Modeling SRAM Start-Up Behavior for Physical Unclonable Functions

Mafalda Cortez Apurva Dargar Said Hamdioui

Delft University of Technology
Faculty of EE, Mathematics and CS
Mekelweg 4, 2628 CD Delft, The Netherlands
{A.M.M.O.Cortez, S.Hamdioui}@tudelft.nl

Geert-Jan Schrijen

Intrinsic-ID B.V.
High Tech Campus 9,
Eindhoven, The Netherlands
Geert.Jan.Schrijen@intrinsic-id.com

***Abstract*—One of the emerging technologies for cryptographic key storage is hardware intrinsic security based on *Physical Unclonable Functions* (PUFs); a PUF is a physical structure of a device that is hard to clone due to its inherent, device-unique and deep-submicron process variations. SRAM PUF is an example of such technology that is becoming popular. So far, only a little is published about modeling and analysis of their *start-up values* (SUVs). Reproducing the same start-up behavior every time the chip is powered-on is crucial to produce the same cryptographic key. This paper presents an analytical model for SUVs of an SRAM PUF based on *Static Noise Margin* (SNM), and reports some industrial measurements to validate the model. Simulation of the impact of different sensitivity parameters (such as variation in power supply, temperature, transistor geometry) has been performed. The results show that out of all sensitivity parameters, variation in threshold voltage is the one with the highest impact. Industrial measurements on real memory devices validate the simulation results.**

I. Introduction

The industry is recognizing the importance of hardware security to combat semiconductor device counterfeiting, theft of service and tampering, for which secure cryptographic key storage is an essential component. Traditional methods use *Non-Volatile Memories* (NVMs) to permanently store key/data, which are highly prone to physical attacks [1–3]; hence, the methods are no longer secure. Ideally, the cryptographic key would *not* be permanently stored in the system but generated *only* when required. One of the emerging technologies satisfying this requirement is hardware intrinsic security based on PUFs. A PUF is an inherent function that is embedded in a physical structure, such as an *Integrated Circuit* (IC). A PUF is hard to clone due to its inherent, device-unique and deep-submicron *process variations* (PVs). When challenged, a PUF generates a response based on the unique *fingerprint* inherent in an IC. There are several types of PUFs such as Optical PUF [4], Coating PUF [5], Silicon PUF [6], Flip-Flop PUF [7], Butterfly PUF [8] and SRAM PUF [9]. Because SRAM PUFs are standard components and easy to manufacture, no extra effort is invested for their implementation. Therefore, SRAM PUFs are one of the most popular PUF types today [6,10,11].

Although SRAM cells are symmetrical, small and random deviations during manufacturing process cause an intrinsic mismatch. SRAM PUF fingerprints are a consequence of the mismatch in SRAM cells. When powered-up, due to this mismatch, the cells take their preferred values - either a logic 0 or logic 1. Each SRAM cell provides one fingerprint bit. The SRAM cells *start-up values* (SUVs) together generate a fingerprint that uniquely identifies each device. This fingerprint is further processed to generate a unique cryptographic key. To be used as a source for key generation, the fingerprint needs to be reproducible over time, even under changing environmental conditions. Thus, it is crucial to understand the different parameters impact on the fingerprints robustness to design reliable SRAM PUF based systems.

Even though SRAM PUFs are becoming popular, very limited work has been published about modeling the robustness of its SUVs, not to mention actual silicon verification. In [10], the authors used soft decision information in helper data algorithms to correct the SUVs of non-robust cells. In [12] and [13], the authors proposed the use of SRAM for *Field Programmable Gate Array* (FPGA) Intellectual Property protection and studied SRAM PUF fingerprint statistical characteristics, such as entropy. However, their work was not directed towards the physical randomness source that causes fingerprints. In [14], the authors presented a technique called stable-PUF-marking to identify robust SRAM cells; only these cells are used for cryptographic key generation as an alternative for error correction. However, the authors assumed that the cells mismatch is based on the threshold voltage alone. In [15], the authors studied the impact of non-technology parameters (e.g., temperature) on the robustness of SRAM fingerprints. However, the work did not consider the impact of technology parameters such as transistor channel length. Understanding the impact of both technology and non-technology parameters on the SUVs enables the design of robust and reliable SRAM PUFs based systems. An appropriate model is therefore needed.

This paper presents an analytical model of start-up behavior of an SRAM. The model is further used to perform a sensitivity analysis to identify the impact of different technology and non-technology parameters. Validation of the model is done by comparing simulation results with silicon measurements.

