Hardware implementation of Ascon authenticated cipher based on CMOS/STT-MRAM

N. Roussel[1], O. Potin[1], J. B. Rigaud[1], and J. M. Dutertre[1]

[1]Mines Saint-Etienne, CEA, Leti, Centre CMP, F-13541 Gardanne France
nathan.roussel@emse.fr

Abstract

The proliferation of Internet of Things (IoT) objects has highlighted the necessity to enhance the energy efficiency and security of IoT devices. Recent attacks targeting IoT [1] have pointed out that the security has often been neglected in their design. LightWeight Cryptography (LWC) algorithms have been proposed to address both energy and security aspects.

IoT devices constructed with CMOS integrated circuits are suffering from high dynamic and static power consumption. Moreover, the data manipulated in CMOS architectures are volatile, prone to data loss due to sudden power failures. The Magnetic Random-Access Memory (MRAM) is a promising emerging technology offering several features: non-volatility, high cyclability and low power [2]. Combined with CMOS, it can overcome volatility and power consumption issues of CMOS circuits.

In this work, we propose a hardware implementation of Ascon authenticated cipher by hybridizing Spin Transfert Torque MRAM (STT-MRAM) with CMOS. Ascon is a finalist of the LWC standardization process organized by the NIST [3]. It has already been selected as primary choice for lightweight cryptography by the CAESAR competition [4].

We set up dedicated design flow allowing us to perform hardware description, simulations, synthesis and power consumption estimation of such circuits. We used the 28nm CMOS FD-SOI Design Kit from STMicroelectronics. Our architecture is compared with pure CMOS implementation of Ascon in terms of area and power consumption. The security aspect will be tackled in future works.

This work is supported by the MISTRAL project [5]. MISTRAL is a collaborative project founded by the French National Research Agency (ANR).

References

[1] E. Ronen et al. “IoT Goes Nuclear: Creating a ZigBee Chain Reaction”. In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, pp. 195–212. DOI: 10.1109/SP.2017.14.

[2] J. S. Meena et al. “Overview of emerging nonvolatile memory technologies”. In: *Nanoscale Research Letters* 9.1 (2014), p. 526. ISSN: 1556-276X. DOI: 10.1186/1556-276X-9-526.

[3] *NIST LWC*. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

[4] *CAESAR Competition*. URL: https://competitions.cr.yp.to/index.html.

[5] ANR. *Sécurisation d’algorithmes cryptographiques par hybridation MRAM/CMOS – Projet MISTRAL*. Feb. 2020. URL: https://anr.fr/Projet-ANR-19-CE39-0010.