derived from different Buskeeper PUFs. The first evaluation is performed by creating a Hamming Distance Test of the different enrollment patterns from the Temperature Variation Test using the FHDs between the different PUFs. This results in a distribution of FHDs that can be approximated as a Gaussian curve with an average value μ and a standard deviation σ. To get an indication whether PUFs are uniquely identifiable, the value of μ should be close to 0.5. In case of the tested Buskeeper PUFs μ = 0.49015 and σ = 0.007162. Therefore, this is a good first indication that these PUFs are uniquely distinguishable.

Figure 8: Hamming Distance distribution of enrollment data Temperature Variation Test



Entropy Estimation To estimate the entropy of Buskeeper PUFs, we use a compression algorithm (to estimate an upper bound) and calculate the min-entropy (which leads to a lower bound). The actual entropy of these PUFs will be somewhere between these boundaries. Context-Tree Weighting (CTW) is an optimal compression method for a stationary ergodic source, which we assume the PUF data to be. This algorithm can be used to check the ability to compress PUF response strings. The amount of compression will give an estimate of the upper bound of the entropy of our PUF responses. When the algorithm is capable of compressing the PUF responses, the responses do not have full entropy. This test was carried out by first concatenating all enrollment patterns from the Temperature Variation Test into one string. As can be seen in Table 16, very little compression is achieved by CTW. This indicates that only little non-randomness is present in these PUF responses.

Table 16: Results of CTW compression test

Original Size (bits)	Size after CTW (bits)	Compression ratio
192*8192 = 1572864	1553605	98.8%

Besides the compression factor, it is also possible to estimate the min-entropy of the Buskeepers. Min-entropy is the worst-case (i.e., the greatest lower bound) measure of uncertainty for a random variable. For this purpose we use the method that is described below (taken from appendix C of NIST specification 800-90).

Output values of binary sources have a probability of occurring p_0 and p_1 respectively (sum of these probabilities is 1). When p_{max} is the maximum value of these two probabilities, the definition for min-entropy of a binary source is:

$$H_{min} = -\log^2(p_{max})$$

Assuming that all bits from the PUF start-up pattern are independent (which is plausible, since Buskeepers can be spread randomly over the entire surface of an IC), each bit of the pattern can be viewed as an individual binary source. For n independent sources (in this case n is the length of the start-up pattern) the definition below holds, which is a summation of the entropy from each individual bit.

$$H_{min\_total} = \sum_{i=1}^{n} -\log^2(p_{i\,max})$$

For our calculations we take the enrollment patterns that we have used during the Temperature Variation Test. These patterns are bitwise summarized to calculate a weight W per bit, which can have a value between 0 and the number of enrollment patterns (m). Based on this W, p_{max} can be calculated for each individual bit of the start-up pattern:

$$\text{If } W_i > m/2: \; p_{i\,max} = W_i/m$$
$$\text{Else:} \quad p_{i\,max} = (m-W_i)/m$$

Based on these values for p_{max}, the min-entropy of each individual bit (source) and the total min-entropy of the start-up pattern can be calculated using the formulas above. Finally, the average min-entropy per bit of a memory is calculated by dividing H_{min_total} by the length of the pattern n.

Figure 9: Min-entropy development over the number of enrollment files (m)

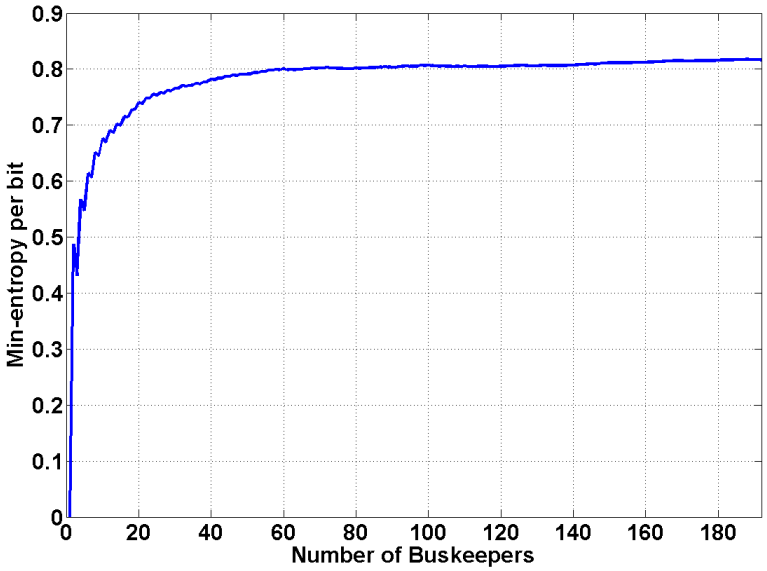


Figure 9 displays how the average min-entropy per bit of the Buskeepers develops over an increasing m. It can be seen that after using 192 devices for this min-entropy test (the total number of instances measured for this paper), the average min-entropy per bit is 0.82 and still rising. This means that the values found by this test are conservative estimates, since these values would increase with more devices. From the results we conclude that the entropy of the tested Buskeeper PUFs is a value between 0.82 and 0.988 per bit.

5 Security evaluation

5.1 Reverse Engineering

5.1.1 Package visual inspection

Three ASIC devices were used for reverse engineering analysis:

- One is used for cross-section.
- Two are used for deprocessing.

Standard front side chemical decapsulation does not keep device functionality because of Cu bonding wires. Indeed, hot nitric acid etches copper very fast.

To avoid this problem and maintain device functionality, a backside preparation is selected for EMMI attacks. Backside opening is done by mechanical polishing with the ASAP machine.

For reverse engineering, packages are plunged into hot nitric acid and the stand-alone chips are retrieved.

Figure 10: Package top view

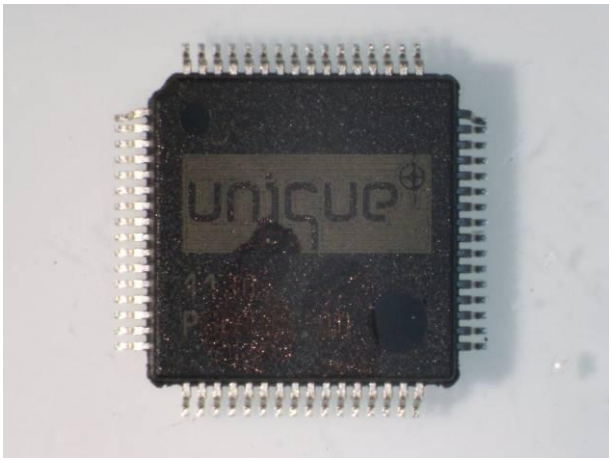
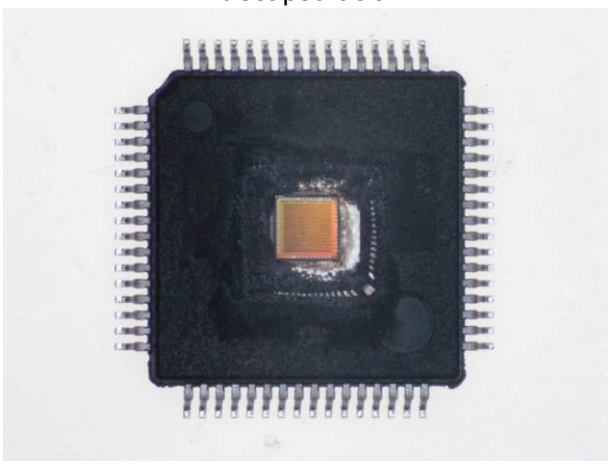


Figure 11: Package after front side decapsulation.



5.1.2 Cross section by FIB

A cross-section was performed by Focused Ion Beam (FIB) to characterize the process used and to adapt the deprocessing method to the device under test. This cross-section was localized in SRAM memory array.

The ASIC process is characterized by:

- Full planar technology.
- 10 metal layers: M10 layer is Al and M9 to M1 layers are Cu. M10 level is only used for pads. M9 Cu layer is very large, whereas M8 to M1 are thinner.
- One poly level for transistors gates. Minimum poly gate width is measured ≈65nm in good agreement with a 65nm technological node.
- Vias are made with Cu.
- Contacts on active areas are made with TiW. Their diameters are around 100nm.
- Active isolations are performed by Shallow Trench Isolation (STI).

Figure 12: FIB cross-section in SRAM array. 9 Cu layers in this area.

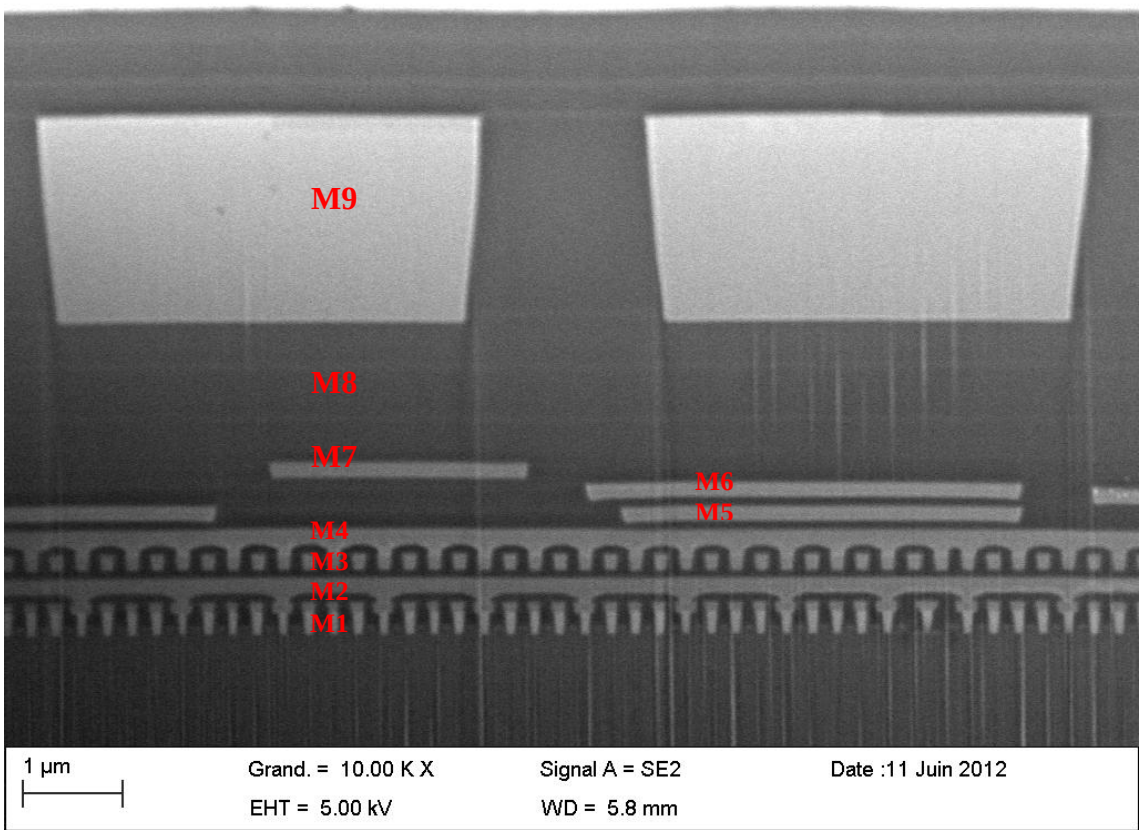
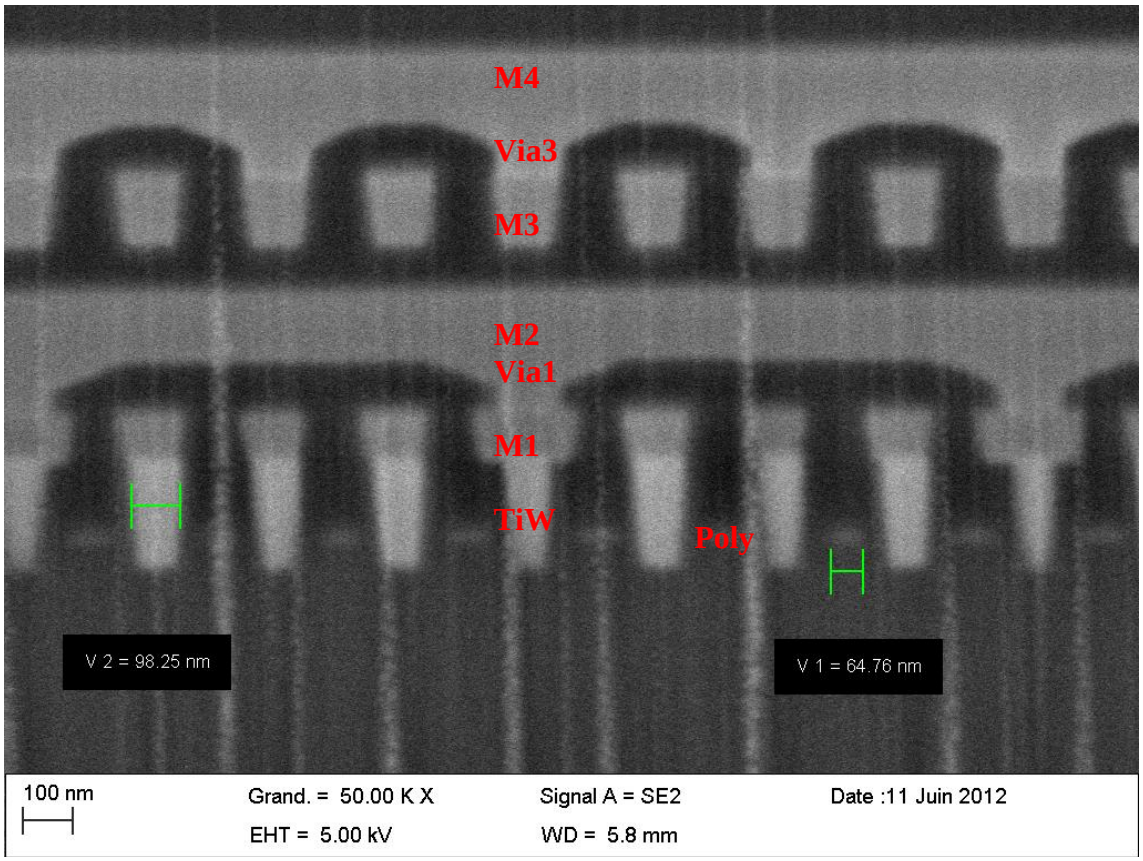


Figure 13: Zoom on transistor gates. Gate width is measured around ≈65nm.



5.1.3 Deprocessing

M10 and M9 layers

M10 level (aluminium made) is only used for pads.

The rest of the circuit has 9 copper (Cu) layers.

Large M9 Cu lines are only used for power distribution. The M9 layer obscures the functional blocks in the figure below.

Figure 14: ASIC general view trough passivation layer (M10 and M9 layers are visible). Chip dimensions and cross-section localisation.

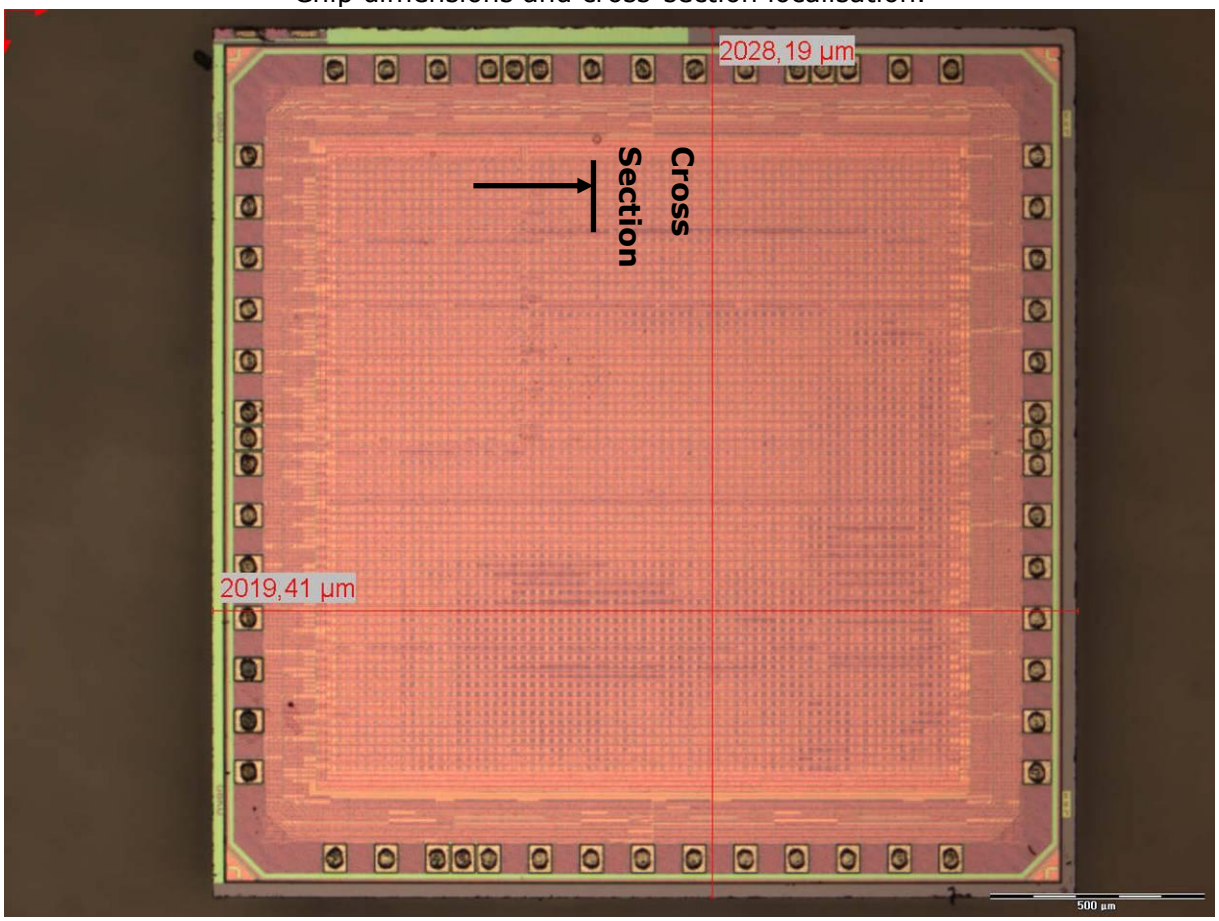


Figure 15: Pad level (M10 layer in Al)

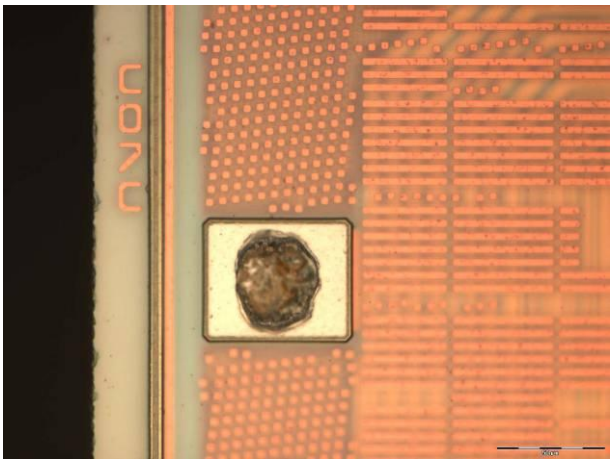
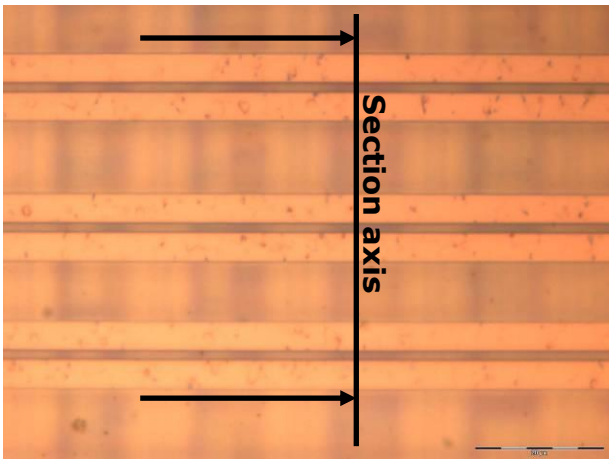


Figure 16: SRAM cells (M9 layer in Cu). Cross-section axis.



5.1.3.1 M8 layer

Few functional blocks start to appear at M8 Cu layer.

Most of M8 layer is used for metal fills.

Few M8 connections lines are present in the ring oscillator area. They are the first accessible internal signal lines available from top side analysis.

Figure 17: ASIC general view at M8 level.

