A Novel PUF based on Cell Error Rate Distribution of STT-RAM

Xian Zhang[1], Guangyu Sun[1,2] {zhang.xian, gsun}@pku.edu.cn
Yaojun Zhang[3], Yiran Chen[3], Hai Li[3] {yaz24, yic52, hal66}@pitt.edu
Wujie Wen[4] wwen@fiu.edu
Jia Di[5] jdi@uark.edu

[1]Center for Energy-Efficient Computing and Applications, Peking University, Beijing 100871, China
[2]Collaborative Innovation Center of High Performance Computing, NUDT, Changsha 410073, China
[3]Department of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh PA 15261, USA
[4]Department of Electrical and Computer Engineering, Florida International University, Miami FL 33199, USA
[5]Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville AR 72701, USA

Abstract—Physical Unclonable Functions (PUFs) have been widely proposed as security primitives to provide device identification and authentication. Recently, PUFs based on Non-volatile Memory (NVM) are widely proposed since the promise of NVMs' wide application. In addition, NVM-based PUFs are considered to be more immune to invasive attack and simulation attack than CMOS-based PUFs. However, the existing NVM-based PUF either shows the unreliability under environmental variations or need extra modifications to the IC manufacturing process. In this work, we propose err-PUF, a novel PUF design based on the cell error rate distribution of STT-RAM. Instead of using the distribution directly, we generate a stable fingerprint based on a novel concept called Error-rate Differential Pair (EDP) without modifications to the read/write circuits. Comprehensive results demonstrate that err-PUF can achieve sufficient reliability under environmental variations, which can significantly impact the cell error rates. Moreover, compared with existing approaches, err-PUF has a higher speed and lower power consumption with negligible overhead.

I. Introduction

In order to provide secure and low-cost identification and authentication, Physical Unclonable Functions(PUFs) have been extensively investigated. There exist various types of PUFs, most of which take advantages of random physical disorders in CMOS process technologies [14]. They include SRAM PUFs based on SRAM power-up states [5, 4], RO PUF based on latency of oscillator [16], Arbiter PUF based on wire connection delay [11], etc. Unfortunately, recent work has shown that these CMOS-based PUFs are increasingly prone to simulation attack [14]. In addition, they are vulnerable to invasive attack [12]. Consequently, several PUFs based on various Non-volatile Memories (NVMs) have been proposed to address the security issues.

These NVM-based PUFs include Memristor PUF [14], FPUF[13], PCM PUF [21], DWM PUF[6] and STT-PUF[20], etc. They have several advantages over the CMOS-based ones. First, NVM-based PUFs are more energy and area efficient to be used in some resource-constraint scenarios such as sensor nodes. Second, it is more complex to simulate a NVM-based PUF so that it becomes more difficult to launch a simulation attack[14]. Third, NVM-based PUFs are also less vulnerable to invasive attack [12] because the storage units (e.g. GST for PCM, MTJ for STT-RAM, and metal-oxide for RRAM) are stacked atop of the control transistors [18]. Note that all these NVM-based PUFs are CMOS-compatible.

Despite the advantages of NVM-based PUFs, there are two main limitations of current designs. The first limitation is that some designs do not evaluate the environmental impacts which may degrade PUFs' reliability. For example, in FPUF[13], the program cycles before inducing a disturb error for every cell are first evaluated. Then, the correlation coefficient is calculated to distinguish the genuine chip from the faked chips. Beside program cycles, variety of latency and program wear are also measured as a source of randomness. However, when environmental variations are considered, all the measured parameters above may greatly change[17] and FPUF's response may be unreliable. For Memristor-based PUFs, in which node voltage[14] is leveraged to generate random and unique fingerprints, the same limitation remains. The second limitation is that some designs require substantial modification to the peripheral circuitry to assist the extraction of device-level parameters, such as voltage sensors in every cell node [14], specified amplifier[21], differential circuit[20] and voltage to digital converter[2]. This will increase the design overhead and may affect normal read and write operations.

In order to overcome the limitations, we propose our err-PUF, which maximizes the hardware reuse with existing read-/write circuits in STT-RAM and demonstrates the reliability under environmental variations . We use STT-RAM to demonstrate our design since STT-RAM has been considered as one of the most promising alternatives for on-chip memory(e.g. SRAM) [22, 19, 20]. The major contributions of this work are listed as follows.

