Comparative analysis of SRAM memories used as PUF primitives

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

***Abstract*—In this publication we present the results of our investigations into the reliability and uniqueness of Static Random Access Memories (SRAMs) in different technology nodes when used as a Physically Unclonable Function (PUF). The comparative analysis that can be found in this publication is the first ever of its kind, using different SRAM memories in technologies ranging from 180nm to 65nm. Each SRAM memory presents a unique and unpredictable start-up pattern when being powered up. In order to use an SRAM as a PUF in an application, the stability of its start-up patterns needs to be assured under a wide variety of conditions such as temperature and applied voltage. Furthermore the start-up patterns of different memories must be unique and contain sufficient entropy. This paper presents the results of tests that investigate these properties of different SRAM memory technology nodes. Furthermore, it proposes the construction of a fuzzy extractor, which can be used in combination with the tested memories for extracting secure cryptographic keys.**

I. Introduction

Due to deep-submicron manufacturing process variations every transistor in an Integrated Circuit (IC) has slightly different physical properties that lead to measurable differences in terms of its electronic properties like threshold voltage and gain factor. Since these process variations are uncontrollable during manufacturing, the physical properties of a device can neither be copied nor cloned. It is very hard, expensive and economically not viable to purposely create a device with a given electronic fingerprint. A Physically Unclonable Function (PUF) is an electronic circuit that measures the underlying fingerprint in the transistors that it is made of. Because of its dependency on the deep-submicron process variations, PUFs are very hard to reproduce by construction. However, in order to be able to use implementations of PUFs they should also be easy to challenge and their responses easy to measure.

A. Related Work

In 2001, Pappu [12] introduced the concept of PUFs as Physical One-Way Functions. The indicated technology was based on the response (scattering) obtained when shining a laser on a bubble-filled transparent epoxy wafer. Gassend et al. introduced Silicon Physical Random Functions [4] in 2002, which use manufacturing process variations in ICs 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 for characterisation. This circuit is nowadays known as a Ring Oscillator PUF. Another PUF based on delay measurements, the Arbiter PUF, was first described by Lee et al. in 2004 [9]. Besides hardware intrinsic PUFs based on delay measurements a second type, based on the measurement of start-up values of memory cells, is known. This type includes SRAM PUFs introduced by Guajardo et al. in 2007 [5], so-called Butterfly PUFs introduced in 2008 by Kumar et al. [8] and finally D flip-flop PUFs also introduced in 2008 by Maes et al. [11].

978-3-9810801-8-6/DATE12/©2012 EDAA

As stated, the focus of this paper is a comparative analysis of SRAM PUFs. Temperature variation measurements on embedded SRAMs were first presented in [5] (90nm FPGA devices). Publications from Holcomb et al. [6] use SRAM start-up measurements from ISSI SRAM, TI microcontrollers and Intel WISP devices (without mention of technology sizes).

B. Our Contribution

This publication contains the first ever comparative analysis of several types of SRAM memories from different technology nodes used as PUFs. The wide range of tested technologies varies from 180nm downto more recent 65nm nodes. SRAM instantiations from different vendors have been evaluated based on reliability and uniqueness of their PUF behavior. It is important to carry out such experiments, because SRAM memories are not designed for having good start-up (PUF) behavior. Furthermore, there are many SRAM design parameters that may influence the start-up behavior.

The results from this publication demonstrate that all of the tested SRAMs can be used as PUFs, independent of the chosen technology nodes or vendors. This is shown by designing a fuzzy extractor based on the worst-case measurement results, which can be used in combination with all tested memories.

C. Organisation of Manuscript

Section II gives an introduction of SRAM PUFs. This introduction contains the PUF construction, an overview of the PUF framework and specific PUF properties that are important when evaluating the behavior of SRAM PUFs. The tests that have been performed in order to evaluate these properties and their results are described in section III. These results lead to a fuzzy extractor construction that is suitable to create a PUF implementation with each of the tested SRAMs. Section IV describes the design of this worst-case fuzzy extractor. Finally, section V contains the conclusions of this publication.

