A Cautionary Note When Looking for a Truly Reconfigurable Resistive RAM PUF

Kai-Hsin Chuang[1,2], Robin Degraeve[2], Andrea Fantini[2], Guido Groeseneken[2,3], Dimitri Linten[2] and Ingrid Verbauwhede[1]

[1] imec-COSIC, KU Leuven, Belgium,
kai.hsin.chuang@imec.be,ingrid.verbauwhede@esat.kuleuven.be
[2] imec, Belgium, firstname.lastname@imec.be
[3] ESAT, KU Leuven, Belgium

Abstract. The reconfigurable physically unclonable function (PUF) is an advanced security hardware primitive, suitable for applications requiring key renewal or similar refresh functions. The Oxygen vacancies-based resistive RAM (RRAM), has been claimed to be a physically reconfigurable PUF due to its intrinsic switching variability. This paper first analyzes and compares various previously published RRAM-based PUFs with a physics-based RRAM model. We next discuss their possible reconfigurability assuming an ideal configuration-to-configuration behavior. The RRAM-to-RRAM variability, which mainly originates from a variable number of unremovable vacancies inside the RRAM filament, however, has been observed to have significant impact on the reconfigurability. We show by quantitative analysis on the clear uniqueness degradation from the ideal situation in all the discussed implementations. Thus we conclude that true reconfigurability with RRAM PUFs might be unachievable due to this physical phenomena.

Keywords: physically unclonable function · reconfigurable · nonvolatile memory · resistive RAM

1 Introduction

Physically unclonable functions (PUFs) are emerging hardware primitives for cryptographic applications. The silicon PUFs enable the on-chip secret key generation and entity authentication [MVHV12, SD07]. The key generation applications of PUFs harvest entropy from the intrinsic process variation of solid-state devices including field-effect transistors (FETs) and memory elements. These elements form the arrays that produce readable random data with the number of bits linearly proportional to the number of elements, which is noted as "weak" PUF. The number of output bits from weak PUFs is normally in the range of a few thousands which is capable to produce secret keys of 128-bits or 256-bits after the post-processing step. Although the weak PUFs provide a more secure and low-cost alternative compared to storing the secret key in a nonvolatile memory (NVM), they have a drawback that the keys are not updatable. Since some applications require an update mechanism, it is really attractive to develop PUFs that can be reconfigured, discarding the previous key material. It should be noted that the "strong" PUFs with a huge amount of challenge-response pairs (e.g. 2^{64}) are usually not memroy-based and thus not further discussed.

IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, Vol. 2018, No. 1, pp. 98–117
DOI:10.13154/tches.v2018.i1.98-117

1.1 Reconfigurable PUF

Reconfigurable PUFs have the ability to reproduce a new array of unpredictable PUFs after a reconfiguration procedure [KSS+09]. The reconfigurability can be useful in case the original key has been revealed and a new key is needed, or it can be used when the application needs to revoke or update the ownership of the PUF-based token [KKVDL+11, YLX10, RJA11]. There exist two groups of reconfigurable PUFs depending on their reconfiguration methods. One is called the *logically reconfigurable* PUF [KKVDL+11, YLX10] and the other is called the *physically reconfigurable* PUF [KSS+09, RJA11, ZKC+14, Che15]. The logical reconfiguration is controlled by logic circuits and algorithms, which require additional hardware primitives and is still vulnerable to the attacks on the non-reconfigurable part. On the other hand, the physically reconfigurable PUF is reconfigured by changing the physical structure. As long as the change of the structure is unpredictable, the renewed key materials are also unpredictable. Consequently, the physically reconfigurable PUFs are more robust and can potentially provide new keys with the same level of security. In the rest of the paper, we will only discuss the physically reconfigurable PUFs and they are denoted as reconfigurable PUFs for simplicity.

1.2 RRAM-based reconfigurable PUFs

Recently, many kinds of emerging memory elements have been proposed aiming at replacing the traditional volatile and nonvolatile memories. The feasibility and reliability studies of these memory elements also show the possibility for them to be used as PUFs exploiting their underlying variability [FGD+15]. For the case of reconfigurable PUFs, there are also candidates in the family of emerging memories. One implementation is based on phase change memory (PCM) [ZKC+14, ZFC+14] and another on resistive random access memory (RRAM) [Che15]. Especially RRAM has drawn a lot of attention in recent years, and PUFs implemented by RRAM are widely discussed. One of the important facts about RRAM operation is that in each programming cycle, the physical structure within the RRAM element is profoundly changed, making it a viable candidate for implementation as a reconfigurable PUF.

1.3 Operation and reconfiguration of RRAM PUF

In order to understand the potential of reconfigurability in the RRAM PUFs, we first show the construction flow of the conventional PUF comparing to the RRAM PUF. The conventional PUFs such as the SRAM PUF harvest and amplify the intrinsic process variation on the metal-oxide-silicon (MOS) transistors as illustrated in Figure 1(a). The PUF behavior originates from the transistor-to-transistor variation, resulting in the cell-to-cell variation (randomness) and the chip-to-chip variation (uniqueness). The result is then readout as the PUF response in digital format, and the non-ideal read-to-read variation is introduced at this stage. Regarding to the physical reconfigurability, the transistor-to-transistor variation, which determines the PUF response, will not change except for long-term aging. Therefore the array cannot be reconfigured per request.

The RRAM-based PUFs rely not only on the variation induced by the fabrication and forming process, but also on the variability within the RRAM cells during the programming phase as shown in Figure 1(b). If we do not consider reconfigurability, the resulting resistance-to-resistance variation is similar to the transistor-to-transistor variation of the SRAM arrays. With any particular circuit configuration, the variations of these resistance can be transformed into PUF responses. Several research papers have shown that the RRAM-based PUF can provide enough randomness and uniqueness [YKO+16, LWP+16]. The read-to-read variation is also relatively small due to the nonvolatile property, resulting in a good stability.

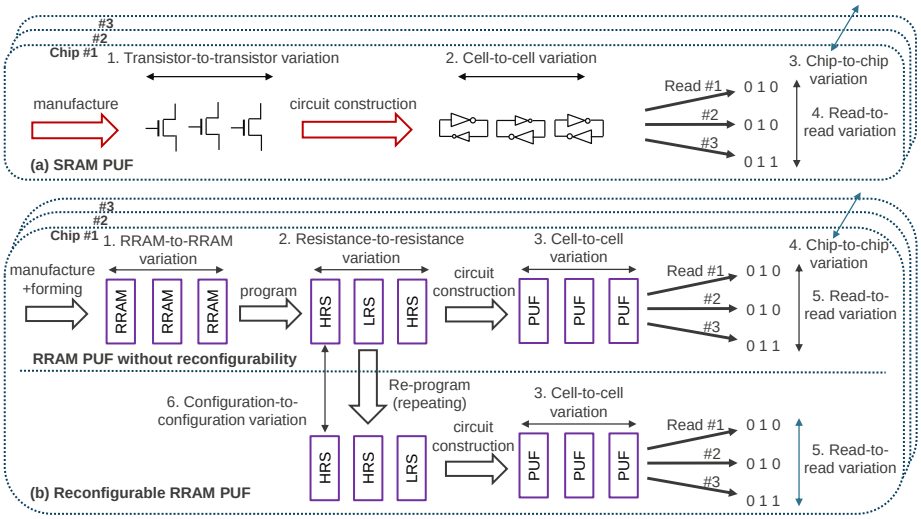

Figure 1: The operation flow and different types of variation on (a) conventional SRAM PUF and (b) reconfigurable RRAM PUF

The reconfigurability of the RRAM PUFs is enabled if the RRAM devices can be reprogrammed into new resistive states as shown in Figure 1(b). The switching variability of the RRAM devices introduces the configuration-to-configuration variation, making the new configurations and the resulting PUF responses different to the original ones. Since the PUF properties of the non-reconfigurable part have been well-studied, we will focus on the uniqueness between different configurations from the same RRAM array.

