D2.1

Report on novel cell and architecture concepts based on technology dependent research

Project number:	317930
Project acronym:	HINT
Project title:	Holistic Approaches for Integrity of ICT-Systems
Start date of the project:	1st October, 2012
Duration:	36 months
Programme:	FP7/2007-2013

Deliverable type:	Report
Deliverable reference number:	ICT-317930 / D2.1/ v1.0
Work package contributing to the deliverable:	WP 2
Due date:	MAR 2014 – M18
Actual submission date:	31.03.2014

Responsible organisation:	IFAT
Editor:	IFAT (H. Bock)
Dissemination level:	Public
Revision:	1.0

Abstract:	One dimension of the HINT integrity concept is built on hardware integrity anchors based on weak PUFs with special cell arrays. Unstable cells in SRAM-like PUFs foist a huge burden on the post processing. D2.1 describes research on root causes of such instabilities and optimization of raw-data quality as well as consequences to the PUF cell and module architecture.
Keywords:	Hardware integrity, PUFs, CMOS design, TCAD simulation, Error Correction, FPGA

Editor

Bock, Holger (IFAT)

Contributors

Böhm, Christoph (IFAT)

Bucci, Marco (IFAT)

Deutschmann, Martin (TEC)

Hofer, Maximilian (IFAT)

Hübner, Thomas (MOR)

Luzzi, Raimondo (IFAT)

Schellekens, Dries (KUL)

Disclaimer

The research leading to these results has received funding from the European Union’s Seventh Framework Programme (FP7/2007-2013) under grant agreement n_ 317930.

Executive Summary

This deliverable D2.1 of the HINT project describes concepts for improved hardware structures on cell and architecture level as well as the investigations in 65 nm CMOs flash technology leading to these concepts. Distinction of noise dependent stochastic errors and temperature dependent deterministic errors is crucial for the design decisions to be made.

Based on previous test-chip measurements of dedicated 90 nm two stage PUF cells and simulations in 65 nm technology cell structures could be optimized and architectural improvements could be investigated. Thus we can project that with concepts like N-transistor mismatch-pairs, sense-amplifier sharing and bias-source sharing we will be able to develop a very dense cell-array with robust raw-data output. Besides biasing methods a variety of novel pre-selection mechanisms based on noise amplification is available to select stable cells for use and to omit unstable cells. This shall in addition improve efficiency of post-processing and thus lead to cost-optimized and reliable hardware integrity anchors.

The behaviour of the optimized cell array is being modelled and emulated in an FPGA-based prototype setup, which allows for easy integration with novel post-processing algorithms being researched in later phases of the HINT project.

Contents

List of Figures

Chapter 1 Introduction

This document describes and reports on work mainly performed in task 2.1 and task 2.2 in the HINT project as defined in the Annex-1 to the grant agreement (description of work [DoW]). This document will have strong impact on the research towards post-processing in task 2.3 and on attack scenarios in task 2.4.

One of the WP2 objectives in the HINT project had been defined as: **”better and fully understand technology limitations for reliability of today’s hardware integrity anchors.”**

As a second objective we targeted the **area- cost- and energy-optimization of analogue as well as digital components** for novel hardware based integrity anchors, both, in terms of hardware-footprint as well as in terms of overhead for firmware / software post-processing.

While detailed research on the behaviour of 65 nm CMOS transistor devices allowed on the one hand for optimizations in terms of cell structures and design variants we had to accept on the other hand that some deterministic temperature effects cannot be avoided by design measures in SRAM-like cross-coupled structures. Due to the statistical distribution of parameters influencing these effects we will always see some potentially instable cells in an array. Therefore mechanisms to avoid use of such potentially instable cells have to be implemented such that the error rate of extracted raw data vectors needs to be small in order to enable use of optimized post-processing. In addition, methods had to be developed to characterise cells and to distinguish which candidate cells probably will or will not be stable over the specified temperature range.

By means of this document we report, that the first of the above mentioned objectives of WP2 has clearly been achieved, and that for the second objective all analogue and cell-array relevant optimizations have been researched, most of them designed and simulated to be prepared for use in a next instance of a test chip silicon. Digital components for post-processing and firmware / software components are not part of this report.

There are four main topics covered within this report:

- Understanding artefacts and CMOS-technology properties and their nature, severity, and impact in 65 nm CMOS flash technology
- Novel cell concepts for hardware genuineness anchors
- Novel architecture concepts for area and power/energy optimization
- Novel concepts to distinguish robust from instable cells during manufacturing test

Research performed towards advanced post-processing in hardware, firmware and software as well as FPGA-implementation of the novel cell- and architecture concepts will be reported in deliverable D2.2 – “FPGA-prototype including advanced post-processing methods and techniques”. Attack scenarios will be described in deliverable D2.3 – "Report on success/failure of attacks and countermeasures on the newly proposed integrity anchors”

Chapter 2 Integrity Anchors in the HINT Context

Integrity checking as we understand it for the HINT context is composed of two - basically orthogonal - approaches:

On the one hand the genuineness of hardware as well as the connection of software to a dedicated piece of silicon and the possibility to test for such a connection shall add an additional layer of trust in ICT systems. Based on such connection a vertical stack of trust dependencies could be achieved, e.g. portions of encrypted code could be decrypted by such key and only lead to meaningful results and executable code if that very key is extracted in the correct way and thus is of integrity in itself. Such a key that is embedded and hidden in a process variation dependent, chip-individual storage would be available only during runtime, or even shorter, only on demand.

On the second hand Hardware Trojan (HT) detection based on side channel information is a method to ensure system integrity from an outer, horizontal view to the system. In this case the side channel behaviour of a "golden device" is compared with the extracted side channel data of the device or system under test. The aim is HT detection before the Trojans get activated which often is too late to prevent from damage to the ICT system and harm to users. Inside the HINT project research on HT detection is performed in work package WP3.

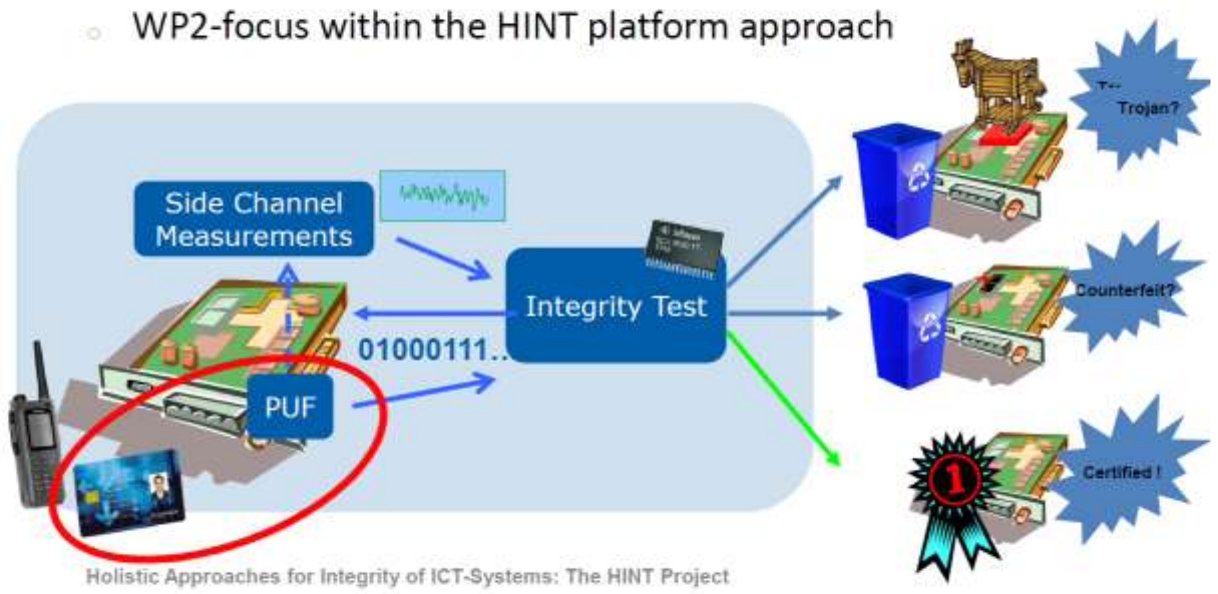

WP2-focus within the HINT platform approach
Side Channel Measurements
Integrity Test
01000111..
PUF
Trojan?
Counterfeit?
Certified !
Holistic Approaches for Integrity of ICT-Systems: The HINT Project

Figure 1: Focus point Hardware Genuineness Anchor within the HINT project

While the overall HINT goals are formulated as to research towards such holistic approaches for integrity of ICT systems, the work in task 2.1 within WP 2 is a necessary sub-group of research questions towards these goals. This research focuses on exploitation of material based production variations as they are used for physically unclonable function (PUF) modules. Its aim is to understand instabilities and artefacts which partly prevent their commercial exploitation and definitely foist a huge burden on the post processing. As a consequence such post processing is harder and more expensive to implement in a secure way to minimize side channel leakage when finally extracting the key on which security relevant protocols shall be based.