II. PUF and Properties

A. SRAM PUF construction

The initial state of an SRAM cell is a function of process variation due to the manufacturing process. Each memory cell has a preference to start-up as either zero or one, due to random mismatch in the cross-coupled inverters (because of process variations) that make up an SRAM cell. It is unpredictable which cell has which preferred start-up state. The SRAM PUF patterns subject of our analyses, consist of start-up values from multiple bit cells.

B. PUF Framework

Physically Unclonable Functions are physical structures (consisting of many random components) that are easy to measure, but hard to characterize. An important application of PUFs is their use as a secure cryptographic key storage mechanism [13]. In this application one can distinguish two phases: Enrollment and Key Reconstruction.

Enrollment: In the enrollment phase the key is programmed into a device (comparable to the key programming phase for other secure key storage mechanisms in non-volatile memory). In order to do this, the PUF in the device is challenged and the measured response (called the reference PUF response) is the input to a so-called fuzzy extractor [2] [3]. The fuzzy extractor derives a cryptographic key from this reference PUF response and computes helper data. Later on, in the key reconstruction phase, the helper data enables the fuzzy extractor to reconstruct the exact same (“programmed”) cryptographic key from a PUF response. The helper data is stored in non-volatile memory attached to the device and is not sensitive (public information).

Key Reconstruction: In the key reconstruction phase the PUF is challenged and the measured response is fed into the fuzzy extractor. The fuzzy extractor reads out the helper data stored in non-volatile memory and derives the cryptographic key that was “programmed” during enrollment based on the helper data and the PUF response. If the measured PUF response is close enough to the reference PUF response, the original key will be successfully reconstructed.

Fuzzy Extractor: Two main functions of the fuzzy extractor to derive a cryptographic key from a PUF response are:

- Information reconciliation: Use the helper data to correct errors on the measured PUF response.
- Privacy amplification: Assuming that an attacker has partial information on the PUF response (because of information from helper data), compress the resulting bit string into a cryptographic key with maximum entropy.

C. PUF properties

To evaluate PUF behavior of SRAM PUFs, two properties are very important:

Reliability: Reliability means that for a given device, whenever the PUF responses are measured anew, one should be able to recognize the reference measurement that was originally taken during the so-called enrollment phase. When PUF responses are measured on the same device multiple times (either under varying or stable conditions) a number of errors (bit flips) will occur with respect to the reference measurement due to noise. The information reconciliation step in the fuzzy extractor algorithm allows to handle a certain amount of noise in those measurements, depending on the implemented error correction code. Smaller noise percentages in the PUF responses make it possible to use more efficient error correcting codes that require less redundant information [1].

Uniqueness: Uniqueness is the other important property, both within a single PUF response as well as between responses. To achieve this property, the following is required:

- All bits within a single PUF response should be random and unpredictable. In other words, bits in a single response do not supply information about each other and cannot be predicted.
- There is enough entropy in the source across devices. This means that statistically speaking, each device is unique, and the probability that two devices have a PUF response that is “close” to each other is negligibly small.

III. PUF tests and results

This section presents descriptions and results of the tests that have been performed for a comparative analysis of reliability and uniqueness of different SRAM memories used as PUFs. The results are quantitative and there is no technology/architecture analysis given in this paper. Reason is that the authors did not have access to SRAM architectures of all of the tested memories (SRAM vendors tend not to supply this information). Table I contains an overview of the studied SRAMs and the number of available devices. Naturally the higher this number of devices, the more accurate the statistical analyses of the corresponding memory will be.