These definitions will be further used in the remaining contexts and is summarized as the following:

1. **RRAM-to-RRAM variation**: The structural differences after the RRAM array is fabricated and formed, which will not change after normal operations including the programming and reading as a memory device.

2. **Resistance-to-Resistance variation**: The variation between the resistive states of the devices in an RRAM array after a programming step.

3. **Cell-to-Cell variation**: The variation between PUF bits generated by the unit cells constructed by the programmed RRAMs. It represents the *randomness* of the PUF and the ideal case is that every cell has a 0.5 probability to differentiate from one another.

4. **Chip-to-Chip variation**: The variation between the PUF bits at the same location from different PUF chips. It represents the *uniqueness* of the PUF and is normally assessed by the *inter-chip hamming distance*, which has an ideal distribution with a normalized mean equals to 0.5.

5. **Read-to-Read variation**: The variation between different PUF readouts, which represents the *stability* of the PUF. In the ideal case, the hamming distance between readouts should be zero. The SRAM PUFs have higher read-to-read variations comparing to the NVM-based PUF.

6. **Configuration-to-Configuration variation**: The variation between the old and new configurations after the RRAM array is re-programmed, which determines the

uniqueness between the reconfigured key materials. It can also be assessed by the *inter-configuration* hamming distance, and the ideal distribution has a normalized mean equals to 0.5. The focus of this paper is to show that the RRAM PUFs cannot approach the ideal case based on the physical model and experiments.

1.4 Contribution

- First, we summarized several PUF implementations using filamentary oxygen vacancy-based RRAM from literature. We unified them using a RRAM model to show the PUF behaviors and the possible true reconfigurability.
- Second, we describe the two types of variability existing in this RRAM, showing that the configuration-to-configuration variation enables the reconfigurability and the RRAM-to-RRAM variation is limiting the reconfigurability.
- Finally, using an existing physics-based model, a quantitative analysis on how reconfigurability is degraded with the RRAM-to-RRAM variation is demonstrated.

1.5 Paper organization

The remainder of this paper is organized as follows. Section 2 introduces the oxygen vacancy-based RRAM and shows how it can be modeled. Section 3 describes five RRAM PUF implementations that are possibly reconfigurable. Section 4 discusses the RRAM-to-RRAM variability and shows the impact on the reconfigurability. Section 5 provides the quantitative analysis of the uniqueness between the reconfiguration cycles. Section 6 concludes this work.

2 Concept and modeling of the RRAM

The oxygen vacancy-based resistive random access memory has demonstrated robust scaling ability down to 10nm and promising performance and reliability [AS10]. The concept of RRAM operation relies on the voltage-controlled resistance modulation of a conductive filament that is formed in the dielectric material of a metal-insulator-metal (MIM) stack. In the dielectric stack shown in Figure 2, the oxygen vacancies or the charged oxygen ions are identified as the mobile defects, forming the conductive filament [FGD+15]. In this paper, we will focus on oxygen vacancy-based RRAM since we have sufficient understanding and have the ability to model the stochastic behavior within the filament.

2.1 The hourglass model for RRAM switching

The model used in this paper is published in [DFC+12, DFR+13, DFR+14]. It describes the set/reset transient and captures all the main operation features of oxygen-based RRAM devices, including the statistical and stochastic behavior. As summarized in [DFR+14], the hourglass model has five basic ingredients:

- An electron conduction model for describing the current voltage characteristics, based on the quantum point contact model [MFNC08, UZ98]
- A structural model describing the shape of the filament
- A kinetic model describing the vacancy movement inside the filament
- A thermal model describing the heat generation and its catalyzing effect on switching
- A stochastic model describing the statistical variations in the switching behavior

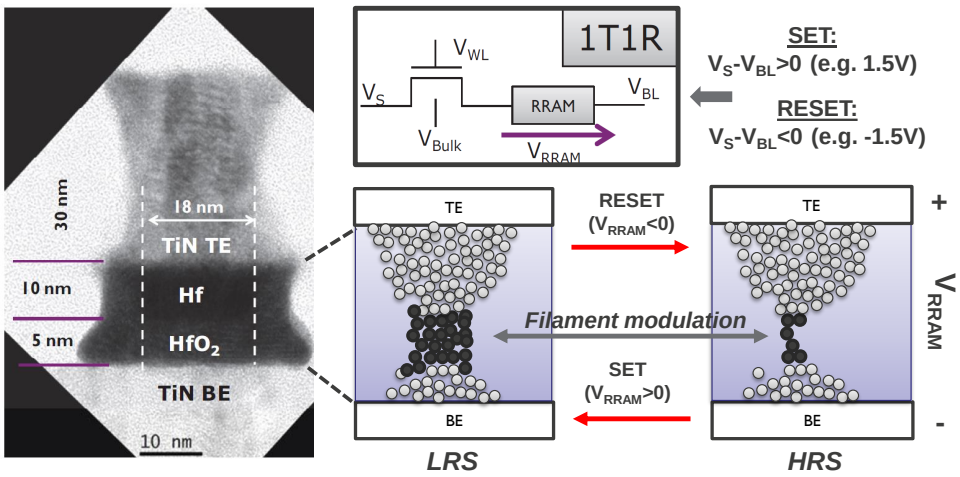

Figure 2: The cross section of an oxygen-based RRAM and the concept of filament modulation resulting from set/reset operations. The RRAM devices using in the experiments are in a one-transistor one-resistor (1T1R) configuration. The black dots in the right-bottom figure shows the mobile defects located in the current-limiting filament constriction. The white dots shows the mobile defects forms the top and bottom conductive part in the filament.

2.2 The RRAM device for experiment and modeling

The RRAM technology used to construct and calibrate the hourglass model is shown in Figure 2. The N-channel driving MOSFET has a channel length of 0.13 μm and was fabricated in a 65nm technology, allowing compatible operating voltages for both forming and set/reset operation. The resistive switching stack consists of 65nm physical vapor deposition (PVD) TiN, 5nm atomic layer deposition (ALD) HfO_2, 10nm PVD Hf, and 30nm PVD TiN. The cross-bar RRAM elements are in a one transistor one resistor (1T1R) configuration, which is demonstrated to have excellent performance down to 10x10nm.

2.3 RRAM switching variability

In general, the data stored in a RRAM is distinguished by the conductivity of the filament. There are two basic states: the *low resistance state* (LRS) and the *high resistance state* (HRS) shown in Figure 2. The SET operation switches the RRAM element from the HRS to the LRS, the RESET operation switches it from the LRS to the HRS. The resistances of both states are known to be statistically distributed variables [FGD+15]. This switching variability is the main feature that caught the attention of PUF-related researches. The underlying stochastic process can be described by the hourglass model, resulting in an accurate fit to the actual data as shown in Figure 3. Note that the distributions of RRAM in this paper are plotted using the *probit* scale, which is commonly used in the RRAM research papers to plot the *lognormal*-like distributions, so as our reference materials. It has the advantages of showing all data points and emphasizing the tail of distribution.

A RRAM device has two sources of variability, the first one is the resistance variation between each set/reset cycle, resulting in the configuration-to-configuration variation mentioned in Figure 1(b). This variation originates from two sources: (i) the varying number of particles in the filament constriction and (ii) the shape of the filament.

