Evaluation of 90nm 6T-SRAM as Physical Unclonable Function for Secure Key Generation in Wireless Sensor Nodes

Georgios Selimis, Mario Konijnenburg,
Maryam Ashouei, Jos Huisken, and Harmke de Groot
Holst Centre / IMEC
http://www.holstcentre.com
Eindhoven, The Netherlands

Vincent van der Leest, Geert-Jan Schrijen,
Marten van Hulst and Pim Tuyls
Intrinsic-ID
http://www.intrinsic-id.com
Eindhoven, The Netherlands

***Abstract*—Due to the unattended nature of WSN (Wireless Sensor Network) deployment, each sensor can be subject to physical capture, cloning and unauthorized device alteration. In this paper, we use the embedded SRAM, often available on a wireless sensor node, for secure data (cryptographic keys, IDs) generation which is more resistant to physical attacks. We evaluate the physical phenomenon that the initial state of a 6T-SRAM cell is highly dependent on the process variations, which enables us to use the standard SRAM circuit, as a Physical Unclonable Function (PUF). Important requirements to serve as a PUF are that the start-up values of an SRAM circuit are uniquely determined, unpredictable and similar each time the circuit is turned on. We present the evaluation results of the internal SRAM memories of low power ICs as PUFs and the statistical analysis of the results. The experimental results prove that the low power 90nm commercial 6T-SRAMs are very useful as a PUF. As far as we know, this is the first work that provides an extensive evaluation of 6T-SRAM-based PUF, at different environmental, electrical, and ageing conditions to representing the typical operating conditions of a WSN.**

I. INTRODUCTION

The integration of security mechanisms in wireless sensor nodes enables their use for applications with high security requirements such as medical devices and systems, assisted living, traffic control and safety, advanced automotive systems, environmental control, avionics, critical infrastructure control (electric power, water resources, and communications systems), defense systems, etc. Proposing security solutions for WSN is a basic step to make these applications feasible. Many activities focus on the design of efficient security protocols for WSN [1], [2], [3]. The main goals of these protocols are the low energy consumption, the reduction of transmitted packets and the scalability in various WSN topologies. This effort makes the integration of security systems in sensors feasible but cannot provide a fully secure solution. Invasive physical attacks [4] on the memory (non-volatile) where the key or other "secret data" are stored make any attempt for building protocol based security mechanisms useless. Making the sensor node secure itself and resistant to physical attacks is an important countermeasure. On the other hand, physical attacks protection remains a hard problem because this type of attacks is based on sophisticated reverse engineering methods (making use of sophisticated microscopes) which try to extract the key from a non-volatile memory. A strong candidate against this type of physical attacks is the Physical Unclonable Function (PUF) technology [5], [6]. PUF is based on an intrisic physical characteristic of an IC such as path delay and storage elements' initial states. These characteristics are introduced due to uncontrollable manufacturing process variations and can be used as a unique and unpredicable id for each IC. PUF based products achieve high security assurance as keys are volatile and derived only when required. This minimizes the time window during which a key is present in the IC [7]. Furthermore, an attacker will destroy with high probability the PUF during the physical attack making it very hard to obtain the key. Another advantage of using a PUF is that additional physical security is achievable without any special manufacturing steps.

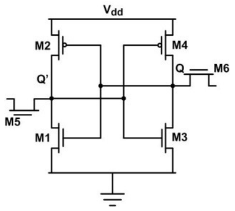

Figure 1: The SRAM 6T cell

The initial state of each SRAM bit cell is a function of process variation due to the manufacturing process. The stabilization of each bit depends on the threshold voltage mismatch between local devices. A 6T-SRAM cell, consisting of cross coupled inverters (M1, M2, M3, and M4) and access transistors (M5 and M6), is presented in Figure 1. The stable states of the indicated SRAM cell are Q'Q=01 and Q'Q=10. When the IC is unpowered both nodes, Q' and Q are low. On power up, depending on the mismatch of the transistors in the cross-coupled invertors, the cell stabilizes to Q'Q=10 or 01. An array of bit cells can be used to produce a unique cryptographic key for an IC.

Unfortunately, the initial state of an SRAM array (henceforth called PUF) cannot be used directly as a cryptographic key. Due to supply voltage fluctuation, temperature variations and other environmental condition changes, the output of the PUF is likely to be slightly different on different evaluations of the same IC. To get a unique ID for each IC, independent of operating conditions, we use a fuzzy extractor circuit [8] that processes the PUF output and performs error correction. Therefore the output of the fuzzy extractor can be used as a cryptographic key.

