RESP: A Robust Physical Unclonable Function Retrofitted into Embedded SRAM Array

Yu Zheng, Maryam S. Hashemian and Swarup Bhunia
Case Western Reserve University, Department of EECS, Cleveland, Ohio, 44106
{yu.zheng3, mxh460, skb21}@case.edu

ABSTRACT

Physical Unclonable Functions (PUFs) have emerged as an attractive primitive to address diverse hardware security issues in Integrated Circuits (ICs). A majority of existing PUFs rely on a dedicated circuit structure for generating chip-specific signatures, which often imposes concerns due to area/power overhead and extra design efforts. Furthermore, existing PUF-based signature generation cannot be employed to authenticate chips already in the market. In this paper, we propose RESP, a novel PUF structure realized in embedded SRAM array, a prevalent component in processors and system-on-chips (SOCs), with virtually no design modification. RESP leverages on voltage-depend memory access failures (during write) to produce large volume of high-quality challenge-response pairs. Since many modern ICs integrate SRAM array of varying size with isolated power grid, RESP can be easily retrofitted into these chips. Circuit-level simulation of 1000 chips using realistic process variation model shows high uniqueness of 49.2% average inter-die Hamming distance and good reproducibility of 2.88% intra-die Hamming distance under temperature $< 85°$C. The device aging effect, e.g. bias temperature instability (BTI), results in only 4.95% estimated unstable bits for ten-year usage.

Categories and Subject Descriptors

K.6.5 [**Security and Protection**]: Authentication

General Terms

Design, Security

Keywords

Hardware security, PUF, SRAM, Signature, BTI

1. INTRODUCTION

In recent years, Physical Unclonable Functions (PUFs) have been widely investigated as a security primitive of integrated circuits (ICs) in variety of applications such as Intellectual Property (IP) counter-plagiarism, chip authentication and embedded system security. PUFs have obvious advantages over traditional digital-key storage in a non-volatile memory (NVM). First, PUFs avoid the high cost of building tamper-resistant NVM system, since any invasive attack may alter internal behavior of an IC leading to incorrect signatures [1]. Moreover, a PUF can produce a large amount of challenge-response pairs that are random and usually difficult to predict, which overcome the limitation of insufficient number (usually only one) of digital-key storage.

PUFs transform the inherent random variations in a manufacturing process (e.g. threshold voltage (V_{th}), channel length (L)) to variations in circuit-level parameters for random digital-key generation. A majority of existing PUFs require dedicated circuit structures [4–6]. Apart from the substantial cost in silicon area, their integration into a system-on-chip (SOC) design needs extra effort on the placement, routing and verification. On the other hand, a separate class of relatively few PUF implementations generates signature from existing on-chip structures, such as PUFs that exploit random mismatch in inner node voltages of memory elements (e.g. SRAM or Flip-Flops) [7–10]. This class of PUFs, however, often requires considerable modifications of the original design. For example, the PUF in [7] adds four extra transistors into each 6-T SRAM cell as twisted NOR gates for initializing the inner voltages, and a programmable word line duty cycle controller is inserted into the SRAM array in [9]. Although the PUF in [8] requires no such modification, the residual charge in the SRAM cell severely impacts the power-up randomness of signature, thus compromising the quality of signature. The intrinsic PUF uses the power-up state of flip-flops in FPGA, however, it requires altering the bit configuration procedure to retain the values and read it out [10]. Moreover, a common disadvantage of these PUFs is small challenge-response space and Shannon entropy. The SRAM cells only generate a signature with the entropy of 1 bit/cell in the best case.

In this paper, we propose *RESP*, **R**etrofitted **E**mbedded **S**RAM **P**UF. Unlike existing PUF structures, which implement a PUF either through insertion of a dedicated PUF IP in a design [4–6] or through design modifications of on-chip structures [7–10], RESP utilizes voltage scaling induced access failures in SRAM array to generate large set of robust signatures. It leverages on the fact that modern ICs usually adopt separate power delivery network (PDN) for the functional blocks and embedded memory [13]. Signature generation in RESP can be accomplished for practically any IC in the market or large volume of legacy ICs with pins to externally control the supply voltage of embedded SRAM. Furthermore, the idea of RESP can be applied during any chip design process by creating separate voltage (VDD) island for SRAM in a die to integrate PUF into SRAM array.

RESP exploits the fact that for a set of SRAM cells in an array, under scaled supply voltage, write access failure occurs only in specific cells in the set depending on device-level process variations. After an initial value is written to this set at the scaled supply, the content in the SRAM cells can be read out to create a random signature for a chip. Fig. 1 illustrates this approach for a typical two-dimensional SRAM array. We first initialize the cells C1,

DAC'13, May 29 - June 07 2013, Austin, TX, USA.

C2 and C3 as ‘1’ to all the chips. Then write an initial value, say all ‘0’ into them under reduced VDD. Next, we read out the values at nominal voltage to generate chip-specific random signatures. Large choice of initial values and voltage levels enables generation of large volume of random signatures from a chip.

We have presented detailed description of the signature generation process. To improve the robustness of signature with temporal variations (e.g. temperature, aging effect), we propose an iterative procedure that satisfies a preset write failure probability by adjusting VDD. We have studied the effectiveness of RESP with extensive simulation using realistic process variation model (for 45nm process) with 15% inter- and 10% intra-die standard deviations on V_{th}. The variations on L and other device parameters are represented as additional contribution to V_{th} variation [14]. We observe that RESP can achieve high uniqueness (49.2% average inter-die Hamming distance) and reproducibility (2.88% unstable bits below 85 °C). We also show that the entropy can be up to 6 bits/cell. The aging-induced V_{th} increase of 17 mV in PMOS due to negative bias temperature instability (NBTI) effect with ten-year usage results in only 4.95% flipped bits. Furthermore, we show that multiple measures can enhance the robustness of signature under simultaneous switching noise (SSN) of VDD.

The remainder of the paper is organized as follows. Section 3 presents the basic structure of an SRAM array and its failure modes. Section 4 introduces the RESP methodology. Simulation results on uniqueness, robustness and aging effect are shown in Section 5. Section 6 analyzes the signature stability under VDD variations. The discussions are in Section 7. Section 8 concludes and provides future directions.

2. RELATED WORK ON PUF

A majority of PUFs rely on dedicated circuit structures. Optical PUF depends on laser speckle fluctuation of coherent radiation to disordered media [2]. In the coating PUF, a sensor array on the top metal layer measures the unit capacitance of coating of random dielectric particles for signature [3]. However, both of them resort to the special material or equipment. To produce signature, the delay-based PUFs compare the delay values of two similar components under process variations [4] [5]. The butterfly PUF employs two cross-coupled latches to construct a cell [6]. Besides the spatial correlation among components that compromises entropy, the dedicated circuits incur large area overhead.

Another class of PUFs consider on-chip resources to reduce area overhead. In [11], the standard FLASH interface measures the distribution of transistor threshold voltage as signature of each FLASH chip. The intrinsic PUF collects the random power-up content of flip-flops as signature in FPGA by modifying the configuration procedure [10]. The symmetric structure of SRAM cell become unbalanced under process variations that enables generating random content [7] [8]. The PUF in [7] adds another four transistors into each 6T SRAM cell. In [8], the entropy of each cell may be greatly reduced due to residual charge in the cross-coupled inverters. *MECCA* PUF incorporates the word-line duration into the challenge that induces write failure in SRAM [9]. *ScanPUF* obtains the signature by exploiting variations in scan path delay [12]. These PUFs, however, do not completely eliminate design modifications and/or compromise quality of signature.

3. BACKGROUND AND PRELIMINARIES

3.1 SRAM Array Structure for RESP

The SRAM organization in Fig. 1 is considered for the proposed PUF due to its wide-spread use as embedded memory. It is comprised of a 2-D cell array and the peripheral components. The cell array is the aggregation of 6-T cells as shown in Fig. 2, while the periphery includes row/column decoder, bitline conditioning and column circuitry.