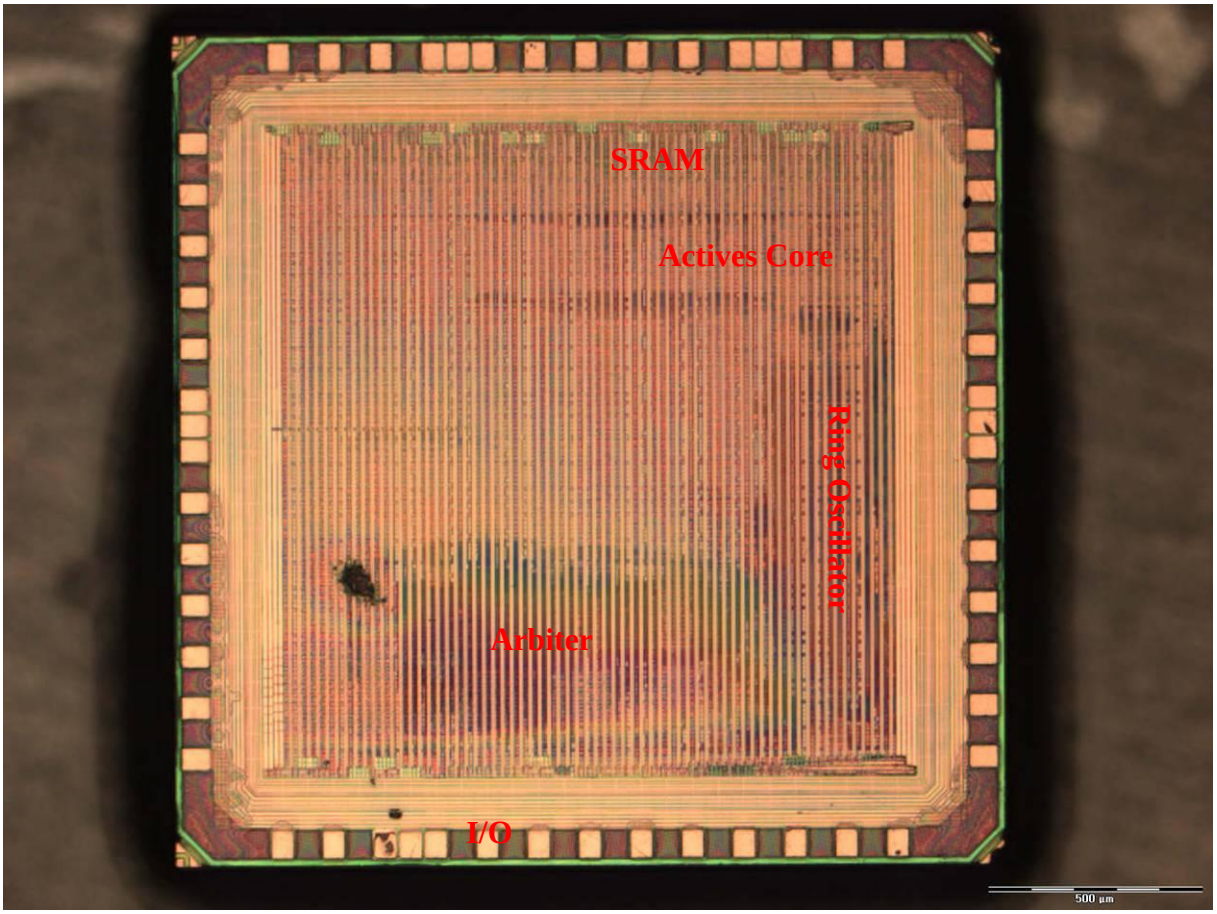


Figure 18:Ring oscillator Power line and some active signal lines (thinner ones)

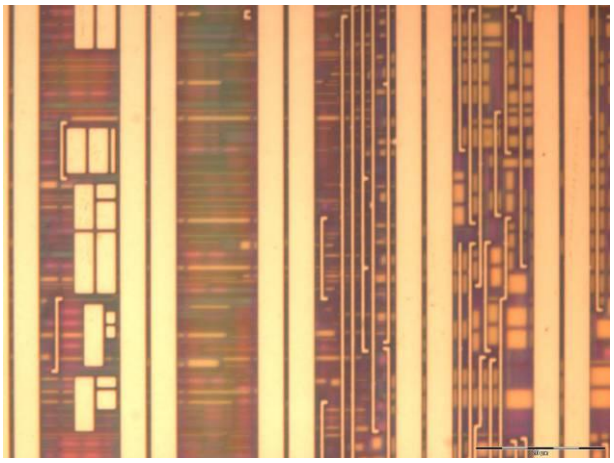
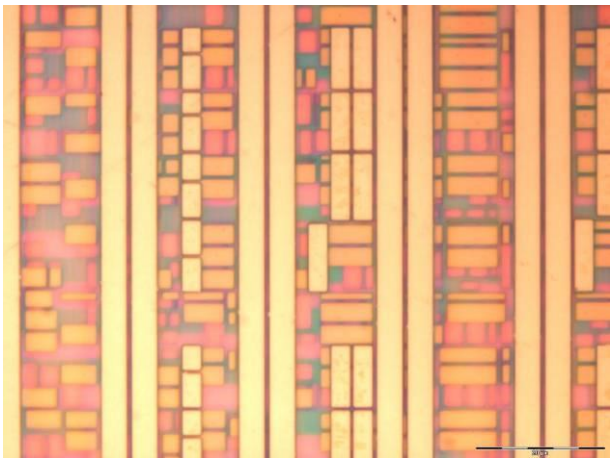


Figure 19:SRAM cells Only power lines and metal filling



5.1.3.2 M7 layer

Some functional blocks are visible at M7 layer: SRAM, arbiter and ring oscillator blocks are well defined. Ring oscillator seems to use M7 lines for driving useful signals. At M7 level, SRAM is still obscured with metal fills. Indeed SRAM cells generally need only three metal layers.

Figure 20: ASIC general view at M7 level.

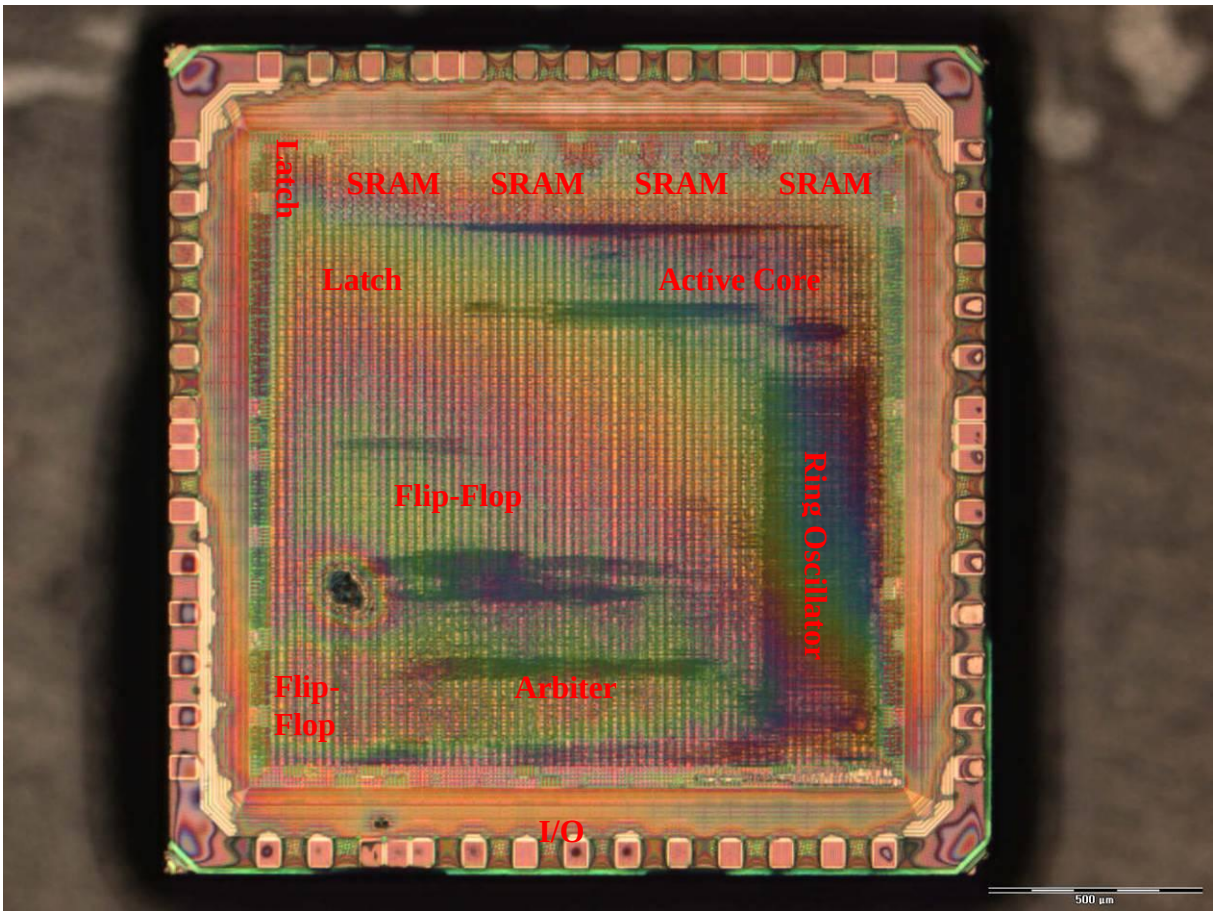


Figure 21:Ring oscillator

A lot of active lines over the area

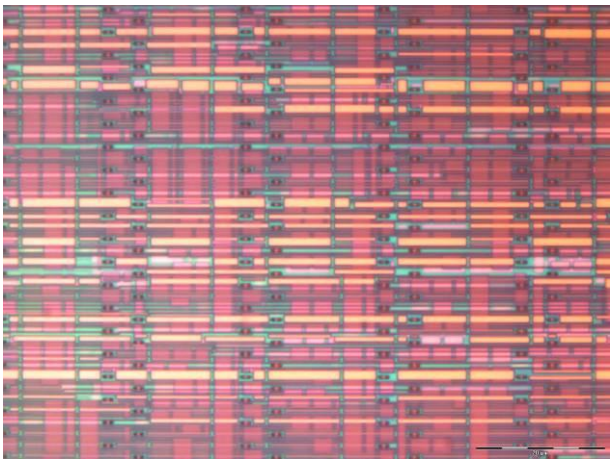


Figure 22:SRAM cells only metal filling and via for power distribution

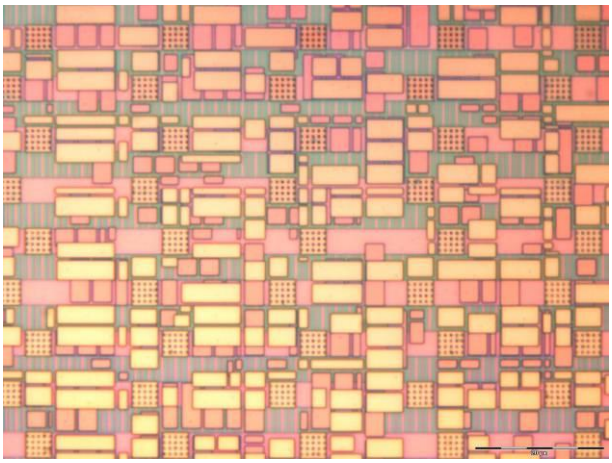


Figure 23: Ring oscillator. Useful lines at M7 layer.

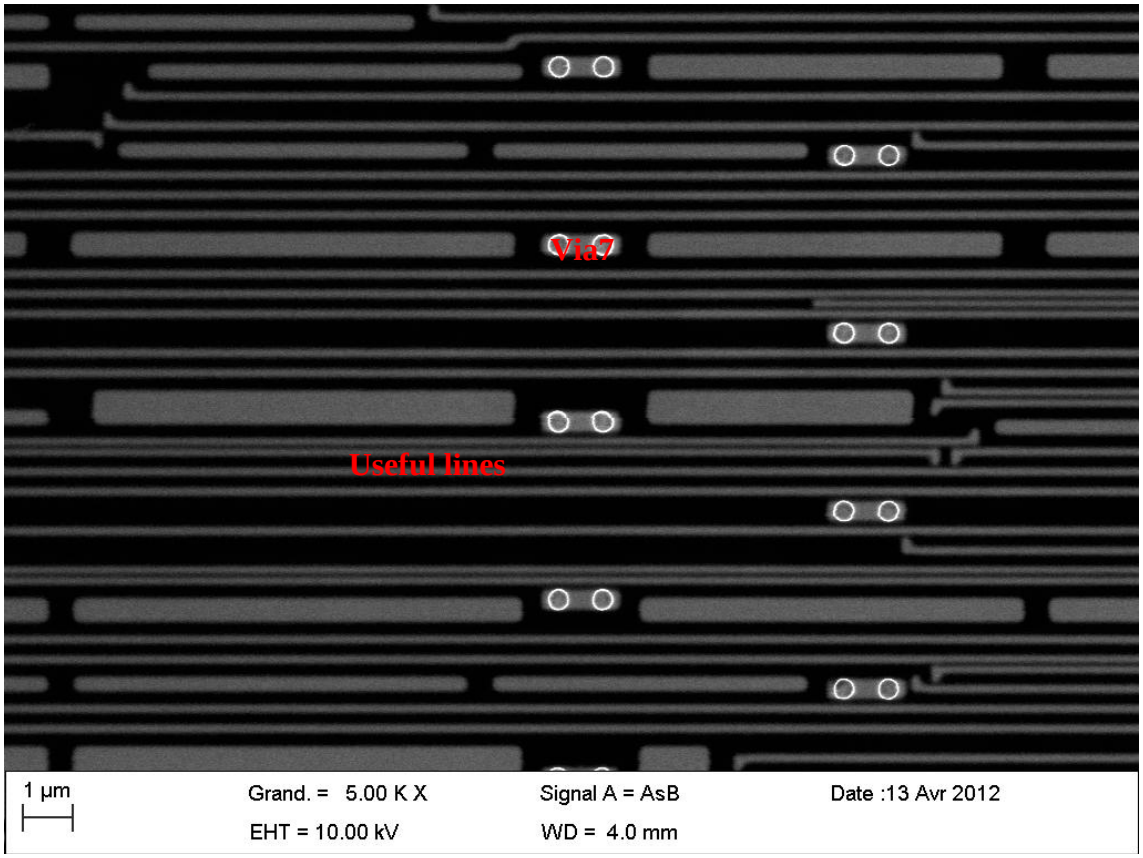
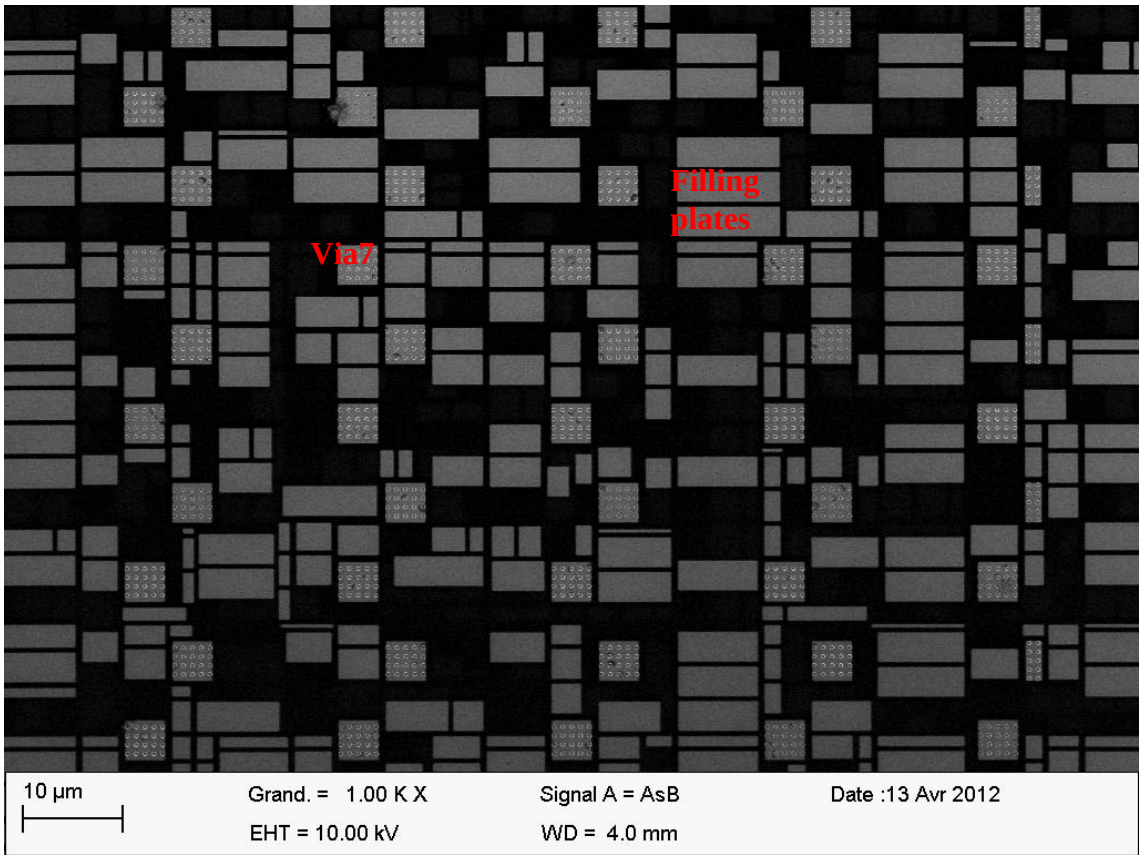


Figure 24: SRAM cells. Metal fills at M7 layer above SRAM cells.



5.1.3.3 Next metal layers

According to:

- the few samples (only 2 samples)
- and the process complexity on the other hand (9 Cu layers, advanced 65nm process node, very thin metal lines and vias)

it was impossible to obtain a nice preparation of the underlying metal layers (M6 to M1) on the whole surface.

Indeed, because of the small thickness of layers, plasma etching times (CF_4 + O_2 gas for removing inter-level dielectric) and chemical etching times (HNO_3 acid for removing Cu layers) must be very short. An overrun of a few seconds can be sufficient to over-etch the underlying layers and destroy any structures of interest. It is well known that the main problem with Cu technology is chemical infiltration because both lines and vias are made with Cu (no chemical selectivity possible between vias and lines).

The only way to solve this problem is to determine the best etching times by experiment, resulting to the destruction of sample after sample to finally reach the objective (intact layers).

For this aggressive ASIC technology, at least one sample per layer (10 samples in total) and a huge amount of time are necessary to adapt the preparation method and fully expose each layer. It would be difficult to accomplish but in principle possible.

5.1.3.4 Poly and active layers

The poly layer was reached by plunging the second chip (which is still at passivation level) into HF acid. HF acid etches all nitride and oxide layers (passivation and Inter-Level Dielectric ILD) in few seconds or minutes. As a consequence, metal layers and vias were lifted. By controlling the etching time, poly layers could be kept on active areas. During this preparation, most contacts were removed but poly lines were still there.

All functional blocks are visible at poly layer. Looking at the floor plan, blocks are easily identified at poly level.

Since the process node is very thin (65nm), gate details are not visible by optical microscopy (even with a 150X objective). So, each block was inspected by Scanning Electron Microscopy (SEM) at high magnification.

Figure 25 : ASIC general view at Poly layer. Functional block identification.