- We reveal the fact that the distribution of cell error rates in a STT-RAM array can be considered as a unique fingerprint for PUF designs. And the major challenge comes from environmental variations.
- We observe that the relationship of error rates between two STT-RAM cells is kept under environmental variations. Thus, we build err-PUF based on a novel concept called Error-rate Differential Pair (EDP) in this work.
- Comprehensive results are presented to demonstrate that err-PUF can achieve sufficient reliability even under substantial environmental variations.
- We synthesize the control logic for err-PUF and compare it with existing mainstream memory-based PUFs, in respect of hardware overhead, performance, and energy consumption.

This work is supported by the National Natural Science Foundation of China (No. 61572045).

978-1-4673-9569-4/16/$31.00 ©2016 IEEE

The rest of this paper is organized as follows. In Section II, we present the error model of STT-RAM to demonstrate the randomness of error rate distribution. Moreover, the challenge from environmental variations is also addressed. In Section III, we present design details of our err-PUF. The reliability, performance, power consumption, and design overhead of err-PUF are evaluated in Section IV followed by conclusions.

II. Prelimilaries

In this section, we first introduce the basics of STT-RAM. Then, we introduce two sources of STT-RAM write errors. At last, we investigate the environmental impacts to cell error rates.

A. Basics of STT-RAM

This work uses a 1T1J (one transistor one MTJ) STT-RAM cell structure. The data stored in STT-RAM cell is represented by the resistance of MTJ(Magnetic Tunneling Junction). When the MTJ is at the Anti-Parallel State (Parallel State), its resistance is high (low). The write operation is to launch a current pulse through the MTJ and switch MTJ's state from high resistance to low resistance or vice versa. The larger the write current, the shorter the time that MTJ takes to switch. The read (sensing) operation is similar to those of conventional memories. Errors may happen during both read and write operations. In this paper, we focus on the write error since the error rate of read is significantly lower than that of write [19, 22].

B. Two Sources of STT-RAM Write Errors

Generally speaking, a write error happens if the write current pulse is shorter than the MTJ switching time. There are two sources that can induce an error [22, 19, 8, 7]:

- **Process variations.** Process variations of both the transistor and MTJ can affect the amplitude of write current. For example, the variations of transistor channel length or width can result in variance of write current driving ability. The variations in MTJ resistance can also influence the bias condition of the transistor, and thus affect the current. The decrease of write current amplitude leads to the increase in MTJ switching time. As a result, it may cause an incomplete MTJ switching.
- **Thermal fluctuation.** Thermal fluctuation happens during the MTJ switching. It is an intrinsic character that randomly affects the MTJ switching time. Thus, the error caused by the thermal fluctuation can only be detected occasionally.

Since both process variations and thermal fluctuation are random effects, the error rates of cells in an STT-RAM array follow a random distribution.

C. Impact of Environmental Variations on Error Rates

Intuitively, if we abstract the error rate of each STT-RAM cell in the array to form a vector, this vector can be used as a fingerprint, which is similar to [13]. However, environmental variations have a significant impact on the reliability of this fingerprint. For example, both decrease of voltage and increase in temperature can reduce the driving ability of the transistor.

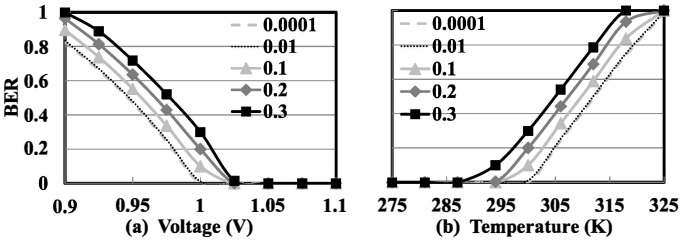

Fig. 1. Variation of error rate of a STTRAM cell due to change of environments: (a) Different Voltages (b) Different Temperatures.

Thus, the amplitude of write current changes, which results in a significant increase in error rates for some cells. Figure 1 shows the impact of different environmental variations on the error rates. The detailed configurations of STT-RAM cells can be found in Table I.

There are five curves in each figure, which represent simulation results of STT-RAM cells with different process variations. The legends in the figure represent the error rates of these cells, when the supply voltage (V) is $1V$ and the temperature (T) is $300K$. From these results, we can find that, when working supply voltage and temperature change, the error rate can vary several orders in magnitude.

