An STT-MRAM Based Strong PUF

Soroush Khaleghi, Paolo Vinella, Soumya Banerjee, and Wenjing Rao [*]
ECE Department, University of Illinois at Chicago, IL, USA
Email: {skhale4, pvinel2, sbaner8, wenjing} @uic.edu

ABSTRACT

Physically Unclonable Functions (PUFs) are an emerging technology that could play the key roles in various security applications. Depending upon the size of its truth-table, i.e., the search space for an attacker to fully specify its behavior, a PUF can be categorized as either "weak" or "strong". While weak PUFs have a limited search space, polynomial with respect to the number of their building components, strong PUFs offer a huge search space, making them more suitable for a wider range of security applications, such as device authentication and logic obfuscation. This paper presents a scheme for making a strong PUF based on Spin-Transfer Torque Magnetic RAM (STT-MRAM), an emerging nanoelectronic memory device. To achieve an STT-MRAM based strong PUF with a huge search space, we proposed the idea of "group formation" to exploit the nano-scale analog disorders of STT-MRAM devices. Simulation results confirm the quality of the proposed strong PUF. In the end, this paper sheds light on how to make a strong PUF in general, by extending the idea of group formation beyond the STT-MRAM devices.

1. INTRODUCTION

Physically Unclonable Functions (PUFs) are an emerging technology that could play the key roles in various security applications. Basically, PUFs can offer a unique key for every chip by deriving it from some noisy physical characteristic of the chip. Particularly, one main advantage of PUFs is that they do not require the key to be explicitly stored on chip; instead, they provide a *challenge-response* mechanism via physical interaction, making them harder to crack for a variety of powerful attacks [2] [4]. For example, any attack on a PUF device must be attempted while the chip is powered on; otherwise, no information can be gained. Furthermore, since PUFs are based on nano-scale structural disorders, they cannot be cloned physically, even by the same manufacturering process.

Each PUF can be essentially seen as a function, providing a unique way of mapping the challenges into the responses. Depending upon the size of its truth-table, i.e., the search space for an attacker to fully specify its behavior, each PUF can be categorized as either "weak" or "strong". Weak PUFs offer a limited search space, polynomial with respect to the number of their building components. Strong PUFs, on the other hand, offer a huge search space, exponential with respect to the number of their components. This makes them suitable for a wider range of security applications [2].

Spin-Transfer Torque Magnetic RAM (STT-MRAM) is an emerging Non-Volatile Memory (NVM) that can offer low bit cell footprint, low power consumption, and high scalability [6]. Technology scaling of NVM devices increases the process variations, thus making them a good candidate for PUFs. The work in [7] proposes a weak PUF based on STT-MRAM, which is capable of producing response bits with desirable randomness and reliability.

It is usually assumed that the type of a PUF, whether strong or weak, is inherently determined by its architecture and the kind of nano-scale analog disorders, based upon which a PUF is built. In this paper, we will show that this assumption is not necessarily true, by presenting a scheme to construct a strong PUF based on STT-MRAM devices. To achieve a huge search space, we propose the idea of "group formation" to exploit the nano-scale analog disorders of STT-MRAM devices. Furthermore, we will discuss the necessary conditions for making a strong PUF in general by extending the idea of "group formation". This paper also applies the generalized idea of "group formation" to a popular CMOS-based weak PUF to form a strong one.

2. PRELIMINARIES

2.1 General Concepts of a PUF

Due to the nano-scale structural disorders, occurring during the fabrication phase of IC production, each chip is slightly different from the others, made with the same fabrication process. A PUF is a physical system that presents unclonability by exploiting these slight variations. A PUF can be stimulated with external inputs, called *challenges*, upon which it reacts with corresponding outputs, called *responses*. Therefore, every PUF implements a unique way of mapping challenges to responses for a specific IC. Since exact control over the manufacturing process is impossible, it is infeasible to build identical PUFs with the same Challenge-Response Pairs (CRPs). Consequently, it is also presumably impossible to predict the behavior of a PUF, unless by testing its all possible CRPs.

[*]This work is supported by NSF Grant 1149661.