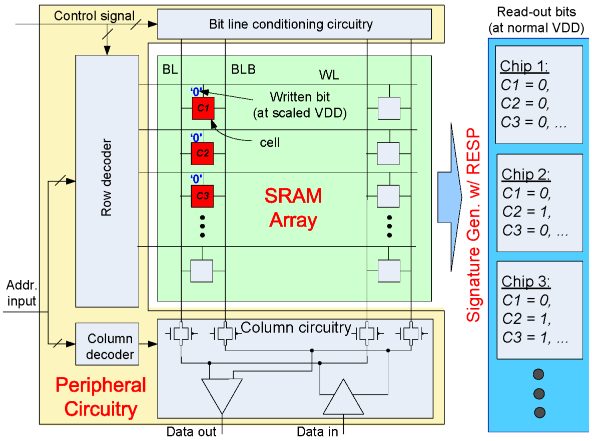


Figure 1: Conventional SRAM architecture.

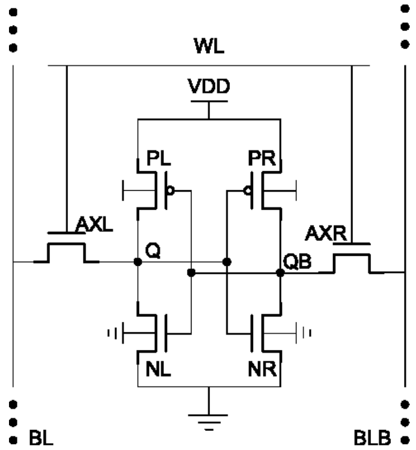


Figure 2: Structure of a typical 6-T SRAM cell [14].

The read and write of SRAM are divided into the precharge and evaluation phase. In the pre-charge phase, BL and BLB in Fig. 2 are both charged to high level (‘1’) and will be floating high at the beginning of evaluation phase. Then the word line (WL) is raised to move the transistor AXL and AXR to ‘ON’ state, connecting BL (or BLB) to node Q (or QB). For reading ‘1’ (Q=‘1’ and QB=‘0’), since NR is stronger than AXR and QB remains below the trip point of inverter PL-NL (readability), BLB is pulled down to a lower voltage (e.g. 0.1VDD) which is sensed by the sense amplifier. During writing ‘0’ into a cell storing ‘1’, since PL is weaker than AXL (writability), Q is pulled lower than the trip point of inverter PR-NR.

The peripheral and cell array either share the same VDD or have distinct ones to improve writability or standby power [15] [16]. In the proposed approach, we consider single power supply, since the double power supply is equivalent to making the two voltages equal.

3.2 SRAM Failure Modes

Under process variations, an SRAM array experiences the following four types of parametric failures [14].

1. Read Failure: It occurs if the data stored in SRAM cells flip during read. For a cell storing ‘1’, it flips if the voltage on QB rises to a value higher than the trip point of the inverter PL-NL.

2. Write Failure: It occurs if a cell cannot be flipped while writing a different value due to insufficient WL duration or weak writability.

3. Access Failure: If the voltage difference between BL and BLB at the time of sense amplifier firing is lower than the required offset voltage, it leads to incorrect sensing of stored content.

4. Hold Failure: The destruction of cell content at a lower VDD is known as hold-stability failure. For a cell storing '1', higher trip point of PR-NR makes it easier to flip thus requiring higher retention voltage.

3.3 Choice of Failure Mode

Appendix B shows the write and access failures are more sensitive to VDD scaling. The six transistors in each SRAM cell can determine the occurrence of write failure, while the access failure additionally relies on sense amplifier that influences the probability of sensing '0' (or '1') for a column. For example, if the sense amplifier is 'strong' under process variation, it can correctly sense small voltage difference between BL and BLB. Hence, the bits in the column are highly likely to be read out correctly providing little or no random information. Hence, we focus on write failure in RESP, although the approach can be extended to other mode of failures.

3.4 Retrofitting PUF into SRAM

Definition 1: A PUF is *retrofitted* into a hardware component, if the component is treated as a black box and no modification (e.g. structure, in/out ports) is incorporated into it. The extra hardware resources outside the component used to support retrofitting a PUF are referred to as retrofitting overhead.

Under nominal voltage and temperature, the failure rate of SRAM cells is expected to be rather low (e.g. typically less than 10^{-8} [14]) with little random information. In RESP, we deliberately reduce the VDD to induce failures during memory access for write. It allows us to retrofit a PUF into memory. Moreover, unlike most PUFs integrated into SOC die as a separate circuit, RESP facilitates obtaining responses to challenge vectors by using existing on-chip resources for memory read/write operations.

Next, we discuss the impact of VDD scaling on peripheral circuits as in Fig. 1 that provides the control signals (e.g. WL) for synchronous and asynchronous SRAM. RESP may not be effective in asynchronous SRAM due to timing errors (e.g. WL rising up in the evaluation phase) caused by the large and unbalanced skewing of control signals at scaled VDD. For synchronous SRAMs, the clock period and duty cycle influence the pre-charge and evaluation phase. However, for synchronous SRAM, when path delay increases beyond clock period due to VDD scaling, timing violation may occur for some cells during write (Appendix A).

3.5 Voltage Scaling Mechanism in RESP

RESP can be realized through off-chip or on-chip control of memory voltage. If a manufactured chip reserves a separate pin for the VDD of embedded SRAM, we can control the supply voltage of SRAM outside the chip using a supply tuning block, which incurs no on-chip design modification. In this case, we need test equipment for external control of supply voltage. It would make signature generation using RESP possible for many legacy chips with separate PDN and dedicated supply pin for the embedded memory. On the other hand, during design process of a new chip, RESP can be realized by deliberately incorporating separate supply pin and PDN for the memory as well as an on-die memory voltage tuning circuit to facilitate signature generation. Since, majority of modern SOC designers typically incorporate separate PDN for embedded memory, the design overhead for RESP is expected to be low, as discussed in Section 7.1.

4. METHODOLOGY FOR IMPLEMENTING RESP

4.1 Voltage Scaling Driven by Write-failure Prob.

Write duration T_{WR} of writing '0' (similarly writing '1'), which is the interval that node Q is discharged to the voltage of trip point V_{TRR} of PR-NR inverter, can be expressed as:

$$T_{WR} \doteq \begin{cases} \left| \int_{V_{TRR}}^{VDD} \frac{C_Q(V_Q)dV_Q}{I_{dsPL}(V_Q)-I_{dsAXL}(V_Q)} \right| & if\ \ V_{WRL} < V_{TRR} \\ \infty & otherwise \end{cases} \tag{1}$$

where C_Q is the net capacitance at Q, and V_{WRL} is the voltage on Q during write, which is determined by the strength of AXL and PL. In the CMOS processes, T_{WR} is affected by both inter-die and intra-die V_{th} variations. The inter-die V_{th} variation is shard by the transistors on the same die and varies from die to die. The intra-die V_{th} is a random shift on each transistor within a die and the standard deviation $\sigma_{th,intra}$ of a gate with L and W is modeled as [14]:

$$\sigma_{th,intra} = \sigma_{th0,intra}\sqrt{\frac{W_{min}L_{min}}{WL}} \tag{2}$$

where $\sigma_{th0,intra}$ is the standard deviation of intra-die V_{th} for a gate of minimum width W_{min} and length L_{min} in a specific CMOS process. Fig. 3(a) shows the distribution of T_{WR} in 200 chips (128 memory cells for each) following the Gaussian-distributed V_{th} variation ($\sigma_{th,inter} = 15\%$ and $\sigma_{th0,inter} = 10\%$) with $VDD = 1.00$ V. The probability density function (PDF) of T_{WR} with a long tail is modeled as a noncentral F function [14]. The write failure probability P_{WF} is

