Implémentation matérielle d'un algorithme de cryptographie légère pour objets connectés

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

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

Le monde de la microélectronique a fait place à l'internet des objets (IoT). Ces objets étant de plus en plus connectés et nomades, ils ont d'abord été conçus avec des fortes contraintes de consommation. Cependant, de récentes attaques ont démontré leur vulnérabilité et la sécurité est devenue une contrainte majeure. Pour répondre à cette problématique, le projet ANR MISTRAL propose de réaliser une implémentation matérielle d'algorithme de cryptographie légère (LWC) en associant CMOS et MRAM. Cet article présente une implémentation pure CMOS d'ASCON, un algorithme de cryptographie légère finaliste du concours du NIST. Cette implémentation servira de référence pour une future implémentation hybride de l'algorithme.

Mots clés – IoT, Sécurité, Cryptographie légère, Implémentation matérielle, ASCON

I. Introduction

L'internet des objets (IoT) est utilisé dans de nombreux domaines tels que la santé, la domotique ou encore l'automotive. Ces objets sont des systèmes embarqués composés de microcontrôleurs et de capteurs qui vont communiquer avec le monde extérieur et stocker des informations dans le «cloud». Ils doivent consommer peu d'énergie (1) et être sécurisés (2). Les récentes attaques (3) ont démontré que la sécurité des objets connectés a souvent été mise au second plan lors de leur conception. C'est dans ce contexte que le projet ANR MISTRAL (4) a été proposé. Il a pour objectif de sécuriser les algorithmes de cryptographie par hybridation CMOS/MRAM. La MRAM est une technologie de mémoire magnétique non-volatile émergente.

Dans le cadre du projet MISTRAL, le choix de l'algorithme s'est porté sur ASCON (5), un des dix finalistes du concours des algorithmes de cryptographie légère (LWC) organisé par l'Institut National des Normes et de la Technologie (NIST). Les travaux présentés aux premières conférences, organisées par le NIST, ont notamment prouvé que les implémentations matérielles des algorithmes doivent être protégées (6).

Cet article présente une implémentation CMOS de ASCON au moyen des outils du flot de conception fournis par le CNFM. Ce circuit servira de référence pour comparer avec une implémentation hybride CMOS/MRAM de l'algorithme. Une analyse des parties les plus consommatrices d'énergie et de surface est également proposée. La technologie CMOS utilisée est la technologie 28nm FD-SOI de STMicroelectronics.

Le reste de cet article est organisé selon 5 parties : le fonctionnement de l'algorithme est décrit en partie II. Les différents résultats obtenus à chaque étape du flot de conception sont présentés dans la partie III. L'analyse de consommation du circuit est présentée en partie IV. Du fait de l'importance des outils proposés par le CNFM, il sera proposé, en partie V, comment ce travail pourrait être transféré de la recherche vers la formation. Suivront les perspectives et la conclusion en partie VI.

II. Description de ASCON

ASCON est un algorithme de chiffrement authentifié avec données associées. Ce type d'algorithme assure la confidentialité, l'intégrité des données et permet une authentification de l'expéditeur du

Article publié par EDP Sciences et disponible sur le site https://www.j3ea.org ou https://doi.org/10.1051/j3ea/20221004

message. Il existe plusieurs variantes de l'algorithme, mais seulement la version ASCON-128 sera présentée. La figure 1 ci-dessous représente les 4 phases de la partie chiffrement :