TABLE I
Studied SRAM memories sorted by technology

Technology	SRAM	Nr of devices	Nr of bytes
65nm	Cypress CY7C15632KV18	10	2048
90nm	Virage HP ASAP SP ULP 32-bit	34[1]	2048
	Virage HP ASAP SP ULP 64-bit	34	2048
130nm	Faraday SHGD130-1760X8X1BM1	40	1750
	Virage asdsrsnfs1p1750x8cm16sw0	40	1750
150nm	Cypress CY7C1041CV33-20ZSX	8	2048
180nm	IDT 71V416S15PHI	8	2048

The reliability of these SRAM PUFs has been evaluated by tests in which either the ambient temperature or the level of the supply voltage has been varied. Temperature influences the characteristics of a transistor and its threshold voltage. Since differences in threshold voltage determine the preferred start-up state of an SRAM cell, temperature is a key influencing factor. The supply voltage affects the behavior of a transistor during the transition between conducting and non-conducting

[1] The 90nm device (designed specifically by IMEC Netherlands for these tests) contains four memories, two of each type. During the tests 17 of these devices have been evaluated, which results in 34 SRAMs of both types.

TABLE II
FRACTIONAL HDS OF DEVICES OVER DIFFERENT TEMPERATURES

SRAM	Technology	Devices	-40^oC			20^oC			$+80^oC$		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15632KV18	65nm	10	5.8%	7.8%	12.2%	3.3%	3.8%	4.3%	6.1%	6.6%	7.1%
Virage HP ASAP SP ULP 32-bit	90nm	34	11.5%	14.8%	19.6%	2.2%	2.9%	3.5%	5.0%	6.5%	8%
Virage HP ASAP SP ULP 64-bit	90nm	34	9.6%	11.8%	17.6%	2.6%	3.5%	4.0%	5.6%	7.7%	17.0%
Faraday SHGD130-1760X8X1BM1	130nm	40	8.4%	10.3%	13.7%	3.6%	4.5%	5.4%	6.7%	9.0%	13.0%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	9.3%	12.0%	19.6%	3.2%	4.8%	5.7%	7.0%	10.5%	20.5%
Cypress CY7C1041CV33-20ZSX	150nm	8	5.8%	6.7%	7.5%	2.9%	3.5%	3.9%	7.1%	8.0%	9.2%
IDT 71V416S15PHI	180nm	8	5.4%	6.0%	6.8%	2.3%	2.8%	3.3%	7.6%	8.4%	9.3%

modes. However, PUF start-up patterns establish themselves in SRAM cells in the first half of a voltage (power-up) ramp. Therefore it is not expected that the supply level, which is the end of the ramp, will have much impact on SRAM PUF reliability. To validate this assumption a test has been performed in which the supply voltage level has been varied.

In order to evaluate the uniqueness and entropy of the start-up patterns a Hamming Weight test, a between-class uniqueness test, a secrecy rate test and a compression test have been performed on the measured data.

A. Temperature test (reliability)

The purpose of the Temperature test is to find out the consistency (or stability) of the start-up values, and hence PUF behavior, of the memories under extreme temperature conditions. For this test all ICs have been placed in a test set-up, which is suitable for varying the ambient temperature. The ICs have been powered up repeatedly and after each power up the contents of the SRAM memories have been read. A measurement at an ambient temperature of $+20^oC$ has been used as reference, to which all other measurements have been compared by calculating fractional Hamming Distances[2] (HDs). Besides the enrollment temperature of $+20^oC$, the focus of the Temperature test is on the ambient temperatures of -40^oC and $+80^oC$ (industrial operating temperature range).

Table II contains an overview of the fractional HDs that have been measured during the Temperature test over all devices.[3] From these results it becomes clear that temperature has a big influence on the start-up patterns of SRAM memories. For each memory type the HDs are higher when the temperature is different from the enrollment temperature of $+20^oC$. The maximum HD that has been measured during the Temperature test is 20.5% (at $+80^oC$ on the 130nm Virage memory).

As an illustrative example, Fig. 1 shows the fractional HDs compared to the reference measurement, for the Temperature test measurements on all 34 Virage HP ASAP SP ULP 32-bit memories. The measured temperatures are displayed at the top of the figure (Temp-40 indicates measurements performed at an ambient temperature of -40^oC). Note: the dip to 0 is the reference measurement (since HD to itself is 0).