The rest of this paper is organized as follows. Section II briefly reviews key storage based on PUFs, the *six transistors* (6Ts) SRAM cell and classifies it according to its ability to reproduce the same start-up behavior. Section III introduces the analytical model based on SNM. Section IV gives the simulation results. Section V reports silicon measurements and compares them with the obtained simulation results. Finally, Section VI concludes this paper.

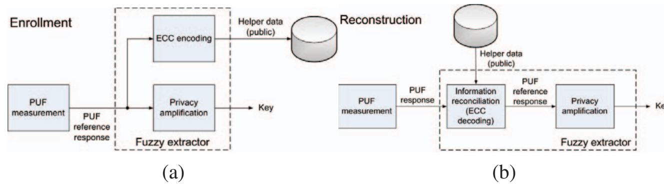
978-1-4673-3042-8 © 2012 IEEE

II. Background on Secure Cryptographic Key Storage based on SRAM PUFs

This section provides background information of PUFs based systems and briefly gives an SRAM cell architecture and behavior overview. In addition, it proposes a classification of SRAM cells upon the reproducibility of their SUVs.

A. Key Storage System based on PUFs

PUFs in general, SRAM PUFs in particular, can be used as a secure cryptographic key storage mechanism [16]. Fig. 1 shows how such mechanism can be integrated to create a PUF based key storage system. Such a system performs two main operations; they are explained next.



(a) (b)

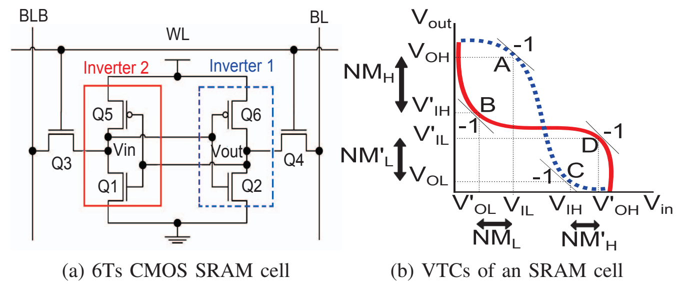
Fig. 1: Operations of a PUF based Key Storage System (a) Enrollment and (b) Reconstruction [17].

1) **Enrollment:** this operation generates a key based on a PUF fingerprint. This key is *programmed* into the device to be protected. This operation can be subdivided in three steps. First, the response of the targeted PUF is measured. This response is called *PUF reference response*. Second, this response is used as the input of the *Fuzzy Extractor* (FE) [18–20], which derives a cryptographic key and computes *Helper data* using ECC coding. Third, the Helper data is stored in a NVM attached to the device and is made as public information.
2) **Reconstruction:** this operation recovers the programmed key. It can be divided in two steps. First, the response of the targeted PUF is measured. This response is called *PUF response*; see Fig. 1(b). Second, this response is used as input of the FE; here, FE uses the stored Helper data and the new response to reconstruct the cryptographic key that was programmed during enrollment. If the measured PUF response is close enough to the PUF reference response (i.e., within the ECC correction capability, typically 25% [17]), the original key is successfully reconstructed.

It is then *crucial* to reproduce the same PUF reference response generated at enrollment during the key reconstruction phase within the error correction capabilities of the ECC.

B. SRAM cell and classification

The popular 6Ts SRAM cell (see Fig. 2(a)) consists of two cross-coupled CMOS inverters formed by four transistors (Q1 with Q5 and Q2 with Q6) and two pass transistors (Q3 and Q4). The pass transistors are used to access the cell for read and write operations. The bitline (BL), the compliment bitline (BLB) and the wordline (WL) are used to access the cell.



(a) 6Ts CMOS SRAM cell (b) VTCs of an SRAM cell

Fig. 2: SRAM cell (a) schematic and (b) VTCs

To be used for cryptographic key generation, it is required that the SUVs of the majority of the SRAM cells are reproducible, even under hostile conditions such as high temperature [15]. Therefore, SRAM cells are classified depending upon the sensitivity of its SUVs to stress conditions as follows:

1) **Non-skewed cell:** the cell has *no* measurable mismatch between its two inverters. This does not mean that PV did not occur in the cell, but just that the combined effects neutralize each other. A non-skewed cell generates randomly either a 0 or 1 at its output, depending mainly upon the noise present in the system.
2) **Partially-skewed cell:** the cell has a *little* mismatch between its two inverters. These kind of cells have a preferred state, depending upon the nature of the mismatch. Therefore, the cell can flip (hence, produce a different SUV) due to variation of external conditions such as the temperature.
3) **Fully-skewed cell:** the cell has a *high* mismatch between its two inverters in such a way that the cell always takes its preferred initial state regardless of the stress conditions. Ideally, SRAM PUFs have majority cells of this type.

