Highly Reliable Memory-based Physical Unclonable Function Using Spin-Transfer Torque MRAM

Le Zhang*, Xuanyao Fong†, Chip-Hong Chang*, Zhi Hui Kong* and Kaushik Roy†
*School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
†Department of Electrical and Computer Engineering, Purdue University, USA

***Abstract*—In recent years, Physical Unclonable Function (PUF) based on the inimitable and unpredictable disorder of physical devices has emerged to address security issues related to cryptographic key generation. In this paper, a novel memory-based PUF based on Spin-Transfer Torque (STT) Magnetic RAM, named as STT-PUF, is proposed as a key generation primitive for embedded computing systems. By comparing the resistances of STT-MRAM memory cells which are initialized to the same state, response bits can be generated by exploiting the inherent random mismatches between them. To enhance the robustness of response bits regeneration, an Automatic Write-Back (AWB) technique is proposed without compromising the resilience of STT-PUF against possible attacks. Simulations show that the proposed STT-PUF is able to produce raw response bits with uniqueness of 50.1% and entropy of 0.985 bit per cell. The worst-case Bit-Error Rate (BER) under varying operating conditions is 6.6×10^{-6}.**

I. Introduction

Physical Unclonable Function (PUF) utilizes the inimitable disorder of device properties stemming from the ineluctable fabrication variations to generate a unique and unpredictable output (known as *response*) when interrogated by an input (known as *challenge*) [1]–[4]. Responses generated from the PUF by the same challenge need to be repeatable in the presence of noise and robust under varying operational and environmental conditions. Error Correction Codes (ECCs) have been widely used as an efficient method to reconcile the noisy responses [5], [6] so as to enhance the reliability of PUF, but design/test complexity or chip-area will be compromised.

Emerging Non-Volatile Memories (NVMs) such as Phase Change Memory (PCM), Spin-Transfer Torque MRAM (STT-MRAM), etc., are gaining significant research interest owing to their superiority in terms of low bit cell footprint, low power consumption, and high scalability [7], [8]. Technology scaling for NVM increases the process variations, which provide new opportunities to the design of Memory-based PUF (MPUF). The unique features of emerging NVMs may help to overcome certain limitations of MPUFs designed based on conventional CMOS technology.

In this paper, we propose a new MPUF utilizing a hybrid STT-CMOS technology, namely STT-PUF, which is capable of producing reliable responses for secure key generation with marginal design overhead. By using an automatic write-back scheme, the STT-PUF can regenerate stable responses securely under varying operating conditions by sensing the resistance difference between two STT-MRAM cells in complementary states, which significantly relaxes the STT-PUF's reliance on ECC for reliability enhancement.

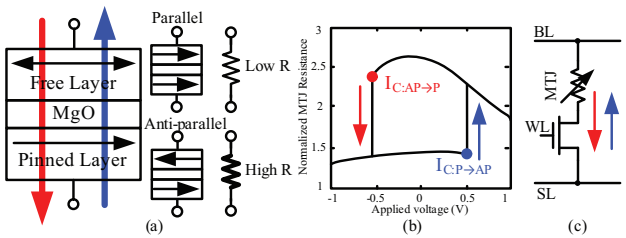

Fig. 1. (a) MTJ device structure and resistance model; (b) resistance-voltage characteristics of MTJ device. State switching happens when current through the MTJ device is large enough, i.e., $AP \to P$ when $I > I_{C:AP\to P}$ and $P \to AP$ when $I > I_{C:P\to AP}$; (c) 1T1R STT-MRAM cell structure.

The rest of this paper is organized as follows. Section II presents preliminaries for understanding the STT-PUF. The design and reliability enhancement technique of the proposed STT-PUF are described in Section III. Section IV presents the quality evaluations and security analysis on the proposed STT-PUF. Finally, Section V concludes the paper.

