CMOS/STT-MRAM Based Ascon LWC: a Power Efficient Hardware Implementation

Nathan Roussel, Oliver Potin, Gregory Di Pendina, Jean-Max Dutertre, Jean-Baptiste Rigaud

Authors' version
ICECS 2022
https://doi.org/10.1109/ICECS202256217.2022.9971037

CMOS/STT-MRAM Based Ascon LWC: a Power Efficient Hardware Implementation

Nathan Roussel*, Oliver Potin*, Gregory Di Pendina†, Jean-Max Dutertre* and Jean-Baptiste Rigaud*
*Mines Saint-Etienne, CEA, Leti, Centre CMP F-13541 Gardanne, France
†Univ. Grenoble Alpes, CNRS, CEA, Spintec, 38000 Grenoble, France
*{nathan.roussel, olivier.potin, dutertre, rigaud}@emse.fr †gregory.dipendina@cea.fr

***Abstract*—The increasing use of Internet of Things (IoT) objects is associated with a necessity to develop low-power and secure circuits. Lightweight Cryptography (LWC) algorithms are used to secure the communications of these connected objects at a limited power consumption. Energy harvesting techniques can provide the power required by IoT objects. However, it can be subject to sudden power loss, causing the system microcontroller to stop. To enable the cryptographic primitive to quickly recover from an unplanned power failure, we propose a CMOS/MRAM-based hardware implementation of the ASCON cipher, a finalist of the National Institute of Standards and Technology (NIST) LWC contest. We focus on the ASIC design flow starting from an MTJ electrical model, without redeveloping the existing EDA tools. As case of study, an intermediate state of the ASCON computations can be stored in the non-volatile memories and restored at startup after a power loss, saving the energy cost of a recalculation of the algorithm first steps. This implementation provides energy saving ranging from 11% to 48% for an area overhead of 5.5%.**

***Index Terms*—ASCON, LWC, STT-MRAM, MTJ, non-volatile**

I. Introduction

The microelectronics domain is strongly driven by the advent of Internet of Things (IoT) technology. IoT enables several opportunities for the deployment and sustainability of connected objects for smart city, smart home, smart health, automotive and more.

IoT objects are required to operate on a wireless and low power environment while protecting themselves from external threats [1]. Most of these objects are battery-operated devices, thus reducing the lifetime due to the battery replacement. To overcome these constraints, several power systems based on energy harvesting of nearby sources have been proposed [2]. Nevertheless, such system cannot ensure a continuous power as the power of ambient sources may be discontinuous, or the energy harvester could not deliver sufficient energy to IoT devices to work properly. Hence, connected objects relying on energy harvesting are prone to data loss. To secure IoT at lowest energy impact, Lightweight Cryptography (LWC) algorithms are an ongoing research, with various applications from authenticated encryption to block cipher and more [3]. However, the existing hardware implementations of such algorithms do not protect themselves from scenario listed above.

To tackle these challenges, a number of new emerging non-volatile memories are currently under intensive research [4]. Among these innovative technologies, the Spin Transfer Torque MRAM (STT-MRAM) is considered as a promising candidate for designing low power circuit given its low power requirements, its easy integration with CMOS manufacturing process and its high endurance [5]. By embedding the STT-MRAMs in registers or flip-flops, it is possible to save circuit current state, preventing a loss of information in case of power failure. In this paper, we propose a power efficient hardware implementation of the ASCON authenticated cipher by substituting usual CMOS flip-flops with non-volatile flip-flops (NVFF) based on CMOS/STT-MRAM hybridization. We have designed and characterized an NVFF in order to perform all steps of the classic ASIC design flow. We have also modeled this NVFF to carry out a logical simulation of the ASCON circuit. We have targeted the CMOS 28nm FD-SOI Design Kit (DK) from STMicroelectronics.

The rest of this paper is structured as follows. In section II, a brief description of the ASCON cipher and the STT-MRAM are presented. A background on hybrid implementations of cryptographic primitives is also introduced. The different steps performed to set up the specific hybrid design flow are described in section III. The proposed hybrid implementation of ASCON and the highlighted results are presented in section IV. Finally, conclusion and future work are discussed in the last section.

