Journal of Electronic Testing
https://doi.org/10.1007/s10836-022-06006-x

A Systematic Bit Selection Method for Robust SRAM PUFs

Wendong Wang[1] · **Adit D. Singh**[1] · **Ujjwal Guin**[1]

Received: 23 December 2021 / Accepted: 31 May 2022

Abstract
A physical unclonable function (PUF) is a digital circuit that can generate a die specific unique and stable response, which can be used for authentication and key generation. Since no major design or manufacturing modifications are required, exploitation of SRAMs to implement PUFs is a promising option. When initially powered up, in dividual SRAM cells acquire unique logic states based on the inherent bias of the cell. At advanced technology nodes, this bias is primarily due to unavoidable random manufacturing process variations, which are unpredictable and vary randomly from cell to cell, as well as chip to chip. When an SRAM is read out, these power-up states provide a unique output that is largely consistent during repeated power-up cycles for a given SRAM, but varies for different copies of the same part, as required of a PUF. However, this powerup state of SRAMs cannot be directly used (e.g. in cartographic key generation), due to unpredictability in some of the SRAM cells caused by electrical and electromagnetic noise and temperature fluctuations. We show in this paper that power-up states are also influenced by the power supply ramp rate at power-up, which can be yet another source of cell instability. To address the general problem of instability in SRAM power-up states that can result in inconsistent responses from SRAM PUFs, we present an effective stable cell selection method to identify the cells in the SRAM that are strongly biased, thereby resistant to circuit noise, voltage and temperature changes, and also aging. The data from the Silicon experiments presented here shows that the selected stable SRAM cells are highly reliable over temperature and voltage variations, with a bit error rate (BER) close to zero.

Keywords Ramp-up time · SRAM PUF · Bias temperature instability · Power-up state

1 Introduction

A physical unclonable function (PUF) is a die-specific random function or a silicon biometric, which can generate a unique predetermined response to an applied stimulus or challenge. The uniqueness of many PUF designs is derived from the variations that occur during the fabrication process in a completely unintentional, random and uncontrollable manner. These unique responses can be used as key generation and authentication in hardware security application [32]. Compared with the alternative of storing the random response information in non-volatile memory, PUFs provide more resilient resistance to physical attack since the information will disappear during power off. Moreover, the response from each PUF is unique, ideally even for copies of the same design in different dies.

A number of PUFs structures have been proposed in recent decades, such as arbiter PUFs, ring oscillator PUFs, Latch PUFs and many more [10, 23]. SRAM-based PUFs have been proposed in [11]. These exploit the power-up value of cells to provide the PUF response, with the corresponding address serving as the challenge. In practice, a SRAM cell can store one specific desired bit of information: either a '0' or '1', depending on the information that has been written in during the write process. However, the information stored in SRAM cells is unpredictable when the array is first powered on without any preceding write operation. This is because the state stored in the SRAM cells will be decided by the relative the strength of the two back-to-back inverters in the

Responsible Editor: M. Taouil

✉ Wendong Wang
wendong@auburn.edu

Adit D. Singh
adsingh@auburn.edu

Ujjwal Guin
Ujjwal.Guin@auburn.edu

[1] Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849, USA

Published online: 07 June 2022

SRAM cells. Ideally, the two inverters in each cell are identical, but in practice they will be slightly different in unpredictable ways because of random process variations (unique to each copy of the circuit) caused by random-dopant fluctuations, line-edge roughness, etc. [15]. Thus, in any SRAM, some of the cells will power up to logical '0' and others to logical '1'. This unique this pattern of 0 s and 1 s in each SRAM has been used for implementing PUFs based on the power-up states of SRAM cells.

SRAMs are widely employed as building blocks in FPGA and many system-on-chips (SoCs), which make the implementation of SRAM PUF simple and require no additional design processes. Although the SRAM PUF provides many attractive features, one of the challenges is the reliability of the SRAM cells. Firstly, the power-up state in SRAM cells is highly sensitive to the noise and temperature/voltage variation. Researchers have reported that 5–10 percent of cells are unstable and do not power up to the same consistent value during multiple power-up cycles. Secondly, aging degradation affects the threshold voltage of MOSFETs and can change the relative strengths of the two inverters in a cell, resulting in a change in the power-up state during operation in the field. In order to exploit the start-up value of the SRAM cells to perform some cryptography function (*i.e.*, key generation), the response or start-up value for each SRAM cell should be highly reliable under different operating conditions (*i.e.*, different temperature or voltage). Consequently, incorporation of a SRAM PUF into an end-user device requires extremely high reliability of the power-up response with with a bit-error-rate (BER) close to zero [22]. Several mechanisms have been proposed to reduce cell instability and increase the reliability of SRAM PUFs:

1. Error Correction Codes(ECC): Here ECC such as BCH code [4] has been exploited to reduce the bit-error rate to a specific level so that the SRAM array can be directly used as PUF.
2. Preselection: Reliably stable SRAM cells have been selected during testing, and only these are used as the PUF [17, 22, 26, 30].
3. Hardening: Reverse burn-in aging has been applied to the SRAM cells to strengthen the response of cells. The BER has to reach a reasonable level before SRAM has been deployed as a PUF [2, 16, 21, 25].

Error Correction Codes (ECC) is a conventional approach to enhance the reliability of SRAM PUF with the target bit error rate less than $1e$–6 [3]. The overall methodology is divided into two steps: enrollment and regeneration. During the enrollment, the ECC will perform the encoding by using a larger amount of raw (unstable) data from the SRAM array. The output of encoding will be the secret key and help data. The help data is public information and can be stored in any non-volatile memory. During the regeneration phase, the user will exploit the help data and the new regenerated raw (noisy) PUF data to recover the secret key. In order to successfully recover the secret key in the field, the raw PUF data size and help data will be much larger than the size of the secret key. Typically, it requires 3.68 raw PUF bits to generate 1 stable PUF bit by using BCH code, for a biterror-rate is of $1e$ 6 and the natural instability of PUF bits as 6% [8]. The low instability nature of the PUF bits increases the size of required raw PUF data and help data. For example, to generate 128 stable bits, ECC implementation will require about 3 K-10 K raw PUF bits and 3 K-15 K bits help data if the nature instability (unreliable bits before applying ECC) is about 15% [3]. The ECC implementation will generally introduce a significant hardware overhead.