In this paper we evaluate the 90nm commercial 6T-SRAM of 17 ICs (each having 4 memory instances) for their capability as a PUF. In order to evaluate the properties of the SRAM as a PUF, we perform a number of specifically selected tests to investigate the behavior of the start-up values of the SRAM memory. Temperature variation tests, voltage variation tests, voltage ramp-up tests, data retention tests and ageing tests examine the reliability of the SRAM circuits as PUFs. The tests will be explained in detail in section III. Also, we prove the uniqueness of each SRAM PUF among all the devices. Each of the tested ICs, which are designed for low power medical applications [9], supports the Quiddikey^{TM} [10] module which provides the functionality of the fuzzy extractor and an AES (Advanced Encryption Standard) [11] cryptographic core for data security. The evaluation of Quiddikey^{TM} and AES core is out of the scope of the paper.

To the best of our knowledge, this is the first work that provides extensive testing and evaluation of a PUF circuitry emulating the real operating conditions (physical and enviromental) in which such circuitry are employed. Our results show that SRAM-based PUF combined with the fuzzy extractor can be used to generate unique cryptographic keys. The remainder of the paper is organized as follows: In Section II the related work is described. In Section III the testing process and results are presented in detail. Finally, conclusions can be found in Section IV.

II. Related Work

Pappu et al. [5], [6], introduced the concept of Physical Unclonable Functions (PUFs). The indicated technology is based on the response (scattering) obtained when shining a laser on a bubble-filled transparent epoxy wafer. Gassend et al. introduce Silicon Physical Random Functions [12] which use manufacturing process variations in ICs with identical masks to uniquely characterize each IC. The statistical delay variations of transistors and wires in the IC were used to create a parameterized self oscillating circuit to measure frequency which characterizes each IC. In [13] Tuyls et al. present a coating PUF in which an IC is covered with a protective matrix coating, doped with random dielectric particles at random locations. The IC also has a top metal layer with an array of sensors used to measure the local capacitance of the coating matrix. These capacitance values are used to characterize the IC. In [14], [15] authors introduce the idea of PUFs based on the start-up values of SRAM memory values. Su et al. [16] present a custom built circuit array of cross-coupled NOR gate latches to uniquely identify an IC. The circuit architecture is similar to 128b SRAM array.

III. Demonstration of PUF Reliability

For our experimental validation, we have used up to seventeen ICs each with four SRAM instances. When evaluating a memory, a measurement of the same memory instance at regular operating conditions (normal ambient temperature, V_{dd} as core voltage, etc.) is taken as the reference to which all other measurements of the same instance have been compared by calculating the fractional Hamming Distance (HD). The Fuzzy extractor used in the Quiddikey^{TM} module can correct up to 25% errors, which is equal to a fractional HD of 0.25. This means that as long as the errors caused by different operating conditions during a test remain below 25%, the fuzzy extractor will be able to derive the correct key from the SRAM PUF under these specific circumstances.

A. Temperature variation test

The purpose of the temperature variation test is to find out the consistency (or stability) of the start-up values of the memories under different temperature conditions. For this test, all seventeen ICs have been placed in a test set-up, which is suitable for varying the ambient temperature. These ICs have been powered up repeatedly and after each power up the contents of the SRAM memories have been read. For each memory instance, a measurement at an ambient temperature of 20^{o}C has been used as the reference, to which all other measurements have been compared by evaluating HDs. Based on this testing process for all the ICs we conclude that the fractional HDs during temperature tests are always below 19%. Since this 19% is well within the correctable bounds of the fuzzy extractor, the memories of the ICs pass the temperature test for all temperatures between -40^{o}C and +80^{o}C, i. e. the fuzzy extractor is capable of reconstructing unique key for this temperature range. Figure 2 shows the fractional HDs of different memory instances compared to their reference measurement at different temperatures. These temperatures are displayed at the top of the figure (Temp-40 ^{o}C stands for measurements performed at -40^{o}C). This figure contains the results for all memories of all measured ICs Measurements of different ICs are shown using different colors. At each temperature, the measurement was repeated multiple times (i.e. measurement number in x-axis) Note: the spike to 0 is the reference measurement (since HD to itself is 0).