The learning from task 2.1, from the research on technology dependent limitations for PUF cells, is then immediately transferred to task 2.2 enabling novel cell and architecture concepts. Such novel concepts shall allow for PUF implementations with improved robustness and cost efficiency including adequate optimizations for mass production (design for manufacturability), and thus becoming better industrially exploitable.

2.1 Application Context and Use Case Environment

Application of hardware based integrity anchors can have various flavours, starting from pure identification of the very integrated circuit in use by a more or less unique identifier. Here the purpose of the PUF is to distinguish one instance of a functionally identical design from another and with the requirement of minimizing collision probability amongst those instances. Robustness issues in terms of bit error rates (BER) after read-out can be easily handled by threshold definitions. Another flavour is to authenticate such instances by means of challenge-response protocols, which can be based on symmetric or asymmetric cryptography. As soon as cryptographic algorithms shall be applied the exact reproducibility of read-out values is getting crucial, since - due to the diffusion property of cryptographic algorithms (1-bit changes at the input shall produce approximately 50% bit changes at the output) - bit errors must be completely corrected before application of the cryptographic protocols. One alternative approach towards this strict rule is to apply algorithms similar to the ones used in biometrical applications.

2.1.1 Hardware Genuineness Anchors for eID applications

As depicted in deliverable D1.1 – "Report on use case and architecture requirements" [D1.1] there are basically two types of PUF principles, so called strong PUFs and weak PUFs. Strong PUFs aim to directly allow for application of challenge-response type protocols whereas weak PUFs are meant for key extraction in order to apply strong cryptographic protocols based on those extracted keys. In these technology-oriented tasks of HINT we do not research on strong PUFs, but focus on key extraction from weak PUFs since the extracted keys allow for a connection of a variety of well known and established cryptographic protocols to the IC they are performed on. Focussing mainly on the “ID card use case” the goal of the WP2 research is to provide raw data with improved robustness and reduced bit error rates. Such raw data with improved quality will allow for minimized footprint of post-processing and thus to best-in-class seamless integration of PUF-based keys into cryptographic protocols, such as Elliptic Curve Cryptography (ECC) based signature generation, which is a typical protocol in the ID card environment. Besides the pure PUF-based derivation of keys (i.e. random values derived from processing variations) it may be of special interest in some cases to embed a specific key to the PUF, which has been generated independently from it in a different step or process, e.g. by means of a true random number generator (TRNG), and thus hide such a key in the material properties of the chip. One advantage may be the use of certifiable TRNGs for the key generation or key generation outside a chip in a secure environment, e.g. to accelerate personalisation in mass production scenarios and ensure sufficient entropy regardless of a PUF’s potentially deficient entropy. Also embedding of e.g. a serial number in a distinct well-defined format (potentially hashed, encrypted, or blinded by another key) into the PUF may be of interest.

In deliverable D1.2 – “Report on specifications and overall architecture” [D1.2] the overall top level schematic of an integrated circuit including PUF module for such an ID card has been shown in Figure 10. Sub-components of the PUF module have been listed and depicted as well in Figure 11, which is here shown again as a reference and to point out graphically the focus area of this deliverable, which is the research on the cell array itself.

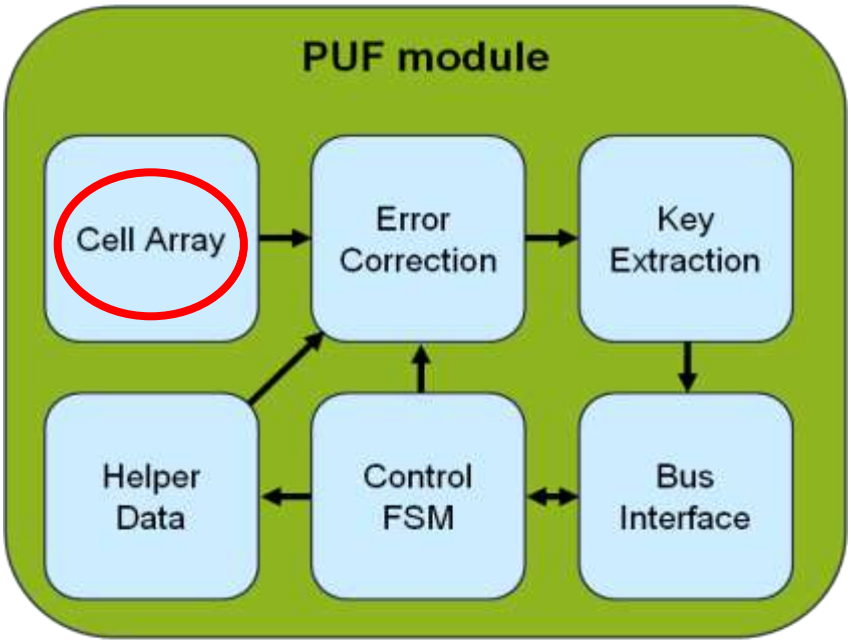


Figure 2: Necessary components of a PUF module to exploit weak PUF based key extraction

2.1.2 Generalization of the impact of research described in this document

In WP2 of the HINT project, and especially in the work associated with this deliverable D2.1, we are focussing heavily on the challenge to improve robustness of read-out raw data in order to enable optimized post-processing. This focus shall improve integration of hardware integrity anchors in all different types of application flavours since it targets the root problem of errors in raw data read-out from silicon. Such increased quality of raw data triggers the improvement of cell design as well as architecture optimizations of the hardware integrity anchors themselves. Thus it does not matter for the research on technology based robustness issues whether extracted keys are later used for challenge-response protocols, for TPM-like integrity checks (e.g. secure boot) or signature generation based on embedded and re-extracted keys.

2.2 So far used Cell Concepts and Architecture

2.2.1 Cell Design

The basis to the improved cell design is a PUF cell that was produced in a 90nm flash technology. The concept behind the cell is a two-stage approach (see Figure 3). During the first phase (*amplification phase*) the mismatch between the mismatch sources (I_bias1 and I_bias2) is amplified. During this phase the influence of parasitic mismatches (e.g. parasitic capacitors or noise) on the output of the cell is minimized. Once the output has settled a trigger signal starts the second phase (evaluation) and the final output of the PUF cell is defined.

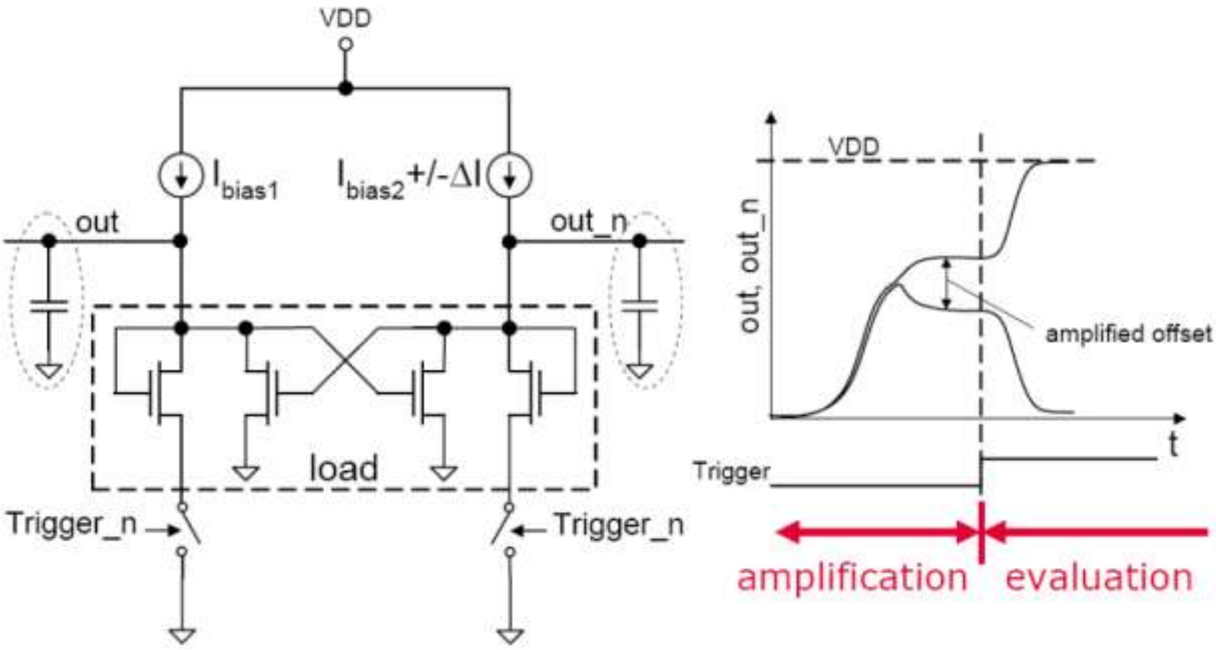


Figure 3: Two-stage PUF (left), the phase concept can be seen on the right.