There are also pre-existing variations after the forming process of the RRAM devices, which is denoted as the RRAM-to-RRAM variation. This variation stays in the device no

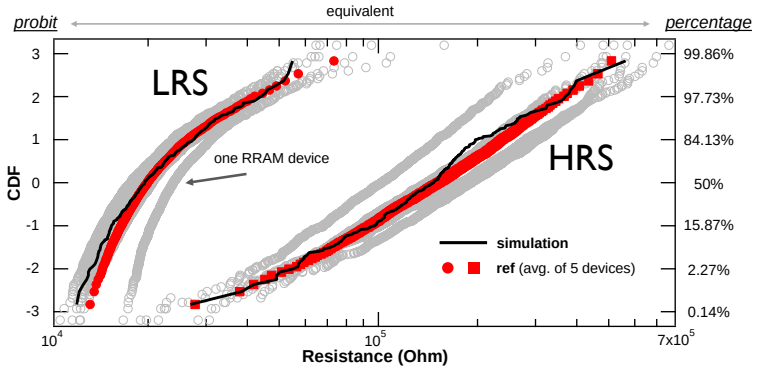

Figure 3: The resistance distributions of LRS and HRS over one thousand set/reset cycles of a RRAM, showing a good match between simulation and the referenced measurement data. The vertical axis shows in probit scale corresponding to the cumulative percentage of a standard Gaussian distribution as illustrated.

matter how many times the device is reprogrammed. In general, the first mechanism is more powerful than the second one, and therefore the impact of the RRAM-to-RRAM variation is often overlooked when considering the RRAM-based reconfigurable PUF implementations.

3 RRAM PUF implementations

In earlier works, several possible implementations of RRAM PUFs have been reported [Che15, CPB14, YKO+16, LWP+16]. Even though in most of these publications, no claim is made with respect to reconfigurability, this potential is always present since the physical filament modulation is the source of entropy in all these implementations. Consequently, we will re-examine these implementations and study their possibility to reconfigure the PUFs. We will reproduce results of these methods based on the simulation using the hourglass model described in the previous section. The measurement results are only collected from our own technology to support the hourglass simulation, since we have no access to the real circuits and measurement data from other RRAM PUF works.

3.1 Resistance variation based PUF

As proposed in [YKO+16], a straightforward implementation is to define a threshold halfway the resistance distribution, be it either the LRS or the HRS. The algorithm is shown in Figure 4 for the case of HRS. The median resistance R_M is defined as the threshold. If the resulting resistance is below or above R_M , it represents "1" or "0" respectively. This method is practical since the HRS distribution of the RRAM is sufficiently wide, resulting in a high reproducibility [YKO+16], even though there is no window between the two decision regions.

3.2 Split resistance variation-based PUF

The temperature and voltage dependence of RRAM resistance may affect the stability of the previous implementation as discussed in [YKO+16]. This reference work proposed a threshold tracking method to find the optimal threshold for different temperatures. This method requires, however, an additional circuit block to perform the realtime tracking, and the tracking procedure delays the data readout. As illustrated in Figure 5, a simpler and more robust modification [CPB14, LWP+16] can be done by comparing the instantaneous

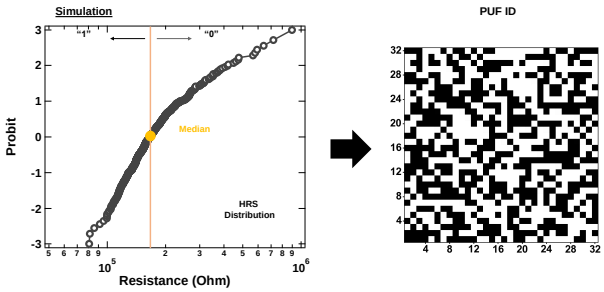

Figure 4: The PUF implementation method using the HRS variation. The threshold value is defined by the median resistance (150 kOhm). The right hand figure show schematically an example of binarized PUF data resulting from the resistance comparison.

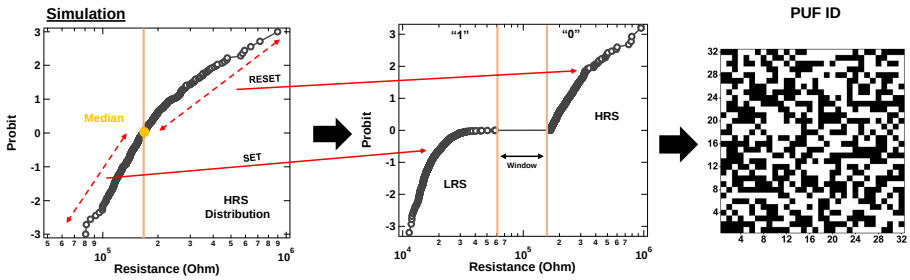

Figure 5: The implementation method using the HRS variation with the split procedure. The threshold for the split procedure is also defined as the median resistance (150 kOhm).

resistance of all cells in HRS to the threshold resistance. The cells having a lower resistance, corresponding to "1", receive a SET pulse, thereby forcing a readout window between the "0" and "1" states. This is referred to as the split procedure. In this way the RRAM PUF can achieve better reproducibility while using exactly the same entropy source. In reference [LWP+16], the authors do not attempt to reconfigure the PUF, although an identical procedure as discussed in Subsection 1.2 can be considered.

3.3 RRAM PUF based on SET failure

Besides the variability on resistance, the set/reset transient is a stochastic process which has a variable success probability depending on the conditions applied to the RRAM. Specifically, the set failure is examined in [DFR+14, FGR+14], showing a clear voltage dependence. This can be well reproduced by the hourglass model as shown in Figure 6. A clear separation can be found between the resistance of the successful and the failed SET operations. This observation can be exploited to generate PUF data, with a failure rate close to 50% using an optimized SET condition. The complete algorithm is shown in Figure 7. Each RRAM has been reset to the HRS before applying a SET pulse with low voltage, so called *half-SET*, with a targeted failure rate of 50%. An additional reinforcement step is applied to all RRAM elements, by applying a SET with full strength to the those devices with low resistance and applying a full strength RESET to those with a higher resistance.

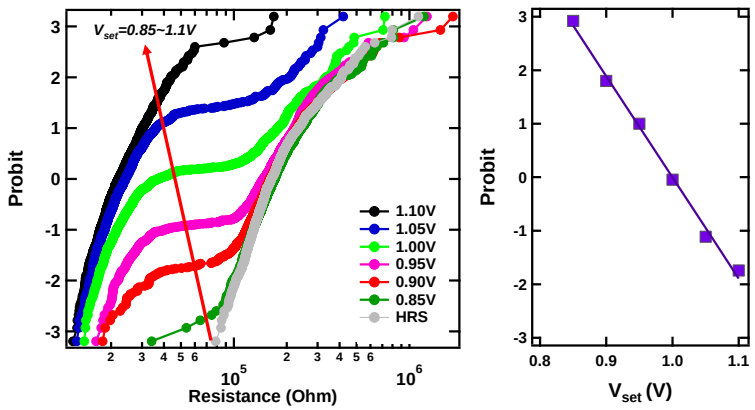

Figure 6: A simulation on the resistance distribution after SET operation for different V_{set}. The right figure shows the set failure probability extracted from the left curves.

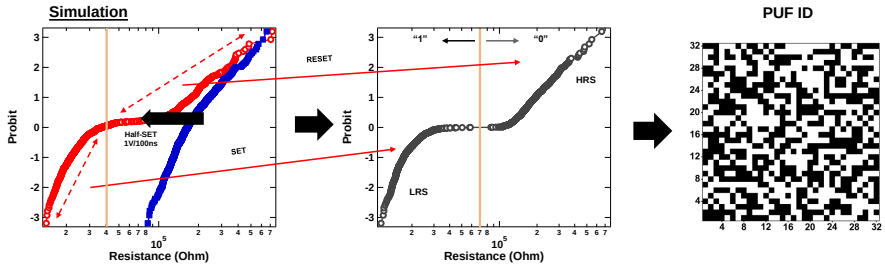

Figure 7: The PUF implementation method relies on (i) first applying a SET pulse aiming at half of the population in LRS, (ii) reading and subsequent reinforcement of LRS and HRS aiming at eliminating the unstable bits. The threshold to determine high/low resistance for the reinforcement is 40 kOhm.