Nanoarch '16, July 18-20, 2016, Beijing, China
© 2016 ACM. ISBN 978-1-4503-4330-5/16/07…$15.00
DOI: http://dx.doi.org/10.1145/2950067.2950080

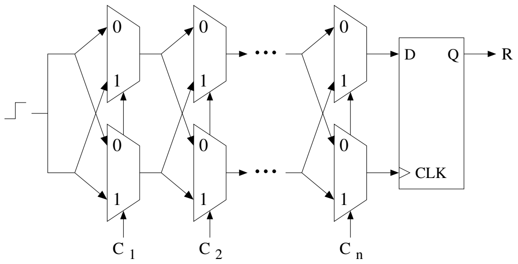


Figure 1: Arbiter PUF circuit: two delay paths are created based on the challenge (C_1 to C_n). Depending on the arrival times of the rising edge at the inputs of the D-FF, the response (R) could become either "1" or "0"

In general, the potential applications of a PUF depends heavily on the number of CRPs that it can offer [2].

2.1.1 Weak PUFs

Some PUFs offer a **limited** number of independent CRPs, ranging from one (in the most extreme case) to polynomial-sized with respect to the number of their building components.

For example, the power-on state of an SRAM cell constitutes a weak PUF [3]. Each SRAM cell has a tendency towards logic 1 or 0, due to process variations. As a result, the initial power-on state of each SRAM cell will be either 1 or 0, making each cell a weak PUF with one CRP: the challenge is the powering on the cell, and the response is the initial state of the SRAM cell. Note that employing more SRAM cells would only increase the number of response bits, not that of CRPs.

Due to their limited number of CRPs, weak PUFs are mostly used for key-generation purposes in cryptography, where a few unique keys must be generated for every chip [2] [5]. However, since the entire truth-table of a weak PUF can be obtained in polynomial time complexity, its CRPs must be kept secret to prevent the potential attackers from building up the entire truth-table of the PUF, and emulating its behavior.

2.1.2 Strong PUFs

Some PUFs, on the other hand, offer a **huge** number of independent CRPs, usually exponential to the number of their building components.

Figure 1 shows an example of a strong PUF, called Arbiter [1]. The actual propagation delay of each Multiplexer (MUX) differs slightly from the others due to process variations. A signal transition, say from 0 to 1, will propagate through two different paths of MUXes, determined by the challenge (C_1 to C_n). Each challenge bit feeds in a set of two MUXes that are positioned vertically, so that the two selected paths would not share any of the MUXes. Depending on the order of arrivals of the rising edge at the terminals of the D-Flip Flop, the response bit (R) would be either 0 or 1. In this PUF, the challenges are the selection of any two complementary paths, a total of 2^n possible CRPs, where n is half the number of MUXes. It must be noted that every CRP in this PUF is ***independent*** from the other ones, i.e., the knowledge of any number of CRPs cannot be used to determine the outcome of another CRP [2].

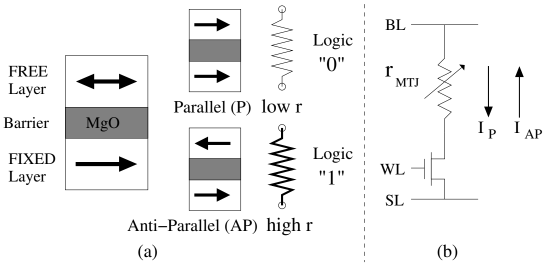


Figure 2: (a) MTJ device structure and its resistance model; (b) The complete structure of an STT-MRAM cell

Due to its huge number of independent CRPs, the security of a strong PUF does not rely on keeping its CRPs secret, but rather on the fact that recovering the entire truth-table of the PUF in a reasonable time is infeasible. Consequently, they can be employed in a wider range of security applications, such as authentication and logic obfuscation [2].

