MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array

Aswin Raghav Krishna, Seetharam Narasimhan, Xinmu Wang,
and Swarup Bhunia

Case Western Reserve University, Cleveland OH-44106, USA
ark70@case.edu

Abstract. The generation of unique keys by Integrated Circuits (IC) has important applications in areas such as Intellectual Property (IP) counter-plagiarism and embedded security integration. To this end, Physical Unclonable Functions (PUF) have been proposed to build tamper-resistant hardware by exploiting random process variations. Existing PUFs suffer from increased overhead to the original design due to their specific functions for generating unique keys and/or routing constraints. In this paper, we propose a novel memory-cell based PUF (MECCA PUF), which performs authentication by exploiting the intrinsic process variations in read/write reliability of cells in static memories. The reliability of cells is characterized after manufacturing by inducing temporal failures, such as write and access failures in the cells using a programmable word line duty cycle controller. Since most modern designs already have considerable amount of embedded memory, the proposed approach incurs very little overhead (<1%) compared to existing PUF designs. Simulation results for 1000 chips with 10% inter-die variations show that the PUF provides large choice of challenge-response pairs with high uniqueness (49.9% average inter-die Hamming distance) and excellent reproducibility (0.85% average intra-die Hamming distance).

Keywords: Physical Unclonable Function (PUF), IC authentication, Memory failures, Negative Bias Temperature Instability (NBTI).

1 Introduction

In recent years, shorter product-cycle marketing requirements in the semiconductor industry have driven chip vendors to reuse their hardware designs and outsource Integrated Circuits (IC) production to external foundries shared by many companies. Apart from reuse, the intellectual property (IP) is often an additional source of income to a vendor through external licensing to other companies who can include the design in their products. However, production outsourcing and IP licensing have exposed the designs to theft and cloning and it is estimated that counterfeit electronics cost the industry upto US$100 billion every year [1]. Counterfeiting attacks on IP/IC can occur at the manufacturing site, e.g. an untrusted foundry makes several copies of the design, or during

B. Preneel and T. Takagi (Eds.): CHES 2011, LNCS 6917, pp. 407–420, 2011.

deployment in the field. These attacks can be broadly classified into two categories: (i) *invasive attacks*, e.g, by delayering the IC through reverse engineering and obtaining circuit function from physical layout; and (ii) *non-invasive attacks* which in turn can be classified as *passive* and *active* attacks. Passive attacks are mounted by observing side-channel information such as power consumption [2], delay or electromagnetic radiation, to obtain secret keys or sensitive information. Active attacks, on the other hand, are induced by the introduction of a fault followed by a passive attack [3]. IP designs can also be stolen from FPGAs during power-up by reading their bitstream information which is stored in an external memory. Building a tamper-proof hardware that is resistant to all forms of attacks is, thus, crucial for securing IP/IC against counterfeit attacks.

Authentication plays an important role in detecting counterfeit products. Simply put, the role of authentication is to check the identity of a product and to validate that it comes from a genuine source. The common practice is to embed a digital secret/ID in a non-volatile memory, e.g. in a RFID tag, and use digital key comparison and encryption for authentication and protection of secret information. However, since the secret information is stored in digital form, it is vulnerable to invasive attacks and providing high tamper resistance environment is very expensive. Furthermore, since each product contains only one unique identifier, it is possible for an attacker to obtain it by intercepting the communication of the key between an authorized reader and a tag and use it for cloning or mounting replay attacks.

Physical Unclonable Functions (PUFs) are rapidly becoming the preferred method for IC/IP identification, authentication and secure system design. They are secure, low-cost, and robust functions built into a design that implement a challenge-response protocol by exploiting the inherent random variations in the manufacturing process to generate unique signatures [4,5]. Inevitable variations in the device paramaters (e.g. threshold voltage) make it practically impossible to clone the original PUF even with the same mask set, foundry and manufacturing process. Typically, the challenge response pairs for each device are stored by the vendor after production in a database and is given to a trusted party who wishes to use the device. The trusted party applies a challenge and checks the corresponding response with the database to verify the authenticity of the device in any environment [6]. PUFs have several advantages that make them robust to cloning and replay attacks. Firstly, since a PUF response is based on random process variations, it is not possible for an attacker to 'predict' the response before or after production. Secondly, since PUFs have a very large set of challenge-response pairs, an attacker must obtain all the pairs to make an identical copy of the PUF - merely obtaining only a few pairs is not useful, since a different pair may be used for authentication. Thirdly, unlike conventional approaches in which the stored keys are preserved digitally in non-volatile memory even after power-down, PUFs generate signatures only when they are powered-up, thus forcing attackers to mount attacks to extract signatures only when the PUF is in operation [6].