II. Background

A. *Description of Ascon*

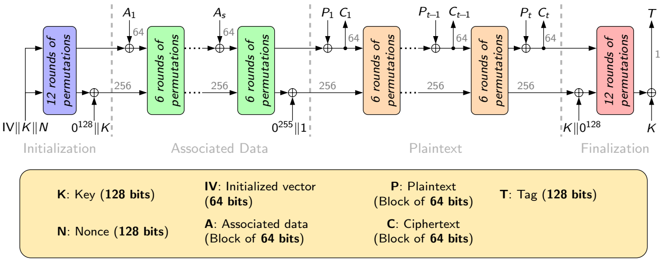
A_1
A_s
P_1 C_1
P_{t-1} C_{t-1}
P_t C_t
T
64
128
256
12 rounds of permutations
6 rounds of permutations
$IV\|K\|N$
$0^{128}\|K$
$0^{255}\|1$
$K\|0^{128}$
K
Initialization
Associated Data
Plaintext
Finalization
K: Key (**128 bits**)
N: Nonce (**128 bits**)
IV: Initialized vector (**64 bits**)
A: Associated data (Block of **64 bits**)
P: Plaintext (Block of **64 bits**)
C: Ciphertext (Block of **64 bits**)
T: Tag (**128 bits**)

Fig. 1. Encryption part of ASCON-128

ASCON is an authenticated encryption with associated data algorithm constructed from the sponge-like mode of operation [6]. It is one of the ten finalists in the National Institute of Standards and Technology (NIST) LWC standardization process. ASCON offers both security and performance characteristics. The encryption process of the ASCON-128 version is depicted

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

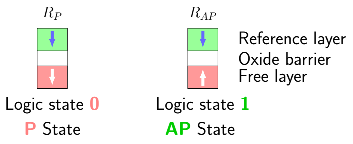

Fig. 2. MTJ with P and AP states

in Fig. 1. The state operates on 320 bits divided into five parts of 64 bits each. The encryption scheme unfolds in 4 phases. The first phase initiates the state with a constant vector, the key and a public nonce. In the second phase, associated data are introduced into the algorithm by block of 64 bits. The plaintext is injected and the ciphertext is retrieved in the third phase. In the last phase, an integrity tag is produced using the key and the algorithm end state. ASCON makes an extensive use of permutation operations consisting in a constant addition, a substitution layer and a diffusion layer.

B. STT-MRAM overview

An STT-MRAM is composed of a Magnetic Tunnel Junction (MTJ) which is the single element formed with an oxide layer sandwiched by two ferromagnetic layers (FM) [5]. An MTJ representation is illustrated in Fig. 2. The magnetization of the reference FM layer remains fixed, while the free layer can vary between parallel or antiparallel state (resp. P and AP). When the two FM layers have the same magnetization direction, the MTJ has a low resistance (denoted R_P), while it has a high resistance (R_{AP}) when the two FM layers have opposite magnetization direction. Conventionally, R_P represents logic 0 and R_{AP} logic 1. The read and write operations are achieved by injecting a current through the MTJ. The resistance ratio between the two magnetic states is defined as the tunnel magnetoresistance ratio $TMR = (R_{AP} - R_P)/R_P$.

C. Hybrid implementation of cryptographic primitives

Some implementations of lightweight ciphers associating CMOS and STT-MRAM have already been put forward in the literature [7, 8]. These architectures embed non-volatile flip-flops and dedicated logic. They underlined the interest of MRAM-based circuit for energy savings. In this work, we are focusing on the implementation of a design flow capable of realizing a circuit embedding hybrid cells starting from an MTJ electrical model conceived in former project [9], without redeveloping the existing tools of the ASIC design flow. To the best of our knowledge, our work is the first CMOS/STT-MRAM implementation of the ASCON authenticated cipher.

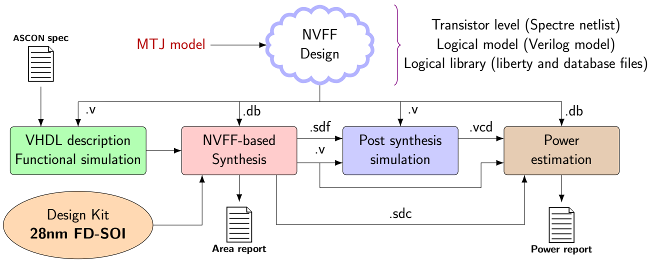

Fig. 3. ASIC design flow implemented to design the ASCON non-volatile circuit

III. FROM CELL LEVEL TO HYBRID DESIGN KIT

Fig. 3 illustrates the specific methodology followed in this work. As we did not have access to a hybrid DK, we had to start at transistor and MTJ levels. In order to compare a hybrid implementation with a pure CMOS one, an architecture of the non-volatile flip-flop (NVFF) had to be introduced. The implemented NVFF is an edge-triggered D flip-flop with an asynchronous reset as represented in Fig. 4. It is based on a classic FF design where the non-volatile part is plugged to the internal nodes of the slave latch. The read mechanism is close to the one proposed in [10]. After transistor sizing, the electrical simulation is done with the MTJ compact model. Table I gives the MTJ related parameters considered with this model. MTJ parameters are extracted from MRAMs state-of-the-art [5, 11].