2.2 STT-MRAM Devices

Spin-Transfer Torque Magnetic RAM (STT-MRAM) is an emerging nano-electronic memory device that can offer significant performance improvement and power reduction [6]. Figure 2 shows the architecture of an STT-MRAM device. As it is shown in Figure 2(a), the storage part of the device is a Magnetic Tunnel Junction (MTJ), consisting of three layers: two ferromagnetic layers, separated by an insulating oxide layer. One of the ferromagnetic layers, called the "fixed layer", has a fixed magnetization vector in any operating condition, while the other one, called the "free layer", has a magnetization vector that is free to switch between two directions. Accordingly, the MTJ cell has two states, shown in Figure 2(a):

1. ***Parallel (P)***: when the magnetization directions of both ferromagnetic layers are the same, the MTJ cell has a **low** resistance, associated with **logic 0**.
2. ***Anti-Parallel (AP)***: when ferromagnetic layers have opposite magnetization directions, the MTJ cell has a **high** resistance, associated with **logic 1**.

Figure 2(b) shows a commonly used structure of an STT-MRAM cell. By allowing a current to flow through the device, this structure enables both Read/Write operations without relying on an external magnetic field. The magnetization direction of the free layer, which specifies the logic value of the cell, is determined by the direction of the current flow through the device. By comparing the resistance of a cell with a fixed reference resistance, the value of the cell, either 0 or 1 (P or AP) can be determined.

2.3 An STT-MRAM Based Weak PUF

Due to process variations, the equivalent resistance of an STT-MRAM cell in either of its states (P or AP) would be slightly different from those of the other cells [7] [6]. Figure 3 depicts the architecture of a weak PUF based on the idea presented in [7]. The main idea behind this PUF is to compare the resistance of two cells, set to the same state (either both to P or both to AP), as shown in Figure 3(a). Depending upon which cell has a slightly higher resistance, the response bit would be either 1 or 0.

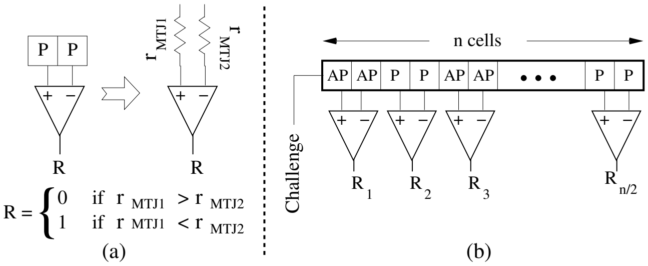


Figure 3: An STT-MRAM based weak PUF: (a) The main idea: comparing the resistances of two identical cells with the same magnetization; (b) The complete architecture of the PUF

Figure 3(b) shows the complete architecture of such a PUF: a memory composed of n STT-MRAM cells. In this PUF, the challenges are the pattern of magnetization (P or AP) of each pair of cells, and the responses are the outputs of the sense-amplifiers, comparing the resistances of adjacent cells. As it is shown in Figure 3(b), every pair of adjacent cells in such a PUF must be set to the same state; otherwise, the output of their corresponding sense-amplifier can be easily predicted by an attacker, as state AP has a higher resistance than state P.

In order to verify that such architecture is a weak PUF, one must consider the number of independent CRPs that can essentially reveal the entire truth-table of the PUF. Assuming that the outputs of all sense-amplifiers form a single response (consisting of $n/2$ bits), there exist $2^{n/2}$ CRPs for such a PUF. However, most of these CRPs are not independent from each other. In fact, the entire truth-table of this PUF can be obtained by examining the following two CRPs: the one with every pair set to P, and the one with every pair set to AP. All other CRPs can be predicted by referring to these two independent CRPs. This is due to the fact that the value of the response bit for each pair is independent from the states of other pairs. In other words, each pair of cells can only offer 2 valuable bits of information.

3. A STRONG PUF BASED ON STT-MRAM

3.1 Motivation

Basically, every PUF is made by exploiting some noisy analog feature, presented at the implementation level of identically designed components. For example, the gate delays are the analog feature used in designing an Arbiter PUF; and the resistances of the MTJ cells are the analog feature in the given STT-MRAM based PUF example. These noisy analog features will eventually "collapse" into some digital bits, before they can be used as CRPs for security applications.