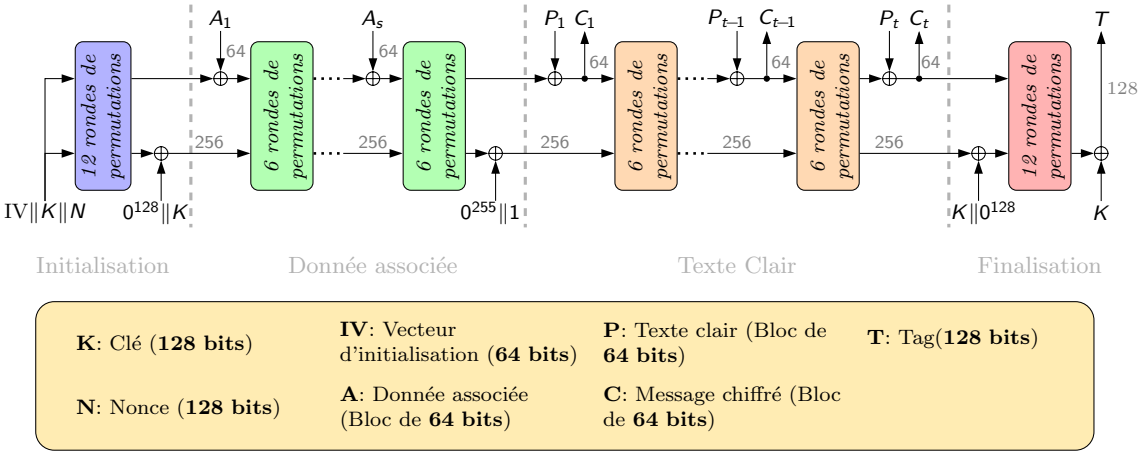

Fig 1 Schéma de ASCON-128

L'algorithme est initialisé avec un vecteur d'initialisation, la clé et le nonce. Le nonce protège les communications des attaques par rejeu. Dans le cas d'usage normal, il est différent à chaque chiffrement. La seconde étape permet d'introduire la donnée associée dans le calcul de l'algorithme. Cette donnée permet d'éviter qu'un attaquant remplace un message chiffré par un autre message chiffré avec la même clé. La troisième étape consiste à introduire le message à chiffrer et à obtenir le message chiffré. La génération du tag est réalisée lors de la dernière étape. Le tag correspond à un hachage unique des données chiffrées et il permet de vérifier l'intégrité du chiffrement. En cas d'attaque par rejeu ou dans le cas où le message chiffré est remplacé, si le nonce et la donnée associée sont différents à chaque chiffrement, alors le tag obtenu sera incorrect.

La taille du chemin de donnée est de 320 bits, divisé en 5 parties $x0, x1, x2, x3, x4$ de 64 bits. La permutation de ASCON est composée de 3 opérations : un ajout de constante sur le vecteur x_2, une couche de substitution où, 64 Sbox 5 bits, sont appliquées en parallèle et une couche de diffusion.

Dans le cadre du projet MISTRAL, la donnée associée, le message à chiffrer et le message chiffré ont une taille de 64 bits et une ronde de la permutation s'effectue en un coup d'horloge.

III. Implantation matérielle de l'algorithme

La structure d'ASCON est constituée de 4 sous-modules : une machine d'états (FSM) pour générer les signaux de contrôles, un compteur 4 bits pour exécuter le bon nombre de rondes (6 ou 12), la permutation et un registre pour stocker la valeur du tag. La figure 2 présente l'organisation de la permutation :

Ce sous-bloc contient un registre d'état courant sur 320 bits, un registre pour stocker le message chiffré sur 64 bits et les 3 opérations de la permutation. En sortie du registre d'état intermédiaire, un multiplexeur est utilisé pour introduire soit le texte clair ou bien la donnée associée sur x_0. Deux autres multiplexeurs sont ajoutés pour introduire la clé sur x_1 et x_2 au début de la phase de finalisation. Après les 3 opérations de la permutation, 2 multiplexeurs sont insérés pour introduire la clé sur x_3 et x_4 à la fin de la phase d'initialisation et de finalisation. Cette architecture est proche de celle présentée dans la référence (7).

La synthèse de ce circuit en 28nm FD-SOI a été réalisée à l'aide de l'outil Design Vision version R-2020.09-SP4 de Synopsys. La fréquence d'horloge est fixée à 100MHz et la tension d'alimentation à 1V. Les surfaces utilisées par les différents blocs du circuit sont regroupés dans le Tableau I.

