Towards a Highly Reliable SRAM-based PUFs

Elena Ioana Vatajelu, Giorgio Di Natale, Paolo Prinetto

Towards a Highly Reliable SRAM-based PUFs

Elena Ioana Vatajelu[1], Giorgio Di Natale[2], Paolo Prinetto[1]
[1]Politecnico di Torino, Dip. di Automatica e Informatica, Turin, Italy
[2]LIRMM, Montpellier, France

***Abstract*— Physically Unclonable Functions (PUFs) are emerging cryptographic primitives used to implement low-cost device authentication and secure secret key generation. Several solutions exists for classical CMOS devices, the most investigated solutions today for weak PUF implementation are based on the use of SRAMs which offer the advantage of reusing the memories that already exist in many designs. The high reliability of SRAM-PUFs achieved today by using Fuzzy extractor structures combined with complex error correcting codes (ECCs) which increase the complexity and cost of the design. In this paper we define an effective method to identify the unreliable cells in the PUF implementation based on SRAM stability test. This information is used to significantly reduce the need for complex ECCs resulting in efficient, low cost PUF implementations.**

Keywords—SRAM; PUF; reliability; stability test

I. INTRODUCTION

Physically Unclonable Functions (PUFs) exploit intrinsic manufacturing variability of the CMOS fabrication process to generate a signature unique to each single device [1]. The PUF response is obtained by exploiting physical randomness introduced explicitly or indirectly into the device. Silicon PUFs exploit variation in manufacturing (intrinsic randomness) across different dies and wafers to generate robust, unclonable, unpredictable outputs.

From a mathematical point of view, a PUF is a function that generates an output (also called *response*) starting from an input (also called *challenge*). The challenge-response pairs (CRPs) set must be unique for a single device. PUFs with a significant amount of CRPs are classified as strong PUFs while those with small amount of CRPs are defined weak.

Weak PUF are typically adopted for key generation and storing. The signature must be unique from device to device in order to prevent clonability and thus to guarantee the security of the generated secret key. Moreover, for a same device, it must be robust with respect to aging and environmental variations in order to generate the same value each time. One of the most investigated weak PUF solutions is the memory-based PUFs. Such PUFs use the random initial state of memory bits on device start-up to generate the PUF signature. In this case, the challenge of the PUF is the memory address of a bit and the response is its start-up value. The most common memory-based PUF is based on CMOS SRAM cells [2].

Work has started in earnest to improve the reliability of generated SRAM-based PUF responses. The conventional method to improve PUF reliability is based on the use of error correction codes (ECC). Starting from the raw PUF response (i.e., the one obtained by reading every cells of the SRAM), an ECC is first calculated during the so-called enrollment phase. This code is then re-used as helper data to reconstruct the stable PUF response from the raw PUF response. These ECC blocks generally have significant area overheads, which scale quickly up as the number of correction bits increases [3]. Further, they require the generation and handling of the helper data.

In order to reduce and avoid the need of complex ECC mechanisms, various techniques have been proposed to intrinsically improve the reliability of the PUF. One proposal of increasing the PUF reliability is to use aging effects (NBTI - Negative Bias Temperature Instability) to change the circuit characteristics after manufacturing. By heating the device, the mismatch between the SRAM inverters is increased such that the difference in their electrical characteristics increases in magnitude, and hence strengthens the preference of the affected cell for one of the stable states [4]. However, this method requires a high temperature stress, which cannot be localized to the target cells, therefore aging the entire chip. To eliminate this problem, another method to improve PUF reliability has been proposed in [5] where Hot Carrier Injection (HCI) is used to reinforce the desired PUF response in short stress times without affecting the surrounding circuit. This method is based on a type of bi-stable element PUF that uses sense amplifiers (SA) as the core element. The offset of the SA is the indicator of PUF reliability. Post-manufacturing, HCI stress is applied to the SA to increase its offset, in this way assuring increased PUF reliability. Another approach to increase PUF response reliability is based on strategic selection of the bit-cells in the SRAM array to be used for PUF implementation [6,7]. In [6] the authors propose a strategy for selecting the words used to form the identifier in such a way that the bit flipping can be considerably reduced. In [7] they present a methodology to identify critical conditions for enrollment tests that can identify unreliable bits. Based on this, a bit-selection algorithm is developed that can assist with key selection from the reliable bits obtained at enrollment tests. These methods require multiple enrollment steps (in different environmental conditions) in order to identify the bits severely affected by noise.

