Light-Weight Cipher Based on Hybrid CMOS/STT-MRAM: Power/Area Analysis

M. Kharbouche-Harrari, Gregory Di Pendina, R. Wacquez, B. Dieny, D. Aboulkassimi, J. Postel-Pellerin, J.-M. Portal

Light-Weight Cipher Based on Hybrid CMOS/STT-MRAM : Power/Area Analysis

M. Kharbouche-Harrari*†‡, G. Di Pendina‡, R. Wacquez*, B. Dieny‡, D. Aboulkassimi*, J. Postel-Pellerin† and J-M. Portal†

*CEA Tech, Centre CMP, Equipe Commune CEA Tech - Mines Saint-Etienne, F-13541 Gardanne France

†Aix-Marseille Univ., CNRS, IM2NP, 13397 Marseille Cedex 20, France

‡Univ. Grenoble Alpes, CNRS, CEA, INAC-SPINTEC, 38000 Grenoble, France

***Abstract*—Internet of Things (IoT) applications deployment relies on low-power circuits. Nowadays, on top of power consumption, security concern has become a real issue. Light-Weight Cryptography (LWC) has been developed to answer this challenge. In the lightweight cryptographic landscape, the PRESENT algorithm exhibits low power and small area features. At the same time, emergent resistive memory technologies such as Spin Transfer Torque Magnetic Random Access Memory (STT-MRAM) seem to be a strong candidate for Flash replacement with advanced design features such as hybridization with CMOS. In this context, we propose a hybrid CMOS/STT-MRAM technology for PRESENT cryptographic circuit for normally-off IoT applications. We demonstrate that the hybrid implementation is more power-efficient than the CMOS implementation when switched off for a period longer than 49.1 ms for a 180 nm CMOS core process with an area overhead of x7. Based on this result, trends down to 28 nm node are studied and lead to outstanding performances with a power-effeciency of the hybrid version reached after 185 μs in standby mode. In this scenario, an energy of 6,1 pJ is sufficient to store data in the Non-Volatile Flip-Flops (NVFFs) with a reduced area overhead of x0.23.**

***Index Terms*—Hardware Implementation, STT-MRAM, PRESENT, Hardware Security, IoT, Non-Volatile Memory.**

I. INTRODUCTION

Microelectronics downscaling paved the way to the Internet of Things (IoT) era. These emerging fields lead to exponentially increase communications between the objects [1] [2]. Low power and small area circuits were the main constraints of IoT deployment. However, during these past years, security has become a major concern for IoT at the hardware and software levels. Thus, the security of IoT objects must be considered as a must have feature together with low-power/small area constraints. In this context various emerging ciphers have been developed in order to become the new cryptographic standard by highlighting their low power consumption, area efficiency and speed compared to the AES (Advanced Encryption Standard [3] [4]), its the advent of the Light-Weight Cryptography (LWC) [5]. PRESENT in the LWC landscape is a symmetric Substitution-Permutation Network crypto-algorithm [6] that exhibits very low-power, small area together with high speed encryption performance. This algorithm is an ISO/IEC 29192-2 :2012 standard [7].

At the same time, emerging resistive memory technologies appear to be a promising alternative to eFlash standard for circuits supporting IoT applications. Indeed, such memories can be integrated in the BEoL (Back-End of Line) of CMOS process and have working voltages compatible with the logic part of the circuit. From this remark, hybrid CMOS/Spin-Transfer Torque Magnetic Random Access Memory (STT-MRAM) design can clearly outperform regular CMOS implementation in term of power consumption since their standby power is nil. Consequently, the integration of this promising hybrid technology (CMOS/STT-MRAM) is valuable to be studied for an hybrid PRESENT cryptographic circuit. Even if the CMOS circuit is attacked, the circuit can resume its last saved operation by getting back the stored data in the STT-MRAM junctions. To the best of our knowledge this work is one of the first to establish an hybrid CMOS/Non-Volatile memory cipher [8]. Beyond security aspects, the impact of the hybridization must be determined at the circuit level in terms of power consumption versus area overhead for normally-off applications, through technology scaling, i.e. CMOS scaling as well as Magnetic Tunnel Junction (MTJ) diameter scaling.