The infinite precisions of such analog features are inherently capable of offering an unlimited number of independent CRPs. The reason why some PUFs are "strong", while the others are "weak" has to do with how much precision of those analog features is exploited, before collapsing them into the digital domain. In the case of the weak PUF based on STT-MRAM cells, the resistance of a cell (an analog value) is compared with that of another cell to form a digital response (0 or 1). If instead of comparing two cells at a time, the resistances of a *group* of cells can be *combined*, and then compared with that of *another group*, a huge number of new CRPs can be introduced, exponential to the number of cells. We will provide two motivational examples to introduce the main elements that will be used in the proposed strong PUF.

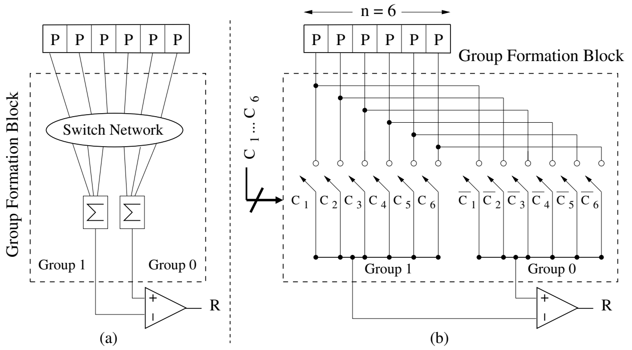


Figure 4: (a) The idea of forming 2 groups to increase the number of CRPs; (b) An example architecture for implementing the Group Formation Block for a PUF with 6 cells

1) Group Formation

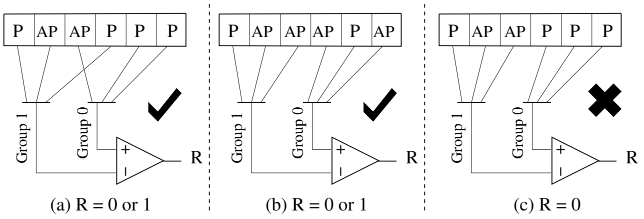
The main idea of combining the resistances of a group of cells, before collapsing them into a digital signature, is to compare their overall resistance with that of another group. This is demonstrated with an example shown in Figure 4(a). This Figure shows a memory with 6 STT-MRAM cells, all of which are set to a **same fixed** magnetization (P in this case). The functionality of the *Group Formation Block* is to allow the formation of two 3-cell groups, so that the overall resistances of the two groups can be compared to form a response bit (signal *R)*. Based on the number of choices for the two groups, the total number of independent CRPs becomes $\frac{1}{2}\binom{6}{3} = 10$.

Figure 4(b) shows the architecture of the Group Formation Block. The two groups of cells (Group 1 and Group 0) are each connected to one port of the sense-amplifier. Each cell i can be selected to join either Group 1 or Group 0, by setting its corresponding challenge bit C_i. It must be noted that a cell cannot be connected to both groups at the same time, due to the fact that the current division for each cell must be avoided. This is achieved by using 6 challenge bits (C_1 to C_6) to control 12 switches, in such a way that if the corresponding switch of any cell is ON for one group, the corresponding switch of the same cell for the other group is OFF, and vice versa.

2) Bit Pattern

Besides allowing the formation of two groups with multiple cells, another dimension to increase the number of CRPs is changing the bit pattern (magnetization vector) of cells. Even though such a dimension was used as the basis of the previous weak PUF, it was only exploited to a very limited extent. Under the group formation framework, changing the bit pattern of cells can significantly boost the number of CRPs.

Figure 5(a) shows an example of changing the bit patterns for a PUF with 6 STT-MRAM cells. In this example, each group has two cells in state P and one cell in state AP, which makes their resistance comparison able to serve as a



(a) R = 0 or 1 (b) R = 0 or 1 (c) R = 0

Figure 5: (a)(b) Examples of valid CRPs by changing the bit patterns and group formations; (c) An invalid CRP: Group 1 with two *AP*'s and one *P* has a higher resistance than Group 0 with three *P*'s

PUF response bit. Figure 5(b) shows another valid CRP by changing both the groups and the bit pattern of the cells. Figure 5(c) is an example of an invalid CRP, because the total resistance of Group 1 is predictably larger than that of Group 0, as there are two cells in state AP in Group 1, while all the cells in Group 0 are in state P. Even though not all the CRPs are valid in such a PUF, there exists $\sum_{i=0}^{3}\binom{3}{i}^2 = 20$ valid independent CRPs for every single selection of two groups, enabled by changing the bit patterns of cells.