In this paper, we propose a novel (ME)mory (C)ell-based (C)hip (A)uthentication PUF - MECCA PUF for authentication and key generation based on the concept of failure mechanisms in the memory array. It is observed that more than 50% of System-On-Chip (SOC) area is used for memory with estimates indicating that the number could increase to 90% in 2013 [7]. The proposed PUF leverages on the fact that most designs already contain embedded SRAM memory array for their operation and hence can also be used for generating signatures. The basic idea is to control the word line duty cycle of the SRAM cells to determine their vulnerability to failures during read/write access. Word line controllability allows us to generate multiple responses from the array and hence increase the number of challenge-response pairs. The random process variations of the cells' parameters across the chip determine the reliability (low or high) of the cells; the cells' reliability is translated to a digital response. We analyze the effectiveness of MECCA PUF in detail and show that it provides excellent unclonability, uniqueness and robustness of signatures. Since environmental effects such as temperature and device ageing effects (such as bias temperature instability or BTI [22]) affect the repeatability of signatures, we propose an ageing-tolerant scheme to make the cells generate highly stable responses. Simulation results show that the proposed PUF offers several advantages: 1) very less area overhead (<1%); 2) high uniqueness (49.9% average inter-die Hamming distance); and 3) high reproducibility. Additionally, the delay controller circuit can also be integrated with a Design-for-Test (DFT) technique [8] for detecting stability faults in memory, thus allowing it to serve dual purposes and to further reduce the cost per function.

The remainder of the paper is organized as follows: Section 2 describes prior works on PUF circuits. Section 3 describes the methodology of the proposed MECCA PUF along with theoretical analysis of PUF properties. Simulation results and analysis are presented in Section 4. Finally, we conclude in Section 5.

2 Related Work

Several silicon PUFs have been published in literature. Silicon PUFs can be classified as memory PUFs and delay PUFs [9]. Delay PUFs such as Ring Oscillator PUF [6, 10] and Arbiter PUF [11, 12] translate the process variations into random delay variations to produce a digital signature. These PUFs involve introduction of the circuits which are solely used for key generation and authentication and hence present substantial area overhead. Existing memory based PUFs rely on the random initializations of the cells due to process variations for generating signatures [13, 14, 15]. However, these PUFs only provide a single bit response per cell and have limited challenge-response pairs [9]. Furthermore, these PUFs are prone to cloning attacks in the foundry as the entire random initialization memory map can be copied to produce the signatures as the original PUF. Another type of PUF, known as Butterfly PUF [16], is based on exploiting interconnect variations in cross-coupled latches during startup. A major disadvantage with this PUF is that attaining the metastable point for

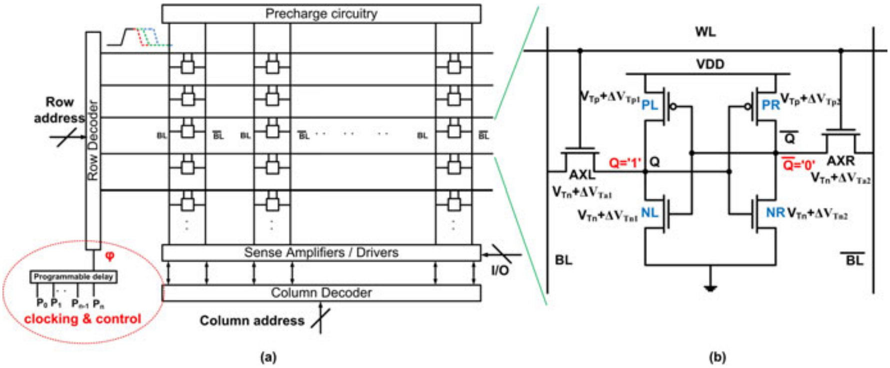

Fig. 1. MECCA PUF architecture: (a) Memory block with peripheral circuitry and programmable delay circuit, (b) Schematic of an SRAM cell

each cross-coupled latch prior to key generation is difficult due to the finite delays of the latches and interconnects which causes the outputs of the latches to oscillate. This oscillation imposes precise timing requirements of the control (excite) signal for reproducible keys. Finally, PE-PUFs [9] couple process variations with environmental effects, such as temperature, power supply noise and noise due to circuit activity, for generating signatures. However, PE-PUFs require long interconnects and placement over the entire chip which can result in significant area overhead/routing constraints in modern technologies.

3 MECCA PUF

The concept of the proposed MECCA PUF architecture can be explained with the help of Fig. 1. The PUF contains an SRAM array along with peripherals and a programmable delay generator. Most modern designs already contain one or more memory block(s) for their normal operation and the delay generator introduces only a minor area penalty. In the core array, inter-die and intra-die variations in the device parameters cause a mismatch in the strengths of transistors which can be exploited to cause failures in cells. However, some cells are more prone to failure than others because of the random effect of process variations.

The failure mechanisms [20, 21] observed in a memory cell are as below:

Write failure: Occurs when the internal node in an SRAM cell cannot be discharged through the access transistors during the word line's active duration.