A schematic of the cell can be seen in Figure 4. Here, the PUF transistors are two PMOS transistors (m1, m2) followed by two cascode transistors. The lower part of the circuit builds the sense amplifier which should have no influence on the decision.

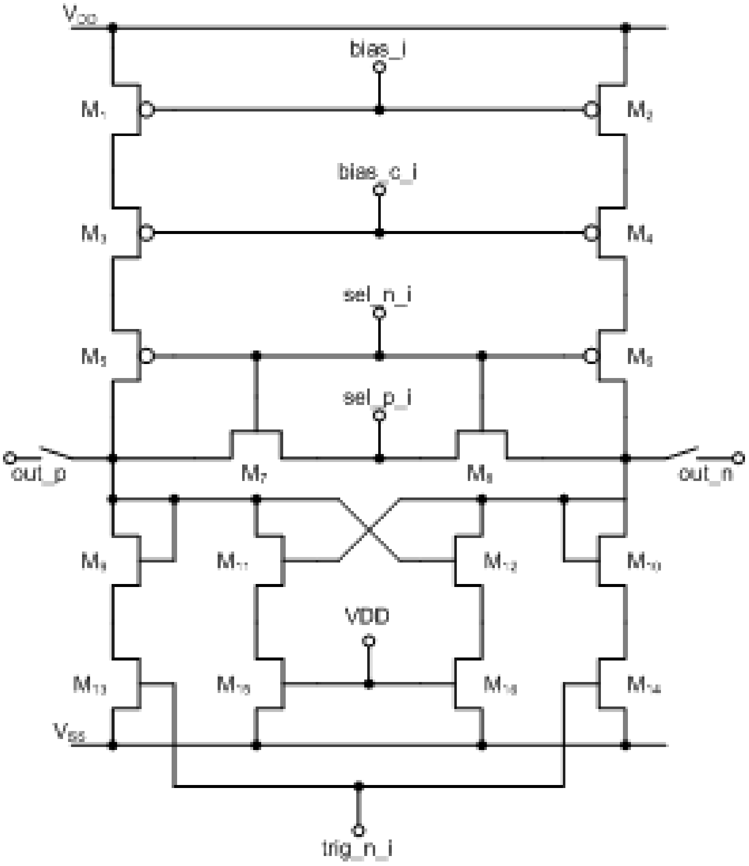


Figure 4: Symmetric cell concept with biasing exploiting mismatch in PMOS transistor pairs.

2.2.2 Measurement Results:

Each test chip consists of 4096 cells. 240 chips were measured and analysed. Figure 5 shows the crucial results. The blue curve shows the noise induced intra-chip errors which are below one percent. The low noise induced error rate shows the expected behaviour of the two-stage approach. The biggest problem occurs during temperature shifts. Here, the error rate increases to values higher than six percent.

Due to a strong focus on symmetrical layout and cell design no significant correlations between bits and chips could be found. Furthermore, neither significant imbalances nor shifts to either ‘1’ or ‘0’ could be detected.

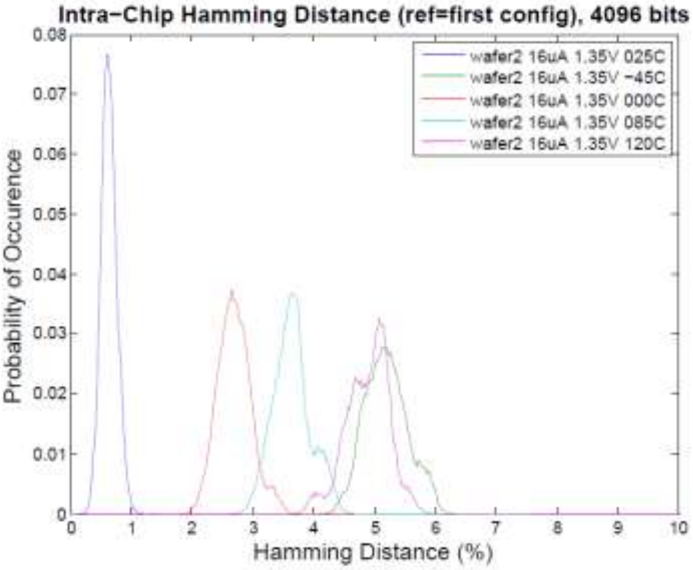


Figure 5: Measurement results of the PUF: Temperature dependent output.90nm two-stage.

2.3 Understanding Technology Artefacts

To achieve robustness and manufacturability for mass production of PUFs it is essential to understand technology artefacts as observed on the 90nm test chips and to project further the impact of such artefacts by appropriate simulation to state-of-the art CMOS technologies used for novel PUF cells before prototype production. Based on such understanding appropriate measures can be designed, like biasing of ideally symmetric branches in the cell-structure for robustness-testing and consecutive distinction between robust and not so robust cells.

2.3.1 Sources of instability of (SRAM-like) PUF cells

There are mainly four stability issues concerning the PUF cell output.

- Noise: Noise influences the decision process of a PUF cell. Especially for cells with small mismatch the noise can get the dominant factor and thus the cell’s output becomes unreliable.

- Line stability: Noise on the supply voltage can influence the operation point of the mismatch transistors. This can force the transistors in regions where the mismatch between the transistors changes which can lead to different outputs and thus to errors.
- Temperature dependencies: The biggest problem in PUF cell design is the temperature behaviour of the cells. Temperature coefficient mismatch of the involved transistors leads to an instability of the PUF output.
- Aging: In general also the aging process of the transistors may have an effect on the PUF cell output. Since our dedicated PUF cells are in power down state most of the time, the problem of aging can be considered being minimized in such a way that the aging mechanisms are not effective over the life cycle of an IC using such a PUF (e.g. up to 10 years in eID applications).

2.3.2 Measures against instability

There are different ways to cope with the sources of PUF errors. Some are described below:

- Noise: Noise induced errors can be reduced by multiple read-outs of a single cell. A majority decision of the outcome defines the final cell output. Furthermore a pre-selection of cells showing a high mismatch can reduce the noise induced errors.
- Line stability: Line stability can also be reduced by multiple read outs. Furthermore, a supply-voltage insensitive voltage reference/current source and compensate by adapting the bias voltage for the mismatch transistors. Also, pre-selection can help.
- Temperature dependencies: Temperature coefficient mismatch induced errors can be reduced by pre-selection. Thus, only those cells are used that show a high mismatch between the cells, high enough to exceed effects of the temperature bias within a defined temperature range. So, even if a temperature coefficient mismatch exists, such cells will then not change their outputs in this temperature range.
- Aging: If the cell is not biased constantly and the currents through the cells are minimized aging also can be minimized. This can be done by removing the supply as long as the PUF is not used and by biasing the cell with a constant current source.

2.3.3 Measurements and statistical evaluations

To evaluate the performance of the PUF cells, the following tests have to be applied to the measurement data.

Mean value: The distribution of the mean values of output bit values from all the PUF cells of each chip should follow a binomial distribution. Then, the output may be considered being unpredictable. An example can be seen in Figure 6.