One interesting observation is that these curves in Figure 1 do not cross with each other. This is because of that for every cell, the bias of device parameters caused by the process variation is fixed after fabrication. Though the environmental variations severely impact cell error rates, cells with certain parameters are more immune to errors while others not. It means that the difference of error rates between two cells is more stable than the error rates themselves. Thus, we propose our err-PUF design based on a novel concept called *Error-rate Differential Pair* (EDP). EDP reflects a stable relationship of bit error rates between two cells even with environmental variations. The detailed concept is introduced in the next section.

III. err-PUF design

In this section, we will first introduce a key concept called Error-rate Differential Pair (EDP). Based on EDP, we propose a robust PUF design which is called err-PUF to tolerate the wild change in the cell error rate distribution.

A. Error-rate Differential Pair (EDP)

In order to simplify the description of EDP, we first introduce several definitions as follows.

- **Normal Working Environment.** It refers to the working environment, under which the PUF authentication works. For example, under the working environment of STT-RAM in Section IV, the supply voltage and temperature vary in the ranges of $0.9V - 1.1V$ and $275K - 325K$, respectively.
- **Error-Most-State.** Error-Most-State means the extreme case of a normal working environment, under which the STT-RAM has the highest error rate. For the example of STTRAM, the supply voltage is set to 0.9V and the temperature is 325K for the Error-Most-State.
- **Error-Least-State.** Error-least-State means the extreme case of a normal working environment, under which the STT-RAM has the lowest error rate. For the above example of STTRAM, the supply voltage is set to 1.1V and the temperature is 275K.

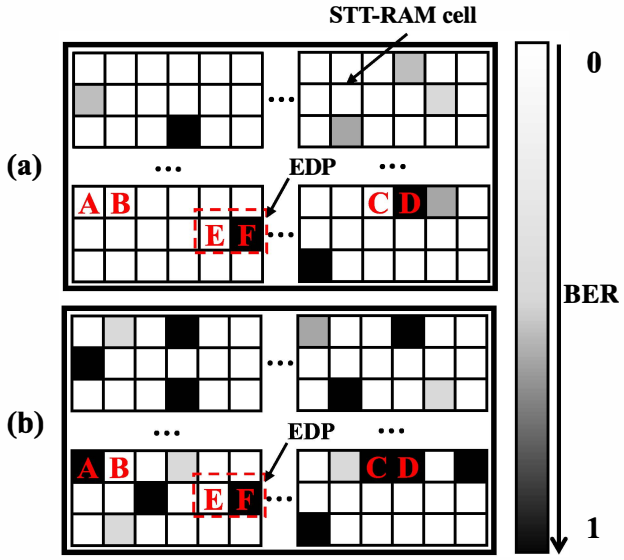

Fig. 2. Error Rates of a STT-RAM array in (a) Error-Least-State and (b) Error-Most-State. A-B and C-D are not EDPs. E-F is an valid EDP.

- **Read-Write-Read (RWR) Test.** In order to detect a cell error, the test is carried out in three steps: (1) read out the bit value in a cell, (2) write back the compliment bit to the cell, and (3) read the bit out again for comparison.

Having these terminologies, an EDP is defined as a pair of cells, cell A and cell B, that satisfy the following condition in both Error-Least-State and Error-Most-State. For **N**-round RWR tests, we have

$$|Err_A - Err_B| \geq N_{th} \quad (1)$$

Err_A and Err_B represent the total number of errors occur in N round of tests for cell A and cell B, respectively.

EDP is the foundation of err-PUF design. Statistically, for two cells in an EDP, they have considerable different error rates even with the environmental variation. An example of valid EDP is shown in Figure 2. As shown in the figure, a STT-RAM cell is abstracted as one unit block. The color depth of a block represents the bit error rate (BER) of the cell. The cell error rates of the same STT-RAM array under Error-Least-State and Error-Most-State are shown in Figure 2 (a) and (b), respectively. In this example, three pairs of cells are highlighted in the figure: A-B, C-D, and E-F. Only the E-F pair is a valid EDP. Pair A-B is not an EDP because errors in cell A are not detectable at Error-Least-State. Similarly, cell pair C-D are not an EDP either because both error rates of them reach one at Error-Most-State.

In our err-PUF design, the difference gap of error rates between two cells in an EDP has an impact on PUF verification. EDPs with a large gap of error rates are preferred. Since the detection of EDP is based on statistical testing results, it is possible that two cells with close error rates are detected as a pair of EDP. We can find that identifying EDPs in a STT-RAM array relies on the setup of N and N_{th}. If we increase N and N_{th}, the probability is decreased for identifying an EDP with low error rate difference. However, increasing N includes more timing overhead in the process of detecting EDPs in a STT-RAM array. The total number of EDPs that can be found in a STT-RAM array is decreased with a higher N_{th}. Later in Section IV, we provide more discussion about how to select proper N and N_{th}.