Read failure: Flipping of the data in SRAM cell during a read operation.

Access failure: Occurs when the voltage difference between the bitlines is lower than the offset voltage of the sense amplifier when it is activated.

Hold failure: When the supply voltage is lowered during standby, leakage currents through the NMOS transistors can cause internal node voltage to reduce below the switching threshold of the inverter for a data flip.

The idea of using memory failures in PUFs has been investigated earlier in [17, 18] by inducing read/write collisions or using metastability in the cross-coupled

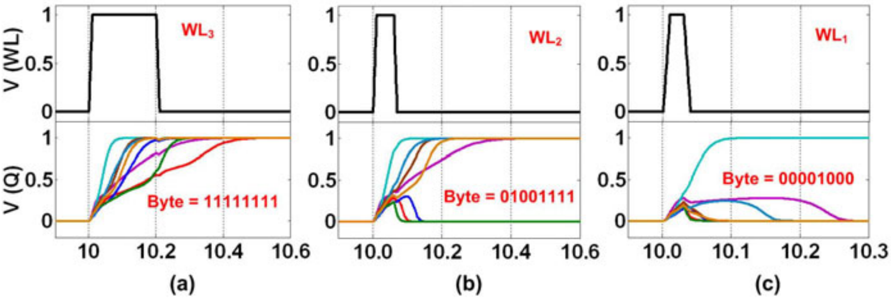

Fig. 2. Reliability of 8 cells for different word line duty cycles; $WL_3 > WL_2 > WL_1$ (WL_3 is used for normal memory operation)

loop to generate responses. In the MECCA PUF, we use a different approach of evaluating the reliability of a single SRAM cell by inducing a write failure by changing the word line duration. Assume that the cell stores a ‘0’ and we wish to write a ‘1’. This is accomplished by setting BL to ‘1’ and $\overline{BL}$ to ‘0’ which causes the cross-coupled inverters to change states. As shown in Fig. 1(b), the different transistors have varying ΔV_T components imposed on nominal V_T due to process variations. Equating the dc currents through the transistors AXL and NL, we compute the internal node voltage, V_Q as shown in eqn. (1), where the required pull-up ratio of the cell, PUR, is decided such that V_Q is below the switching point of the inverter.

$$V_Q = V_{DD} - (V_{Tn} + \Delta V_{AXL}) - [((V_{DD} - (V_{Tn} + \Delta V_{AXL}))^2 - 2 \times PUR \\ \times (\frac{\mu_p}{\mu_n})((V_{DD} - |(V_{Tp} + \Delta V_{PR})|) \times V_{DSATp}) - (\frac{V_{DSATp}^2}{2}))]^{0.5} \qquad (1)$$

In a realistic scenario, the V_T and ΔV_T components of the other transistors also play an important role as the cell starts switching due to regenerative feedback. For normal memory operation, the word line (WL) duration is selected such that a write operation can be successfully performed under all process corners. When the memory is used as a PUF, we purposely reduce the WL duration such that a stable cell at a normal WL length may or may not be stable at a reduced length as determined by process variations. For example, by using a programmable delay word line, the WL duty-cycle is shortened which will randomly cause some of the cells to have write failure. The effect of reducing WL duration is shown in Fig. 2 where the values of 8 cells are compared for 3 durations. For each WL duration, by selecting a set of R cells, we obtain a signature consisting of both good cells (which are written correctly even with shorter WL) and defective cells (which have write failure). Access failure may also be exploited in the MECCA PUF to evaluate reliability of a cell by reducing the WL duration required for discharging one of the bit-lines for a read operation.

In contrast, read and hold failures are static failures which cannot be controlled by WL duration and hence are not useful for evaluating the reliability of

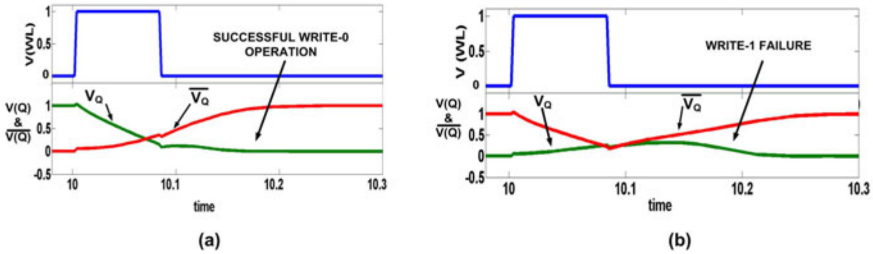

Fig. 3. Dependence of stability of a cell on write value (In both cases, the reduced word length ON time is the same) (a) Successful write-0 operation. (b) Write-0 failure.