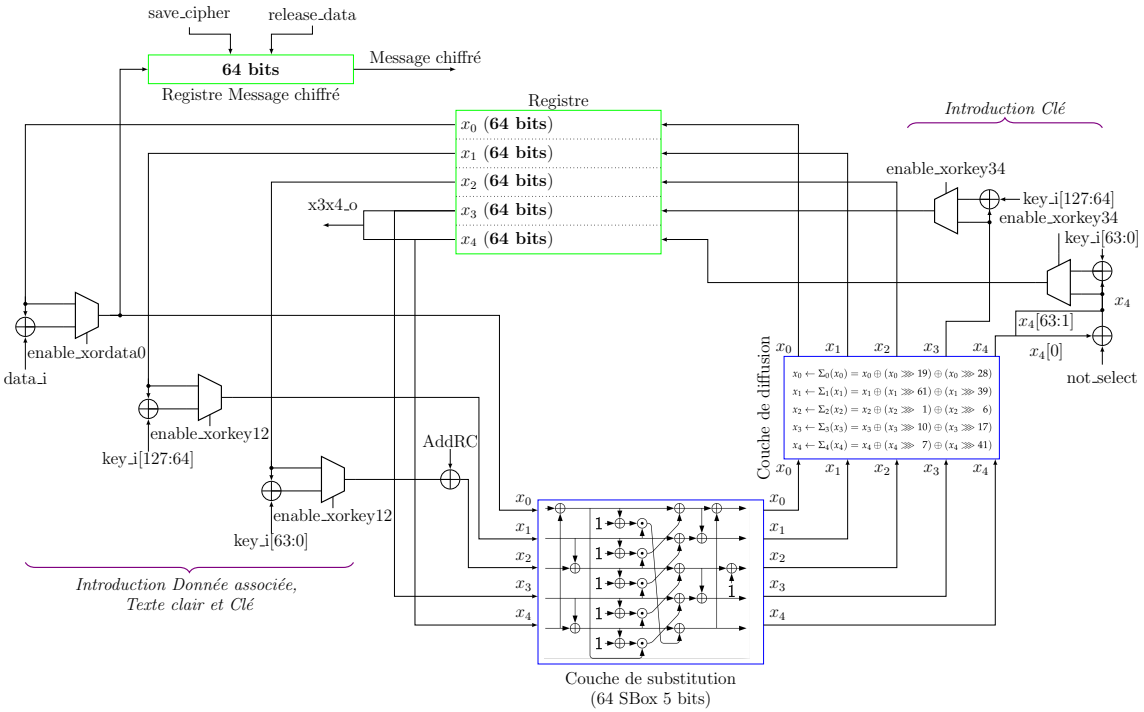

Fig 2 Schéma bloc de la permutation de ASCON

Tableau I. Surface utilisée par les différents blocs du circuit

Bloc	Surface (μm^2)	Surface (GE)
Machine d'états	128.6	262.7
Compteur 4 bits	27.1	53.4
Registre Tag	628.6	1283.9
Permutation	**4186.4**	**8550.7**
Ajout de constante	10.4	21.2
Couche de substitution	887.8	1813.3
Couche de diffusion	678.9	1386.6
Registre message chiffré	544.9	1112.9
Registre état courant	**1201.2**	**2453.4**
Multiplexeurs et XOR	525.2	1072.7
Circuit complet	**4970.7**	**10153**

La synthèse du circuit identifie les blocs ayant une empreinte matérielle importante. Il s'agit de la permutation, et plus particulièrement du registre d'état courant. La surface du circuit est proche de celle présentée dans la référence (8) pour la technologie 28nm ($5279.36\mu m^2$).

Néanmoins, un circuit spécifique pour comparer les performances de plusieurs algorithmes de cryptographie légère a été interfacé avec le circuit ASCON de la référence (8). Ceci explique la différence entre notre architecture et celle publiée dans la littérature.

Après la synthèse du circuit, l'étape de placement et routage du circuit a été réalisée à l'aide de l'outil Innovus version 20.10 de Cadence. Le *floorplan* a une taille de $80\mu m \times 80\mu m$. Les entrées/sorties du circuit sont placées le long du circuit. La surface du circuit après placement et routage est estimée à $\mathbf{5000.6\mu m^2}$.

Une extraction des parasites a été ensuite effectuée à l'aide de Quantus version 21.1.1-s329. Pour des raisons de confidentialité, STMicroelectronics ne donnant pas accès aux vues layouts complètes des cellules, l'extraction des parasites ne comportera donc que les parasites dues aux interconnexions entre les cellules.

IV. Estimation de consommation

A partir du circuit placé routé et de l'extraction des parasites, une estimation de consommation du circuit peut être ainsi réalisée. La puissance consommée par un circuit est la somme de la puissance statique et de la puissance dynamique :

$$P_{tot} = P_{sta} + P_{dyn} \quad [1]$$

La puissance statique est due aux courants de fuites lorsque le circuit n'est pas actif. Pour la technologie FD-SOI, elle s'exprime par :

$$P_{sta} = I_{fuite} V_{DD} = (I_{sub} + I_G) V_{DD} \quad [2]$$

Où I_G correspond aux fuites au niveau de la grille des transistors et I_{sub} la fuite sous le seuil.