II. Fundamentals of Spin-Transfer Torque MRAM

STT-MRAM is a promising candidate for the implementation of low-power, high-performance universal memory. The storage device of STT-MRAM is the Magnetic Tunnel Junction (MTJ) (Fig. 1(a)), which is formed by two ferromagnetic layers sandwiching a thin tunnel barrier: one of the ferromagnetic layer is magnetically pinned (which we call PL) while the other is free (which we call FL). The resistance of the MTJ is high (denoted as R_H or R_{AP}, representing logic "1") when the magnetization directions of PL and FL are anti-parallel (AP), and low (R_L or R_P, representing logic "0") if they are parallel (P) (see Fig. 1(a)). The distinguishability of the AP and P states is given by the Tunnel Magnetoresistance Ratio (TMR), defined as $(R_{AP} - R_P)/R_P$. FL magnetization may be switched by passing a current which is larger than the critical current, I_C, through the MTJ. This phenomenon is illustrated in Fig. 1(b). Fig. 1(c) shows the basic STT-MRAM memory cell commonly used for high density memory applications.

Technology scaling results in significant process variations that affect the operation of STT-MRAM. Two main sources of process parameter variations we consider in the MTJ are 1) cross-sectional area ($area$) and 2) oxide layer thickness

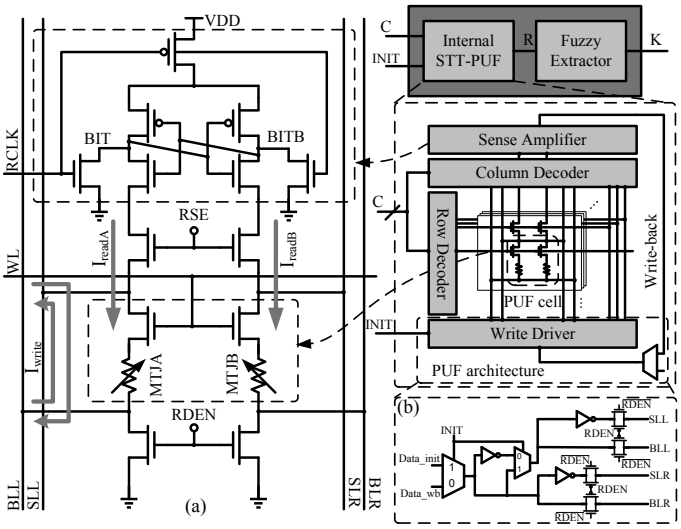

Fig. 2. STT-PUF circuits and system. (a) 2T2R STT-PUF cell and sense amplifier. Responses generated from inner STT-PUF are post-processed by a Fuzzy Extractor to produce the final keys (as shown in the top-right corner); (b) Write driver. $INIT$ is set to switch the phase of STT-PUF between *enrollment* and *regeneration*.

($tMgO$) [9]. It was found that the MTJ resistance is related to $area$ and $tMgO$ by

$$RA \propto \left(e^{a_0 t_{MgO}+b_0} + \sum_{m=1}^{c} (-1)^{m-1} V_{MTJ}^{2m} e^{a_m t_{MgO}+b_m} \right)^{-d} \quad (1)$$

where RA is the resistance-area product, a_0, b_0, a_m, b_m, c and d are the parameters calibrated against experimental data [10], and V_{MTJ} is the biasing voltage of the MTJ. Variations in both $area$ and $tMgO$ affect the distributions of R_P and R_{AP}, and variations in $tMgO$ also affect TMR [9]. Apart from the MTJ device, variations in the access transistor (e.g., V_{th}, etc.) also influence the dynamics of the STT-MRAM cell.

III. Proposed STT-PUF

A. Circuits and Principles

Due to process variations, random bits can be generated by comparing the resistances of two MTJs initialized to the same state. Therefore, the proposed STT-PUF is built by modifying the conventional STT-MRAM array in a way such that the memory address and the cell data are the challenge (c) and response bit (r), respectively (Fig. 2). Each STT-PUF cell consists of two STT-MRAM cells (2T2R). During a read operation, the STT-PUF cell is selected by RSE and WL (STT-PUF challenge), and the MTJ elements, MTJ_A and MTJ_B, are initialized to the same state, AP or P. The output of the sense amplifier is determined by the resistance mismatch between the MTJs in the STT-PUF cell during the read operation. The output bits, which are the raw responses of STT-PUF, are then post-processed by a Fuzzy Extractor [11] to produce the cryptographic key.