$$P_{WF}(t_{wp}) = Pr\{T_{WR} > t_{wp}\} = 1 - \Phi(t_{wp}) \tag{3}$$

where $\Phi(\cdot)$ is the cumulative density function (CDF) of T_{WF} and t_{wp} is the WL duration. We assume $t_{wp} = 0.7$ ns as the minimum WL duration in Fig. 3(a). Fig. 3(b) illustrates the samples of T_{WR} in the fast and slow chips for the scaled voltage $VDD = 0.70$ V. All the SRAM cells in those chips simultaneously experience (or avoid) write failure for $t_{wp} = 0.7$ ns, which implies no random information. Hence, the distinct inter-die V_{th} deviations lead to different P_{WF} of the chips under identical VDD. We specify the VDD around $P_{WF} = 0.5$ at temperature 25 °C without aging effect. Fig. 4(a) shows that P_{WF} increases to 0.90 on average, when the temperature rises to 85°C at the nominal VDD. In Fig. 4(b), if V_{th} of PMOS is increased by 0.20 V due to the aging effect such as NBTI, P_{WF} becomes 0.65 on average. As P_{WF} reflects the number of zeros in the signature, each chip needs its own VDD to achieve a specific P_{WF}. The choice of VDD also should consider temperature fluctuation and aging effect.

4.2 RESP Architecture and Procedure

The challenges of retrofitted PUF include the cell locations, pre-stored values ('0' or '1') and VDD tracking the process and temporal variations, implying more challenge-response pairs than other SRAM PUFs using power-up state.

Fig. 5(a) explains the architecture of RESP, including a programmable reference generator and a voltage regulator, which is similar to the VDD tuning structure in [17]. Assume the reference generator outputs the lower voltage set $[V_1, V_2, ..., V_n]$ satisfying $V_1 > V_2 > ... > V_n$. The voltage we need is output of an n:1 multiplexor and stabilized by a regulator. Note Fig. 5(a) shows only the functional blocks for

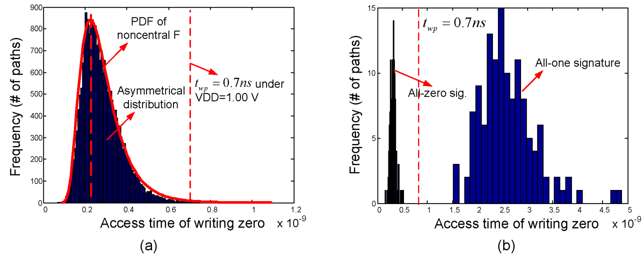


Figure 3: Histogram of T_{WR} for writing '0': (a) $VDD = 1.00$ V; and (b) fastest and slowest chips for $VDD = 0.70$ V.

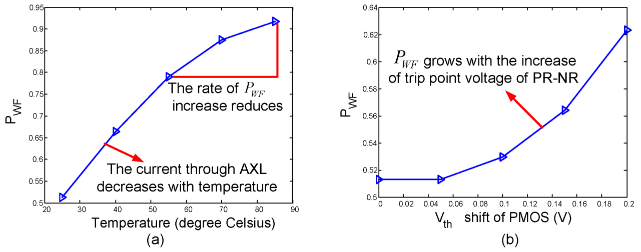


Figure 4: P_{WF} variation with: (a) temperature; and (b) NBTI-induced aging effect.

RESP that can be implemented either on the PCB (off-chip scheme) or on the die (on-chip scheme). Fig.5(b) illustrates the two steps of RESP: (1) preparation, (2) iterative VDD adjustment to find the acceptable signature for each chip. The preparation specifies the address of SRAM cell to generate signature with $P_{WF} = p_{wf}$, as well as the acceptable error Δp between p_{wf} and p'_{wf}. Note p_{wf} is a preset value of P_{WF} in RESP and each chip can have its own p_{wf}; p'_{wf} is the measured value of P_{WF} for the chip in each iteration. Δp is determined by the resolution of VDD. With higher resolution, we can set smaller Δp. Assume at least one voltage among $[V_1, V_2, ..., V_n]$ satisfies $|p_{wf} - p'_{wf}| \leq \Delta p$ found by iteratively tuning VDD. In each iteration, write '0'(or '1') into the SRAM cells successfully at the normal supply voltage $VDD = V_{norm}$. Then write '1'(or '0') into the same address under $VDD = V_i \leq V_{norm}$, where i is initialized as $\lfloor n/2 \rfloor$. Read out the contents with $P_{WF} = p'_{wf}$. If $|p'_{wf} - p_{wf}| \leq \Delta p$, accept it as a signature and stop; if $p'_{wf} - p_{wf} > \Delta p$ (or $p'_{wf} - p_{wf} < -\Delta p$), $i \leftarrow i - 1$ (or $i \leftarrow i + 1$) and repeat a new iteration. The procedure is amenable for automation. In addition, signature generation can be performed at run time using the idle SRAM blocks.

p_{wf} helps us to obtain unique and robust signatures from a chip. Appendix E shows that, if an attacker knows part of the signature, revealing p_{wf} may reduce the min-entropy of unknown part. To address it, the system can randomly choose a p_{wf} among multiple candidates when the signature is needed.

5. SIMULATION RESULTS AND ANALYSIS

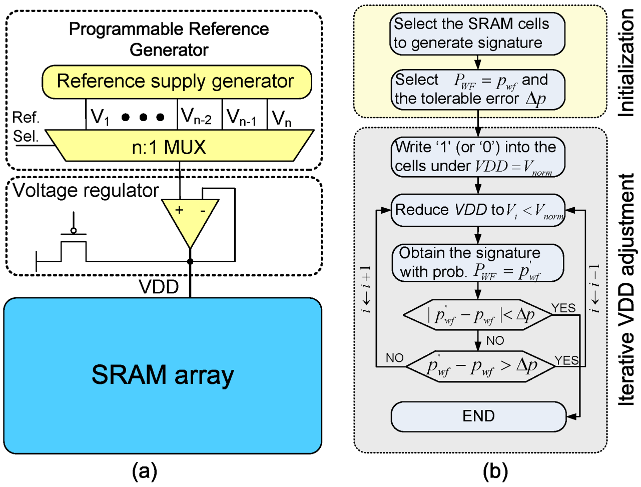
RESP is evaluated for uniqueness and robustness of 128-bit signature for $m = 1000$ 32KB SRAM prototypes in the Monte-Carlo Hspice simulation using PTM 45nm CMOS Process, with V_{th} variation of $\sigma_{th,inter} = 15\%$ and $\sigma_{th0,intra} = 10\%$ [18]. VDD is chosen between 0.67 V and 0.87 V with the tuning step 0.01 V. VDD is assumed ideal and the noise impact is discussed in Section 6.

5.1 Uniqueness Analysis

For authentication, the signatures need to be as different as possible from each other. We use the Hamming distance (HD) to evaluate the signature distance quantitatively. The uniqueness of signature is evaluated among the chips for a specific range of p_{wf}. We select an arbitrary value of p_{wf} within $[0.40, 0.60]$). Fig. 6(a) shows about 50% (64 bits) inter-die HD, i.e. one-bit entropy for each SRAM cell. The probability of zero for each bit in Fig. 6(b) is around 0.5, which is skewed from 0.5 to 0.4 and 0.6, respectively for $[0.50, 0.70]$ and $[0.30, 0.50]$, as shown in Fig. 7. Assuming $HD_{i,j}$ is the HD between chip i and chip j, the average HD for m chips, denoted by HD_{avg}, is calculated as [20]

$$HD_{avg} = \frac{2}{m \cdot (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{i,j} \qquad (4)$$

When $p_{wf} \in [0.40, 0.60]$, HD_{avg} is 49.2% near the theoretical value 50% ($128 \times 0.5 = 64$ bits). For $[0.50, 0.70]$ and $[0.30, 0.50]$, HD_{avg} is reduced to 46.70% and 47.32% respectively. Since HD_{avg} is not affected severely as the chips choose different p_{wf}, the accuracy of tuning VDD can be equivalently reduced. The Shannon entropy is dependent on VDD selection, which is up to 6 bits/cell as described in Appendix C.