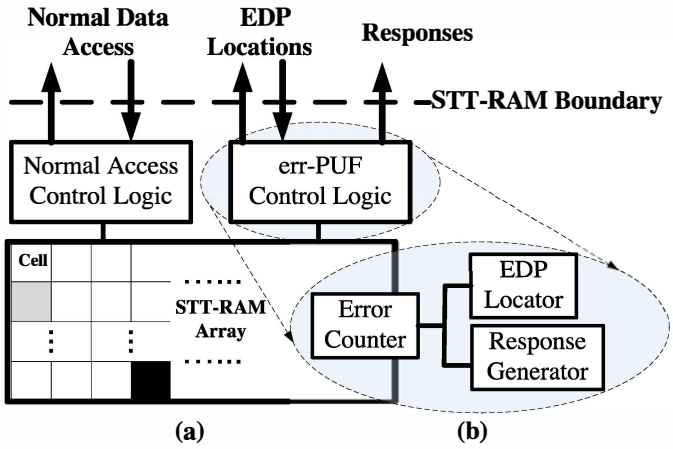

Fig. 3. Illustration of err-PUF architecture.

B. err-PUF Architecture and Workflow

The architecture of a STT-RAM with err-PUF is illustrated in Figure 3. As we have addressed, the PUF itself is embedded inside the STT-RAM array naturally. Thus, only the memory access control logic needs modification. As shown in the Figure 3, we add a component called "err-PUF control logic". The logic share the same read/write interfaces for normal data access but bypass the ECC component. Thus, when the STT-RAM device enters the mode for PUF verification, cell errors can be captured by err-PUF control logic and processed for verification. The logic consists of several components for different phases of the err-PUF work flow, which is described as follows.

Algorithm 1: Pre-process Phase.

Input : All odd addresses of STT-RAM
Output: Locations of EDPs
for each odd address *Addr* **do**
  Test if cells at *Addr* and *Addr+1* is an EDP ;
  Output *Addr* if true otherwise not;
end

B.1 Pre-process Phase

The pre-process phase includes two steps (Algorithm 1):

- Step-1. Identify all EDPs by scanning all cells in pair.
- Step-2. Store the location information of these EDPs to a database for later PUF verification.

The purpose of this phase is to identify all EDPs in a STT-RAM array after it is fabricated. Then, the location information of these EDPs in the array is stored in a database for later PUF verification. In order to achieve a secure PUF design, there should be enough number of EDPs in the array. Discussions about security are introduced in the subsection C.

Algorithm 2: Enrollment Phase.

Input : N_{sec} EDP locations
Output: Reference responses
Intermediate_Result=0;
for each EDP location *EDP_Addr* **do**
  if less error occurs at *EDP_Addr* than that of *EDP_Addr+1* **then**
    Intermediate_Result=Intermediate_Result+1;
  end
end
Output = 1 if *Intermedia_Result*$\geq \frac{N_{sec}}{2}$ else Output = 0;

B.2 Enrollment Phase

The enrollment phase includes four steps (Algorithm 2):

- Step-1. Randomly select $\mathbf{N_{sec}}$ EDP locations from the database as an input (i.e. a challenge).

- Step-2. When err-PUF receives the input, it will perform **R**-round RWR tests to the correlated EDPs. For each pair of two cells under test, if the first cell has more errors, a bit '0' is generated. Otherwise, a bit '1' is generated.
- Step-3. Add up all N_{sec} bits generated in the last step together and then compare it with $\frac{N_{sec}}{2}$. The comparison result is the final output of PUF circuits.
- Step-4. Store the output to a secure database as a reference.

The purpose of enrollment phase is to find CRPs for PUF verification. Step-2 is to detect which cell in the EDP has a higher bit error rate. Consequently, the selection of R relies on the difference gap of error rates between two cells in an EDP. N_{sec} is a parameter that determines the security strength of our design. We will discuss how to determine N_{sec} in subsection C. It means that there exists trade-off among R, N, and N_{th}. More details about the trade-off is included in Section IV.

Algorithm 3: Evaluation Phase.