III. Analytical Model for SRAM PUFs

In this section the concept of Static Noise Margin (SNM) is used to develop an analytical model for SRAM SUVs. First, the SNM is briefly reviewed. Then, a model is presented. Finally, a classification of parameters that could impact SRAM PUF SUVs is given.

A. SNM concept

SNM is the metric for quantifying the maximum noise voltage that an SRAM cell can tolerate before changing its state. SNM is calculated as the shortest side of the largest square that can fit inside the eyes of the *Voltage Transfer Curves* (VTCs) of the cross-coupled inverters that compose the cell; see Fig. 2(b). The dashed curve presents the VTC of Inverter 1 and the solid that of Inverter 2. The intersection of these lines forms two eyes. The side of the largest square that can fit inside *both* eyes is the SNM value [21]. To find the SNM value, the coordinates of four critical points A, B, C and D as shown in Fig. 2(b) have to be determined.

The traditional SNM model proposed by [21] takes all 6Ts into account as all of them affect the SRAM cell stability. The calculation is made for read-access mode as it is the worst case scenario. It is known that cell asymmetries are due

to PV affecting the size of the VTCs eyes [15,22]. Hence, by determining the relative size of the eyes, it is possible to determine the cell's preferred state. Perfectly symmetrical eyes indicate a non-skewed cell, small asymmetry between the eyes indicate a partially-skewed cell and a large asymmetry indicates a fully-skewed cell [23].

The traditional SNM model cannot be directly used to analyze the SUVs of SRAM cells because: (a) SUVs are generated during power-up and not during read-access mode, (b) the transistors that play a major role in determining the SUVs of SRAM cells are the ones forming the cross-coupled inverters, (c) pass transistors of SRAM PUF have no impact since the WL is not active and (d) SUVs are not only determined by the noise tolerance of the cell but also by the relative strength of SRAM cells inverters. Hence, a new *PUF SNM* (PSNM) is needed.

B. SRAM PUF Static Noise Margin (PSNM)

To determine the value of PSNM, we assume that only the noise and the mismatch of the cross-coupled inverters may impact the SUVs. As shown in Fig. 2(b), the PSNM square size depends on the coordinates of the four critical points denoted by A (V_{IL}, V_{OH}), B (V'_{OL}, V'_{IH}), C (V_{IH}, V_{OL}) and D (V'_{OH}, V'_{IL}). For each of the four points, the transistors involved are either in linear or saturation mode, assuming noise levels above the threshold voltage [24]. At point A, Q_2 is in saturation mode and Q_6 is in linear mode; at point B, Q_1 is in linear mode and Q_5 is saturation mode; at point C, Q_2 is in linear mode and Q_6 is in saturation mode, while at point D, Q_1 is in saturation mode and Q_5 is in linear mode. To calculate the coordinates of each of the critical points we performed the following steps. Due to space limitations we present the procedure and results only for point A; a similar approach is performed on points B, C and D [23].

1) Write the drain current equations for the transistors in their respective modes of operation. For point A, $I_{D_{Q2}} = I_{D_{Q6}}$. This results into:

$$\beta_2 \quad (V_{in} - V_{th_2})^2(1 + \lambda_2 V_{out}) = \beta_6[2(V_{in} - V_{dd} - V_{th_6})(V_{out} - V_{dd}) - (V_{out} - V_{dd})^2] \qquad (1)$$

where $\beta_{2,6}$ are the transconductances, $\lambda_{2,6}$ are the channel length modulation parameters, $V_{th_{2,6}}$ are the threshold voltages of $Q2$ and $Q6$ respectively, V_{out} and V_{in} are respectively the output and input voltage of Inverter 1 (see Fig. 2(a)), and V_{dd} is the supply voltage.

2) Differentiate the equations obtained in step 1 with respect to V_{in} and then replace the derivative with $\frac{dV_{out}}{dV_{in}} = -1$.

3) Utilize the equations in steps 1 and 2 to derive an expression for the coordinates of the critical point A; this results into:

$$V_{OH} = \frac{\frac{\beta_2}{\beta_6}(V_{IL} - V_{th_2}) - \frac{1}{2}\frac{\beta_2}{\beta_6}\lambda_2(V_{IL} - V_{th_2})^2}{2 - \frac{\beta_2}{\beta_6}\lambda_2(V_{IL} - V_{th_2})} + \frac{+V_{IL} - V_{th_6} + V_{dd}}{2 - \frac{\beta_2}{\beta_6}\lambda_2(V_{IL} - V_{th_2})} \qquad (2)$$

V_{IL} is obtained by substituting V_{out} of Eq. 1 into Eq. 2.