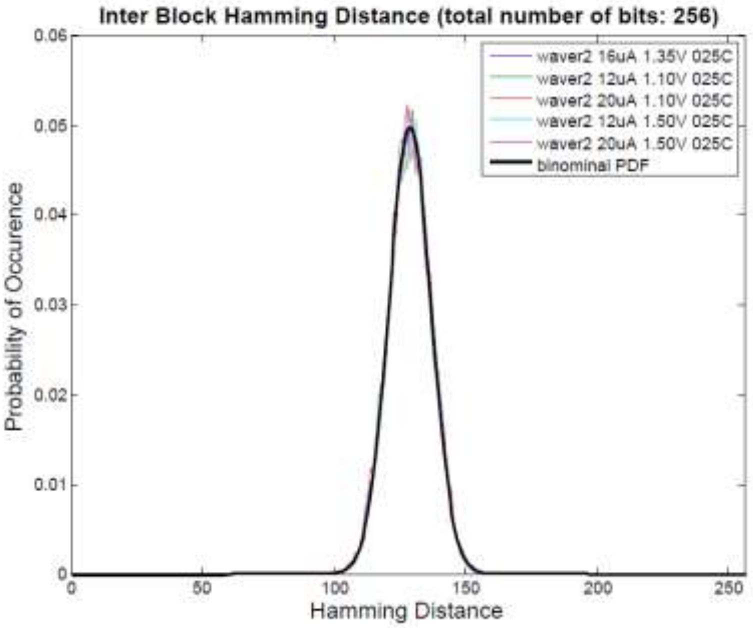


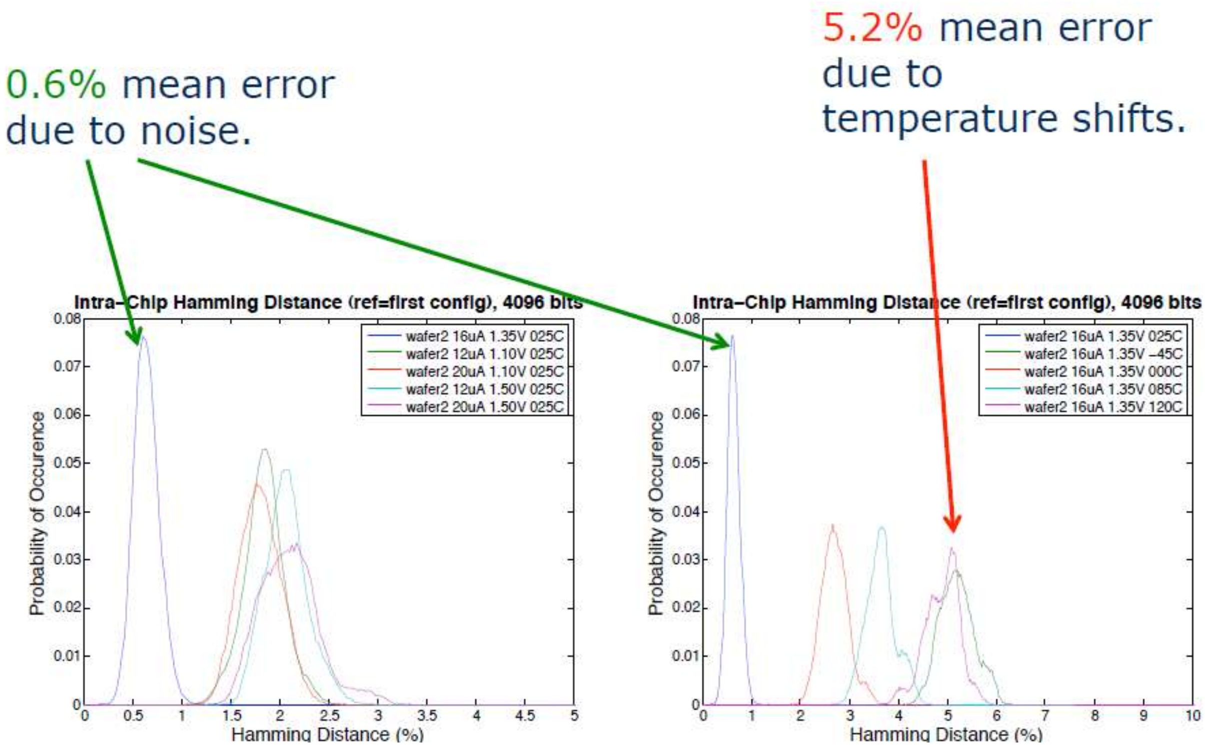
Figure 6: Binomial distribution of 90nm PUF cell output.

Bit Error Rate (BER): The so-called intra-chip Hamming Distance shows the error rate with respect to an initial vector. As an initial vector we refer to the bit-wise mean-value of a repeatedly read-out block of bits at room temperature. For the PUF output the intra-chip HD should be always minimized especially if the PUF is used for key generation purposes.

Correlation (intra, inter): The correlation between the PUF output bits within one chip and also between chips should be zero. To test this property, the simple correlation can be calculated. Intra-chip correlation may appear in cases where parts of the circuits are shared between different PUF cells or if the chip layout biases the output. Inter-chip correlation could appear mainly due to layout issues.

2.3.4 Observations

As shown in Figure 7, the influence of noise is rather small. The mean error rate due to noise is about 0.6%. The left diagram in the following figure shows that, as soon as the transistor bias changes, the transistor mismatch move and thus the error rate increases up to 3.5%. The bigger problem arises from temperature coefficient mismatches. Such errors can be seen in the right diagram of the figure. Here, errors up to 6.5% were measured.



0.6% mean error due to noise.

5.2% mean error due to temperature shifts.

Figure 7: Noise based versus temperature based BER.

In Figure 8 the temperature dependence of the error rate is shown.

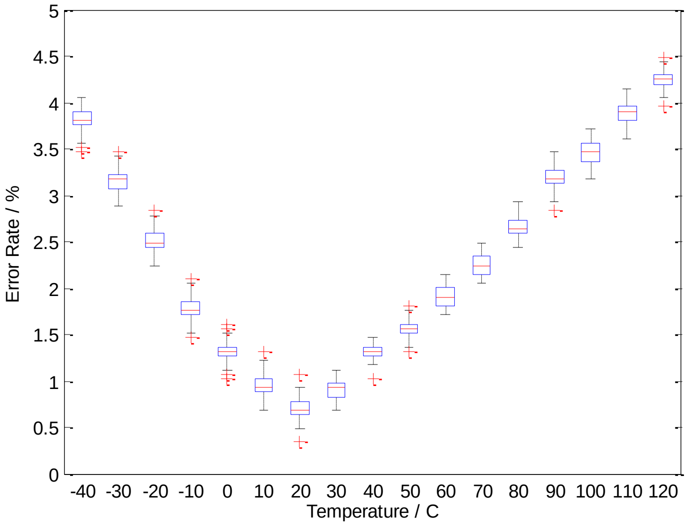


Figure 8: Temperature dependent error rate.

2.3.5 Deeper Analysis of Temperature Behaviour

To be able to predict the behaviour of the 65nm CMOS PUFs, the 65nm transistors were analysed in a transistor simulation tool called TCAD. TCAD allows simulating the physical behaviour of the transistors and thus to make assumptions on the real chip behaviour independently of the available spice models. As in the 90nm node, the results for the 65nm node show the temperature coefficient mismatches. The proposed way to provide that mismatch to the spice models is as follows:

For minimal size transistors (which are used in PUF cell design to maximize the mismatch) the halo implants from the source and the drain region are touching each other and form a channel doping which is different from the well doping (Figure 9, left side).

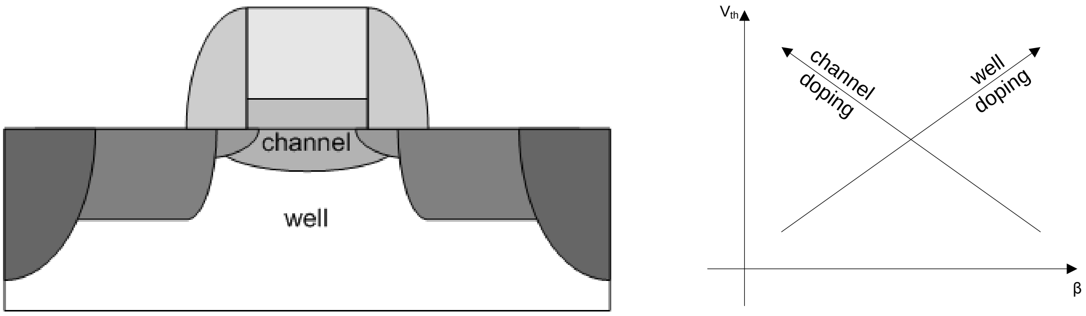


Figure 9: Minimal size transistor (left), threshold voltage [V_{th}] vs. mobility [beta] (right).