3.4 RRAM PUF based on multiple SET

Following the SET failure phenomenon of the previous section, there is another possible implementation which was first proposed for anti-fuse OTP memories [LHSB10], aiming for the exactly 50% of "0" and "1" bits. Similar to the half-SET method, the first step is to apply a SET pulse with reduced voltage or pulse-width (low-SET), resulting in a SET probability lower than 50%. The algorithm then checks the percentage of cells successfully set to LRS. If the result is below 50%, the low-SET pulse is repeated. This loop will continue until the resistance distribution of RRAM cells is sufficiently close to 50/50 HRS and LRS. The low-SET is also followed by the same reinforcement step applied as in Subsection 3.3 to further separate high and low resistance. The method proposed in this section can be summarized as an *active control* algorithm compared to the method in Subsection 3.3.

3.5 Coupled RRAM PUF with parallel SET

The last implementation discussed in this paper is proposed in [BAC+16], originally to implement a true random number generator (TRNG). This implementation requires an one-transistor/two-resistor structure as shown in Figure 9. Note that the voltage of the

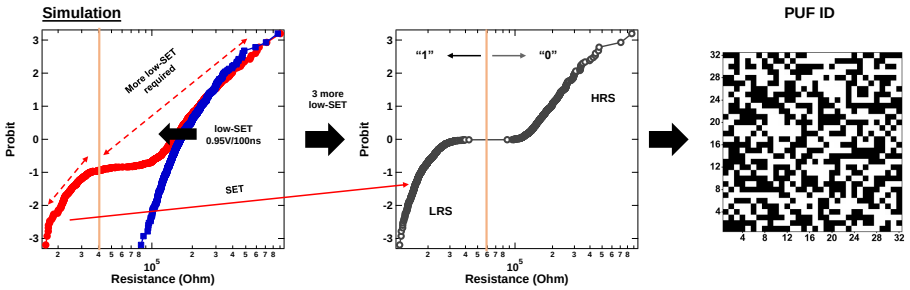

Figure 8: The PUF implementation method using multiple SET: (i) first applying a SET pulse aiming at under 50% of the population in LRS (ii) repeating the SET pulses until the population in LRS is sufficiently close to 50%. The threshold to determine SET failure is 40 kOhm.

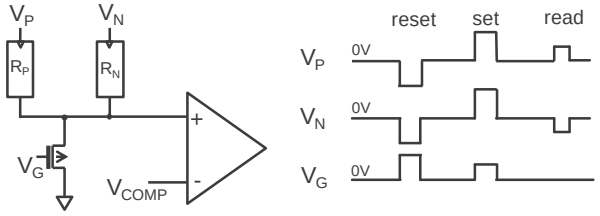

Figure 9: Schematic and timing diagram of the RRAM with parallel SET. The readout can be done by comparing the voltage at middle node to a reference voltage.

two RRAMs can be applied separately. A SET pulse with nominal operation voltage is applied to both RRAMs in parallel. The voltage will drop equally over the two RRAMs, thus starting the SET process simultaneously. Since the SET transient is stochastic, one of the RRAMs will switch to the LRS before the other does. As soon as one RRAM switches from HRS to LRS, the voltage across both RRAMs will significantly drop due to the voltage divider between the RRAMs and the transistor. Consequently, the SET process is terminated as the voltage is insufficient to introduce a second SET transition. As a result, one RRAM is in LRS and the other one is in HRS. As proposed in [BAC+16], the output can be read by applying a readout voltage across V_P and V_N. The comparator will give an output "1" or "0" bits if R_P or R_N is set to LRS respectively. The strong advantage of this implementation is that it requires only one SET step and there is no need to track V_{set} or the median resistance. The 50/50 probability is naturally given if the two RRAM sharing an identical dynamic behavior.

4 RRAM to RRAM variation and the reconfigurability

All the implementations discussed above rely on the stochastic switching behavior of RRAM, which is assumed to provide completely independent results for every new set/reset operations. Therefore, the reconfiguration process can be done by resetting all cells to the same resistive state and perform the programming algorithms discussed above. Note that the resistance distributions in previous section solely show the configuration-to-configuration variation. It means that all the RRAM elements are assumed to have the same resistance distribution over configurations. If this assumption is valid, all of these implementations can be reconfigurable since each element has the equal probability to change state in every new set/reset operations.

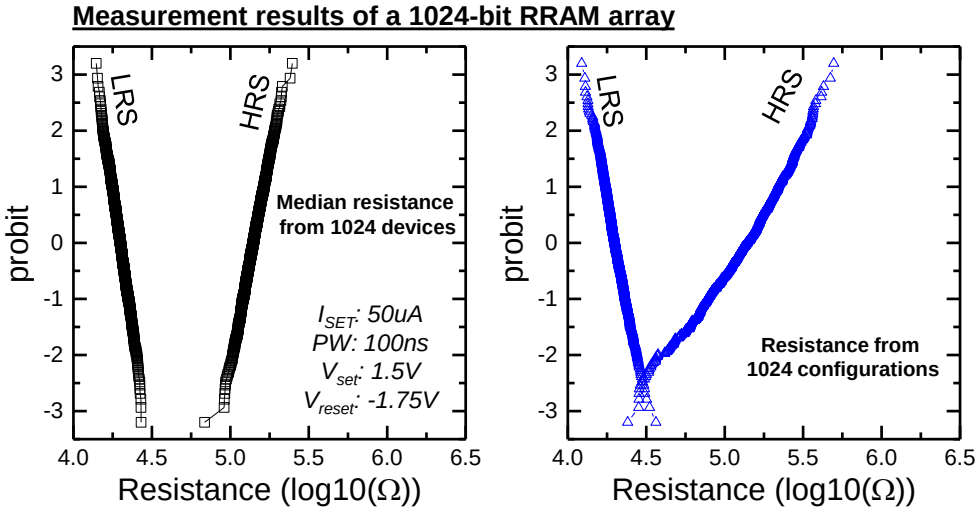

Figure 10: The median resistance distribution from 1024 RRAM devices and the resistance distribution from 1024 randomly selected configurations.

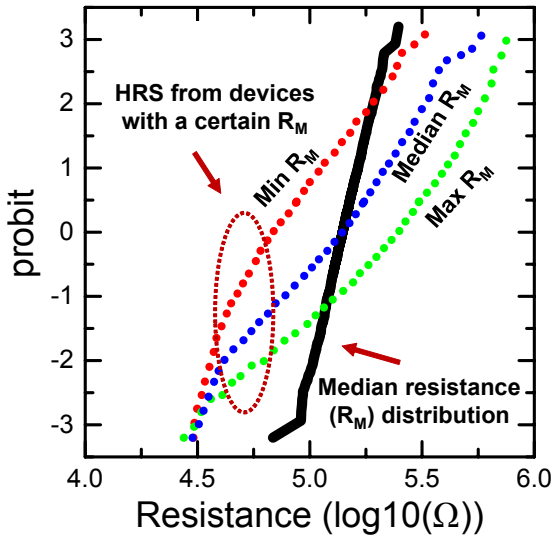

Figure 11: The HRS distributions from the devices with the min/max and median of the median resistance. With a fixed threshold, the probabilities to produce "1" and "0" show large deviations between each devices, which disprove the reconfigurability of this algorithm.