Programmable Reference Generator
Reference supply generator
Ref. Sel.
V1 • • • Vn-2 Vn-1 Vn
n:1 MUX
Voltage regulator
+ -
VDD
SRAM array
(a)
Select the SRAM cells to generate signature
Select $P_{WF} = p_{wf}$ and the tolerable error Δp
Initialization
Write '1' (or '0') into the cells under $VDD = V_{norm}$
Reduce VDD to $V_i < V_{norm}$
Obtain the signature with prob. $P_{WF} = p'_{wf}$
$|p'_{wf} - p_{wf}| < \Delta p$
YES
NO
$p'_{wf} - p_{wf} > \Delta p$
NO
YES
$i \leftarrow i+1$
$i \leftarrow i-1$
END
Iterative VDD adjustment
(b)

Figure 5: (a) Hardware architecture of RESP; and (b) Signature generation procedure.

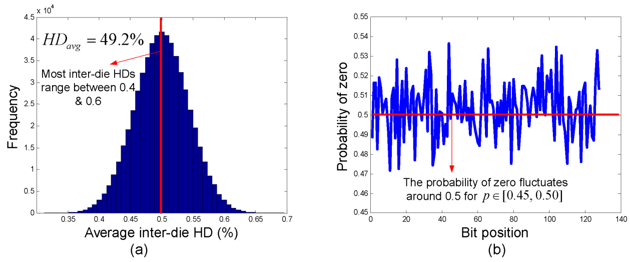


Figure 6: For $p_{wf} \in [0.40, 0.60]$, (a) inter-die HD of 1000 chips; and (b) probability of zero in each bit position.

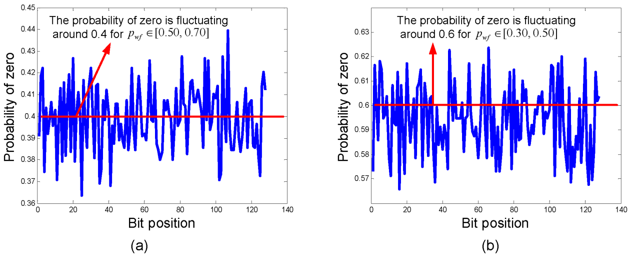


Figure 7: Probability of zero on each bit position for: (a) $p_{wf} \in [0.50, 0.70]$; and (b) $p_{wf} \in [0.30, 0.50]$.

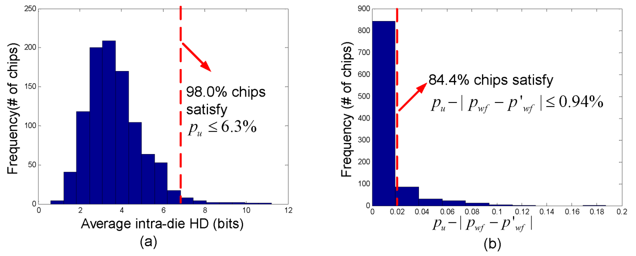


Figure 8: Distribution of: (a) p_u under temperature variation; and (b) $p_u - |p_{wf} - p'_{wf}|$ for $m = 1000$ chips.

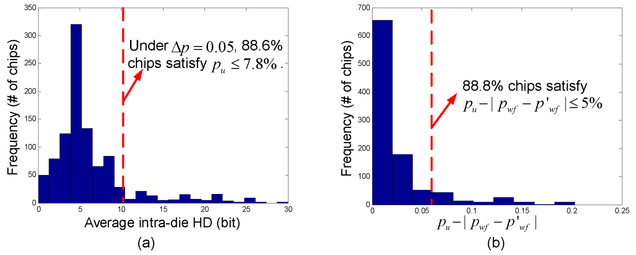


Figure 9: Distribution of: (a) p_u under NBTI; and (b) $p_u - |p_{wf} - p'_{wf}|$ for $m = 1000$ chips.

5.2 Robustness under Temperature Variation

The robustness measures the signature reproducibility under non-ideal environment such as temperature variation, which results in unstable bits. Considering precise value of $P_{WF} = p_{wf}$ may be difficult to achieve due to environmental fluctuations and limited VDD resolution, we accept an error of $|p_{wf} - p'_{wf}| \leq \Delta p$ to stop tuning VDD in Fig. 5(b). Under this condition, the overall ratio of flipped bits is p_u for a given temperature. Therefore, we can derive $p_u \geq |p_{wf} - p'_{wf}|$ for each chip. When the temperature rises from 25 °C to 85 °C at the interval of 15 °C, p_u is nearly 2.88% on average for $\Delta p = 0.05$. In particular, Fig.8(a) shows 95.4% chips with $p_u \leq 6.3\%$. $p_u - |p_{wf} - p'_{wf}|$ can correspond to the flipped bits under the unlimited VDD resolution yielding $p_{wf} = p'_{wf}$. Fig. 8(b) shows the histogram of 1000 chips for $p_{wf} \in [0.40, 0.60]$ and $\Delta p = 0.05$. More than 84.4% chips satisfy $p_u - |p_{wf} - p'_{wf}| \leq 0.94\%$. It means 84.4% chips would have only 0.94% unstable bits under $p_{wf} = p'_{wf}$. Hence, the non-zero $|p_{wf} - p'_{wf}|$ may contribute significantly to p_u. The unstable bits can be tolerated by the post-processing procedures [21].

5.3 Aging Effect

In the nano regime, the V_{th} degradation of PMOS due to NBTI plays a major role in temporal performance degradation of circuits. If V_{th} of PMOS PL and PR is increased by 17.3 mV after a simulated ten-year usage [19], p_u is 4.95% on average for $\Delta p = 0.05$ with 25 °C. Furthermore, Fig. 9(a) shows that 88.6% chips achieve $p_u \leq 7.8\%$. In Fig. 9(b), the histogram of 1000 chips shows that 88.8% chips satisfy $p_u - |p_{wf} - p'_{wf}| \leq 5\%$. We can estimate the proportion of unstable bits caused by NBTI in the design cycle and choose more powerful error-correcting codes to tolerate them in the fuzzy extractor [21].

6. STABILITY UNDER SUPPLY FLUCTUATION

6.1 Signature with Supply Fluctuation

Simultaneous switching noise (SSN) from current variation of the switching logic generates the voltage spikes on the supply [22]. Therefore, the VDD across the selected SRAM cells may deviate from the desired value. In the Monte-Carlo simulation, we specify inter-die V_{th} deviation percentage as low (±5%), medium (±15%) and high (±25%) respectively, and set $\sigma_{th0,intra}$ as 10% and 20% to obtain the unstable percents in Table 1 for $p_{wf} \in [0.4, 0.6]$.

Table 1: Unstable % of signature bits under different process and voltage variations

Inter-die corner,	Supply shift (mV)				
$\sigma_{th0,intra}$	±2	±4	±6	±8	±10
low, 10%	2.85%	5.76%	8.58%	11.46%	14.09%
low, 20%	1.57%	3.09%	4.71%	6.36%	7.93%
medium, 10%	2.82%	5.54%	8.23%	10.86%	13.40%
medium, 20%	1.63%	3.08%	4.49%	6.16%	7.62%
high, 10%	2.74%	5.53%	8.20%	10.88%	13.46%
high, 20%	1.55%	3.05%	4.78%	6.24%	7.56%

In Table 1, the number of unstable bits grows with the fluctuation of VDD. Up to 10 mV, the worst case is 14.09% flipped bits in a signature on the low inter-die variation corner. However, the number of unstable bits decrease with the increasing intra-die variation. For example, for 5% inter-die deviation, when $\sigma_{th0,intra}$ is increased to 20% from 10%, the unstable percent becomes 5.79%. It is reasonable, since the larger $\sigma_{th0,intra}$ can expect more chances to have the cells of large $|T_{WR} - t_{wp}|$. With the same $\sigma_{th0,intra}$, the inter-die shift makes negligible impact on the number of unstable bits, because VDD is tuned to track the inter-die corner for p_{wf}. The aggressive scaling of CMOS process leads to increase in intra-die variation (e.g. random dopant fluctuation) resulting in better tolerance of supply fluctuation.