Quant à la puissance dynamique, elle dépend de deux termes : la charge et la décharge des capacités en sortie des cellules (puissance de transition) et la puissance dissipée à l'intérieur des cellules (puissance interne). Cette dernière dépend du courant circulant entre l'alimentation et la masse lorsque le signal en entrée d'une porte logique commute (courant de court-circuit) et de la charge et décharge des capacités intrinsèques des cellules. Elle est définie par :

$$P_{dyn} = P_{tr} + P_{int} = \alpha C_{load} V_{DD}^2 f_{horloge} + \alpha C_{int} V_{DD}^2 f_{horloge} + i_{sc} V_{DD} \quad [3]$$

α est un facteur représentant le nombre moyen de transitions sur un nœud pour une période d'horloge, C_{load} est la capacité de charge en sortie, C_{int} est la capacité intrinsèque des cellules et $f_{horloge}$ est la fréquence d'horloge du circuit.

L'estimation de consommation est réalisée à l'aide PrimeTime PX version R-2020.09-SP4 (Synopsys). Afin de produire des résultats qui reflètent le mieux la consommation d'un circuit fabriqué, il est nécessaire de fournir plusieurs fichiers à cet outil :

- La *netlist Verilog* du circuit placé routé.
- Les fichiers *liberty* de la technologie CMOS utilisée. Ces fichiers contiennent les caractérisations temporelles et en consommation des différentes cellules du Design Kit. Ils sont également utilisés par l'outil de placement routage.
- Le fichier *Synopsys Design Constraints* (SDC) qui contient toutes les contraintes temporelles, de puissance et de surface du circuit. Il est généré lors du placement routage.
- Le fichier *Standard Parasitic Exchange Format* (SPEF) contenant tous les parasites du circuit liés aux interconnexions.
- Le fichier *Value Change Dump* (VCD) contenant les événements se produisant sur les signaux du circuit à chaque instant de la simulation. Ce fichier donne la valeur d'un signal à un instant donné ainsi que le moment où s'effectue une transition sur ce signal. Il est généré lors de la simulation fonctionnelle après placement routage.

La figure 3 regroupe le flot de simulation suivi pour l'estimation de consommation.

Les vecteurs de test utilisés ainsi que les résultats pour un chiffrement complet de l'algorithme sont résumés dans le Tableau II et le Tableau III.

Tableau II. Vecteurs de test utilisés pour l'estimation de consommation

Vecteur	Valeur
Texte clair	1F98BBFAE1678F15
Donnée associée	C351D9E0BD6D88E0
Nonce	CB4E10B435761A1BADB349F72F0561D6
Clé	C18025AB7C988FD0AF127F6E6F5CE5C0
Message chiffré	4A38629A7B0DCA08
Tag	726CB37DD977B5F961593C0C45ADACE2

Cette analyse de consommation met en évidence la partie du circuit qui consomment le plus d'énergie : le registre d'état courant de la permutation. Sa consommation est détaillée dans le Tableau IV.