TABLE I. MTJ parameters 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

For this architecture, the voltage supply was set to 1V and the operating frequency was fixed at 100 MHz. It is defined according to the application target. The transistor level operation of the NVFF is depicted in Fig. 5. For the CMOS side, the output Q is updated at each positive edge of the clock CLK. When the $reset$ signal goes down, the output is set to 0. In the non-volatile part, the two MTJs are written when the $write$ signal is activated. When the power is disabled, the output value is lost but the magnetic state of each MTJ remains unaltered. Once the power is on, the output value is restored as soon as the $read$ signal is enabled. In order to prevent any delay between power restart and restore operation causing a cell malfunction, the $read$ becomes active 5 ns after positive edge of vdd. The drive of the output buffer has been validated with a capacitive load of 13.4 pF.

To confirm the robustness of the NVFF under process variations, Monte Carlo (MC) simulations has been carried out with Cadence Spectre simulator. In this regard, the simulation set-up were 3σ (yield 99.87%) [12] for both CMOS transistors

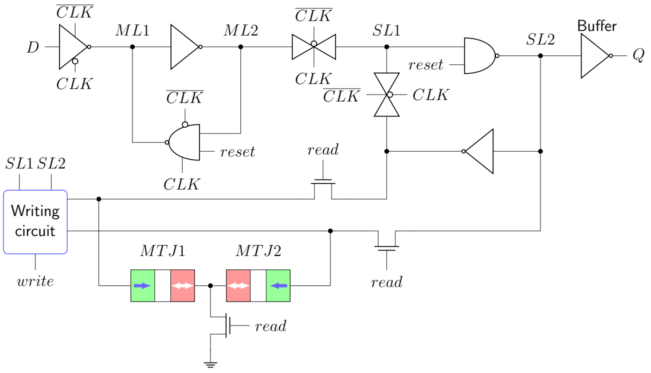

Fig. 4. Non-volatile flip-flop schematic

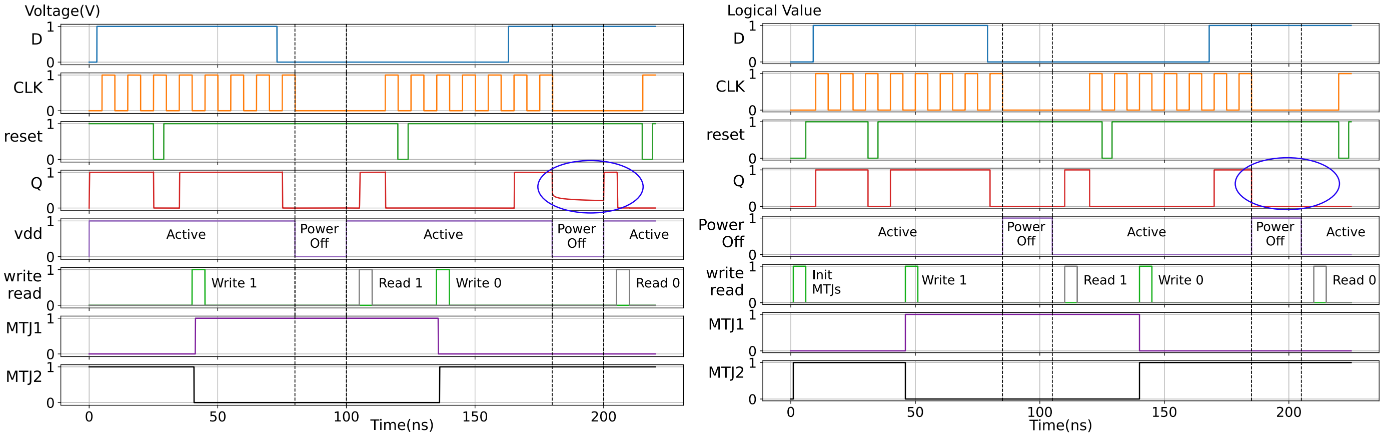

Fig. 5. (a) NVFF electrical simulation issued from Spectre

(b) NVFF logical simulation performed with Questasim

and MTJ parameters. The simulator was configured so that it stops automatically when the targeted yield is reached. To simplify the exploitation of the results, a Python script using the skillbridge library [13] has been implemented. This library allows sending SKILL commands to Virtuoso tools. The developed script can set the MC parameters and design parameters. The signal values are plotted on-the-fly from the script between two MC simulations. The waveforms produced by the script are similar to those of Fig. 5. This script monitors the simulation flow and enables us to precisely identify the number of defective circuits among all MC simulations, in an automated manner. From 2303 simulations, only 3 exhibit defects when reading the MTJs, mainly due to read disturbance.

