2023 Design, Automation & Test in Europe Conference (DATE 2023)

Security Evaluation of a Hybrid CMOS/MRAM Ascon Hardware Implementation

Nathan Roussel, Olivier Potin, Jean-Max Dutertre and Jean-Baptiste Rigaud
Mines Saint-Etienne, CEA, Leti, Centre CMP F-13541 Gardanne, France
{nathan.roussel, olivier.potin, dutertre, rigaud}@emse.fr

Abstract—**As the number of IoT objects is growing fast, power consumption and security become a major concern in the design of integrated circuits. Lightweight Cryptography (LWC) algorithms aim to secure the communications of these connected objects at the lowest energy impact. To reduce the energy footprint of cryptographic primitives, several LWC hardware implementations embedding hybrid CMOS/MRAM-based cells have been investigated. These architectures use the non-volatile characteristic of MRAM to store data manipulated in the algorithm computation. We provide in this work a security evaluation of a hybrid CMOS/MRAM hardware implementation of the ASCON cipher, a finalist of the National Institute of Standards and Technology LWC contest. We focus on a simulation flow using the current EDA tools capable of carrying out power analysis for side-channel attacks, for the purpose of assessing potential weaknesses of MRAM hybridization. Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) are conducted on the post-route and parasitic annoted netlist of the design. The results show that the hybrid implementation does not significantly lower the security feature compared to a reference CMOS implementation.**

Index Terms—**ASCON, LWC, STT-MRAM, MTJ, Side-channel attack**

I. Introduction

In recent years, the Internet of Things (IoT) objects have played a crucial role for the deployment of smart city, smart home, smart health, and more. These emerging fields have resulted in battery-less IoT devices (energy harvesting of ambient sources) [1], emphasizing the necessity to develop energy efficient architectures. Furthermore, many IoT objects share sensitive data, thus implying to protect IoT nodes from external threats [2]. However, conventional cryptography algorithms are not well suited for resource-constrained environments. To fulfill security, power and area requirements of IoT devices, several Lightweight Cryptography (LWC) algorithms have emerged, offering several security features and low energy [3].

The use of energy harvesters has enabled IoT systems to operate autonomously. Nonetheless, they cannot ensure a continuous operation of IoT devices for two main reasons. First, the source availability is not permanent. Second, the energy delivered by energy harvesters could be depleted before the end of device operations. Given that data manipulated in hardware implementation of LWC algorithms are volatile, all intermediate states will be lost in case of power failure. This implies additional energy and time resources due to the recalculation of the algorithm from the first step.

To address the volatility issue of current architectures, the use of emerging memories with non-volatility criteria seems to be an efficient strategy. Among these innovating devices, the Spin Transfer Torque MRAM (STT-MRAM) has been identified as a promising candidate for implementing low-power applications, given its low-power requirements, its compliance with CMOS process and its high endurance [4].

In this regard, a hardware implementation of the ASCON authenticated cipher associating CMOS and STT-MRAM has already been put forward in the literature [5]. This implementation has been designed with non-volatile flip-flops (NVFF) in order to save intermediate state and the algorithm progression. The proposed architecture can save up to 48% energy in case of power failure, by avoiding a loss of information. However, the outlined results are issued from a synthesized netlist of ASCON. The authors did not address the placement routing of CMOS/MRAM cells, and therefore did not process the complete ASIC design flow. Furthermore, no security evaluation has been realized to ascertain that the hybrid circuit does not reduce the security level of a CMOS implementation of ASCON.

In this paper, we extend the work presented on the hybrid ASCON by performing the placement routing and verification steps of the ASIC design flow, using existing EDA tools. We target the CMOS 28nm FD-SOI Design Kit (DK) from STMicroelectronics. We provide a more accurate power characterization, by including the parasitic effect of a full-routed design. We evaluate the security of the hybrid architecture by implementing existing side-channel analysis on ASCON.

This paper is structured as follows. In section II, a description of the ASCON cipher and the STT-MRAM as well as the benefits of hybrid implementations are presented. Existing side-channel attacks on ASCON are also described. Section III is devoted to the placement routing of the hybrid implementation. The security evaluation of ASCON is presented in section IV. The results are discussed in section V. Finally, we conclude in the last section.