6.2 Stable Signature Extraction through Multiple Measurements

Considering the current variation at each clock cycle, the fluctuation of VDD denoted by $\Delta V(t)$, can be simplified as a stochastic process within $[V_r - \Delta V_1, V_r + \Delta V_1]$ ($\Delta V_1 > 0$), where V_r is the desired value. Two assumptions are made about $\Delta V(t)$:

1. It is the ergodicity process that $\Delta V(t_0)$, $\Delta V(t_1)$,..., can traverse all values in $[V_r - \Delta V_1, V_r + \Delta V_1]$.

2. $\Delta V(t_i)$, $i = 0, 1, ...$ is statistically independent and follows the identical distribution.

Further, we model $\Delta V(t)$ as [22]

$$\Delta V(t) = \Delta V_1 sin(\omega t + \theta) \tag{5}$$

where ω is the oscillation frequency and θ is the initial phase. Assume the range $[V_r - \Delta V_e, V_r + \Delta V_e]$ yields the acceptable intra-die HD as Table. 1. Based on Appendix E, within N times signature measurements, the probability P_{hit} that the VDD is sampled in $[V_r - \Delta V_e, V_r + \Delta V_e]$ is

$$P_{hit} = 1 - (1 - (2/\pi)arcsin(\Delta V_e/\Delta V_1))^N \tag{6}$$

P_{hit} relies on N and the ratio $\Delta V_e/\Delta V_1$ as shown in Fig. 10. For ΔV_e takes up to half of V_1 (small noise or high fluctuation tolerance), $N = 10$ achieves the high probability (approximately 1) to sample VDD within $[V_r - \Delta V_e, V_r + \Delta V_e]$. When $\Delta V_e/\Delta V_1 = 0.1$, N becomes 50 for $P_{hit} \approx 0.9$. Hence, the high supply noise needs a large N. Correspondingly, the multiple measurements under the same VDD need be incorporated into the procedure of RESP in Fig.5(b).

7. DISCUSSIONS

7.1 Hardware Overhead Analysis

If a chip provides a pin to control the VDD of embedded SRAM array from outside, no modification is carried out and the on-chip retrofitting overhead is zero. Or if the embedded SRAM has the VDD self-tuning structure as [17],

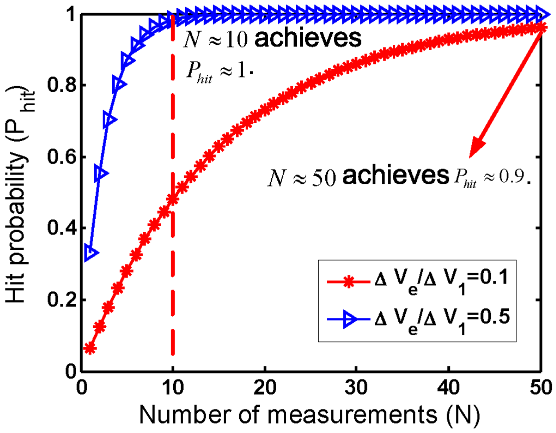


Figure 10: P_{hit} for different $\Delta V_e/\Delta V_1$.

RESP can be realized in it directly, resulting in virtually zero retrofitting overhead when no more components are needed to increase the number of references voltages. In cases of SOCs equipped with multiple voltage islands, we can use the on-chip voltage regulators during design process to minimize overhead. Hence, the retrofitting overhead would be primarily due to a multiplexor to choose specific voltage level. Moreover, such an approach can also be employed to reduce the SRAM power through dynamic voltage fluctuation as in [17].

7.2 Resolution of Supply Voltage Adjustment

In RESP, VDD resolution (i.e. the steps at which the VDD is adjusted), represents a trade-off between number of signatures (due to varying challenge vectors) and robustness of signatures. In our simulation, we have observed that the voltage step of 0.01 V provides acceptable value of robustness. Increasing voltage levels compromises reproducibility of signature under temporal voltage variations. However, the multiple-measurement approach as described in Section 6 can be used to achieve finer voltage steps leading to increased signature space.

8. CONCLUSION AND FUTURE WORK

We have presented RESP, a methodology to retrofit PUF into embedded SRAM array, a prevalent on-chip structure, by exploiting voltage scaling induced random write failures in SRAM cells. Using extensive simulations under realistic process variations, we have shown that it can generate large set of unclonable signatures. These signatures provide high entropy (since vast set of challenge-response pairs can be generated with selection of cell locations and scaled supply voltages), good reproducibility, and high stability under temporal fluctuations in voltage/temperature as well as aging effects. Since embedded SRAM is an integral component of modern processors and most SOCs, and often a memory core is associated with isolated supply grid/pin, RESP can be retrofitted to existed chips not designed with PUFs. Furthermore, RESP may provide the advantage of virtually zero hardware and design overhead for these chips.

Future work may exploit other forms of memory failures. In particular, hold or data retention failure can be used to generate random signatures. In addition, one can also target application of RESP into field programmable gate array (FPGA) devices.

9. REFERENCES

[1] J. R. Anderson, G. M. Kuhn, “Low cost attacks on tamper resistant devices,” *IWSP*, 1997, pp. 125-136.

[2] R. Pappu, “Physical one-way functions,” PhD thesis, Massachusetts Institute of Technology, 2001.

[3] P. Tuyls, G. Schrijen, B. Skoric, “Read-proof hardware from protective coatings,” *CHES*, 2006, pp. 369-381.

[4] D. Lim, *et al*, “Extracting secret keys from integrated circuits,” *IEEE Trans. VLSI Syst.*, vol. 13, no. 10, pp. 1200-1205, 2005.

[5] G. E. Suh, S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” *DAC*, 2007, pp. 9-14.

[6] S. Kumar, *et al*, “The butterfly PUF: protecting IP on every FPGA,” *HOST*, 2003, pp. 2809-2825.

[7] Y. Su, J. Holleman and B. Otis, “A 1.6J/bit 96% stable chip ID generating circuit using process variation,” *ISSCC*, 2007, pp. 406-611.

[8] D. E. Holcomb, W. P. Burleson and K. Fu, “Power-up SRAM state as an identifying fingerprint and source of true random numbers,” *IEEE Trans. on Computers*, vol. 58, no. 9, pp. 1198-1210, Sep., 2009.

[9] A. R. Krishna, *et al*, “MECCA: a robust low-overhead PUF using embedded memory array,” *CHES*, 2011, pp. 407-420.

[10] R. Maes, P. Tuyls and I. Verbauwhede, “Instrinsic PUFs from flip-flops on reconfigurable devices,” *WISSec*, 2008.

[11] Y. Wang, *et al*, “Flash memory for ubiquitous hardware security functions: true random number generation and device fingerprints,” *SP*, 2012, pp. 33-47.

[12] Y. Zheng, A. Krishna and S. Bhunia, “ScanPUF: robust ultralow-overhead PUF using scan chain,” *ASP-DAC*, 2013.

[13] D. E. Lackey, *et al*, “Managing power and performance for system-on-chip designs using voltage islands,” ICCAD, 2002, pp. 195-202.