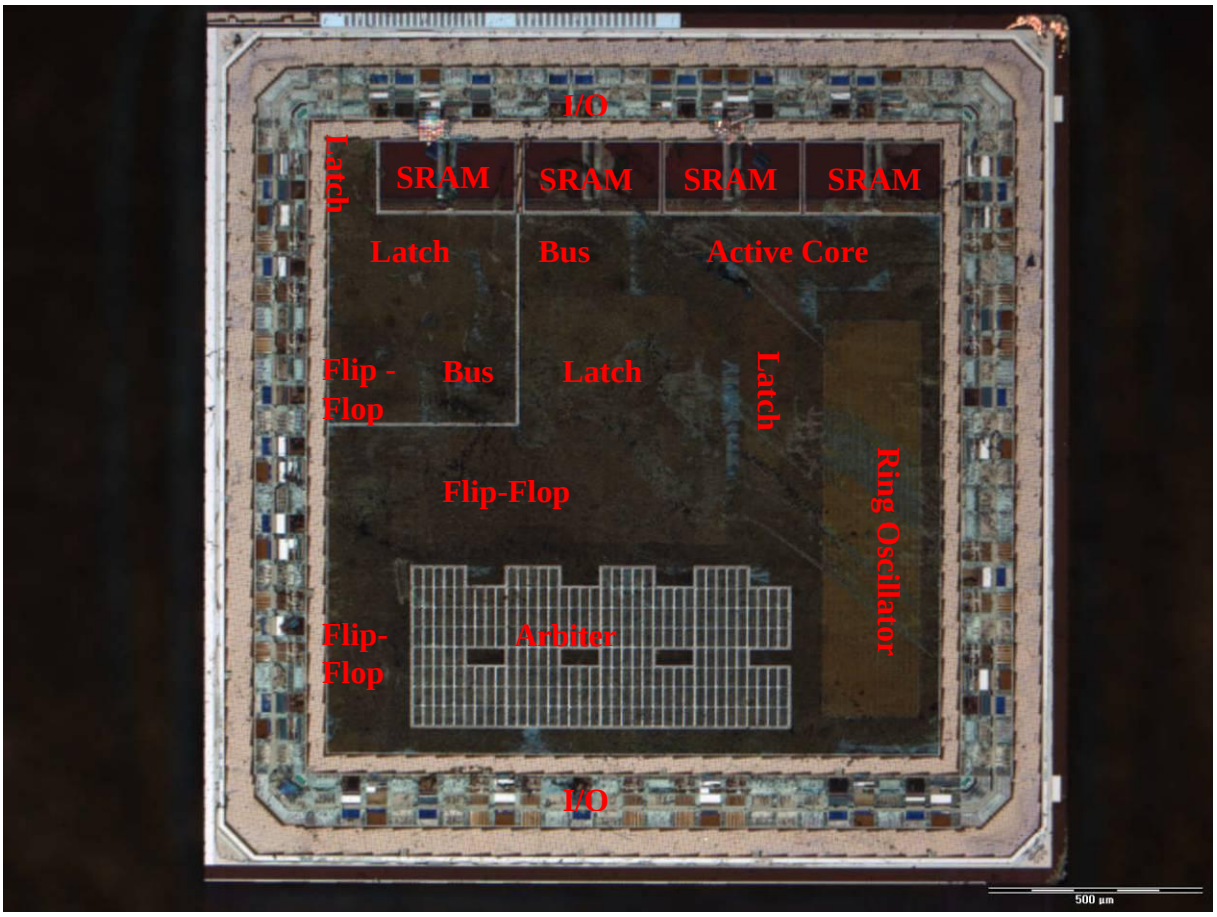


Figure 26: Floor plan

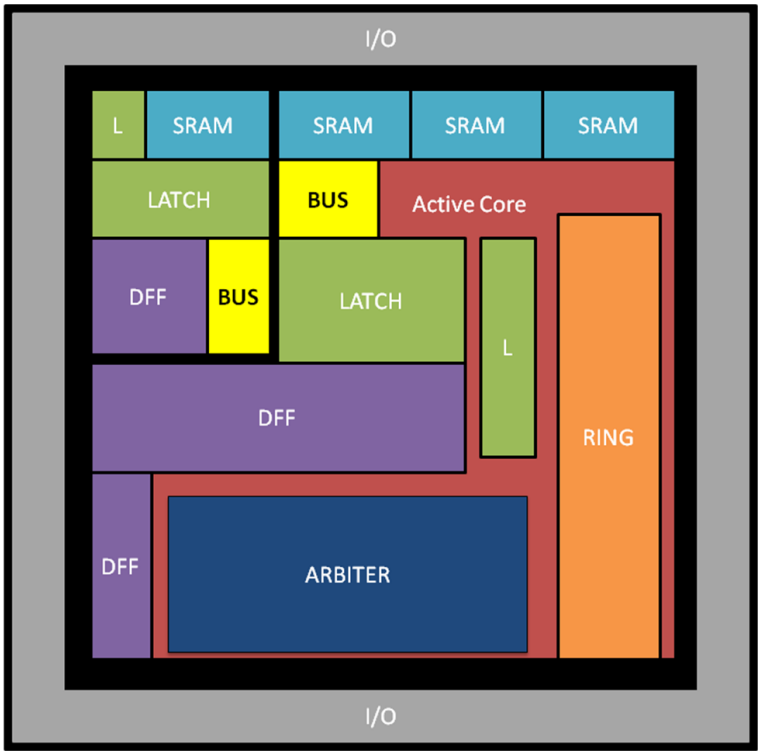


Figure 27: Latch cell

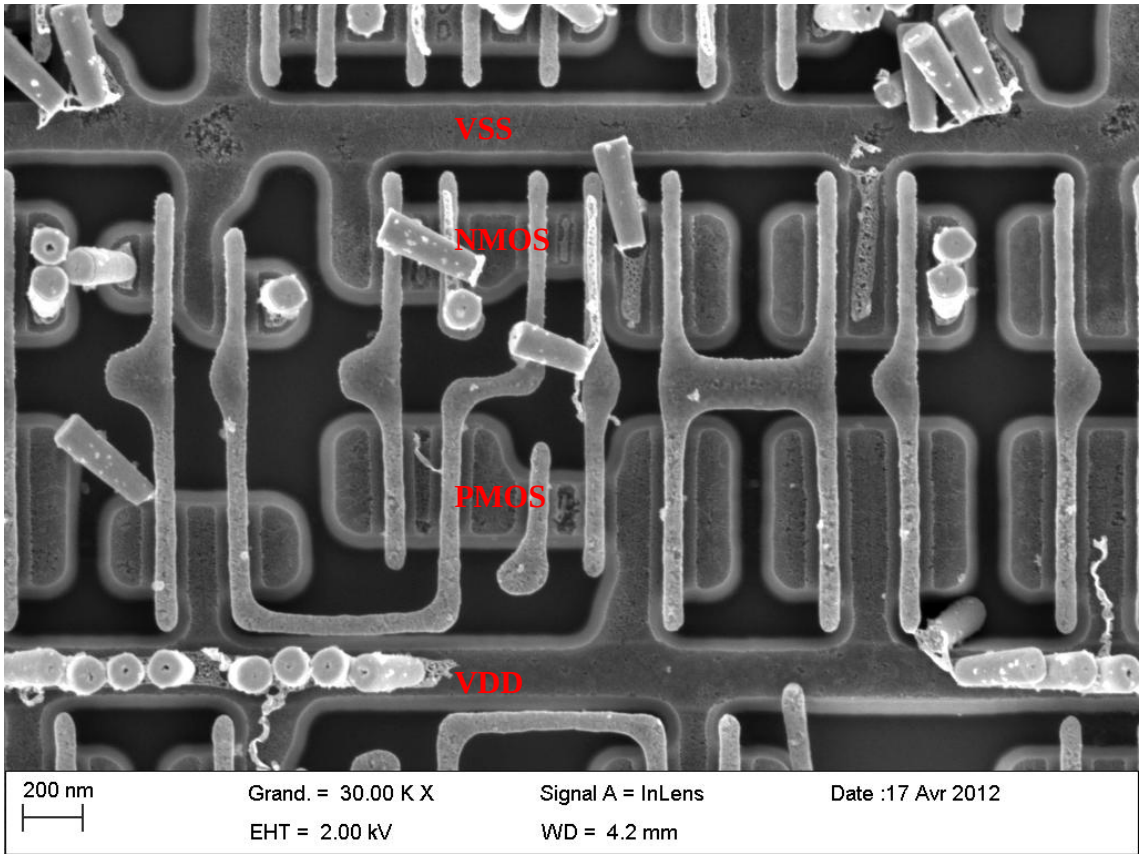


Figure 28: Ring Oscillator. Succession of inverters (one inverter = one PMOS + one NMOS)

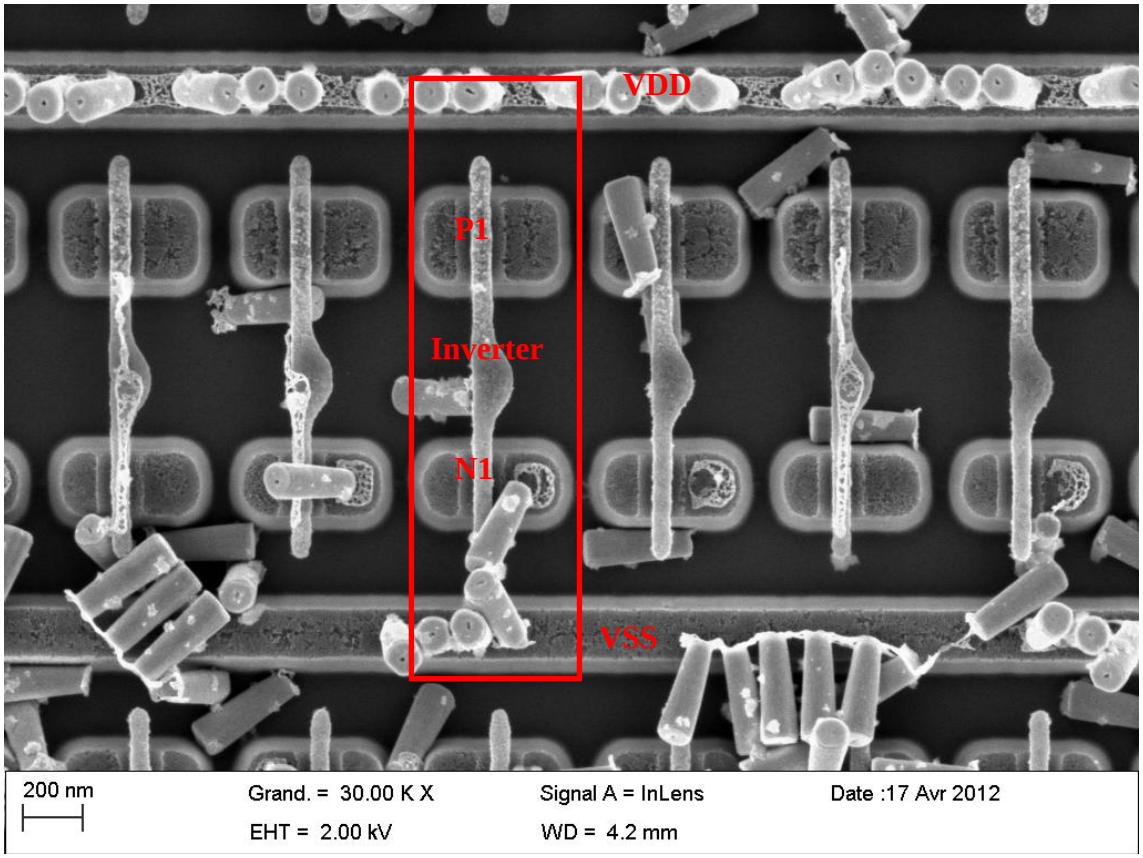


Figure 29: Flip-Flop cell

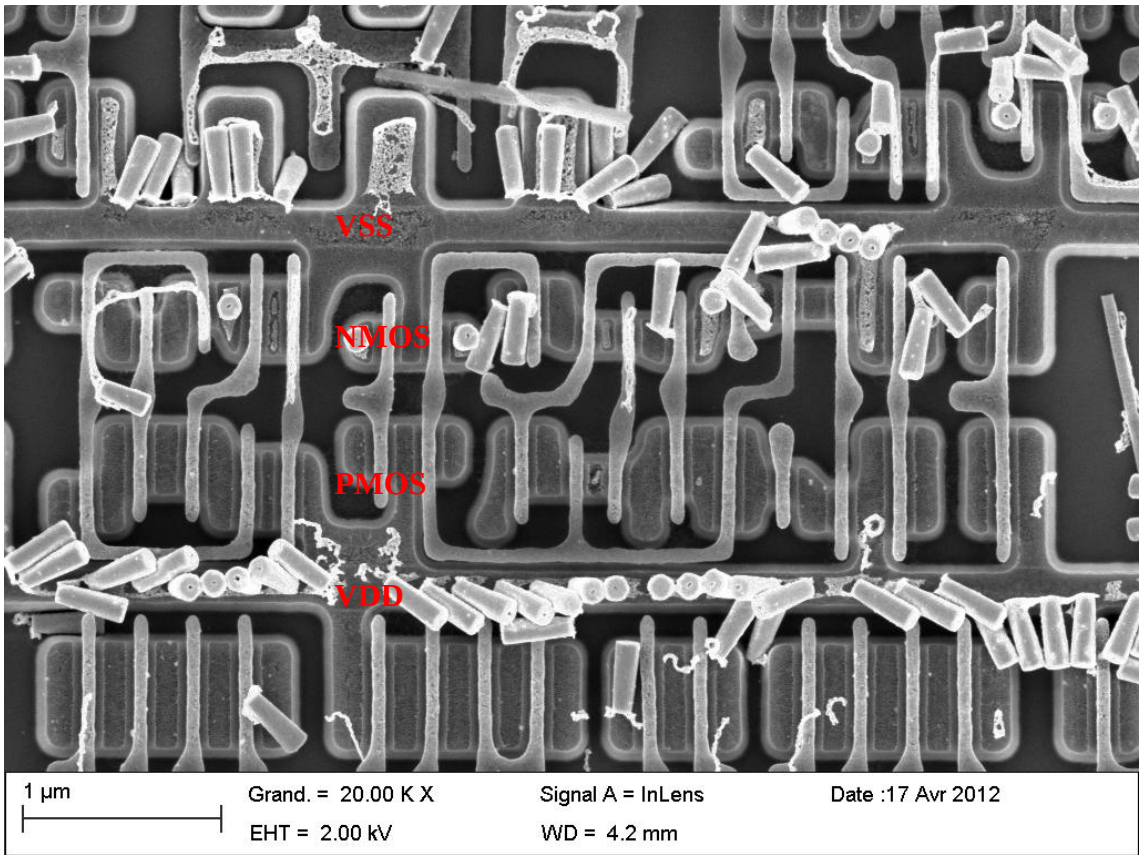


Figure 30: SRAM cell. Standard 6 transistors cell (see reverse in next paragraph).

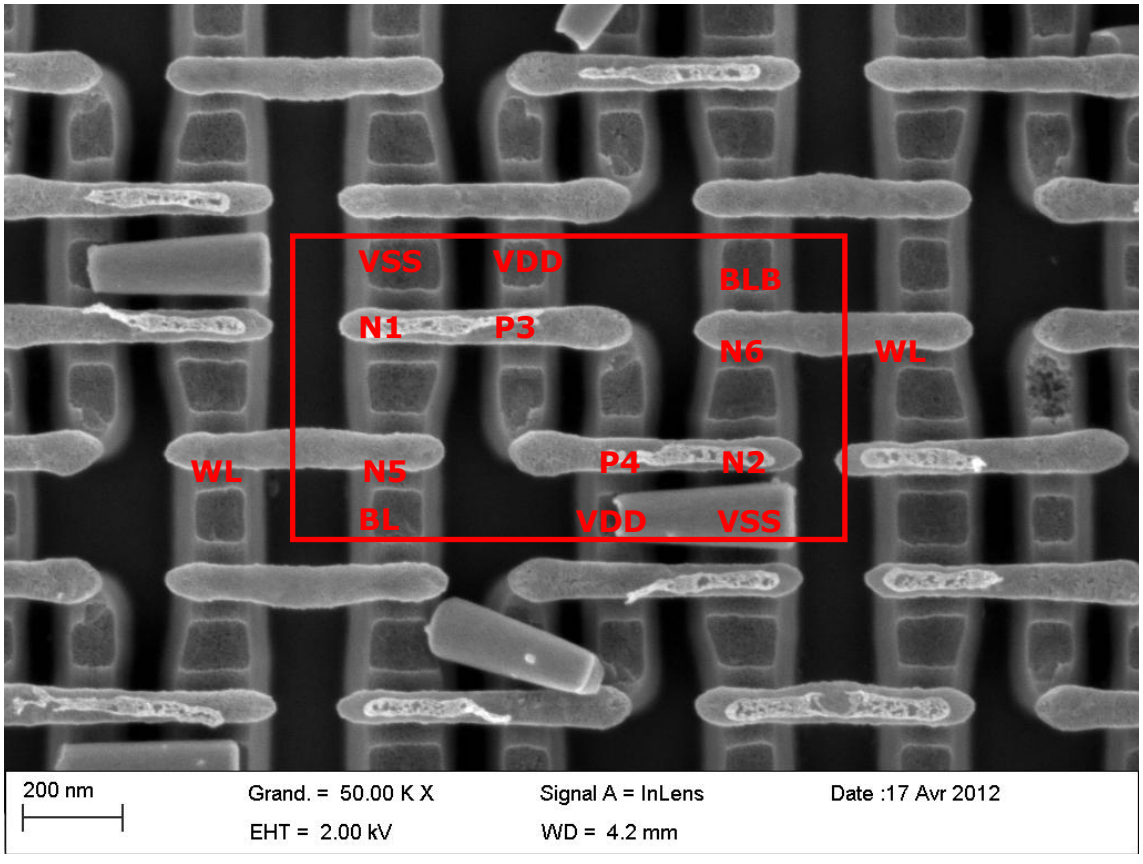


Figure 31: Bus keeper

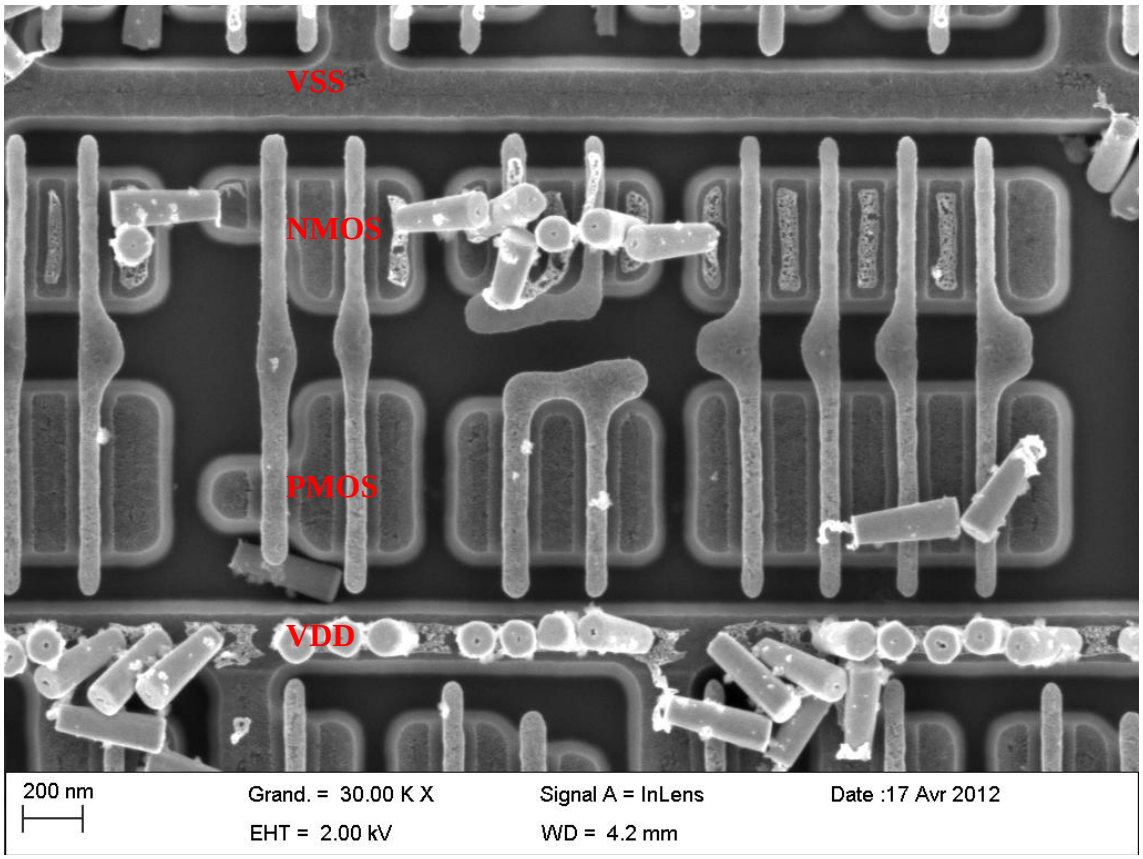


Figure 32: Arbiter. 12 transistors per cell (6 PMOS + 6 NMOS)

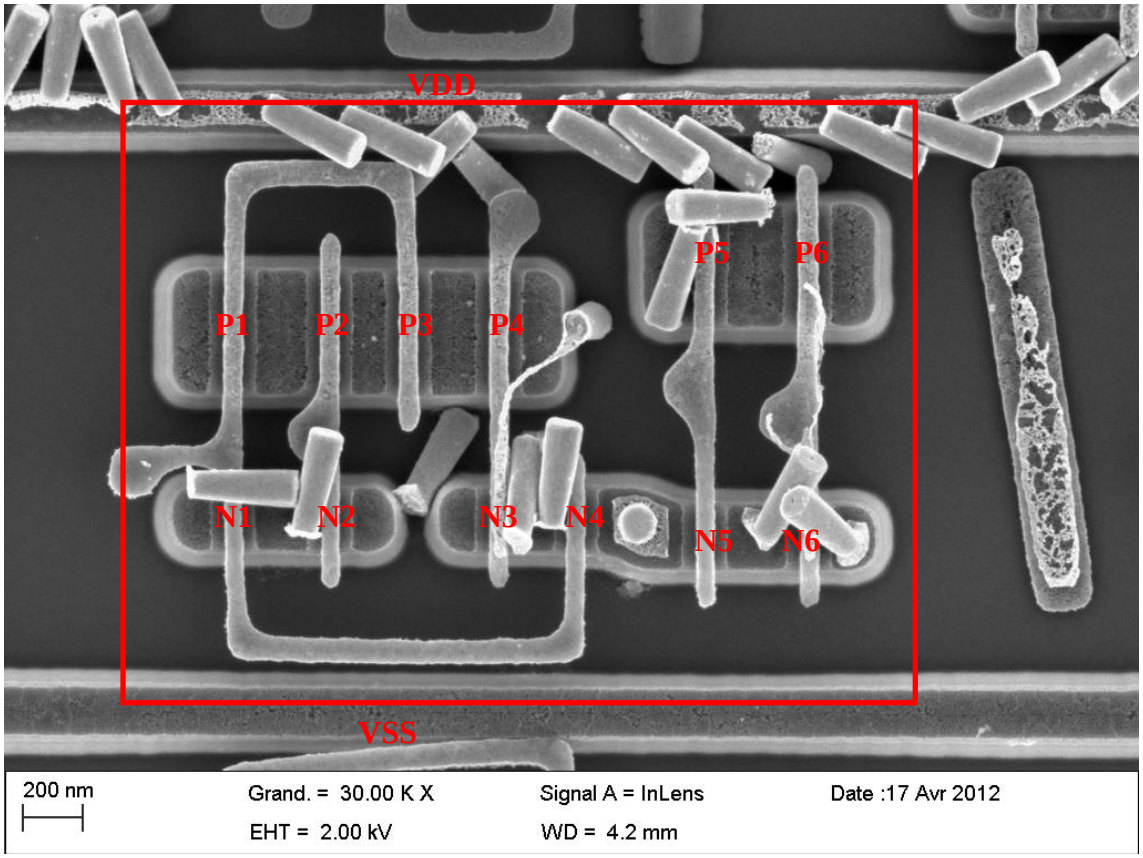
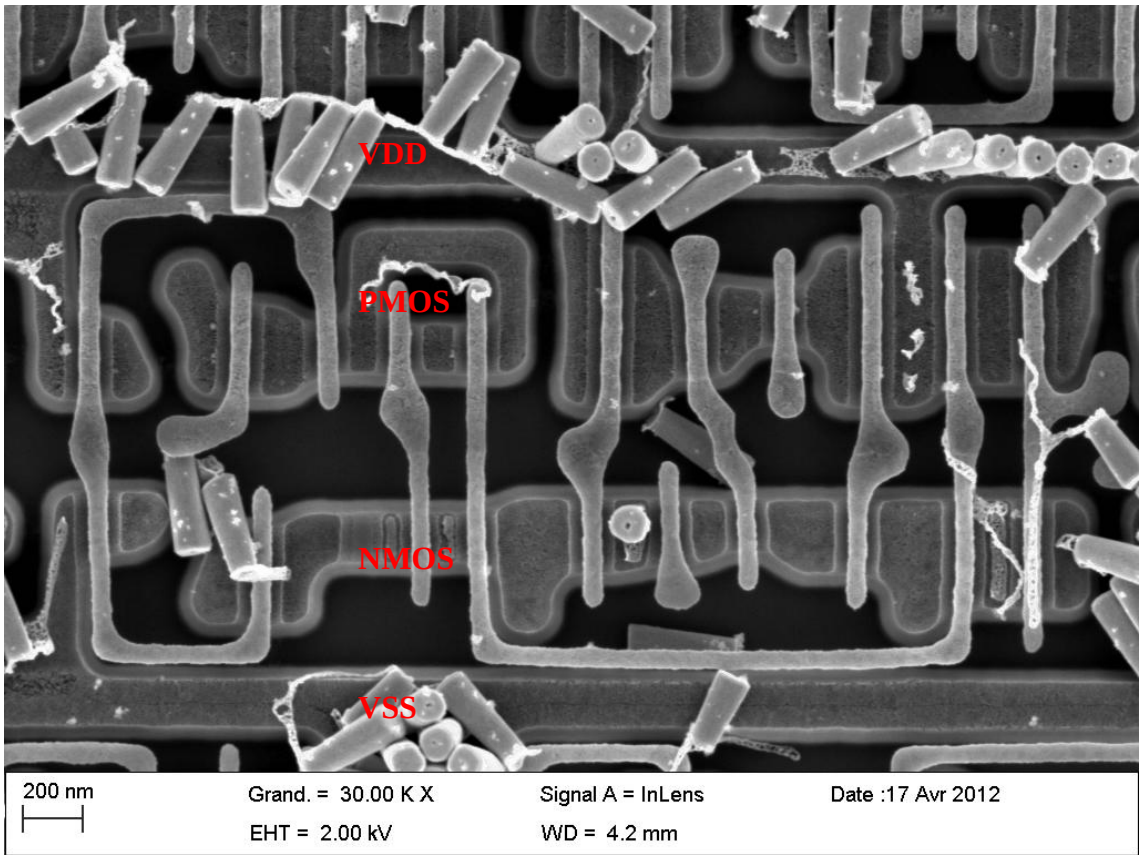


Figure 33: Active Core



5.1.4 Reverse of SRAM cells

For doing reverse engineering of cells, we need SEM pictures at each layer (poly and metals) at the same magnification. Each layer must be intact, that is to say no via or line missing. Pictures of all layers are then superimposed and the electrical design is deduced.