In this paper we propose a novel and effective methodology to identify the unreliable bits in a SRAM-PUF based on a modified stability test strategy.

This paper is organized as follows. In the next section we describe the stability issues faced by SRAM cells and standard stability test methodologies. The proposed stability test strategy for the improvement of the reliability in SRAM-based PUF is presented in Section III, while simulation results to show the validity of our proposed method are presented in Section IV. Section V concludes the paper.

II. SRAM CELL STABILITY AND STABILITY EVALUATION

The SRAM cell stability analysis is of great interest to the memory design and test communities and many methods based on static and dynamic analysis have been proposed to evaluate and improve the bit-cell stability [8-11].

In SRAM-based PUF implementations we are interested in the behavior of the bit-cell at power-up. In this scenario we are not concerned with the access transistors, since the control signals are disabled. The same situation is found when the memory cell is in data retention mode.

Data retention stability analysis is concerned with identifying the minimum possible unintended violations (noise) that will flip the data stored by a bit-cell. Traditionally, the immunity to noise is expressed in terms of Static Noise Margin (SNM) which is defined as the maximum value of static noise that can be tolerated by the cross-coupled inverters at the internal nodes (L and R in Fig. 1) before the memory state flips. The SNM can be estimated by drawing and mirroring the voltage transfer characteristics (VTC) of the two inverters (black solid lines in Fig. 2, a.k.a., 'butterfly curve'). The SNM is given by the side of the maximum square which can be inscribed in the wings of the butterfly (dotted line in Fig. 2). If the two inverters of the SRAM cell are identical the butterfly curve is symmetrical (Fig. 2a) and the cell's SNM is given by either one of the maximum squares, i.e., SNM = SNM1 = SNM2. If, on the other hand, the two inverters of the SRAM cell are not identical, the butterfly curve is not symmetrical (Fig. 2b) and, in this situation, the SNM is given by the smaller of the two maximum squares that can be inscribed in the wings of the butterfly, i.e., SNM = SNM2.

However, since the basic 6T SRAM bit-cell is a truly nonlinear time variant system, and its state after power-up is set by a dynamic behavior, a dynamic stability analysis is required. The SRAM bit-cell can be represented as a system of six nonlinear devices (voltage controlled current sources) and two capacitors (the total lumped capacitance at the output node of each inverter) - as shown in Fig. 1. The dynamic behavior of the SRAM cell can be described by a second order nonlinear system. This behavior can be described using the state space analysis. A state space representation is a mathematical model of a physical system based on the input, output and state variables, related by differential equations. The state of the system can be represented as a vector within the state space. A phase space is a space in which all possible states of a system are represented, with each possible state of the system corresponding to one unique point in the phase space. The free evolution in time of each possible state towards the equilibrium point is called state trajectory (green lines in Fig. 2).

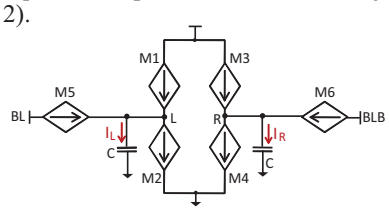

Fig. 1. 6T SRAM bit-cell

An SRAM cell has three equilibrium points: two are stable, associated with the logic '0' and logic '1' (S1 and S2 in Fig. 2), while one is meta-stable (M in Fig. 2). Each stable equilibrium point has its region of attraction in the state space; the boundary between these regions is called separatrix (red dotted lines in Fig. 2). Starting from any initial condition in the region of attraction, the state trajectory will tend towards the equilibrium point as time increases. Starting from any initial condition on the separatrix the state trajectory will move towards to the meta-stable point.

The evolution in time of the bit-cell state can be determined by knowing the position of the separatrix in the phase plane, the cell's initial state, and the input signals. The separatrix of a perfectly symmetrical memory cell coincides with the first bisetrix of the phase plane as can be seen in Fig. 2a. When the bit-cell is asymmetrical, the location of the separatrix changes, as can be seen in Fig. 2b. The phase plane in Fig. 2b corresponds to an SRAM bit cell for which he inverter (M1&M2) is stronger than the inverter (M3&M4). In the complementary case, when the inverter (M3&M4) is stronger than the inverter (M1&M2), the separatrix is above the first bisetrix. The strength of the mismatch determines how far the separatrix is from its ideal position.