II. Background

A. Description of Ascon

ASCON is an Authenticated Encryption with Associated Data (AEAD) algorithm based on sponge construction [6]. It was already selected as the primary choice for lightweight authenticated encryption in CAESAR competition [7]. It is also part of the finalists of LWC standardization process initiated by the National Institute of Standards and Technology (NIST) [8].

This work was supported by the French National Research Agency (ANR) under grant ANR-19-CE39-0010.

978-3-9819263-7-8/DATE23/© 2023 EDAA

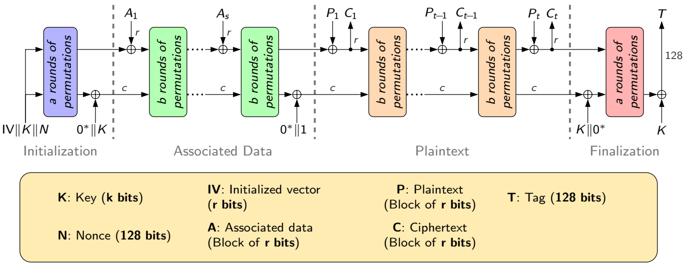

Fig. 1. Sponge construction of ASCON encryption process

It is composed of 320-bit state S which is split into a part S_r of r bits and a part S_c of c bits. The rate r and the capacity $c = 320 - r$ as well as the number of rounds are derived from ASCON variants.

The initial state is constituted of a constant vector, a 128-bit nonce and the key as depicted in Fig 1. The associated data and the plaintext are processed after the initialization phase and injected into the algorithm by block of r bits. The corresponding ciphertext is squeezed out of the sponge construction. In the finalization phase, the key is xored with the algorithm end state to produce the 128-bit tag.

The permutation of ASCON is a consecutive execution of the round transformation. The internal state is divided into five 64-bit words x_i during the application of the permutation. The round transformation is composed of a constant addition to x_2, a substitution layer and a diffusion layer. The substitution layer is a nonlinear operation consisting in an application of a 5-bit Sbox.

The version of the algorithm used in this paper is ASCON-128, leading to $r = 64$, $c = 256$, $k = 128$, $a = 12$ and $b = 6$.

B. STT-MRAM

The basic element of an STT-MRAM is a Magnetic Tunnel Junction (MTJ) formed with a thin oxide barrier sandwiched by two ferromagnetic layers (FM). An MTJ stack with its different configurations is represented in Fig 2. The magnetization of the reference FM layer is fixed, while the other FM layer can take either parallel or antiparallel state (resp. P and AP). When the two FM layers exhibit the same magnetization direction, the MTJ has a low resistance (denoted R_P), whereas it has a high resistance (R_{AP}) when the two FM layers show an opposite magnetization direction. The resistance ratio between the two magnetic states is characterized by the Tunnel Magnetoresistance Ratio $TMR = (R_{AP} - R_P)/R_P$. This ratio allows us to store data and discriminate the P state (logic state 0) from the AP state (logic state 1).

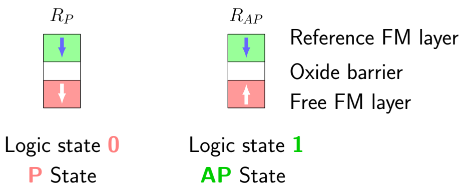

Fig. 2. MTJ with P and AP states

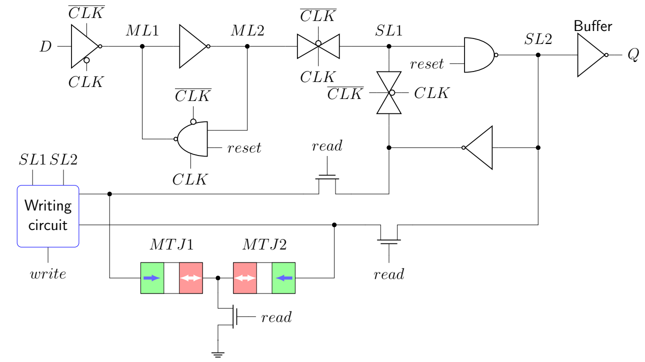

Fig. 3. Non-volatile flip-flop schematic

C. Benefits of hybrid CMOS/STT-MRAM architecture

Several CMOS/STT-MRAM implementations of cryptographic primitives have already been reported in the literature [9, 10]. They have implemented non-volatile flip-flop and non-volatile logic. Their works demonstrated MRAM-based architecture can reduce the energy footprint of cryptographic calculation. In [5], the authors propose a hybrid design kit to conceive a MRAM-based implementation of the ASCON cipher. This circuit is capable of saving the intermediate state and the control logic (counter value and FSM states). They claim that the proposed architecture of the cipher ensures energy savings ranging from 11% to 48% compared to a CMOS native implementation in case of power failure. The area overhead is estimated at 5.5%. These results were extracted from post synthesis simulations. In this work, we followed their methodology to conceive our hybrid circuit of ASCON.