Input : One challenge used in the enrollment phase
Output: Responses to be checked
Intermediate_Result=0;
r **for** each EDP location *EDP_Addr* **do**
  if less error occurs at *EDP_Addr* than that of *EDP_Addr+1* **then**
    Intermediate_Result=Intermediate_Result+1;
  end
end
Output = 1 if *Intermedia_Result*$\geq \frac{N_{sec}}{2}$ else Output = 0;

B.3 Evaluation Phase

The evaluation phase includes five steps (Algorithm 3):

- Step-1. Randomly select a challenge generated in the enrollment phase as an input. .
- Step-2. When err-PUF receives the input, it will perform **R**-round RWR tests to the correlated EDPs. For each pair of two cells under test, if the first cell has more errors, a bit '0' is generated. Otherwise, a bit '1' is generated.
- Step-3. Add up the N_{sec} results together and then compare it with $\frac{N_{sec}}{2}$, the comparison result is the output.
- Step-4. Compare the output bit with reference output in the database. If two values are different, it means that the response is incorrect.
- Step-5. Repeat step 1 to step 4 for certain times (e.g. 128) and record the total number of incorrect responses (i.e. Hamming Distance of two multi-bit outputs). If the hamming distance (HD) is below a threshold value, the authentication succeeds. Otherwise, the authentication fails.

C. Security Analysis

err-PUF's security relies on the fact that no one knows the comparative relationship of the error rate within an EDP. Based a single err-PUF output, the probability of guessing all comparative relationships is $2^{-N_{sec}}$. For simplicity, we just set N_{sec} to be 128. If many outputs are obtained by the adversary, the modeling attack [15] can be launched to obtain the comparative relationships. To prevent it, we should ensure the CRP selection space is large enough. Actually, the total number of EDPs (N_{EDP}) is approximately 700 for a typical 1MB STT-RAM design [19]. Thus the space of CRP is $\binom{N_{EDP}}{128}$ which makes the modeling attack costly. In addition, a feed-forward structure can be adopted to further enhance security of err-PUF [16, 11, 10].

TABLE I
SUMMARY OF SIMULATION PARAMETERS

		Parameters	Mean	Standard Deviation
Device Parameters	Transistor	Channel Length L	45nm	2.25nm
		Channel Width W	design dependent	2.25nm
		Threshold Voltage V_{th}	0.466V [1]	δV_{th0}=30mV
	MTJ	MgO Thickness τ	2.2nm	2% of mean
		Cross Section A	$50 \times 130nm^2$ [3]	5% of mean
		Low Resistance R_L	1000Ω	by calculation
		High Resistance R_H	2500Ω	by calculation

	Parameter	Value
Simulation Setup	Data Size	1MB
	Operation Voltage	$0.9 \sim 1.1V$
	Operation Temperature	$275 \sim 325K$
	N, N_{th}, R, N_{sec} #	(3,3,4,128)
	RWR Latency	10ns [3]

IV. EVALUATION

In this section, we present evaluation results to demonstrate that our err-PUF achieves enough reliability. We also evaluate the randomness of err-PUF's output. In addition, we compare err-PUF with previous memory based approach, in respect of hardware overhead, performance, and power consumption. At last, we present the sensitivity analysis of configuration parameters.

A. Experimental Setup

Table I lists detailed experimental setup used in this section. For device-level modeling, we select typical values of state-of-art 1T1J STT-RAM technology to build its error model [22, 19, 3]. We assume that parameters of the MTJ and the control transistor follow Gauss distributions. And the CMOS process variations are independent to MTJ variations because they are manufactured with different processes.

The size of STT-RAM is set to 1MB, which is common in modern SoC design. According to our err-PUF workflow, it is easy to understand that a more reliable PUF is achieved with a larger size of STT-RAM. In subsection C, we will discuss how to determine the minimum size of STT-RAM to design a reliable err-PUF. We set both configuration numbers, N and N_{th} in pre-process phase, to 3. The testing round number R is set to 4 in enrollment and evaluation phases. We provide sensitivity analysis of these configuration numbers in subsection C and discuss how to select proper values for them. The variations of supply voltages and temperatures are set to $0.9V - 1.1V$ and $275K - 325K$.