In our case, we only have a SEM picture of cells at poly layer. At this layer we could identify:

- Each transistor of a cell,
- Bit Line (BL), Bit Line Bar (BLB), ground (VSS) and power (VDD) contacts.

This identification implies that the ASIC uses a standard 6 transistors SRAM cell. Its design is given below:

- 2 access NMOS transistors : N5 and N6
- 2 storage NMOS transistors : N1 and N2
- 2 storage PMOS transistors : P3 and P4

The memory effect is performed by a flip-flop composed of two inverters connected to each other. The first inverter is N1 +P3 and the second is N2+P4.

This flip-flop cell is selected by two access transistors N5 and N6. Their drains are connected to the Bit Line (or BLB) and their sources to the flip-flop. Their gates drive Word Lines signals (WL).

Figure 34: Reverse engineering of SRAM cells. Identification of transistors and active areas.

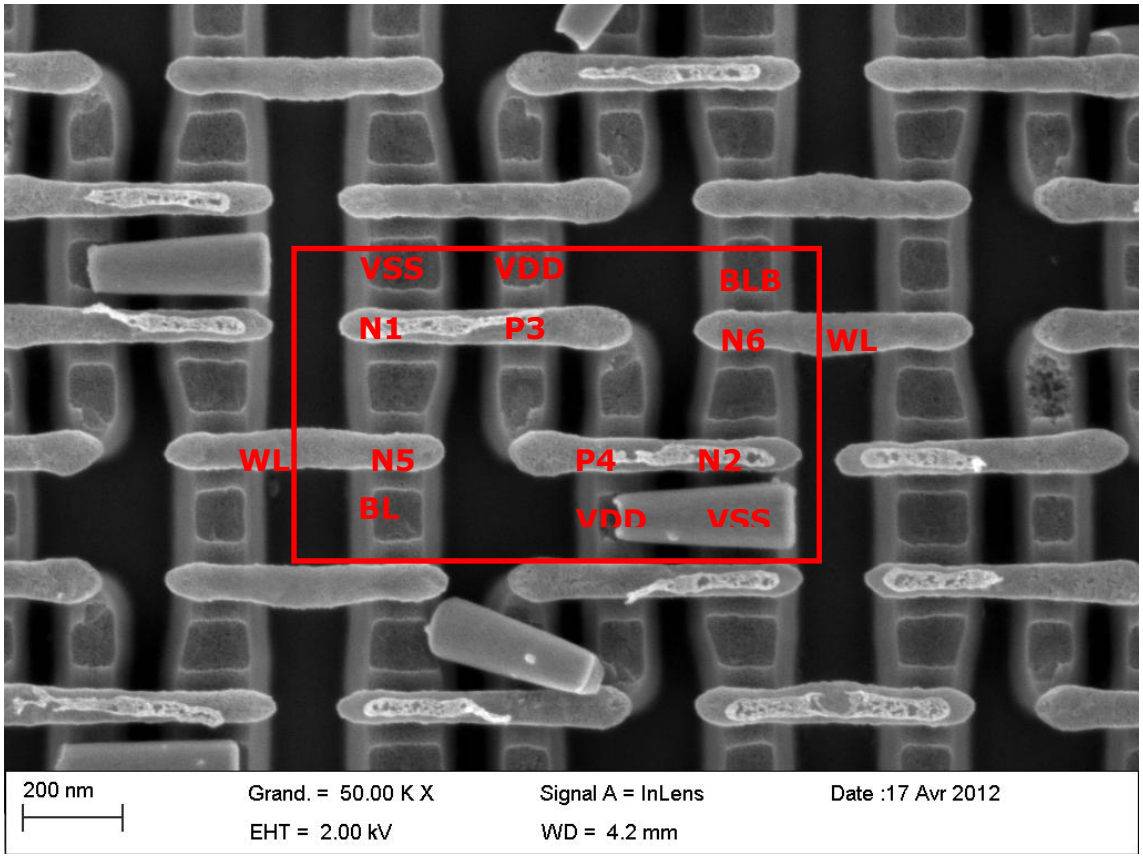
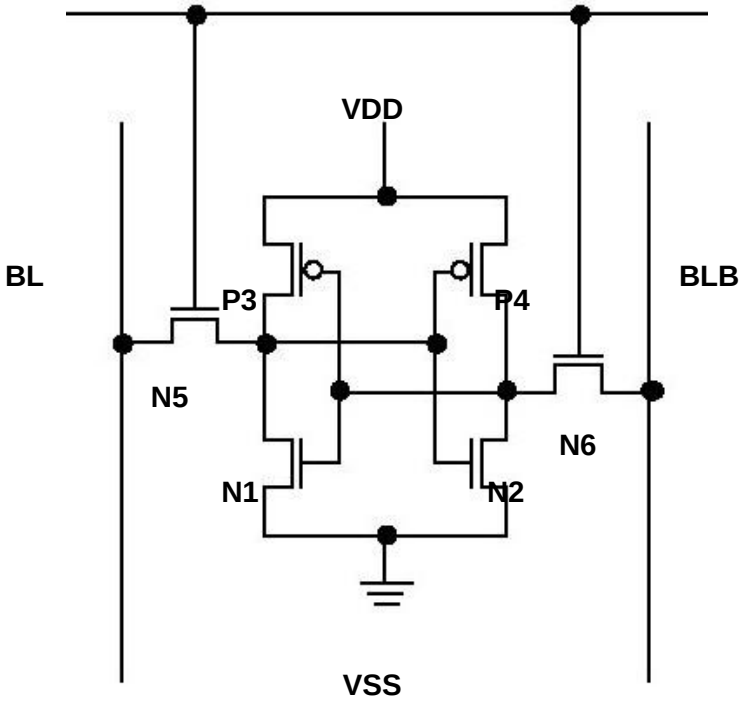


Figure 35: Deduced design of SRAM cells



5.1.5 Conclusions

As described in the previous chapters we did not perform a full reverse engineering task. The main limitation on this activity came from the technology used for the ASIC manufacturing. The device has been fabricated using a 65nm 10 metal layer technology. In order to make a complete sample preparation, more than 10 samples and several more months would have been necessary.

Nevertheless the partial reverse engineering performed allows highlighting some security issues.

The main observation we made deals with the capability from an attacker to identify which kind of PUF technology is used. Indeed some PUF technologies (mainly the ring oscillators and arbiters) require strong constraints in term of place and route to ensure that their final characteristics rely only on process variations and not on design. As a consequence they will be very easy to identify and localise on the final product. On the other hand, memory based PUFs will be much more difficult to identify. The SRAM based PUF will not induce any additional specific cells in the circuit since the same RAM will be use for normal operations. For Latch, Flip-flop or Buskeeper PUFs, they can be hidden in the whole logic and so be very difficult to identify.

5.2 PUF tamper evidence

One of the main claims of PUF security behaviour is that PUFs will respond to tampering such that any chip modification will cause a modification in the PUF response. The goal of this test scenario is to measure the real effect of tampering on the PUF response.

The test scenario is:

1) Measure the PUF response at T0 on normal operating conditions
2) Package opening (front side and back side on different samples)
3) Measurement of PUF response and comparison with initial data
4) Backside thinning (to around 50 µm)
5) Measurement of PUF response and comparison with initial data

PUF tampering is performed by different steps:

- chemical for frontside opening
- mechanical for backside opening and Si thinning
- Fib milling for ultimate thinning

5.2.1 Package opening

Three UNIQUE ASIC devices were given for FIB attacks:

- One is used for front side opening
- Two are used for backside opening

5.2.1.1 Frontside opening

Standard frontside chemical decapsulation does not keep device functionality because bonding wires are Cu made. Indeed, hot HNO_3 acid etches Cu very fast.

Figure 36: Package top view

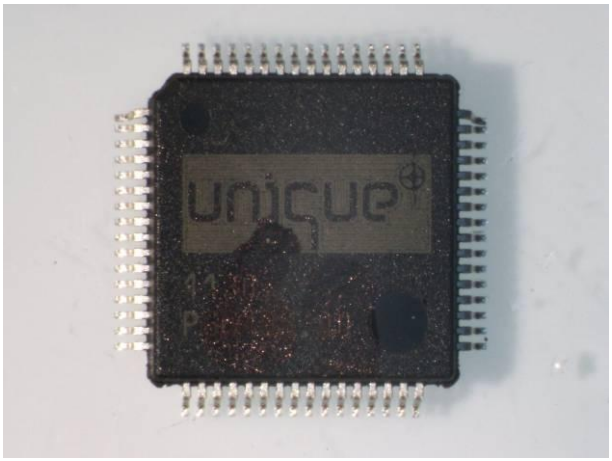
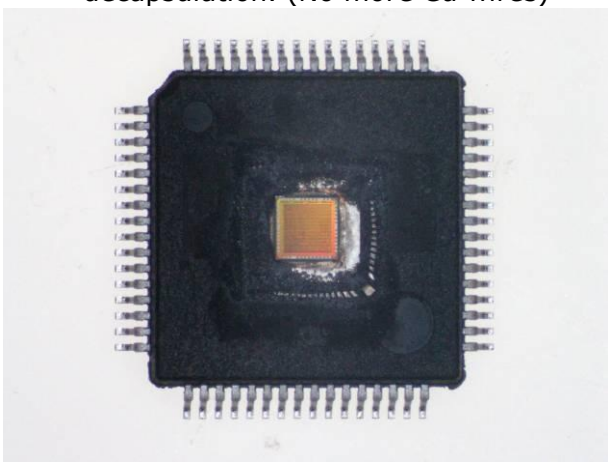


Figure 37: Package after front side decapsulation. (No more Cu wires)



For Cu wires, a new decapsulation system must be performed with HNO3 at 10°C. This method needs lots of devices to find the good recipes.

In this case, it was impossible to work on a functional device with front side opening.

5.2.1.2 Backside Opening

To keep functionality, a backside preparation is selected for EMMI and FIB attacks. Backside opening is done by mechanical polishing with the ASAP machine.

The method to make a backside opening is described below:

- RX inspection of the device allows precise die localisation.
- Laser marking on package with SESAME for precise alignment
- ASAP package opening
- ASAP Cu lead frame opening
- Cleaning and SI precise measurement by PHEMOS (thickness device 225µm)
- ASAP Si thinning.

Figure 38: RX image for backside opening localisation

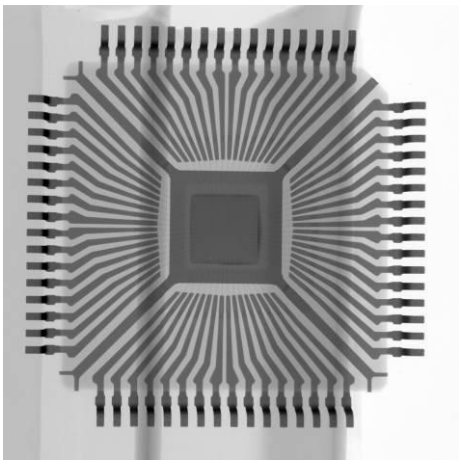
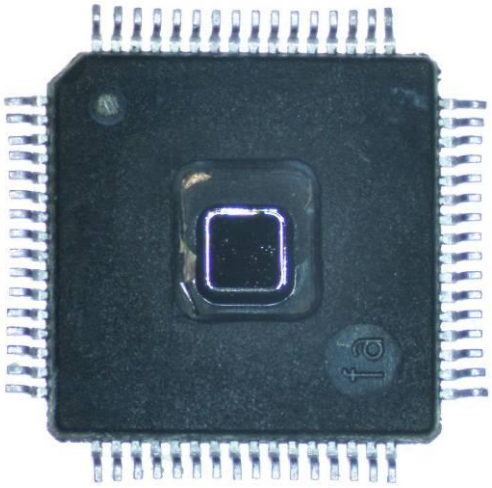


Figure 39: Package after backside opening.



Two devices are prepared for backside analysis.

First device: Package opening and substrate thinning up to a remaining 25 µm of silicon

Second device: Package opening and substrate thinning up to a remaining 50 µm of silicon

For those two devices the PUF response was measured at T0 on normal operating conditions and after package opening.

First device (25µm thickness):

Table 17: Comparison of PUF reading before and after backside opening and thinning at 25 µm

PUF response at t0	PUF response after backside thinning
-- DUMP FULL RO PUF 00, 000, 000000FF, 000000D3 01, 000, 000000FF, 000000D2 …… -- DUMP LATCH PUF 1 CF77D5EBFEC7DBBC78F5BDD6FFF17FB37FCDBB3FFE53 B76EBB53BA77FFFE7C3F FB94F473FD6BB3BDABF47ADEDF7FBF77FFBF1EDFFFAFB A6EEFD7F5BFEBB7BBFB … -- DUMP SRAM PUF 4 5F53552601AA507CFFE927C21193E0B84FFAFC38BA425 D7DD0EF66D348E7C019 E2F2DD920DB124CE90FB7E05FEA344D10DFFB7E7B890 D86EB5226F364968286E …… -- DUMP DFF PUF 1 E519ED13FCFAF5866C5AEF4FE6717BA873F0AE94F7E49 B3775F1BF1EFE7E297F E66D7F4EF191FEF7DE737D3F91955B785F2EF73AA4B11 F1EFC7FE279BCCDFD1E … -- DUMP ARBITER PUFs 54018A25 …… -- DUMP BUSKEEPER PUF 1 97EB72FD873E3E6D988518D6CE74F7931F7D741FAE7E 55112CE09870CFA3323C D40DD554E86EA3B81357D5AC08986F6D44C80FDBAE0F 5A32A7621AB78495CC6C	-- DUMP FULL RO PUF 00, 000, 000000FF, 000000D3 01, 000, 000000FF, 000000D1 ….. -- DUMP LATCH PUF 1 CF7750EBFEC6D3BC78F59DD7FFD16A937FADBB3 D3E53B76EBB73B876FFFE743F FB957473FD6BB3BDBFFC7ADE5F79FF77FFAF16DF FBBFB87FEFD7F526EBB79BFA … -- DUMP SRAM PUF 1 356045ACF13495C6A3E372DEC74E78D71D606F0 73D48DF81ECBEF136764B60BB 35FFC6262B6B85148574CA19375648C34262F353 5D36C2C124BF65B43AB6E9AB …….. -- DUMP DFF PUF 1 EF9DFD73FCFAF7CEEC5AE74FE7773BA87BF08E94 E7E49B3775F9BFFEFE7EAB7F F6E9FF4EF197FEF7DE7FFD3F9B955BFB5F2EFF3BA 5F7DF1EFD7FE279FCCFFF5E …. -- DUMP ARBITER PUFs 1401CA34 …. -- DUMP BUSKEEPER PUF 1 87AB72FD072E3E6D989508D6CE9476931F5D701 EAA3C551124E0B870CE23222C 500DD550E84E23381151D5AC08886E4D40480ED BAC075A30A7621AB40005CC4C

Second device (50µm thickness):

Table 18: Comparison of PUF reading before and after backside opening and thinning at 50 µm

PUF response at t0	PUF response after backside thinning
-- DUMP FULL RO PUF 00, 000, 000000FF, 000000D5 01, 000, 000000FF, 000000D4 …… -- DUMP LATCH PUF 1 F79A1DFFFD7FDEEDF571FC7BBEFFDDBFD5DFFB6FEFFF46E5DDB414BFBDE737FF F7FDD377F6FFCE9FF1CEFBFEDCDB4CFF73F37B2B67FBEDB7FDE7BB3DFE7FB7C7 … -- DUMP SRAM PUF 4 72BA3C3B1302539FB0F44479A7B7F4CA81E0C9FCE158B8B2535D242EF4F5C2FB F14460595FD61D79013E303851FC98AABA9A145BFCA7F5B5EB31F925846451CF … -- DUMP DFF PUF 1 C1623EC1110347B804FC51F472C647060792915511BB806CB8B0410D08F989A4 17D198454B564D408AC637C671736856A88657FB2A2864544A7A81F977365835 … -- DUMP ARBITER PUFs 00002212 086451A9 … -- DUMP BUSKEEPER PUF 1 086451A9CE62F635A43867957C678A70500EAA0CC14945E6D47E82F51D5A059C C0552A0BF2213220394298B00999488011153E18D53CC03441082A9B94F5524A …	-- DUMP FULL RO PUF 00, 000, 000000FF, 000000D5 01, 000, 000000FF, 000000D4 … -- DUMP LATCH PUF 1 F79ADDFFFD3FCEEDF571FC7BBFFFFDBEF5DFFB6FEFFF46E5DDB424BFBDE737FF F7FDD377F6FFCE9FF1CEFBFEFCDA4CFF73F37B2BE7FBE9B7FD679B3DFE6FB7C7 … -- DUMP SRAM PUF 4 6AFA383B130253DFB8F44479A7B7F44A80E0C9FCE15DB9B2535D242AF4F582FB F164605D5FD61F79013E303859FC98AABC9B945BFCA7F1B5EB307927846459CF … -- DUMP DFF PUF 1 CBF37EFBB9EBC7BCB4FCB7FFFFD7FFEF27B2DFFD7DBB5B7FBE95C12F2AFBB9A4 1FD3FE714BDF5DEEFFF73FF67773EBD6FEDFDFFBFF2A6F5F6F7BCFFFFF3E79FD …… -- DUMP ARBITER PUFs 08002211 086459A9 … -- DUMP BUSKEEPER PUF 1 086459A9CE42FE35A43867955C278A70104EAA0CC14945E6DC5E82F51D5A059C D0552A4BF221222019C29890099948C011153E18D53CC03449082A9B84F5524A

To conclude our analysis, it can be noted that for the two devices analyzed, RX inspection, SESAME laser ablation and ASAP Si thinning did not change the PUF response.

5.2.1.3 Backside Fib ultimate thinning

The OPTIB from DCG System is a Focused Ion Beam especially developed for frontside and backside design modifications. The Ion beam is assisted by different gases which allow milling selectivity:

- X2F2 for oxide and silicon milling
- I2 for Aluminium milling
- NH3 for copper milling
- Pt for metal deposition
- SiOx for oxide deposition

Frontside modifications are not presented in this part because of the difficulty to prepare a sample (Cu wires).

Indeed only backside ultimate thinning are presented on three different places of the device. Ultimate thinning means that on a 200µm*200µm box the Si thickness is less than 4µm; this allows to see the actives layers by transparency. This is the last step before setting test points / performing design modifications with FIB.

5.2.1.3.1 FIB ultimate thinning on the RING

The device is prepared by mechanical thinning first up to a thickness of the sample's bulk of 25µm.

The response of the PUF is measured first after ASAP thinning and for a second time after FIB milling.

Figure 40: Floor plan ASIC for FIB box localisation

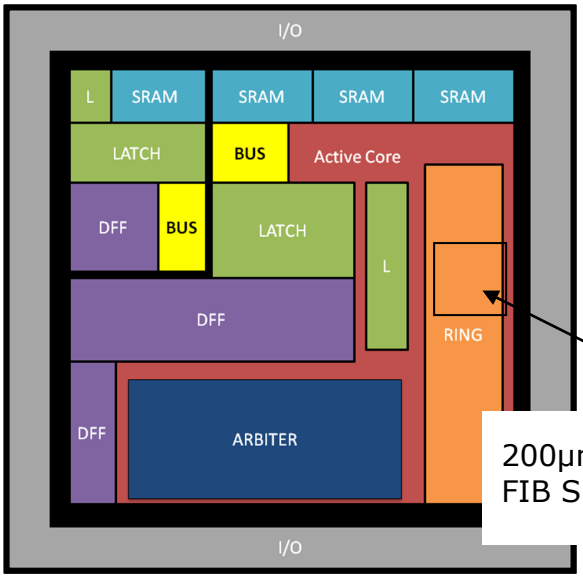
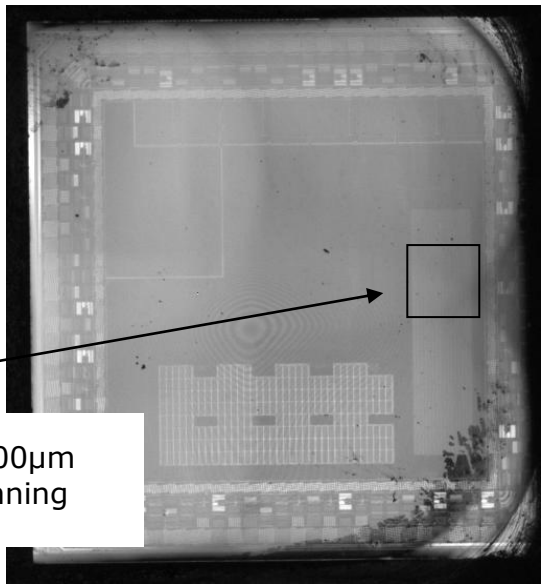


Figure 41: Backside laser image for FIB box localisation



The images below show the process of a FIB backside ultimate thinning:

The FIB contains different filters which allow seeing by transparency the structure under the Si. Photos bellows show ionic and optical image of the ring. This step is to clean the Si surface by 6 cycles of Ion milling and I2 milling.