4) Calculate the smallest of the noise margins (NM) per VTC of as:
   - NM = min ($NM_H = V_{OH} - V'_{IH}$, $NM_L = V_{IL} - V'_{OL}$)
   - NM'= min ($NM'_H = V'_{OH} - V_{IH}$, $NM'_L = V'_{IL} - V_{OL}$).

5) Determine two metrics:
   a) $PSNM_{ratio}$ as NM/NM'. The preferred value of the SRAM cell is 1 if $PSNM_{ratio}$ is greater than 1 and 0 if $PSNM_{ratio}$ is smaller than 1. The higher or lower the $PSNM_{ratio}$ than 1, the higher the asymmetry within its cross-coupled inverters; hence, the more reproducible its SUVs.
   b) $PSNM_{noise}$ = min(NM, NM'). The higher the $PSNM_{noise}$ the higher the tolerance of the cell to the noise.

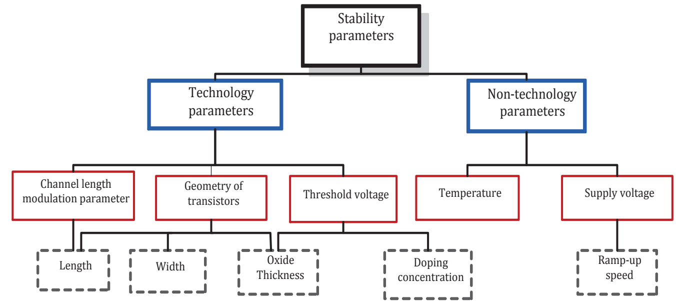


Fig. 3: Classification of sensitivity parameters for SRAM PUFs

C. Classification of SRAM PUF stability parameters

Inspecting Eq. 1 and Eq. 2, used to calculate both PSNM metrics, reveal that the following parameters can impact the SUV:

- Channel length modulation λ; this parameter strongly depends on the transistor length L [25];
- MOSFET transconductance β; this parameter depends on the transistor length L, transistor width W and the gate oxide thickness t_{ox} [25];
- Threshold voltage V_{th}; this parameter is determined mainly by gate oxide thickness t_{ox}, intrinsic doping carrier concentration n_i, donor and acceptor doping carrier concentration $N_{D,A}$ and temperature T [25];
- Supply voltage V_{dd}. Note that *voltage supply ramp-up speed* t_r is also known to impact SUV stability [15]. Nevertheless, the proposed model does not deal with t_r; this needs a new model (ongoing work).

PSNM sensitivity parameters can be classified into two groups: technology and non-technology; see Fig. 3. We assume that technology parameters are the ones that are directly dependent upon the technology node such as L, and non-technology parameters are the ones that can be controlled externally such as T and V_{dd}. Note that the temperature is orthogonal to n_i and V_{th}.

The two previously defined metrics can be used to study the SUVs reproducibility. $PSNM_{ratio}$ can be used for technology parameters as these are the ones that cause the inverters' intrinsic mismatch; this metric provides the relative strength of one inverter as compared to the other. $PSNM_{noise}$ can be

TABLE I: Parameters for $65nm$ BSIM4 model

Parameter	NMOS	PMOS
Temperature T (in °C)	20	20
Supply voltage V_{dd} (in V)	1.2	1.2
Length L (in nm)	65	65
Width W (in nm)	195	130
Threshold voltage V_{th} (in V)	0.423	0.365
Gate Oxide Thickness t_{ox} (in nm)	1.85	1.95

used for the non-technology parameters as these are the ones that can vary the noise tolerance of the cell during operation (after manufacturing). Moreover, these parameters influence all the cell components in a homogeneous way.

IV. Simulation results

In this section, we analyze the impact of technology parameters and the combination of technology and non-technology on PSNM. First, the set-up and experiments are described. Thereafter, the results are presented and discussed.

A. Set-up

We simulate the start-up behavior of an SRAM cell using SPICE and BSIM4 $65nm$ models [26]. The CMOS parameters nominal values used in the simulations are listed in Table I. Note that analyzing the impact of non-technology parameters *alone* is not realistic as PV is always present.

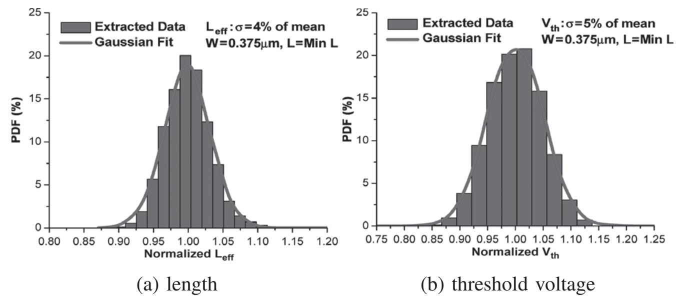
We perform two types of experiments: (1) We vary one technology parameter of one of the MOSFETS of Inverter 1 at a time and analyzed its impact on both $PSNM_{ratio}$ and $PSNM_{noise}$ and conclude about which parameter has the most impact on the reproducibility of the SUVs, (2) we introduce a mismatch on a cell by means of the most dominant parameter and determine the impact of each non-technology parameter on both $PSNM_{ratio}$ and $PSNM_{noise}$.