A simulator is developed to evaluate the reliability of err-PUF. The inputs of our simulator include device-/system-level configurations and the error model of a STT-RAM array. Based on these inputs, it can generate the bit error rate of each cell in the STT-RAM array under different working environments. Then, all three phases in the workflow of err-PUF are simulated using Monte-Carlo method for evaluation. For each authentication process, we use 128 sets of challenges to generate a 128 bit width response. Note that one set of challenge is composed of location information of N_{sec} EDPs in the STT-RAM array. In addition, we use parameters in [3] to estimate the performance

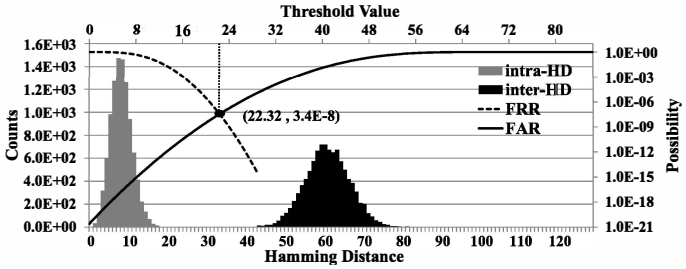

Fig. 4. inter-HD/intra-HD distribution and correlated FAR/FRR curves at 300K, 1.0V

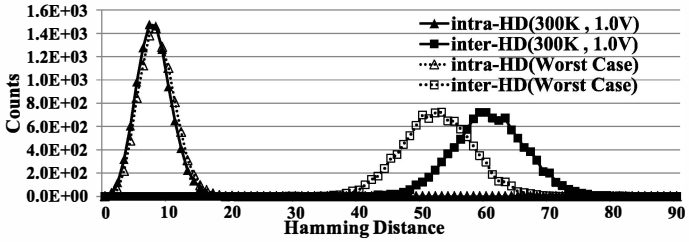

Fig. 5. inter-HD and intra-HD distribution at 300K, 1.0V and the worst case of inter-HD(@1.1V, 275K) and intra-HD(@0.9V, 325K)

and power consumption of err-PUF and compare it to those of other memory based PUF approaches.

B. Evaluation Results

In this subsection, we first demonstrate the reliability of our err-PUF design in a fixed working state. Then, we prove its robustness against considerable environmental variations. We also investigate the randomness of err-PUF's output. Finally, we compare our design with other NVM-based PUFs in respect of hardware overhead, energy consumption, and the latency of evaluation phase.

B.1 Reliability w/o Environmental Variation

The err-PUF is evaluated in a fixed environment state (V = $1.0V$ and T = $300K$) for both enrollment and evaluation phases. In the Monte Carlo simulation, 10000 sets of challenges are used. The experimental results of intra-HD and inter-HD in our experiments are illustrated in Figure 4. The mean value of intra-HD is 7.76 with a variance of 7.29. For inter-HD, the mean value is 60.56 and the variance is 32.31. Based on these distributions, we can generate results of False Acceptance Rate(FAR) and False Rejection Rate(FRR) with different thresholds [9], which is also shown in Figure 4. From the results, we have the minimum max(FAR, FRR)=3.4×10^{-8} when the threshold is set to 22.32. If we set the threshold at 23, the FAR and FRR are still less than 1×10^{-7}. Thus, it is acceptable for authentication for a large population of STT-RAM devices [9, 16].

B.2 Reliability with Environment Vibration

In this subsection, we first set the working state with V = $1.0V$ and T = $300K$ for the enrollment phase to get the reference. Then we explore the worst case of evaluation phase when both variations are considered to demonstrate the reliability of err-PUF. By exhausted experiments, we find that the worst case (highest FAR and FRR) happens at the state-A (V = $1.1V$, T = $275K$) for inter-HD and state-B (V = $0.9V$, T = $325K$) for intra-HD, which is shown in Figure 5. We can see that there is a obvious bias of inter-HD distribution. But even in the worst case, we have FAR=6.2×10^{-8} and FRR=1.3×10^{-7}, when the threshold is selected as 23. In conclusion, we can set the threshold as 23 to ensure FAR and FRR below 1×10^{-7} even with environmental variation.

B.3 Randomness of err-PUF

Note that there is nearly no overlap between different STT-RAM arrays' EDP positions, thus the false PUF will always output 0 with the same input of location information. Therefore, the inter-HD can present the randomness of our PUF's outputs which is shown in Figure 4. We can find that there is a slight bias between our result and the ideal one whose mean value should be 64. Despite the slight bias, the guessing probability of err-PUF's 128-bit output is still very low(about 2^{-118})

B.4 Comparison Results with other NVM-based PUFs

In order to compare err-PUF with other typical NVM-based PUFs, we synthesize a prototype of our err-PUF control logic with the 45nm technology. Results of other PUFs are listed in Table II by estimation or by references. Our hardware cost is trivial mainly because we share most hardware with existing structure including the Read/Write control logic and STT-RAM cells. The only cost comes from little extra multiplexors and adders. Also, the test rounds of evaluation phase in our design are substantially fewer than those of SRAM PUF or FPUF. In the evaluation phase, only the cells within EDPs are being read or written, which reduces the dynamic power of our design. Note that we assume that the read/write width of the STT-RAM array is 512-bit. And the energy consumption and latency are calculated when 128-bit response is generated.