Since the conventional ECC implementation introduces unwanted hardware overhead, some researchers proposed a preselection scheme, which filters out the unstable cells leaving behind only stable cells as the PUF output. In this way, the final PUF output will be virtually 100% reliable and the bit-error rate will approach zero. At the same time, the overall hardware overhead is negligible since only the address of the selected cell requires to be stored in nonvolatile memory. To identify stable SRAM PUF cells, the researchers in [30] exploit the spatial correlation of the SRAM PUF cells indicating the higher likelihood of the most stable cells to be surrounded by the stable cells. However, this selection method still requires high-temperature/low voltage (HTLV) and low-temperature/low voltage (LTLV) to perform the enrollment test, which will increase both the test time and the cost. Some researchers propose a revised design of the SRAM cells to fulfill the selection of the strong cells [22, 26]. The theory behind this approach is to introduce a skew or tilt to the cells through the revised structure of the SRAM cells. If the natural mismatch of a cell is larger than the introduced tilt, the cell will not change the value before or after introducing the tilt and will be considered as a strong cell for the PUF application. However, this selection method requires the modification of traditional SRAM cells, which will increase design costs and limit the range of application. A remanence-based method has been proposed to evaluate the strength of the SRAM PUF [17]. A value of either a '1' or '0' will first be written to the SRAM cells followed by turning off the power for a very brief controlled period. Thereafter, the cell is powered back on to observe the value. If the cell flips the value that has been written in previously to the cell, it will be considered as a strong PUF cell. However, the selection method requires precise control of the power-off time. This may present implementation challenge for advanced CMOS technology.

In our previous work [29], we have proposed a method that can identify the most stable SRAM cells (strongest cells), where only the V_{DD} voltage needs to be controlled

and not the power-off time. This can be implemented more easily in the practical application. However, only simulation results were provided in the initial paper, and the impact of temperature, voltage variation, and aging effect were not considered in the context of the analysis. In this extended version of the paper, our contributions include:

1. A discussion of the start-up behavior of the SRAM cell and a detailed analysis of the ramp rate effect.
2. Proposal for a comprehensive methodology to perform pre-selection of the strong stable SRAM cells.
3. Presentation of the corresponding data from silicon experiments, including performing voltage and temperature variation and aging experiments to validate the reliability of the selected SRAM cells.

The main objective of this paper is to show that our proposed bit selection method can reliably select the strongest SRAM cells for PUF application. The details of implementation (overhead, power consumption et al.) will greatly depend on the real-world application, such as the memory type, the manufacturing technology, how the memory is tested-externally or with on-board memory BIST, and many other variables. These optimizations are left to be addressed by the SoC designer.

The rest of the paper is organized as follows. In Sect. 2, the necessary background of the SRAM PUF has been discussed: SRAM cell characteristic along with the related work to improve the SRAM PUF reliability and uniqueness. In Sect. 3, we discuss the model of the power-up behavior of the SRAM cells and how the ramp rate effects the start-up value of these SRAM cells. In Sect. 4, the data retention test has been introduced. We shows how it can facilitate selection of the strong cells for PUF applications. In Sect. 5, we propose a comprehensive methodology to identify those strong SRAM cells for PUF application. Section 6 presents data from the silicon experiments and discusses the reliability of the selected SRAM cells. We conclude In Sect. 7.

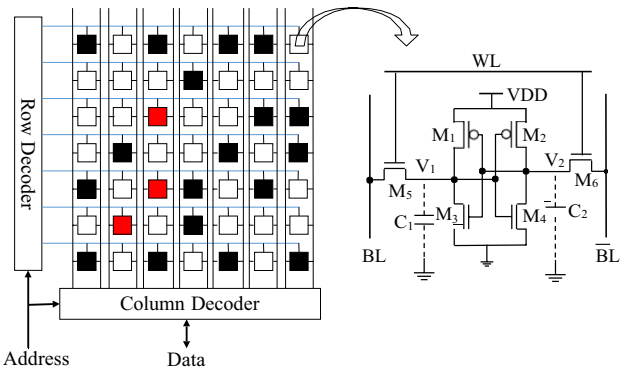
2 Background

In this section, we discuss the details of SRAM PUF, the circuit theory behind it and some of its challenges. Subsequently, we will discuss the related research and our new contributions.

2.1 SRAM PUF

The SRAM PUF is one of the appealing PUF candidate due to its easy implementation and nearly zero hardware penalty [30]. The idea of using the power-up value of the SRAM array as a response of PUFs was firstly proposed in [11]. The response uniqueness of SRAM PUFs is also competitive among the candidate of the existing PUFs [11]. A particularly attractive design for PUFs is based on the static random access memory (SRAM) array, as depicted in Fig. 1a. When an SRAM is initially powered up, each cell acquires a '0' or a '1' logic value. Figure 1b shows the circuit schematic for a 6-transistor SRAM cell. Each cell has a pair of NMOS pull-down transistors, PMOS pull-up transistors, and NMOS pass transistors connecting each of the two (complimentary) cell output to the bit lines. In an ideal SRAM cell, if each transistor pair as described above is identical in every respect, including layout associated parasitic components, then the cell is perfectly balanced. In the absence of an asymmetric electrical noise, such a cell has a random 50% chance of acquiring either a '0' or a '1' state at power-up. However, even a small imbalance within a pair of transistors can result in a cell being biased towards either a '0' or a '1' power-up state. In nanometer-scale technologies, because of uncontrollable small random manufacturing variations, no two transistors in an SRAM cell are truly identical in practice. Consequently, when the SRAM array has been powered up, the process variation along with the noise and environment variation will classify the cells into two main parts:

– Neutral cell: The cell has no strong mismatch among pull-up PMOS pairs and pull-down NMOS pairs. It does



(a) A typical SRAM array. **(b)** A six-transistor SRAM cell.

(c) Bitmap of 64kb SRAM array

Fig. 1 Systematic and random process variations

not mean no process variation happened in M_1 M_2 M_3 M_4 as depicted in Fig. 1b. It only indicates the mismatch among these MOSFETs cancel each other and overall cells have no preference to the states 0 or 1. The final state of these cells will be determined by the noise present in the circuit.

– Skewed cell: The cell has relatively high mismatch among pull-up PMOS pairs (M_1 and M_2) and pull-down NMOS pairs (M_3 and M_4). These cells will have their preferred/consistent state, either a '0' or a '1'.

Figure 1c is a bitmap for a 64 K bit SRAM array. In this bitmap, the red dots represent neutral cells, which show inconsistent power-up state during 100 power-up scenarios. The white dots and black dots represent the skewed cells, which indicate a consistent power-up value during 100 power-up scenarios. Based on the bitmap, about 90% cells hold consistent values. However, among these 90% cells, some cells may only obtain limited mismatch among pull-up MOSFETs and pull-down MOSFETs. In other words, these cells may change their response over time due to device degradation or under different environment such as temperature, supply voltage, or electromagnetic noise. These potential 'weak'/ 'neutral' cells will raise a challenge for SRAMbased PUF since it requires 100% reliability under PUF application.