3.2 Architecture

The overall architecture of the proposed strong PUF, which is based on the ideas of group formation and changing the bit patterns, is depicted in Figure 6(a). Similar to the motivational examples, this architecture supports the combination of $n/2$ cells per group. By setting the challenge bits (C_1 to C_n), two groups of resistances would be connected to the two ports of the sense-amplifier. Then, the overall resistances of these two groups are compared to form a single response bit.

Figure 6(b) shows an example of choosing a CRP for a PUF with 6 STT-MRAM cells. In this example, the cells 1, 2, and 4 are selected to form Group 1 (by setting $C_1 = C_2 = C_4 = 1$), and the other three cells are selected to form Group 0 (by setting $C_3 = C_5 = C_6 = 0$).

It must be noted that in such architecture, the overall resistance of each group is the *equivalent parallel resistance* of all the cells in that group. Consequently, the overall resistances of Group 1 (r_{G1}) and Group 0 (r_{G0}) in Figure 6(b) are determined by the following equations:

$$\frac{1}{r_{G1}} = \frac{1}{r_1^P} + \frac{1}{r_2^{AP}} + \frac{1}{r_4^P} \quad \textit{and} \quad \frac{1}{r_{G0}} = \frac{1}{r_3^{AP}} + \frac{1}{r_5^P} + \frac{1}{r_6^P} \quad (1)$$

Since the overall resistances of the two groups must be equal in theory, the following constraints must be satisfied when selecting these groups:

1. the number of cells in each group must be equal to $n/2$; otherwise, the groups would be unbalanced and not useful. [1]
2. the number of cells in states P and AP must be equal in both groups; otherwise, the group with more cells in state AP would have a higher resistance, and the response can be predicted.

3.3 Analysis

To prove that the proposed PUF is in fact a strong one, we need to show that the number of independent CRPs is exponential (or larger) with respect to the number of elements in the PUF. As it was motivated in the previous section, each **challenge** in this PUF consists of 2 parts:

1. **Group Formation:** A part of challenge (C_1 to C_n) selects two groups of cells to be connected to the two ports of the sense-amplifier. Taking into account the 1st constraint above, there are $\frac{1}{2}\binom{n}{n/2}$ possible combinations of these groups for a PUF with n cells.

2. **Bit Pattern:** A part of challenge (initialization of STT-MRAM cells) specifies the state of each cell. Taking into account the 2nd constraint above, for a certain selection of the two groups (each with $n/2$ cells), the total number of possible combinations for the states are $\sum_{i=0}^{n/2}\binom{n/2}{i}^2$.

By putting together these two factors, the total number of independent CRPs for the given PUF is given as follows:

$$\frac{1}{2} \times \binom{n}{\frac{n}{2}} \times \sum_{i=0}^{n/2} \binom{\frac{n}{2}}{i}^2 = \frac{1}{2}\binom{n}{\frac{n}{2}}^2 \qquad (2)$$

It can be shown that the total number of CRPs, given in Eq. 2 grows faster than exponentially (factorial growth) with respect to the number of cells in the memory. As it was illustrated in the motivational examples, the information of none of these CRPs can be used to determine the responses of new challenges; thus, the proposed PUF is in fact a strong one.

In terms of hardware cost, only a single sense-amplifier is needed, compared to the $n/2$ sense-amplifiers in the weak PUF. $2n$ switches are required for implementing the Group Formation block. In terms of time overhead, the previous weak PUF can generate $n/2$ response bits at one cycle. For the proposed strong PUF, one bit is generated per clock cycle. Nevertheless, this time overhead is not an important issue in most of the security applications, especially due to the fact that at any time, one would only require to examine a few CRPs.