D. Passive Side-Channel attacks on Ascon

Power Analysis (PA) is a widely used hardware attacks to retrieve the secret key from cryptographic devices. The well-known Differential Power Analysis (DPA) [11] and Correlation Power Analysis (CPA) [12] attacks require a leakage model to perform a complete key recovery attack.

Both DPA and CPA have been conducted on hardware implementations of the ASCON cipher, using the Hamming distance model [13–15]. They targeted either the intermediate registers or the substitution layer.

New security flaws may have been introduced by the non-volatile architecture of ASCON. Nevertheless, no initial analysis has been performed to ensure such design does not pave the way for new critical vulnerabilities.

In this article, DPA and CPA will be carried out on a hybrid implementation of ASCON. The results will be compared to a pure CMOS implementation to assess whether or not the MRAM-based architecture is more vulnerable to passive side-channel attacks. To this end, specific methodology using the existing EDA tools will be set up.

III. PHYSICAL IMPLEMENTATION OF THE HYBRID CIRCUIT

The schematic of the implemented NVFF is given in Fig 3. It has been designed from classical Transmission Gate D Flip-Flop (TGDFF). For electrical simulations, the MTJ compact model from [16] was used. The MTJ parameters are given in

TABLE I
MTJ PARAMETERS USED IN THE STT COMPACT MODEL

Parameters	Description	Value
D	MTJ diameter	28 nm
$TMR(0)$	TMR at 0V, 300K	1.5
R_p	Parallel resistance (P state)	4.87 $k\Omega$
$RA(0)$	Resistance area product at 0V, 300K	3 $\Omega.\mu m^2$
t_{ox}	Thickness of the oxide barrier	1.48 nm
t_{fl}	Thickness of the free layer	1.3 nm

Table I. All values are retrieved from MRAM cells state-of-the-art [4, 17].

To investigate and confirm the functionality of the NVFF under process variation, Monte Carlo simulations with 3σ variations have been achieved with Cadence Spectre simulator. Regarding the NVFF layout generation, we have increased the CMOS DFF area by 20% in order to represent the cost of the non-volatile part. This allows us to provide an overall estimation of the hybrid ASCON circuit.

The NVFF logical library (liberty file) was generated thanks to Cadence Liberate. The produced file was then compiled and converted into database format (.db) with Synopsys Library Compiler. The power consumption related to non-volatile circuitry was defined as leakage power in the liberty file to ensure a correct interpretation by downstream power analysis tools.

To carry out logical simulations with NVFF cells, a verilog model based on User-Defined Primitives (UDPs) was created and validated with Siemens Questasim simulator.

As stated earlier, the hybrid implementation aims to restart its computation from a previous state saved in MTJ devices in case of power loss to save energy. To do so, the intermediate state register and the control register must be hybridized. In consequence, the ASCON flip-flops of its counter, its FSM and its permutation were substituted by NVFFs. The circuit thus contains 329 NVFFs. Regarding the operating conditions, the frequency is set to 100MHz and the voltage is fixed at 1V. One round transformation is executed in a single clock cycle.

Synopsys Design Compiler was used to synthesize the design. Post-synthesis simulations with Standard Delay Format (SDF) back annotation was conducted to ascertain the functionality of the synthesized circuit.

Providing accurate sizing characteristics of the cell is compulsory to place and route an NVFF-based circuit. In this respect, the physical library, comprising the abstract view and the Library Exchange Format (LEF) file was produced. Note that the cell dimensions specified in the LEF file is a multiple integer of site. A site is the minimum unit of placement defined by the DK. During the manufacturing process, the MTJ are typically inserted between Metal 3 and Metal 4 [18]. Thus, obstruction zones have been specified to take into account the area occupied by the MTJs.

A reference CMOS implementation of the cipher has been also designed to estimate the impact of non-volatile circuitry in terms of area and power consumption. The placement and routing have been conducted with Cadence Innovus. The layout of the hybrid implementation is given in Fig 4. The same floorplan size was used for both circuits. The input and output pins are disposed along the circuit. Pins related to non-volatile circuit are managed externally, as primary input. This enables to easily control the read and write operations, to perform further security analysis.