This study is performed at the circuit level for a mature technological node (CMOS 180 nm and MTJ diameter 200 nm) for its robustness and availability for manufacturing and evaluated from Non-Volatile Flip Flops (NVFFs) simulations for advanced nodes (CMOS 28 nm and MTJ diameter 40 nm). First of all, these hybrid solutions are evaluated compared to a pure 180 nm CMOS solution. On the one hand, the two first scenarios proposed are full serial programming and partial parallel programming using a 180 nm CMOS technology and a 200 nm MTJ diameter. Both scenarios achieve power reduction after respectively 675 ms and 49 ms of standby operation but with large area consumption, respectively x9 and x8. The third and fourth scenarios, on the other hand, outline a MTJ reduction from 200 nm down to 40 nm and a fully parallel writing scheme, with respectively a 180 nm and 28 nm CMOS platform. In the best case, the backup consumption can be lowered up to 99 % with an area overhead limited to x0.23. This full analysis at the circuit level shows that the hybrid PRESENT can be a real alternative to CMOS, if the MTJ diameter allows a full parallel store/restore process.

After a background introduction in section II, this paper describes the hybrid PRESENT implementations in section III. Section IV presents the power estimation for the different PRESENT implementations. Section V concludes this paper.

II. Background

A. The STT-MRAM Technology

The STT-MRAM technology is a two terminal structure based on MTJs which are nanostructures composed of ferromagnetic layers separated by an insulating tunnel barrier (represented in Figure 1.a) [9]. While the reference layer magnetization is fixed, the magnetization of the storage layer can be modified from one direction to its opposite as illustrated in Figure 1.a. When the storage layer is in the same (resp. opposite) direction as the reference layer then the junction is in a Parallel P (resp. Anti-Parallel AP) configuration as illustrated in Figure 1.b. The read/write functions are carried out by a spin-polarized current injected through the MTJ stack. The written value depends on the current direction. This technology has been identified as one of the most promising emerging technology for a large range of applications by the International Technology Roadmap for Semiconductors (ITRS) [10]. Indeed, STT-MRAM technology is compatible with CMOS process, has a high integration density and uses low voltage levels for reading and writing operations [11] (making possible the STT-MRAM/CMOS hybridization) and exhibits a reduction of its power consumption with downscaling. As plotted in Figure 1.c, Landau-Lifshitz-Gilbert (LLG) equations [12] [13] show that the MTJ writing current decreases with its diameter, opening the way to ultra dense hybrid-design with reduced power consumption in advanced technology nodes and instantaneous store/restore process.

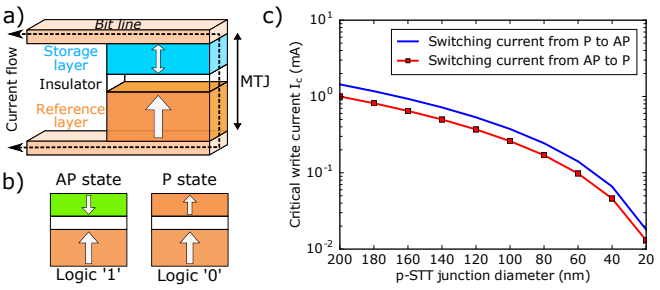

Fig. 1. a) The MTJ structure and current flow in STT-MRAM. b) P and AP states c) Evolution of the current as a function of the junction diameter.

B. PRESENT cryptographic algorithm

The PRESENT cryptographic algorithm [6] is a Substitution-Permutation Network block cipher implemented with a serial architecture fashion as illustrated in Figure 2. The ciphertext of this cryptographic algorithm is reached after the 32nd clock cycle. The first step of this cryptographic algorithm is to XOR the main plaintext and the master key of this cipher. The result of this operation gets through bit-sliced substitution layers and a permutation circuit as specified in [6]. Meanwhile the key is updated by :

- Shifting the 80-bits content of the key by 61-bits to the right. If the master key can be defined as $[k_{79} \cdots k_{20} k_{19} k_{18} k_{17} \cdots k_0]$ where k_i is the ith bit of the considered key. Then the resultant key of this shift is $[k_{18} k_{17} \cdots k_1 k_0 k_{79} \cdots k_{20} k_{19}]$ (illustrated in Figure 2).
- Altering this (i+1)th key as described below:
  - The 0th up to the 14th bits remain unchanged.
  - The 15th up to the 19th bits with the counter's content go through a XOR function. For each key update the counter is incremented.
  - The 20th up to the 75th bits remain unchanged.
  - The 76th up to the 79th bits are substituted through a substitution box (SBox in Figure 2).