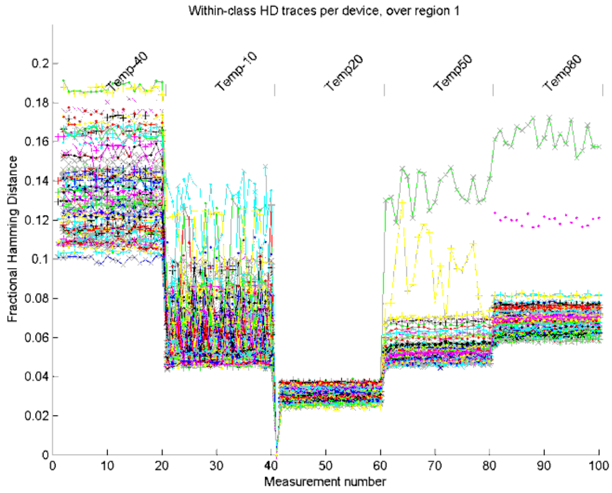

Figure 2: Frac. HDs vs. temperature (17 ICs with 4 memories per ICs)

B. Voltage variation test

The purpose of the voltage variation test is to find out the consistency of the start-up values of the memories under slight variations of the power supply voltage level. Four of the ICs have been placed in a test set-up, which is suitable for varying the core voltage of the IC. The ICs have been powered up and the contents of the memories have been read. We evaluate each SRAM instance for different core voltages (90% of V_{dd}, 95%, 100%, 105% and 110%). One measurement at 100% of V_{dd} (1.2V) per memory per IC has been used as reference, to which all other measurements of the same instance have been compared. The results from the voltage variation test are based on the fractional HDs between the measurements of the memory and the reference measurement. The outcome of the indicated experimental process is that the fractional HD is low (around 6%, see Figure 3) and approximately constant over all supply voltages. Therefore, supply voltage variation will not have a negative influence on the PUF properties of these SRAM memories.

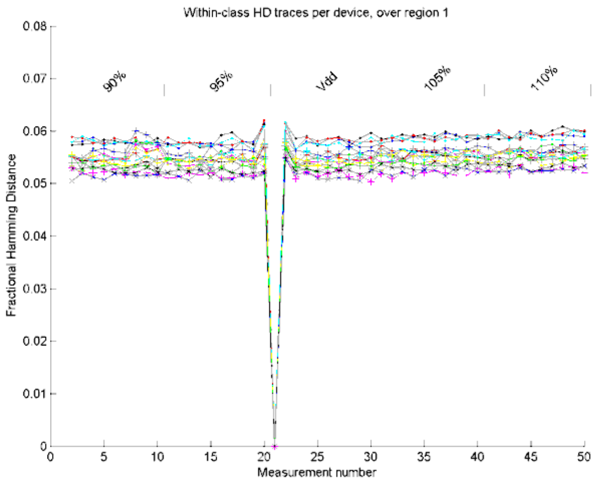

Figure 3: Frac. HDs vs. supply voltage (4 ICs with 4 memories per IC)

C. *Voltage rump-up test*

The purpose of the voltage ramp-up test is to determine the reliability of the initial state of the memories under different voltage ramp-up times. For the voltage ramp-up test, four ICs have been placed in a test set-up, which is suitable for varying ramp-up time (during start-up) of the IC core voltage. For each memory instance, a measurement with a ramp-up time of 50µs (steepest ramp possible in the test set-up) has been used as reference, to which all other measurements have been compared.

Figure 4 shows the fractional HDs of the tested memories (four devices, each with four memories) versus the ramp-up time. The fractional HDs increase when increasing the ramp-up time. From this figure a requirement for the maximum ramp-up time of the SRAM power supply can be derived. Given the fact that at 1ms the noise levels of the measurements remain below 10% and because 1ms is sufficient time for the power supply of these devices to rise, it is safe to conclude that the ramp-up time of the power supply will not cause a problem for these memories to operate as PUFs.

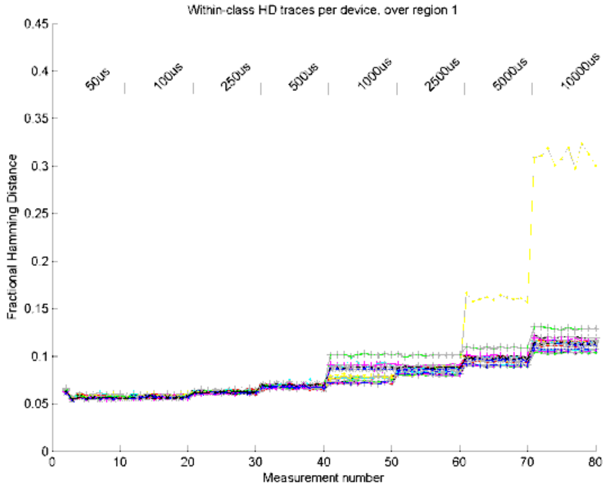

Figure 4: Frac. HDs vs. ramp-up times (4 ICs with 4 memories per IC)

D. *Data retention test*

In order to find out the susceptibility of power dips on the initial state of the SRAMs, the data retention test has been performed. This test determines at which supply voltage the SRAMs lose their data. In case a dip in the power voltage would occur (for instance during start-up) it is important to know above which threshold the supply should remain in order not to influence the (initial) state in the SRAM.