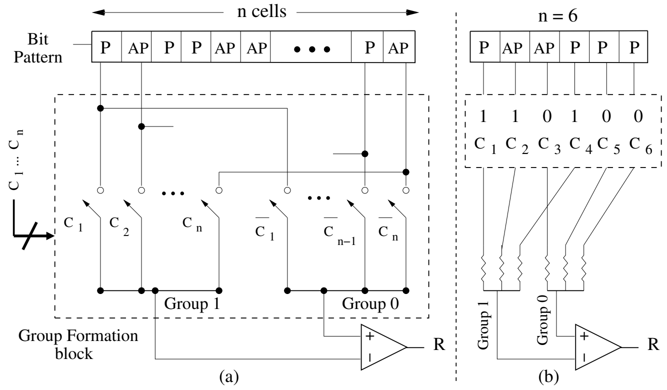
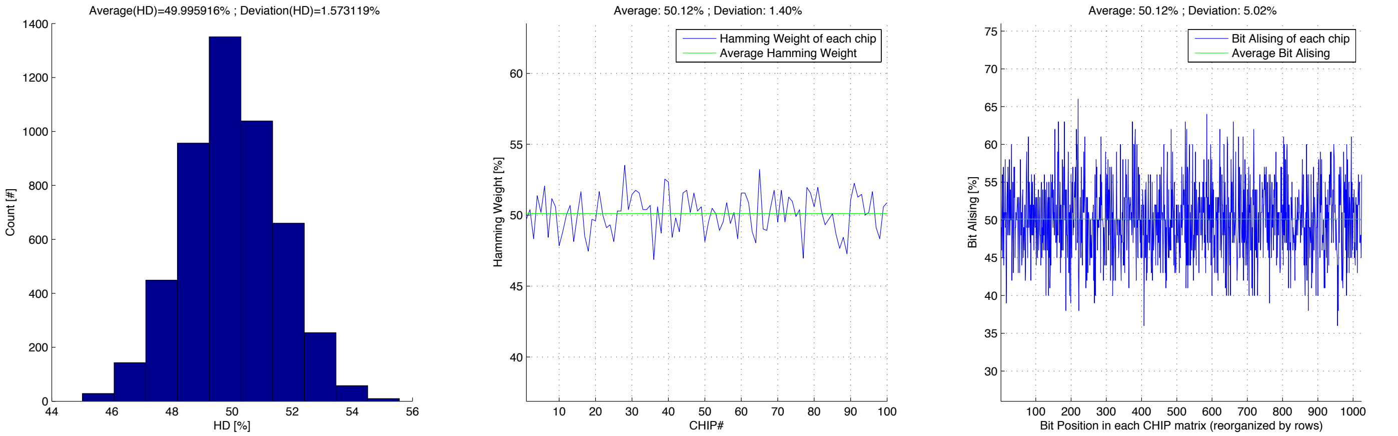


Figure 6: (a) The overall architecture of the proposed strong PUF; (b) An example for n=6: each group has two *P*'s and one *AP*

[1] It must be noted that the proposed architecture does not allow the formation of groups with equal number of cells, other than $n/2$ cells per group. This is to avoid the CRP information of the smaller groups to be used for determining that of the larger ones, which can be exploited by an attacker to characterize the PUF.



(a) Inter-chip Hamming Distance Distribution

(b) Hamming Weight

(c) Bit Aliasing

Figure 7: The quality of the proposed strong PUF with respect to three parameters: (a) Inter-chip Hamming distance: measuring the randomness among different chips; (b) Hamming weight: measuring the randomness among various bits of a same response within a same chip; (c) Bit aliasing: measuring the randomness for each response bit among various responses within a same chip

3.4 Simulation Results

The purpose of this section is to verify the quality of the proposed strong PUF. Basically, a good PUF must offer maximum randomness of the responses within a chip (*intra-chip* uniqueness), and among different chips (*inter-chip* uniqueness). In other words, applying various challenges to a same PUF must generate random responses. Furthermore, applying the same challenges to various PUFs must result in random responses as well. Such uniqueness is usually measured by metrics such as *Hamming Distance*, which shows the number of positions at which the two responses are different. In a fully random distribution (the ideal situation), the Hamming distance is equal to 50%.