B. Impact of technology parameters

We performed four experiments in which we vary a single parameter per experiment; these are L, W, V_{th} or t_{ox}. The experiments reveal that the impact of technology parameters on $PSNM_{noise}$ is negligible; e.g., increasing the NMOS V_{th} by +10% increases $PSNM_{noise}$ by only 0.7%. The results on $PSNM_{ratio}$ are reported next.

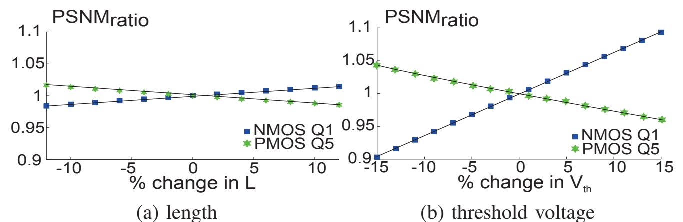
1) Impact of the transistor length L: We simulate the start-up behavior for different values of L, up to $\pm 12\%$ with a step of 2%. This variation corresponds to the worst case scenario for $65nm$ node, where the ratio of standard deviation to mean variation (σ) for L due to PV is $\pm 4\%$ [27]; see Fig. 4(a). The figure shows the PV *Probability Distribution Function* (PDF) of L for this technology. Note that the impact of λ is also reflected in L due to their interdependency.

Fig. 5(a) shows the results of the performed simulation; they reveal the following: (a) $PSNM_{ratio}$ is linearly dependent on L, (b) $PSNM_{ratio}$ indicates that the preferred value of the cell is 1 for an increasing in NMOS L or a decreasing PMOS L, (c) the preferred value of the cell is 0 for a decreasing NMOS L or an increasing PMOS L, and (d) the percentage change in $PSNM_{ratio}$ due to both PMOS and NMOS is similar for same variation in L; e.g., a variation of +10% in PMOS L varies $PSNM_{ratio}$ with 1.4%.



(a) length (b) threshold voltage

Fig. 4: Process variation PDF for $65nm$ [27]



(a) length (b) threshold voltage

Fig. 5: Impact of length and threshold voltage on $PSNM_{ratio}$

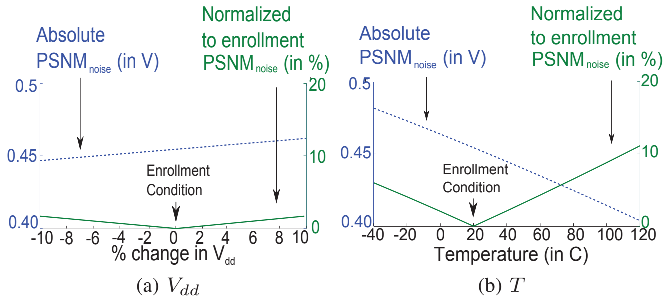
2) Impact of the transistor width W: We simulate the impact of W on start-up behavior in a similar way as we did for L. The results show the same trend as that observed for L, but with opposite effect, e.g., a decrease of W of NMOS results in a $PSNM_{ratio}$ above 1, hence, preferred value 1. Moreover, W has a similar impact as that of L variation.

3) Impact of the transistor threshold voltage V_{th}: We simulate the start-up behavior for different values of V_{th} up to $\pm 15\%$ with a step of 2%. This variation corresponds to the worst case scenario, where σ for V_{th} due to PV is $\pm 5\%$ [27]; see also Fig. 4(b). The simulation results are given in Fig. 5(b); based on the figure we can conclude that (a) the variation in V_{th} has a severe impact on $PSNM_{ratio}$ for both NMOS and PMOS, (b) the impact of NMOS V_{th} variation is the double of that of PMOS; e.g., +10% in NMOS V_{th} increases the $PSNM_{ratio}$ by 6%, (c) $PSNM_{ratio}$ indicates that the preferred value of cell is 1 for an increasing NMOS V_{th} or a decreasing PMOS V_{th}, and (d) $PSNM_{ratio}$ indicates that the preferred value of cell is 0 for a decreasing NMOS V_{th} or an increasing PMOS V_{th}.