[14] S. Mukhopadhyay, H. Mahmoodi, K. Roy, “Modeling of failure probability and satistical design of SRAM array for yield enhancement in nanoscale CMOS,” *IEEE TCAD*, vol. 24, no. 12, pp. 1859-1880, 2005.

[15] A. Kawasumi, *et al*, “A single-power-supply 0.7V 1GHz 45nm SRAM with an asymmetrical unit-β-ratio memory cell,” ISSCC, 2008, pp. 382-383.

[16] K. Zhang, *et al*, “A 3-GHz 70-Mb SRAM in 65-nm CMOS technology with integrated column-based dynamic power supply,” *IEEE JSSC*, vol. 41, no. 1, pp. 146-151, 2006.

[17] Y. Lai, S. Huang and H. Hsu, “Resilient self-VDD-Tuning scheme with speed-margining for low-power SRAM,” *IEEE JSSC*, vol. 44, no. 10, pp. 2817-2823, 2009.

[18] Predictive Technology Model, http://ptm.asu.edu/

[19] L. Hong, *et al*, “Modeling of PMOS NBTI effect considering temperature variation,” *ISQED*, 2007, pp. 139-144.

[20] A. Maiti, *et al*, “A large scale characterization of RO-PUF,” *HOST*, 2010, pp. 94-99.

[21] Y. Dodis, L. Reyzin and A. Smith, “Fuzzy extractors: how to generate strong keys from biometrics and other noisy data,” *EUROCRYPT*, 2004, pp. 523-540.

[22] M. S. Gupta, *et al*, “Understanding voltage variations in chips multiprocessors using a distributed power-delivery network,” *DATE*, 2007, pp. 624-629.

[23] H. Nambu, *et al*, “A 1.8-ns access, 550-MHz, 4.6-Mb CMOS SRAM,” *IEEE JSSC*, vol. 33, no. 11, pp. 1650-1658, 1998.

APPENDIX

A. INFLUENCE OF VOLTAGE REDUCTION ON PERIPHERAL CIRCUITS

The VDD scaling increases T_{WR} of SRAM cells to generate write failure for signature, as well as the latency of paths in the peripheral circuits (e.g. row decoder). Fig. 11 shows a typical structure of row decoder in the synchronous SRAM with clock Φ to separate the pre-charge ($\Phi = 0$) and evaluation phase ($\Phi = 1$) [23]. When $\Phi = 0$, the output of WL is low to make the access transistors in the off state. In addition, the signal propagation on the two paths (red and blue) marked in Fig.11 is required to be completed when $\Phi = 0$ in each cycle. However, if it does not occur when Φ becomes high to start evaluation phase, the WL may not rise up in that cycle; or produce a glitch shorter than the normal duration as shown in Fig. 12. The short glitch may result in the write failure for all the activated SRAM cells. To address it, the address can stay unchanged for more than one cycle to provide sufficient time for decoding. Fig.12 shows the WL duration can recover the nominal value for write in the second cycle. Since in each cycle BL and BLB are re-charged to '1', the multiple-cycle operations would not influence the write failure probability on the evaluation phase.

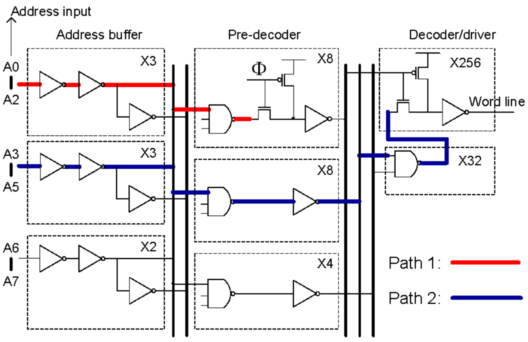


Figure 11: Typical architecture of row decoder in SRAM [23].

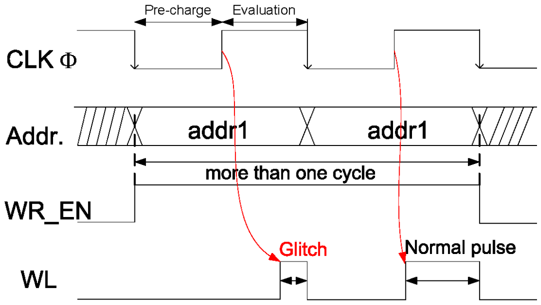


Figure 12: Waveform with more than one cycle decoding latency.

B. SENSITIVITY OF FAILURES UNDER VDD SCALING

We assume the peripheral circuits (e.g. row decoder and bit line conditioning) share the supply VDD_{peri} and SRAM cells have the supply VDD_{cell}. Simply, if $VDD_{peri} = VDD_{cell}$, it is considered as a single supply SRAM; otherwise a dual supply SRAM. Next, the sensitivity of four types of failures to the VDD_{peri} and VDD_{cell} scaling is analyzed. Fig. 13(a) shows the simplified structure related to read and access failure when reading '1'. Capacitor C needs to be discharged through node QB. However, the charge of capacitor C makes the voltage of QB rise to certain level (V_{rd}) transiently. The read failure occurs, if V_{rd} is higher than the trip point of PL-NL. Fig. 14(a) shows that V_{rd} goes up with VDD_{peri} in the Hspice simulation. Hence, the supply scaling on VDD_{peri} cannot aggravate the read failure. Still based on Fig. 13(a), considering the larger resistance on AXR with the smaller VDD_{peri}, the interval of minimum distance (e.g. 0.1VDD) between BL and BLB is augmented, which is verified in Fig. 14(b). As a result, more access failures can be expected.

P_{WF} increases with T_{WR} in (1). In Fig. 13(b) that shows the simplified structure when writing '0', T_{WR} is related to both VDD_{peri} and VDD_{cell}. The Hspice simulation in Fig. 15 shows that T_{WR} grows with VDD_{peri} reduction or VDD_{cell} augment. Moreover, compared with that when VDD_{cell} is changed from 1.00 V to 0.80 V, T_{WR} is increased much more with the same change scale on VDD_{peri}. Therefore, T_{WR} is more sensitive to the VDD_{peri} variation.

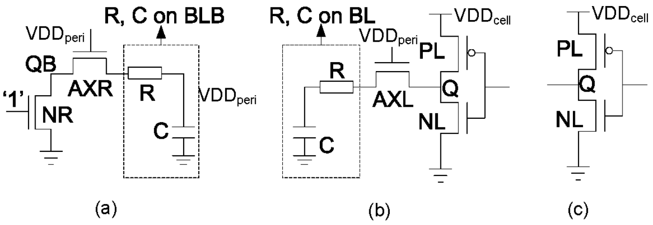


Figure 13: (a) Read and access failure; (b) write failure; and (c) hold failure.

For the hold failure (Q='1' for example) as shown in Fig. 13(c), the voltage of Q gradually reduces to the standby VDD_{cell}, depending on the leakage current through NL below the trip point of inverter PR-NR determined by the device parameter (e.g. W, L and V_{th}). Hence, the exploitation of hold failure may severally rely on the length of standby duration. In addition, the residual charge on Q also impacts the randomness of stored value after VDD_{cell} is resumed to the nominal value. If the above two problems can be handled properly, exploiting the hold failure as PUF is also a potential choice. Based on the above analysis, the access failure and write failure are more proper to be employed to induce failure in the supply scaling for PUF.

C. DERIVATION OF SHANNON ENTROPY

The challenges of RESP include the cell locations, write contents ('0' or '1') and supply voltage VDD. In this section, we consider the maximum entropy achieved by tuning VDD for cells storing '1' when writing '0'.