a cell in our PUF. For example, for a read-1 failure, the node voltage ($V_{\bar{Q}}$) which is determined by voltage division across the resistances of transistors AXR and NR, must rise above the switching threshold (V_S) of the subsequent inverter for the cell to flip its value. The voltage division is independent of the WL duration and hence read failures cannot be induced by varying the WL duration. Hold failures occur due to leakage currents and hence cannot be induced by controlling the WL duration. The reliability of a cell also depends on the logic value being written into the cell at reduced word-line duration. As shown in Fig. 3, the cell has high reliability for a write-1 but a low reliability (write failure) for a write-0 operation for the same WL. This is due to the fact that different PMOS and access NMOS transistors (and hence different V_T variations) are involved at the initialization of write-0 and write-1 operations before the other transistors play a role in engaging positive feedback. This dependence on write value is very useful in increasing the number of unique signatures since a write-0 success (failure) does not imply a write-1 success (failure) at the same WL.

The major steps for generating unique signatures are as follows.

1. We choose the address of the R-cells as part of the input challenge.
2. A background write operation of 0 (or 1) in cell(s) is performed at the normal word line duration depending on whether we want to exploit the reliability for a write-1 or write-0. This is required to ensure that the cells are in a known initialized state, thus ensuring that a possible successful write is not due to random initialization. Next, the bitlines are precharged to their respective values depending on the values to be written.
3. We reduce the word line duration using the programmable delay circuit and perform the write operation at this reduced duration for all the chips.
4. Finally, we read out the values stored in the cells to give an R-bit response.

Word Line Duty Cycle Controller: Fig. 4 illustrates a programmable word line duty cycle controller that is used for inducing write failures in the SRAM array. The circuit consists of a chain of inverters with the outputs of k subgroups of odd number of inverters connected to the inputs of a k X 1 mux. The programmable select bits, which become part of the challenge, choose one out of k possible duty cycles to generate a shortened word line, e.g. by acting as the

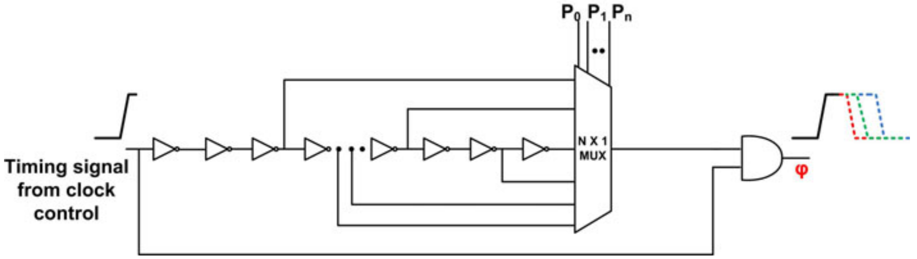

Fig. 4. Programmable word line duty cycle controller

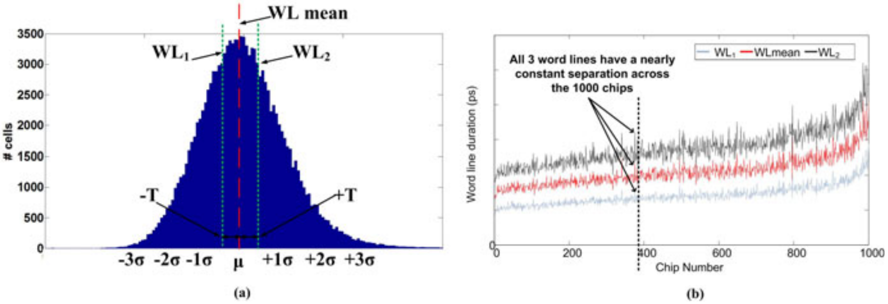

Fig. 5. (a) Write-time distribution of 1000 chips, (b) Programmable delay variation across 1000 chips

enable signal for the address row decoder. The k duty cycles consist of $n = k - 1$ duty cycles used for PUF operation and one for normal memory operation.

The word line durations can be chosen from the distribution of write-time (Fig. 5(a)) of all the cells in the chips. For PUF operation, we choose the mean word line to be the nominal, μ, of the write-time distribution since the cells will have equal probability of write failure and success. The inverter chain is then tapped for outputs to obtain n duty cycles such that they fall within $\pm T$ from the nominal. The n levels must be separated such that they don't overlap with each other due to V_T variations in the duty cycle controller as shown in Fig. 5(b) where three WL durations are sorted in increasing order of inter-die V_T. Also, it is interesting to note that since the controller and the SRAM array are at the same inter-die V_T for a particular chip, all n levels will move in the same direction (albeit by different amounts) and only the intra-die variations need be considered for choosing T. For a C chosen based on the accepted distribution of '1's and '0's in the responses, i.e., $P(X < \mu - T) < C$, T can be computed in terms of σ. As an added layer of security, a challenge to address-duty cycle mapping or other well-known techniques (e.g. controlled PUFs [19]) can be used to make it harder for an attacker to model the PUF. We investigate the following properties of PUFs:

Unclonability: From a security perspective, a PUF itself must not be prone to cloning by an attacker by observing a few challenge response pairs. In the case of our PUF, an attacker must obtain the addresses of the cells, the word line duration and the values being written into each cell for each challenge. In this context, we are referring to an attacker in the foundry who has complete access to the chips. Choosing an arbitrary WL and observing the values of all the cells in the array to clone a copy by skewing will not be useful to the attacker since the values in all the cells in the original MECCA PUF will be different from the values in the skewed design for different word line durations; the attacker must skew the design such that each cell has the same response at each WL for a write-0 and write-1 - a significantly difficult challenge.

Entropy: Different signatures can be obtained by measuring the reliability of different sets of cells, i.e., by using a different set of addresses (challenges). Moreover, as the WL duration can be controlled to generate different sets of low and high reliability cells for a chosen set of addresses, the WL duration is also part of the challenge and can be used to produce many keys from a given set of addresses. As an example, for a set of chosen addresses (A_0, A_1, A_2,. . . A_n), by setting WL duration to, say WL_1, we obtain a signature as (D_0, D_1, D_2 . . . D_n) where D_i is 0 or 1 depending on whether the cell at A_i is a high reliability cell (with no write failure) or low reliability cell (with write failure) respectively. By changing the WL duration to WL_2, we can obtain another signature set (S_0, S_1, S_2,. . . S_n) for the same addresses (A_0, A_1, A_2,. . . A_n), with $D_k \neq S_k$ for some cells for 0≤k<n. For example, the address set (900, 100, 500, 825,. . ., 1024) in a 1024 SRAM array for a write-1 can have a signature

- (1, 0, 0, 1,. . .,1) for word line length, WL_1, where cells at 900, 825 and 1024 are high reliability cells (1s) and cells at 100, 500 are low reliability cells (0s)
- (1, 0, 1, 1,. . ., 1) for word line length, WL_2, (such that $WL_2 > WL_1$) where cells at 900, 500, 825 and 1024 are high reliability cells (1s) and the cell at 100 is a low reliability cell (0)

As mentioned before, measurement of reliability is relative among cells and word line durations, i.e., a cell (such as A_2 in the above example) which has high reliability for a given WL duration can have low reliability for a shorter WL. However, since the delay circuit is designed to produce n-levels of durations close to the nominal required write-time of the cells, the values at many bit positions in an R-bit response will be different for a shorter WL duration. Additionally, the dependence of reliability on the value being written for a given WL duration also increases entropy by choosing different write values for the given set of addresses.

4 Simulation Results and Analysis

The proposed PUF has been implemented with an SRAM array designed for the 45nm *Predictive Technology Model* (PTM) [28]. Simulations were carried out using Synopsys *HSPICE* for 1000 chips for generating 128 bit responses. The effect of process variations for the chips was introduced by running Monte Carlo simulations for inter-die variations with $\sigma = 10\%$ and random intra-die

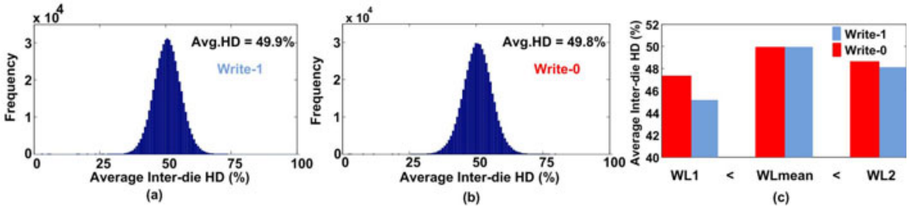

Fig. 6. HD distribution of inter-die responses of 1000 chips for (a) write-1 at mean WL (b) write-0 at mean WL (c) Avg. inter-die HD for 3 WL_S for write-0 and write-1

variations with $\sigma = 6\%$. The duty cycle controller was implemented as shown in Fig. 4 to produce n=3 duty cycles. The SRAM cells were brought to a known initialization state with a background write at the normal WL duration. The challenge consisted of the addresses of the cells along with the select inputs to the duty cycle controller. After a pattern was applied, the values of the 128 cells were extracted as a signature at a short WL duration for all the chips.

