Adiabatic/MTJ based Physically Unclonable Function for Consumer Electronics Security

Zachary Kahleifeh, *Student Member, IEEE* and Himanshu Thapliyal, *Senior Member, IEEE*, Syed M. Alam, *Senior Member, IEEE*

***Abstract*—Consumer electronics require secure operation in the face of the many emerging threat vectors. One hardware security primitive is the Physically Unclonable Function (PUF). PUFs utilize process variations to give a device a digital fingerprint and are an important resource in secure hardware. One drawback of the addition of secure hardware is the increased energy consumption. In this paper, we look to design a secure, low-energy PUF using both adiabatic logic and Magnetic Tunnel Junctions (MTJ). Adiabatic logic reduces the dynamic energy consumption of the PUF while the MTJs offer a near zero-leakage power, non-volatile memory option. MTJs have two stable states depending on the magnetization direction of the free layer with respect to that of the fixed layer. Hence, the proposed adiabatic/MTJ PUF offers two modes of operation depending on the orientation of the MTJ. Our proposed adiabatic/MTJ PUF has average reliability of 97.07% and 96.97% between the two modes of operation while taking into account temperature, supply voltage, and TMR variations. The two modes of our proposed PUF consume 5.2 fJ and 5.1 fJ per bit.**

***Index Terms*—Hardware security, Low-energy, Magnetic tunnel junction (MTJ), Adiabatic logic, CMOS/MTJ, Physically Unclonable Functions (PUF)**

I. Introduction

Consumer electronic devices such as those found in the Internet of Things (IoT) ecosystem are a part of a rapidly growing environment that is expected to reach 125 billion devices by 2030 [1]. Many of these devices are expected to occupy homes in the form of smart electronics as well as in the industrial sector [2]. Many consumer electronics are portable and thus energy consumption is an important design consideration.

Furthermore, security is a major issue with consumer electronic devices. There is close to $600 billion lost to cybercrime each year [3]. This alarming amount has raised the need for secure hardware implementations as an added layer of defense. Numerous companies and researchers have proposed dedicated secure hardware implementations to defend against cyber-physical attacks [4]. One security primitive that can be used for secure hardware is the Physically Unclonable Function (PUF). A PUF is a device that uses inherent variations in the manufacturing procedure to create a unique and unclonable identification. PUFs have been shown to be useful secure devices in numerous applications such as smart grids, medical devices, and wireless transceivers [5]–[7].

Security primitives such as PUFs can consume substantial energy. The Bulk-MOSFET-based CMOS circuits that typically makeup PUF circuits consume substantial dynamic energy. Furthermore, as transistor technology size scales down the leakage power increases at a substantial rate. To this end, we explore the use of adiabatic logic to reduce dynamic energy and Magnetic Tunnel Junctions (MTJ) to reduce leakage power. Thus, we propose a PUF based on both adiabatic logic and MTJs. Adiabatic logic is a low-energy design technique that saves energy by recycling unused energy from the load capacitor back into the power clock to be reused again in the next cycle. Adiabatic logic can be combined with MTJs to form hybrid adiabatic/MTJ circuits [8]. MTJs are non-volatile storage elements that have near-zero leakage power, high integration density, and easy compatibility with CMOS [9]–[11].

In this paper, we propose a combination of adiabatic logic and MTJs to design a low energy and secure PUF. The source of process variation will be dominated by the variation of the MTJs. MTJs have two stable states depending on the magnetization direction of the free layer with respect to the fixed layer, i.e, either parallel or anti-parallel. Accordingly, the proposed PUF have two operation modes that result in different responses. PUF metrics such as uniformity, uniqueness, and reliability are simulated and presented in this paper. When in the parallel orientation, our PUF has a uniformity of 50.18%, a uniqueness of 49.98% and average reliability of 97.07%. When in an anti-parallel orientation, our proposed PUF has a uniformity of 50.17%, a uniqueness of 49.99% and average reliability of 96.97%. Furthermore, our proposed adiabatic/MTJ PUF has an energy consumption of 5.2fJ and 5.1fJ per bit for the parallel and anti-parallel orientations, respectively.

The rest of the paper is organized as follows. Section II contains background information on Magnetic Tunnel Junctions, Adiabatic Logic, and Physically Unclonable Functions. Section III presents our proposed adiabatic/MTJ PUF and explains its operation. Section IV goes into detail on our simulation results of our proposed PUF. Section V compares the results of our proposed PUF with other PUFs in the literature. Section VI concludes the paper.

Zachary Kahleifeh is currently a PhD candidate in the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY 40506, USA.

Himanshu Thapliyal is currently with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA. (e-mail: hthapliyal@ieee.org).

Syed M. Alam is currently with Everspin Technologies Inc., Austin, Texas, USA

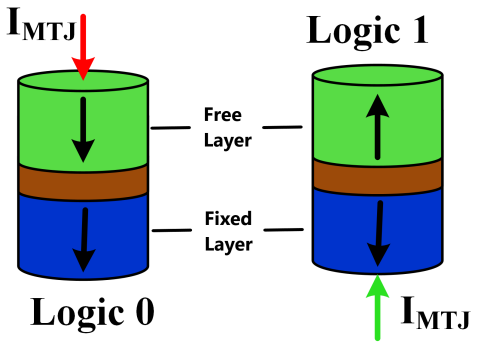


Fig. 1: Structure of Magnetic Tunnel Junction with Spin Transfer Torque (STT) switching.

II. Background

This section presents the background information required to understand the structure and operation of the proposed adiabatic/MTJ PUF.

A. Magnetic Tunnel Junction

MTJs are non-volatile spintronic-based memories. The structure of MTJs consists of two ferromagnetic (FM) layers and a thin oxide layer that separates the two FM layers [12]. For MTJs to act as storage elements, one of the FM layers is fixed to a certain magnetization (referred to as the fixed layer) while the remaining layer (referred to as the free layer) is free to take either a parallel or anti-parallel magnetization with respect to the fixed layer [13].