Since the proposed strong PUF can generate one response bit per challenge, every 1024 response bits are treated as one response to measure intra-chip randomness. A total of 100 chips, each with 1000 CRPs are studied in this experiment. All simulations are performed in MATLAB by adopting the mathematical models of STT-MRAM devices from [7].

Figure 7(a) shows the distribution of the inter-chip average Hamming distance for 100 chips. Basically, the average Hamming distance between every possible pair of chips is calculated by computing the Hamming distances of the same CRPs for every pair of chips. Then, the distribution of the average Hamming distance is plotted. As it can be seen from the graph, the median of this distribution is 49.99%, which shows a promising inter-chip randomness.

In order to evaluate the intra-chip randomness, two metrics are employed: 1) *Hamming Weight*, which measures the randomness of bits within the same response for a certain chip; and 2) *Bit Aliasing*, which measures the randomness of bits, placed at the same position among different responses for a certain chip. Figure 7(b) plots the Hamming weight of every chip, which is calculated by calculating the average Hamming weights of all possible pairs of responses within each chip. Figure 7(c) plots the bit aliasing of each chip, based on the bit positions, calculated for every possible pair of responses as well. As it can be seen from these graphs, the average values for both of these metrics are 50.12%, which verifies a promising randomness within each chip as well.

4. STRONG PUF BEYOND STT-MRAM

In this section, we will extend the idea of "group formation" beyond the STT-MRAM devices, and discuss the necessary conditions for making a strong PUF in general.

As it was discussed earlier, each PUF is built upon some noisy analog feature with infinite precision. To make a strong PUF, such infinite precision of those analog features must be exploited extensively before collapsing them into the digital domain, in such a way that the number of independent CRPs grows exponentially with respect to the building components of the PUF. There are two necessary conditions for making a strong PUF:

1) Device-level compatibility for group formation: The key idea for making a strong PUF is to see whether or not, the analog feature of a given component can be *combined* to from a group of components, *before* being collapsed into the digital domain. If so, the options of which components to be combined into groups will greatly increase the search space of the PUF. For example, the group formation is inherently supported by the analog feature of the STT-MRAM devices, the resistances of the MTJ cells.

However, such a combination of components is not always supported by the analog feature of the PUF device. For example, as is stated in section 2.1, the power-on state of a traditional SRAM cell is a weak PUF. In this case, the analog noisy feature is the two identical positive feedback at the device level, forcing the cell to either of the states during a write operation. In this example, the analog feature, which is not accessible at any design-level higher than the device level, does not support the necessitated feature as discussed to work in the group formation framework.

2) Architecture-level support to achieve independent CRPs: Once the feasibility of combining the analog feature is determined, the same principle can be adopted in various architectures to boost the number of CRPs. However, the challenge is to design an architecture with an exponential number of **independent** CRPs.

Next, we provide some insights on how to make a strong PUF in general based on the group formation scheme by presenting a case study of a popular CMOS-based PUF.

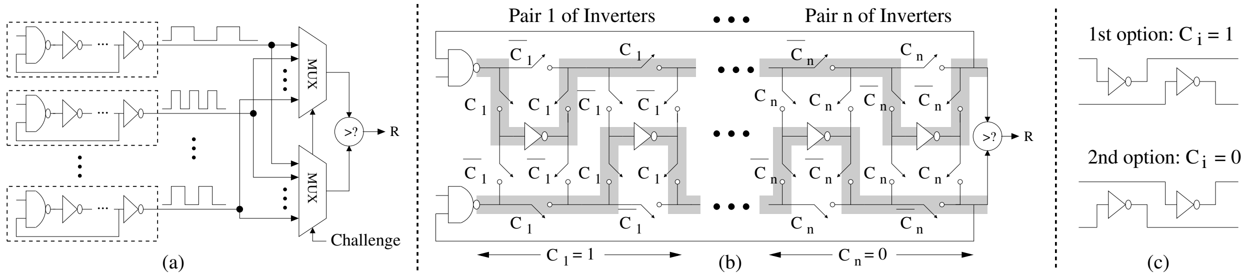


Figure 8: (a) RO-based weak PUF circuit: the frequencies of two ROs are compared to form the response bit R; (b) The proposed Strong PUF based on the idea of group formation: each Inverter in every pair belongs to one of the two ROs; (c) The two options for each pair of Inverters $(1 \leq i \leq n)$