The results from the Temperature test prove that the fuzzy extractor has to be designed in a way that will make sure that the SRAM PUF is robust for variations in ambient temperature. This can be achieved by choosing an error correcting code, which can deal with the highest measured noise margins. When taking the 130nm Virage memory as an example, the maximum measured HD is 20.5%. Therefore, using this memory as a PUF at an ambient temperature between -40^oC and 80^oC, the error correcting code should be able to correct this amount of errors with very high probability. An example of such a fuzzy extractor can be found in section IV.

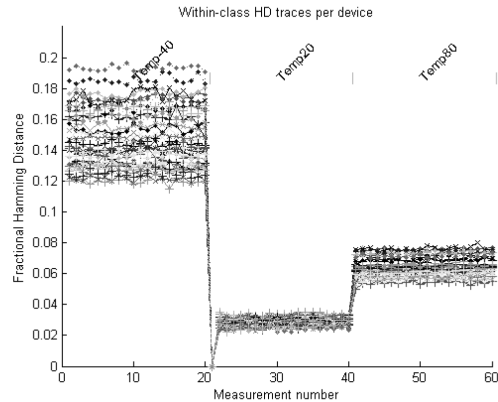

Fig. 1. Temperature test on Virage HP ASAP SP ULP 32-bit memory

B. Voltage variation test (reliability)

The purpose of the Voltage variation test is to verify the consistency of the start-up values of the memories under certain variations of the power supply voltage level. For this test 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 repeatedly to different voltage levels and the contents of the memories have been read. We evaluate each SRAM at different supply voltages (90% of nominal supply voltage Vdd, 100% and 110%). These voltages represent the normal operating range of the devices. One measurement per memory at Vdd has been used as reference, to which all other measurements of that memory have been compared by calculating fractional HDs to this reference measurement.

[2]Hamming Distance is defined as the number of bits that differ between two bit strings. In case of fractional HDs the number of differing bits is divided by the length of the compared bit strings.

[3]The authors would have preferred to represent the HD distributions as Gaussian (with μ and σ). However, the HD distributions were not suitable for this due to the limited number of devices. Therefore, the current representation has been used for all tables in this publication.

TABLE III
FRACTIONAL HDS OF DEVICES OVER DIFFERENT SUPPLY VOLTAGES

SRAM	Technology	Devices	90% of Vdd			Vdd			110% of Vdd		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15632KV18	65nm	10	3.3%	3.9%	4.4%	3.4%	3.8%	4.4%	3.4%	3.8%	4.5%
Virage HP ASAP SP ULP 32-bit	90nm	8	5.0%	5.5%	6.0%	4.9%	5.5%	6.2%	5.1%	5.5%	6.1%
Virage HP ASAP SP ULP 64-bit	90nm	8	4.9%	5.5%	6.2%	4.9%	5.5%	6.3%	4.9%	5.6%	6.2%
Faraday SHGD130-1760X8X1BM1	130nm	10	4.0%	4.6%	5.2%	4.0%	4.6%	5.4%	3.9%	4.7%	5.4%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	10	4.0%	5.4%	6.3%	3.7%	5.5%	6.2%	3.9%	5.5%	6.4%
Cypress CY7C1041CV33-20ZSX	150nm	8	3.2%	3.5%	3.8%	3.1%	3.5%	3.9%	3.1%	3.5%	3.8%
IDT 71V416S15PHI	180nm	8	1.6%	1.8%	2.0%	1.5%	1.7%	1.9%	1.7%	1.9%	2.2%