4) Impact of the transistor gate oxide thickness t_{ox}: The t_{ox} for $65nm$ node is in the order of $2nm$, i.e., 4 to 5 atoms [28]. The roughness introduced by PV, although small between silicon and silicon dioxide, can be of one or two atomic layers [28]. For the given technology node, t_{ox} for both PMOS and NMOS is indicated in Table I. Since there was no available distribution function for t_{ox} for this technology node, we assumed the worst case variation up to $\pm 30\%$ with a step of 10% and analyzed its impact. The simulation results show similar trends as that of V_{th}; see Fig. 5(b). However, the impact of t_{ox} is $2\times$ less severe than that of V_{th}.

C. Combined impact of stability parameters

The objective of this experiment is to investigate the impact of different supply voltages (i.e., $\pm 10\% V_{dd}$) and temperatures (i.e., from -40°C up to 120°C) on the $PSNM_{noise}$ in a cell with a mismatch in the most dominanting technology



(a) V_{dd} (b) T

Fig. 6: Impact of $PSNM_{noise}$

parameter, which is NMOS V_{th} according to our simulation results. It is worth noting that when considering the non-technology parameters only, the impact on $PSNM_{ratio}$ is negligible; simulation results show that (a) a temperature decrease from 20°C to −40°C increases $PSNM_{ratio}$ by 0.07% and (b) that a supply voltage increase of +10% increases $PSNM_{ratio}$ by 0.01%. The impact results on $PSNM_{noise}$ are reported next.

1) Impact of V_{dd} variation for NMOS V_{th} mismatched cell: For these simulations, a mismatch is introduced on the SRAM cell by increasing the V_{th} of the NMOS transistor Q_1 by 5%. We simulate the start-up behavior for different voltage values up to $\pm 10\% V_{dd}$ with a step of 2% and determined its $PSNM_{noise}$. Fig. 6(a) presents the results; the variation in V_{dd} is represented on the x-axis whereas the y-axis represents the absolute (left) and normalized to enrollment (right) $PSNM_{noise}$ for a particular variation. The figure shows that the impct of V_{dd} on the $PSNM_{noise}$ is negligible for the considered range of values. Absolute $PSNM_{noise}$ increases linearly with V_{dd} increase; e.g., +10% increase in V_{dd} increases $PSNM_{noise}$ by 1.7%. Normalized to enrollment $PSNM_{noise}$ decreases linearly with V_{dd} increase/decrease; e.g., $\pm 10\% V_{dd}$ decreases $PSNM_{noise}$ by 1.7%.

2) Impact of T variation for NMOS V_{th} mismatched cell: For these simulations, the previously NMOS V_{th} mismatch is considered. Fig. 6(b) shows the simulation results for the range of T values considered. The variation T is represented on the x-axis whereas the y-axis represents the absolute (left) and normalized to enrollment (right) $PSNM_{noise}$ for a particular variation. The figure shows that the impact of T on the $PSNM_{noise}$ is severe. Absolute $PSNM_{noise}$ decreases linearly with T increase; e.g., an increase in T from −40°C to 120°C decreases the $PSNM_{noise}$ by 19.3%. Normalized to enrollment $PSNM_{noise}$ decreases linearly with T increase/decrease; e.g., −40°C decreases $PSNM_{noise}$ normalized to enrollment by 6%. However, small variations around enrollment T, e.g., $\pm 10\% T$ $PSNM_{noise}$, have negligible impact.

D. Discussion

An SRAM PUF must have a majority of fully-skewed cells to be reproducible (see Section II). Moreover, an SRAM fingerprint is considered to be reproducible if at least 75% of its SUVs are reproducible. In other words, if the maximum of its non-reproducible SUVs are within the error capability of its ECC, i.e., 25% [17].

Our simulation results showed that from all sensitivity parameters, NMOS V_{th} is the one with the most impact on $PSNM_{ratio}$ and therefore on the reproducibility of SRAM SUVs. To compute the minimum $PSNM_{ratio}$ between two SRAM PUF cell inverters that will reproduce the same SUV (to be fully-skewed), we consider the Gaussian distribution of V_{th}; see Fig. 4(b). From the figure we need to extract the NMOS V_{th} variation that corresponds to 25%. The Gaussian distribution equation is:

$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu)^2/2\sigma^2} \tag{3}$$

where σ is the standard deviation of V_{th}, x represents the variation in V_{th} and μ is the mean of V_{th}. The V_{th} variation a that corresponds to 25% of the cells is:

$$25\% = \int_{\mu-a}^{\mu+a} P(x)\,\mathrm{d}x \implies a = 1.6\% \tag{4}$$

where μ = 1 and σ = 0.05 [27]; see Fig. 4(b). The minimum $PSNM_{ratio}$ for which an SRAM PUF cell starts being fully-skewed is 1.005 if 1 skewed, or 0.995 if 0 skewed; see Fig. 5(b). This calculation is done by assuming the variation in one MOSFET parameter at a time. Although this count may vary when considering all sensitivity parameter variations, this calculation indicates that the cell has a high probability of being fully-skewed; hence, reproducible.