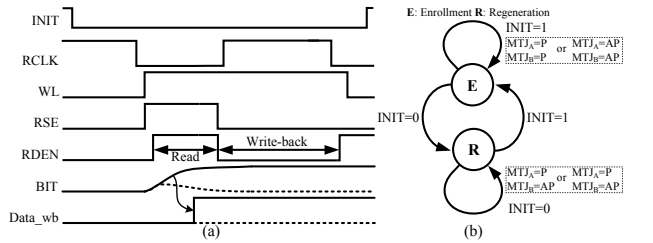

Fig. 3. (a) Timing diagram of the AWB; (b) state diagram of STT-PUF.

B. Automatic Write-Back Scheme

The reliability and repeatability of responses generated by PUFs are often deteriorated by noise and operating condition fluctuations. An Automatic Write-Back (AWB) scheme [12] exploiting the non-volatility of STT-MRAM is proposed to enhance the reliability of the STT-PUF (Fig. 2(b)). With the incorporation of the AWB, the STT-PUF operates in two phases:

- *Enrollment* phase: In this phase, MTJs in an STT-PUF cell are initialized ($INIT = 1$) to the same state of either AP or P. A response bit is then generated by sensing the mismatch of MTJ resistances in the selected STT-PUF cell. Upon completion of the read operation, the bit sensed from the cell is automatically written back to the MTJs, i.e., the MTJs are set to complementary states corresponding to the write-back data bit.
- *Regeneration* phase: In this phase, $INIT$ is set to zero. Since the response bit of the cell has been written back after enrollment and stored as the complementary MTJ states in the STT-PUF cell, the response bit can be robustly reproduced when the STT-PUF cell is addressed by the same challenge.

The timing diagram and state transition of STT-PUF incorporated with AWB scheme is shown in Fig. 3(a) and (b), respectively.

IV. Analysis on the Quality of STT-PUF

The quality of proposed STT-PUF was evaluated and analyzed using 45 nm bulk CMOS Predictive Technology Model (PTM) and a 40 nm compact MTJ device model [10] based on a simulation framework shown in Fig. 4. The process parameters that are considered as random variables and electrical parameters used in the simulation are tabulated in Table I. Other relevant device parameters and their corresponding values were extracted from [10] and [13].

A. Uniqueness and Randomness

The uniqueness of STT-PUF responses evaluates *how the change in PUF challenge affects its response bits*. It can be evaluated by calculating the fractional Hamming distance (H) given as

$$H = \frac{2l}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \mathsf{HD}(R_i, R_j) \quad (2)$$

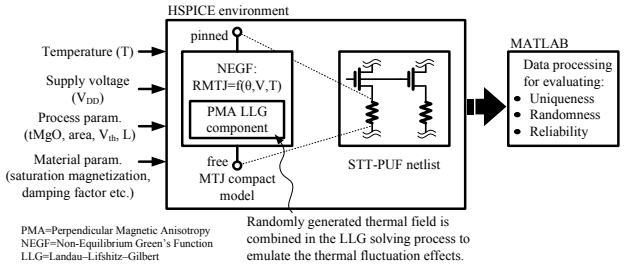

Fig. 4. Simulation framework.

TABLE I
GAUSSIAN DISTRIBUTED PROCESS PARAMETERS AND ELECTRICAL PARAMETERS.