A XOR function is then realised between the 1st updates of the plaintext and key. This operation is repeated 31 times.

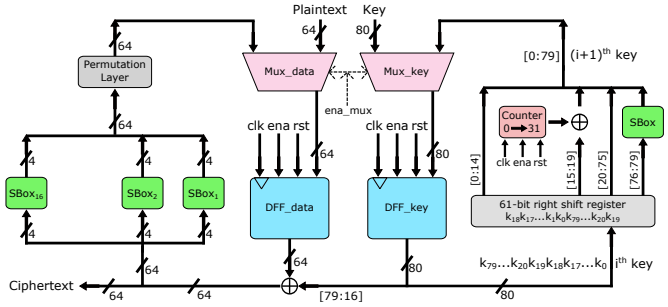

Fig. 2. PRESENT algorithm implemented in serial (minimal area solution).

III. Hybrid PRESENT

A. Design description

The main contribution of this paper is the evaluation of four hybrid PRESENT cryptographic circuits based on hybrid NVFFs (CMOS technology with STT-MRAM junctions). The main difference between these circuits and the original CMOS PRESENT circuit is that some FFs have been strategically replaced by the NVFFs defined in [14]. The main attribute of this component is the addition of two magnetic junctions operating in differential mode and a power-gating circuitry. By changing the registers DFF_data, DFF_key and counter (as represented in Figure 2) from volatile to non-volatile leads to store the data, key and counter round being currently treated in order to restore them at a later time. This new kind of cipher allows to have a storing (resp. restoring) system before (resp. after) the system poweroff. Indeed, there is no standby consumption when the circuit is powered off since saved data are non-volatile. It is important to note that hybrid circuits open new functionalities for security purpose, like for example restoring proper context when attacks are detected.

B. CMOS vs Hybrid power consumption

In this context, the critical aspect for the approval of this solution is the evaluation of the store/restore power energies (resp. E_{store} and $E_{restore}$) in the hybrid architecture versus the standby energy $E_{standby\ CMOS}$ of the pure CMOS at circuit level, as depicted in Figure 3. The area estimation for mature and advanced CMOS/STT-MRAM technology nodes is also a crucial consideration that has to be taken into account.

Thus, the sleeping energy ($E_{sleep\ hybrid}$) of this hybrid cryptographic algorithm can be defined as in Equation 1 and in Figure 3 as :

$$E_{sleep\ hybrid} = E_{store} + E_{restore} \quad (1)$$

Hence, in order to determine the minimal standby time $t_{standby}$ for which the hybrid cipher would be more power-efficient than the CMOS PRESENT cryptographic algorithm, the comparison of the energy consumption while the ciphers are OFF is necessary. The hybrid PRESENT is more efficient for $E_{sleep\ hybrid} < E_{standby\ CMOS}$ With: $E_{standby\ CMOS} = P_{static\ CMOS} * t_{standby}$.

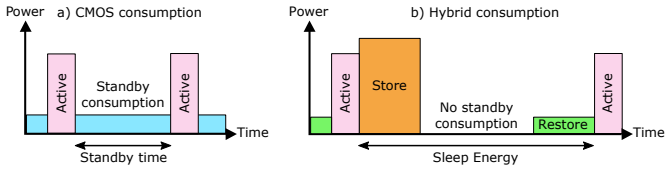

Fig. 3. a) PRESENT CMOS power consumption for active or standby mode. b) Hybrid PRESENT power consumption for active or sleep mode.