Interference fringes indicate the topography of the surface and the thickness of the Si.

Figure 42 : FIB image of the 200µm*200µm Si surface on the ring

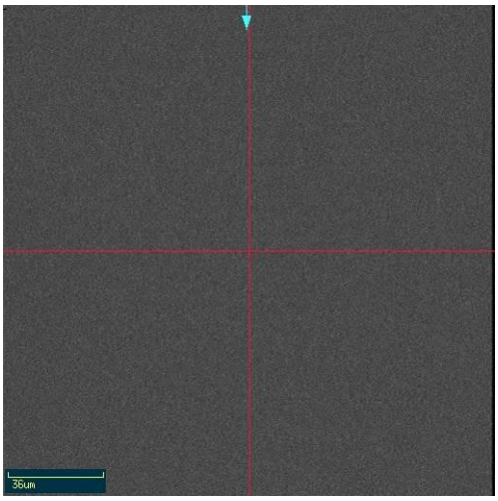
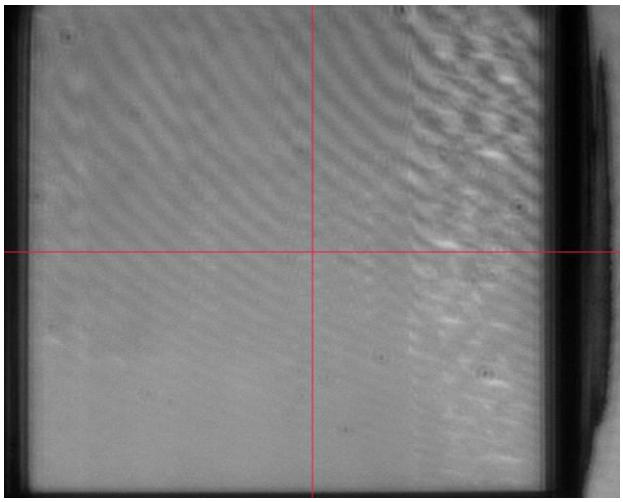


Figure 43 : FIB optical image of same zone: 1000nm filter allows to see by transparency the structure of the ring



After 35 min Ion milling assisted by X2F2 gas, the interferences fringes appears with the 500nm filter (means that Si thickness is less than 4 µm) and the structure of the die begins to appear on optical image through the remaining silicon even on visible light (500 nm optical filter).

Figure 44 : FIB image of the 200µm*200µm Si surface of the ring (structure appears)

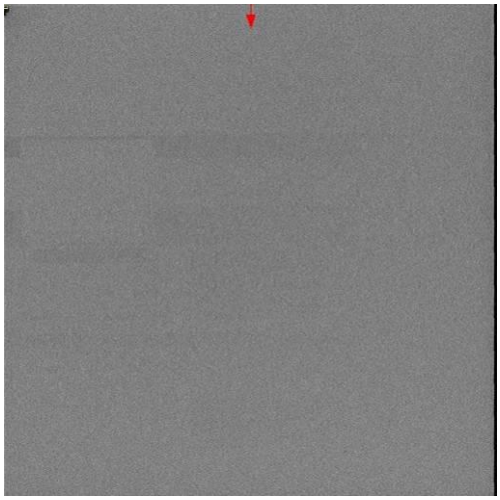
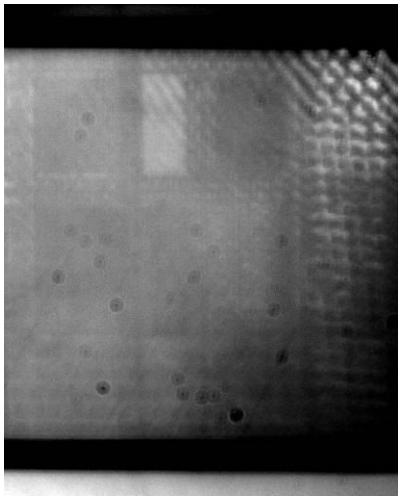


Figure 45 : FIB optical image of same zone :500nm filter allows to see by transparency the structure of the ring



Next step is oxide deposition which allows trench protection but also reveals nwells.

Figure 46 : FIB image of the ring ultimate thinning after oxide deposition

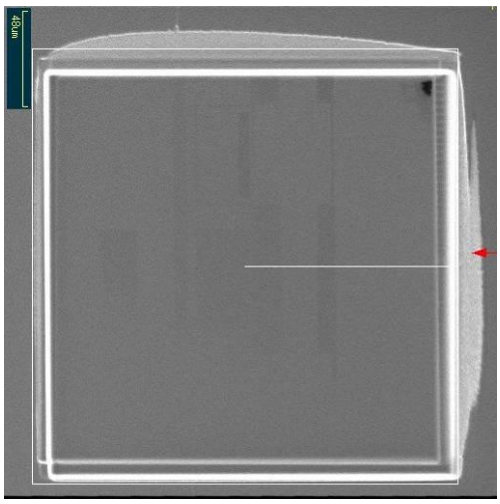
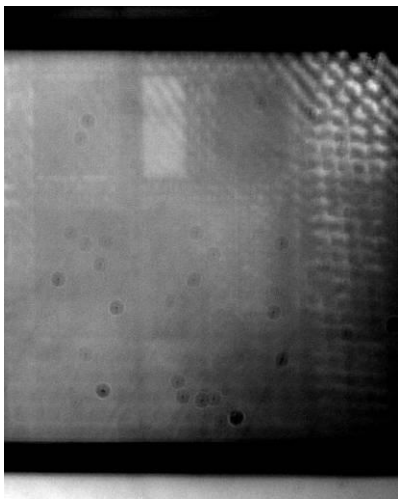


Figure 47 : Optical FIB image of the ring ultimate thinning



The PUF response is measured after FIB milling and compared with measurements after ASAP thinning.

Table 19: Comparison of RO PUF reading before and after FIB ultimate thinning

PUF response after asap milling	PUF response after FIB backside thinning
-- TEST CODE : -- DUMP FULL RO PUF 00, 000, 000000FF, 000000D3 01, 000, 000000FF, 000000D1 02, 000, 000000FF, 000000D5 03, 000, 000000FF, 000000D5 04, 000, 000000FF, 000000D3 05, 000, 000000FF, 000000D1 06, 000, 000000FF, 000000D2 07, 000, 000000FF, 000000D2 08, 000, 000000FF, 000000D3 09, 000, 000000FF, 000000D4 10, 000, 000000FF, 000000D3 11, 000, 000000FF, 000000D3 12, 000, 000000FF, 000000D3 13, 000, 000000FF, 000000D5 14, 000, 000000FF, 000000D0 15, 000, 000000FF, 000000D2 …… 00, 255, 000000FF, 000000D0 01, 255, 000000FF, 000000D1 02, 255, 000000FF, 000000D1 03, 255, 000000FF, 000000D3 04, 255, 000000FF, 000000D2 05, 255, 000000FF, 000000D3 06, 255, 000000FF, 000000D4 07, 255, 000000FF, 000000D5 08, 255, 000000FF, 000000D4 09, 255, 000000FF, 000000D3 10, 255, 000000FF, 000000D2 11, 255, 000000FF, 000000D4 12, 255, 000000FF, 000000D4 13, 255, 000000FF, 000000CF 14, 255, 000000FF, 000000CF 15, 255, 000000FF, 000000D0	-- TEST CODE : -- DUMP FULL RO PUF 00, 000, 000000FF, 000000D2 01, 000, 000000FF, 000000D2 02, 000, 000000FF, 000000D4 03, 000, 000000FF, 000000D5 04, 000, 000000FF, 000000D3 05, 000, 000000FF, 000000D1 06, 000, 000000FF, 000000D1 07, 000, 000000FF, 000000D2 08, 000, 000000FF, 000000D3 09, 000, 000000FF, 000000D3 10, 000, 000000FF, 000000D3 11, 000, 000000FF, 000000D2 12, 000, 000000FF, 000000D2 13, 000, 000000FF, 000000D5 14, 000, 000000FF, 000000CF 15, 000, 000000FF, 000000D2 … 00, 255, 000000FF, 000000D0 01, 255, 000000FF, 000000D1 02, 255, 000000FF, 000000D1 03, 255, 000000FF, 000000D2 04, 255, 000000FF, 000000D2 05, 255, 000000FF, 000000D3 06, 255, 000000FF, 000000D4 07, 255, 000000FF, 000000D5 08, 255, 000000FF, 000000D4 09, 255, 000000FF, 000000D3 10, 255, 000000FF, 000000D1 11, 255, 000000FF, 000000D4 12, 255, 000000FF, 000000D4 13, 255, 000000FF, 000000CF 14, 255, 000000FF, 000000CF 15, 255, 000000FF, 000000D0

The observed variation does not overcome one bit and is comparable to the measurement noise observed when making the same measurement twice on a fresh device.

To conclude, the ultimate thinning on the ring does not change the PUF response significantly.

5.2.1.3.2 FIB ultimate thinning on the SRAM2

The same process as outlined in section 5.2.1.3.1 is done on the SRAM2. The pictures below show the results: the same device is used to find if there is a limitation in the number of FIB trenches.

Figure 48 : Floor plan ASIC for FIB box localisation

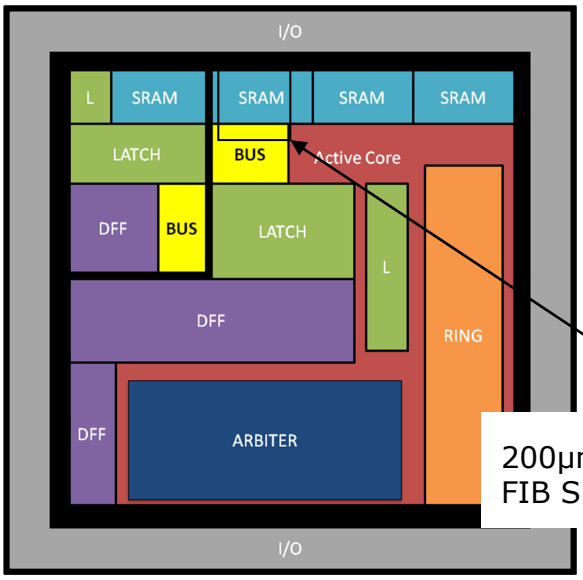


Figure 49 : Backside laser image for FIB box localisation

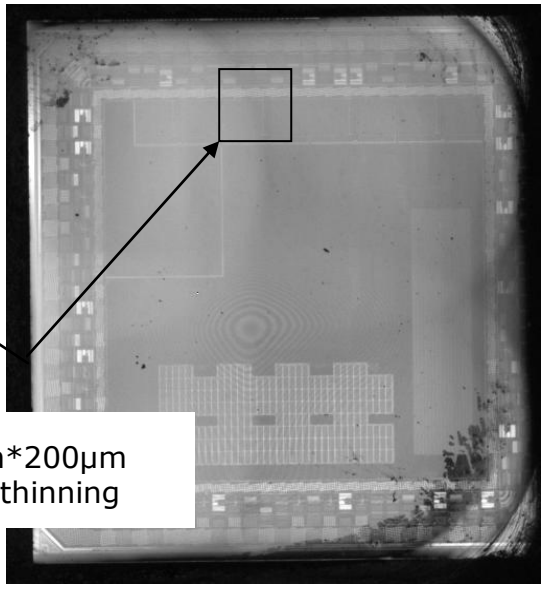


Figure 50 : FIB image of the 200µm*200µm Si surface of theSRAM2

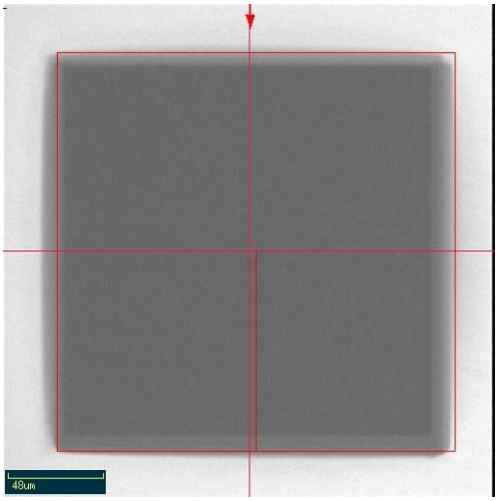
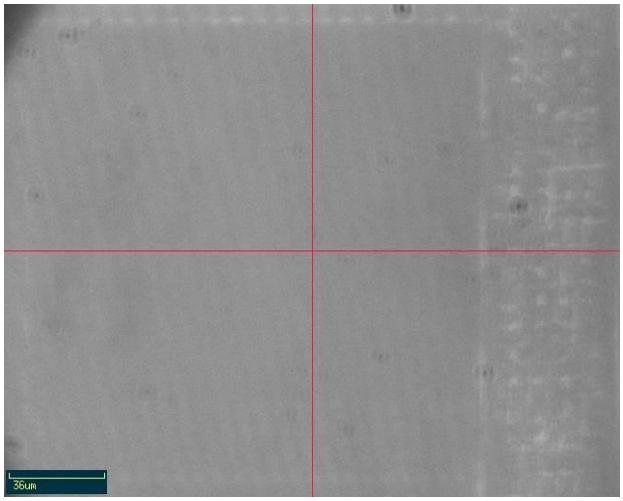


Figure 51 : FIB optical image of same zone: 1000 nm filter allows to see by transparency the structure of the ring



After 38 min Ion milling assisted by X2F2 gas, the interferences fringes appears with the 500nm filter (means that Si thickness is less than 4 µm) and the structure of the die becomes clear and begins to appear by transparency on FIB image.

Figure 52 : FIB image of the SRAM2 ultimate thinning after oxide deposition

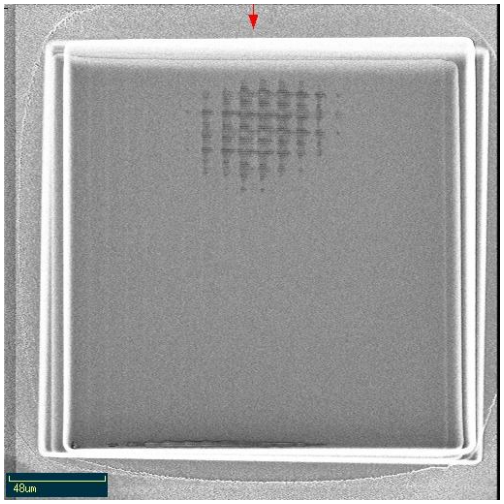
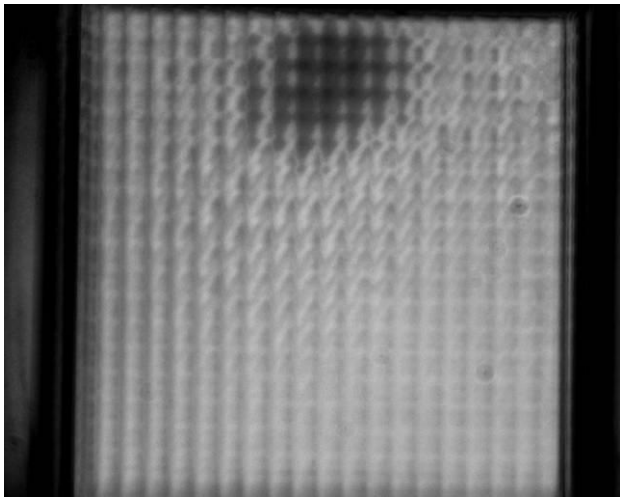


Figure 53 : Optical FIB image of the SRAM2 ultimate thinning



The PUF response is measured after FIB milling and compared with ASAP thinning.

Table 20: Comparison of PUF response before and after backside opening and thinning at 50 µm

PUF response after ASAP milling	PUF response after FIB backside thinning
-- DUMP SRAM PUF 4 5F53152225AB407CFDE926421103E8FC0F72FC38BA425 D7DD0AF62D308F7C059 E6F2DCD20DB124CF90FB7E05FEE304D90DFE37E3B898 D86AB5227F064A78AC4E 1E7CCEB20825144DDE8BEF34BFB815D748CBD4FD4A59 A4161EE56B3931FA71F7 EEBFFAFF12E3BDC7D3055C2496F3966EDF325C0EDE1C0 CE9DE5115EDD117D6D4 FB9CD83B44DD20007FD9DD989BBE6D4B47237E061E9B B962A46B795908762D44 C55085298006C4E1DE94842937314C4826208C0263B43 FB731760091E4723F85 D168A91965FDD0C15186746737AC5F548732E332F2126 95FE3E7F44C53B0B6B8 EBFB5D773A07C5FDA060577834A2D516799754F219BA7 F8FAB334DFAF7D61DF1 A9FBDFAF75BD1374464C612E55E1632D58E642F09DA6C 8FE5282C57E8DEC528B 7CAD87AFD85AD57D446AFCFEF05D2E100D9CBB22F501 68A29ED787BEEE559695 8C11540B8854528F58B1000827497F745D143AC8C240F A2F51B6297D8E05FFFF 16C51153D1511F683E3965186C51D4903B66A07C19DD 5F7C65545DD1EB87DFBF 523BF699904628BBB4E06EA5A354ACEE128017725CECA A6F9E9783BD9A25115B	-- DUMP SRAM PUF 4 5F53552601AA507CFFE927C21193E0B84FFAFC38BA425 D7DD0EF66D348E7C019 E2F2DD920DB124CE90FB7E05FEA344D10DFFB7E7B890 D86EB5226F364968286E 1E7CDEB208213465DA8BEF14BFB811F540CBD47D4A49 A4161EA76B38317A74F7 EE8FFAFF52F7BEC3D315552484F3966EDF323E1EDE1E0 CE9CA4115ED9117D6D4 FF9CD83B44D620007FD0ED989B3C6D4B47237E061E9B BA62A06B7B6908762D44 C49085298106D4E34E948C2B27334C486230AC0263F4B F3731760091E47A3F85 91408B1B65FD70C15006746737A45F748797E312E2126 9F7E3E7F46C56F0B6B8 EBFA5F777A07C5FFA060457824A0D556798754F218BAF E8FAB336DBA73D699F1 A9FBDFEF7FBD1372474C61EE55E3673D58EA42F89DB6C EFE5282C16E8DEC528B 7CA787AFD8DA515D446AFCFEF05D2E100D98AB22F501 68A296D787BEEE559695 8C11540B8014528F58B1000827497F605C103ACAE240A A2F41B43B7D8E05FFEF 1685115391511FE83E7965186451D4901A26207C194D5 F6C2D545D51EB879FBF 523BF699904E2ABB94E86EA7A154B4AE12A017725C6DA E6F9E9783B99A2515DB

To conclude, ultimate thinning on the SRAM2 does not change the PUF response and the fact that there are two ultimate thinnings (SRAM2 +RING) also does not modify the result.

5.2.1.3.3 FIB ultimate thinning on the LATCH

The same process as outlined in section 5.2.1.3.1 is performed on the LATCH. Pictures below show the results:

A new device is used. Its Si thickness is more important than for the previous device (50µm).

Figure 54 : Floor plan ASIC for FIB box localisation

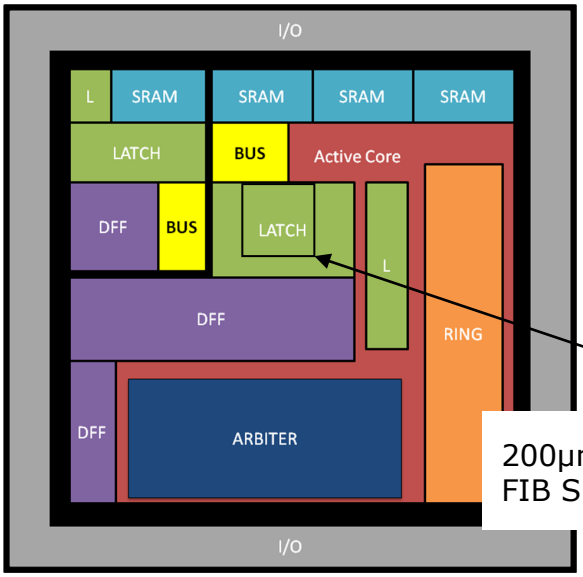
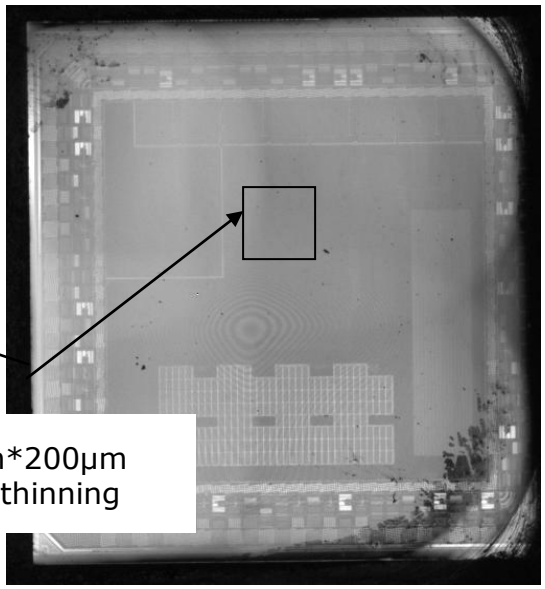


Figure 55 : Backside laser image for FIB box localisation



Because of the thickness of the device (50µm instead of 25 for the first device), it is more difficult to see through the substrate even with IR filters and the ion milling process assisted by X2F2 gas is longer. (80 min instead of 35 min). The FIB box was reduced to a 100µm*100µm box. Moreover, the structures are too small to see them accurately by transparency.