Uniqueness Analysis: To determine the uniqueness of the MECCA PUF, we plotted the distribution of the inter-die Hamming distance (HD) of 1000 MECCA PUFs for write-0 and write-1 operations for the 3 WL durations as shown in Fig. 6; the horizontal axis represents the number of bits differing between responses of any two chips for a given challenge while the vertical axis represents the number of comparisons among the 1000 chips corresponding to a HD. To quantify the uniqueness property, we computed the average inter-die Hamming Distance (HD_{Avg}) [29] of the signatures of m=1000 chips with percentage HD (out of r response bits) between any two chips m_1 and m_2 as follows:

$$HD_{Avg} = \frac{2}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{perc}(m_1, m_2). \tag{2}$$

The average inter-die HD was found to be close to the ideal 50% for write-0 and write-1 operations at the mean WL but reduced by a maximum of 2.5% (for a write-0 operation) for WL_1 and WL_2. The reduction in inter-die HD is due to bit-skewing at some bit positions in the responses from the 1000 chips. Ideally, each bit in the responses from all the chips should have 50% probability of being a 0 or a 1 to center the inter-die HD distribution about 50%. However, if some bit has higher probability towards 0 or 1, then the inter-die HD for that bit becomes close to zero. In our case, the skewing is due to the fact that a cell failure at a longer WL implies a failure at a shorter WL for a given write value (Fig. 7).

Robustness Analysis: The robustness of a PUF shows how reproducible are the signatures from the chips in changing operating conditions. The HD between responses from the same PUF in different operating conditions must be as low as possible for high reproducibility. We estimated the intra-die HD among the

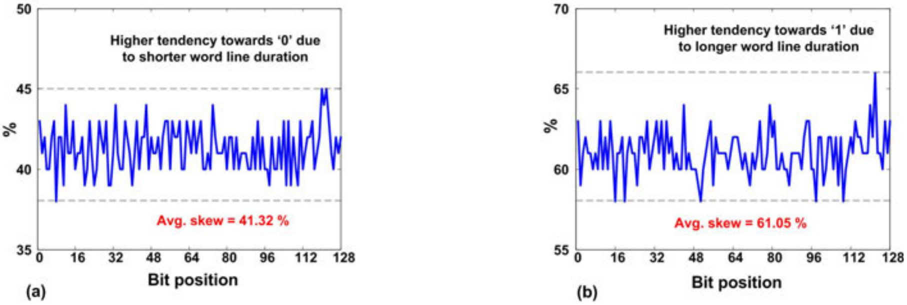

Fig. 7. Bit-skewing for write-1 at (a) $WL_1 <$ mean WL (b) $WL_2 >$ mean WL

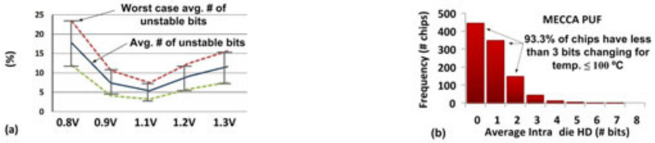

Fig. 8. Average intra-die HD from 1000 chips for MECCA PUF (a) for supply voltage variation (compared to nominal Vdd=1V), and (b) for temperature variation

128-bit responses for each chip for supply voltage variations and compared them with that obtained at nominal voltage (Fig. 8(a)). At the worst-case voltage of 0.8V, the intra-die HD is as high as 23 bits (≈ 18%). Fig. 8(b) shows the intra-die HD for temperature variations for each chip at room temperature compared with that obtained at 5 temperatures (for the same challenge) till 100°C in steps of 15°C. Most of the responses (≈ 93.3%) from the 1000 chips change by less than 3 bits with very few responses changing by 5 bits or more (≈ 1%) for mean WL showing that the PUF is very stable even at high temperatures. From the two figures, the overall conclusion is that the PUF showed lower reliability due to voltage variations than due to temperature variations.

Ageing Effects: Ageing effects due to temporal variations in device parameters also affect the reliability of a device over its lifetime [23, 24, 25]. With continuous scaling in device dimensions, stronger electric fields have resulted in an increase in the number of interface traps in PMOS transistors over time at high temperatures. The increase in traps has resulted in an increase in the V_T of transistors causing reliability issues due to negative bias temperature instability (NBTI) [26, 27]. In the case of a PUF, V_T degradation of the transistors can affect the uniqueness and reproducibility of signatures. In the MECCA PUF, the transistor marked PL in the cell suffers from NBTI due to a strong electric field across gate-source ($|V_{gs}| = V_{dd}$), as shown in Fig. 9(a). Due to temporal variations in V_T, a cell A_1 (refer Fig. 9(b)) which fails at word length WL_2 can pass through that level and become successful at WL_2 (unfilled brown (dark) circle) and hence produce an incorrect bit output.