2.2 Related Works

In order to address the reliability problem for SRAM based PUFs, some complex statistical solutions have been proposed to extract a stable signature [5, 7, 20, 31]. Figure 2 shows a basic step for PUF key generation based on soft error correction. In Fig. 2, the overall procedure is divided into two phases: enrollment and key generation. For the enrollment phase, the raw PUF response will be fed into the ECC encoding part and the corresponding help data will be the output. These help data will be stored in the non-volatile memory (NVM) and are public in nature. When the users target to generate the key in the field, the help data will be loaded from NVM and fed into the ECC decoding part. Along with the new raw PUF response, the key will be generated as the output. This key generation scheme has two main drawbacks. Firstly, the ECC implementation usually requires significant hardware overhead. For example, if the target is to generate 128 bits key with a bit-error-rate less than $1e$ 6, the ECC typically needs 3 k-10 k PUF raw bits and the nature bit-error-rate for this raw PUF bits have to be less than 15%. Furthermore, for this case, the ECC will generate 3 k-15 k bits of help data and need to be store in the NVM [3]. The other drawback will be the weakness of the help data. It has been shown that the help data/syndrome bits are a source of leaking information [13, 20, 31]. This requires further careful design of the help data generation.

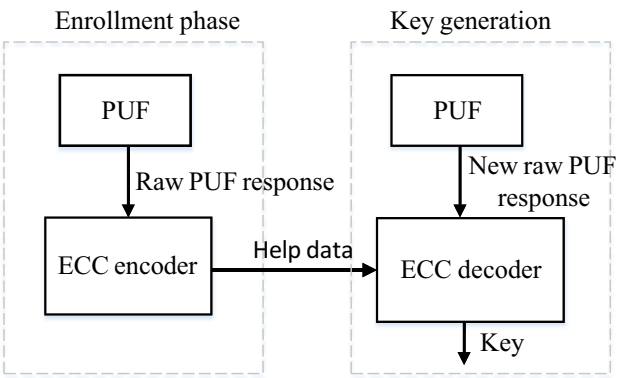


Fig. 2 Operation of SRAM PUF based key generation system

It has also been shown that the SRAM PUF cells will suffer from the reliability issue due to the aging effect in [18]. This is the first time that the authors in [2] exploit the potential benefit of the aging effect to reinforce the reliability of the SRAM PUF cells. The idea behind this is that the aging effect will increase the threshold voltage of the MOSFETs. Since the power-up state of the SRAM cells is highly dependent on the mismatch of two pairs of MOSFETs, the nature mismatch can be exaggerated by precisely choosing to apply the aging effect to specific MOSFETs. In [9], the authors show that the cells will have a bias of 1 when the cells have been aged with 0 (storing 0) and the cells will lean towards 0 bias when the cell have been aged with 1. By writing a proper value to the SRAM array and applying burn-in aging, the SRAM PUF cells can become more reliable. However, the bit-error rate cannot achieve a safe level by purely applying the burn-in aging and the ECC is still required afterwards [2, 19, 21, 25]. In [16], instead of Negative-Bias Temperature Instability (NBTI) burn-in, the author exploit the Hot Carrier Injection (HCI) burn-In to reach nearly 100% reliable SRAM PUF cells. However, to efficiently introduce controlled HCI degradation into SRAM cells, the design of the SRAM cells needs to be modified and this increases the design cost and time, and also limits occasional reuse of functional SRAMs as PUFs. The operating conditions are another core element that affects the powerup state of SRAM cells. Normally, the cells that are always power-up in a consistent state become less stable in the presence of Vdd variations, and cell stability also decreases with changes in temperature [1, 12, 14]. Some researchers have exploited this phenomenal provide to develop a different approach for identifying strong/stable SRAM cells for PUF application [1, 21, 25, 30]. However, performing tests at multiple voltages and temperatures increases the test cost and time. Our proposed bit selection method only requires one VDD/temperature condition, which will reduce the testing cost and time.

In this paper, to address the reliability problem of SRAM PUFs caused by unstable cells, the cell pre-selection method is utilised as the primary tool. The overall strategy is to run tests that select only highly stable cells as the PUF cells, ensuring high reliability. As a result, the bit-error rate (BER) of the selected cells will be extremely low along with reliability close to 100% under varied operating environments (*i.e.*, different supply voltage and temperature). Other similar approaches include [30], where the authors exploit the spatial relation between the strong cells and selects the potentially qualified cells. However, this approach is more effective against systematic variations than the random variations observed in modern processes. Moreover, the BER cannot reach a safe level, and it still requires the application of ECC following the cell selection methodology. In [22, 26], the authors introduce a tilt or bias to the SRAM cells to facilitate the selection of strong 1 and strong 0. However, to introduce the tilt, the SRAM cell needs to be modified. In [17], the authors exploit a phenomenon that the cell will flip to its preferred value after a short power-off time when an opposite value has been written previously. However, the design that is used in [17] is based on ultra-low leakage technology allowing much longer time before the flips. In more typical advanced technology with significant leakage, this method will be less practical because of the difficulty of reading all the cells within a very short time of writing. Else it becomes difficult to distinguish the intensity in the cell bias/tilt. Moreover, the ramp rate at power-on and power-off impact bit flipping, and this has not been considered. In [24], the author exploits the Maximum Trip Supply Voltage (MTSV) method to identify the strongest SRAM cells for PUF application. Compared with work in [24], we systematically analyze how the ramp rate (power-up time) affect the powerup value of SRAM cells and how to exploit different ramp rate to facilitate us selecting those most strong SRAM cells for PUF application.

3 Ramp Rate Impact on Reliability of SRAM PUF

In this section, we discuss the effect of the V_{DD} ramp rate on the power-up value of SRAM cells in a systematic way and develop a model to analyze this phenomenon. We then present a short discussion that includes how the ramp rate effect the reliability of SRAM PUF cells.

In theory, the power supply to an SRAM can be turned ON very quickly, for example raising the high voltage power rail from VSS (ground) to V_{DD} in nanoseconds or less. It can also be raised very slowly, over several seconds. Observe that here fast and slow time ramp rates must be defined relative to the charging/discharging time constants of the internal capacitances at the circuit nodes of the SRAM. These can range from hundreds of picoseconds (ps) to hundreds of milliseconds (ms) depending on whether the nodes are being charged/discharged by actively conducting transistors or by extremely small leakage currents. In practice, while there are generally no lower limits on allowable slow power supply ramp rates, a quick power supply ramp can be limited by the drive strength needed to charge the large power rail capacitances internal to the IC. This is typically design dependent, particularly if the SRAM power supply has to be switched on-chip, as would be the case if the SRAM PUF is to be read while the system-on-chip (SoC) containing the PUF is in the operating condition. Earlier work [6, 29], has discussed the ramp rate effect on the power-up state of SRAM cell in an informal way. In this paper, we analyze the ramp rate effect more systematically.