Unfortunately, the pre-existing RRAM-to-RRAM variation also contributes in the reconfiguration process, which biases the set/reset probability for different devices. In this section we will discuss the impact of the RRAM-to-RRAM variation on the reconfigurability of RRAM PUFs.

4.1 RRAM to RRAM variation on an array

We investigated the resistance statistics for RRAM devices from a fabricated 1Mb array in a CMOS technology. The RRAM-to-RRAM variation is extracted by measuring 1024 devices, each for 1024 set/reset configurations. Figure 10 shows the median value from the resistance distribution of each devices. Both the LRS and HRS can be described by a lognormal distribution, and the dispersion of the resistance is about half a decade. This is indeed significantly lower than the configuration-to-configuration variation and can therefore be easily overlooked. By observing the median resistance distribution, a reconfiguration problem is immediately identified for the implementations in Subsection 3.1 and Subsection 3.2 that directly use the resistance distribution.

The threshold in these two methods is by definition the median of the mixed distribution. Since the same threshold is applied to all the RRAM devices, while the medians of the corresponding individual HRS distributions are different, the probability to choose "0" or "1" is not identical for all devices. As shown in Figure 11, the RRAM device with the highest median resistance has only about 13% probability to produce "1", in contrast, the RRAM device with the lowest median resistance has about 88% probability to produce "1". Consequently, the configuration-to-configuration variation is much weaker for the devices with a rather large or small median resistance. A more quantitative analysis will be presented in Section 5, illustrating the severity in this bias.

4.2 Source of the RRAM to RRAM variation

Before studying the impact of the RRAM-to-RRAM variation on other implementations, we first have to understand its source. As described in the hourglass model, the statistics of the HRS can be attributed to the number of vacancies, N_C, in the filament and the shape of the filament constriction [AS10, DFR+13]. In general, the more vacancies make up the constriction, the lower the resistance will be. During the RESET operation, the vacancies are moved out of the constriction with an ion mobility determined by the reset voltage (V_{res}) [FGD+15]. This results in a higher resistance for a higher V_{res}. Although the process variation of the MOS transistors can impact the actual V_{res} drop over the RRAM devices, this impact is relatively small since the transistors are operated in the linear low resistance region. The measured RRAM-to-RRAM variation can, therefore, not be generated by variations of V_{res}.

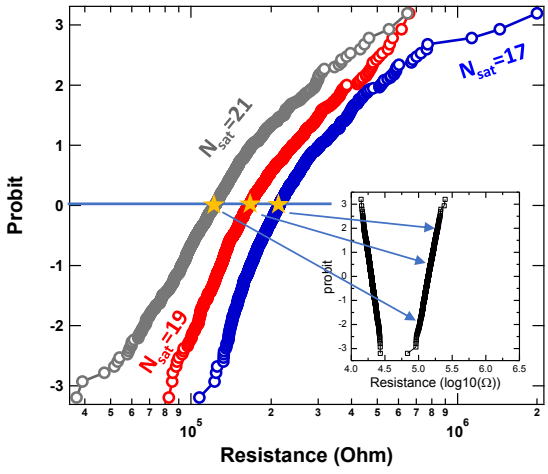

Figure 12: The simulated HRS distribution resulting from three different N_{sat} values. The median resistance stay within the measurement result in Figure 10.

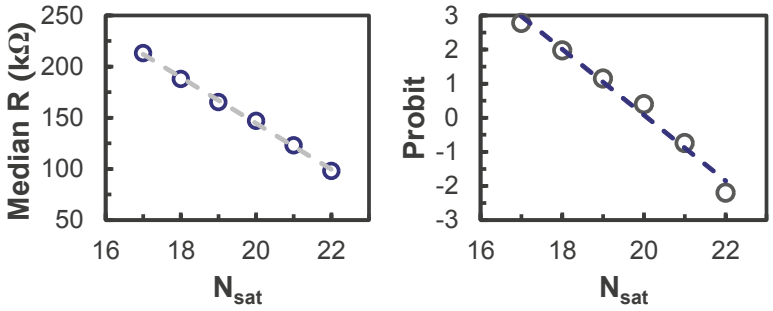

Figure 13: The median of the HRS distributions starting from different N_{sat} values. The right figure shows the corresponding probability to find an N_{sat} in an array, which is mapped by the real measurement data.

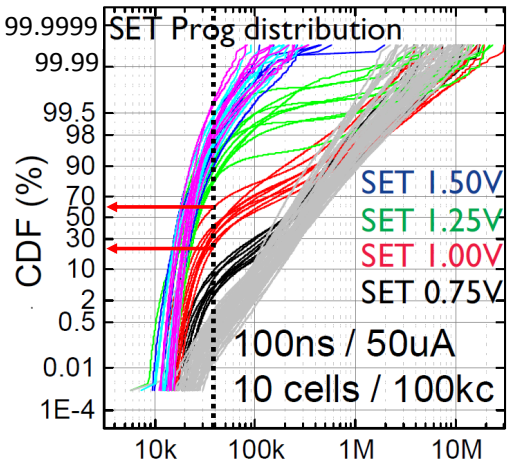

Figure 14: The measured SET failure probability of 10 devices with four different V_{set} (figure in [FGR+14]). The failure probabilities at 1V show a deviation about 30-40% within only 10 devices. The grey curves are the resistive state before SET operation.

The only possible cause of the RRAM-to-RRAM variation originates from the filament. The experimental analysis shows that the HRS saturates at a maximum value that can be modeled by a minimum saturation number of vacancies N_C inside the filament constriction. This number is denoted as N_{sat}, and the number of vacancies cannot decrease beyond N_{sat} after RESET with normal operation conditions. Figure 12 shows the hourglass simulation of the HRS distributions for three different N_{sat} values. The HRS distributions are shifted from right to left corresponding to increasing N_{sat}. Following this simulation, the distribution of N_{sat} can be mapped onto the measurement data as also shown in Figure 12 (inset).

The mapped median resistance and the corresponding probability of finding these N_{sat} values in a device are shown in Figure 13. Note that the linear fitting is a parameterization allowing intermediate fitting.

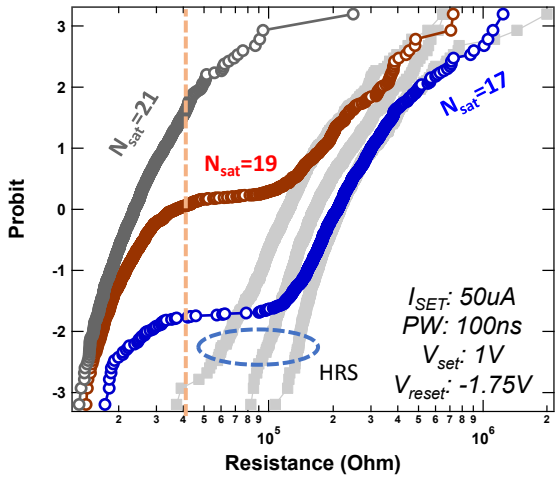

Figure 15: Simulation results of the resistance distribution after half-SET starting from different N_{sat} values. The SET failure rate decreases as N_{sat} increases, the threshold to determine a SET failure is 40 kOhm

4.3 Relation between RRAM-to-RRAM variation and SET failure

Besides having direct impact on the resistance, the variation in the filament also has a strong impact on the switching probability when applying SET at low voltage as is done in the procedures described in Subsection 3.3 and Subsection 3.4. Figure 14 shows an experiment using ten devices with SET at different voltages (V_{set}) starting from the same HRS. As expected, the probability of SET failure decreases with increasing V_{set}. Moreover, it also shows significant differences between devices. It should be noted that the maximum difference between two devices is about 30-40% for a population of only 10 devices. For real cases with thousands of devices, the deviation can be expected to be very severe. Note that because of the large number of measurement (100k/condition), there is no issue with error bar. Even though the absolute difference between failure probability decreases at the lower or higher voltages, this is not considered as an advantage since the failure probability is too far from 50%.