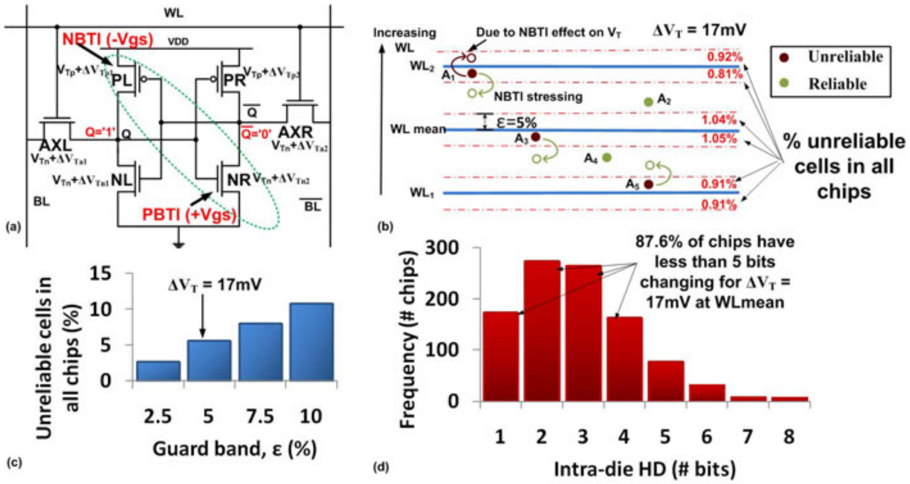

Fig. 9. Ageing effects in memory. (a) NBTI effect in SRAM cell. (b) Characterization of cells as reliable and unreliable cells for expected ΔV_T=17mV. (c) % unreliable cells in all the chips as a function of ε (and ΔV_T). (d) Number of unreliable bits per chip at mean WL.

To quantify the temporal reliability of cells, we design a guard band around the WLs based on an expected V_T shift of 17mV based on results in [22] over a 10-year lifetime of the product.Accordingly, we included the V_T shift (on top of process variations) in our PMOS model file and performed monte-carlo simulations to obtain the number of temporally unreliable cells and change in intra-die HD. The word line duty cycle controller can be used to produce additional WLs to characterize the cells post-production and identify unreliable cells (within a guard band). The numbers on the right in Fig. 9(b) show the distribution of the unreliable cells for guard band, ε=5% for ΔV_T=17mV. It can be seen that approximately only 6% of the cells (out of all cells in all chips) fall within the guard band and can potentially produce an incorrect output over the products' lifetime. The actual number of unreliable cells per chip at mean WL is shown in Fig. 9(d), from which it can be seen that 87.6% of the chips have less than 4 bits for a ΔV_T=17mV (corresponding to ≈2% unreliable cells around mean WL in Fig. 9(b)). We propose the following solutions to ageing: 1) discarding the temporally unreliable cells (by choosing more cells); 2) if the number of unreliable bits is tolerable (low avg. intra-die HD), they can be used in the signature generation; 3) intentional ageing can be done to those few unreliable cells (at high temperature and high supply voltage) to ensure that the cells are moved out of the guard band to make it a temporally reliable cell (dotted green circle in Fig. 9(b)). Additionally, since the V_T shift can be reduced by flipping contents of the cells [23, 22], it is possible that fewer cells can produce incorrect outputs due to V_T recovery during normal operation of the memory.

Table 1. Area Overhead Comparison

PUF	RO-PUF	MECCA PUF	
		including memory	w/o memory
Area $(\mu m)^2$	3122	520	21

Overhead: We computed the area overhead of the MECCA PUF and compared it with that of a RO-PUF (as an example of delay based PUF) to generate a 128-bit key. For the RO-PUF, assuming all orderings of the ROs are likely, 35 ROs are required. This would require two 35 X 1 MUXs, two 32-bit counters and one 32-bit comparator along with the 35 ROs (5 stages) to produce the key. For the MECCA PUF, we used a 128 cell SRAM array along with the peripherals (a 4 X 16 row address decoder, 8-bit I/O with buffers, sense amplifiers and precharge circuitry) and the programmable delay circuit. Both PUFs were synthesized using Synopsis *Design Compiler* and Table 1 shows the area comparison of the MECCA PUF and RO-PUF. Even if the chip has no memory, i.e. (the memory has to be implemented), the total overhead of the MECCA PUF is small compared to the RO-PUF ($\approx$ 16.6%). As mentioned earlier, since most modern designs already contain embedded memory which can be used as the PUF, the area overhead is only due to the programmable delay circuit and is extremely small compared to the RO-PUF ($\approx$ 0.6%).

5 Conclusion

In this paper, we have presented MECCA, a novel memory based PUF that exploits the intrinsic variations in static memory cells by inducing failures for cryptographic operations. We have shown that even moderate variations in the device parameters provides high-quality signatures (in terms of uniqueness, reproducibility and entropy) while incurring significantly less hardware overhead compared to other PUFs by using the embedded memory array already present in most designs. Furthermore, we analyze the effect of voltage/temperature variations as well as ageing effects on the robustness of the PUF outputs and propose solutions using temperature induced stressing to further improve the reliability. With increasing effect of parameter variations in nanoscale memory, effectiveness of the proposed method is expected to increase in future technology nodes. Extending the proposed approach to other forms of memory, e.g. flash, would be subject of future research.