Parameters	μ	σ/μ
MTJ contact area ($Area$)	40×116 nm^2	5%
MgO layer thickness ($tMgO$)	1.15 nm	2%
MOSFET channel length (L)	45 nm	10%
MOSFET threshold voltage (V_{th})	0.466 V	10%
Supply voltage (V_{DD})	1 V	-
Read cycle	10 ns	-
Write cycle	40 ns	-

where R_i and R_j are l-bit response strings, i.e., $R = r_1||r_2||\dots r_{l-1}||r_l$, and each of the response bits, r, is generated from an STT-PUF cell selected by a random challenge. m is the sample size of the generated response strings. The operator $\mathsf{HD}(.,.)$ computes the Hamming distance between two binary strings. We instantiated a 64×1024 STT-PUF array, and generate two groups of 1000 64-bit (i.e., $m = 1000$, $l = 64$) responses from the array by randomly selecting STT-PUF cells. One group contains cells that are initialized to P state and the other to AP state. To evaluate the impact of V_{MTJ} as formulated in Eq. 1, the supply voltage was varied so as to indirectly change V_{MTJ} in the STT-PUF cells. The results are plotted as histograms in Fig. 5. The fractional Hamming distances for all the six cases are very close to 50% and their mean value is 50.1%.

A high degree of response uniqueness (when H is close to 50%) results in a low probability that two different challenges will yield identical responses. Assuming the number of different bits in two 64-bit raw responses generated from randomly chosen challenges are distributed binomially, the probability that there are more than p identical bits in the responses is

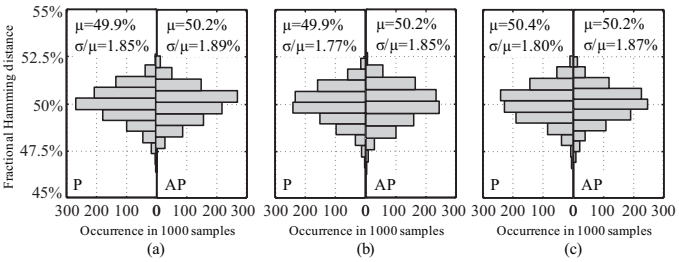

Fig. 5. Histograms of calculated fractional Hamming distances when V_{DD} is (a) 0.9 V, (b) 1 V, and (c) 1.1 V.

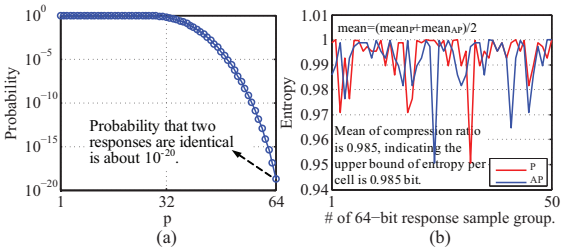

Fig. 6. (a) The relationship between the probability of finding two identical responses and the length of the responses, given an estimated average Hamming distance of 49.9%; (b) estimated average entropies for the 50 sample groups of 64-bit responses.

$\mathsf{F}(64-p, 64, 0.501)$, where $\mathsf{F}(t,n,e) = \sum_{i=0}^{t} \binom{n}{t} e^i (1-e)^{n-i}$ is the binomial cumulative distribution function. We calculated this probability by varying p and the results were plotted in Fig. 6(a). It can be seen that the probability of producing two identical responses, i.e., $p = 64$, is extremely low ($\sim 10^{-20}$).

The randomness of l-bit response is evaluated by its entropy E, which can be computed by the entropy equation:

$$E = -\sum_{R \in \mathcal{R}} log(\mathbf{Pr}(R))\mathbf{Pr}(R) \tag{3}$$

where $\mathcal{R} = \{0,1\}^l$ is the response space. It is non-trivial to evaluate E directly by using Eq. 3 when the size of $\mathcal{R}$ is large (i.e., $l = 64$ in our case). An alternative method is to utilize the Context Tree Weighting (CTW) algorithm [11], which estimates the compression ratio of random sources, to approximate the upper bound of entropy. A sample group of 2000 64-bit responses was formed by randomly selecting cells from the STT-PUF, and a total of 50 such sample groups were generated. Their estimated compression ratios were computed by means of CTW algorithm and shown in Fig. 6(b). The mean compression ratio is 0.985, which indicates that the upper bound of entropy contained in each cell is 0.985 bit on average.