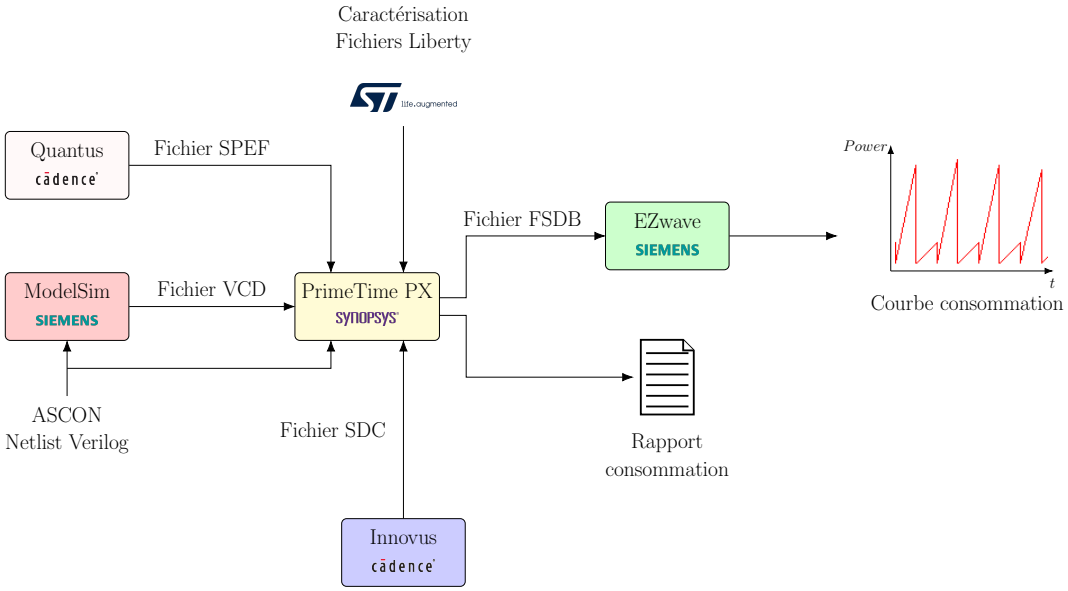

Fig 3 Flot de simulation utilisé pour l'estimation de consommation du circuit d'ASCON

Tableau III. Puissance consommée par le circuit

Groupe	Puissance interne (μW)	Puissance de transition (μW)	Puissance statique (μW)	Puissance totale (μW)
Horloge	18.5	79.5	3.7e-2	98
Registre	**327.1**	25.1	1.2	**353.4**
Combinatoire	111.6	234.4	1.5	347.5
Circuit entier	457.2	339	2.7	798.9

Cette consommation comprend également la puissance consommée par le réseau d'acheminement de l'horloge jusqu'au registre.

Tableau IV. Puissance consommée par le registre d'état courant

Puissance interne (μW)	Puissance de transition (μW)	Puissance statique (μW)	Puissance totale (μW)
213	36.3	0.71	**250**

La puissance consommée par le circuit en fonction du temps de simulation est représentée en figure 4.

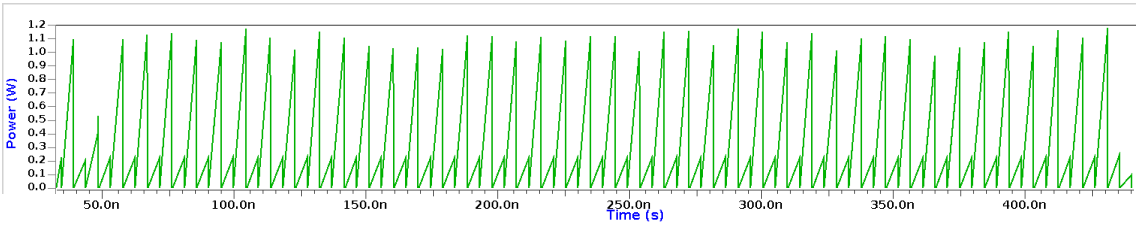

Fig 4 Puissance consommée par le circuit en fonction du temps de simulation tracée sous EZwave 2021.1

Cette première estimation de consommation permettra d'effectuer par la suite la caractérisation sécuritaire du circuit. Il est envisageable d'utiliser les courbes de consommation produites par PrimeTime pour réaliser des attaques par canaux cachés telles que l'analyse différentielle de la consommation (9). La figure 5 permet de mettre en évidence la différence de consommation pour 3 chiffrements différents qu'il est possible d'exploiter pour retrouver la clé secrète.