Figure 3a shows a typical 6 transistors SRAM cell. During the normal power-up, the word line will not be activated and the pass transistors M_5 and M_6 are typically off. Figure 3b is the simplified model for the power-up state of the SRAM cells. C_1 and C_2 are the diffusion capacitors from pass transistors and line respectively. The pass transistors can be ignored since they are generally off. When the SRAM cell is powered up under extremely quick ramp, the PMOS transistors M_1 and M_2 turn completely ON nearly instantly since their V_{gs} exceeds $|v_{th}|$ because V_1 and V_2 remain at their initial voltage 0 V. This is because the potential at V_1 and V_2 cannot change instantaneously

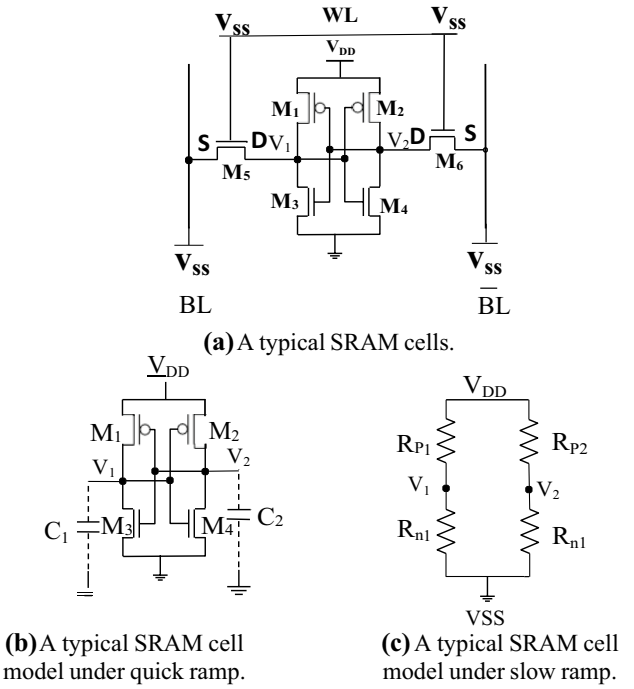


Fig. 3 SRAM power up analysis model under different ramp

at power up due to the need for capacitances C_1 and C_2 to acquire charge. Furthermore, the M_3 and M_4 are OFF during the early phase of power up due to the same reason. Consequently, the currents that flow into the $C1$ and C_2 to build up the potential at V_1 and V_2 are mainly dependent on the strength of M_1 and M_2; the effect of two NMOS M_3 and M_4 can be ignored. On the other hand, when the SRAM cell is powered up under an extremely slow ramp, at each point in time, the supply voltage V_{DD} can be nearly regarded as a DC voltage with the circuit in equilibrium, since any change in V_{DD} overt time is quite small. The capacitors C_1 and C_2 will almost be in the quasi-equilibrium state and will not influence the powerup state. Under this extremely slow ramp, the two MOSFET pairs can be assumed as an equivalent to channel resistors for simplified analysis. Figure 3c indicate corresponding analysis model for extremely slow ramp. The R_{P1}, R_{P2}, R_{n1}, and R_{n2} represent the channel resistors for the four MOS- FETS. Under this analysis model, the V_1 and V_2 will be decided by the value of the four resistors because of the voltage divider structure. In other words, either V_1 will be larger than V_2 or V_2 will be larger than V_1 that would be decided by the strength of the four MOSFETs. During the positive feedback in the SRAM cells, either V_1 or V_2 will be logical 1 in a short time in the final state. Note in this model, the effect of the capacitor has been removed. To simply sum up, if powering the SRAM cell under an extremely quick ramp, the effect of two NMOS (M_3 and M_4) can be ignored. If powering the SRAM cell under an extremely slow ramp, the effect of the capacitance can be ignored. If powering the SRAM cell under middle range ramp, the strength of the four MOSFETs as well as the value of the two capacitors, combined together, decide the final power-up state of the SRAM cell (either V_1 or V_2 will be logical 1).

To further verify the impact of ramp rate on the power-up state of the SRAM cell, two specific simulation cases have been investigated through the HSPICE. Figure 4 indicate the parameter of corresponding simulation. Case 1, introduces the difference between the four MOSFETs (M_1, M_2, M_3, and M_4) and the value identified in Fig. 4 that represents the threshold voltage of the MOSFETs. Note that M_1 is stronger than M_2 and M_3 is stronger than M_4 in this case. Here the cell have been powered up under quick and slow ramp. The quick power up time is 7 ns and slow one is 10 s. If these cells have been powered up by a quick ramp, the effect of M_3 and M_4 will be removed. The V_1 will be logical 1 after powering up since M_1 is stronger than M_2 and more current will flow into C_1 to built the potential of V_1. Figure 5a shows the corresponding HPSICE simulation result and the blue curve (V_1) follow the V_{DD} and finally increase to logical 1. This validates our previous analysis. If the cell in case 1 has been powered up under a slow ramp, all four MOSFETs will be considered to decide the final value. Since the V_{th} difference between M_3 and M_4 is larger than the difference between M_1 and M_2, the V_1 will finally be logical 0. HSPICE simulation also validate this result (see Fig. 5b). Similarly, for the SRAM cell of Case 2, we only introduce the difference between two NMOS and capacitors respectively. Under the quick ramp, since the NMOS effect will be removed and C_1 is less than C_2, the V_1 will finally become logical 1. Under the slow ramp, since the capacitor effect on power-up state has been removed and M_3 is stronger than the M_4, the V_1 will be logical 0. The HSPICE simulation result also validate the analysis (see Fig. 5c and d).

Based on the previous analysis and the simulations in this section, we can conclude that some SRAM cells may have inconsistent power-up values under different ramp rates depending on the circuit parameters of the cell itself. These cells that display inconsistent values under different ramp-up rates may be the potential'unstable' cells for SRAM PUF applications. This is because both cells of case 1 and case 2 have conflicted inner bias either from the NMOS and

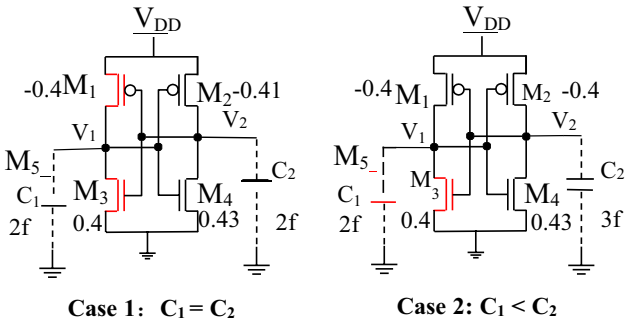


Fig. 4 SRAM power up analysis model under different ramp

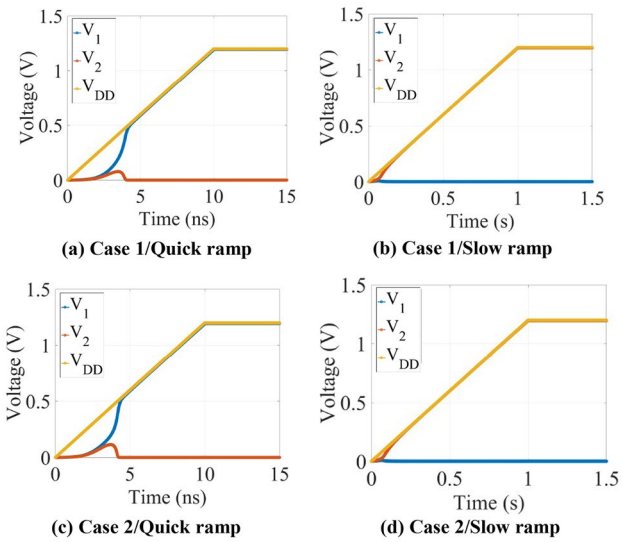


Fig. 5 SRAM power up analysis model under different ramp

PMOS or from the NMOS and capacitors. We will exploit this phenomenon to facilitate the selection of the strong cell for PUF application.