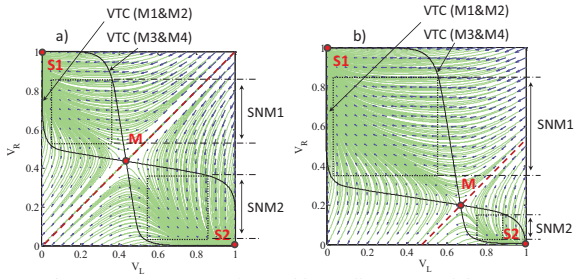

Fig. 2 - Phase space representation and butterfly curves of the 6T SRAM cell in data retention mode: a) for a perfectly symmetrical cell, b) for an asymmetrical bit-cell

At power-up, the SRAM memory is connected to supply voltage (V_{DD}) and the control lines are disabled. Before power-up, the internal nodes of the bit-cell (node L and R) are discharged, i.e., the cell stores no data. This translates in (0,0) initial state in the phase space (blue circles in Fig. 3). Once the circuit is powered-up, the drain-to-source voltages of the PMOS transistors (M1, M3) start increasing. If the transistors are identical, the inversion layer formations are simultaneous resulting in identical voltages on the internal nodes. In turn, this voltage controls the NMOS transistors. If these two are also identical, there is no preferred state of the cell, causing the bit-cell to stabilize in its meta-stable state. The cell's trajectory in the state space follows the separatrix (Fig. 3a). If there is a mismatch between the strengths of transistors two cases are identified. The stable state S1 is preferred by any memory cell for which the transistor mismatch leads to inverter (M1&M2) to be stronger than inverter (M3&M4), as illustrated in Fig. 3b. If the transistors mismatch causes inverter (M3&M4) to be stronger than inverter (M1&M2), the preferred stable state is S2 (Fig. 3c).

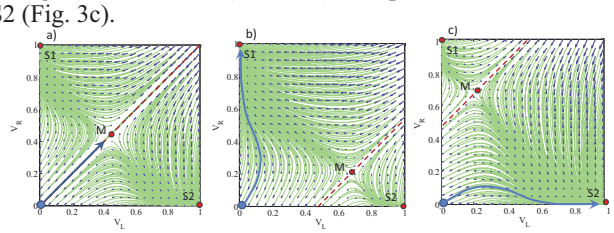

Fig. 3 - Phase space of the SRAM bit-cell and state evolution at power-up: a) for a perfectly symmetrical cell, b) for an asymmetrical bit-cell with inverter (M1&M2) stronger than inverter (M3&M4), c) for an asymmetrical bit-cell with inverter (M3&M4) stronger than inverter (M1&M2).

III. Proposed SRAM Stability Test

Classical stability tests are designed to detect the unstable SRAM cells causing memory faulty behavior. One of the most common cell-stability tests is the data retention test. This test is performed by writing all cells to '1'. Next, the supply voltage of the memory core is decreased to its critical value and the memory array is held in data retention for a predetermined number of clock cycles. Next, the supply voltage is increased to its nominal value and the data is read from the memory array. The unstable cells will flip during data retention at low supply voltage and detected during the read operation. The

procedure is repeated with the memory array being initialized with all cells to '0'.

This method, however, is impractical for the purpose of this work, i.e., to detect the most stable SRAM cells, the ones that will cause unreliability of the PUF response. In order for this method to be relevant, the data retention voltage has to be decreased beyond the critical value used for traditional data retention test and data retention time has to be considerably increased to guarantee that all targeted cells have flipped. This method, as well as any other method dedicated to stability test for memory operation, is not efficient when the highly symmetrical cells are targeted. We propose a test strategy based on dynamic evaluation of bit-cell stability. Figure 4 illustrates the underlying difference between classical stability test and our proposed method. It shows that the classical test detects the most unstable cells, while the proposed test strategy detects the cells with high data stability. As a measure of data stability we use the static noise margin metric described in the previous section, more precisely, the difference between the metrics determined for each of the wings of the butterfly: *SNM1-SNM2*. For perfectly symmetrical cells this difference is zero, and its absolute value increases with the mismatch between the two cross-coupled inverters.