C. Configuration Sensitivity Analysis

In this subsection, we present the sensitivity analysis of configurations for N, N_{th}, and R. Since these numbers affect the performance of err-PUF, the basic goal is to minimize these numbers with a constraint of FAR and FRR.

Apparently, the error rate difference of an EDP increases statistically with a higher (N,N_{th}). Thus, a smaller R is needed to detect the difference of error rates of an EDP in enrollment and evaluation phases. In order to quantitatively explore relationship between (N,N_{th}) and R, we investigate the R for different configurations of $(N,N_{th}) \in (1,1),(2,1),(2,2),(3,1),(3,2),(3,3),(4,4),(5,5)$. For the same constraint of FAR and FRR, the results of R are listed in Figure 6 (a). It is easy to find that we only need about two rounds of test in enrollment and evaluation phase when we have $(N,N_{th}) \in (4,4),(5,5)$.

However, as we discussed in Section III, the number of EDPs in a STT-RAM array decreases when we increase (N,N_{th}). We investigate the minimum size of STT-RAM to find enough EDPs for different configurations and list them in Figure 6(b). The results show that, under the same error model, we cannot find enough EDPs when $(N,N_{th}) = (5,5)$. Consequently, we need to select a proper (N,N_{th}) under the constraint of $N \leq 4$.

The FAR and FRR of different configurations are listed in Figure 6(c). Although we can have the smallest R with

TABLE II
COMPARISON RESULTS BETWEEN NVM-BASED PUFS

	STT-PUF[20]	PCM PUF[21]	Memristor PUF[14]	FPUF[13]	err-PUF
Technology Node	45nm	45nm	45nm	45nm	45nm
Extra Circuit Area (μm^2)	5.5×10^3	1.7×10^3	9.1×10^3	3.3×10^2	2.9×10^2
Evaluation Phase Latency (μs)	7.18	12.8	10.1	1.5×10^7	2.32
Energy Consumption (pJ)	4.1×10^2	1.1×10^3	9.0×10^4	4.8×10^4	3.1×10^2

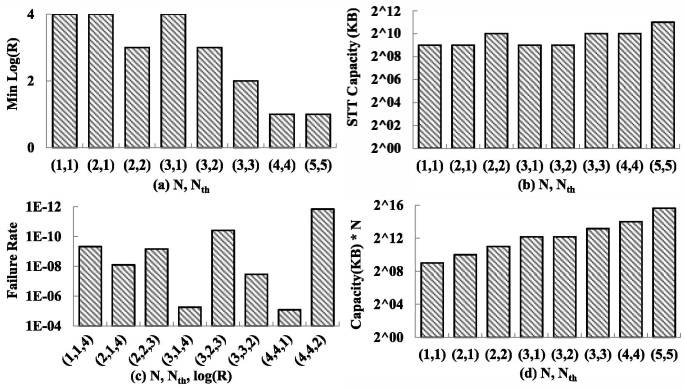

Fig. 6. Diagrams for sensitivity analysis

$(N,N_{th}) = (4,4)$, the smallest failure rate is achieved when we have $(N,N_{th},R) = (3,3,4)$. Meanwhile, as shown in Figure 6(d), when $(N,N_{th}) = (3,3)$, the product of capacity and N is also smaller than that when $(N,N_{th}) = (4,4)$. It indicates that the preprocess is faster when $(N,N_{th}) = (3,3)$. Thus, $(3,3,4)$ should be the best parameters for (N,N_{th},R).

As a summary, there is a trade-off among performance, false rate, and minimum size of STT-RAM to implement err-PUF. A proper configuration depends on the requirements of a real case.

V. CONCLUSIONS

With a careful study of STT-RAM cell error rates, we show that they can be employed for PUF design. We also address that the major challenge comes from environmental variations. Based on the concept of EDP, we overcome it and propose a reliable err-PUF. Compared with existing approaches, our err-PUF can achieve higher performance, lower energy consumption, and comparable design overhead.