4 Data Retention Voltage for Strong Cell Selection

The traditional data retention test for memories is designed to identify the most unstable SRAM cell that will cause faulty behavior during reading and writing operation [27]. The test is performed by writing all '1' to the cell and then lowering the SRAM supply voltage to a critical level ($V_{DD,Min}$). The entire SRAM array is held at this lower power level for a while, following which, V_{DD} is raised back up to its nominal value. A read operation is then performed for the entire array to identify the potential unstable or faulty SRAM cells that flip their values to '0' during this lower voltage power supply excursion. If not containing a stuck-at fault, these cells are inherently strongly biased towards the logic 0 state The same procedure can be repeated by writing '0' to SRAM array initially to identify cells with a strong 1 bias.

This same data retention test can be exploited for identifying the most strongly biased stable SRAM cells that power up to either a 0 or 1 state. Recalling the definition of skewed cells In Sect. 2, these asymmetric cell will also be the most reliable candidates for PUF application. Figure 6a show the selection of strong '0' process. Initially, the entire SRAM array has been written with 1 and then V_{DD} has been reduced to a critical level. After that, the V_{DD} is powered back to the nominal value again and the entire SRAM read out. The bitmap in Fig. 6a shows the bit values after the final read operation. Here the white dots represent the flipped bits and are the potential strong 0 cells for PUF candidates. Similarly Fig. 6b shows the process of selecting strong '1'. The black dots represent the candidates cell for strong '1'.

Table 1 shows the simulation results and indicate the efficiency of selecting strong cell for PUF application based on the data retention test. In the simulation, 500 SRAM cells have been created and have a consistent bias from both the NMOS and PMOS transistors. The V_{th} for each transistor is randomly drawn from a normal distribution with standard deviation sigma of 20mv. From the 32 nm technology files, the NMOS nominal V_{th} is 0.42252 V and the PMOS nominal V_{th} is -0.41174 V. All cells are firts written with all 0 (1), powered down to V_{DD} minimum for several seconds and then powered back up to nominal value again. The cells that observed to have flipped their initial value are selected as

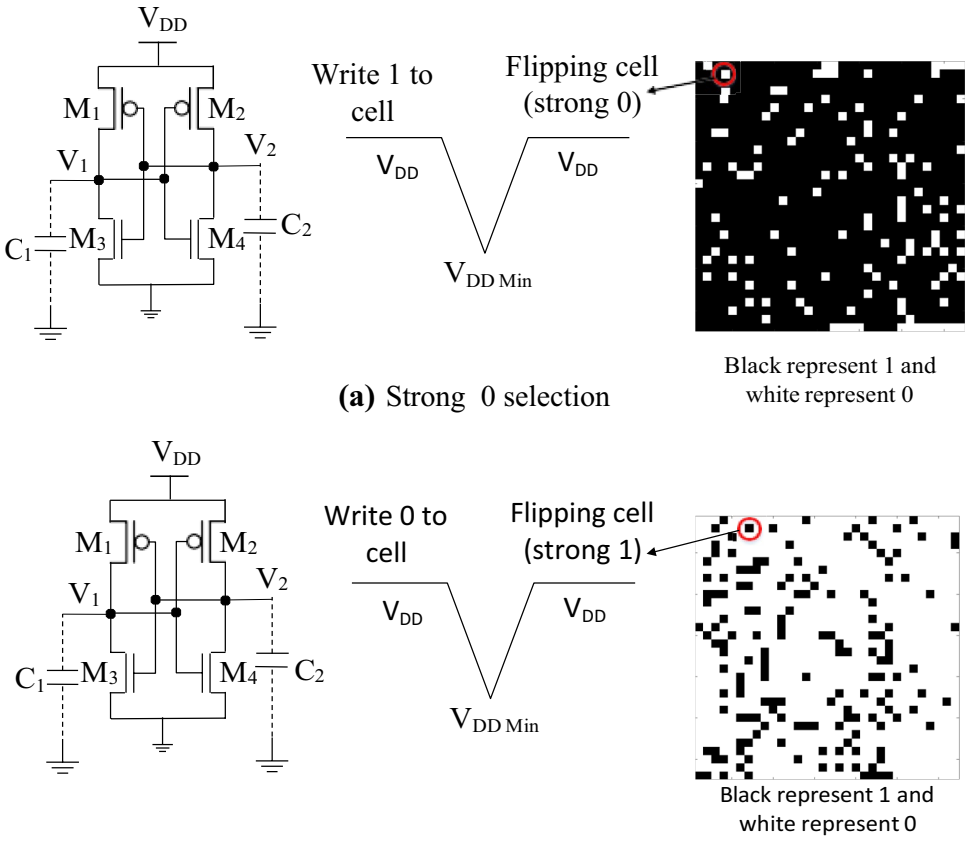


Fig. 6 Selection of strong cells based on data retention voltage

Table 1 Simulation Results for Strong Cell Calibration and Selection

VDD,Min	Avg $\Delta NMOS$	Avg $\Delta PMOS$	Δ NMOS + $\Delta PMOS$	No of selected cells
0.14	0.044	0.042	0.086	356
0.15	0.048	0.046	0.094	253
0.16	0.051	0.049	0.101	198
0.17	0.054	0.055	0.109	139
0.18	0.059	0.060	0.120	93
0.19	0.066	0.068	0.135	51
0.2	0.066	0.075	0.141	34
0.21	0.074	0.083	0.157	17
0.22	0.079	0.083	0.163	7

the strong cells. In Table 1, the first column shows the V_{DD} minimum value and the last column represents the number of cell have flipped their initial value. The fourth column presents the sum of biases V_{th} from the NMOS pair and PMOS pair. Observe from Table 1, that as the V_{DD} minimum value increases, the selected cell will be more biased because of the larger value of $\Delta NMOS + \Delta PMOS$. This simulation result shows that the data retention $V_{DD,Min}$ voltage can allow us to calibrate the strength of the selected cells for PUF applications.

5 Systematic Selection Method for Reliable SRAM PUFs

Our challenge is how to reliably select those reliable SRAM cell for PUF application. In this section, a systematic selection method for reliable SRAM PUF cells is proposed.

Recalling the discussion In Sect. 3, the power-up state of some SRAM cells may have different power-up values under quick and slow V_{DD} ramp rates because of opposing inherent bias in the PMOS and NMOS transistors. Thus cells display conflicting power-up bias from the individual contributions of capacitive and MOSFETs imbalances. Recall the case 1 and 2 examples In Sect. 3. These cells are potentially unreliable cells for PUF application. In strong cells both the PMOS and NMOS transistors should display the same directional bias. Furthermore, In Sect. 4, we proposed exploiting data retention voltage to calibrate the strength of this bias in the SRAM cells. By combining these two properties, a systematic selection strategy can be developed for targeting virtually 100% reliable cells for PUF application.