The simulations show that an increase in channel doping leads to an increase in threshold voltage (V_{th}) in combination with a decrease of mobility (beta) (see Figure 9, right side). At the same time, an increase in well doping is also followed by an increase in threshold voltage but now also increases the mobility. Since both effects are coupled to a shift in the temperature coefficients, there exist transistors that show the same current flow at a certain temperature but a different current flow once the temperature is shifted.

The TCAD simulations results can be seen in Figure 10. Here, the current flow at three different temperatures is shown through transistor 1 (blue) and transistor 2 (red), forming a mismatch pair as used in the PUF cell. For the upper two temperatures transistor 1 is weaker than transistor 2. At the lower temperature transistor 1 is stronger. To provide this effect also in Monte-Carlo simulations, the models can be adapted in a way to adjust the temperature coefficients once either the threshold voltage or the mobility changes its value.

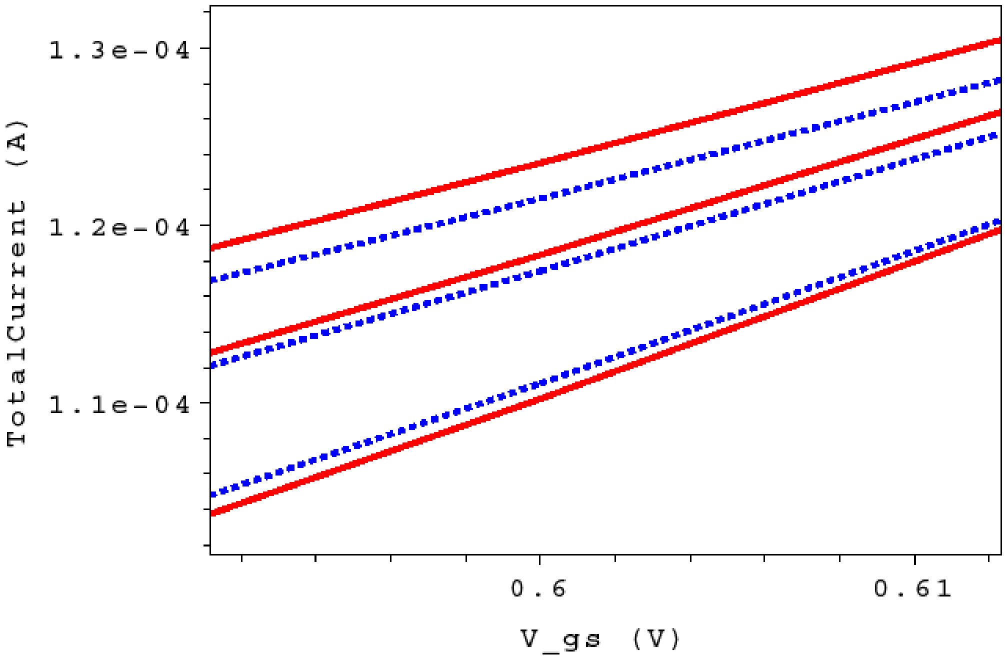


Figure 10: TCAD simulation results: Drain current of two transistors (red, blue) at three different temperatures.

Chapter 3 Novel approaches for Integrity Anchors

3.1 Design approaches towards a 65nm Test-Chip

There were two major problems related to the first test chip: The error rate especially for temperature shifts was too high to be able to use simple (e.g. one-step) error correction algorithms. Furthermore, the absolute size of the PUF cell array was too big. Solutions for both problems are presented below.

3.1.1 Making use of inherently greater mismatch of NMOS transistors

To minimize the size of a PUF cell and at the same time maximize the mismatch within the cell, NMOS transistors are used instead of PMOS transistors. NMOS transistors show a higher degree of V_{th} mismatch and thus should be preferred in PUF cell design. Furthermore, due to the inherent higher free charge mobility, the NMOS transistor can be around three times smaller than the PMOS counterparts. A NMOS PUF cell can be seen in Figure 11.

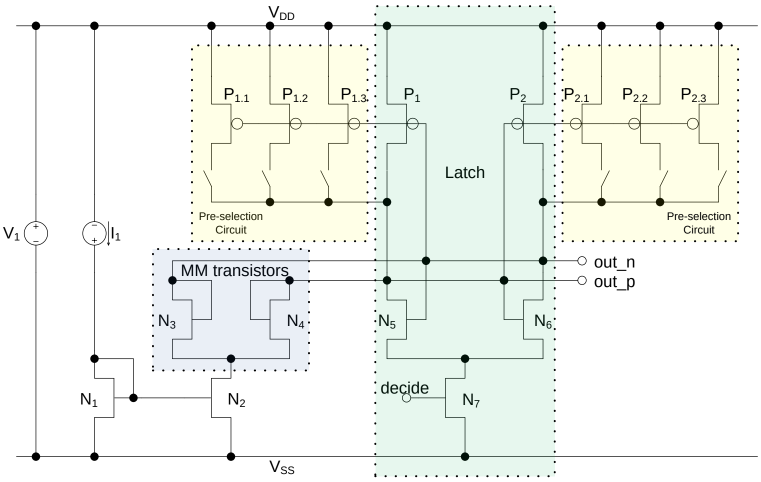


Figure 11: Novel cell concept exploiting NMOS transistor V_{th} mismatch and pre-selection concept.

3.1.2 Pre-select relevant cells

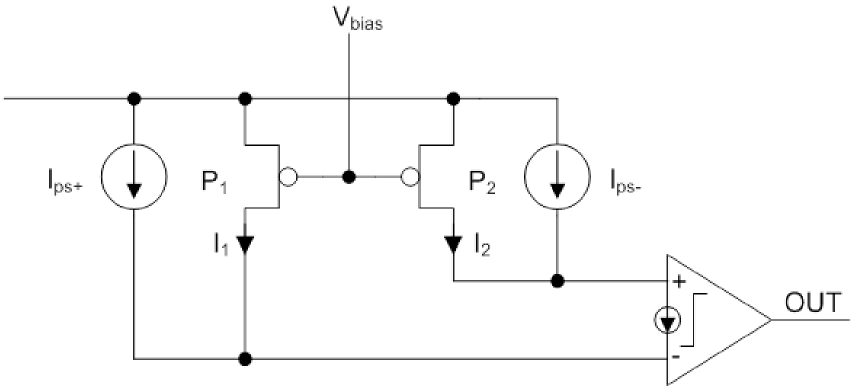


Figure 12: Pre-selection concept.

A way to reduce the error rate is to pre-select those cells, that show a high mismatch and thus are less likely to switch the output with respect to any change of operation region. Using this approach all kinds of errors can be reduced: temperature related errors, noise related, aging related and supply related errors. The idea behind the pre-selection approach is rather simple: Before defining a reference output (which is done once in the Fab and then used from then on), all cells are biased in both direction with a pre-defined bias level. Only those cells will be used that provide the same output independently of the applied bias. An example can be seen in Figure 12. Here, an additional current can be applied either P1 or to P2. Figure 13 show measurement results of a PUF with pre-selection. Depending on the bias level, the number of used cells (efficiency) is increased or decreased, respectively.

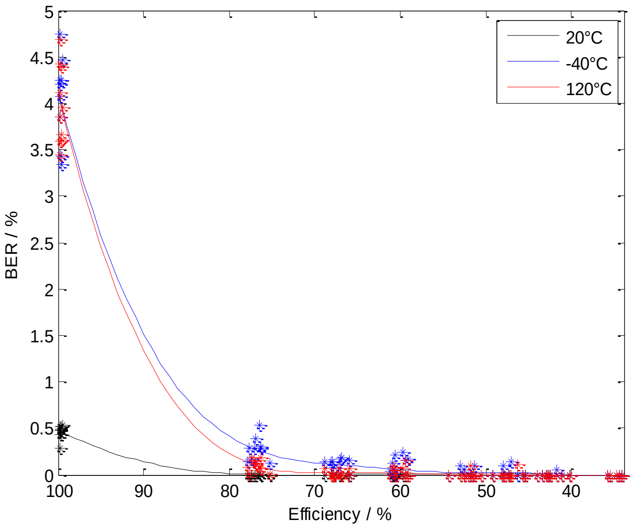


Figure 13: Error rate vs. selection rate (efficiency) at three different temperatures.

The measurement results show that for selection rates of 80%, the overall error rate (including all temperatures) decreases below 1%. The implementation example can be seen in Figure 11.