This can be seen in Figure 1 as the bottom layer of the MTJ is fixed and the top layer is free to take a direction either parallel or anti-parallel to the fixed layer. Information is stored in the form of resistance differences between the two orientations of the MTJ. If the MTJ shows a parallel magnetization (R_P) then it will have lower resistance than when it has an anti-parallel magnetization (R_{AP}) [14]. The MTJ structure and two configurations are shown in Figure 1. Figure 1 also shows the current required to switch the MTJ using the STT effect [15], [16]. The STT effect involves a spin-polarized current inducing a torque that switches the direction of the MTJ free layer.

An important property of MTJs is the tunnel magnetoresistance ratio (TMR) which is given as $TMR = (R_{AP} - R_P)/R_P$. MTJs with higher TMR have been shown to have greater reliability and implementation capability in high-speed MRAM [17], [18]. Table I contains the MTJ device parameters used in the simulations of the proposed adiabatic/MTJ PUF. In Table I, σ represents a variable that follows a Gaussian distribution with $\sigma = 3\%$.

The MTJ is the dominating source of process variation within our proposed adiabatic/MTJ PUF. Thus, it is important to verify the variations are substantial enough to produce strong randomness. Within an MTJ there are many sources of uncontrolled process variation such as the oxide thickness, free layer thickness, and the TMR ratio [19]. The variations of the aforementioned sources can lead to a variation in the resistance of the MTJ device. This can be seen in the resistance equation (Equation 1) specified by the model used in the simulations of our proposed design where t_{ox} is the oxide thickness, F is a fitting parameter, $\overline{\psi}$ is the average potential barrier height of MgO, coef is a fitting parameter, and Area is the area of the MTJ [20]. Figure 2 shows the variation of resistance that occurs within MTJs based on 200 Monte Carlo simulations.

TABLE I: Magnetic Tunnel Junction parameters used in simulations. σ represents a parameter that follows a Gaussian distribution with $\sigma = 3\%$.

Parameter	Description	Value
t_{sl}	Thickness of free layer	σ1.3nm
a	Length of surface long axis	40nm
b	Width of surface short axis	40nm
r	Radius of MTJ	20nm
t_{ox}	Thickness of the Oxide barrier	σ0.85nm
TMR	Tunnel Magnetoresistance ratio	σ200%
RA	Resistance Area Product	5 $\Omega\mu^2$
F	Fitting parameter that is a function of RA	$\frac{3322.53}{RA}$
$\overline{\psi}$	Potential barrier height of MgO	0.4eV
Area	MTJ layout surface	40nm x 40nm x $\frac{\pi}{4}$
R_p	Parallel resistance	6.21 kΩ
R_{ap}	Anti-parallel resistance	18.64 kΩ

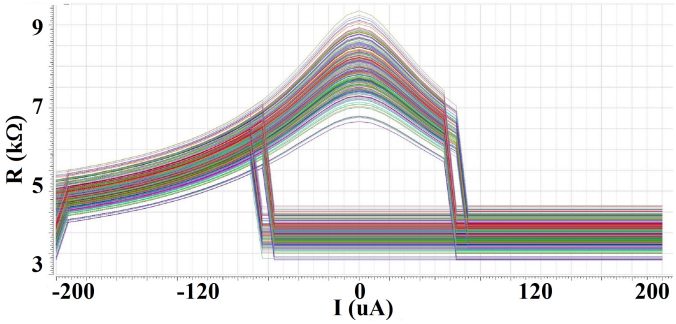


Fig. 2: Process variation results in different MTJ resistances based on 200 Monte Carlo simulations.

$$R_p = \frac{t_{ox}}{F \cdot \overline{\psi}^{\frac{1}{2}} \cdot Area} \cdot exp(coef \cdot t_{ox} \cdot \overline{\psi}^{\frac{1}{2}}) \quad (1)$$

B. Adiabatic Logic

Adiabatic logic is a circuit design technique for designing ultra-low-energy circuits [22]. Through the use of time ramp voltage power clocks, adiabatic logic recovers energy stored in load capacitors to be reused again in the next cycle thus reducing energy consumption. Adiabatic power clocks utilize capacitors and inductors to generate the clock signal while also using these devices to store the recovered energy [23]. Energy is stored in these devices through an electric charge in the capacitors and magnetic energy in the inductor. The energy dissipated in an adiabatic circuit is given by:

$$E_{diss} = \frac{RC}{T} C V_{dd}^2 \quad (2)$$

Where T is the charging period of the capacitor, C is the output load capacitor, and V_{dd} is the full swing of the power

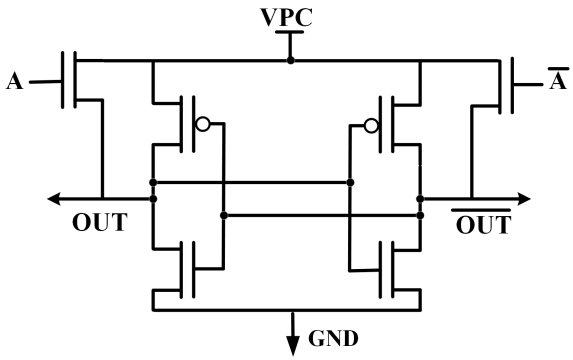


Fig. 3: Positive Feedback Adiabtic Logic (PFAL) buffer as an example of an adiabatic circuit [21].

clock. For an adiabatic circuit to be energy efficient when compared with CMOS the charging time must satisfy the following condition $T > 2RC$. Figure 3 shows an example of an adiabatic circuit known as Positive Feedback Adiabatic Logic (PFAL) [21].

C. Physically Unclonable Function

A PUF is a security primitive that uses random process variation to give a device a unique digital fingerprint. PUFs can be used in a range of applications from generating encryption keys [24] to secure authentication [25]. PUFs are ideal implementations in consumer electronics because they are an inexpensive form of security [26]. There have been various proposed PUFs that include the arbiter PUF [27], ring oscillator PUF [28], and memory-based PUFs such as the SRAM PUF [29]. The contents of this article focuses on the CMOS/MTJ Memory-based PUF within the silicon PUF class.