First, we consider the ith set of supply voltage, denoted as vector $\underline{VDD^{(i)}} = (VDD_1^{(i)}, VDD_2^{(i)}, ..., VDD_m^{(i)})$, is provided for the overall m chips; specifically, $VDD_j^{(i)}$ is for chip j yielding $P_{WF} = p_j^{(i)}$. Denote $WF^{(i)}$ as the event of write under $\underline{VDD^{(i)}}$; $WF^{(i)} = 1$ means the write failure occurs, while $WF^{(i)} = 0$ corresponds to the successful write. Given the random intra-die process variation, the write failure happens on each cell of chip j with probability $p_j^{(i)}$. Assuming the uniform distribution for chip selection, the probability of choosing chip j, $j = 1, 2, ..., m$, is $1/m$. The write failure probability for chip j is $P(chip\, j,\, WF^{(i)} = 1) = (1/m) \cdot p_j^{(i)}$. We can obtain $P(WF^{(i)} = 1) = \sum_{j=1}^{m} P(chip\, j) \cdot P(WF^{(i)} = 1 | chip\, j) = \sum_{j=1}^{m} (1/m) \cdot p_j^{(i)}$. Hence, the entropy of each cell under the ith supply vector is

$$H(WF^{(i)}) = -P(WF^{(i)} = 1) \cdot log_2(P(WF^{(i)} = 1)) - P(WF^{(i)} = 0) \cdot log_2(P(WF^{(i)} = 0)) \quad (7)$$

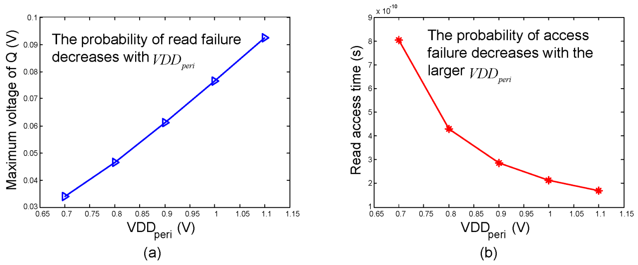


Figure 14: (a) Maximum voltage of Q during read; and (b) read access time.

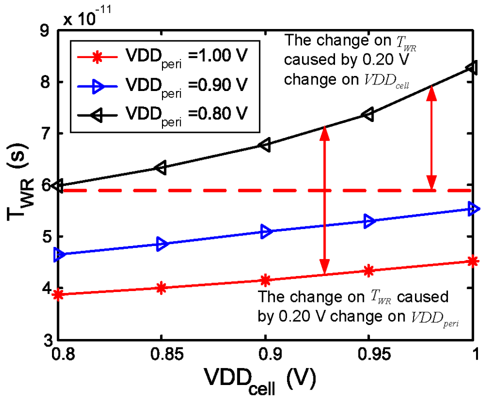


Figure 15: Change of T_{WR} for different VDD_{peri} and VDD_{cell}.

where $P(WF^{(i)} = 0) = 1 - P(WF^{(i)} = 1)$. $H(WF^{(i)})$ can be maximized as 1 bit when $P(WF^{(i)} = 0) = P(WF^{(i)} = 1) = 0.5$. Next, we supplement another supply vector $P(WF^{(i')})$, $i \neq i'$ and derive the joint entropy $H(WF^{(i)}, WF^{(i')})$. It can be obtained that $H(WF^{(i)}, WF^{(i')}) = H(WF^{(i)}) + H(WF^{(i')}|WF^{(i)})$. Considering both $H(WF^{(i')}|WF^{(i)})$ and $H(WF^{(i)})$ are no more than 1 bit, $H(WF^{(i)}, WF^{(i')}) \leq 2$ bit. Further,

$$\begin{aligned} &H(WF^{(i')}|WF^{(i)}) = \\ &-P(WF^{(i)} = 0) \cdot H(WF^{(i')}|WF^{(i)} = 0) \\ &-P(WF^{(i)} = 1) \cdot H(WF^{(i')}|WF^{(i)} = 1) \end{aligned} \tag{8}$$

Without losing generality, we first consider $VDD_j^{(i')} < VDD_j^{(i)}$, $j = 1, 2, ..., m$. Then the term $H(WF^{(i')}|WF^{(i)} = 1)$ in (8) become zero, due to $P(WF^{(i')} = 1|WF^{(i)} = 1) = 1$ under the reduced supply voltage. (8) can be simplified as $H(WF^{(i')}|WF^{(i)}) = P(WF^{(i)} = 0)H(WF^{(i')}|WF^{(i)} = 0)$. For $H(WF^{(i)}) = 1$ bit, $P(WF^{(i)} = 0)$ is set as 0.5. The maximum $H(WF^{(i')}|WF^{(i)} = 0)$ can be achieved by $P(WF^{(i')} = 0|WF^{(i)} = 0) = P(WF^{(i')} = 1|WF^{(i)} = 0) = 0.5$, which is shown in Fig. 16 as the condition $area1 = area2$ for chip j under $VDD_j^{(i')}$ and $VDD_j^{(i)}$. Hence, it can be derived that $H(WF^{(i')}, WF^{(i)})$ is maximized as 1.5 bits.

We further derive $H(WF^{(1)}, WF^{(2)}, ..., WF^{(d)})$ of d supply voltage sets, $\underline{VDD^{(1)}}$, $\underline{VDD^{(2)}}$, $\underline{VDD^{(3)}}$,...$\underline{VDD^{(d)}}$, satisfying $VDD_j^{(1)} > VDD_j^{(2)} > VDD_j^{(3)} > ... > VDD_j^{(d)}$, $j = 1, 2, ..., m$. As a result,

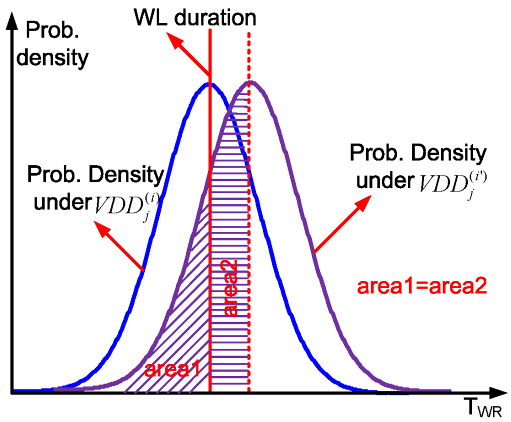

Prob. density
WL duration
Prob. Density under $VDD_j^{(i)}$
Prob. Density under $VDD_j^{(i')}$
area1=area2
area2
area1
TWR

Figure 16: Illustration of maximizing $P(WF^{(i)} = 0)H(WF^{(i')}|WF^{(i)} = 0)$.

$$\begin{aligned} &H(WF^{(1)}, WF^{(2)}, ..., WF^{(d)}) = H(WF^{(1)}) + \\ &H(WF^{(2)}|WF^{(1)}) + H(WF^{(3)}|WF^{(1)}, WF^{(2)}) + \\ &H(WF^{(4)}|WF^{(1)}, WF^{(2)}, WF^{(3)}) + ... \end{aligned} \tag{9}$$

where $H(WF^{(3)}|WF^{(1)}, WF^{(2)}) = (0.5)^2 \times 1$ =0.25 bit, $H(WF^{(4)}|WF^{(1)}, WF^{(2)}, WF^{(3)}) = (0.5)^3 \times 1$ =0.125 bit. Hence, the entropy limit when $d \to \infty$ is

$$Lim_{d\to\infty} H(WF^{(1)}, WF^{(2)}, ..., WF^{(d)}) = \frac{1}{1 - 0.5} = 2 \ bits$$

By repeating the above procedure for $VDD_j^{(1)} < VDD_j^{(2)} < ... < VDD_j^{(d)}$, $j = 1, 2, ..., d$, extra 1-bit entropy is provided as $d \to \infty$. Therefore, the entropy upper bound is 3 bits per SRAM cell storing '1' when writing '0'.

For writing '1' into the cell storing '0', another 3 bits can be expected, since writing '0' and '1' deals with different transistors in the SRAM cell. Hence, each SRAM cell can ideally generate up to 6-bit entropy for write with tuning VDD.