Four ICs have been placed in a test set-up, which is suitable for varying the core voltage of the IC. While powered at V_{dd} (1.2V) the memories have been filled with 0xFF (all 1s). The supply has been lowered to a certain percentage of V_{dd} for 1 second. Then the supply is set to V_{dd} again and the contents of the memories have been read out. For each supply value (from 100% to 10% in steps of 10%) this test has been performed 10 times. The outcome of the indicated experimental process is that as long as the supply voltage remains at least 30% of V_{dd}, no data in the memory is lost (pattern is still 0xFF). When the supply voltage becomes lower, bits start flipping. Assuming that a power dip doesnot reduce the supply below 30% VDD, SRAM can work properly as a PUF.

E. *Ageing test*

The main failure mechanism that causes the SRAM startup values to change over time is NBTI (Negative Bias Temperature Instability). This mechanism is accelerated in the ageing test by keeping the SRAM under high voltage and temperature conditions. The amount of acceleration achieved is estimated. The total acceleration factor [17] is the product of the thermal acceleration factor (TAF) and the voltage acceleration factor (VAF), which are computed as:

$TAF = e^{(E\alpha/k)*(1/Top-1/Tstress)}$, $VAF=e^{\gamma*(Vstress-Vop)}$

E_α (0.5 eV) is the activation energy, k ($8.62*10^{-5}$ eV/K) is Boltzmann`s constant, Top (313K (40°C)) is the normal operating temperature, T_{stress} (353K (80°C)) is the temperature used in the stress test,(2.6) is the voltage exponent factor, Vstress (1.32V) is the core voltage under stress conditions and Vop (1.2V) is the core voltage under normal operating conditions. This results in a total estimated acceleration factor of TAV*VAF = 8.17*1.37=11.2.

One IC has been placed in a test set-up under the above specified stress conditions to speed up the ageing process. Every three days the ambient temperature is lowered to +20°C and the SRAM start-up values are measured. After five repetitive measurements, the temperature is increased back to +80°C. One measurement at an ambient temperature of 20°C before starting the ageing test has been used as reference, to which all other measurements are compared.

The IC has been kept under the aforementioned stress conditions for a total of 156 days. With the estimated acceleration factor of 11.2, this simulates an effective ageing of around 4.7 years. The results show that within this time frame the ageing is quite limited. The fractional HD remains below 14% for all the memories on the IC.

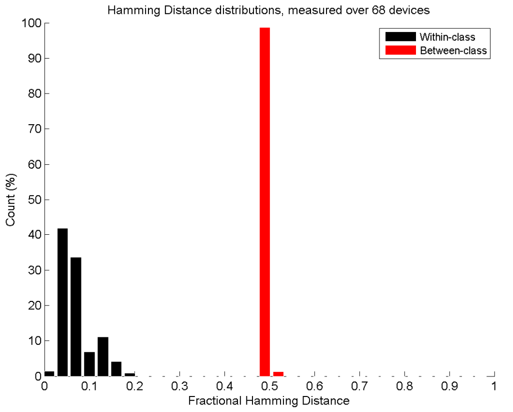

Figure 5: HD distributions of temperature test (all memories)

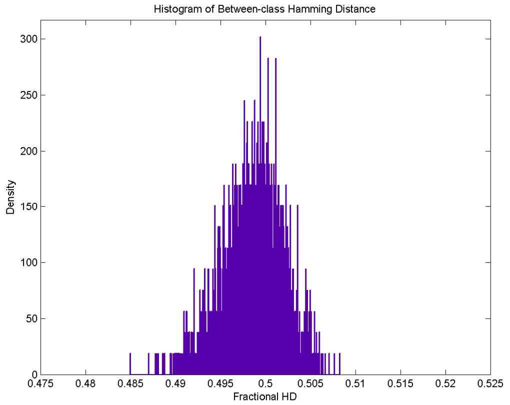

Figure 6: ***Between-class*** HD distribution of temperature test (all memories)