To carry out functional and post synthesis simulations as represented in Fig. 3, a Verilog model of the NVFF based on user-defined primitives (UDPs) have been created. This model contains two primitives: one describes the behavior of the MTJ and the other the behavior of the slave latch and the non-volatile part. Regarding the master latch, it is implemented with predefined gate primitives. To permit further timing simulations with Standard Delay Format (SDF) back annotation, a second Verilog file instantiating the previous NVFF model and defining all timing checks and path delays was also developed. Fig. 5 shows a logical simulation of the proposed Verilog model. Results are very similar, except some transient levels can be observed on the transistor-level simulation, as emphasized in the inset. The On/Off states are emulated thanks to the *PowerOff* pin. It acts as a control signal of power gating transistors: the cell is in standby mode when *PowerOff=1*. At the beginning of the simulation, the MTJs must be initialized to operate properly.

We did not draw the layout of the proposed NVFF, we rather considered the CMOS DFF layout that area was increased by 20%, representing the cost of the non-volatile circuitry. It makes possible to estimate the area of our circuit.

Providing accurate characteristics pertaining to the proposed cell is compulsory to synthesize an NVFF-based implementation and to correctly estimate the area and power of the circuit as depicted in Fig. 3. In this respect, Cadence Liberate was used to characterize and create the logical library (liberty file) of the NVFF. Specific vectors have been applied to ensure correct characterization of the cell. Special regard must be given to the power representation of the non-volatile circuit. Downstream power tools except that internal power is momentary, mainly due to short-circuit current and switching current. Nonetheless, the power consumption of read/write operations is constant. Therefore, this power must be reported as leakage power since it is 'static'. For the *PowerOff* pin, the resulting leakage power in standby mode has been calculated according to the maximum current consumed by the cell. The created liberty file was compiled into database format with Synopsys Library Compiler to check the syntax and use the logical library in all electronic design automation (EDA) tools.

As all the files have been created, the NVFF can now be integrated as standard cell into the ASIC flow of the Fig. 3.

IV. Proposed hardware implementation of Ascon

The Ascon hardware implementation is formed by a Finite State Machine (FSM), a 4-bit counter, a permutation with 320-bit register and two registers to store outputs. One round of permutation is executed in one clock cycle. There are other architectures of Ascon [14]. This work could be tailored to an area optimized version of the cipher thereafter. We first designed a reference CMOS implementation to evaluate the impact of non-volatile circuit in terms of area and power consumption.

The design objective was the ability of this Ascon implementation to restart its computation from a backup state (saved in MTJ devices) in case of power loss. To this end, the flip-flops in the counter, in the FSM and in the permutation block were substituted by NVFFs. This leads to hybridize 329 flip-flops. Pins related to read/write operation modes are primary inputs of the circuit to have a complete control of NV use. They could also be managed by a specific utility [15].

We used Siemens Questasim logical simulator to validate the operation of the circuit. The synthesis step was performed with Synopsys Design Compiler. The area difference between the CMOS and the hybrid implementations are summarized in Table II. Considering the area requirement stated in section III, the hybrid implementation have a negligible impact on the overall area of the circuit (1.055×).

TABLE II. Area of the proposed circuit

GE: Gate Equivalent	Ascon CMOS		Ascon CMOS/MRAM		Δ (%)
Instances	μm^2	GE	μm^2	GE	μm^2
FSM	128.6	262.7	136.4	278.6	6.07
4-bit counter	27.1	55.4	30.4	62.1	12.2
Permutation	3641.5	7437.7	3905.9	7977.7	7.3
Tag and cipher registers	1173.6	2397.1	1173.6	2397.1	0
Total	4970.8	10152.9	5246.3	10715.5	5.5

Synopsys PrimePower tool was used to estimate the power consumption. The activity file (VCD) was generated thanks to post synthesis simulation with SDF back annotation. Table III reports the power consumption for both CMOS and hybrid implementations in no context saving mode. The logical library provided by the foundry is characterized with the physical netlist containing all parasitic components extracted from DFF layout, while our logical library was generated thanks to the netlist issued from the NVFF schematic. Furthermore, the DFF sizing is slightly different from our NVFF sizing. This explains the substantial difference observed in the internal power group.