Figure 56 : FIB image of the 100µm*100µm Si surface of the LATCH

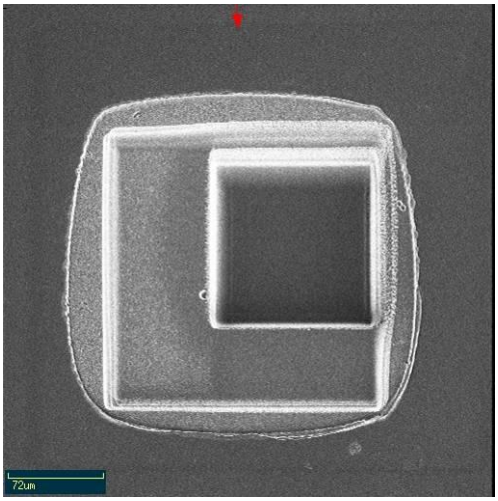


Figure 57 : FIB optical image of same zone: 1000 nm filter does not allow the structure of latch to be observed because of the structure size much smaller than used wavelength.

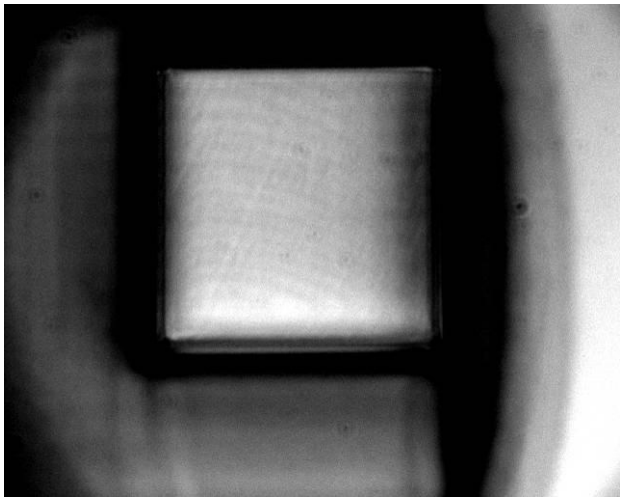


Figure 58 : FIB image of the LATCH ultimate thinning after oxide deposition

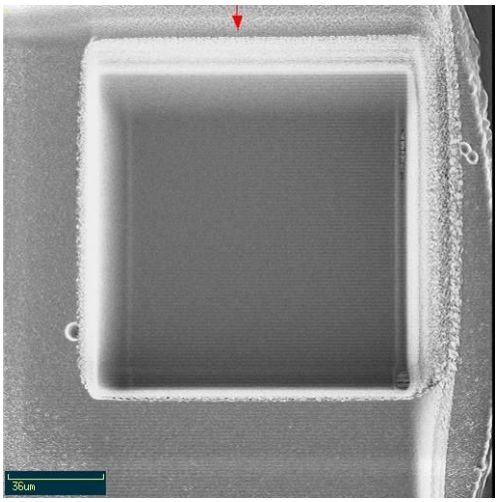
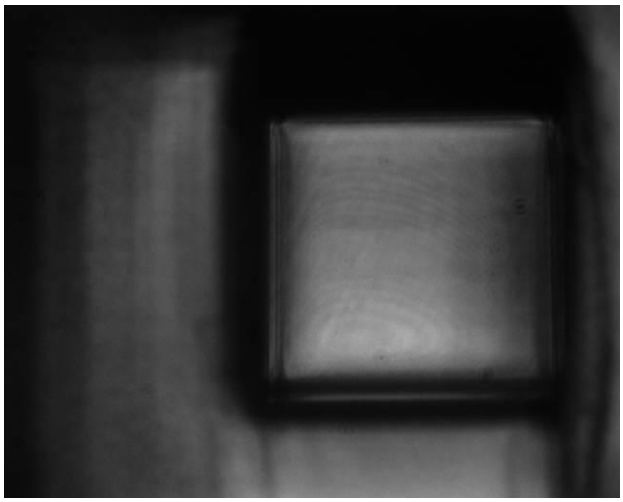


Figure 59 : Optical FIB image of the SRAM2 ultimate thinning



It was impossible to conclude testing for ultimate thinning on the LATCH because the device was no longer functional. The fact is that in the LATCH area, because of the structure size, the difficulty was to stop before Si opening and before the ion beam touches an active surface.

More investigation would have to be done in this zone during further research.

Figure 60 : FIB image of the LATCH ultimate thinning after oxide deposition

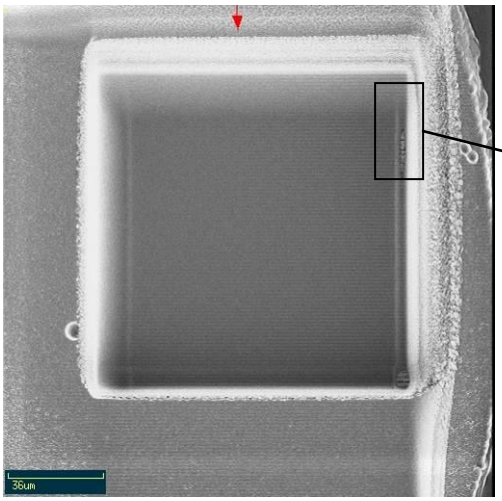
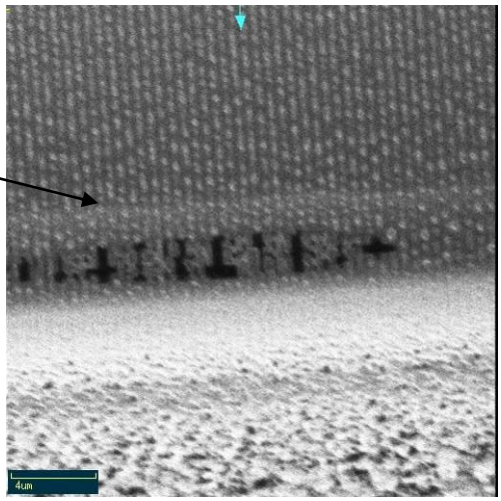


Figure 61 : Si opening on active structures



5.2.1.4 Test point deposition on a contact (RING zone)

Once the backside thinning and the oxide deposition are done, the goal is to open a zone into active structure to deposit PT on a contact in order to allow the internal signal to be probed.

Figure 62 : FIB trench on the RING

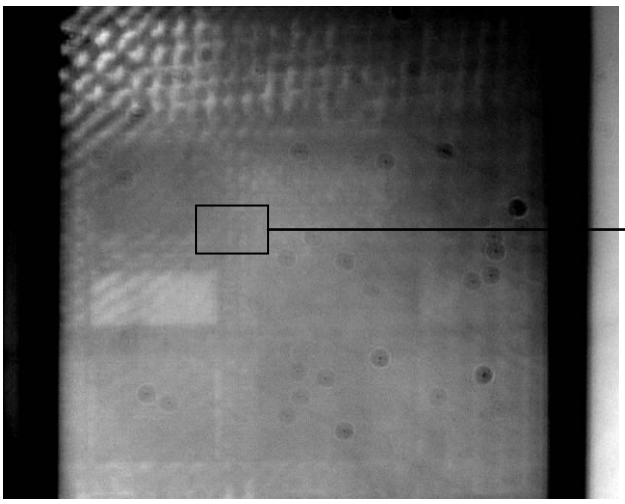
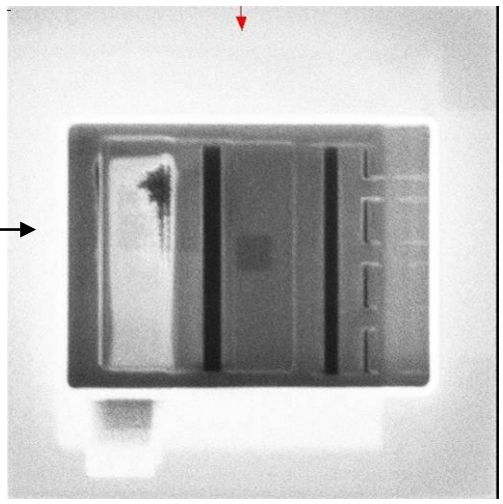


Figure 63 : Opening trough Si to active structures



After Si opening, the device is tested but not functional anymore.

Our results suggest that maintaining device functionality after carrying out FIB operations is difficult at this technology node and process complexity.

Remark:

These tests did not allow definitive conclusions about the intrinsic tamper-resistance of PUFs. Indeed, on each attempt we were confronted with process issues before observing any impact on the PUF answers. Nevertheless, we performed deep backside sample preparation on 2 samples across 3 kinds of different PUF structures without any visible effects on the PUFs answers.

5.3 Side channel analysis

5.3.1 General Observation

The first side channel test will consist of analysing/observing the current consumption and/or electromagnetic emanation of each PUF to see if they present any significant signature. This kind of signature, if present, can reveal the presence of a PUF function which is in and of itself valuable information for any attacker.

In order to make this analysis each PUF function has been operated only in a first step to characterize its signature. Then we tried to identify when a specific PUF is used while other PUFs or an internal noise generator are working.

A preliminary test was performed in order to compare the noise level with and without Active Core. To do this a trigger was generated before the communication process between the FPGA board and the UNIQUE ASIC. The results of this test can be found in Figure 64 and Figure 65.

Figure 64: Ring Oscillator PUF response without Active Core

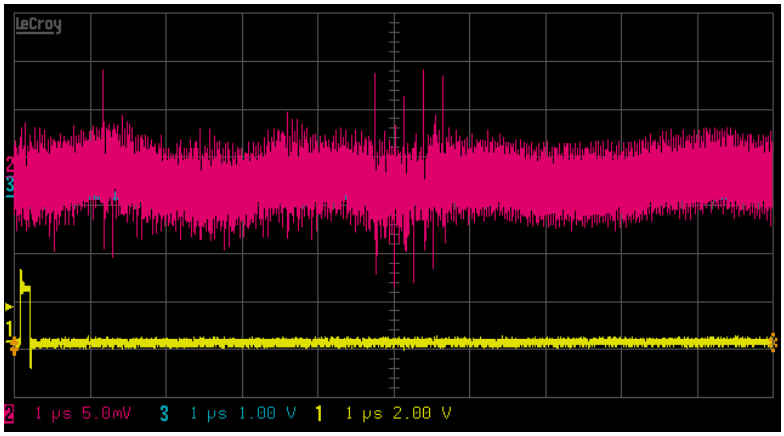
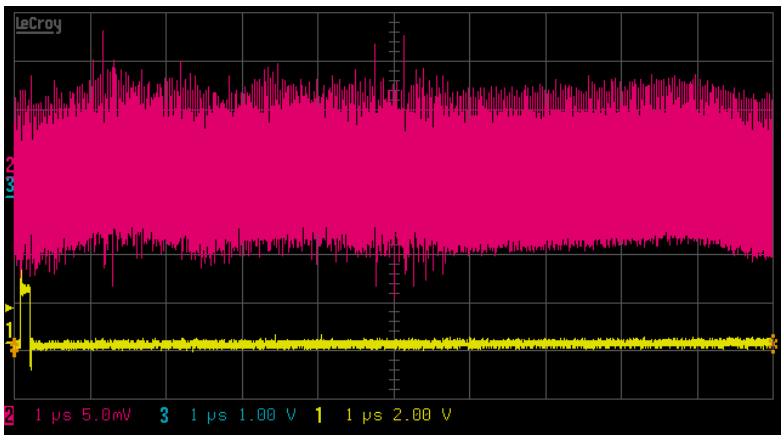
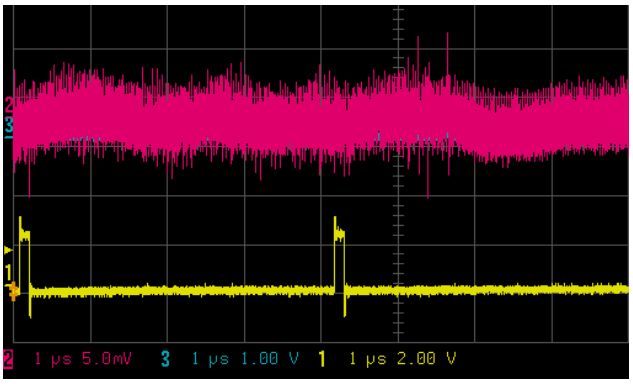


Figure 65: Ring Oscillator PUF response with Active Core

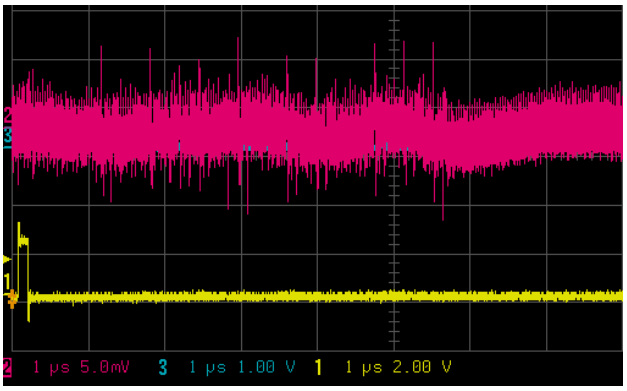


Then a second trigger was generated before each PUFs operation in order to locate and characterize the signature of each PUF response. However, due to the very low power consumption level of the 65 nm technologies, no distinguishable current signature was detected. This lack of information makes any further power analysis attacks quite impossible. Indeed Simple Power Analysis does not permit to clearly identify the targeted internal operations such as memory reading and/or running of ring oscillator. We did not identify any DPA (Differential Power Analysis) attack scenario. The only interesting activities appear during the communication process. These activities correspond to a PUF response. The different PUF responses are detailed in the following table.

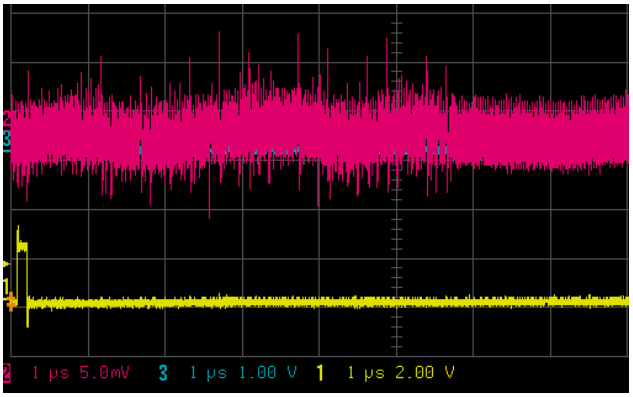
Table 21 : SPA trace of each PUF response during the communication process



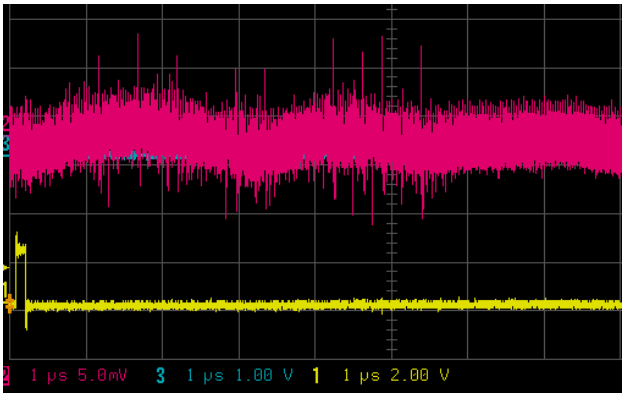
ARBITER PUF



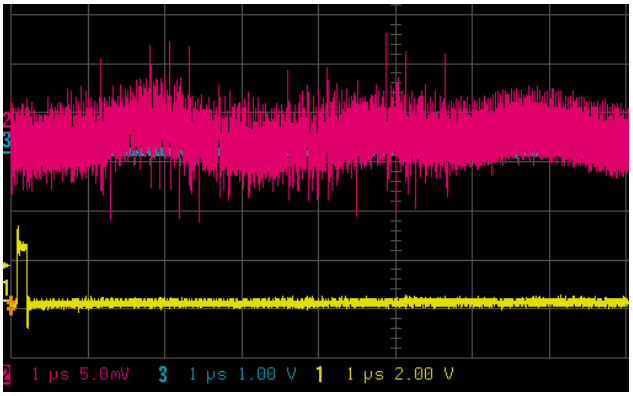
BUSKEEPER PUF



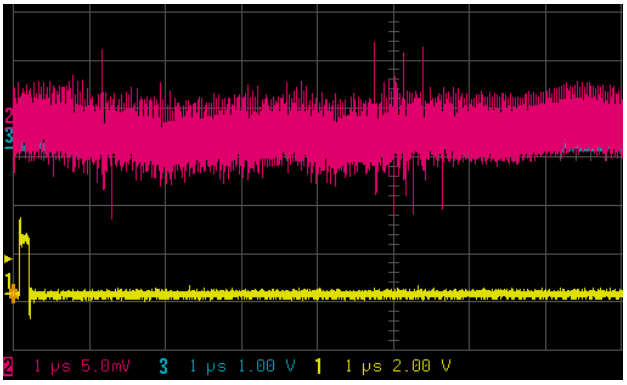
DFF PUF



LATCH PUF



SRAM PUF



RING OSCILLATOR PUF

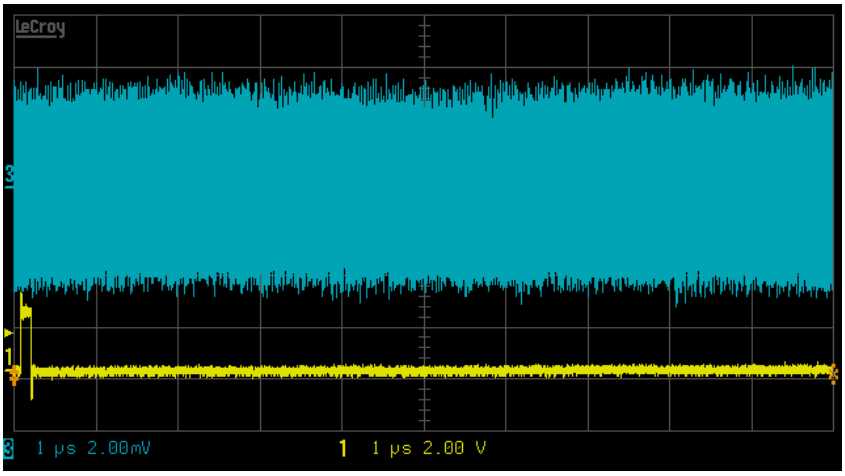
However these results do not permit to perform a complete power consumption attack on the UNIQUE ASIC. Indeed as mentioned above, the only visible signals are linked to the activation of I/O pins. The current variations induced by PUF activation are fully hidden by the noise and we did not succeed in identifying any point of interest during PUF activity. This limitation is due to two main factors. First the PUF activation is done from the external FPGA and no internal timer is used so the influence of external IO for the activation induces additional noise during PUF activity. The second main point is directly linked to the very low power consumption of the process. During the activation of a single PUF there is only a few internal cells activated and their contribution on power measurement is very small compared to the noise level.

5.3.2 Ring Oscillator based PUF characterization

For ring oscillator-based PUFs the knowledge of the free oscillating frequency of each ring can be very useful for an attacker. In this case a deeper study has been carried out to see if we can characterize each oscillator and find out when each oscillator is used. We tried to retrieve which oscillator is activated through the characterization of its signature. To carry on this activity, we tried to use Electromagnetic analysis (EMA) instead of power analysis. Indeed we see in the previous chapter than the current consumption was not suitable due to the low signal to noise ratio. In addition, EMA analysis permits to have higher bandwidth for the acquisitions which is required for the targeted analysis (comparison of free running frequencies of RO).

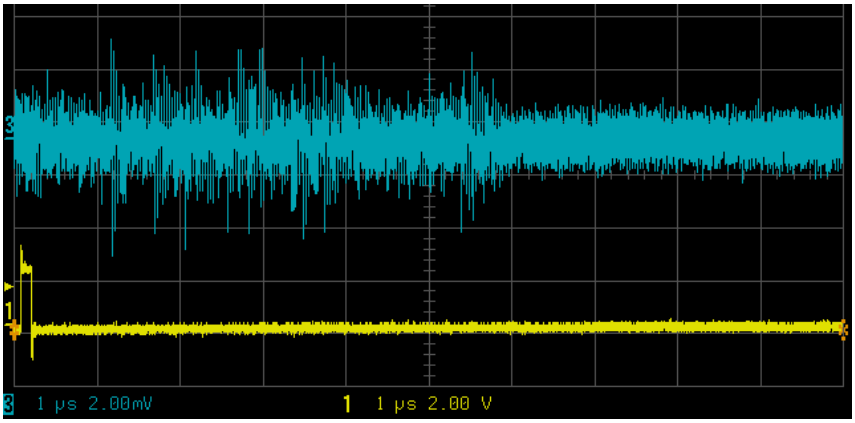
In the same way the power consumption was observed but due to the very low power consumption level of the 65 nm technologies, no distinguishable Electromagnetic activity was detected and only some noise appeared.

Figure 66 : EMA - Ring Oscillator PUF EM emanation (with AC)



As for the SPA, the only interesting activities appear during the communication process which correspond to a PUF response. A Ring Oscillator response example is shown in the following figure.