It is important to validate the security of our proposed PUF using metrics common between other proposed PUFs. To that end, we introduce three common metrics that are reported from our experiments: uniqueness, uniformity, and reliability.

1) Uniqueness: The uniqueness of a PUF is used to determine how different one PUF instance is from another. The ideal uniqueness value is 50%. Uniqueness is defined as

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{n} \cdot 100 \quad (3)$$

Where R_i and R_j are two different PUF instances, HD is the hamming distance between the two instances, k is the number of PUF instances, and n is the bit length of the PUF response. In our testing, we use k = 200 and n = 128.

2) Uniformity: Uniformity tells us the number of 0's and 1's in a PUF response. An ideal uniformity is 50% which reflects an equal number of 0's and 1's in the response. Uniformity is defined as

$$Uniformity = \frac{1}{n \cdot k} \sum_{i=1}^{k-1} r_{i,l} \cdot 100 \quad (4)$$

Where n is the bit length of the response, k is the number of PUF instances, and $r_{i,l}$ is the l^{th} bit from the instance i.

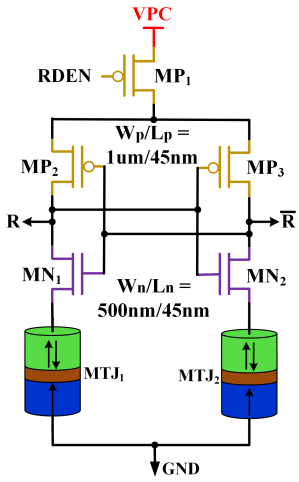


Fig. 4: Proposed adiabatic/MTJ PUF. Proper connection to MTJ terminals avoids read disturbs.

3) Reliability: Reliability tells us how the PUF response changes as environmental parameters change such as temperature and supply voltage. Reliability is defined as

$$Reliability = 100 - \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_i, R'_{i,t})}{n} \quad (5)$$

R_i is the response of a golden PUF that is used as a comparison to determine how much the response has changed. $R'_{i,t}$ is the response of the PUF that is affected by the environment change. The ideal value of reliability is 100% which represents no changes between the golden PUF and the PUF in non-ideal conditions.

In this paper, we vary three parameters to test the reliability of our proposed PUF. Temperature is varied from -40°C to 100°C with 27°C (room temperature) used as our reference temperature. The supply voltage is varied from 0.8V to 1.2V with 1.0V used as our reference voltage. The Tunnel Magnetoresistance ratio (TMR) is varied from 100% to 300% with 200% used as our reference ratio.

III. Proposed Adiabatic/MTJ Physically Unclonable Function

Our proposed PUF utilizes both adiabatic logic and MTJs to generate energy-efficient and secure responses. The ramping effect of an adiabatic clock allows for energy recovery while the variation of the MTJs allows for randomness. In section II-A, we showed there are many sources of uncontrolled randomness within an MTJ such as the oxide thickness, free layer thickness, and the TMR ratio [19]. In our proposed PUF we intend to use these variations to generate strong responses.

Figure 4 shows the schematic representation of the proposed adiabatic/MTJ PUF. The proposed PUF contains the following components, an enable transistor, a sense amplifier, and two MTJs. The enable transistor is used to generate a response while the sense amplifier is used to sense differences in the resistances of the MTJs. This is the first work that has utilized the principles of energy recovery to develop a novel adiabatic

sense amplifier which is combined with MTJ elements to form a low energy PUF. The sense amplifier utilizes a 2-Phase adiabatic clock generator in place of a constant voltage supply source. The two MTJs are set in the same state, i.e, either parallel or anti-parallel orientation of the free layer compared to the reference layer. As a result of process variation, one of these MTJs will have a higher resistance causing more current to flow through the other MTJ. It should be noted, the sizing of the transistors should be increased to reduce process variation that occurs with transistors so that the response of the PUF is dominated by the variation of the MTJ [30].

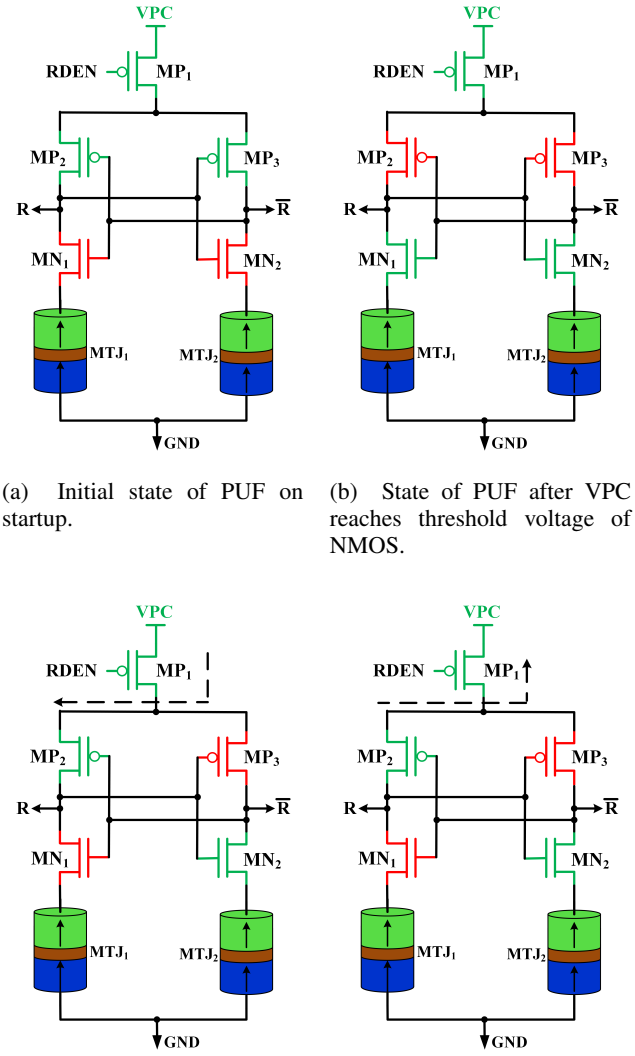
It should be noted, the proposed design will act as a dedicated security circuit rather than a memory circuit. In a typical memory operation, the two MTJs would need to be differential i.e two opposite orientations (P or AP). Further, the variation of the circuit needs to be as low as possible to reduce the Bit Error Rate (BER). To reduce the BER, the size of the MTJs and transistors are increased in memory design. However, in our proposed design we do not need to increase the MTJ sizing as the variation of the MTJs is used to our advantage.