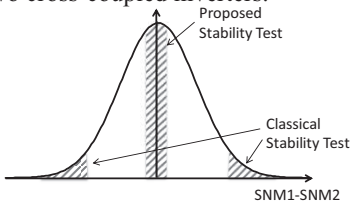

Fig. 4 - Stability test detection: Classical test detects the most unstable cells, while the proposed test strategy detects the cells with high data stability

Our proposed solution for cell stability estimation is based on the dynamic evolution of the cell's state at power-up. The purpose of this analysis is to identify the bit-cells most likely to cause unreliability of the PUF response, i.e. the cells with high symmetry. The underlying principle of our proposed test strategy is illustrated in Fig. 5. If the internal state of the memory cell before power-up is skewed towards the stable state S1, i.e., $V_{L0} = V_{skew}$ and $V_{R0} = 0$, after power-up a symmetrical cell will evolve towards the S1 state and at equilibrium its internal node voltages will be $V_L = V_{DD}$ and $V_R = 0$. In the same way, if its internal state is slightly skewed towards the stable state S2, i.e., $V_{L0} = 0$ and $V_{R0} = V_{skew}$, after power-up it will evolve towards the S2 state and at equilibrium its internal node voltages will be $V_L = 0$ and $V_R = V_{DD}$ (as shown in Fig. 5a).

Nevertheless, if the cell is not symmetrical, for instance the inverter (M1&M2) is stronger than inverter (M3&M4), after power-up, the internal state of the cell will evolve towards stable state S1, regardless of the initial state skew (Fig. 4b) direction. Fig. 4c shows the opposite case where the inverter (M1&M2) is weaker than inverter (M3&M4).

The proposed method uses a 2-step procedure where the memory is first powered-up with initial state of the cells skewed towards the state S1, and then the memory is powered-up again with initial state of the cells skewed towards the state S2. If the state of the cell stabilizes in S1 in the first step and in S2 in the second step, the cell is highly symmetrical and thus not suitable for PUF purposes (unreliable bit in the PUF response). On the contrary, if the state of the cell stabilizes in the same state in both cases, the cell is not asymmetrical, therefore very stable in the PUF context.

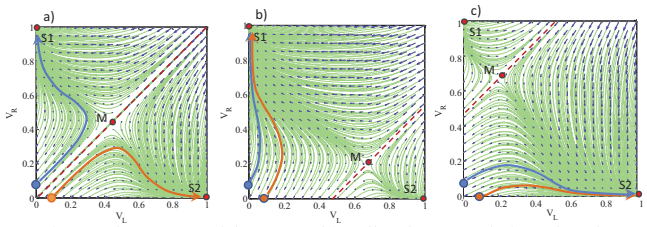

Fig. 5 - Phase space of the SRAM bit-cell and state evolution when the proposed method is implemented: a) for a perfectly symmetrical cell, b) for an asymmetrical bit-cell with inverter (M1&M2) stronger than inverter (M3&M4), c) for an asymmetrical bit-cell with inverter (M3&M4) stronger than inverter (M1&M2).

In order to implement the proposed test strategy, the classic SRAM memory design is modified as shown in Fig. 6. The added hardware (marked in red) is used to set the initial state of the cell internal nodes before power-up. In today SRAM memory design the supply voltage of the peripheral circuit is decoupled from the supply voltage of the memory array to save power when the memory is in data retention and in some cases to increase the reliability. We take advantage of the double supply voltage to perform the power-up in two steps. First, the peripheral supply voltage is enabled and the word lines are selected, i.e., $V_{WL} = V_{DD}$. In this way the access transistors are ON and the cross-coupled inverters are OFF. The bit-lines are decoupled from the pre-charge circuit (PRE) and also from the read/write driver (SA/WD) since no bit-line is selected. Next, the test sequence is initiated by enabling the signal TE ($V_{TE} = V_{DD}$ and $V_{TEB} = 0$). In this way, the bit-line BLB is connected to ground ($V_{BLB} = 0$) and the bit-line BL is connected to the proposed V_{skew} generator ($V_{BL} = V_{skew}$). These voltages are transferred to the cell's internal nodes through the access transistors. Next, the TE signals (TE and TEB) and WL signals are disabled separating the core cells from the bit-lines and the supply voltage of the memory array is enabled. During ramp-up of the memory array supply voltage, the memory cells will stabilize in one of the two stable states. After the power-up process is complete, the memory content is normally read. Once the read operation is completed, the supply voltage of the memory array is disabled and the data is erased from the array.