Figure 67 : EMA - Ring Oscillator PUF EM emanation



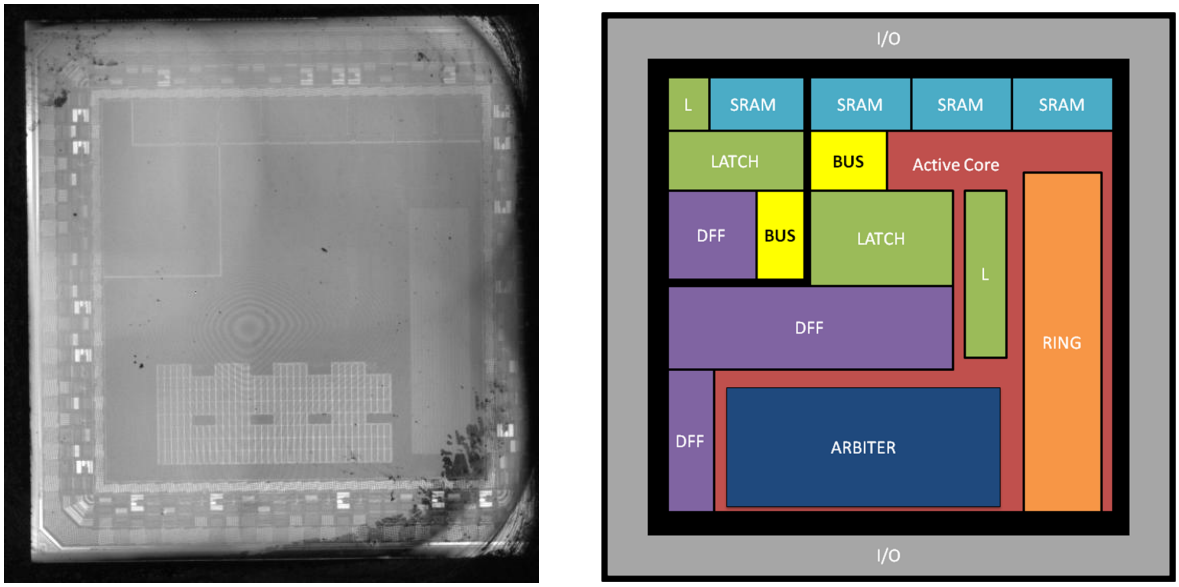
However these results do not permit to characterize oscillators and find out when the oscillators are used. The only visible activity was found during data exchanges between the FPGA and the ASIC. We did not succeed by spatially scanning the ASIC to find a position where the ring oscillators' activity was measurable. We tried to make some FFT analysis on the acquired waveforms for different RO activations but did not see any differences on the obtained results.

5.4 Light Emission Analysis

5.4.1 General activity

The preliminary measurements have been performed to observe the general activity of the UNIQUE ASIC. To observe the light emitted, the chip needs to be opened from the backside. For the backside package opening, the silicon substrate is mechanically thinned down and polished to a thickness of 25 μm. Indeed the thinning is necessary to decrease the absorption rate of the silicon substrate and also to maximize the generation of photo carriers in the silicon. Then a backside laser imaging has been performed as shown on Figure 68.

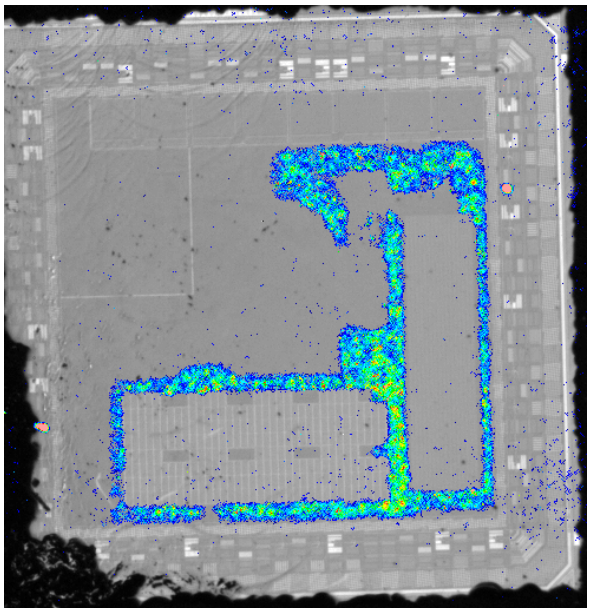
Figure 68: Backside laser imaging compare to ASIC floor plan (D2.2 – 5.6)



The photons emitted can be collected by a specific device equipped with a high sensitivity photon sensor mounted on the optical axis of a conventional microscope. Due to small transistor size and high silicon doping of the 65nm technology, at normal power supply voltage, the photon emission is at a maximum in the 900 nm - 1100 nm range. In this spectral range InGaAs detectors have the best quantum efficiency. In order to perform our experiments we used PICA TriPHEMOS equipment able to acquire time and spatial information about the emitted photons.

Prior to any acquisitions, the light emission activity induced by the active core needs to be localized in order to have a reference mapping of the emitted light. This is done by a static scan, consisting in acquiring the light emitted during 1 minute in order to obtain photon cartography of the whole ASIC. The results of this test can be found in Figure 69.

Figure 69: Reference light emission activity (AC core ON)

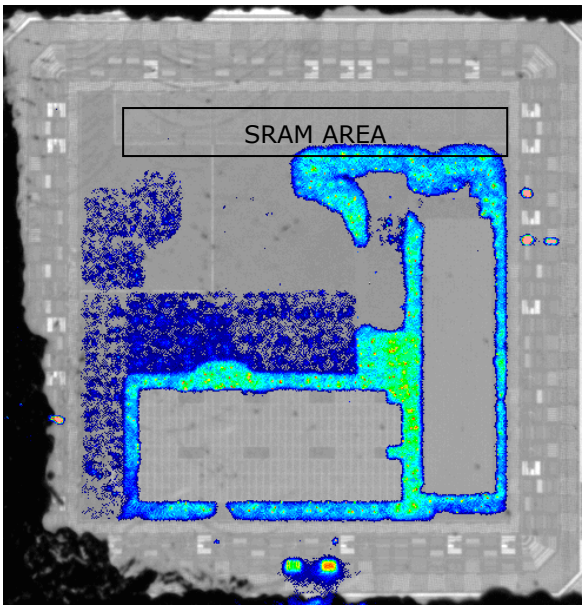


It can be seen in this Figure that the light induced by the active core corresponds to the AC core scheme on the floorplan.

5.4.2 SRAM PUF activity

The SRAM PUFs have been activated in order to establish whether it is possible to measure the initial state of an SRAM cell at power on. By cycling the power of the chip between VDD and 0V one can expect to see differences between cells that exhibit preponderantly a 1 or a 0. The acquisition was performed during 120 seconds in normal voltage configuration (the same acquisition was performed in over-voltage configuration to increase light emission). The results can be found in Figure 70.

Figure 70: SRAM PUF light emission activity (with AC core ON)



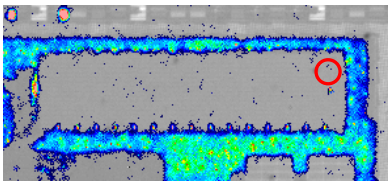
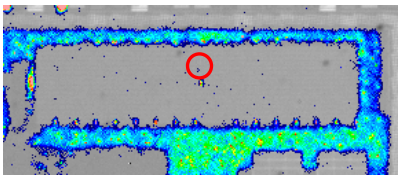
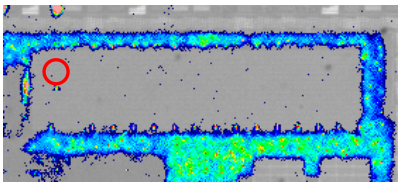
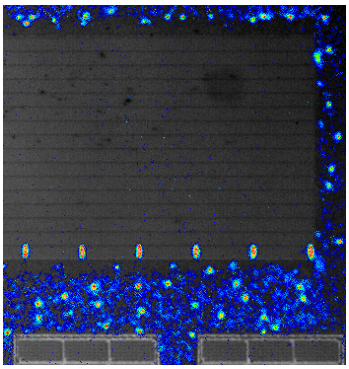
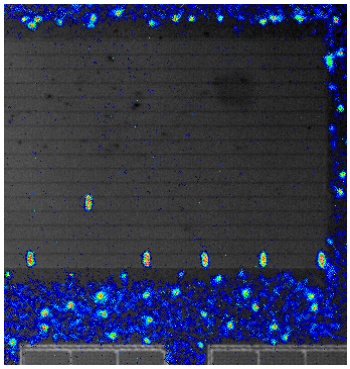
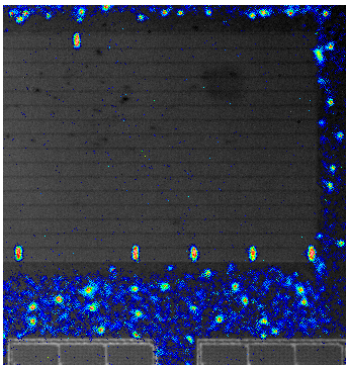
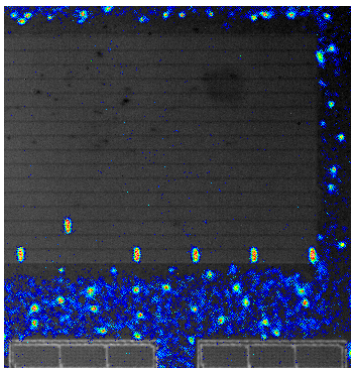
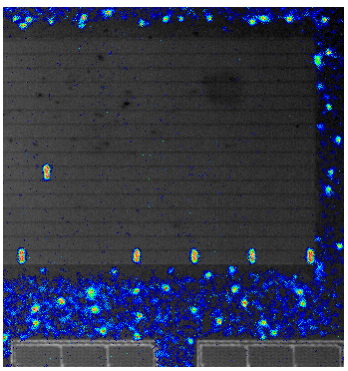
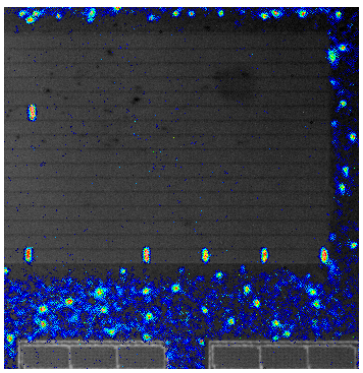
We can see on this acquisition that SRAM PUFs do not emit light therefore it is impossible to distinguish a 0 or a 1 and read the initial state of the SRAM.

To confirm the previous results a second series of acquisitions was performed. This second series consisted of looping Read/Write cycles on all the addresses of the 4 SRAM PUF with an alternate pattern [0x00 / 0x55] during 120s. This alternation is needed to force the memory cells to reset. When reset cells switch to 1, light emission should occur. Indeed, light emission only occurs during cells transitions when the transistors operates in saturation mode and some carrier are heated when crossing the pinch off area. The same kind of acquisition was performed on 1 address of the SRAM PUF 1, 1,280,000 times. In both case we were not able to collect photons above the RAM area neither the RAM interface. A possible explanation can be that the actual frequency of the RAM access were to low due to communication delays between the ASIC and the FPGA.

5.4.3 Ring Oscillator PUF activity

For this test the RO PUFs were activated with the goal of identifying the location of each RO. For ring oscillator-based PUFs the knowledge of the free oscillating frequency of each ring can be very useful for an attacker. In this case a deeper study will be carried out to see if we can characterise each oscillator and find out when each oscillator is used. This attack could lead to the leakage of the full raw data set of ring oscillator PUFs. The results of these acquisitions can be found in next table.

Table 22: RO PUF light emission activity - RO position

		
RO_PUF **batch 0** RO 200_5x_60s	RO_PUF **batch 7** RO 200_5x_60s	RO_PUF **batch 14** RO 200_5x_60s
		
RO_PUF batch 4 **RO 0**_5x_60s	RO_PUF batch 4 **RO 4**_5x_60s	RO_PUF batch 4 **RO 14**_5x_60s
		
RO_PUF batch 4 **RO 50**_5x_60s	RO_PUF batch 4 **RO 150**_5x_60s	RO_PUF batch 4 **RO 250**_5x_60s

We can see on this table that the acquisitions allow identifying each batch and each oscillator of the RO PUF. Thanks to these results it becomes possible to recover the physical architecture of the ring oscillator PUF.

5.5 Fault Injection

5.5.1 Preliminary test

A preliminary test was performed in order to measure the fault injection sensitivity of the unique ASIC. To do this, a laser scan was performed on the whole chip during an SRAM PUF enrolment/reconstruction process. Laser scanning of the SRAM area during enrolment caused subsequent reconstructions to fail.

5.5.2 SRAM PUF

Fault injection can permit setting or resetting some memory nodes. This technique and mainly a safe error approach can permit the retrieval of the initial value of a PUF if an attacker is able to independently set or reset each of the memory cells involved in the PUF.

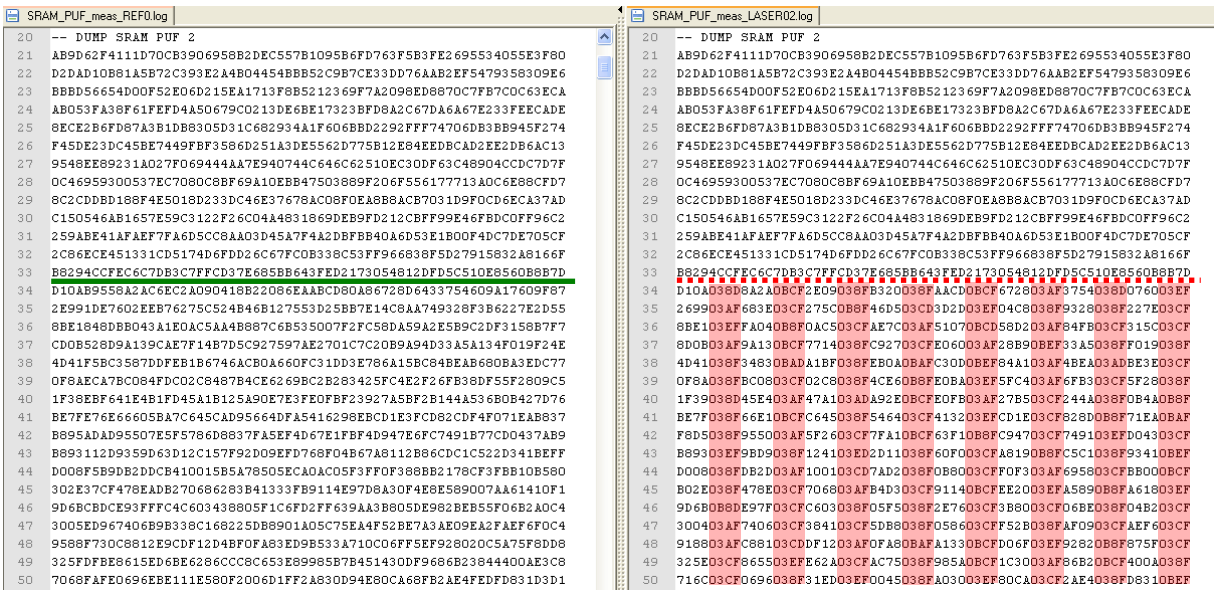
The attack must be composed of the following steps. First, set the memory cells to known values. Then scan the chip surface (backside) with a laser. For each position send a laser pulse then read back the content of the memory to check for a potential switch of the previously stored value.

Once the setup was done, a measure campaign is performed on SRAM based PUFs 1, 2, 3 and 4. For each measurement the following parameters were modified: laser power, pulse width, repetition frequency. A spatial scan was done to test different parts of each SRAM. The results of the fault injection on SRAM3 can be found on Figure 71.

Figure 71 : Fault injection on SRAM3

We notice that the SRAM PUF seems to be sensitive to the fault injection. Indeed half of the data length read is stuck at 0xDE97 value. A second interesting result on SRAM2 is shown on Figure 72.

Figure 72 : Fault injection on SRAM2 during SRAM dump



The laser was focused on the SRAM2 and active during the memory dump. We can notice that the SRAM PUF is modified when we had activated the laser. The fault injection induces an alteration of read data.

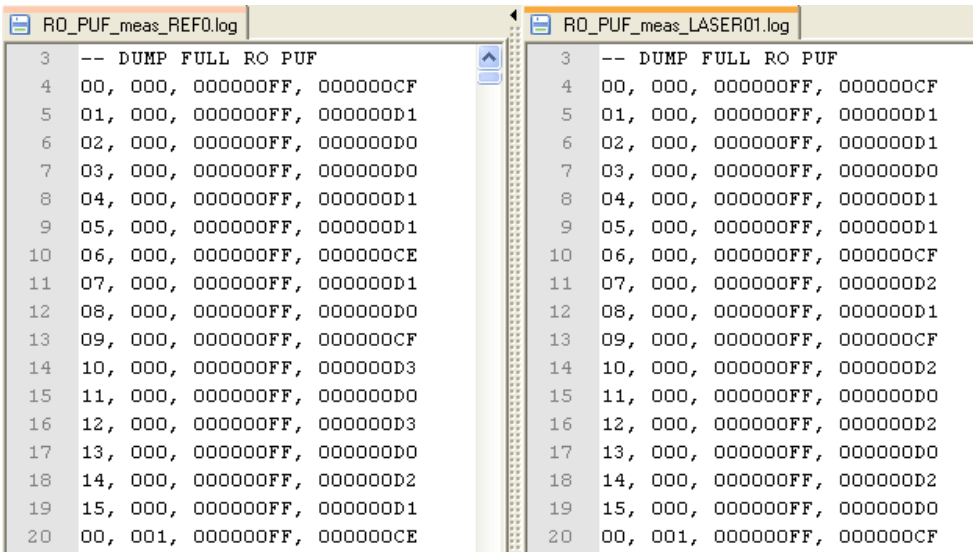
If we succeed in finding some relevant position with a repetitive fault injection effect (stuck at one or stuck at zero model) we can verify the effect of the error on the power on state of the memory and so retrieve the initial value used for PUF generation. As we can notice the laser modifies too many memory cells at the same time, we cannot modify the cell independently; therefore it becomes difficult to retrieve the initial value for PUF generation.

5.5.3 Ring Oscillator PUF

Fault injection techniques can be used in order to modify/characterize ring oscillator frequencies and as a result change the normal behaviour of RO based PUFs. We investigated the effect of light perturbation/injection techniques on the oscillators to see how these techniques could be used in order to predict/modify the PUF's answers.

For a delay-based PUF, the idea was to affect the circuit by slowing down some gate. This kind of perturbation allows the characteristics of 2 oscillators (or 2 paths) to be compared and to retrieve which path is used and/or which path is faster. A series of laser tests was performed on the Ring Oscillator PUF and on each measurement the following parameters were modified: laser power, pulse width, repetition frequency. The results are inconclusive as shown in the example of the Figure 73, the laser injection has no effect on the behaviour of the ring oscillator.

Figure 73 : Fault injection on RO



RO_PUF_meas_REF0.log

```
3   -- DUMP FULL RO PUF
4   00, 000, 000000FF, 000000CF
5   01, 000, 000000FF, 000000D1
6   02, 000, 000000FF, 000000D0
7   03, 000, 000000FF, 000000D0
8   04, 000, 000000FF, 000000D1
9   05, 000, 000000FF, 000000D1
10  06, 000, 000000FF, 000000CE
11  07, 000, 000000FF, 000000D1
12  08, 000, 000000FF, 000000D0
13  09, 000, 000000FF, 000000CF
14  10, 000, 000000FF, 000000D3
15  11, 000, 000000FF, 000000D0
16  12, 000, 000000FF, 000000D3
17  13, 000, 000000FF, 000000D0
18  14, 000, 000000FF, 000000D2
19  15, 000, 000000FF, 000000D1
20  00, 001, 000000FF, 000000CE
```

RO_PUF_meas_LASER01.log

```
3   -- DUMP FULL RO PUF
4   00, 000, 000000FF, 000000CF
5   01, 000, 000000FF, 000000D1
6   02, 000, 000000FF, 000000D1
7   03, 000, 000000FF, 000000D0
8   04, 000, 000000FF, 000000D1
9   05, 000, 000000FF, 000000D1
10  06, 000, 000000FF, 000000CF
11  07, 000, 000000FF, 000000D2
12  08, 000, 000000FF, 000000D1
13  09, 000, 000000FF, 000000CF
14  10, 000, 000000FF, 000000D2
15  11, 000, 000000FF, 000000D0
16  12, 000, 000000FF, 000000D2
17  13, 000, 000000FF, 000000D0
18  14, 000, 000000FF, 000000D2
19  15, 000, 000000FF, 000000D0
20  00, 001, 000000FF, 000000CF
```

Finally, we cannot modify ring oscillator frequencies and change the normal behaviour of RO-based PUFs with laser fault injection techniques.

5.6 High temperature testing

A few additional tests have been performed on 5 samples at 25°C and 125 °C. In addition one sample has been tested at 150°C, 175°C, 200°C and 225 °C. Tests at 225 °C have been only partially done since the socket was not designed to support such high temperatures and we lost the contact with the sample before we completed the test.

The use of this low number of samples does not really permit a full statistical analysis, nevertheless they are sufficient to make some observations.