A. Operation of Proposed Adiabatic/MTJ PUF

In this section, we will go into greater detail on the operation of the proposed PUF. The proposed PUF operates using a two-phase adiabatic clock. The operation can be divided into two phases corresponding with the two phases of the clock, the evaluation phase and, the recovery phase.

1) Evaluate Phase: The first phase or the evaluate phase is where the PUF response is generated. In this phase, RDEN is set to 0 and VPC begins rising from GND to VDD. Both MTJ's are set to the same orientation, either parallel or anti-parallel. As a result of process variations, one MTJ will have a higher resistance than the other MTJ. MP2, MP3, MN1, and MN2 make up a sense amplifier that senses the difference in resistance and drives the outputs to either logic 0 or 1.

The operation of the proposed PUF is illustrated in Figure 5. In this example it is assumed that $R_{MTJ1} > R_{MTJ2}$ as a result of process variations. The operation begins with MP1, MP2, and MP3 conducting current and charging both outputs to the threshold voltage, V_{th} (Figure 5a). At this point, MN1 and MN2 are both conducting current through each respective MTJ (Figure 5b). As a result of MTJ1 having a higher resistance, more current is flowing through MTJ2 thus pulling $\overline{R}$ to ground and turning MP2 on. Output R is charged full VDD and output $\overline{R}$ is pulled to GND (Figure 5c). The output waveform for the response (R and $\overline{R}$) are shown in Figure 6. Both outputs charge until the variation of the MTJs dominate and force one output to logic 1 and the other output to logic 0. The operation is further exemplified in Figure 7. Figure 7a shows the current through each MTJ when a response is generated. As explained previously, one MTJ has higher resistance than the other which will force one output to charge to VDD and the other to be pulled to GND. Figure 7b shows a closer look at the current when the MTJ forces one of the outputs to charge to logic 1.



(a) Initial state of PUF on startup.

(b) State of PUF after VPC reaches threshold voltage of NMOS.

(c) One MTJ dominates the variation and thus causes output to go high.

(d) Recovery phase of proposed PUF.

Fig. 5: Operation of proposed adiabatic/MTJ PUF including the evaluate and recovery phase.

2) Recover Phase: In the second phase or the recover phase, the clock begins to ramp down from VDD to GND. At this point, the output is at a higher potential than the clock thus current travels from high potential to low potential back into the adiabatic clock to be reused in the next cycle. The operation of the recovery phase is shown in Figure 5d as current is recovered through MP2 and MP1 back into the clock.

IV. Simulation Results

It is important to validate our proposed circuit to ensure energy efficiency and functionality. In this section, we present the simulation results of our proposed circuit. Simulations are performed using a Spice simulator with 45nm CMOS technology with perpendicular anisotropy CoFeB/MgO MTJ model [20]. Both MTJ orientations, parallel (P) and anti-

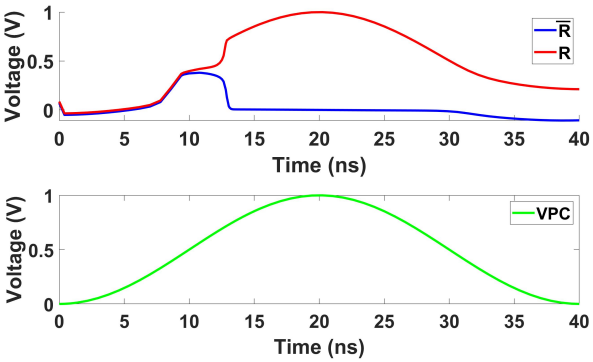
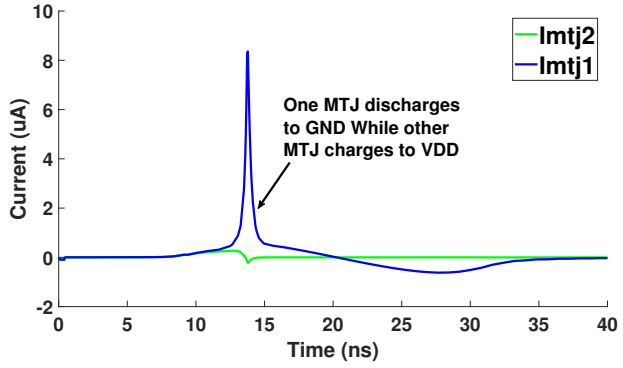
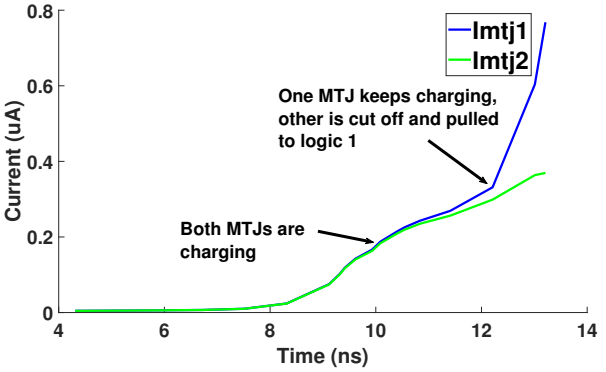


Fig. 6: Output waveform of the proposed MTJ PUF and waveform of the 2-Phase adiabatic power clock.