We can also quantify the impact on SET failure using the hourglass model simulation. Figure 15 shows the simulated distributions for V_{set}=1V starting from three HRS distributions corresponding to three N_{sat} values. The probability of SET failure has a clear dependence on N_{sat}. This is in agreement with the experiment shown in Figure 14 and confirms that N_{sat} can be used to model the RRAM-to-RRAM variation. Consequently, through this mechanism, the RRAM-to-RRAM variability intrinsically destroys the reconfigurability of the RRAM PUF algorithms proposed in Subsection 3.3 and Subsection 3.4.

4.4 Transition time

The underlying mechanism controlling the observations in Figure 14 and Figure 15 can be traced back to the variations of the HRS-to-LRS transition time. Similar to the time-to-breakdown in oxides [DGB+98], the transition times of RRAM are also statistical distributions with strong voltage dependences. This explains the dependence of the switching probability to the set voltage and the pulse-width (not shown). Moreover, the kinetic model described in [DFC+12,DFR+13] shows that the transition time is determined by four time constants, that are inversely related to the initial number of vacancies in the constriction. That is, with more initial vacancies, the transition time is on average

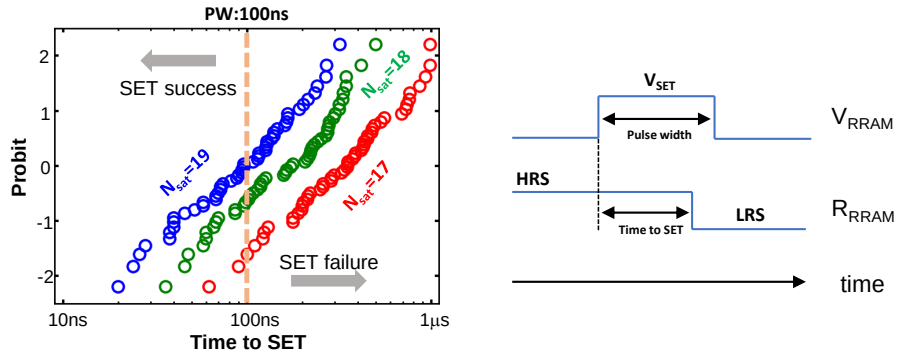

Figure 16: Simulated time of the SET transition time starting from different N_{sat} values and the relation to SET failure with a given pulse-width. The relation between the pulse-width and time-to-set is illustrated in the righthand-side. A set-failure can be observed when the time-to-set is longer than the pulse-width.

smaller. On the other hand, with the same pulse-width, the RRAM devices with more initial vacancies are more likely to be successfully switch to LRS. The distributions of transition time with different N_{sat} are plotted in Figure 16.

The transition time is the entropy source of the coupled RRAM PUF with the parallel SET mechanism as described in Subsection 3.5. Ideally, if both RRAMs have identical transition time distributions, the probability to produce "0" or "1" will exactly equal to 0.5. In reality, the two RRAMs are not identical, e.g. one can have N_{sat}=18 and the other with N_{sat}=19, according to the distributions shown in Figure 12. Consequently, the one with N_{sat}=19 is more likely to switch faster during the next reconfiguration cycle. Therefore, the coupled RRAM PUF is also biased because of the existence of the RRAM-to-RRAM variation on the transition time.

5 Reconfigurability assessment

In order to assess the reconfigurability of all of the implementations discussed in Section 3, we simulate different types of 1024-bit RRAM PUFs calibrated by the real measurements shown in Figure 10 and Figure 11. The main performance metrics for PUFs are randomness, uniqueness and reproducibility. In particular, regarding the reconfigurability, the uniqueness is the key parameter. That is, the randomness and reproducibility should always be satisfied no matter the PUF is reconfigurable or not. For the RRAM PUFs demonstrated in the earlier works [YKO+16, LWP+16, CPB14], these two properties are also proven.

For the unreconfigurable PUF implementations, the uniqueness is assessed by computing the hamming distance between different chips, so called the inter-chip hamming distance (HD_{inter}). This type of uniqueness for the RRAM PUFs has also been proven by earlier works, and therefore is not discussed here. For the reconfigurable PUF implementations, the uniqueness is now calculated between reconfiguration cycles, referred to as the inter-configuration hamming distance (HD_{config}). An ideal reconfigurable PUF will have a HD_{config} identical to the ideal HD_{inter} (50% with normalization), i.e. *reconfiguring the PUF gives the same security as replacing it with a new chip.*

5.1 Reconfigurability using HRS distribution

The relation between RRAM-to-RRAM variation and N_{sat} is well characterized in Subsection 4.2, and serves as the base to construct the RRAM PUF for the assessment. As

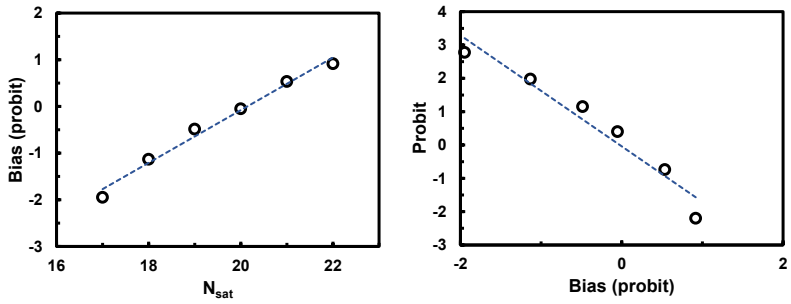

Figure 17: The biased probability of producing "0" or "1" bits by comparing the resistance (described in Subsection 3.1 and Subsection 3.2) for different N_{sat} values. The bias is mapped to the probability of finding N_{sat} (Figure 13), as shown in the right figure. The fitted probability of the RRAM-to-RRAM bias is used for RRAM array simulation.

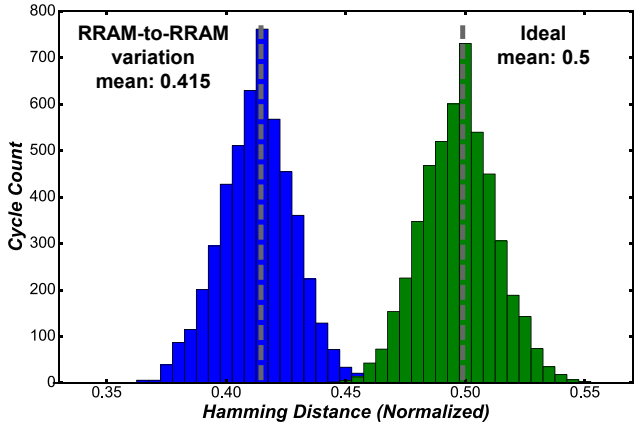

Figure 18: The simulated inter-configuration hamming distance with and without RRAM-to-RRAM variability. The HD_{config} is shifted lower as more devices are likely to produce the same result after reconfiguration.

shown in Figure 11, the HRS distribution is different for different N_{sat}, resulting in biased probabilities to produce "1" and "0" when a fixed threshold resistance is applied. Figure 17 shows the bias to produce "1" as a function of N_{sat} with the threshold of 150 kΩ. This relation is then mapped to the probability of finding N_{sat} (Figure 13), resulting in the bias between configurations. We use the thresholding method described in Subsection 3.1 to simulate the hamming distance between configurations. Note that the split procedure in Subsection 3.2 has impact only on the stability, and therefore it was skipped. The resulting HD_{config} of the RRAM PUF with and without RRAM-to-RRAM variation are shown in Figure 18, illustrating a severe degradation in terms of the configuration-to-configuration uniqueness in the real case.