D. DERIVATION OF P_{HIT} UNDER RESONATING CURRENT

The step current and resonating current are existent in real chips. The step current is caused by the sudden arouse of large logic gates from the standby or start-up state of chips. Since we can start to obtain the signature after such initialization process, the analysis is ignored in the paper. As periodic pulses, resonating currents have frequencies in the resonant band of the PDN [22]. Small current pulses may produce large peak-to-peak swings around the nominal voltage (voltage ripple) even in the steady state. According to Section 6.2, the supply fluctuation at time t_i, namely $\Delta V(t_i)$, $i = 0, 1, ...$ is assumed an ergodicity process. Statistically independent $\Delta V(t_i)$ follows the identical distribution with CDF $P_V(\cdot)$ in the range $[V_r - \Delta V_1, V_r + \Delta V_1]$. Assume the supply fluctuation range leading to small intra-die HD is $[-\Delta V_e, \Delta V_e]$. For one measurement of signature at certain time, the probability to sample VDD within $[V_r - \Delta V_e, V_r + \Delta V_e]$ is $\Delta P_r = P_V(V_r + \Delta V_e) - P_V(V_r - \Delta V_e)$. Hence, for N times statistically independent measurements, such probability (P_{hit}) can be expressed as

$$P_{hit} = 1 - (1 - \Delta P_r)^N \tag{10}$$

From Section 6.2, the influence from resonating currents is

$\Delta V(t)$ modeled as

$$\Delta V(t) = \Delta V_1 sin(\omega t + \theta) \tag{11}$$

Where ΔV_1 and ω are the oscillation peak magnitude and frequency respectively; θ is the initial phase. From $-\Delta V_e \leq \Delta V(t) \leq \Delta V_e$, we can obtain the inequality as $-\Delta V_e/\Delta V_1 \leq sin(\omega t + \theta) \leq \Delta V_e/\Delta V_1$. The solutions of $sin(\omega t + \theta) = \Delta V_e/\Delta V_1$ and $sin(\omega t + \theta) = -\Delta V_e/\Delta V_1$ in the first and fourth quadrants are

$$t = \begin{cases} (arcsin(\Delta V_e/\Delta V_1) - \theta)/\omega & first\ quadrant \\ (arcsin(-\Delta V_e/\Delta V_1) - \theta)/\omega & fourth\ quadrant \end{cases} \tag{12}$$

Hence, the sample time t is in $[0, (arcsin(\Delta V_e/\Delta V_1) - \theta)/\omega]$, $[\pi + (arcsin(-\Delta V_e/\Delta V_1) - \theta)/\omega, \pi + (arcsin(\Delta V_e/\Delta V_1) - \theta)/\omega]$ and $[2\pi + (arcsin(-\Delta V_e/\Delta V_1) - \theta)/\omega, 2\pi]$. Further, we assume t uniformly locates in each cycle. As a result, $\Delta P_r = (2/\pi) arcsin(\Delta V_e/\Delta V_1)$. ΔP_r increases with $\Delta V_e/\Delta V_1$, which means the smaller supply fluctuation or better tolerance capability of SRAM cells (larger ΔV_e) can gain the larger P_{hit}. Further, (10) can be re-written as

$$P_{hit} = 1 - (1 - (2/\pi) arcsin(\Delta V_e/\Delta V_1))^N \tag{13}$$

E. POSSIBLE INFORMATION LEAKAGE OF REVEALING P_{WF}

In this section, we present a concise derivation to show the possible min-entropy reduction with the revealed p_{wf}, when the attackers know part of the signature. First, let's assume that for the m-bit signature, each bit is statistically independent. The min-entropy of each bit position excluding the first m_1 bits without revealing p_{wf} is

$$H_\infty(R_i) = -log_2(max(p_{wf}, 1 - p_{wf})) \tag{14}$$

$R_i = 1$ if write failure occurs on bit position i; otherwise $R_i = 0$, $i = m_1 + 1, m_1 + 2, ...m$. When the attacker has known p_{wf} and the write failure occurs on m_1' bits (random variable M_1') among the first m_1 bits, $mp_{wf} - m_1'$ bits should have write failure among the latter $m - m_1$ bits of the probability $p_c(m_1') = (mp_{wf} - m_1')/(m - m_1)$, $m_1 \neq 0$. In addition, $m_1' \geq max(0, mp_{wf} - (m - m_1)) = m_l$ and $m_1' \leq min(m_1, mp_{wf}) = m_u$ are the lower and upper bound respectively. As a result, $H_\infty(R_i|m_1') = -log_2(max(p_c, 1 - p_c))$. The conditional min-entropy comes from [21]:

$$\begin{aligned} H_\infty(R_i|M_1') &= -log_2(\mathbb{E}_{m_1' \leftarrow M_1'}[2^{-H_\infty(R_i|m_1')}]) \\ &= -\, log_2(\mathbb{E}_{m_1' \leftarrow M_1'}[max(p_c, 1 - p_c)]) \\ &= -\, log_2(\sum_{i=m_l}^{m_u} S_i \cdot max(p_c(i), 1 - p_c(i))) \end{aligned} \tag{15}$$

where $S_i = \frac{\binom{m_1}{i}(p_{wf})^i(1-p_{wf})^{m_1-i}}{\sum_{i=m_l}^{m_u}\binom{m_1}{i}(p_{wf})^i(1-p_{wf})^{m_1-i}}$. We consider $p_{wf} \geq 0.5$ (similar to $p_{wf} < 0.5$) for discussing the relationship between $H_\infty(R_i)$ and $H_\infty(R_i|M_1')$. The key derivation is as follows:

$$\begin{aligned} & -log_2(\sum_{i=0}^{m_1} S_i \cdot max(p_c(i), 1 - p_c(i))) \\ & = H_\infty(R_i|M_1') + \Delta \leq -log_2(\sum_{i=0}^{m_1} S_i \cdot p_c(i)) \\ & = log_2 p_{wf} = H_\infty(R_i) \end{aligned} \tag{16}$$

Δ is a relaxed variable for (16), which is zero for $m_l = 0$ and $m_u = m_1$. Based on (16), if $\Delta = 0$ and $max(p_c(i), 1 - p_c(i)) = p_c(i)$, $H_\infty(R_i|M_1') = H_\infty(R_i)$ always holds, which means no loss of min-entropy with revealing p_{wf}. Or $\Delta > 0$ results in $H_\infty(R_i|M_1') < H_\infty(R_i)$. Specifically, when $p_{wf} = 0.5$, $max(p_c(i), 1 - p_c(i))$ should always be larger than 0.5. Hence, $H_\infty(R_i|M_1') < H_\infty(R_i)$ leads to the information leakage. Fig.17 further shows that the information leakage is also related to m_1. When $m_1 = 20$ in Fig.17(a), the loss of min-entropy caused by revealing p_{wf} is negligible. The main difference locates in the range around $p_{wf} = 0.5$. However, it becomes more obvious as the augment of m_1 shown in Fig. 17(b) for $m_1 = 60$.

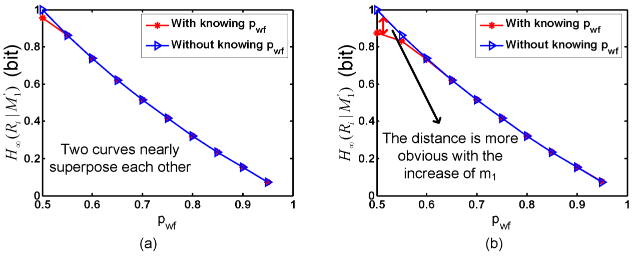


Figure 17: Min-entropy of $p_{wf} \in [0.5, 0.95]$ (a) $m_1 = 20$; and (b) $m_1 = 60$.