TABLE IV
FRACTIONAL HWS OF DEVICES OVER DIFFERENT TEMPERATURES

SRAM	Technology	Devices	-40^oC			20^oC			$+80^oC$		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15634KV18	65nm	10	48.6%	49.6%	50.8%	48.6%	49.7%	50.7%	48.6%	49.9%	51.1%
Virage HP ASAP SP ULP 32-bit	90nm	34	48.7%	49.8%	51.1%	47.0%	49.3%	51.3%	46.8%	49.2%	51.1%
Virage HP ASAP SP ULP 64-bit	90nm	34	48.5%	49.6%	50.6%	48.0%	49.2%	50.6%	47.5%	48.9%	50.9%
Faraday SHGD130-1760X8X1BM1	130nm	40	49.2%	51.3%	54.0%	50.1%	53.5%	58.9%	49.9%	55.9%	65.2%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	48.7%	50.0%	51.1%	49.1%	50.1%	51.1%	48.9%	50.0%	51.2%
Cypress CY7C1041CV33-20ZSX	150nm	8	48.1%	50.0%	51.0%	49.1%	50.1%	51.1%	49.3%	50.1%	51.1%
IDT 71V416S15PHI	180nm	8	40.4%	42.1%	43.4%	40.5%	42.1%	43.5%	40.4%	41.9%	43.6%

The test results from the Voltage variation test (and number of tested devices) can be found in Table III. As can be seen in this table, the outcome of this test is that the fractional HDs are always low and approximately constant over the measured supply voltages. Therefore, we conclude that supply voltage variation does not influence the reliability of these SRAM memories when used as PUFs.

C. Hamming Weight test (uniqueness)

Using the Hamming Weight[4] (HW) test on a set of PUF responses can be helpful to detect whether these strings are biased towards zero or one. This can simply be done by calculating the fractional HW of the start-up patterns, which should be around 0.5 for unbiased strings. In case the HW is significantly higher than 0.5, the string contains too many ones. A significantly lower HW indicates too many zeros. Biasing has a negative impact on the uniqueness of PUFs. When start-up patterns of PUFs are biased, the resemblance between different devices will increase. Therefore, the fuzzy extractor will require more input bits in order to derive a unique key from the SRAM suitable for cryptographic purposes. This phenomenom has been described, for memory based PUFs, in more detail in [10].

Table IV contains the results from the Hamming Weight test over different temperatures. Most of the SRAM memories studied during the test do not show significant biasing at the tested temperatures. Both average HWs as well as the minimum and maximum values of HW are close to 0.5. However, the 130nm Faraday memory clearly has more ones than zeros in its start-up patterns (especially at +20°C and +80°C). Furthermore, the IDT (180nm) memory is clearly biased towards zero at all temperatures. As stated earlier, biasing has a negative impact on the uniqueness of the SRAM PUFs. When the start-up patterns are biased the randomness between different SRAMs decreases and hence more bits will be required for the fuzzy extractor to derive unique keys from each individual SRAM (privacy amplification).

[4]Hamming Weight is defined as the number of of bits with the value one in a bit string. In case of fractional HWs this number of bits is divided by the length of the bit string.

D. Between-class uniqueness test (uniqueness)

Another way to evaluate the uniqueness property of SRAM PUFs is by calculating the fractional HDs between start-up patterns of different devices. When two devices are unique and independent their "between-class" (fractional) Hamming Distance (BCHD) should be approximately 0.5. If the HDs between different devices are distributed around 0.5, this is an indication that correlation between the start-up patterns of the devices is low, which makes them unpredictable and unique. To test the uniqueness of the SRAM start-up patterns one measurement of each SRAM has been performed at an ambient temperature of +20°C and a supply voltage of Vdd. The between-class HD distribution is calculated by comparing the different patterns and calculating their HD. Using n different memories results in $n*(n-1)/2$ between-class comparisons. These HDs together form a distribution, which can be fitted to a Gaussian function with mean μ and standard deviation σ. Based on these statistical values the correlation between SRAM memories from different devices can be evaluated. For an indication of low correlation (and hence unique patterns), μ should be close to 0.5 and σ should be small.

The results from fitting the BCHD distributions can be found in Table V and an example for the Virage HP ASAP SP ULP 32-bit memory fit is depicted in Fig. 2. Evaluating the results, it becomes clear that the memories from the 130nm device have most correlation between different devices. This conclusion is based on the fact that these memories have the lowest values for μ as well as the highest σ.