4.1 Case Study of a RO-based Strong PUF

Figure 8(a) shows an example of a popular weak PUF based on identical Ring-Oscillators (ROs), proposed in [5]. The actual frequency of each RO is slightly different from the other ones within the same chip. In such a PUF, the challenges are the selection of any two ROs, and the responses are either 1 or 0, depending on which of the two ROs has a slightly higher frequency. This PUF has a total of $\binom{n}{2}$ possible CRPs, which is polynomial with respect to the number of ROs.

It can be seen that the analog feature in this PUF is the gate delays of the Inverters, which supports the idea of group formation at the device level, i.e., combining a number of Inverters can make ROs with slightly different frequencies. Figure 8(b) depicts the architecture of a RO-based *strong* PUF. Similar to the proposed strong PUF based on STT-MRAM devices, it guarantees the exponential number of independent CRPs by maintaining the following two conditions: 1) fixing the group size to be always equal to n (for $2n$ components); and 2) allowing each component to be in one of the two, bot not both, groups.

This architecture has n pairs of Inverters that play the key roles in obtaining the exponential number of ROs. As illustrated in Figure 8(c), the status of switches for every pair of Inverters are strongly correlated, so that if one Inverter belongs to one RO, the other Inverter in the pair belongs to the other RO (total of two options per pair). This is to ensure that each RO has exactly n Inverters (condition 1). Furthermore, each Inverter can belong to either of ROs, but it cannot belong to both of them at the same time (condition 2). As an example, the highlights in Figure 8(b) correspond to the first and the last pair of Inverters for $C_1 = 1$ and $C_n = 0$, respectively. Since there are two options for each pair of the Inverters, there exists a total of 2^n CRPs in this PUF. Since all these CRPs are independent, this architecture is in fact a strong PUF.

In general, if the group formation is supported by the analog feature of a device, then, the implementation of the two above mentioned conditions in an architecture with $2n$ components can result in a total of 2^n independent CRPs, thus achieving a strong PUF. The first conditions essentially forbids the formation of groups with equal number of cells, other than n cells per group. Otherwise, an attacker can use the CRP information of the smaller groups to determine that of the larger ones. The second condition guarantees the exponential number of CRPs by allowing each component to belong to either of the two groups; thus doubling the search-space of the PUF for each additional component.

5. CONCLUSIONS

In this paper, we present a method for making a strong PUF based on STT-MRAM technology. Simulation results confirmed the effectiveness and uniqueness of the proposed strong PUF. We also discussed the possibility of making a strong PUF in general, by presenting the required conditions both at the device-level and the architecture-level. Even though the security of PUFs is still under investigation, and it is not clear which technology could be used in which applications, the proposed approach of group formation in this paper is of a general framework that can be applied to a wide range of devices for building strong PUFs.

6. REFERENCES

[1] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal. Design and Implementation of PUF-based Unclonable RFID ICs for Anti Counterfeiting and Security Applications. *IEEE International Conference on RFID*, pages 58–64, April 2008.

[2] C. Herder, M. Yu, F. Koushanfar, and S. Devadas. Physical Unclonable Functions and Applications: A Tutorial. *proceedings of the IEEE*, 102:1126–1141, May 2014.

[3] D. Holcomb, W. Burleson, and K. Fu. Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Transactions on Computers*, 58:1198 – 1210, 2009.

[4] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling Attacks on Physical Unclonable Functions. *Proceedings of the 17th ACM conference on Computer and communications security*, pages 237–249, 2010.

[5] G. Sush and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. *IEEE/ACM Design Automation Conference*, pages 9–14, 2007.

[6] S. Wolf, J. Lu, M. Stan, E. Chen, and D. Trege. The Promise of Nanomagnetics and Spintronics for Future Logic and Universal Memory. *proceedings of the IEEE*, pages 2155 – 2168, 2010.

[7] L. Zhang, X. Fong, C.-H. Chang, Z. Kong, and K. Roy. Highly Reliable Memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM. *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2169 – 2172, 2014.