Figure 6 shows our procedure of selecting reliable cells. A two-level selection process has been created. In the first level, individually, quick and slow V_{DD} power on ramp rates will be applied to the SRAM array. Then the bitmaps of the SRAM array under these two power up ramp rates are collected. Next, a combined bitmap is created indicating where the two bitmaps agree, i.e. by the XNOR the bitmaps of the quick ramp and slow ramp. All the black bits in this bitmap represent potential reliable bits for our application. Data retention tests, which comprise the second-level in this test procedure, are next performed to calibrate the strength of the potentially reliable bits identified by the first level testing. In Fig. 6, the bitmaps 3 and 4 represent the corresponding bitmap after performing the data retention test by writing all 1 and all 0. The white dots represent potential strong 0 cells in bitmap 3 and black dots represent potential strong 1 in bitmap 4. In the bitmap 6 is the final bitmap pool for all potential reliable cells for PUF application (black dots in bitmap 6). The bitmap 6 is generated by checking whether black dots in bitmap 3 is still black in bitmap 5 and whether white dots in bitmap 4 is still black in bitmap 5. If the dots in bitmap 3 and 4 fulfill the condition, black dots will be placed in the same location in bitmap 6 and this represents this cell is a reliable cell for PUF application and the rest of the location will be put white dots.

Following manufacturing, we propose the application of the two level test to select candidate stable cells and develop the dark-bit mask. The specific PUF register size, for example 128 bits or 256 bits, can be chosen from the dark-bit mask based on the application requirement. To maximize PUF response stability, the dark bits can be further rank ordered based on the $V_{DD,Min}$ voltage of the second level test to allow selection of the most stable bits for use in the PUF. The address information of selected cells can be stored in nonvolatile memory, for use in efficiently generating the PUF response.

6 Silicon Results

In this section, we present and discuss silicon results for the power-up stability and reliability of SRAM cells that have been selected based our proposed method. We have conducted experiments using commercial off-the-shelf (COTS) SRAM memories to demonstrate the effectiveness of our proposed approach. The chips are Microchip and 23K640I/SN SPI Bus Low-Power Serial SRAM memories. The total memory capacities of both SRAM chips are 64 K bits. The power-up time of SRAM has been controlled by a function generator (TeKtronix AFG3952C) and this function generator can allow us to vary the power-up time from 7 ns to 100 s.Due to the limitation of the power rail within the chip (with its large RC constant), the real internal power-up time at individual cells may be somewhat reduced in practice. However, in this silicon experiment, we set the power up time with 7 ns as our quick ramp by exploiting the function generator and this is the quickest ramp that we can generate in the lab.

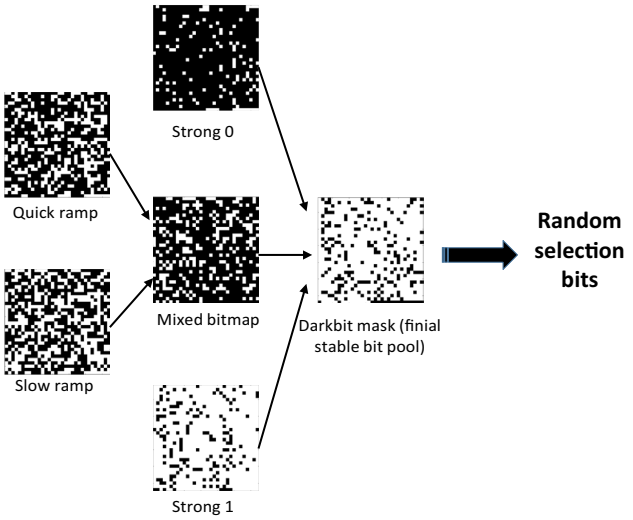


Fig. 7 A systematic selection method toward reliable SRAM PUF

In first test, the SRAMs are powered up under extreme quick and slow ramps and corresponding bit-maps generated (see Fig. 7). The second level test is the data retention test. In this test, we exploit a DC source to provide the power for SRAM chip reading since no precise power up time require to be controlled in this test. The measured power-up time for this experiment is approximately a millisecond level. In the real world, the different chips may experience somewhat different ramps depend on the power rail loading. Here, different $V_{DD,Min}$ are employed for data retention testing to select and rank order the strongest cells in the array. The results from the two test levels are combined as describe above. In this way, the selected cells can achieve very high reliability.

Figure 8 presents the different data retention voltage $V_{DD,Min}$ versus % of 1 s observed after powering up back to nominal V_{DD} voltage. The x axis represents the $V_{DD,Min}$ which is the minimal voltage in the data retention test (see Sect. 4). From the plot, it can be observed that the number of cells that flip from the initial written value become fewer as the $V_{DD,Min}$ is raised. Thus the silicon experiments validate our results from simulation in Table 1.

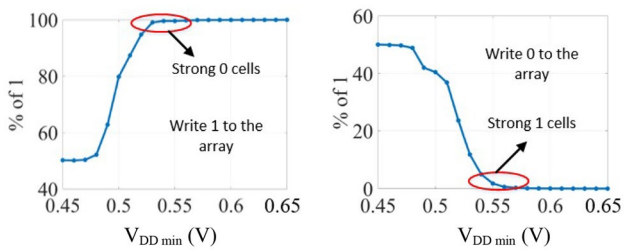


Fig. 8 Percentage (%) of 1 s in 64 K SRAM array during data retention tests

In the next experiment, these cells will be powered up under different temperature and voltage to evaluate their reliability in different environmental conditions.

Groups of SRAM cells selected using the stability testing approach described earlier (for different V_{DD} minimum) were tested for consistency of their power-up states under different temperature (25 °C 50 °C 85 °C). Three chips were heated using a ThermoSpot direct contact probe system (see experimental setup for accelerated aging in Fig. 9). This system is an industry standard benchtop temperature cycling system, used for testing circuits over a wide range of temperatures. Table 2 presents the results of the reliability test for three different temperature for the three chips. The chips were powered up 1000 times at each temperature and the power-up value read out and recorded. To evaluate the reliability of the selected cells, the percentage (%) of unstable cells is calculated. This is defined as follows: number of unstable cells divided by number of selected cells. The number of unstable cells are those that show an inconsistent powerup value anytime during the 1000 read-outs. Table 2 verifies in silicon that, as expected, cells that have been selected using larger $V_{DD,Min}$ show better reliability because the percentage (%) of unstable cells decrease as $V_{DD,Min}$ increases. Note that if the $V_{DD,Min}$ of 0.58 V (or higher) is employed during the data retention test, all the selected cells are stable for 1000 power up cycles, and their use in a PUF will ensure very high reliability. Observe also, from comparing data for 85 °C and the data for 50 °C, the percentage (%) of unstable cells at 85 °C is larger than that at 50 °C. This is because it is well known that higher temperature causes higher cell instability [28].