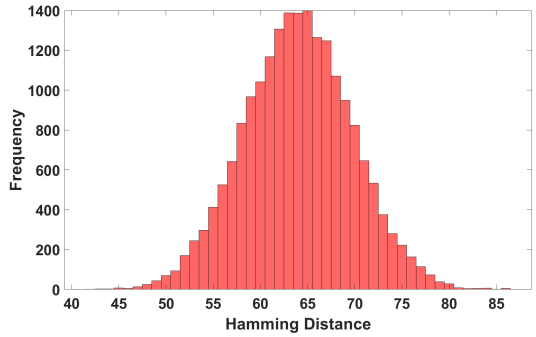


(a)

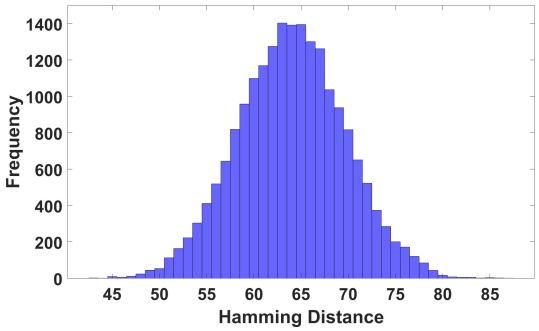


(b)

Fig. 7: Current waveform for the proposed adiabatic/MTJ PUF. 7a shows the current across the entire response generation. 7b shows the current at the moment of switching.



(a) Parallel



(b) Anti-parallel

Fig. 8: Histogram of hamming distances between different PUF instances for both parallel and anti-parallel MTJ orientations.

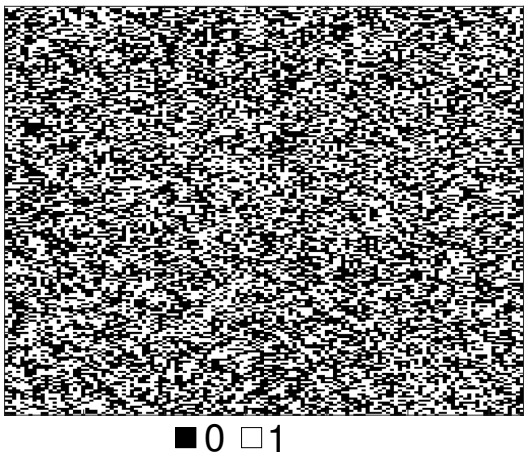
parallel (AP) are taken into consideration when simulating and are both presented in the results.

Each bit of the response is from an individual PUF cell. One application of the proposed PUF is the generation of an encryption key thus in our simulations we have designed a 128-bit PUF array. In our simulations, we have chosen to run 200 Monte Carlo Simulations to mimic 200 unique integrated circuits. The Monte Carlo simulations take into account process variation of both the transistors and the MTJs.

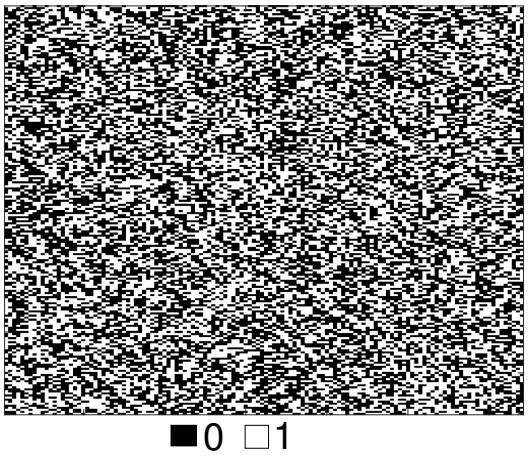
A. Uniqueness Evaluation

Through simulations, we have determined that our proposed PUF has a uniqueness of 49.98% when the MTJ's are in a parallel orientation. While in the anti-parallel orientation our proposed PUF has a uniqueness of 49.99%. Regardless of orientation, the proposed PUF has very strong uniqueness values. A histogram of hamming distances between the 200 instances of the proposed 128-bit PUFs can be seen in Figure 8.

Furthermore, it is interesting to investigate whether the two orientations of the MTJ can result in two different PUF responses. We can utilize reliability to determine how many bits flip between the two orientations. Reliability tells us the percent bit flip between two PUF instances when environmental conditions change. We can utilize the same idea by changing the orientations of the PUF and determining the reliability between the two instances. The bit flip percentage can then be determined by



(a) Parallel



(b) Anti-parallel

Fig. 9: Greyscale bitmap of the 200x128 proposed PUF for both parallel and anti-parallel orientations.

$$BitFlip\% = 100 - Reliability \tag{6}$$

We have determined that the bit flip percentage is 0.5%.

B. Uniformity Evaluation

The uniformity of our proposed adiabatic/MTJ PUF is 50.18% and 50.17% for the parallel and anti-parallel orientations, respectively. Both implementations are close to the ideal value of 50% implying that the proposed PUF response is difficult to predict. A greyscale bitmap of the two orientations is shown in Figure 9. Black boxes represent a ”0” and white boxes represent a ”1”.

C. Reliability Evaluation

The average reliability of our proposed PUF across various temperatures, voltages, and TMR ratios is 97.07% and 96.97% for the parallel and anti-parallel orientations respectively. The worst-case reliability is 85.92% at a temperature of 100°C.

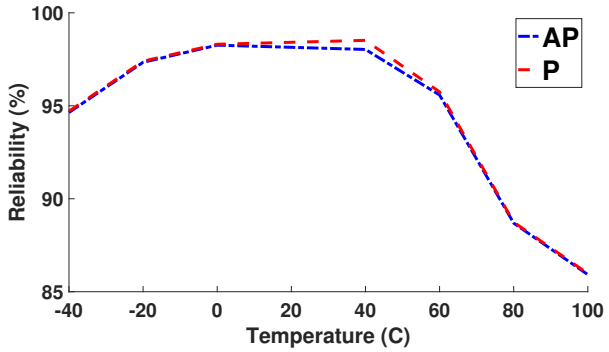


Fig. 10: Reliability of proposed PUF across various temperatures. VPC = 1V (peak of waveform) and TMR = 200%.