TABLE II
AREA OF THE ASCON HYBRID CIRCUIT

GE: Gate Equivalent	ASCON CMOS		ASCON CMOS/MRAM		Δ (%)
Area	μm^2	GE	μm^2	GE	μm^2
Total	5001.1	10214.7	5275.4	10774.9	5.5

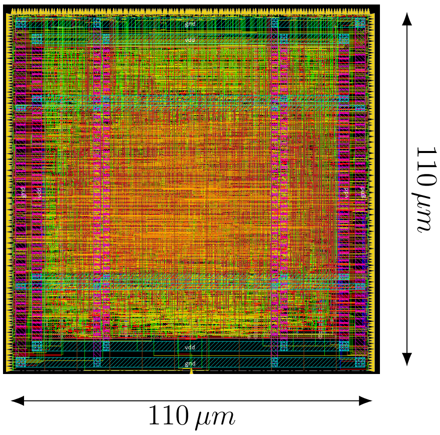

Fig. 4. Layout of ASCON hybrid circuit

TABLE III
ENERGY CONSUMPTION FOR ONE ENCRYPTION IN CASE OF POWER FAILURE AFTER ASSOCIATED DATA PROCESSING

	ASCON CMOS	ASCON CMOS/MRAM	
Associated data size	Energy (pJ)	Energy (pJ)	Δ (%)
64-bit	624.4	521.2	19.8
256-bit	959.9	689	39.1
512-bit	1407.2	912.6	54.2

The area comparison is reported in Table II. The core density (without physical cells) of the CMOS and hybrid implementation is 61.8% and 65.2% respectively, for a floorplan size of $110\,\mu m \times 110\,\mu m$.

Design Rule Check (DRC) and Layout Versus Schematic (LVS) verifications have been performed with Cadence PVS. The NVFFs are defined as black box cells. The Standard Parasitic Extraction Format (SPEF) file containing parasitic information of the design is produced with Cadence Quantus. This file allows producing a more accurate power estimation. The circuit functionality has been validated thanks to post-route simulation with Siemens Questasim. Synopsys PrimePower tool was used to estimate the power consumption of the circuit.

The hybrid architecture is capable of restoring the previous state in case of power failure. The energy required to write and restore data must be lower than the energy required to recompute lost data plus the energy wasted due to power loss. In other words, the hybrid implementation is more energy efficient than the CMOS implementation when $E_{write} + E_{restore} < E_{wasted} + E_{recomputation}$. As a reminder, the encryption process is composed of 4 phases (see Fig. 1).

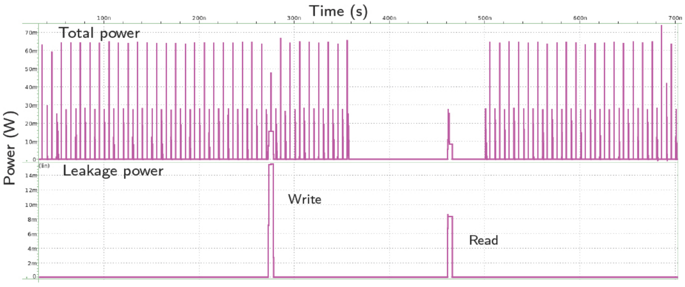

Fig. 5. Power over time for one encryption with write and read operations

With this circuit, it is not possible to save the progression of the last two phases, as it would also require to hybridize cipher and tag registers. The comparison between both implementations after a power failure at the end of AD processing as function of the AD size are summed up in Table III. These results are extracted from post-route simulation with parasitic annotation. The hybrid implementation outperforms the CMOS implementation in terms of energy consumption when power suddenly shuts down, by 19% to 54%, for an area overhead of 5.5%. The power waveform issued from PrimePower for one encryption is plotted in Fig 5.

IV. Side-channel analysis of the hybrid circuit

A. *Simulation flow considered for power analysis*

As stated in the previous section, electrical behavior of the MTJ is described thanks to the STT compact model from [16]. A significant set of power traces (∼20,000) is needed to perform power analysis. The use of an electrical simulator cannot be considered as it would require high computational and time resources. Accordingly, a dedicated simulation flow based on VCD activity file has been implemented. It is depicted in Fig 6. A similar approach has already been presented in [19].