Groups of strong cells were similarly also selected to evaluate their stability for different supply voltage level (2.7 V 3.3 V 3.6 V). Table 3 shows the corresponding test results. All chips were again powered up 1000 times to test stability at the different operating voltages. The percentage (%) of unstable cells is again calculated for different groups of selected cells. In Table 3, also observe that the

Fig. 9 Testing the SRAM at different temperatures with ThermoSpot direct contact probe system

Table 2 Evaluation of reliability of selected cells under temperature variation

$V_{DD,Min}$	Chip1			Chip2			Chip3		
	80 °C	50 °C	25 °C	80 °C	50 °C	25 °C	80 °C	50 °C	25 °C
	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells
0.53	5.01	4.40	4.30	5.71	5.45	5.43	5.13	4.36	4.31
0.54	2.91	2.71	2.71	4.81	4.33	4.33	3.21	3.17	3.12
0.55	1.29	1.28	1.28	4.32	4.08	4.01	1.60	1.58	1.55
0.56	0.46	0.46	0.46	0.95	0.88	0.88	0.61	0.60	0.58
0.57	0.12	0.12	0.12	0.13	0.13	0.13	0.15	0.15	0.15
0.58	0	0	0	0	0	0	0	0	0

Table 3 Evaluation of reliability of selected cells under voltage variation

$V_{DD,Min}$	Chip1			Chip2			Chip3		
	3.6 V	3.3 V	2.7 V	3.6 V	3.3 V	2.7 V	3.6 V	3.3 V	2.7 V
	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells	% of unstable cells
0.53	4.18	4.30	4.07	5.47	5.43	5.41	4.50	4.31	4.37
0.54	2.65	2.71	2.60	4.33	4.33	4.33	3.01	3.12	3.15
0.55	1.20	1.28	1.16	4.01	4.01	4.01	1.68	1.55	1.57
0.56	0.466	0.46	0.46	0.88	0.88	0.883	0.56	0.58	0.59
0.57	0.12	0.12	0.12	0.13	0.13	0.135	0.17	0.15	0.18
0.58	0	0	0	0	0	0	0	0	0

percentage (%) of unstable cells reduces as V_{DD} minimum keep increase. If the V_{DD} minimum is 0.58 V, the corresponding group of selected cells is 100% reliable.

Finally, the experiment was also repeated to study the impact of aging on the stability of the selected strong cells. Here we applied controlled random aging to the SRAM chips to mimic normal operation in the field. Random patterns were written into the SRAM, with the ratio of 40% 1 s and 60% 0 s. These random patterns are modified and updated periodically. After 2 weeks of this controlled random aging, the start-up value of each SRAM chip was read out 1000 times to check the reliability of the selected cells. Table 4 shows the percentage (%) of unstable cells for selected cells after controlled random aging. The result again indicates the of unstable cells have been decreases as the $V_{DD,Min}$ increases. If the V_{DD} minimum is 0.58 V, the selected groups of cells is 100% stable and reliable.

Based on the reliability expriments presented for varying voltages, temperatures and aging, it has been shown that by selecting an appropriate $V_{DD,Min}$ voltage for stable cell strength selection, it is always possible to ensure desired reliability of an SRAM PUF. The trade-off is that while using a higher $V_{DD,Min}$ during cell selection yields more stable and reliable cells, there are fewer such cells in any given size of an SRAM array. This limits the reliability of the PUF (with a given number of bits) that can be realized from any size of SRAM array.

Table 4 Evaluation of reliability of selected cells under aging

$V_{DD,Min}$	Chip1	Chip2	Chip3
	% of unstable cells	% of unstable cells	% of unstable cells
0.53	4.45	5.75	4.58
0.54	2.73	4.43	3.15
0.55	1.31	4.16	1.58
0.56	0.46	0.88	0.61
0.57	0.12	0.13	0.15
0.58	0	0	0

7 Conclusion

While SRAM arrays are particularly attractive for use as PUFs, errors in the PUF response due to instability caused by voltage, temperature, environmental noise, and degradation due to aging is a challenge. In this paper we show for the first time that power-up states are also influenced by the power supply ramp rate at power-up, which can be yet another source of cell instability. To address the general problem of instability in SRAM power-up states that can result in inconsistent responses from SRAM PUFs, we present an effective stable cell selection method to identify the cells in the SRAM that are strongly biased, and thereby resistant to circuit noise, voltage and temperature changes, and also aging. The data from the Silicon experiments presented here shows that the selected subsets of SRAM cells are highly reliable over temperature and voltage variations, with a bit error rate that can be brought down (BER) close to zero.

Funding This paper is based in part upon research supported by the National Science Foundation under Grant No. CCF 1910964.

Data Availability The authors declare that the data supporting the fndings of this study are available within the article.

Declarations

Conflict of Interest/Competing Interest The authors have no conficts of interest to declare that are relevant to the content of this article.