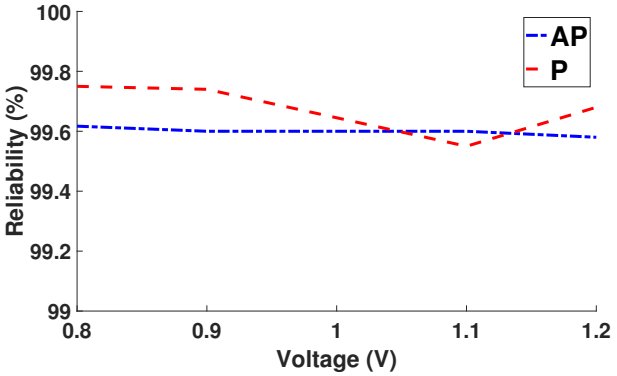


Fig. 11: Reliability of proposed PUF across various supply voltage levels. Temperature = 27°C and TMR = 200%.

When varying one of the three parameters we keep the other two parameters at the following nominal values: Temperature = 27°C, supply voltage, VPC = 1V, and TMR = 200%.

The reliability across various temperatures can be seen in Figure 10. Reliability values remain above 95% at temperatures between -40°C and 40°C. Between temperatures of 40°C and 100°C, the reliability of our proposed PUF drops to 85%. Whether our proposed PUF is in the P or AP mode has no strong correlation with the reliability. It should be noted that temperature has a strong effect on the reliability of MTJ based PUFs. To minimize the effects of temperature on reliability, Zhang et al. has proposed an automatic write-back feature to improve the reliability of MTJ based PUFs [31]. Dodo et al. has also performed a test on how their reliability is effected by temperature [32]. As the TMR value was not known in [32] we did not compare our work with the values reported in [32].

The reliability of our proposed PUF across various voltages can be seen in Figure 11. The reliability of the proposed PUF remains above 99% for supply voltage values between 0.8V and 1.2V. At 0.8V, the reliability of the proposed PUF in parallel mode is 99.75% while in the anti-parallel mode has a reliability of 99.61%. At 1.2V, the reliability of the proposed PUF in parallel mode is 99.68% while in the anti-parallel mode has a reliability of 99.58%.

The reliability of our proposed PUF across various TMRs can be seen in Figure 12. The reliability of the proposed PUF

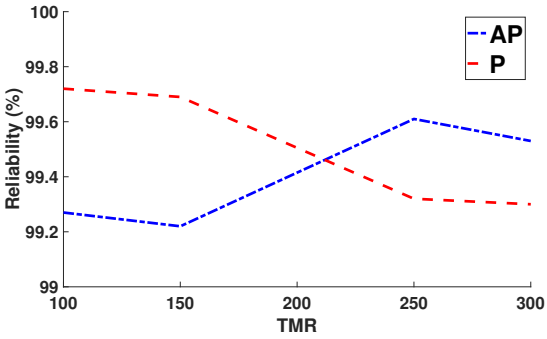


Fig. 12: Reliability of proposed PUF across various TMR values. Temperature = 27°C and VPC = 1V (peak of waveform).

remains above 99% for TMR values between 100% and 300%. At a TMR of 100%, the reliability of the proposed PUF in parallel mode is 99.72% while in the anti-parallel mode has a reliability of 99.27%. At a TMR of 300%, the reliability of the proposed PUF in parallel mode is 99.30% while in the anti-parallel mode has a reliability of 99.72%.

V. Comparison with State-of-the-Art PUFs

In this section, we compare the energy consumption and security metrics of the proposed adiabatic/MTJ PUF with other state-of-the-art PUFs reported in the literature.

A. Energy Consumption Comparison

The energy consumption of consumer electronic devices is an important metric, especially when considering battery-operated devices. Table II shows the energy per bit of the proposed adiabatic/MTJ PUF and other state-of-the-art PUFs. Our proposed adiabatic/MTJ PUF consumes 5.2fJ and 5.1fJ per bit in the parallel and anti-parallel orientations, respectively. From table II, it can be seen that the proposed PUF has lower energy consumption compared with the other PUFs. Further, we compared with another CMOS/MTJ based PUF [33] that reports an energy consumption of 1.00fJ per bit, the MTJ model used in this PUF has substantially lower resistance values and thus lower energy consumption.

B. Security Metric Comparison with State of the Art PUFs

Table II summarizes the comparison of results that are obtained verbatim from the respective papers. When compared with other CMOS/MTJ designs our proposed adiabatic/MTJ design has slightly better reliability values. The uniqueness value of the proposed adiabatic/PUF is closer to the ideal value of 50% when compared with the purely CMOS-based PUFs. The CMOS/MTJ PUF in [33] has a comparable uniqueness value to the proposed PUF. The uniformity of the proposed adiabatic/MTJ PUF is comparable with the CMOS-based designs as the best case uniformity is 0.04% away from the ideal value while our proposed PUF uniformity is 0.17% and 0.18% away from the ideal value. When compared with another 45nm/CMOS-based PUF our proposed PUF has lower energy consumption making it an ideal candidate for battery-constrained designs.

VI. Conclusion

In this paper, we have presented a low energy and secure adiabatic/MTJ based PUF. A two-phase adiabatic clock is used to reduce the dynamic energy consumption while the MTJ is used to generate the response bits. MTJs can either be in a parallel or anti-parallel orientation when referenced with the fixed layer. We investigate both orientations to determine the uniformity, uniqueness, reliability, and energy efficiency of the proposed adiabatic/MTJ PUF. We have determined that our proposed PUF is energy-efficient when compared to many CMOS and CMOS/MTJ based PUFs. Low energy consumption and ideal uniqueness and uniformity values make our proposed adiabatic/MTJ PUF an ideal candidate for energy-constrained devices. The proposed PUF can be implemented in encryption key generation algorithms, device fingerprinting for intellectual property protection and device authentication, etc.