Synopsys PrimePower was used to generate power waveforms. To do so, VCD file is generated thanks to post-route simulation with Siemens Questasim. The simulation time is reduced by the elaboration file feature of the logical simulator. Questasim simulator command is invoked and directly send the output VCD file to PrimePower. No VCD is stored on the disk, enabling significant space saving (∼16 GB for 20,000 traces). The power traces are then converted into Comma-Separated Values (CSV) format by Synopsys CustomWave. The pointless header created by CustomWave is deleted thanks to a shell script (*sed* command). The power waveform generation from VCD to CSV takes approximately 10 hours for 20,000 traces.

B. *Power analysis on Ascon*

For passive side-channel analysis, either the intermediate state register [13, 14] or the S-box output [15] within the Initialization phase are targeted. As the substitution layer has not been modified in the hybrid implementation, we target the intermediate state register. The state at initialization is formed by a constant vector IV, the key $K = K_0||K_1 = x_1||x_2$ and a public nonce $N = N_0||N_1 = x_3||x_4$. Both Hamming Distance (HD) and Hamming Weight (HW) model can be used [14]. We use the HW model in this work. Only the key part remains unknown. We denote the initialized registers as x_j, the substitution layer outputs as s_j and the register outputs after one round computation as y_j. The output register y_0 is defined by:

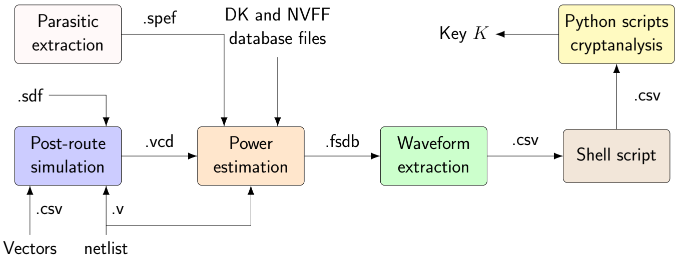

Fig. 6. Simulation flow implemented for side-channel analysis

$$y_0 = s_0 \oplus (s_0 >>> 19) \oplus (s_0 >>> 28) \tag{1}$$

With:

$$s_0 = x_1(x_4+1) + x_1x_2 + x_1x_0 + x_3 + x_2 + x_0 \tag{2}$$

All bits that do have a constant impact on power consumption can be removed:

$$s_0 = x_1(x_4+1) + x_3 = k_0(n_1+1) + n_0 \tag{3}$$

The Sbox output depends on one bit from key register (K_0) and two bits from two registers of the nonce (N_0 and N_1). By injecting (3) into (1), we get:

$$\begin{aligned} y_0^i = k_0^i(n_1^i+1) + n_0^i + k_0^{i+45}(n_1^{i+45}+1) \\ + n_0^{i+45} + k_0^{i+36}(n_1^{i+36}+1) + n_0^{i+36} \end{aligned} \tag{4}$$

To retrieve the second key part, the register y_1 can be attacked. In the same way as above, y_1 can be expressed as:

$$\begin{aligned} y_1^i = n_0^i(l^i+1) + n_1^i + n_0^{i+3}(l^{i+3}+1) + n_1^{i+3} \\ + n_0^{i+25}(l^{i+25}+1) + n_1^{i+25} \end{aligned} \tag{5}$$

Where $l^i = k_0^i + k_1^i + c_{round}$. By varying the nonce for each run, the key can be recovered entirely. Note that (5) implies to find K_0 before K_1. More details of the attack can be found in [13].

To conduct both DPA and CPA, four cases have been investigated: power analysis on native CMOS implementation (case #1), on hybrid implementation without non-volatile use (case #2), on hybrid implementation during read operation (case #3) and on hybrid implementation during write operation (case #4). For the case #3, we write the MTJ devices at the first round of the initialization stage, and read back the MTJs several clock cycles later. For all analysis, the success rate $SR = \frac{\#key\ bits\ correct}{key\ size}$ versus the number of traces has been computed. We have considered the attack successful for $SR = 1$. Nonetheless, it remains possible to recover last key bits by exhaustive research for $SR > 0.8$. Additive Gaussian White Noise (AGWN) has been added on power signals to model the impact of ambient noise on the success rate. The noise level is set to $-60\,dB$ and $-70\,dB$. The sampling time