3.1.3 Shared sense amplifiers

To reduce the size of the PUF array, the cell size can be reduced not only by using NMOS transistors but also by sharing the biggest part of a PUF cell which is the sense amplifier. An example can be seen in Figure 14. Here, a number of cells share the same amplifier. As a consequence, the risk of correlation becomes the biggest problem. If the design and the layout of the amplifier is not done carefully, all the cells which are connected to on amp provide the same output value in a worst case scenario. Such a design must be done in a way to minimize the local mismatches and biases of the amplifier. The sense amplifier sharing was implemented in a test chip in 90nm. The correlation results can be seen in Figure 15 and Figure 16. In Figure 15 a PUF with no correlation between the bits can be seen. In Figure 16 the PUF with a sharing of 16 cells is shown. Here, the mean correlation (red line) is clearly above the uncorrelated mean. Signal processing mechanisms can be used to compensate for such kind of correlation.

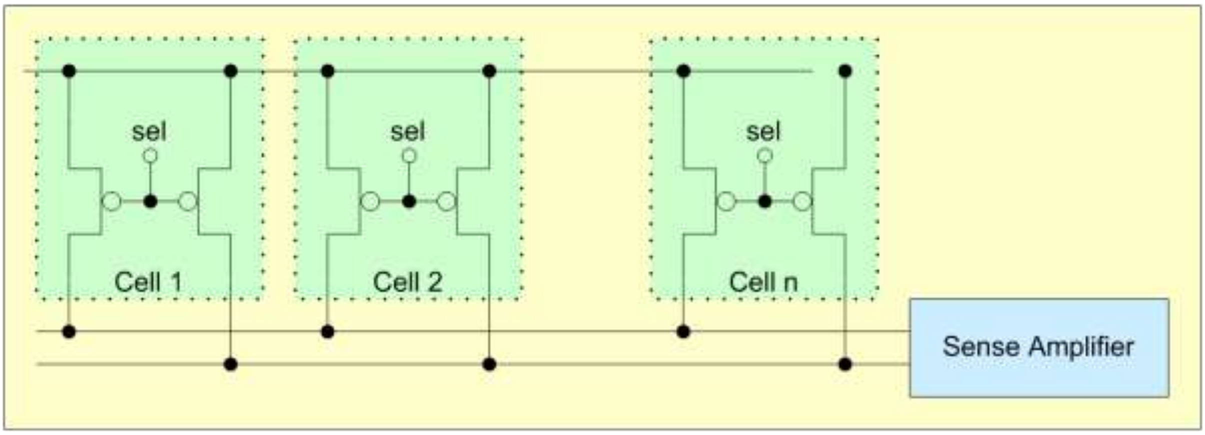


Figure 14: Shared sense amplifier concept.

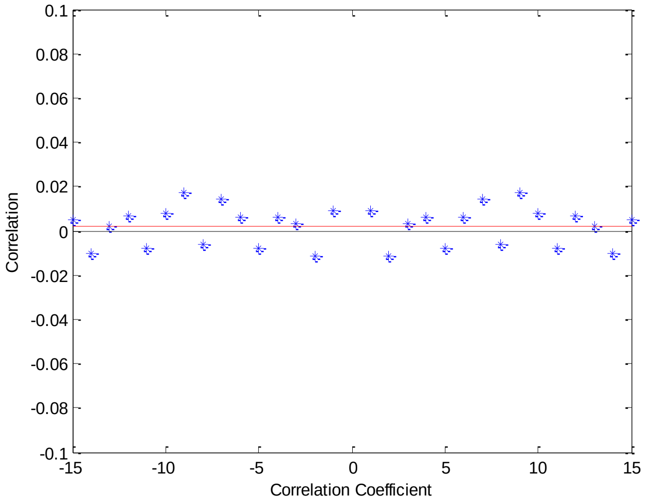


Figure 15: Correlation between block of cells amplifier sharing. The red line marks the mean correlation value.

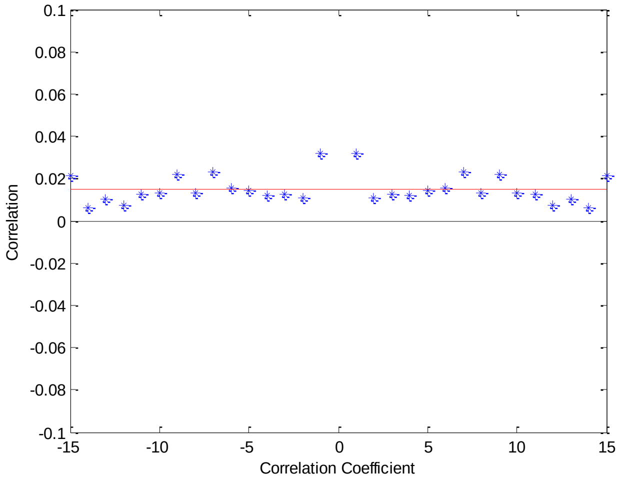


Figure 16: Correlation between block of cells amplifier sharing. The red line marks the mean correlation value.

3.1.4 Implementation in a 65nm Technology

The latest test chip was implemented within the HINT context. The technology is a 65nm flash technology. The new test chip combines the optimization approaches of its predecessors and further implementation ideas: The chip contains a two-stage approach to minimize the influence of mismatches induced by parasitic, like e.g. layout dependent capacitances. A single cell consists of only 4 NMOS transistors which optimizes the area and maximizes the local mismatch. The sense amplifier is shared by a number of cells. The sense amplifier sharing is a trade-off between area consumption and cell correlation. The layout of the shared sense amplifier including the array of PUF cells is done in a way that the overall area per bit (including sense amplifier) is smaller than the size of an SRAM cell. The implementation of the pre-selection is also done in a novel way. Instead of providing additional current via current sources, the gate voltages of the mismatch transistors are biased directly (see Figure 17). Thus, the area overhead of the pre-selection is reduced to a minimum since the circuitry is needed only once for all the PUF cells. A schematic overview of the novel cell concept can be seen in Figure 18. Since the chip is just produced there are no measurement data available yet.

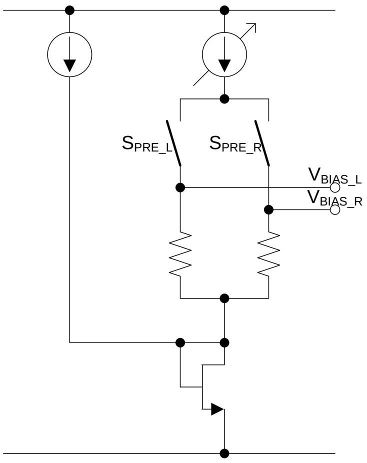


Figure 17: Implementation of pre-selection circuit of latest 65nm test chip.

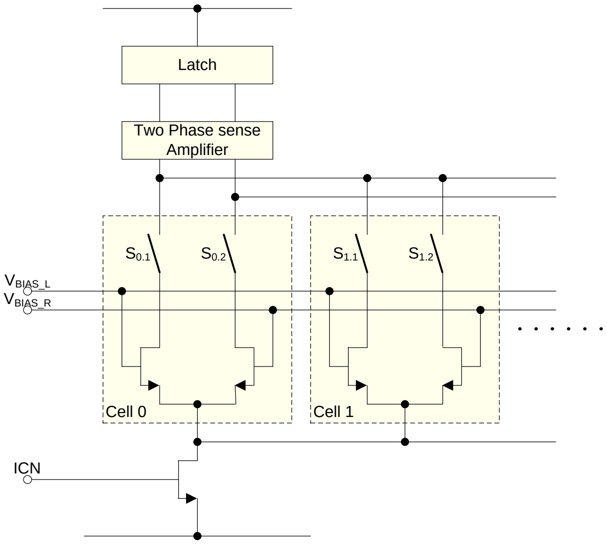


Figure 18: Implementation of cell concept of latest 65nm test chip.

3.2 PUF Error Reduction Concepts

Within the HINT context, different novel approaches of error reduction of PUF outputs were developed. Two of the approaches are described below:

3.2.1 Pre-Selection by Increasing the Noise

3.2.1.1 Concept

The proposed solution increases the influence of noise. By reading out the PUF multiple times during an initial phase, unstable cells can be detected.