V. Silicon results and validation

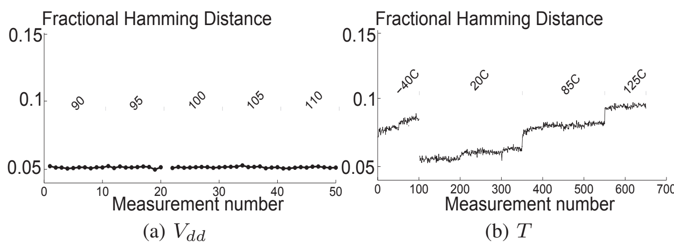
To validate the developed model and have better feeling about the reality, industrial experiments are performed on TSMC and NXP SRAM devices, 20 each, produced in $65nm$ node; all memory devices have a size of 65536 bits. Two experiments are performed to analyze the impact of supply voltage and temperature. In the rest of this section first the results of these experiments are presented and thereafter compared with the simulation results to validate the proposed model.

A. Supply voltage experiment

The SUVs of each of the above mentioned memory devices are measured for five V_{dd} values (i.e., $-10\% V_{dd}$, $-5\% V_{dd}$, V_{dd}, $+5\% V_{dd}$, and $+10\% V_{dd}$) at $20°C$. Each device is powered-up repeatedly ten times with intervals of one second; after each power-up, the SRAM SUVs are read and stored in a binary dump, which are then analyzed using MATLAB.

Fig. 7(a) shows the reproducibility analysis of the measurements performed on a single TSMC device at different V_{dd}. The remaining devices follow the same trend. The metric used to analyze the reproducibility is *Fractional Hamming Distance* (FHD); FHD gives a percentage of the total number of SUVs that have *different* values when compared to enrollment. Ideally, FHD should be zero. In our case, enrollment is performed at nominal V_{dd}. Fig. 7(a) shows that V_{dd} has a negligible impact on FHD.

The experiment was redone for NXP devices. The results show similar trends as those obtained for TSMC devices, but



(a) V_{dd} (b) T

Fig. 7: FHD for several enrollment conditions

with a FHD 1.5x higher. It can be concluded that the probability of reproducing the same SRAM SUVs is marginally impacted by V_{dd} variations.

B. Temperature cycle experiment

In this experiment SUVs are measured for different temperatures: $-40°C$, $20°C$, $80°C$ and $125°C$ with a V_{dd} of 1.2V. Each device is powered-up repeatedly 100 times for $-40°C$ and $125°C$, 250 times for $20°C$ and 200 times for $80°C$ with intervals of one second; after each power-up, the SUVs of the memories are read and stored in a binary dump.

Fig. 7(b) shows the FHD for a single TSMC device at different T; it reveals that FHD decreases for both higher and lower T as compared with enrollment; e.g., at $125°C$ FHD is 10% and $-40°C$ is 7%. As it can be seen a variation of $165°C$ in T results only in 10% variation in FHD. A similar experiment was performed on NXP devices and the results shows similar trends, but with a FHD 1.2x higher.

C. Comparison of measurements with simulation results

Both $PSNM$ metrics analysis are performed for a single cell. FHD analysis is performed for 65536 cells (bits) per SRAM device for 40 devices in total. $PSNM$ metrics are therefore a trend indicator of FHD. Next, simulation results are compared with silicon measurements.

1) For supply voltage experiment: Both simulation results and silicon measurements have shown that for 65nm technology node, a variation in the supply voltage V_{dd} has a negligible impact on the SUV reproducibility. Therefore, as silicon measurements follow the same trend as the simulation results, the correctness of the simulation results with regard to V_{dd} behavior can be concluded.

2) For temperature cycle experiment: Simulation results predict a $PSNM_{noise}$ when normalized to enrollment of 6% at $-40°C$ and of 11% for $120°C$. Silicon measurements have shown the same trend but $2\times$ less severe than the simulations predictions. This might be due to the consideration of a single parameter at a time during simulations. Note that the more variation within the SRAM cell technology parameters, the higher the $PSNM_{ratio}$ and hence the SRAM cell stability.

Note that the behavior of the silicon data matches with that of the simulation results from the analytical model, with regard to T.