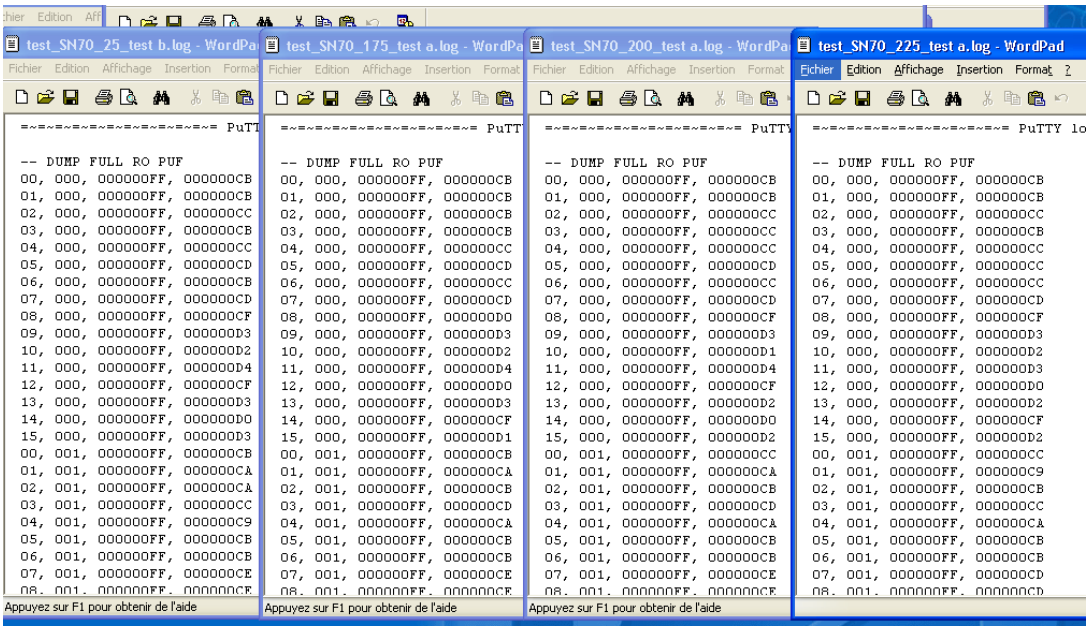
Table 23: Comparison of RO PUF at 25°C and 125°C

PUF answer at 25°C	PUF answer at 125 °C
-- DUMP FULL RO PUF SN 65	-- DUMP FULL RO PUF SN 65
00, 000, 000000FF, 000000D2	00, 000, 000000FF, 000000D2
01, 000, 000000FF, 000000D2	01, 000, 000000FF, 000000D2
02, 000, 000000FF, 000000D5	02, 000, 000000FF, 000000D6
03, 000, 000000FF, 000000D3	03, 000, 000000FF, 000000D3
04, 000, 000000FF, 000000D2	04, 000, 000000FF, 000000D2
05, 000, 000000FF, 000000D0	05, 000, 000000FF, 000000D1
06, 000, 000000FF, 000000D1	06, 000, 000000FF, 000000D2
07, 000, 000000FF, 000000D3	07, 000, 000000FF, 000000D3
08, 000, 000000FF, 000000D3	08, 000, 000000FF, 000000D4
09, 000, 000000FF, 000000D1	09, 000, 000000FF, 000000D2
10, 000, 000000FF, 000000D3	10, 000, 000000FF, 000000D2
11, 000, 000000FF, 000000D2	11, 000, 000000FF, 000000D2
12, 000, 000000FF, 000000D1	12, 000, 000000FF, 000000D2
13, 000, 000000FF, 000000D2	13, 000, 000000FF, 000000D2
14, 000, 000000FF, 000000D1	14, 000, 000000FF, 000000D1
15, 000, 000000FF, 000000D0	15, 000, 000000FF, 000000D0
…	…
00, 255, 000000FF, 000000D3	00, 255, 000000FF, 000000D2
01, 255, 000000FF, 000000D0	01, 255, 000000FF, 000000D1
02, 255, 000000FF, 000000D3	02, 255, 000000FF, 000000D4
03, 255, 000000FF, 000000CF	03, 255, 000000FF, 000000CF
04, 255, 000000FF, 000000D3	04, 255, 000000FF, 000000D4
05, 255, 000000FF, 000000D1	05, 255, 000000FF, 000000D1
06, 255, 000000FF, 000000D1	06, 255, 000000FF, 000000D0
07, 255, 000000FF, 000000D2	07, 255, 000000FF, 000000D2
08, 255, 000000FF, 000000D0	08, 255, 000000FF, 000000D0
09, 255, 000000FF, 000000D1	09, 255, 000000FF, 000000D2
10, 255, 000000FF, 000000D0	10, 255, 000000FF, 000000D0
11, 255, 000000FF, 000000D5	11, 255, 000000FF, 000000D4
12, 255, 000000FF, 000000D2	12, 255, 000000FF, 000000D2
13, 255, 000000FF, 000000D1	13, 255, 000000FF, 000000D1
14, 255, 000000FF, 000000D2	14, 255, 000000FF, 000000D2
15, 255, 000000FF, 000000D2	15, 255, 000000FF, 000000D1
-- DUMP FULL RO PUF SN 66	-- DUMP FULL RO PUF SN66
00, 000, 000000FF, 000000D3	00, 000, 000000FF, 000000D3
01, 000, 000000FF, 000000D0	01, 000, 000000FF, 000000D2
02, 000, 000000FF, 000000D0	02, 000, 000000FF, 000000D0
03, 000, 000000FF, 000000D2	03, 000, 000000FF, 000000D3
04, 000, 000000FF, 000000D4	04, 000, 000000FF, 000000D4
05, 000, 000000FF, 000000D2	05, 000, 000000FF, 000000D2
06, 000, 000000FF, 000000D2	06, 000, 000000FF, 000000D1
07, 000, 000000FF, 000000D1	07, 000, 000000FF, 000000D2
08, 000, 000000FF, 000000CD	08, 000, 000000FF, 000000CE
09, 000, 000000FF, 000000D4	09, 000, 000000FF, 000000D3
10, 000, 000000FF, 000000CF	10, 000, 000000FF, 000000CF
11, 000, 000000FF, 000000D0	11, 000, 000000FF, 000000D0
12, 000, 000000FF, 000000D3	12, 000, 000000FF, 000000D2
13, 000, 000000FF, 000000D0	13, 000, 000000FF, 000000CF
14, 000, 000000FF, 000000D0	14, 000, 000000FF, 000000D0
15, 000, 000000FF, 000000CE	15, 000, 000000FF, 000000CE
00, 255, 000000FF, 000000CF	00, 255, 000000FF, 000000CF
01, 255, 000000FF, 000000D1	01, 255, 000000FF, 000000D2
02, 255, 000000FF, 000000D1	02, 255, 000000FF, 000000D1
03, 255, 000000FF, 000000D1	03, 255, 000000FF, 000000D1
04, 255, 000000FF, 000000D2	04, 255, 000000FF, 000000D3
05, 255, 000000FF, 000000D3	05, 255, 000000FF, 000000D3
06, 255, 000000FF, 000000CD	06, 255, 000000FF, 000000CE
07, 255, 000000FF, 000000D2	07, 255, 000000FF, 000000D1
08, 255, 000000FF, 000000CF	08, 255, 000000FF, 000000CF
09, 255, 000000FF, 000000D3	09, 255, 000000FF, 000000D3
10, 255, 000000FF, 000000D1	10, 255, 000000FF, 000000D1
11, 255, 000000FF, 000000D1	11, 255, 000000FF, 000000D1
12, 255, 000000FF, 000000CF	12, 255, 000000FF, 000000CF
13, 255, 000000FF, 000000D1	13, 255, 000000FF, 000000D1

14, 255, 000000FF, 000000CE 15, 255, 000000FF, 000000D1 …	14, 255, 000000FF, 000000CE 15, 255, 000000FF, 000000D2

For the Ring Oscillators PUF the observed variations are very small. Only a few bits are impacted by the temperature variations. Even at 225°C the RO-PUF answer doesn't change significantly.

Figure 74 : RO variations over temperature



For the Latch PUF, we observed that at 125°C, most of the latches are set at one at power-up. This induces huge variations between the 2 temperatures and so the latch based PUFs are not suitable for high temperature operations

Table 24: Comparison of Latch PUF at 25°C and 125°C

PUF answer at 25°C	PUF answer at 125 °C
-- DUMP LATCH PUF 1 SN 65 BBEFCA6FDDD7AEF7F3EB4B9FBDA45FB25CD752FEBBEC D3BFB9B7CDD3EFDFBFEF 2F2B7B4E5B3FF6EF0FE76BEEBF9B19BD5F36BB2D57EAE 2A0EDF29FFF09D6C83D AFD23ECB525DF76EFF92F35E6FA6F7FBFFBB7E93C673D F5EAFFDEEA5DAFBFDDF EEBBFA7DE7DFFB647BABEBB7FBFE7FE7E17FFF7FB7DBB F67C7B5FEA6F7ECD1F3 EE5CA0FF68FC7B3ED7FB65DDEF72BB2FBBD77A89D45A AFC9FC925A47EF8FCB5D … -- DUMP LATCH PUF 2 SN 65 FCF0EFA5F92F592EDEBEBB9BE67FCDCADDF37BE5BFFD 9F7D2F5FE93DA90DFDFB 523FBE7E8FFEFFB8FCE6EE6CCFD4DFCF19E6F56EF0EB5 E8FB1E8A2AFB46D0243 F7F1FEFBB9D39EE74DBAD725F9DB3D2DB77CB07C1EF9 FD3E4A192CFBEC0724DD FFABBF2DB29FDEC1F6F5F66018B76FDFD6DEEB58FD55 6A7793652BFEEF7EDFDB F7BFBDC0F9523F4637E4B6C98ADFBD8FC9E1CF3E3CF2 BB83FF39883F3DE3DBE6 E6E3CA6AEBEAEFAD972CAA5E77CC05DAE9B3EFFFD740 BAF4FDFADDDDD1727ED2 -- DUMP LATCH PUF 1 SN 66 FBB6E2EEF6CECDBEE7F0ED9FFFB77B7DDF9D1BBFDDFF 7F37FD3F7F7FFF53F6EF D7F9FBFFFFC373DE6EA1D75FE7FC7957FFB3DBFFB9FCF CD5FDC6F3AFDBF57EF1 FEE5E3F94BFFFFD7FFE7BEDFFFBFFD9EEFE7EECBCABFB BDFF7B73AC6DD0AA7EF FFFB7BBEBAAFFBE7FFF9DA3FDFFF97FDEFFFACDEFEDAB 5F99B9EBB32B7FC7FD3 CF6F5DD2ABFF53B56FEEF51FFE5A6F9BDADFBD7E3E52 1CF6A376B8E493FF0EB7 -- DUMP LATCH PUF 2 9FBBAFF7BEF3FDFEEDEFFDDBFBDBE7DB7C6B59BF4FBB FF6E4D77A82EDFFF1BDF F2E1F3BEFFDD7F5F3FBF23EDA7CF0D5EFFB7FF3DBFBBF F79EFC33FBCDBF336DB 2D3FDEFDF7AF9ABF7FE4AD9FDB5FE4EFDBA59CDD70DE 7F6BFEDF72E7B5EBD0FF AD79F77BFEFDFC36FDEFFBDB53FFFEF2CB3F8BEF779DF FDEFFDCE4DDDEDFE7DF 2BE93F377CFFAADDFC8D9ED2DF7FDFACDF79FBF8FEE3 BC93A7CF7A7E7DB5FBF9…	-- DUMP LATCH PUF 1 BF7FCEEFDDDFEEBFFFEBCF9FBFF57FBEDAF7D3FE 9FEF53BFBCBF5DFBEFFFBFFF 3FEFFF4E5FFFF7FF2FFF7FEFBFFFBBFD7F76FFFF57 FEEEFBFDF39FFF9DD6FC7D EFFB3FF77FDCFFFFFF9EFFFFFFE4F7DBFFFB7E3FD E7FF77EAFFFFAAFDEFFFFFF FEBFF76FFFDFFF76FBBBEFDFFFFEFFEFEBFFFF6FBF FBB767F79FFEBED7ECFDF7 FE5DFEFF1DFEFFFFC7FFE7DDFFF7FFAFFFFFFADBF 4DEFFEFFFF6FFE7FF8FDBFF … -- DUMP LATCH PUF 2 SN 65 FFFFFFFFFFFFFFFEFFFFFFBFF6FFCDEBDDF7FFFDBF FD9F7F2FDFE9FFBB2DFFFF 7A7FBE7FBFFEF7FFDDEEFD7CFFFEFFFFBDFFF5EEF FFB5F8DBBEDABBFFEFFF3D7 FFFBFFFFFBFBDEEFDDFED765FFDFBF2FFFFEF67C DFF9FDBECBFFFCFFED2F6FFB FFABFFEDBF9FFFFBFEF7FEE93AB6FFFFDE5BEF7EE D1FFEFF9FF7BFFFFFFFDFDF F7BFFDC0F952BF4E7FF4B7AFDAFFBFFFF9D3DFBF 3EDABF83FFBB99FFFFE3DBEE EEFBFA7A9FEEBFFFF7EFBAFEFFEF6FDFEFFBFFFFD D78BEFEFDFBFFFDFF7AFEFE -- DUMP LATCH PUF 1 SN 66 FBB3E2EFFEFEC5BFFFF2ADBFDFF77B7DD7C95BFF EDFA7FBFFFB77D7FFF17F3EF DFF7FBFFDEC39BDC7EA5F77FEFFDFFD6FDFBFFFD F97FFEDFFDA6F7AFCFF7FEF1 BFCDFBF96BFFFFDFFDE7BFF6F7BFFFFEEDF7FF5FD ABFBFDFF7B79BC6FD9FBFEF FFFFFFBEFFDFFFF7FFFFF9BFF7FFFFFFFFFFAFFFFED FBBFFDBB7BFBFB7FFFFF6 EF765FD7BBFF77FEFFFFF53FFEDEFF97FBFFFDFF3 FF69C76A375A9A59BFF1CB3 -- DUMP LATCH PUF 2 FF7BBFFFFFFBFFFEFDE37DFFFBCBEFDFFCE95D37 5F9BBFB66D57B6EADFFF1F57 D6E5E3FEFFDD7EDFBFBF73ADEFC71DFEFF37FF3D DFBBFF7DE7C15FF4DBF35FDB EF3FFCFFF7AFBAFF7FCDAFBFD7DFCCEFDF85DCD D72FCFF6FF7DFFEE6F5EBD0F7 FD79F7FBFEF7DC7EEF7FBBFBD3DDFEF2EB3DBBE F769DFFF7FFDEE4FFFFF7E3DF 6FFFFF377CFFAAFDFDED96F7FF7FCFEEFFF9FBFDF DFE2C95A7CB5E7B7FB5FBF9

For other PUFs we did not observe any significant modifications between the 2 temperatures, even for higher temperatures up to 200 °C

6 Conclusion

The ASIC low-level functional tests, including the SRAM PUF self-test, have reported three minor bugs which do not disturb the PUF assessment or the PUF data behaviour.

Aging tests which have been mainly designed to assess memory-based PUFs have provided very encouraging results by showing that aging does not affect PUF data reliability when the PUF mechanism is powered down. This means that aging effects can be drastically reduced by powering down memories when not using them for PUF purposes.

Robustness tests which measure the ability of PUFs to return similar responses when queried with the same challenge multiple times have been done following voltage and temperature variations. The bit error rate for SRAM, Buskeeper, ring oscillator and arbiter PUFs in temperature variation stays below 20% which means that the errors are correctable at reasonable cost while this bit error rate for flip-flop and latch PUFs is higher than the other types. In voltage variation, the assessment showed that all PUFs responses of all chips remain robust.

PUF unpredictability was estimated by performing several statistical tests such as hamming weight measurement in different operating conditions, entropy/min-entropy approximation and hamming distance over chip measurements.

Hamming weight measurements show that responses from SRAM and ring oscillator PUF are uniformly random and independent of the different operating conditions. Responses from flip-flop and latch PUFs are biased and depend on temperature but not voltage variations. Moreover, the context-tree-weighting (CWT) tests confirm the previous results.

Entropy estimation results are in line with hamming weight conclusions. The entropy and min-entropy distributions of SRAM and ring-oscillator PUF responses does not depend on operating conditions while flip-flop and latch PUF responses min-entropy remains stable in voltage variation but not in temperature variation.

The Hamming distance test which gives information about the independence of each PUF chip response to a same challenge showed that SRAM and ring oscillator PUF data have the ideal hamming distance. On the other hand, this test shows that there may be dependencies between responses coming from different arbiter PUF instances to a same challenge. This can make modelling attack possible.

The hamming distance test also shows that flip-flop and latch PUF responses are dependent of operating conditions. This can also permit modelling attack. Buskeeper PUF entropy assessment which has been done independently concludes that the hamming distance value, computed from the PUF data of 192 UNIQUE chips, is near to ideal. Results confirmed by a CWT test.

Finally, the robustness and unpredictability tests conclude that SRAM following by Buskeeper PUF are the most reliable type of PUF, while the other type of PUF give responses which are not enough robust neither unpredictable or both.

Regarding penetration testing we demonstrate that the tamper evidence claims for PUFs are weak since we were able to deeply modify the samples without any significant change of PUF answer. Nevertheless, we did not succeed in mounting a full probing attack but we were much more limited by the process (65nm 10 metal layers) than by the PUF themselves.

For side channel analysis, the main limitations we were confronted with came from intrinsic characteristics of the process and some setup limitations. The low power consumption of the process implied very low leakage level. Neither power consumption, electromagnetic emission nor light emissions allowed the retrieval of sensitive information from the PUFs.

7 References

[1] Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Advances in Cryptology (EUROCRYPT). LNCS, vol. 3027, pp. 523–540. Springer Berlin/Heidelberg (2004)
[2] Maes, R., Verbauwhede, I.: Physically unclonable functions: A study on the state of the art and future research directions. In: Towards Hardware-Intrinsic Security. pp. 3–37. Information Security and Cryptography, Springer Berlin Heidelberg (2010)
[3] Armknecht, F., Maes, R., Sadeghi, A.R., Standaert, F.X., Wachsmann, C.: A formal foundation for the security features of physical functions. In: IEEE Symposium on Security and Privacy (SSP). pp.397–412. IEEE Computer Society (May 2011)
[4] Marsaglia, G.: The marsaglia random number CDROM including the diehard battery of tests of randomness. http://www.stat.fsu.edu/pub/diehard/
[5] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Special Publication 800-22 Revision 1a, NIST(April2010)
[6] Willems, F.M.J., Shtarkov, Y.M., Tjalkens, T.J.: The context-tree weighting method: basic properties. IEEE Transactions on Information Theory 41(3), 653–664 (May1995)
[7] Ignatenko, T., Schrijen, G.J., Škorić, B., Tuyls, P., Willems, F.: Estimating the Secrecy-Rate of physical unclonable functions with the Context-Tree weighting method. In: IEEE International Symposium on Information Theory (ISIT). pp. 499–503. IEEE (Jul 2006)
[8] Tuyls, P., Škorić, B., Ignatenko, T., Willems, F., Schrijen, G.J.: Entropy estimation for optical PUFs based on Context-Tree weighting methods security with noisy data. In: Security with Noisy Data. pp. 217–233. Springer London (2007)
[9] Hammouri, G., Dana, A., Sunar, B.: CDs have fingerprints too. In: Cryptographic Hardware and Embedded Systems (CHES). LNCS, vol. 5747, pp. 348–362. Springer Berlin/Heidelberg (2009)
[10] van der Leest, V., Schrijen, G.J., Handschuh, H., Tuyls, P.: Hardware intrinsic security from D flip-flops. In: ACM Workshop on Scalable Trusted Computing (ACM STC). pp. 53–62. ACM, New York, NY, USA (2010)
[11] Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., Schmidhuber, J.: Modeling attacks on physical unclonable functions. In: ACM Conference on Computer and Communications Security (ACM CCS). pp. 237–249. ACM, New York, NY, USA (2010)
[12] Willems, F.: CTW website. http://www.ele.tue.nl/ctw/
[13] Holcomb, D.E., Burleson, W.P., Fu, K.: Power-Up SRAM state as an identifying fingerprint and source of true random numbers. IEEE Transactions on Computers 58(9), 1198–1210 (2009)
[14] Altera. Reliability report 52 q3 2011. http://www.altera.com/literature/rr/rr.pdf.

8 Glossary

A

AES	Advanced Encryption Standard
ALU	Arithmetic Logic Unit
ASIC	Application-Specific Integrated Circuit
ASAP	Automated Selected Area Polisher (Package opening equipment)

B

BIST	Built-In-Self-Test

C

CMOS	Complementary Metal Oxide Semiconductor
CPUF	Controlled Physical Unclonable Function
CRP	Challenge Response Pair

D

DES	Data Encryption Standard
DH	Diffie-Hellman
DPM	Direct Part Marking
DRAM	Dynamic Random Access Memory
DRM	Digital Right Management
DSA	Digital Signature Algorithm

E

ECB	Electronic Code Book Mode
ECDSA	Elliptic Curve DSA
ECRYPT	European Network of Excellence in Cryptology
EDA	Electronic Design Automation
EEPROM	Electrically Erasable Programmable ROM
EMA	Electromagnetic Analysis
EMMI	Emission Microscopy

F

FIB	Focused Ion Beam
FPGA	Field Programmable Gate Array

I

IC	Integrated Circuit
ICT	Information and Communications Technology
IKE	Internet Key Exchange
ILD	Inter Layer Dielectric
InGaAs	Indium Gallium Arsenic

IP	Intellectual Property
IPSec	Internet Protocol Security
IR	Infra Red wavelength
JIL	Joint Interpretation Library

K

KEM	Key Encapsulation Mechanism
KDF	Key Derivation Function

L

LVP	Laser Voltage Probing

M

MD5	Message Digest Algorithm 5

N

NESSIE	New European Schemes for Signatures, Integrity and Encryption
NIST	National Institute of Standard and Technology
NVRAM	Non-Volatile Random-Access Memory

O

OAEP	Optimal Asymmetric Encryption Padding
OEM	Original Equipment Manufacturer
OFB	Output Feedback Mode
OTP	One-Time Programmable

P

PCB	Printed Circuit Board
PLD	Programmable Logic Device
PLL	Phase-Locked Loop
PRF	Pseudo-Random Function
PSS	Probabilistic Signature Scheme
PUF	Physically Unclonable Function

R

RAM	Random Access Memory
RFID	Radio-Frequency Identification
ROM	Read-Only Memory

S

SEM	Scanning Electron Microscope

SIL	Solid Immersion Lens
SIA	Semiconductor Industry Association
SRAM	Static Random Access Memory
STM	Scanning Tunnelling Microscopy
SCA	Side Channel Analysis
SPA	Simple Power Analysis

T

TRE	Time Resolved Emission
TSMC	Taiwan Semiconductor Manufacturing Company