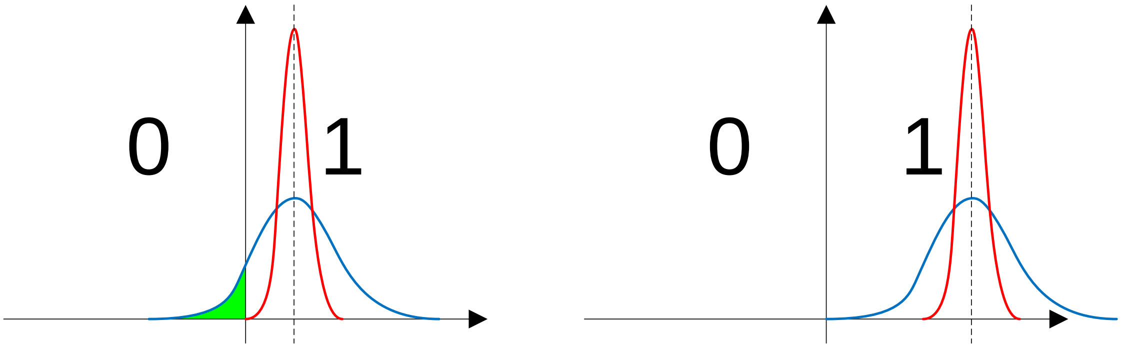


Figure 19: Increasing the noise artificially (blue) helps to discriminate potentially instable cells with small mismatch (left) from more stable cells with large mismatch (right). Without noise increase (red), the instable cell cannot be determined.

In Figure 19 the idea is depicted. On the x-axis the overall mismatch of one PUF cell is shown. In this case, the mismatch is positive (dashed line) and thus the cell returns a ‘1’ at the output. The influence of noise on the cell's decision is shown in by the red Gaussian distribution. The noise adds to the mismatch and may cause a wrong decision. It can be seen that the probability that this cell will output a '0' is very small. After introducing noise artificially (blue curve) the probability of a wrong output increases. Applying artificial noise to all the cells can be used to separate the stable from the unstable cells. Here, the number of unstable cells is determined by the power of the noise which one has to define in advance.

3.2.1.2 Practical Realisation

3.2.1.2.1 <u>Power Supply Boosting</u>

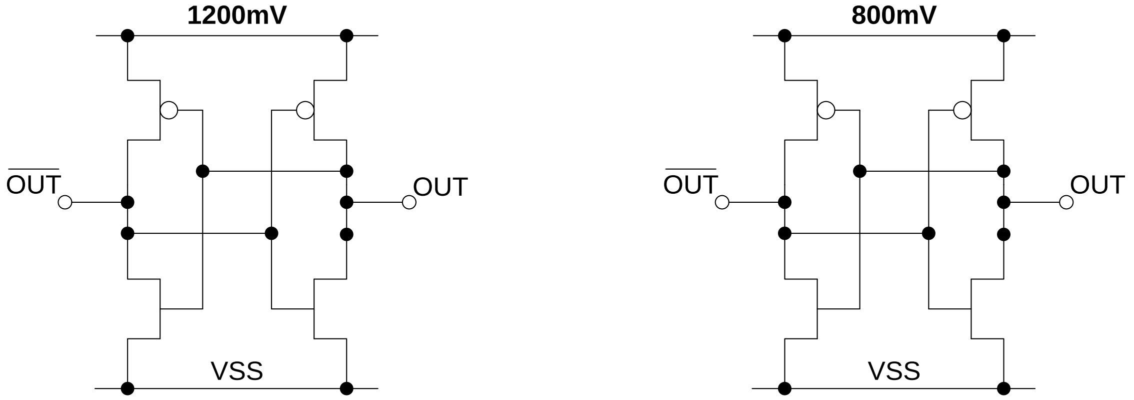


Figure 20: SRAM cell with high (left) and low (right) power supply.

In the left schematic of Figure 20, the supply voltage is increased to maximize the influence of noise during the decision (power-up of SRAM cell). In operation mode, the supply voltage is decreased (right schematic) and the decision process in the cell will be slower. Thus an averaging of the noise occurs.

3.2.1.2.2 <u>Averaging noise with capacitances</u>

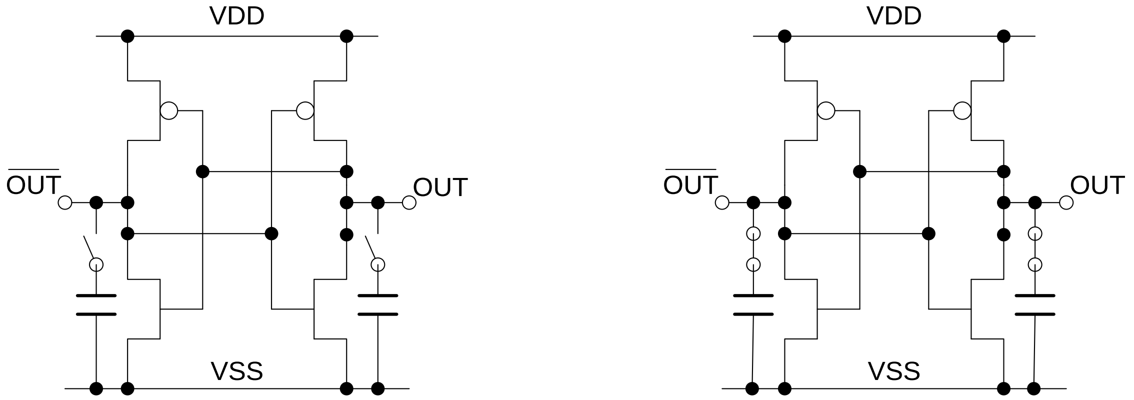


Figure 21: SRAM cell with high input cap (left) and low input cap (right).

In the left schematic of Figure 21, the decision is done very fast without a cap (initial phase) and thus the influence of noise is maximized. During operation the decisions will be done much slower (right circuit) with reduced noise at the inputs.

3.2.1.2.3 Noise Generator based approach

A more complex approach is shown in Figure 22. Here, a noise generator has to be attached to the circuit. In the left schematic the noise generator is enabled (pre-selection phase). During operation mode (left figure) the noise source is switched off.

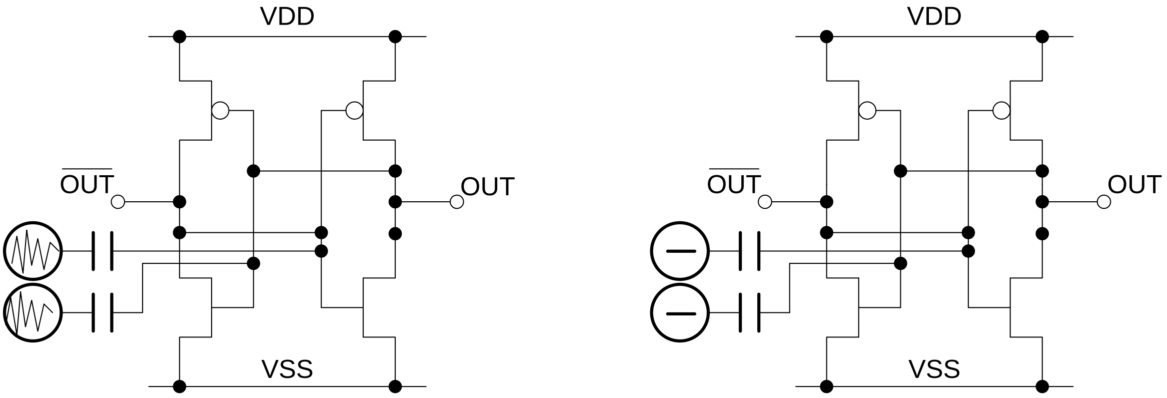


Figure 22: SRAM cell with additional noise generator.