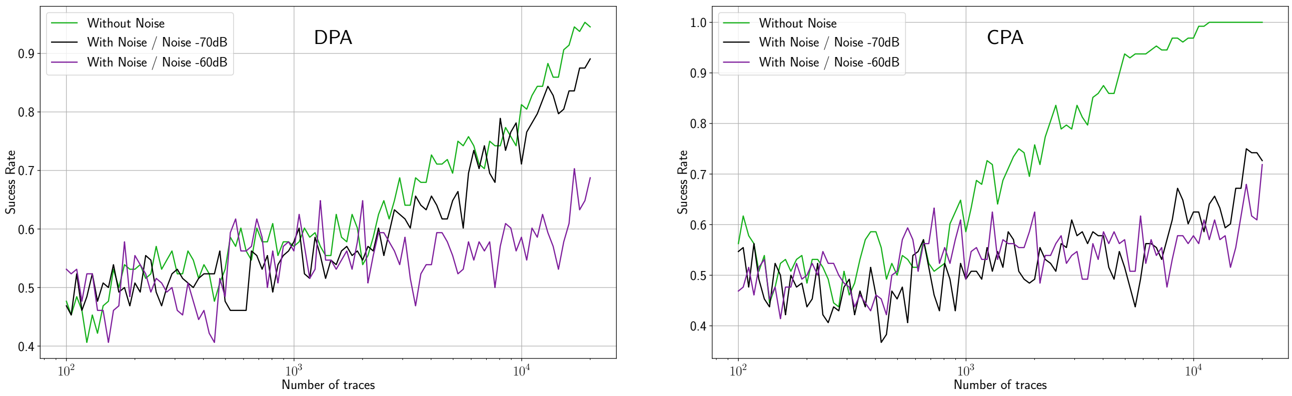

Fig. 7. Case #1 : Power analysis on CMOS implementation

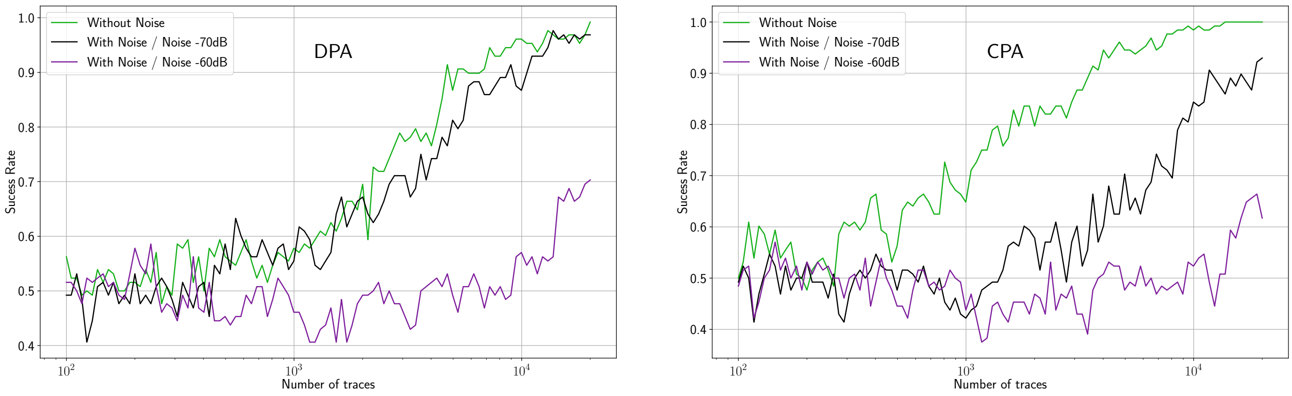

Fig. 8. Case #2 : Power analysis on hybrid implementation without non-volatile use

is set to $0.1\,ns$. Timing window is fixed at $10\,ns$ for cases #1 and #2, corresponding to a single clock period. For cases #3 and #4, the timing window is set to $5\,ns$, the duration of read/write operations.

The success rates as a function of the number of traces for the case #1 are plotted in Fig 7. The reference CMOS implementation is vulnerable to both DPA and CPA. Without noise, 12,000 traces are needed to completely recover the key for CPA and more than 20,000 traces are needed for DPA. With the effect of ambient noise, more than 20,000 traces are necessary for both DPA and CPA. The results for the case #2 are illustrated in Fig 8. These simulations show that the hybrid architecture without the non-volatile use does not reduce the security feature compared to the pure CMOS architecture. The number of traces required for hybrid implementation is 12,000 without noise and more than 20,000 for a noise level of $-70\,dB$.