As stated earlier, the fit of the distributions that are created

TABLE V
RESULTS OF FIT ON BETWEEN-CLASS DISTRIBUTION OF DIFFERENT DEVICES

SRAM	Technology	Devices	Number of BCHD values	μ	σ
Cypress CY7C15634KV18	65nm	10	(10*9)/2 = 45	0.500	0.0033
Virage HP ASAP SP ULP 32-bit	90nm	34	(34*31)/2 = 496	0.497	0.0046
Virage HP ASAP SP ULP 64-bit	90nm	34	(34*31)/2 = 496	0.496	0.0043
Faraday SHGD130-1760X8X1BM1	130nm	40	(40*39)/2 = 780	0.467	0.014
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	(40*39)/2 = 780	0.451	0.023
Cypress CY7C1041CV33-20ZSX	150nm	8	(8*7)/2 = 28	0.499	0.0034
IDT 71V416S15PHI	180nm	8	(8*7)/2 = 28	0.486	0.0041

TABLE VI
CTW COMPRESSION AND MUTUAL INFORMATION RESULTS

SRAM	Technology	Devices	Compressed size (bits)	Original size (bits)	Compression ratio	Minimum I(R,R')	Average I(R,R')	Maximum I(R,R')
Cypress CY7C15632KV18	65nm	10	16392	16384	100.0 %	0.62	0.64	0.65
Virage HP ASAP SP ULP 32-bit	90nm	34	16385	16384	100.0 %	0.38	0.59	0.69
Virage HP ASAP SP ULP 64-bit	90nm	34	16389	16384	100.0 %	0.49	0.63	0.73
Faraday SHGD130-1760X8X1BM1	130nm	40	13896	14000	99.3%	0.52	0.61	0.69
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	13903	14000	99.3%	0.47	0.57	0.67
Cypress CY7C1041CV33-20ZSX	150nm	8	16392	16384	100.0 %	0.60	0.70	0.76
IDT 71V416S15PHI	180nm	8	16091	16384	98.2%	0.57	0.70	0.79

using a small number of devices will be less accurate than those with more devices. However, the results of each fit do give a reasonable idea of which memories have more entropy than others. In this case both Cypress memories as well as the 90nm Virage memories achieve high scores in this test.

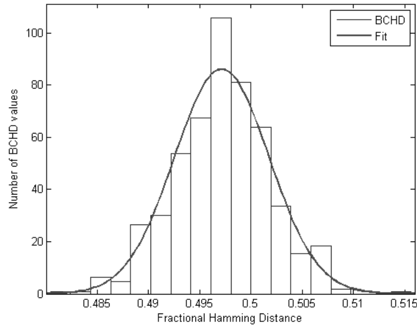

Fig. 2. Distribution of BCHDs from Virage HP ASAP SP ULP 32-bit, including Gaussian fit of the distribution

E. Secrecy rate & compression test (uniqueness & reliability)

The minimal amount of compression required in the privacy amplification step of the fuzzy extractor is expressed in the secrecy rate S_R as $1/S_R$ [7]. The maximum achievable secrecy rate is given by the mutual information $I(R, R')$ between strings derived during enrollment (R) and reconstruction (R'). In order to estimate this mutual information, we use the Context-Tree Weighting (CTW) algorithm from [14]. The enrollment string R is composed by concatenating enrollment strings of all memory devices of a certain type. Different reconstruction strings R' are formed by concatenating strings of all devices measured under a specific temperature or voltage condition. First the entropy $H(R)$ is estimated by compressing R with CTW. Then the conditional entropy $H(R|R')$ is estimated by compressing bits from R with bits from R' as CTW context. Different contexts and context lengths are tried to find an optimal compression result. The mutual information is then computed as $I(R, R') = H(R) - H(R|R')$ for bit strings R from all temperatures (-40°C,+20°C,+80°C) and voltages (Vdd+/-10%). Fractional mutual information values $I(R, R')$ are computed by dividing by the length of the input bit strings R. Note that the computed $I(R, R')$ is an indicator of both reliability and uniqueness. Noise and non-randomness in start-up patterns will both decrease $I(R, R')$.