Acknowledgment

This work is partially supported by National Science Foundation CAREER Award No. 1845448.

References

[1] J. Howell, "Number of connected iot devices will surge to 125 billion by 2030 . , ihs markit says," Oct 2021. [Online]. Available: https://technology.ihs.com/596542/

[2] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with iot," in *Internet of Things and Big Data Analytics for Smart Generation*. Springer, 2019, pp. 27–51.

[3] M. CSIS, "Economic impact of cybercrime-no slowing down," *Retrieved October*, 2018.

[4] S. Johnson, D. Rizzo, P. Ranganathan, J. McCune, and R. Ho, "Titan: enabling a transparent silicon root of trust for cloud," in *Hot Chips: A Symposium on High Performance Chips*, vol. 194, 2018.

[5] V. C. Patil and S. Kundu, "Realizing robust, lightweight strong pufs for securing smart grids," *IEEE Transactions on Consumer Electronics*, 2021.

[6] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[7] M.-K. Oh, S. Lee, Y. Kang, and D. Choi, "Wireless transceiver aided run-time secret key extraction for iot device security," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 1, pp. 11–21, 2019.

[8] Z. Kahleifeh and H. Thapliyal, "Ee-acml: Energy-efficient adiabatic cmos/mtj logic for cpa-resistant iot devices," *Sensors*, vol. 21, no. 22, p. 7651, 2021.

[9] Y. Gang, W. Zhao, J.-O. Klein, C. Chappert, and P. Mazoyer, "A high-reliability, low-power magnetic full adder," *IEEE Trans. Magn.*, vol. 47, no. 11, pp. 4611–4616, 2011.

[10] W. Kang, W. Lv, Y. Zhang, and W. Zhao, "Low store power high-speed high-density nonvolatile sram design with spin hall effect-driven magnetic tunnel junctions," *IEEE Trans. Nanotechnol*, vol. 16, no. 1, pp. 148–154, 2016.

[11] W. Kang, Y. Zhang, Z. Wang, J.-O. Klein, C. Chappert, D. Ravelosona, G. Wang, Y. Zhang, and W. Zhao, "Spintronics: Emerging ultra-low-power circuits and systems beyond mos technology," *ACM J. on Emerg. Technol. in Comput. Syst. (JETC)*, vol. 12, no. 2, pp. 1–42, 2015.

[12] J. S. Moodera, L. R. Kinder, T. M. Wong, and R. Meservey, "Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions," *Physical Review Lett.*, vol. 74, no. 16, p. 3273, 1995.

[13] R. Zand, A. Roohi, S. Salehi, and R. F. DeMara, "Scalable adaptive spintronic reconfigurable logic using area-matched mtj design," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 63, no. 7, pp. 678–682, 2016.

[14] B. Behin-Aein, J.-P. Wang, and R. Wiesendanger, "Computing with spins and magnets," *MRS Bulletin*, vol. 39, no. 8, pp. 696–702, 2014.

TABLE II: Security metrics and energy consumption of proposed adiabatic/MTJ PUF compared with state of the art PUFs.

PUF	Tech.	VDD	Key Size	Uniqueness	Uniformity	Reliability	Energy/bit	Strong/Weak
[34]	90nm	1.2V	64	NA	NA	97%	37.5fJ	Strong
[35]	65nm	0.6V	128	50.04%	49.5%	99.05%	10.3fJ	Weak
[36]	45nm	1V	128	49.48%	49.41%	99.75%	0.08fJ	Weak
[37]	90nm/PCM	NA	256	49.69%	48.14%	88.74%	8.49pJ	Weak
[38]	90nm/RRAM	1V	NA	50.17%	50.34%	95.6%	NA	Strong
[39]	RRAM	1/1.2V	128	49.85%	49.99%	NA	NA	Weak
[33]	45nm/MTJ	1V	128	51.01%/49.89%	50.20%/49.90%	96%	1.00fJ	Weak
[32]	40nm/MTJ	1V	128	49%-51%	49%-51%	96.73%	NA	Weak
Proposed (P)	45nm/MTJ	1.0V	128	49.98%	50.18%	97.07%	5.2fJ	Weak
Proposed (AP)	45nm/MTJ	1.0V	128	49.99%	50.17%	96.97%	5.1fJ	Weak

[15] J. C. Slonczewski, "Current-driven excitation of magnetic multilayers," *Journal of Magnetism and Magnetic Materials*, vol. 159, no. 1-2, pp. L1–L7, 1996.

[16] L. Berger, "Emission of spin waves by a magnetic multilayer traversed by a current," *Physical Review B*, vol. 54, no. 13, p. 9353, 1996.

[17] A. D. Kent, "Perpendicular all the way," *Nature materials*, vol. 9, no. 9, pp. 699–700, 2010.

[18] R. W. Dave, G. Steiner, J. Slaughter, J. Sun, B. Craigo, S. Pietambaram, K. Smith, G. Grynkewich, M. DeHerrera, J. Akerman *et al.*, "Mgo-based tunnel junction material for high-speed toggle magnetic random access memory," *IEEE Trans. Magn.*, vol. 42, no. 8, pp. 1935–1939, 2006.

[19] S. Sahay and M. Suri, "Recent trends in hardware security exploiting hybrid cmos-resistive memory circuits," *Semiconductor Science and Technology*, vol. 32, no. 12, p. 123001, 2017.

[20] Y. Wang, H. Cai, L. A. de Barros Naviner, Y. Zhang, X. Zhao, E. Deng, J.-O. Klein, and W. Zhao, "Compact model of dielectric breakdown in spin-transfer torque magnetic tunnel junction," *IEEE Trans. Electron Devices*, vol. 63, no. 4, pp. 1762–1767, 2016.

[21] A. Vetuli, S. Pascoli, and L. Reyneri, "Positive feedback in adiabatic logic," *Electronics Letters*, vol. 32, no. 20, pp. 1867–1869, 1996.