5.2 Reconfigurability using half-SET

Using the same methodology as in previous section, the bias and HD_{config} are calculated for the half-SET procedure described in Subsection 3.3. The probability for successful SET at V_{set}=1V is shown in Figure 19 and also mapped to the probability of finding N_{sat} (Figure 13). The threshold resistance to define SET failure is 40kΩ. The resulting HD_{config}

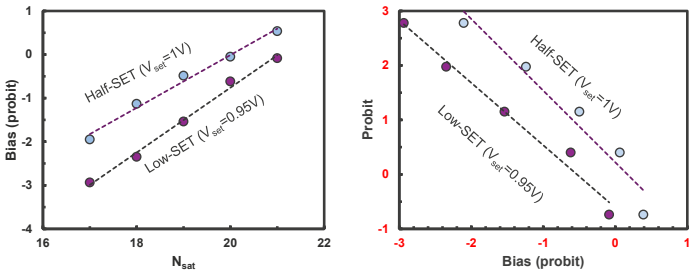

Figure 19: The biased probability of producing "0" or "1" bits by the half-SET and multiple-SET algorithms (described in Subsection 3.3 and 3.4) for different N_{sat} values. The fitted probability of the RRAM-to-RRAM bias in the right figure is used for RRAM array simulation.

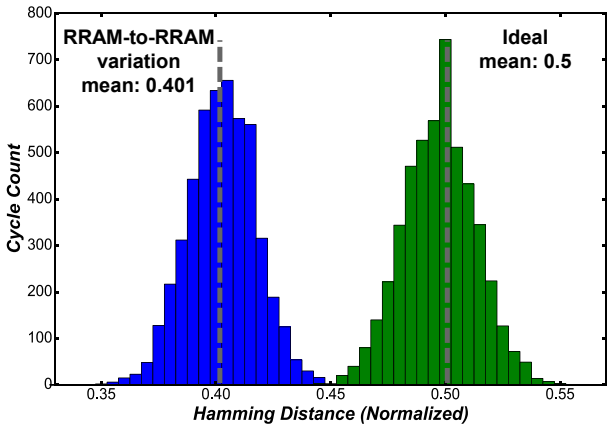

Figure 20: The simulated inter-configuration hamming distance with and without the RRAM-to-RRAM variation. The HD_{config} is shifted even lower than the one in Figure 18, implies that the RRAM-to-RRAM variation has more impact on the SET failure.

of the simulated PUFs with and without RRAM-to-RRAM bias are shown in Figure 20. The degradation is even more severe than in Subsection 5.1. The result shows that the half-SET method does not have good reconfigurability, and is more sensitive to RRAM-to-RRAM variation than directly using the HRS variation.

5.3 Reconfigurability using multiple SET

The PUF generation method using multiple SET, described in Subsection 3.4, uses the same mechanism as the half-SET discussed previously. By applying a low SET pulse, the probability of having a SET failure is increased comparing to the results shown in Figure 19, which results an decreased bias. Following the algorithm described in Subsection 3.4, the PUF data are reproduced for 100 cycles, and the resulting HD_{config} with and without RRAM-to-RRAM variation are shown in Figure 21.

The HD_{config} is the most biased of the three studied cases with 1T1R configurations. The RRAM-to-RRAM variation is amplified by the repeated SET. Note that the mean of the ideal HD_{config} is not equal to 0.5, due to the inherent entropy loss discussed in [LHSB10].

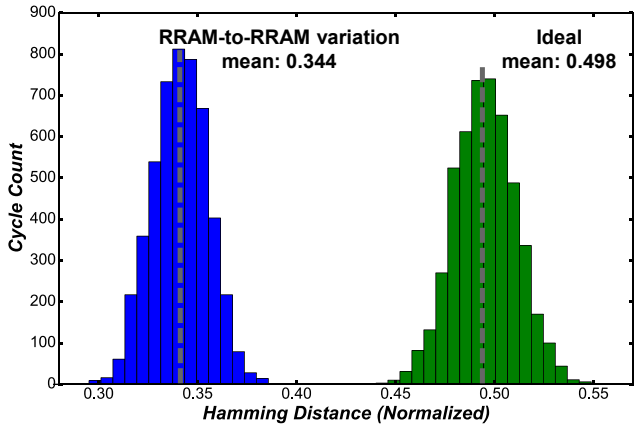

Figure 21: The simulated inter-configuration hamming distance with and without the RRAM-to-RRAM variation using the multiple SET algorithm.

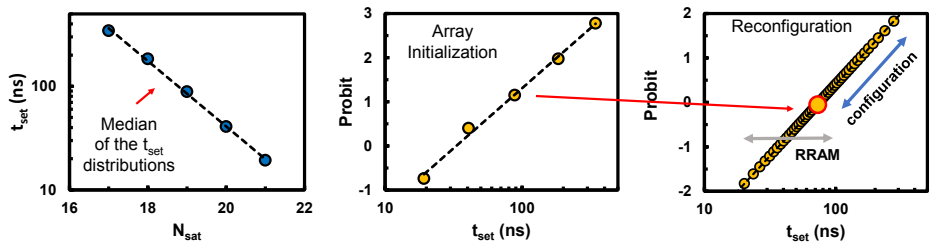

Figure 22: The median SET transition time (t_{set}) for different N_{sat} values and the mapping to the probability of finding N_{sat} (Figure 13) as shown in the middle figure. The median transition time is then used to construct the configuration-to-configuration transition time distribution for each RRAM elements used in the simulation as shown in the right figure.

5.4 Reconfigurability using parallel SET

For the coupled RRAM PUF using parallel SET, as described in Subsection 3.5, the analysis becomes more complicated since the hourglass model is not simulating the interaction between two RRAMs. In order to simulate the transient of two RRAMs in parallel, we first generate an 1024-bit array of coupled RRAMs, where each RRAM device has a median set transition time sampled from the distribution shown in Figure 22. In each reconfigurations, the transition time of each RRAM device is sampled from the configuration-to-configuration distribution and compared. If the transition time of the R_P or R_N (Figure 9) is lower, the output will be "1" or "0" respectively. With this method we are able to simulate the HD_{config} for 100 configurations with and without RRAM-to-RRAM variation, as shown in Figure 23. As observed, this implementation shows the most severe degradation among all implementations.

6 Conclusion

We have discussed the possible methods to implement reconfigurable PUFs using oxygen vacancy-based RRAM. Even though in theory all the individual RRAM devices can be

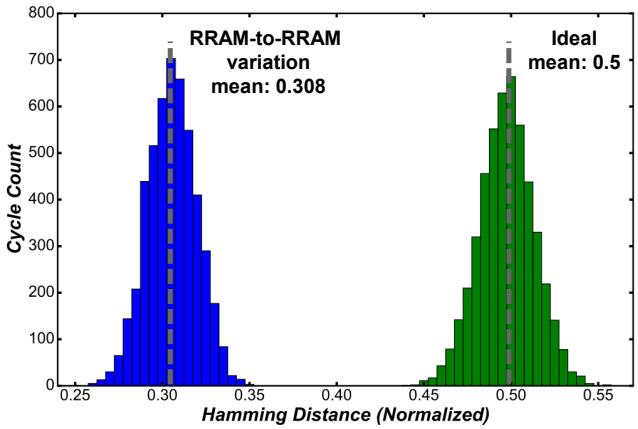

Figure 23: The simulated inter-configuration hamming distance with and without the RRAM-to-RRAM variation using the parallel SET algorithm.

completely reconfigured using a set/reset cycle, there remains a noticeable configuration-to-configuration correlation when the variation inside a full array of devices is considered. This inherent RRAM-to-RRAM variation will create different optimal operating conditions for each resistive RAM device. Using a single algorithm to reconfigure all devices introduces an inevitable bias. The impact can be quantified by the inter-configuration hamming distance and, depending on the used algorithms, is found to be between 31% to 42% as opposed to the ideal 50%.