IV. Power Estimation

This section is devoted to the analysis of the different scenarios implemented : fully serial (scenario #1) / partially parallel (scenario #2) / fully parallel (scenarios #3 & #4) programming schemes. For all these scenarios:

- Area is evaluated in term of Gate Equivalents (GE) since NVFF transistors sizing may strongly vary depending on the involved programming current. Knowing that standard FFs are equivalent to 7 GE, the worst case is for 200 nm diameter MTJ where NVFFs [14] are equivalent to 99 GE area, whereas considering 40 nm diameter MTJ, NVFFs [15] are only equivalent to 13 GE area. Moreover, control circuit overhead is also considered. The GE metric has been validated through full circuit layout in the case of a 180 nm CMOS process and 200 nm MTJ diameter (scenario #1 and scenario #2). Scenarios #1 and #2 area demand is respectively 352836 μm^2 and 294294 μm^2 whereas the implemented pure CMOS version represents 39800 μm^2. Outlined scenarios #3 and #4 area is estimated based on the realised layouts and NVFF sizes.
- Energy consumption during storing process is estimated at NVFF level and then computed depending on the store configuration (serial/partially parallel, fully parallel), whereas the restore process is assumed to be a full parallel process, thus the restoring energy is directly the energy of one NVFF multiplied by the number of NVFFs (151).

These different scenarios are compared to the pure CMOS cipher which counts 1922 GE for its area and a standby consumption feature : $P_{static\ CMOS}$ that is determined to be equal to 78,27 μW and 32,9 nW for a clock-gated version.

For the stated scenarios, the cipher operates as follows:

- Backup or store operation : the MTJs are written.
  Before powering off the cryptographic algorithm, the writing circuit is activated. When the control signal to write the MTJs Wr is set to 1, all the MTJs of the NVFFs are written. n clock cycles are needed in order to store all the data, with n = 151 for the first scenario (fully serial), 30 for the second one (partially parallel), and 1 for the third and fourth scenarios (fully parallel).
- The cipher can then be turned off.
- Restore operation : the MTJs are read.
  After the cipher wake-up, stored data can be restored in the NVFFs. When the read signal RdN = 0 (active at low level), all the MTJs are read in parallel and the data is restored into the NVFFs.
- Cipher resume :
  When all the information contained in the NVFFs are resumed, the cipher can then proceed its operation and finish the data encryption without losing any information.

A. Power Consumption PRESENT circuit on mature technology (180 nm CMOS / 200 nm MTJ)

First of all, if we consider a 180 nm CMOS technology node with 200 nm tunnel junction diameter, the energy consumption of 151 NVFFs would be too significant if the MTJs are written in parallel. Thus, serial or partially parallel programming has to be set-up. We propose to evaluate two circuits fully serial/partially parallel to write the MTJs of the NVFFs.

1) Scenario #1 (fully serial): The MTJs are written one by one in serial through 151 clock cycles as illustrated in Figure 4. In terms of area, this implemented hybrid cryptographic solution needs 18264 GE which is almost 9 times larger than the pure CMOS implementation. This strong area overhead is due to larger NVFFs (integrating supplementary power-gating circuitry) than classical FFs and to the circuits controlling the read/write process in the MTJs.

Moreover, the $E_{sleep\ hybrid}$ is determined to be equal to 22,22 nJ. So, for a 10 MHz clock frequency (for shift acknowledgement of the write operation in the MTJs), the minimal standby time $t_{standby}$ for which this implementation scenario is power-efficient is 675 ms. If the circuit is OFF for a period of time longer than this $t_{standby}$ value, then the hybrid CMOS/STT-MRAM is more power-efficient than the pure CMOS cipher variant.

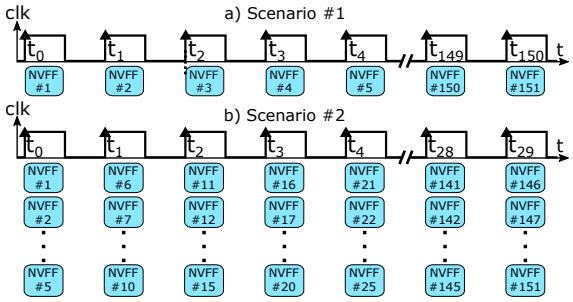

Fig. 4. Writing scenarios for the hybrid PRESENT cipher. a) The first implemented scenario (fully serial). b) The second scenario (partially parallel).

2) Scenario #2 (partially parallel): The scenario #2 is based on partially parallel storing process. In this case, the NVFFs are written five by five, during 30 clock cycles as depicted in Figure 4. This 2nd hybrid cryptographic solution needs 16382 GE which is almost 8 times larger than the pure CMOS version. In this case, $E_{sleep\ hybrid}$ was determined to

be equal to 1,61 nJ. Thus, this implementation is more power-efficient and presents a lower area overhead versus scenario #1. For the same 10 MHz clock frequency, the minimal standby time for which this hybrid structure of the PRESENT cryptographic algorithm is power-efficient is 49,1 ms.