By compressing sequences of SRAM start-up patterns directly with the CTW algorithm, we can get another indication of their uniqueness. The resulting compression length can be seen as an indicator for the entropy of a start-up pattern. The procedure is as follows. From each SRAM a start-up measurement taken at room temperature and nominal supply voltage (Vdd) is compressed with CTW. The resulting compression length is divided by the length of the measurement data. This ratio is defined as the compression ratio. A compression ratio close to 100% indicates that the bit string cannot be compressed and hence that there is no indication that the bit string does not have full entropy. Compression rates below 100% indicate that there is non-randomness, so less uniqueness in the SRAM start-up patterns.

Table VI shows the results of this test. They indicate that the SRAMs from the technology nodes 65nm, 90nm and 150nm have the most randomness. Their patterns cannot be compressed. The patterns of the 130nm and 180nm SRAMs can be compressed and hence do not have full entropy, which is probably related to the biasing as shown in section III-C.

The Table also shows that the average mutual information $I(R, R')$, measured over different SRAM devices, voltages and temperatures, lies between 0.57 and 0.70. Since the $I(R, R')$ is an upper bound for the secrecy rate S_R, the minimum $I(R, R')$ is the strictest measure for the secrecy rate. The lowest value for the minimum $I(R, R')$ is found in the Virage

HP ASAP SP ULP 32-bit devices. The fuzzy extractor should in this worst case take at least $N/S_R = N/0.38 = 2.6 \cdot N$ source bits to derive an N bit key according to the theory of [7]. The best performing memory type in this test is the 65nm Cypress memory. Since the minimum $I(R, R')$ value for this memory is 0.62, the fuzzy extractor requires at least only $N/S_R = N/0.62 = 1.6 \cdot N$ source bits to derive an N bit key.

IV. Fuzzy Extractor Construction

The fuzzy extractor has to be designed to deal with SRAM start-up pattern variations due to variations in ambient temperature. At the same time the fuzzy extractor must take into account the entropy that is present in the PUF patterns. In this section we give an example of a fuzzy extractor that takes both aspects into account and is based on worst-case results from all previous analyses. Although this approach will not lead to the most efficient implementation for specific SRAMs, it shows that for each type of memory a solution can be constructed.

For creating a fuzzy extractor construction, we investigate the possibility of deriving a 128 bit cryptographic key with a failure rate $< 10^{-9}$. Hence, the probability that errors in the SRAM start-up pattern can not be corrected is smaller than 10^{-9}, which is acceptable for commercial products.

Based on our reliability results, we conclude that the worst-case noise for the fuzzy extractor is 21%, slightly above the measured maximum HD in the Temperature test (+80°C for 130nm Virage memory). In terms of uniqueness, the worst-case estimation is given by the secrecy rate test of the Virage HP ASAP SP ULP 32-bit memory, with a value of $S_R = 0.38$.

According to the theory presented in [7] we need to reconstruct at least $128/S_R = 337$ secret bits. In the privacy amplification phase these bits can be compressed into a device unique key with a length of 128 bits with full entropy.

Using concatenated error correcting code constructions with BCH codes and repetition codes as shown in [1] gives efficient results in terms of minimum SRAM size. A search for the most efficient BCH and repetition code combination for our situation gives the following result: a repetition-11 code with parameters $[n_1, k_1, d_1]$=[11,1,11] applied 765 times in combination with a BCH code with parameters $[n_2, k_2, d_2]$=[255,115,43] applied 3 times. This solution uses 1.03kB of SRAM (e.g. the first 1.03kB of a bigger SRAM memory) and provides 345 secret bits, enough for compressing into a 128 bit key under worst-case entropy assumptions.