The same procedure is repeated, and this time the signal TEB will be enabled before power-up, connecting the bit-line BLB to the V_{skew} generator and the bit-line BL to ground. After the power-up process is complete, the memory content is normally read.

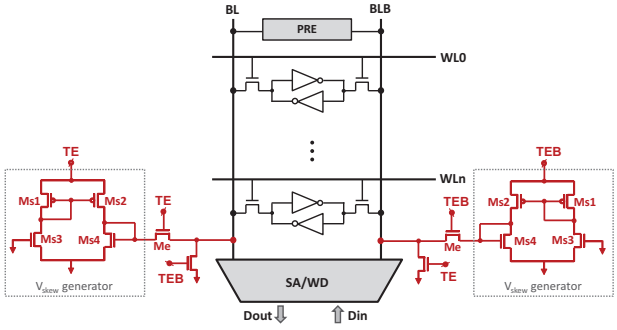

Fig. 6 - Schematic representation of an SRAM memory array column with the dedicated circuit for stability testing marked in red.

The addresses for which the read operations output complementary values are either stored in a nonvolatile memory or on a server, and are used as helper data when the memory is used for PUF implementation. They are the addresses not to be taking into account when a PUF response is

generated. By eliminating these bits from the PUF response, its reliability is greatly improved. The value of the V_{skew} voltage directly affects the efficiency of the method. Using a low V_{skew} value while performing the proposed test allows detecting only the highly symmetrical cells. Increasing this value leads to the detection of slightly asymmetrical cells as well. If the value chosen for V_{skew} is too low, there is the risk of under-testing, i.e., some of the cells which cause unreliability of the PUF response remain undetected during test. If the value chosen for V_{skew} is too high, there is the risk of over-testing, i.e., more bits are eliminated from the PUF response then necessary leading to over sizing the PUF implementation.

The proposed testing methodology has been simulated in HSPICE. Selected results are illustrated in Fig. 7. The behavior of various SRAM cells subjected to random process variability has been simulated using the classical power-up methodology and the two modified power-ups in the proposed stability test methodology (1, 2, and 3 respectively in Fig. 7). Three cells have been selected for illustration purpose only, one symmetrical, and two asymmetrical (a, b, and c, respectively in Fig.8). Both wave form and phase space representations are shown in Fig. 7. The simulation results show high correlation with the theoretical reasoning dynamic cell behavior.

To demonstrate the viability of our proposal, we have performed statistical HSPICE simulations accounting for local and global fabrication induced variability. We generate 500 instances of the SRAM-based PUF implementation, designed with 1024-bit memory. Each PUF instance was once enrolled and then challenged 100 times assuming different noise seeds in the circuit. The results show the number of unreliable cells is between 71 and 108. The 500 instances of our PUF implementation have been tested using the proposed methodology. The test was performed assuming different values for the V_{skew} voltage. When a low value was chosen for the V_{skew} voltage (i.e., 15% of the nominal value of the static noise margin) the number of detected unreliable bits for PUF implementation is between 72 and 107. All cells deemed unreliable by the stability test have shown unreliability when the PUF response was challenged. However, the test coverage is lower than 100%, i.e., not all unreliable bits have been detected. Increasing the value of the V_{skew} voltage (to 20% of the nominal value of the static noise margin) the number of detected unreliable bits for PUF implementation is between 76 and 112. All cells deemed unreliable by the stability test have shown unreliability when the PUF response was challenged and the test coverage is larger than 100% in all cases.

Choosing the right V_{skew} voltage is paramount in the efficiency of the proposed stability test in the detection of PUF unreliable bits. However, since at design time the expected variability range of the fabricated circuit is known, so is the nominal static noise margin, an educated estimation of the optimum V_{skew} is possible.