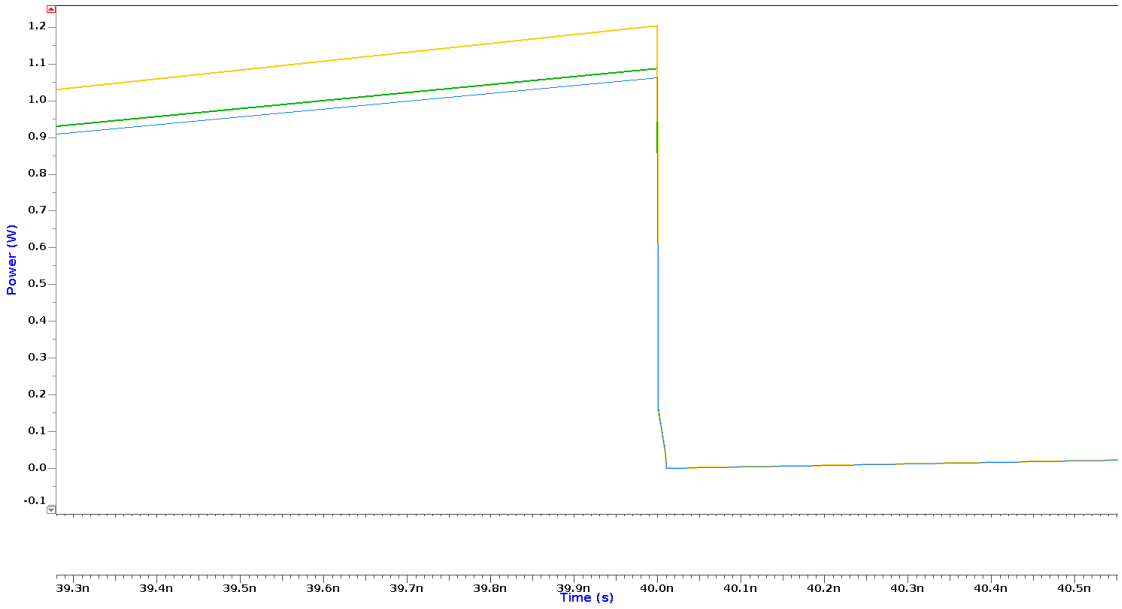

Fig 5 Différence de consommation pour 3 chiffrements différents

V. Travail de recherche à transférer vers la formation

Le travail de recherche présenté dans les parties précédentes ne serait pas possible sans la mise à disposition par le réseau CNFM des outils de CAO. Il met en œuvre la conception et la caractérisation en surface et en consommation d'un algorithme de cryptographie légère.

Le cycle d'ingénieur spécialisé ISMIN, dispensé à Mines Saint-Étienne, formant une partie de ses élèves aux métiers de la microélectronique, ne propose actuellement pas de module dédié à l'estimation de consommation d'un circuit intégré. Un des enjeux de la *Filière Électronique* (10) étant la transition énergétique, il serait donc intéressant de transférer une partie de ce travail vers la formation et ainsi sensibiliser les élèves aux problématiques de basse consommation.

Le choix de la technologie pourrait très bien se reporter vers un autre Design Kit. Pour cela, avec l'aide du CMP, la technologie AMS C35 serait ciblée. En effet, cette technologie est la référence pour former les étudiants aux métiers de la conception de circuits intégrés. Dans une approche court terme, les étudiants pourraient donc :

- Faire une description VHDL de ASCON et vérifier son fonctionnement à l'aide d'une simulation fonctionnelle (avec ModelSim par exemple),
- Réaliser une synthèse du circuit sous Design Vision en utilisant la technologie AMS,
- Effectuer une simulation après synthèse pour générer le fichier d'activité nécessaire à l'estimation de consommation,
- Proposer une analyse des parties les plus consommatrices d'énergie à l'aide de PrimeTime de Synopsys.

Cette première approche permettrait d'initier les étudiants à l'estimation de consommation et à l'utilisation des outils de caractérisation des circuits intégrés.

Dans le cadre d'un projet d'étude plus long, les élèves pourraient réaliser le placement et routage d'ASCON à l'aide d'Innovus de Cadence, procéder aux étapes de vérifications (DRC et LVS) du circuit avec PVS ou Calibre, extraire les parasites à l'aide de Quantus et effectuer une analyse de la consommation du circuit annoté avec PrimeTime.