The described fuzzy extractor deals with worst-case entropy and noise assumptions from the presented test results. For specific SRAMs, more efficient error correcting codes can be used that will require far less than 1kB of memory.

V. Conclusions and Future Work

We conclude that all of the tested SRAM memories are suitable for use as a PUF in combination with a fuzzy extractor implementation. Even though test results vary slightly between different memories, for all memory types a suitable fuzzy extractor can be implemented. This has been proven in section IV by designing a fuzzy extractor for the worst-case situation, as derived from the measurement results. The fuzzy extractor uses an efficient error correcting code, which corrects noise levels up to 21% with failure probabilities below 10^{-9}. The lower uniqueness of some memory types (with resulting lower secrecy rate) has been compensated by using more secret bits to derive a cryptographic key of 128 bits. The authors' future work consists of several topics:

- Test smaller technology nodes and larger sets of devices.
- More reliability tests will be performed. Examples: study influence of varying speed at which supply voltage rises during start-up, investigate effects of combining variations in supply with different ambient temperatures, etc.
- SRAM modelling and technology analysis should provide insights into which design parameters influence PUF performance. At this moment all results are empirical. It will be worthwhile to translate these results into a model for SRAM technologies and/or architectures.

Acknowledgements

The authors would like to thank IMEC Netherlands for designing the 90nm device of which the SRAMs have been tested for this paper. Work performed in this study, has been supported by the European Union's FP7-project UNIQUE.

References

[1] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, P. Tuyls, *Efficient Helper Data Key Extractor on FPGAs.* In the proceedings of CHES 2008, LNCS volume 5154, pp. 181–197, Springer-Verlag, 2008.

[2] X. Boyen, *Reusable Cryptographic Fuzzy Extractors*, Proceedings of 11th ACM Conference CCS 2004, pp. 82–91, 2004.

[3] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data*, SIAM J. Comput. vol. 38(1), pp. 97–139, 2008.

[4] B. Gassend, D. E. Clarke, M. van Dijk, and S. Devadas, *Silicon Physical Random Functions*, ACM CCS 2002, pp. 148–160, ACM, 2002.

[5] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, *FPGA Intrinsic PUFs and Their Use for IP Protection*, In proceeding of CHES 2007, LNCS volume 4727, pp. 63–80, Springer-Verlag, 2007.

[6] D.E. Holcomb, W.P. Burleson, K. Fu, *Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers*, IEEE Transactions on Computers, 2009.

[7] T. Ignatenko, G.J. Schrijen, B. Skoric, P. Tuyls and F. Willems, *Estimating the Secrecy-Rate of Physical Unclonable Functions with the Context-Tree Weighting Method*, In IEEE International Symposium on Information Theory, pp. 499-503, Seattle, USA, July 2006.

[8] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, *The Butterfly PUF: Protecting IP on every FPGA*, IEEE International Workshop HOST 2008, pp. 67–70, IEEE Computer Society, 2008.

[9] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, *A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications*, in Proceedings of the IEEE VLSI Circuits Symposium, pp. 176–179, 2004.

[10] V. van der Leest, G.J. Schrijen, H. Handschuh and P. Tuyls, *Hardware Intrinsic Security from D flip-flops*, Proceedings of the fifth ACM workshop STC2010, pp.53-62, 2010.

[11] R. Maes, P. Tuyls, and I. Verbauwhede, *Intrinsic PUFs from Flip-flops on Reconfigurable Devices*, In Workshop WISSec 2008, 17 pages, 2008.

[12] R. S. Pappu, *Physical one-way functions*, PhD. Thesis, Massachusetts Institute of Technology, March 2001.

[13] P. Tuyls, B. Skoric, T. Kevenaar. *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer-Verlag, 2007.

[14] F.M.J. Willems, Y.M. Shtarkov and Tj.J. Tjalkens, *The Context-Tree Weighting method: Basic Properties*, In IEEE Transactions on Information Theory, Vol.IT-41, pp. 653-664, May 1995.