Using a measurement-calibrated physics-based model, these observation can be understood and explained. We have shown that the RRAM-to-RRAM variation not only affects the optimal threshold to determine 0/1 in a single resistance distribution, but also changes the probability of SET failure and the SET transition time. Consequently, PUFs using oxygen vacancy-based RRAM are not fully reconfigurable, regardless of the algorithm used. Designers should be aware of the degraded uniqueness between configurations when trying to reconfigure the RRAM PUFs.

References

[AS10] Hiroyuki Akinaga and Hisashi Shima. Resistive random access memory (reram) based on metal oxides. *Proceedings of the IEEE*, 98(12):2237–2251, 2010.

[BAC+16] Simone Balatti, Stefano Ambrogio, Roberto Carboni, Valerio Milo, Zhongqiang Wang, Alessandro Calderoni, Nirmal Ramaswamy, and Daniele Ielmini. Physical unbiased generation of random numbers with coupled resistive switching devices. *IEEE Transactions on Electron Devices*, 63(5):2029–2035, 2016.

[Che15] An Chen. Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. *IEEE Electron Device Letters*, 36(2):138–140, 2015.

[CPB14] Wenjie Che, Jim Plusquellic, and Swarup Bhunia. A non-volatile memory based physically unclonable function without helper data. In *Computer-*

Aided Design (ICCAD), 2014 IEEE/ACM International Conference on, pages 148–153. IEEE, 2014.

[DFC+12] Robin Degraeve, Andrea Fantini, Sergiu Clima, Bogdan Govoreanu, Ludovic Goux, Yang Yin Chen, DJ Wouters, Ph Roussel, Gouri Sankar Kar, Geoffrey Pourtois, et al. Dynamic 'hour glass' model for set and reset in HfO_2 RRAM. In *VLSI Technology (VLSIT), 2012 Symposium on*, pages 75–76. IEEE, 2012.

[DFR+13] R Degraeve, A Fantini, N Raghavan, YY Chen, L Goux, S Clima, S Cosemans, B Govoreanu, DJ Wouters, Ph Roussel, et al. Modeling RRAM set/reset statistics resulting in guidelines for optimized operation. In *VLSI Technology (VLSIT), 2013 Symposium on*, pages T98–T99. IEEE, 2013.

[DFR+14] Robin Degraeve, Andrea Fantini, Nagarajan Raghavan, Ludovic Goux, Sergiu Clima, Yang-Yin Chen, Attilio Belmonte, Stefan Cosemans, Bogdan Govoreanu, DJ Wouters, et al. Hourglass concept for RRAM: a dynamic and statistical device model. In *Physical and Failure Analysis of Integrated Circuits (IPFA), 2014 IEEE 21st International Symposium on the*, pages 245–249. IEEE, 2014.

[DGB+98] Robin Degraeve, Guido Groeseneken, Rudi Bellens, Jean Luc Ogier, Michel Depas, Philippe J Roussel, and Herman E Maes. New insights in the relation between electron trap generation and the statistical properties of oxide breakdown. *IEEE Transactions on Electron Devices*, 45(4):904–911, 1998.

[FGD+15] Andrea Fantini, Georgi Gorine, Robin Degraeve, Ludovic Goux, Chao-Yang Chen, Augusto Redolfi, Sergiu Clima, Alessandro Cabrini, Guido Torelli, and Malgorzata Jurczak. Intrinsic program instability in HfO_2 RRAM and consequences on program algorithms. In *Electron Devices Meeting (IEDM), 2015 IEEE International*, pages 7–5. IEEE, 2015.

[FGR+14] Andrea Fantini, Ludovic Goux, Augusto Redolfi, Robin Degraeve, G Kar, Yang Yin Chen, and Malgorzata Jurczak. Lateral and vertical scaling impact on statistical performances and reliability of 10nm TiN/Hf(Al)O/Hf/TiN RRAM devices. In *VLSI Technology (VLSI-Technology): Digest of Technical Papers, 2014 Symposium on*, pages 1–2. IEEE, 2014.

[KKVDL+11] Stefan Katzenbeisser, Ünal Koçabas, Vincent Van Der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, Heike Schröder, and Christian Wachsmann. Recyclable pufs: logically reconfigurable pufs. *Cryptographic Hardware and Embedded Systems–CHES 2011*, pages 374–389, 2011.

[KSS+09] Klaus Kursawe, Ahmad-Reza Sadeghi, Dries Schellekens, Boris Skoric, and Pim Tuyls. Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage. In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pages 22–29. IEEE, 2009.

[LHSB10] Nurrachman Liu, Scott Hanson, Dennis Sylvester, and David Blaauw. Oxid: On-chip one-time random id generation using oxide breakdown. In *VLSI Circuits (VLSIC), 2010 IEEE Symposium on*, pages 231–232. IEEE, 2010.

[LWP+16] Rui Liu, Huaqiang Wu, Yachun Pang, He Qian, and Shimeng Yu. A highly reliable and tamper-resistant RRAM PUF: Design and experimental

validation. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*, pages 13–18. IEEE, 2016.

[MFNC08] E Miranda, P Falbo, M Nafría, and F Crupi. Electron transport through electrically induced nanoconstrictions in HfSiON gate stacks. *Applied Physics Letters*, 92(25):253505, 2008.

[MVHV12] Roel Maes, Anthony Van Herrewege, and Ingrid Verbauwhede. PUFKY: A fully functional PUF-based cryptographic key generator. *Cryptographic Hardware and Embedded Systems–CHES 2012*, pages 302–319, 2012.

[RJA11] Ulrich Rührmair, Christian Jaeger, and Michael Algasinger. An attack on puf-based session key exchange and a hardware-based countermeasure: Erasable pufs. In *International Conference on Financial Cryptography and Data Security*, pages 190–204. Springer, 2011.

[SD07] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14, June 2007.

[UZ98] Stefan Ulreich and Wilhelm Zwerger. Where is the potential drop in a quantum point contact? *Superlattices and microstructures*, 23(3-4):719–730, 1998.

[YKO+16] Y Yoshimoto, Y Katoh, S Ogasahara, Z Wei, and K Kouno. A ReRAM-based physically unclonable function with bit error rate< 0.5% after 10 years at 125 C for 40nm embedded application. In *VLSI Technology, 2016 IEEE Symposium on*, pages 1–2. IEEE, 2016.

[YLX10] H. Yu, P. H. W. Leong, and Q. Xu. An FPGA chip identification generator using configurable ring oscillator. In *2010 International Conference on Field-Programmable Technology*, pages 312–315, Dec 2010.

[ZFC+14] Le Zhang, Xuanyao Fong, Chip-Hong Chang, Zhi Hui Kong, and Kaushik Roy. Feasibility study of emerging non-volatile memory based physical unclonable functions. In *Memory Workshop (IMW), 2014 IEEE 6th International*, pages 1–4. IEEE, 2014.

[ZKC+14] Le Zhang, Zhi Hui Kong, Chip-Hong Chang, Alessandro Cabrini, and Guido Torelli. Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions. *IEEE Transactions on Information Forensics and Security*, 9(6):921–932, 2014.