VI. Conclusion

In this paper an SRAM start-up behavior model based on SNM is developed and the impact of both technology and non-technology parameters on the reproducibility of such behavior is analyzed. First, considering only variations on technology parameters, our model reveals that NMOS V_{th} has the most significant impact. Second, it shows that the reproducibility for combined variations in technology and non-technology parameters around enrollment conditions is more sensitive to V_{dd}. Furthermore, large T variations impact severely the reproducibility. These results are validated by silicon data.

References

[1] http://www.cl.cam.ac.uk/šps32/SG_talk_OSSC_a.pdf
[2] C.Y. Ng *et al.*, "RFID Privacy Models Revisited", *13th European Symp. on Research in Computer Security*, pp. 251-266, 2008.
[3] A.R Sadeghi and D. Naccache, "Towards Hardware-Intrinsic Security: Foundations and Practice", *Springer*, 2010.
[4] R. Pappu, "Physical one-way functions", *Massachusetts Institute of Tech.*, PhD thesis, 2001.
[5] P. Tuyls *et al.*, "Read-proof hardware from protective coatings", *Cryptographic Hardware and Embedded Systems Workshop*, 2006.
[6] http://homes.esat.kuleuven.be/ rmaes/puf.html, 2011.
[7] R. Maes, P. Tuyls and I. Verbauwhede, "Intrinsic PUFs from Flip-flops on Reconfigurable Devices", *3rd Benelux Workshop on Information and System Security*, 2008.
[8] S.S. Kumar *et al.*, "The butterfly PUF protecting IP on every FPGA", *IEEE Int. Workshop on Hardware-Oriented Security and Trust*, pp. 67-70, 2008.
[9] J. Guajardo *et al.*, "FPGA Intrinsic PUFs and Their Use for IP Protection", *Workshop on Cryptographic Hardware and Embedded Systems*, 2007.
[10] R. Maes, P. Tuyls and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs", *IEEE Int. Symp. on Information Theory*, pp. 2101-2105, 2009.
[11] R. Maes, P. Tuyls and I. Verbauwhede, "Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs", *Workshop on Cryptographic Hardware and Embedded Systems*, 2009.
[12] J. Guajardo *et al.*, "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection", *Field Programmable Logic and Applications*, pp.185-195, Aug. 2007.
[13] J. Guajardo *et al.*, "FPGA Intrinsic PUFs and Their Use for IP Protection", *Workshop on Cryptographic Hardware and Embedded Systems*, pp.63-80, Sept. 2007.
[14] M. Hofer and C. Boehm, "An Alternative to Error Correction for SRAM-Like PUFs", *Workshop on Cryptographic Hardware and Embedded Systems*, pp. 335-350, 2010.
[15] D.E. Holcomb *et al.*, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Number", *IEEE Transactions on Computers*, vol. 58, no. 9, September 2009.
[16] B. Skoric, P. Tuyls and W. Ophey, "Robust key extraction from physical unclonable functions", *Applied Cryptography and Network Security, vol. 3531 of LNCS*, pages 99-135, Springer Berlin / Heidelberg, 2005.
[17] V. vd Leest, P. Simons and E. vd Sluis, "Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs", *HOST*, 2012.
[18] X. Boyen, "Reusable cryptographic fuzzy extractors", *ACM Conference on Computer and Communications Security*, pages 82-91, 2004.
[19] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", *LNCS 3027*, 2004.
[20] J.P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates", *Proceedings of AVBPA'03 Springer-Verlag*, pages 393-402, Berlin, Heidelberg, 2003.
[21] E. Seevinck, F.J. List and J. Lohstroh, "Static-Noise Margin Analysis of MOS SRAM Cells", *IEEE Journal of Solid-state Circuits*, vol. sc-22, no. 5, October 1987.
[22] A. Pavlov and M. Sachdev, "CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies", *Springer*, 2008.
[23] A. Dargar, "Modeling SRAM Start-up Characteristics for Physical Unclonable Functions", *Delft Univ. of Tech.*, MSc. Thesis, 2011.
[24] A. Sedra and K. Smith, "Microelectronics Circuits", *Oxford*, 2004.
[25] S. Dimitrijev, "Principles of Semiconductor Devices", *Oxford Univ. Press*, 2006.
[26] http://ptm.asu.edu/, 2011.
[27] W. Zhao *et al.*, "Rigorous extraction of process variations for 65nm CMOS design", *European Solid State Device Research Conf.*, pp. 89-92, 2007.
[28] G.N. Silva and A. Chandrakasan, "Leakage in Nanometer CMOS Technologies", *Springer*, 2006.
[29] H. Qin *et al.*, "SRAM Leakage Suppression by Minimizing Standby Supply Voltage", *Int. Symp. on Quality Electronic Design*, pp. 55-60, 2004.