IV. Conclusions

In this paper we focus on weak SRAM-based PUFs and we introduce a novel stability test strategy designed to identify the unreliable bits in a PUF response. The method uses dynamic stability analysis of the SRAM bit-cell and focuses on identifying symmetrical or nearly symmetrical it cells. These cells are unreliable in the PUF context since they do not show a strong preference to any of the two stable states. Simulation results show that the proposed test methodology greatly improves the SRAM-based PUF response reliability.

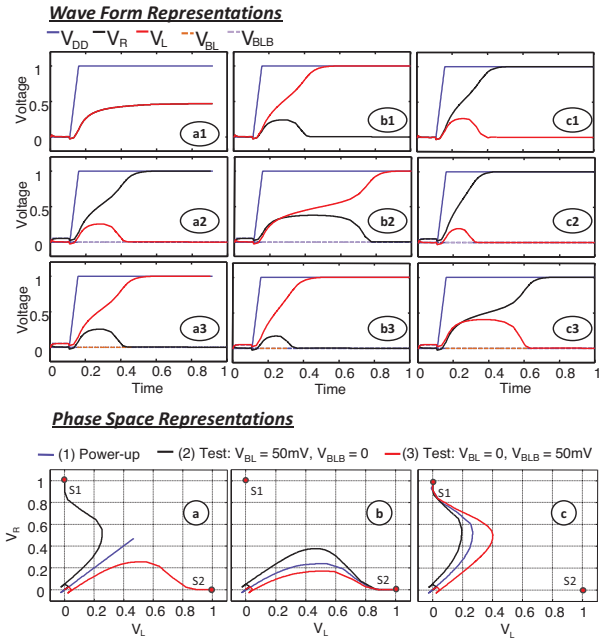

Fig. 7 - Simulation results of an SRAM cell under stability test using the proposed methodology - wave form and phase space representations of the SRAM cell behavior during normal power-up (1), during the two power-up steps of the test algorithm (2) and (3) for a symmetrical bit-cell (a) and two asymmetrical bit-cells (b) and (c).

References

[1] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions, Science, 297(5589), pp. 2026–2030, 2002

[2] J. Guajardo, S. S. Kumar, G.-J. Schrijen, P. Tuyls, FPGA intrinsic PUFs and their use for IP protection, Springer, 2007

[3] M.D. Yu, S. Devadas, Secure and Robust Error Correction for Physical Unclonable Functions, IEEE Design & Test of Computers 27(1), 48–65, 2010.

[4] A. Garg, T.T. Kim, Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect, International Symposium on Circuits and Systems (ISCAS), pp.1941-1944, 2014.

[5] M. Bhargava, K. Mai, A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement, International workshop on Cryptographic Hardware and Embedded Systems (CHES), 90–106, 2013.

[6] S. Eiroa, J. Castro, M.C. Martinez-Rodriguez, E. Tena, P. Brox, I. Baturone, Reducing bit flipping problems in SRAM physical unclonable functions for chip identification, in International Conference on Electronics, Circuits and Systems (ICECS), pp.392-395, 2012.

[7] Kan Xiao; M.T. Rahman, D. Forte, Yu Huang, Mei Su, M. Tehranipoor, Bit selection algorithm suitable for high-volume production of SRAM-PUF, International Symposium on Hardware-Oriented Security and Trust (HOST), pp.101-106, 2014

[8] B. Zhang, A. Arapostathis, S. Nassif, and M. Orshansky, Analytical modeling of SRAM dynamic stability, in International Conference on Computer Aidded Design (ICCAD), pp. 315-322, 2006.

[9] A. Pavlov, M. Sachdev, CMOS SRAM Circuit Design and Parametric Test in Nano-Scaled Technologies, Springer, 978-1-4020-8362-4, 2008

[10] E.I. Vatajelu, G. Panagopoulos, K. Roy, J. Figueras, Parametric failure analysis of embedded SRAMs using fast & accurate dynamic analysis, European Test Symposium (ETS), pp.69-74, 2010.

[11] E.I. Vatajelu, A. Gomez-Pau, M. Renovell, J. Figueras, Sram cell stability metric under transient voltage noise, Microelectronics Journal, vol. 45, no. 10, pp.1348-1353, 2014.