References

1. Baturone I, Prada-Delgado MA, Eiroa S (2015) Improved generation of identifiers, secret keys, and random numbers from SRAMs. IEEE Trans Inf Forensics Secur 10(12):2653–2668
2. Bhargava M, Cakir C, Mai K (2012) Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS. Proc. IEEE International Symposium on Hardware-Oriented Security and Trust. IEEE, pp 25–30
3. Bhargava M, Mai K (2014) An efficient reliable PUF-based cryptographic key generator in 65nm CMOS. Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, pp 1–6
4. Böhm C, Hofer M (2012) Physical unclonable functions in theory and practice. Springer Science & Business Media, US
5. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Proc. International conference on the theory and applications of cryptographic techniques. Springer, pp 523–540
6. Elshafiey AT, Zarkesh-Ha P, Trujillo J (2017) The effect of power supply ramp time on SRAM PUFs. Proc. IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). IEEE, pp 946–949
7. Guajardo J, Kumar SS, Schrijen G-J, Tuyls P (2007) FPGA intrinsic PUFs and their use for IP protection. Proc. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, pp 63–80
8. Guajardo J, Kumar SS, Schrijen G-J, Tuyls P (2007) Physical unclonable functions and public-key crypto for FPGA IP protection. Proc. International Conference on Field Programmable Logic and Applications. IEEE, pp 189–195
9. Guin U, Wang W, Harper C, Singh AD (2019) Detecting recycled SOCs by exploiting aging induced biases in memory cells. Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, pp 72–80
10. Herder C, Yu M-D, Koushanfar F, Devadas S (2014) Physical unclonable functions and applications: A tutorial. Proc IEEE 102(8):1126–1141
11. Holcomb DE, Burleson WP, Fu K (2008) Power-up SRAM state as an identifying fingerprint and source of true random numbers. IEEE Trans Comput 58(9):1198–1210
12. Kim J, Lee J, J Abraham A (2010) Toward reliable SRAM-based device identification. Proc. IEEE International Conference on Computer Design. IEEE, pp 313–320
13. Kusters L, Ignatenko T, Willems FM, Maes R, van der Sluis E, Selimis G (2017) Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios. Proc. IEEE International Symposium on Information Theory (ISIT). IEEE, pp 1803–1807
14. Leest VVD, Sluis EVD, Schrijen G-J, Tuyls P, Handschuh H (2012) Efficient implementation of true random number generator based on SRAM PUFs. Cryptography and Security: from theory to applications. Springer, pp 300–318
15. Li Y, Hwang C-H, Li T-Y, Han M-H (2009) Process-variation effect, metal-gate work-function fluctuation, and random-dopant fluctuation in emerging cmos technologies. IEEE Trans Electron Device 57(2):437–447
16. Liu K, Chen X, Pu H, Shinohara H (2020) A 0.5-v hybrid SRAM physically unclonable function using hot carrier injection burn-in for stability reinforcement. IEEE J Solid State Circuits
17. Liu M, Zhou C, Tang Q, Parhi KK, Kim CH (2017) A data remanence based approach to generate 100% stable keys from an SRAM physical unclonable function. Proc. IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED). IEEE, pp 1–6
18. Maes R, Rozic V, Verbauwhede I, Koeberl P, Van der Sluis E, van der Leest V (2012) Experimental evaluation of physically unclonable functions in 65 nm CMOS. Proceedings of the ESSCIRC (ESSCIRC). IEEE, pp 486–489
19. Maes R, Van Der Leest V (2014) Countering the effects of silicon aging on SRAM PUFs. Proc. IEEE International symposium on hardware-oriented security and trust (HOST). IEEE, pp 148–153
20. Maes R, Van Herrewege A, Verbauwhede I (2012) PUFKY: A fully functional PUF-based cryptographic key generator. Proc. International Workshop on Cryptographic Hardware and Embedded Systems. Springer, pp 302–319
21. Mathew SK, Satpathy SK, Anders MA, Kaul H, Hsu SK, Agarwal A, Chen GK, Parker RJ, Krishnamurthy RK, De V (2014) 16.2 a 0.19 pj/b pvt-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS. Proc. IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC). IEEE, pp 278–279
22. Miller A, Shifman Y, Weizman Y, Keren O, Shor J (2019) A highly reliable SRAM PUF with a capacitive preselection mechanism and pre-ECC BER of 7.4 e-10. Proc. IEEE Custom Integrated Circuits Conference (CICC). IEEE, pp 1–4
23. Rahman MT, Forte D, Rahman F, Tehranipoor M (2015) A pair selection algorithm for robust ro-RO-PUF against environmental variations and aging. Proc. 33rd IEEE International Conference on Computer Design (ICCD). IEEE, pp 415–418
24. Saraza-Canflanca P, Carrasco-Lopez H, Santana-Andreo A, Brox P, Castro-Lopez R, Roca E, Fernandez FV (2021) Improving the reliability of SRAM-based PUFs under varying operation conditions and aging degradation. Microelectron Reliab 118:114049

25. Satpathy S, Mathew SK, Suresh V, Anders MA, Kaul H, Agarwal A, Hsu SK, Chen G, Krishnamurthy RK, De VK (2017) A 4-fj/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS. IEEE J Solid State Circuits 52(4):940–949
26. Shifman Y, Miller A, Keren O, Weizmann Y, Shor J (2018) A method to improve reliability in a 65-nm SRAM PUF array. IEEE Solid State Circuits Lett 1(6):138–141
27. Vatajelu EI, Di Natale G, Prinetto P (2016) Towards a highly reliable sram-based PUFs. Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, pp 273–276
28. Wang W, Guin U, Singh A (2020) Aging-resilient SRAM-based true random number generator for lightweight devices. J Electron Test 36:301–311
29. Wang W, Singh A, Guin U, Chatterjee A (2018) Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs. Proc. IEEE 19th Latin-American Test Symposium (LATS). IEEE, pp 1–6
30. Xiao K, Rahman MT, Forte D, Huang Y, Su M, Tehranipoor M (2014) Bit selection algorithm suitable for high-volume production of SRAM-PUF. Proc. IEEE international symposium on hardware-oriented security and trust (HOST). IEEE, pp 101–106
31. Yu M-D, Devadas S (2010) Secure and robust error correction for physical unclonable functions. IEEE Des Test Comput 27(1):48–65
32. Zhang J-L, Qu G, Lv Y-Q, Zhou Q (2014) A survey on silicon PUFs and recent advances in ring oscillator PUFs. J Comp Sci Technol 29(4):664–678

Wendong Wang received the M.S. degree in Electrical and Computer Engineering from Auburn University, Auburn, AL, USA in 2018. He is pursuing the Ph.D. degree from the Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA. His current areas of research includes hardware security, cryptography primitives components such as TRNG and PUF, and detecting recycled chip.

Adit Singh received the B.Tech. degree from IIT Kanpur, Kanpur, India, and the M.S. and Ph.D. degrees from Virginia Tech, Blacksburg, VA, USA, all in Electrical Engineering. He is currently Godbold Endowed Chair Professor of Electrical and Computer Engineering at Auburn University in Alabama. Earlier, he served on the faculty at the University of Massachusetts in Amherst, and Virginia Tech, in Blacksburg, and has also held visiting professorships, most recently at the University of Tokyo, Japan and the University of Freiburg, Germany. He has authored over 250 research papers and holds international patents that have been licensed to industry. He is particularly recognized for his pioneering contributions to statistical methods in test and adaptive testing. His research interests include VLSI technology, in particular integrated circuit test and reliability. Dr. Singh has had leadership roles as a General Chair/CoChair/Program Chair for dozens of international VLSI design and test conferences. He has also served on the editorial boards of several journals, including the IEEE Design and Test, and on the Steering and Program Committees of many of the major IEEE international test and design automation conferences. He served two elected terms as a Chair for the IEEE Test Technology Technical Council (2007–2011), and on the Board of Governors of the IEEE Council on Design Automation (2011–2015). He is a Life Fellow of the IEEE.

Ujjwal Guin received his PhD degree from the University of Connecticut in 2016. He received his M.S. degree from Temple University, Philadelphia, PA in 2010 and B.E. degree from Bengal Engineering and Science University, India in 2004. He is currently an Assistant Professor in the Electrical and Computer Engineering Department of Auburn University, Auburn, AL, USA. Dr. Guin has developed several on-chip structures and techniques to improve the security, trustworthiness, and reliability of integrated circuits. His current research interests include Hardware Security & Trust, Blockchain, Supply Chain Security, Cybersecurity, and VLSI Design & Test. He is a co-author of the book Counterfeit Integrated Circuits: Detection and Avoidance. He has authored several journal articles and refereed conference papers. He serves on the organizing committees VLSI Test Symposium (VTS) and IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE). He has been serving on the technical program committees in several reputed conferences, such as, DAC, HOST, VTS, PAINE, VLSID, ISVLSI and Blockchain. He is an active participant in SAE International G-19A Test Laboratory Standards Development Committee, and G-32 Cyber-Physical Systems Security Committee. He is a member of both the IEEE and ACM.