[22] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Y.-C. Chou, "Low-power digital systems based on adiabatic-switching principles," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 2, no. 4, pp. 398–407, 1994.

[23] H. Mahmoodi-Meimand, A. Afzali-Kusha, and M. Nourani, "Adiabatic carry look-ahead adder with efficient power clock generator," *IEEE Proc.-Circuits, Devices and Syst.*, vol. 148, no. 5, pp. 229–234, 2001.

[24] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conf.* IEEE, 2007, pp. 9–14.

[25] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender puf protocol: A lightweight, robust, and secure authentication by substring matching," in *2012 IEEE Symp. on Security and Privacy Workshops*. IEEE, 2012, pp. 33–44.

[26] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electron.*, vol. 3, no. 2, pp. 81–91, 2020.

[27] 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 *2004 Symp. on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*. IEEE, 2004, pp. 176–179.

[28] B. L. P. Gassend, "Physical random functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2003.

[29] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *Int. workshop on cryptographic hardware and embedded syst.* Springer, 2007, pp. 63–80.

[30] A. Asenov, S. Kaya, and J. H. Davies, "Intrinsic threshold voltage fluctuations in decanano mosfets due to local oxide thickness variations," *IEEE Trans. Electron Devices*, vol. 49, no. 1, pp. 112–119, 2002.

[31] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable spin-transfer torque magnetic ram-based physical unclonable function with multi-response-bits per cell," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1630–1642, 2015.

[32] S. B. Dodo, R. Bishnoi, S. M. Nair, and M. B. Tahoori, "A spintronics memory puf for resilience against cloning counterfeit," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 27, no. 11, pp. 2511–2522, 2019.

[33] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*, vol. 34, no. 7, pp. 1176–1187, 2015.

[34] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based puf," in *IEEE Int. symp. of circuits and systems (ISCAS)*. IEEE, 2011, pp. 2071–2074.

[35] S. Tao and E. Dubrova, "Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm cmos," *Electronics Lett.*, vol. 52, no. 10, pp. 805–806, 2016.

[36] S. D. Kumar and H. Thapliyal, "Design of adiabatic logic-based energy-efficient and reliable puf for iot devices," *ACM J. on Emerging Technologies in Computing Systems (JETC)*, vol. 16, no. 3, pp. 1–18, 2020.

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

[38] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "mrpuf: A novel memristive device based physical unclonable function," in *International Conference on Applied Cryptography and Network Security*. Springer, 2015, pp. 595–615.

[39] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, "A write-time based memristive puf for hardware security applications," in *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2013, pp. 830–833.

Zachary Kahleifeh is currently a PhD candidate in the Department of Electrical and Computer Engineering, University of Kentucky, Lexington, KY, USA. He completed his Bachelors in Computer engineering from the University of Kentucky. His research interests include low-energy computing, hardware security, emerging memory technologies, and adiabatic computing.

Himanshu Thapliyal (SM'16) is currently an Associate Professor in the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, Tennessee, USA. He received a PhD degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2011 where he received the 'Distinguished Graduate Achievement Award'. From 2012-14, he worked as a designer of processor test solutions at Qualcomm, where he received the Qualcomm QualStar Award for contributions to memory built-in self-test. He joined as an Assistant Professor at the University of Kentucky, Lexington in 2014 where he got promoted to Associate Professor in 2020. He is the recipient of the NSF CAREER award, and IEEE-CS TCVLSI Mid-Career Research Achievement Award. In March 2022, he is selected to the Inaugural Class of IEEE Computer Society Distinguished Contributors that recognizes his distinguished contributions to the society and the profession. He has authored over 150 publications including more than 60 journal articles with over 5100 citations (h-index of 44). He has been ranked in the top 50 among scientists throughout the world in the field of Computer Hardware & Architecture for the calendar years 2019 and 2020. He has received Best Paper awards at the 2021 IEEE International Conference on Consumer Electronics, the 2020 IEEE World Forum on Internet of Things, the 2017 Cyber and Information Security Research Conference, and the 2012 IEEE Computer Society Annual Symposium on VLSI. He is the steering committee vice-chair of the IEEE Symposium on Smart Electronic Systems. He served as the General Chair of the 2020 IEEE Symposium on Smart Electronic Systems. He has served as the Program Chair of the 2022 ACM Great Lakes Symposium on VLSI, the 2020 IEEE International Conference on Consumer Electronics, 2019 IEEE Computer Society Annual Symposium on VLSI, and the 2018 IEEE Symposium on Smart Electronic Systems. He is serving as the Section Editor of the Springer Nature Computer Science and is leading two sections: (i) Quantum Computing and Emerging Technologies, and (ii) Emerging Trends in Sensors, IoT and Smart Systems. He served as the Senior Associate Editor of the IEEE Consumer Electronics Magazine. He is currently serving as Associate Editor of the IEEE Transactions on Consumer Electronics, the IEEE Internet of Things Journal, and the editorial board member of the Microelectronics Journal. His research interests include hardware security of IoT and vehicles, quantum computing, and smart healthcare solutions for older adults.

Syed M. Alam (SM'22) is currently the Sr. Director of Design engineering at Everspin Technologies leading the design functional areas for embedded and standalone STT-MRAM. He has worked on various aspects of design including bitcell, array circuits, architecture, and new product introduction supporting test and high-speed design characterization for MRAM. Dr. Alam received his BS degree in Electrical Engineering from UT Austin in 1999, MS and PhD degrees in Electrical Engineering and Computer Science from MIT in 2001 and 2004, respectively. He served on the program committees for ICCAD, DAC, ISQED, and ISLPED. He is a fellow of ISQED. Dr. Alam currently serves as an editor for IEEE Transactions on Electron Devices (TED). He has mentored/co-advised 5 PhD students for research on 3D integration and logic-in-memory architecture. Dr. Alam has over 90 issued US patents, and multiple journal/conference publications.