F. Between-class Hamming Distance

The tests A-E had the focus of evaluating the same memory instance under different operating conditions to show that the same secure key can be extracted for the same IC. But to satisfy a secure key requirement, a key must be also unique. This property can be evaluated by calculating the fractional HDs between SRAM start-up patterns of different devices. When two devices are unique and independent their "between-class" HD should be approximately 0.5. If all HDs between different devices are distributed around 0.5, there is no correlation between the start-up patterns of the devices, which makes them unpredictable and unique. The between-class HDs of all seventeen ICs have been calculated. Figure 5 shows the results when taking into account all four memories from these devices. The red bars represent the between-class distribution. For comparison, the within-class distribution (i.e., HD from two measurements of the same device) is plotted in black. Zooming in on the between-class distribution results in Figure 6. It can be concluded from these two figures that the between-class HDs are distributed around 0.5 and that they are much larger than the within-class HDs. Therefore, the results of the between-class evaluation prove that there is no correlation between the start-up patterns of different devices, which makes the each PUF response unpredictable and unique. More specifically uniqueness and unpredictability exists between memories on the same chip.

IV. CONCLUSIONS

In this paper 17 ICs, each having four commercial CMOS90 6T-SRAMs, have been evaluated on their capability as PUF. The experimental results prove that the initial state of the SRAMs are stable and consistent (are tolerant to noise) under different testing conditions, like varying ambient temperature and supply voltage level. Also, the derived start-up patterns from these memories are unique and unpredictable among other SRAM circuits. Based on the statistical analysis, we conclude that low power SRAMs are very useful for generating a cryptographic key (in other words, secure key storage without storing the key in non-volatile memory). Future work includes the evaluation of other types of SRAMs, other technologies, and the SRAMs together with Quiddikey^{TM} and security blocks.

REFERENCES

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “SPINS:Security Suite for Sensor networks”, Mobicom’01, 2001.

[2] A. Hodjat and I. Verbauwhede, “The energy cost of secrets in ad-hoc networks”, Proc. IEEE CAS Workshop on Wireless Communication and Networking, September 2002.

[3] An Liu, Peng Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," in Proceedings of IPSN 2008.

[4] A. Becher, Z. Benenson, and M. Dornseif, “Tampering with motes: Real-world physical attacks on wireless sensor networks”, in Proceedings of SPC 2006.

[5] R. S. Pappu. "Physical one-way functions". PhD thesis, Massachusetts Institute of Technology, March 2001. Available at http://pubs.media.mit.edu/pubs/papers/01.03.pappuphd.powf.pdf.

[6] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. "Physical oneway functions". Science, 297(6): pages 2026-2030, 2002. Available at http://web.media.mit.edu/ brecht/papers/02.PapEA.powf.pdf.

[7] P. Tuyls, G.-J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters. "Read-Proof Hardware from Protective Coatings". In CHES 2006, volume 4249 of LNCS, pages 369-383. Springer, October 10-13, 2006.

[8] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin and Adam Smith. "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data". In Eurocrypt 2004.

[9] B. Bousze, F. Bouwens, M. Konijnenburg et. al. "Ultra Low Power Programmable Biomedical SoC for on-body ECG and EEG Processing", accepted for publication in IEEE Asian Solid-State Circuits Conference 2010, Beijing, China.

[10] Quiddikey^{TM}, Intrinsic-ID: http://www.intrinsic-id.com/quiddikey/

[11] FIPS-197: Advanced Encryption Standard, November 2001, available athttp://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[12] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas. "Silicon physical unknown functions", ACM Conference on Computerand Communications Security, CCS 2002, pages 148-160.ACM, November 2002.

[13] P. Tuyls, G.-J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, and R. Wolters. "Read-Proof Hardware from Protective Coatings". In CHES 2006, volume 4249 of LNCS, pages 369-383. Springer, October 10-13, 2006.

[14] Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen and Pim Tuyls. "FPGA Intrinsic PUFs and Their Use for IP Protection". In Cryptographic Hardware and Embedded Systems - CHES 2007.

[15] Daniel E. Holcomb, Wayne P. Burleson, and Kevin Fu. "Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID Tags". In RFIDSec, 2007.

[16] Y. Su, J. Holleman, and B. Otis, “A 1.6pJ/bit 96% Stable Chip-ID Generating Cicuit using Process Variations”, in ISSCC 2007.

[17] "Altera Reliability Report 49 Q1 2010": www.altera.com/literature/rr/rr.pdf.