This evaluation of the hybrid PRESENT circuits features designed on a mature technology (180 nm CMOS technology and a 200 nm diameter MTJ junction) exhibits a good power efficiency that has to be balanced by a large area overhead. Since the area overhead is linked to the writing current and thus to the junction diameter, it is interesting to study the evolution of the hybrid PRESENT circuit for different junctions sizes as well as for an advanced CMOS technology node, as described next section through scenarios #3 & #4.

B. 40 nm MTJs diameters : From 180 nm down to 28 nm FDSOI CMOS node

Knowing that the area of the hybrid circuit is directly linked to the technology node and to the junction diameter through NVFF sizing, the proposed hybrid PRESENT circuit is evaluated for two more scenarios:

- Scenario #3 : CMOS mature (180 nm) and advanced MTJ technology (40 nm), already available for manufacturing.
- Scenario #4 : Advanced CMOS (28 nm) and advanced MTJ technology (40 nm), most advanced technology for manufacturing in the forthcoming years.

The NVFF architecture is the one defined in [15] since with 40 nm diameter junction, current constraints are relaxed, thus allowing the use of more compact architectures. As depicted in Figure 5.a, the write energy (for a given 10 ns write pulse length) needed to switch both MTJs in the NVFF decreases with the MTJ diameter, which is directly linked to the critical current decrease (see Figure 1.c). With this evolution in mind and considering a middle diameter of 80 nm as reference, for a similar NVFF architecture the sizing of MOS transistors follow the critical current evolution giving a strong area increase for diameter above 80 nm and area reduction below as illustrated in Figure 5.b.

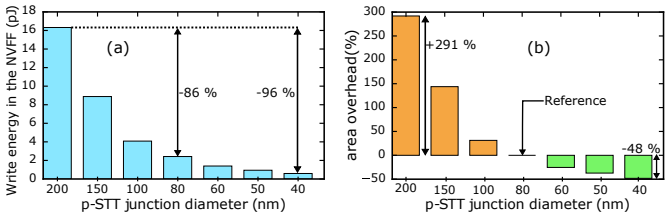

Fig. 5. a) NVFF writing energy evolution as a function of the MTJ diameter. b) NVFF area overhead as a function of the MTJ diameter.

1) Scenario #3 - CMOS mature (180 nm) and advanced MTJ technology (200 nm down to 40 nm): Thanks to the drastic reduction of the writing current, scenario #3 allows a full parallel process to store and restore data in the NVFFs. Thus area overhead is reduced thanks to the NVFF downsizing and light control logic (shift process is not necessary). Indeed, this scenario needs 2843 GE, representing an area overhead of x0.48 versus the pure CMOS solution. Moreover, the store/restore energy is reduced to 90 pJ, thus the minimal standby time defined as $t_{standby}$ is reduced down to 2,7 ms.

2) Scenario #4 - Advanced CMOS (28 nm) and advanced MTJ technology (40 nm): The NVFF [15] was also tested for an advanced 28 nm FDSOI CMOS platform and 40 nm diameter junction. Here also, as for scenario #3, since the MTJs size is highly reduced, the writing current is also drastically scaled down (as represented in Figure 1.c), and thus fully parallel store/restore process is allowed. Moreover, thanks to the enhanced current driving capacity of the 28 nm MOS transistors, NVFFs area is even closer to its pure CMOS counterparts. Thus area is limited to 2367 GE and store energy reduces downto 6,1 pJ.

Area (using similar CMOS node for hybrid and pure CMOS) as well as power consumption for store/restore operation evolution for each scenario are given in Figure 6. On this plot, it clearly appears that NVFF based PRESENT design is a real alternative in terms of power and area for advanced CMOS node versus pure CMOS when considering a fully parallel store/restore process (MTJs diameter below 80 nm).