References

1. ORS-LABS: Counterfeit Electronic Components - An Overview (2007), `http://www.ors-labs.com/pdf/MASH07CounterfeitDevice.pdf`
2. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)

3. Kulikowski, K.J., Karpovsky, M.G., Taubin, A.: DPA on faulty cryptographic hardware and countermeasures. In: Breveglieri, L., Koren, I., Naccache, D., Seifert, J.-P. (eds.) FDTC 2006. LNCS, vol. 4236, pp. 211–222. Springer, Heidelberg (2006)
4. Gassend, B., et al.: Controlled Physical Random Functions. In: Proceedings of 18th Annual Computer Security Applications Conference (2002)
5. Gassend, B., et al.: Silicon Physical Random Functions. In: Proceedings of the Computer and Communication Security Conference (2002)
6. Suh, G.E., Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: Proc. DAC, pp. 9–14 (2007)
7. Semiconductor Industry Association (SIA), International Technology Roadmap for Semiconductors (ITRS) (2005)
8. Ney, A., et al.: A New Design-For-Test Technique for SRAM Core-Cell Stability Faults. In: Proc. DATE, pp. 1344–1348 (2009)
9. Wang, X., Tehranipoor, M.: Novel Physical Unclonable Function with Process and Environmental Variations. In: Proc. DATE, pp. 1065–1070 (2010)
10. Maiti, A., Schaumont, P.: Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive. Journal of Cryptology, 1–23 (2010)
11. Pappu, R.: Physical One-Way Functions, Phd thesis, Massachusetts Institute of Technology (2001)
12. Ozturk, E., Hammouri, G., Sunar, B.: Physical Unclonable Function with Tristate Buffers. In: Proc. ISCAS, pp. 3194–3197 (2008)
13. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 63–80. Springer, Heidelberg (2007)
14. Holcomb, D., Burleson, W., Fu, K.: Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags. In: Proc. the Conference on RFID Security (2007)
15. Su, Y., Holleman, J., Otis, B.: A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations. In: Proc. ISSCC, pp. 15–17 (2007)
16. Kumar, S., Guajardo, J., Maes, R., Schrijen, G., Tuyls, P.: The Butterfly PUF: Protecting IP on Every FPGA. In: Proc. HOST (2008)
17. Guajardo, J., Kumar, S., Tuyls, P., Schrijen, G. : Identification Of Devices Using Physically Unclonable Functions. WIPO Patent Application WO/2009/024913 A2
18. Guyensu, T.: Using Data Contention in Dual-ported Memories for Security Applications. Journal of Signal Processing Systems (2010)
19. Gassend, B., Clarke, D., van Dijkm, M., Devadas, S.: Controlled Physical Random Functions. In: Proc. ACSAC (2002)
20. Mukhopadhyay, S., Mahmoodi, H., Roy, K.: Modeling of Failure Probability and Statistical Design of SRAM Array for Yield Enhancement in Nanoscaled CMOS. In: IEEE TCAD, pp. 1859–1880 (2005)
21. Mukhopadhyay, S., Mahmoodi, H., Roy, K.: Reduction of Parametric Failures in Sub-100-nm SRAM Array Using Body Bias. In: IEEE TCAD, pp. 174–183 (2008)
22. Luo, H., Wang, Y., He, K., Luo, R., Yang, H., Xie, Y.: Modeling of PMOS NBTI Effect Considering Temperature Variation. In: Proc. ISQED, pp. 139–144 (2007)
23. Kumar, S.V., Kim, K.H., Sapatnekar, S.S.: Impact of NBTI on SRAM Read Stability and Design for Reliability. In: Proc. ISQED (2006)
24. Paul, B.C., Kang, K., Kufluoglu, H., Alam, M.A., Roy, K.: Impact of NBTI on the Temporal Performance Degradation of Digital Circuits. IEEE Electron Devices, 560–562 (2005)

25. Kang, K., Gangwal, S., Park, S.P., Roy, K.: NBTI Induced Performance Degradation in Logic and Memory Circuits: How Effectively Can we Approach a Reliability Solution? In: Proc. ASP-DAC (2008)
26. Bansal, A., et al.: Impacts of NBTI and PBTI on SRAM Static/Dynamic Noise Margins and Cell Failure Probability. In: Microelectronics Reliability, pp. 642–649 (2009)
27. Yang, S., Yang, H., Chuang, C., Hwang, W.: Timing Control Degradation and NBTI/PBTI Tolerant Design for Write-Replica Circuit in Nanoscale CMOS SRAM. In: Proc. VLSI-DAT, pp. 162–165 (2009)
28. Predictive Technology Model, `http://www.eas.asu.edu/~ptm/`
29. Maiti, A., Casarona, J., McHale, L., Schaumont, P.: A Large Scale Characterization of RO-PUF. In: Proc. HOST, pp. 94–99 (2010)