TABLE III. Power comparison without save/restore operations (1V/100MHz)

	Ascon CMOS	Ascon CMOS/MRAM	Δ (%)
Internal Power (μW)	521.6	499.2	4.5
Switching Power (μW)	221.6	213.2	3.9
Leakage Power (μW)	2.68	2.47	8.5
Total Power (μW)	745.9	714.8	4.4

As mentioned in the first section, the hybrid architecture is capable of restoring the previous state in case of power failure. To be attractive, the cost in energy required to save and restore data must be lower than the energy required to restart the encryption from the beginning plus the energy wasted due to power failure. The comparison between both implementations after a power failure at the end of the second phase of the algorithm as function of the associated data size are summed up in Table IV. As a reminder, Ascon is constituted of 4 phases (see Fig. 1). With this implementation, we could not save the progression of the last two phases, as it also requires to hybridize the ciphertext and tag registers.

By using a hybrid architecture, it is possible to save energy by preventing a loss of information. The hybrid implementation offers an energy reduction from 11% to 48% compared to the pure CMOS architecture in case of power failure. Regarding the throughput, the hybrid circuit keeps the same data rate in contrary to the CMOS implementation since the encryption restarts from the last backup state.

V. Conclusion and Future Work

In this paper, we have presented the first CMOS/MRAM-based hardware implementation of Ascon authenticated cipher, a finalist of the NIST LWC contest, resilient to power failure. We first designed a non-volatile flip-flop and developed logical model and logical library in order to integrate it into the ASIC design flow. We wisely replaced volatile flip-flops by non-volatile flip-flops in order to save the progression of the encryption. The area overhead of the proposed hybrid architecture is extremely low (5.5%) compared to a pure CMOS architecture. Moreover, the results show that the hybrid implementation outperforms the CMOS implementation in terms of energy consumption when power suddenly shuts down, by 11% to 48%.

TABLE IV. 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	478.9	427.9	11.9
256-bit	736.2	556.5	32.3
512-bit	1079.4	728.1	48.2

As future work, the security analysis will be conducted to find any potential security vulnerability of the Ascon non-volatile circuit and propose dedicated countermeasures.

References

[1] M. Alioto et al. "The Internet of Things on Its Edge: Trends Toward Its Tipping Point". In: *IEEE Consumer Electronics Magazine* 7.1 (2018), pp. 77–87.

[2] M. Gholikhani et al. "A critical review of roadway energy harvesting technologies". In: *Applied Energy* 261 (2020), p. 114388.

[3] V. A. Thakor et al. "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities". In: *IEEE Access* 9 (2021), pp. 28177–28193.

[4] A. Chen. "A review of emerging non-volatile memory (NVM) technologies and applications". In: *Solid-State Electronics* 125 (2016). Extended papers selected from ESSDERC 2015, pp. 25–38.

[5] B. Dieny et al. "Opportunities and challenges for spintronics in the microelectronics industry". In: *Nature Electronics* 3.8 (2020), pp. 446–459.

[6] C. Dobraunig et al. *Ascon v1.2*. Submission to Round 1 of the NIST Lightweight Cryptography project. 2019.

[7] 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.

[8] S. D. Kumar et al. "Novel Secure MTJ/CMOS Logic (SMCL) for Energy-Efficient and DPA-Resistant Design". In: *SN Computer Science* 2.2 (2021).

[9] K. Jabeur et al. "Comparison of Verilog-A compact modelling strategies for spintronic devices". In: *Electronics Letters* 50.19 (2014), pp. 1353–1355.

[10] K. Jabeur et al. "Ultra-energy-efficient CMOS/magnetic non-volatile flip-flop based on spin-orbit torque device". In: *Electronics Letters* 50.8 (2014), pp. 585–587.

[11] G. Prenat et al. "Ultra-Fast and High-Reliability SOT-MRAM: From Cache Replacement to Normally-Off Computing". In: *IEEE Trans. Multi-Scale Comput. Syst.* 2.1 (Jan. 2016), 49–60.

[12] M. Lanuzza et al. "Comparative analysis of yield optimized pulsed flip-flops". In: *Microelectronics Reliability* 52.8 (2012). ICMAT 2011 - Reliability and variability of semiconductor devices and ICs, pp. 1679–1689.

[13] N. Buwen. *Python-Skill Bridge*. 2019. URL: https://unihd-cag.github.io/skillbridge/index.html.

[14] H. Gross et al. "Ascon hardware implementations and side-channel evaluation". In: *Microprocessors and Microsystems* 52 (2017), pp. 470 –479.

[15] W. Cooper et al. *Revolutionizing context save and restore with MSP FRAM microcontrollers*. Texas Instruments, 2015.