The raw responses are subsequently processed by the Fuzzy Extractor, in which a hash function is incorporated to further enhance the uniqueness and randomness [5].

B. Reliability

Reliability quantifies the reproducibility of PUF responses to the same challenge. More specifically, it analyses the probability of response, r_t, generated from the PUF under certain configuration state at time t, to be reproduced as $r_{t+\delta t}$ at time ($t + \delta t$ where $\delta t > 0$) with the same challenge, i.e., $r_t = r_{t+\delta t}$. We consider three different cases for STT-PUF reliability estimation:

1) *Case #1*: r_t and $r_{t+\delta t}$ are both generated in the enrollment phase. In this case, STT-PUF can be regarded as operating without AWB.
2) *Case #2*: r_t is generated in the enrollment phase while $r_{t+\delta t}$ is generated in the subsequent regeneration phase.
3) *Case #3*: r_t and $r_{t+\delta t}$ are both generated in the regeneration phase.

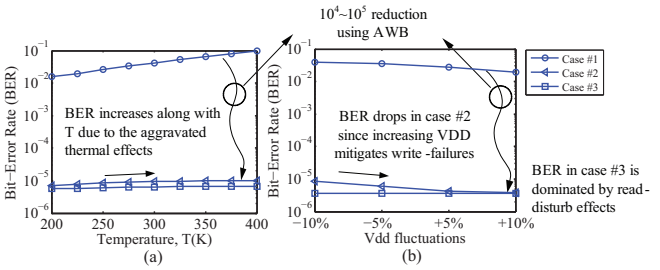

Fig. 7. Estimated BER of STT-PUF under different (a) temperatures (V_{dd} = 1 V) and (b) supply voltage fluctuations (temperature=300 K).

The reliability of response regeneration in case #1 is mainly affected by the thermal noise, whereas operational interruptions such as occasional write-back failure, sense failure and read-disturb, jeopardize the reliability of case #2 and case #3. The contributing factors to operational interruptions include the random distribution of initial angle of FL precession around the easy-axis in an MTJ, which in turn results in a spread of MTJ magnetization switching time [13]; and *thermal fluctuations*, which causes MTJ switching to be a stochastic process [13]. As a consequence, write-failure and read-disturb may degrade the reliability of the STT-PUF. Sense-failures may occur in the presence of thermal noise effects, and/or due to a small TMR which makes it difficult to distinguish between R_{AP} and R_P. In addition, operating condition (i.e., ambient temperature and supply voltage) may also affect these failure modes [13] and therefore triggers reliability issues in STT-PUF.

The three cases were simulated using a combination of Monte Carlo and response modeling methods [10], and the Bit-Error Rate (BER) ($1 - \textit{reliability}$) was obtained as the percentage of cells that produce unreliable bits. BER for initial states of both P (BER_P) and AP (BER_{AP}) were considered, and the average BER, i.e. $(\text{BER}_P + \text{BER}_{AP})/2$, under varying operating conditions were estimated and shown in Fig. 7(a) and (b). The BER of STT-PUF without AWB (case #1) is in the range of 1%~10%, whereas the STT-PUFs incorporated with AWB (cases #2 and #3) can achieve much lower BER[1]($\sim 10^{-6}$). The overall BER for STT-PUF with the proposed AWB can be obtained by summing the values in case #2 and #3, which is $\leq 6.6 \times 10^{-6}$. Note a low BER greatly relaxes the burden of chip design by reducing the complexity of ECC decoder hence, reduces the chip area [6].