REFERENCES

[1] Predictive technology model (ptm). http://www.eas.asu.edu/ ptm/.

[2] W. Che, J. Plusquellic, and S. Bhunia. A non-volatile memory based physically unclonable function without helper data. In *Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on*, pages 148–153. IEEE, 2014.

[3] K. C. Chun, H. Zhao, J. D. Harms, T.-H. Kim, J.-P. Wang, and C. H. Kim. A scaling roadmap and performance evaluation of in-plane and perpendicular mtj based stt-mrams for high-density cache memory. *Solid-State Circuits, IEEE Journal of*, 48(2):598–610, 2013.

[4] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Fpga intrinsic pufs and their use for ip protection. In *Cryptographic Hardware and Embedded Systems-CHES 2007*, pages 63–80. Springer, 2007.

[5] D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *Computers, IEEE Transactions on*, 58(9):1198–1210, 2009.

[6] A. Iyengar, K. Ramclam, and S. Ghosh. Dwm-puf: A low-overhead, memory-based security primitive. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pages 154–159, May 2014.

[7] W. Kang, L. Zhang, J.-O. Klein, Y. Zhang, D. Ravelosona, and W. Zhao. Reconfigurable codesign of stt-mram under process variations in deeply scaled technology. 2015.

[8] W. Kang, W. Zhao, J.-O. Klein, Y. Zhang, C. Chappert, and D. Ravelosona. High reliability sensing circuit for deep submicron spin transfer torque magnetic random access memory. *Electronics Letters*, 49(20):1283–1285, 2013.

[9] P. Koeberl, J. Li, R. Maes, A. Rajan, C. Vishik, M. Wójcik, and W. Wu. A practical device authentication scheme using sram pufs. *Journal of Cryptographic Engineering*, 2(4):255–269, 2012.

[10] S. Konigsmark, L. Hwang, D. Chen, and M. Wong. Cnpuf: A carbon nanotube-based physically unclonable function for secure low-energy hardware design. In *Design Automation Conference (ASP-DAC), 2014 19th Asia and South Pacific*, pages 73–78, Jan 2014.

[11] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on*, pages 176–179. IEEE, 2004.

[12] D. Nedospasov, J.-P. Seifert, C. Helfmeier, and C. Boit. Invasive puf analysis. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*, pages 30–38, Aug 2013.

[13] P. Prabhu, A. Akel, L. M. Grupp, S. Y. Wing-Kei, G. E. Suh, E. Kan, and S. Swanson. Extracting device fingerprints from flash memory by exploiting physical variations. In *Trust and Trustworthy Computing*, pages 188–201. Springer, 2011.

[14] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak. Nano-ppuf: A memristor-based security primitive. In *VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on*, pages 84–87. IEEE, 2012.

[15] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 237–249. ACM, 2010.

[16] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, pages 9–14. ACM, 2007.

[17] N. Tega, H. Miki, T. Osabe, A. Kotabe, K. Otsuga, H. Kurata, S. Kamohara, K. Tokami, Y. Ikeda, and R. Yamada. Anomalously large threshold voltage fluctuation by complex random telegraph signal in floating gate flash memory. In *Electron Devices Meeting, 2006. IEDM'06. International*, pages 1–4. IEEE, 2006.

[18] J. Valamehr, T. Huffmire, C. Irvine, R. Kastner, Ç. K. Koç, T. Levin, and T. Sherwood. A qualitative security analysis of a new class of 3-d integrated crypto co-processors. In *Cryptography and Security: From Theory to Applications*, pages 364–382. Springer, 2012.

[19] W. Wen, Y. Zhang, Y. Chen, Y. Wang, and Y. Xie. Ps3-ram: A fast portable and scalable statistical stt-ram reliability analysis method. In *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE*, pages 1187–1192, 2012.

[20] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy. Highly reliable memory-based physical unclonable function using spin-transfer torque mram. In *Circuits and Systems (ISCAS), 2014 IEEE International Symposium on*, pages 2169–2172. IEEE, 2014.

[21] L. Zhang, Z. H. Kong, and C.-H. Chang. Pckgen: A phase change memory based cryptographic key generator. In *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on*, pages 1444–1447. IEEE, 2013.

[22] Y. Zhang, X. Wang, and Y. Chen. Stt-ram cell design optimization for persistent and non-persistent error rate reduction: A statistical design view. In *Computer-Aided Design (ICCAD), 2011 IEEE/ACM International Conference on*, pages 471–477, 2011.