Regarding the case #3, the results are depicted in Fig 9. According to the curves, 7,000 traces are needed to completely recover the key for CPA. The impact of the noise is more significant as the power consumption of non-volatile is less important (see Fig. 5). In the NVFF, the two MTJs are always in opposite state. The difference in power consumption between 0 logic and 1 logic is due to the reading circuit, included in the slave latch (see Fig. 3). Despite lower set of traces is required to find the secret data, the hybrid circuit does not introduce critical vulnerabilities. An attacker capable of monitoring 7,000 encryptions will have no issue to record the power consumption of 12,000 encryptions. On top of that, we have considered the case where the first round calculation of the initialization stage is restored from MTJ cells. Encryption would not be started before a power off, and thus the intermediate state register content will not be saved from the first round. For the case #4, no vulnerabilities were observed for the write operation as the difference in power consumption is not significant enough to be observable.

V. Discussion

As demonstrated in the previous section, it is possible to retrieve the key by reading MTJ devices. From this observation, one could hypothesize that an attacker would possibly be able to recover an intermediate state during data processing by restoring the information stored in the memory. However, as stated by Ascon's designer, a potential recovery of the secret state does not directly lead to a key-recovery [6]. Therefore, an attacker with the knowledge of intermediate register content cannot find the secret key. Nevertheless, this property applies to the Ascon cipher. An implementation of another hybridized cipher could be vulnerable to state-recovery attack.

In [20], the authors have shown that the read and write latency could provide a larger attack window to an adversary. The NVFF of Fig 3 has been designed to operate with constant write and read pulses of $5\,ns$. Thus, this use case cannot be applied to the circuit presented in the previous section.

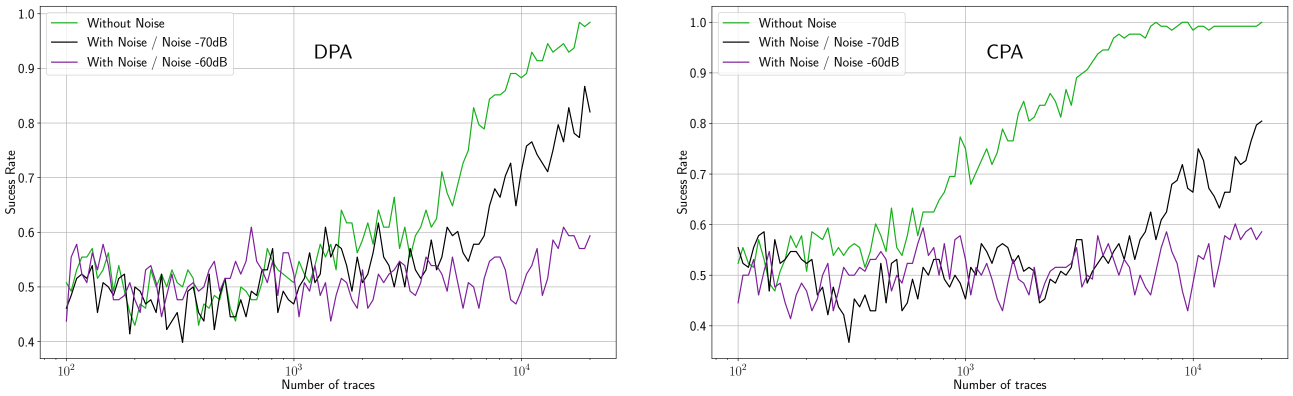

Fig. 9. Case #3 : Power analysis on hybrid implementation during read operation

In addition, exploiting the non-volatile feature offered by MRAM cells could be interesting to protect the circuit from fault injection attacks. The state could be stored in the MTJ devices before fault injection. The faulty state could than be replaced by the correct state to thwart the effect of fault injection, and thus prevent an attacker from retrieving the key. Nonetheless, Kharbouche-Harrari *et al.* [21] have demonstrated that data integrity in STT-MRAM can be altered by an external laser beam. Security analysis must be carefully conducted to assess whether or not a MRAM-based countermeasure remains secure under fault injection targeting MTJ cells.