3.2.2 Temperature Dependent Error Correction

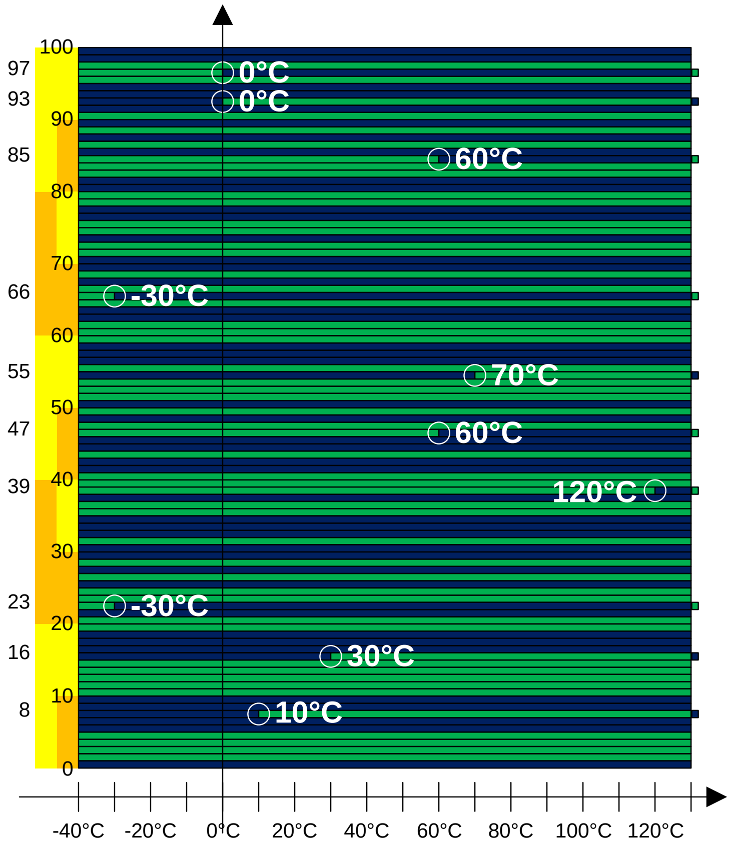


Figure 23: Temperature dependent flipping chart of 100 PUF cells, showing instable cells by changing colour codes and depicting the temperature values at which changes occur.

In Figure 23, a temperature dependent flipping chart of 100 PUF cells in the range between -40°C up to 130°C is shown. Most of the bits are stable over the whole temperature range. Some of the bits toggle in dependence of the temperature. In Figure 23, 10 of the 100 bits flip in the whole temperature range: Bit 8, 16, 23, 39, 47, 55, 66, 85, 93 and 97. The reason for this behaviour is a mismatch in the temperature coefficients. This mismatch is depicted in Figure 24.

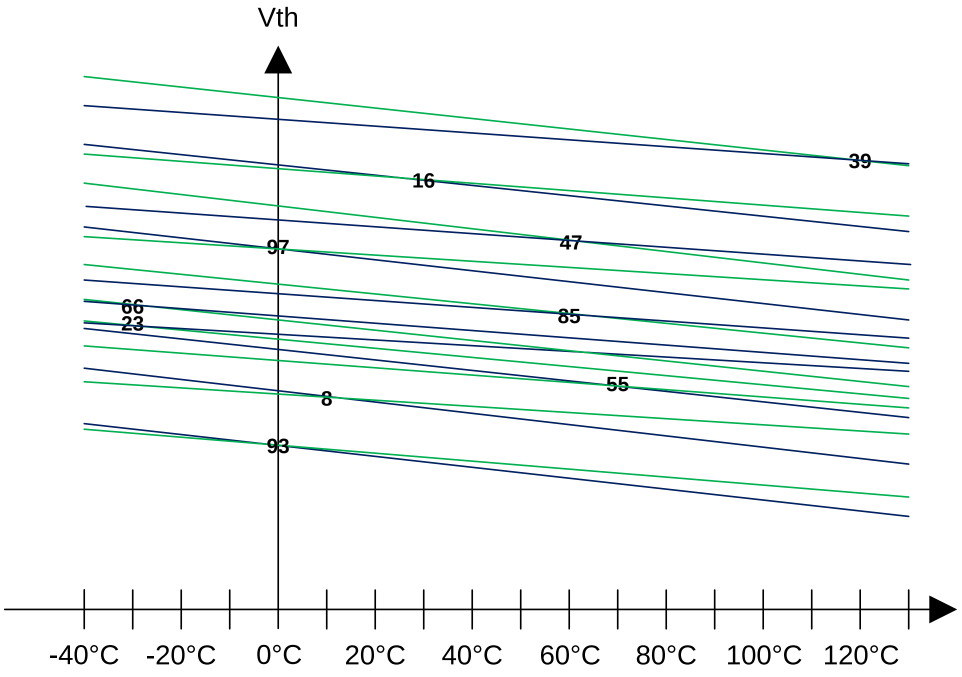


Figure 24: Temperature dependent V_{th} mismatch of affected (Fig. 21) PUF cells.

To allow a temperature dependent error correction, those bits that flip are put into an order depending on the temperature of flipping. For the example of Figure 23, the ordering is done in the following way:

Cell	**Order**
8	5
16	6
23	1
39	10
47	7
55	9
66	2
85	8
93	4
97	3

After sorting, the following order of the unstable bit cells can be derived: 23, 66, 97, 93, 8, 16, 47, 85, 55 and 39. The ordering has to be done during an initial temperature sweep.

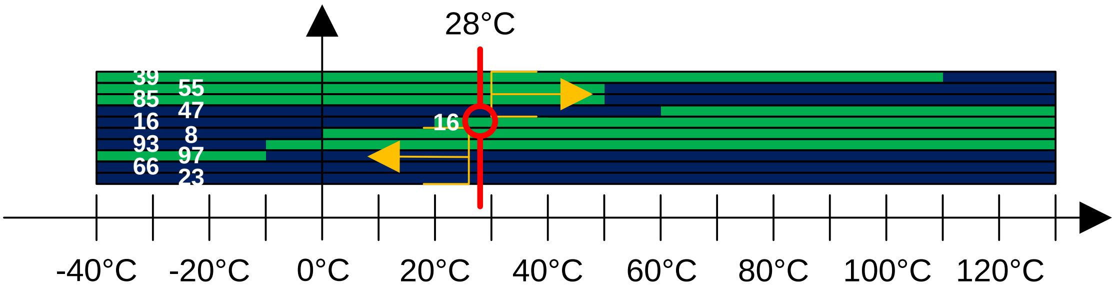


Figure 25: Read out at 28°C.

Once the ordering is known, the error correction can be done as shown in the following example (Figure 25): At 28°C the read out of the PUF cells is done. After multiple read outs it can be seen that the cell #16 flips. Due to this knowledge it is obvious that the cells with a lower order (cells 23, 66, 97, 93, 8) already switched and the cells with a higher order (cells 47, 85, 55, 39) are not switched. One of these groups either the lower order or the higher order group has to be inverted to correct the error with respect to the reference vector. In this case, the right output of the unstable cell #16 cannot be determined and must be corrected by the post-processing error correction.

Chapter 4 Outlook: Modelling, Emulation and Implementation

Exploiting the described research and novel cell and architecture concepts partner IFAT has written a specification for a dedicated PUF array emulator model representing the cell array and bus interface. In addition IFAT has written a MATLAB-script providing sample vectors representing the error behaviour of the bits in the array. Based on the specification and MATLAB-model partner TEC is currently implementing a PUF emulator on a Xilinx ML501 Virtex5 FPGA board. This emulator will then be used as basis for the prototype which will be described in the upcoming deliverable D2.2. The emulator follows the concept of the novel cell architecture.

Basically, the PUF emulator operates like a ROM. Generating the PUF responses is a four step procedure. First of all, the input data is generated by means of a MATLAB scripts (based on the Gaussian distribution) in order to create offset values that are characteristic for the behaviour of the PUF. This information will the in a second step serve as input for the hardware simulation on the FPGA board. In the third step the temperature and some other parameters get updated. This provides some level for the emulator and the functionality can be evaluated for different conditions. The final step is the actual read out of the simulated PUF response. With this PUF emulator it is possible to simulate the response behaviour of one single PUF but also compare different PUF emulations.

Currently, several tests are performed on the emulation in order to align the statistical behaviour of the emulation with the data provided by a physical PUF. The next step will then be to include different error-correcting mechanisms and design a complete system, which is exactly the content of D2.2.

Chapter 5 List of Abbreviations

BER	Bit Error Rate
CMOS	Complementary Metal Oxide Semiconductor
ECC	Elliptic Curve Cryptography
FPGA	Field Programmable Gate Array
FSM	Finite State Machine
HD	Helper Data
HT	Hardware Trojan
NMOS	N-type Metal Oxide Semiconductor
PMOS	P-type Metal Oxide Semiconductor
PUF	Physically Uncloneable Function
RNG	Random Number Generator
SRAM	Static Random-Access Memory
TCAD	A transistor simulation tool
TPM	Trusted Platform Module
TRNG	True RNG
V_{th}	Threshold voltage (of CMOS transistors)

Chapter 6 Bibliography

[DOW] HINT-project “Description of Work”, V2.0, 2012

[D1.1] HINT-project “Report on use case and architecture requirements”, 2013

[D1.2] HINT-project “Report on specifications and overall architecture”, 2013