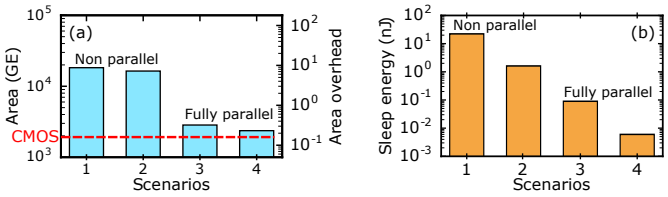

Fig. 6. a) Evaluation of the area in GE and the overhead evolution compared to the pure CMOS structure. b) Sleep energy evolution (nJ).

V. CONCLUSIONS

IoT deployment is based on low-power circuits with security standards that must be kept high. In this paper, we established the hybrid technology interest in cryptographic algorithms for normally-off applications. We have demonstrated from various scenarios (from CMOS 180 nm / 200 nm MTJ down to CMOS 28 nm / 40 nm MTJ) that only fully parallel write process reduces strongly the area overhead from a factor x8 down to 0.23. This area saving added to the fully parallel write process to save data in the STT-MRAMs is directly linked to the MTJ diameter and its direct impact on the writing current. In fact, with the MTJ downscaling the needed current to switch the junction is reduced. This current reduction has a strong impact on energy reduction versus classical CMOS solution for normally-off operation. The different structures presented in this paper were evaluated in term of minimal standby mode period after which the gain in power consumption is noticeable. For the most advanced scenario, this value was determined to be equal to 185 μs. Finally, it is important to note that the 180 nm CMOS process and 200 nm option is chosen as the reference scenario since these implementations have been taped-out and will be used for security evaluation in future works.

REFERENCES

[1] V. Gazis, M. Goertz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, and F. Zeiger, "Short Paper: IoT: Challenges, projects, architectures," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Feb. 2015, pp. 145–147.

[2] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[3] J. Daemen and V. Rijmen, "The Block Cipher Rijndael," in *Lecture Notes in Computer Science - LNCS*, vol. 1820, Jan. 1998, pp. 277–284.

[4] I. T. L. Computer Security Division, "AES Development - Cryptographic Standards and Guidelines | CSRC." [Online]. Available: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

[5] Jaber Hosseinzadeh and Maghsoud Hosseinzadeh, "A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers : Hardware and Software Implementation," *Advances in Computer Science: an International Journal*, pp. 31–41, Jul. 2016.

[6] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, ser. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Sep. 2007, pp. 450–466.

[7] "ISO/IEC 29192-2:2012 Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers," Jan. 2012. [Online]. Available: https://www.iso.org/standard/56552.html

[8] A. Chakraborty, A. Mondal, and A. Srivastava, "Correlation power analysis attack against STT-MRAM based cyptosystems," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2017, pp. 171–171.

[9] Y. Huai, "Spin-transfer torque MRAM (STT-MRAM): Challenges and prospects," *AAPPS*, vol. 18, 2008.

[10] "2013 International Technology Roadmap for Semiconductors (ITRS)." [Online]. Available: https://www.semiconductors.org/resources/2013-international-technology-roadmap-for-semiconductors-itrs/

[11] S. Senni, L. Torres, G. Sassatelli, A. Gamatie, and B. Mussard, "Exploring MRAM Technologies for Energy Efficient Systems-On-Chip," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 6, no. 3, pp. 279–292, Sep. 2016.

[12] L. Landau and E. Lifshitz, "On the theory of the dispersion of magnetic permeability in ferromagnetic bodies," *Phys. Z. Sowjetunion*, vol. 8, no. 153, pp. 101–114, 1935.

[13] J. C. Slonczewski, "Currents, torques, and polarization factors in magnetic tunnel junctions," *Physical Review B*, vol. 71, no. 2, p. 024411, Jan. 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevB.71.024411

[14] M. Tahoori, S. M. Nair, R. Bishnoi, S. Senni, J. Mohdad, F. Mailly, L. Torres, P. Benoit, A. Gamatie, P. Nouet, F. Ouattara, G. Sassatelli, K. Jabeur, P. Vanhauwaert, A. Atitoaie, I. Firastrau, G. D. Pendina, and G. Prenat, "Using multifunctional standardized stack as universal spintronic technology for IoT," in *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, Mar. 2018, pp. 931–936.

[15] K. Ali, F. Li, S. Y. H. Lua, and C. Heng, "Compact spin transfer torque non-volatile flip flop design for power-gating architecture," in *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Oct. 2016, pp. 119–122.