VI. Conclusion

In this paper, we have performed the complete ASIC design flow to design hybrid CMOS/MRAM hardware implementation of the Ascon authenticated cipher. This implementation provides energy saving ranging from 19% to 54% in case of power failure for an area overhead of 5.5%. The core density (without physical cells) of the CMOS and hybrid implementation is 61.8% and 65.2% respectively.

We have conducted a side-channel analysis on both CMOS and hybrid implementations of Ascon. We have implemented a dedicated flow using existing EDA tools to generate power waveforms. We have considered several attack scenarios targeting different operations of the non-volatile circuit. The results have shown that the hybrid implementation does not pave the way for new critical vulnerabilities.

As future work, we will focus on exploiting MTJ devices to protect the Ascon cipher from fault-based attacks.

References

[1] M. Gholikhani, H. Roshani, S. Dessouky, and A. Papagiannakis, “A critical review of roadway energy harvesting technologies,” *Applied Energy*, vol. 261, p. 114 388, 2020.

[2] M. Alioto and M. Shahghasemi, “The internet of things on its edge: Trends toward its tipping point,” *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 77–87, 2018.

[3] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities,” *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[4] B. Dieny *et al.*, “Opportunities and challenges for spintronics in the microelectronics industry,” *Nature Electronics*, vol. 3, no. 8, pp. 446–459, 2020.

[5] N. Roussel, O. Potin, G. Di Pendina, J.-M. Dutertre, and J.-B. Rigaud, “Cmos/stt-mram based ascon lwc: A power efficient hardware implementation,” in *2022 29th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2022, pp. 1–4.

[6] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, *Ascon v1.2*, Submission to Round 1 of the NIST LWC project, 2019.

[7] “Caesar competition.” (2014), https://competitions.cr.yp.to/index.html.

[8] “Nist lwc.” (2019), https : / / csrc . nist . gov / projects / lightweight - cryptography.

[9] M. Kharbouche-Harrari *et al.*, “Light-weight cipher based on hybrid cmos/stt-mram: Power/area analysis,” in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2019, pp. 1–5.

[10] S. D. Kumar, Z. Kahleifeh, and H. Thapliyal, “Novel secure MTJ/CMOS logic (SMCL) for energy-efficient and DPA-resistant design,” *SN Computer Science*, vol. 2, no. 2, 2021.

[11] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Advances in Cryptology — CRYPTO’ 99*, M. Wiener, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[12] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in *Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye and J.-J. Quisquater, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 16–29.

[13] N. Samwel and J. Daemen, “Dpa on hardware implementations of ascon and keyak,” in *Proceedings of the Computing Frontiers Conference*, ser. CF’17, Association for Computing Machinery, 2017, 415–424.

[14] N. Samwel, “Master thesis computing science,” M.S. thesis, Radboud University Nijmegen, 2016. http://www.ru.nl/publish/pages/769526/niels_samwel.pdf.

[15] H. Gross, E. Wenger, C. Dobraunig, and C. Ehrenhöfer, “Ascon hardware implementations and side-channel evaluation,” *Microprocessors and Microsystems*, vol. 52, pp. 470 –479, 2017.

[16] K. Jabeur, F. Bernard-Granger, G. Di Pendina, G. Prenat, and B. Dieny, “Comparison of verilog-a compact modelling strategies for spintronic devices,” *Electronics Letters*, vol. 50, no. 19, pp. 1353–1355, 2014.

[17] G. Prenat *et al.*, “Ultra-fast and high-reliability sot-mram: From cache replacement to normally-off computing,” *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 1, 49–60, Jan. 2016.

[18] O. Coi, G. Di Pendina, G. Prenat, and L. Torres, “Spin-transfer torque magnetic tunnel junction for single-event effects mitigation in ic design,” *IEEE Transactions on Nuclear Science*, vol. 67, no. 7, pp. 1674–1681, 2020.

[19] L. Crocetti, L. Baldanzi, M. Bertolucci, L. Sarti, B. Carnevale, and L. Fanucci, “A simulated approach to evaluate side-channel attack countermeasures for the advanced encryption standard,” *Integration*, vol. 68, pp. 80–86, 2019.

[20] A. Iyengar, S. Ghosh, N. Rathi, and H. Naeimi, “Side channel attacks on sttram and low-overhead countermeasures,” in *2016 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2016, pp. 141–146.

[21] M. Kharbouche-Harrari *et al.*, “Impact of a laser pulse on a stt-mram bitcell: Security and reliability issues,” in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, 2018, pp. 243–244.