C. Efficiency and Security

1) Uniqueness in comparison to other NVMs: STT-PUF with AWB scheme has several advantages: a) MTJ device has *unlimited endurance* so that the PUF reliability degradation due to frequent write-back operations is minimized; b) Unlike other NVMs such as PCMs, storage element of STT-MRAM, i.e., MTJ, relies on the spin polarized current for state switching, which happens completely inside the device. Therefore, accidental disturbance on adjacent cells during the write-back operation can be avoided [8].

2) Robustness to tampering activities: Write operations *only occur during the write-back and the initialization*. Therefore, intentional writing of bits into PUF cells is fully restricted. In addition, physical probing into inner nodes and wire, or measuring MTJ resistances to obtain secret bit from each PUF cell is extremely difficult if not impossible [14].

3) Resilience against side-channel attacks: Using electromagnetic emanations to obtain the write-back bits is infeasible because write operations on MTJ does not rely on large external magnetic field that may be precisely measured [8].

[1]The industrial standard of BER for cryptographic key is in the order of 10^{-6}. For the raw PUF responses that do not meet this requirement, certain type of ECC must be applied.

V. Conclusion

In this paper, a novel STT-PUF based on STT-MRAM is proposed. Simulation results show that the STT-PUF is capable of generating response bits with desirable randomness. The BER of the STT-PUF has been verified to be low by incorporating the AWB scheme under varying operating conditions. The high entropy contained in each cell and high reliability of response regeneration make the proposed STT-PUF a suitable candidature for embedded key generation primitive that necessitates lower chip area and hardware complexity when compared to the conventional PUFs.

References

[1] G. Suh *et al.*, "Physical unclonable functions for device authentication and secret key generation," in *IEEE DAC*, Jun. 2007, pp. 9–14.

[2] Y. Su, J. Holleman, and B. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan. 2008.

[3] G. Selimis *et al.*, "Evaluation of 90nm 6T-SRAM as physical unclonable function for secure key generation in wireless sensor nodes," in *IEEE ISCAS*, 2011, pp. 567–570.

[4] S. Katzenbeisser *et al.*, "PUFs: Myth, fact or busted? a security evaluation of physically unclonable functions (PUFs) cast in silicon," in *CHES*, Sept. 2012, pp. 283–301.

[5] Y. Dodis *et al.*, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *EuroCrypt*, May 2004, pp. 523–540.

[6] C. Bösch *et al.*, "Efficient helper data key extractor on FPGAs," in *Proc. Workshop on Cryptographic Hardware and Embedded Syst.*, Washington, DC, USA, Aug. 2008, pp. 181–197.

[7] H. Wong *et al.*, "Phase change memory," *Proc. IEEE*, vol. 98, no. 12, pp. 2201–2227, 2010.

[8] S. A. Wolf *et al.*, "The promise of nanomagnetics and spintronics for future logic and universal memory," *Proc. IEEE*, vol. 98, no. 12, pp. 2155–2168, 2010.

[9] J. Li *et al.*, "Design paradigm for robust spin-torque transfer magnetic RAM (STT MRAM) from circuit/architecture perspective," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1710–1723, 2010.

[10] X. Fong *et al.*, "Bit-cell level optimization for non-volatile memories using magnetic tunnel junctions and spin-transfer torque switching," *IEEE Trans. Nanotechnol.*, vol. 11, no. 1, pp. 172–181, 2012.

[11] F. Armknect *et al.*, "A formal foundation for security features of physical functions," in *IEEE SP*, May 2011.

[12] Y. Morita *et al.*, "An area-conscious low-voltage-oriented 8t-SRAM design under DVS environment," in *IEEE VLSIC*, 2007, pp. 256–257.

[13] N. Narayan Mojumder and K. Roy, "Proposal for switching current reduction using reference layer with tilted magnetic anisotropy in magnetic tunnel junctions for spin-transfer torque (STT) MRAM," *IEEE Trans. Electron Devices*, vol. 59, no. 11, pp. 3054–3060, 2012.

[14] U. Rührmair *et al.*, "Modeling attacks on physical unclonable functions," in *ACM CCS*, Oct. 2010, pp. 237–249.