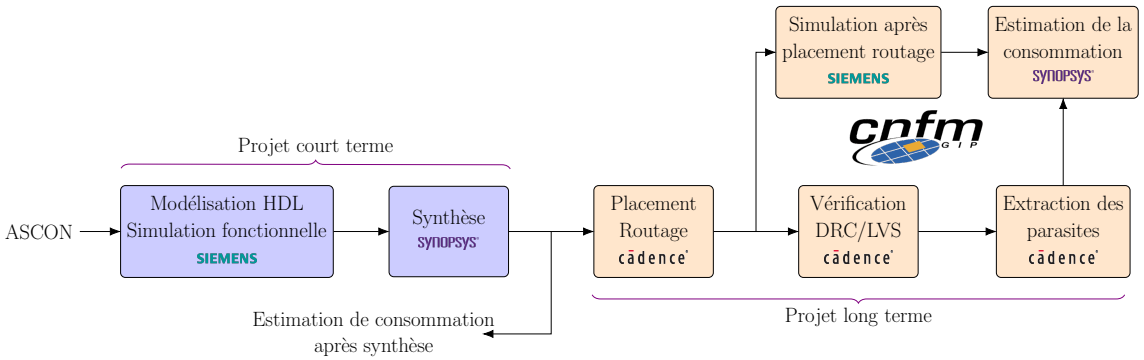

Fig 6 Vue d'ensemble des deux projets réalisables par les étudiants

La figure 6 représente une vue d'ensemble des deux projets décrits précédemment. Ainsi, ces deux approches pourraient compléter l'offre de formation dispensée à Mines Saint-Étienne et de manière plus globale être proposées aux autres formations du domaine.

VI. Conclusion et perspectives

Les travaux imposent l'utilisation d'un grand nombre d'outils du flot de conception d'un circuit numérique fourni par le CNFM. Ces outils permettent d'effectuer une analyse complète en termes de surface consommée et de puissance consommée.

Le rôle de l'hybridation MRAM est de permettre la mémorisation de l'état intermédiaire des calculs dans un but d'économie de puissance lorsque le système est mis hors tension. Appliquée au registre d'état intermédiaire d'ASCON, elle permet d'interrompre et de reprendre le chiffrement sans avoir à reprendre les étapes d'initialisation de la clé et d'incorporation des données associées qui sont fortement consommatrices d'énergie. La poursuite des travaux avec l'hybridation CMOS/MRAM de ce registre constitue un cas d'application permettant de mettre en évidence l'intérêt de cette technologie pour les objets connectés autonomes. L'intérêt d'hybrider d'autres parties du circuit et les conséquences en termes de sécurité seront également étudiés.

D'un point de vue pédagogique, la conception de circuit hybride permet aussi d'envisager l'ouverture de nouvelles formations, basées sur la conception de circuits numériques très basse consommation utilisant des technologies émergentes.

Remerciements

Les auteurs remercient l'Agence National de la Recherche (ANR) pour l'octroiement des fonds nécessaires pour réaliser le projet MISTRAL. Les auteurs remercient également Circuits Multi-Projets pour son aide concernant l'utilisation du Design Kit 28nm FDSOI et la Coordination Nationale de la Formation en Microélectronique et en nanotechnologies (CNFM) qui fournit les licences permettant d'utiliser les outils "sign-off" du flot de conception des circuits intégrés.

Références

(1) K. Mathioudakis *et al.* « Short Paper : IoT : Challenges, Projects, Architectures ». In : *2015 18th International Conference on Intelligence in Next Generation Networks*. IEEE, 2015.

(2) T. Xu *et al.* « Security of IoT systems : Design challenges and opportunities ». In : *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. 2014, p. 417-423. DOI : 10.1109/ICCAD.2014.7001385.

(3) E. Ronen *et al.* « IoT Goes Nuclear : Creating a ZigBee Chain Reaction ». In : *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, p. 195-212. DOI : 10.1109/SP.2017.14.

(4) ANR. *Sécurisation d'algorithmes cryptographiques par hybridation MRAM/CMOS – Projet MISTRAL*. Fév. 2020. URL : https://anr.fr/Projet-ANR-19-CE39-0010.

(5) C. Dobraunig *et al.* *Ascon v1.2*. Submission to Round 1 of the NIST Lightweight Cryptography project. 2019.

(6) K. Ramezanpour *et al.* « Active and Passive Side-Channel Key Recovery Attacks on Ascon ». In : *Lightweight Cryptography Workshop*. Juin 2020.

(7) H. Gross *et al.* « Ascon hardware implementations and side-channel evaluation ». In : *Microprocessors and Microsystems* 52 (2017), p. 470 -479. ISSN : 0141-9331. DOI : https://doi.org/10.1016/j.micpro.2016.10.006.

(8) M. Khairallah *et al.* « Preliminary Hardware Benchmarking of a Group of Round 2 NIST Lightweight AEAD Candidates ». In : 2020.

(9) N. Samwel *et al.* « DPA on Hardware Implementations of Ascon and Keyak ». In : *Proceedings of the Computing Frontiers Conference*. CF'17. Association for Computing Machinery, 2017, 415–424. ISBN : 9781450344876. DOI : 10.1145/3075564.3079067.

(10) *Filière électronique*. URL : https://www.filiere-electronique.fr/.