Fonction Physique Non-clonable pour la Sécurité du Cycle de Vie d'un Objet Cyber-physique

Johan Marconot

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

Spécialité : NANO ELECTRONIQUE ET NANO TECHNOLOGIES

Arrêté ministériel : 25 mai 2016

Présentée par

Johan MARCONOT

Thèse dirigée par **David HELY**, Maitre de Conférence, Université Grenoble Alpes
et codirigée par **Florian PEBAY-PEYROULA**, CEA

préparée au sein du **Laboratoire CEA/LETI**
dans **l'École Doctorale Electronique, Electrotechnique, Automatique, Traitement du Signal (EEATS)**

Fonction Physique Non-clonable pour la Sécurité du Cycle de Vie d'un Objet Cyber-physique

Physical Unclonable Functions for Security of life cycle of a cyber-physical object

Thèse soutenue publiquement le **9 juillet 2020**,
devant le jury composé de :

Monsieur LILIAN BOSSUET
PROFESSEUR DES UNIVERSITES, UNIVERSITE DE LYON, Rapporteur
Monsieur SYLVAIN GUILLEY
PROFESSEUR ASSOCIE HDR, TELECOM PARISTECH, Rapporteur
Madame MARIE-LISE FLOTTES
CHARGE DE RECHERCHE, CNRS DELEGATION OCCITANIE EST, Examinatrice
Monsieur GIORGIO DI NATALE
DIRECTEUR DE RECHERCHE, CNRS DELEGATION ALPES, Président
Madame ASSIA TRIA
CADRE SCIENTIFIQUE, CEA GRENOBLE, Examinatrice

RAPPORT

Thèse *Doctorant : Johan Marconot* *Sujet : Fonction Physique Non-clonable pour la Sécurité du Cycle de Vie des Objets Cyber-physiques*	
Date : 19/05/2020	Révision : 19/05/2020

	Nom	**Fonction**	**Entité**
Auteur	**Johan Marconot**	**Doctorant**	**CEA-Grenoble/LETI**
Liste de diffusion	Johan Marconot – Florian Pebay-Peyroula – David Hely – Lilian Bossuet – Sylvain Guilley – Marie-Lise Flottes – Assia Tria – Giorgio Di Natale		

Remerciements

Je remercie mon directeur de thèse David Hély pour son encadrement exemplaire, pour ses relectures pertinentes et assidues de mes articles ; elles ont grandement contribué à leur qualité. Je remercie mon encadrant Florian Pebay-Peyroula qui m'a accueilli dans l'équipe LSOSP du CEA-Grenoble et m'a permis d'explorer ce nouveau sujet de recherche. Je les remercie tous deux sincèrement pour le suivi régulier de mes travaux, ce sont des encadrants professionnels et de confiance.

Je remercie les membres du jury, Giorgio Di Natale pour la présidence de ma soutenance, Sylvain Guilley et Lilian Bossuet pour l'examen de mon manuscrit et leurs rapports encourageants, Assia Tria pour les échanges que j'ai eu avec elle, et pour terminer Marie-Lise Flottes que je remercie aussi pour son Ecole d'Eté Cyber-in-Occitanie. Je les remercie tous et toutes pour leur participation au jury, pour leur expertise scientifique et les questions pertinentes qu'ils et elles m'ont partagées.

Je remercie mes collègues du LSOSP, pour toutes leurs contributions qu'elles soient scientifiques, méthodologiques ou amicales ; elles ont permis d'établir un cadre de travail accueillant et riche en expérience. Merci à tous et toutes pour leur bienveillance et leurs aides.

Merci à Maxime Lecomte et Antoine Loiseau pour leurs conseils avisés en sécurité matérielle, Maxime Puys pour son expérience d'ancien doctorant qu'il m'a partagé, Majda pour son aide à l'organisation de mes voyages à l'étranger, et Manuel pour son aide sur les outils de CAO.

Merci aux collègues partenaires de football, Romain M. et Thomas L. dévoué à l'organisation des tournois, merci à Antoine D. et aux autres collègues amateurs de randonnées, merci à Mustapha pour la découverte du Maroc, merci à Lukas et Thibault pour toutes les expériences et critiques échangées, merci à tous ceux et celles qui ont partagé des discussions amicales, Claire, Pierre-Henri, Alexis, Thomas H., Meriem, Jean, Sylvain, Matthieu. Merci.

Je remercie les collègues du LCIS qui m'ont accueilli à plusieurs occasions à Valence, notamment pour la journée des doctorants. Merci à Vincent Beroulle, membre de mon comité de suivi, qui m'a conseillé à plusieurs occasions. Et merci à Cyril pour son accueil à Miami.

Je remercie mes amis qui m'ont apporté des moments conviviaux , mais aussi de l'aide, en particulier Nabil et Nicolas pour leurs conseils, Nausicaa pour ses relectures de manuscrit, et pour terminer Lou Morriet pour l'écoute attentive de mes répétitions orales et ses retours pertinents.

Je remercie toutes les autres personnes qui au cours de ces trois années m'ont offert leurs conseils et leurs échanges amicaux.

Je termine en remerciant ma famille, mon oncle Paul, ma tante Geno et Claire pour leurs encouragements, ma mère Eliana toujours prévenante et à l'écoute, et mon père Jean-Marie, fier et heureux du travail que j'ai réalisé.

Merci à vous,

SOMMAIRE

1 Introduction

Les applications dites « IoT » (IoT pour *Internet of Things* : interconnexion entre l'Internet et les objets cyber-physiques) se déploient aujourd'hui dans tous les champs de la société (domestique, industrie, médical…). Leur sécurité devient un enjeu majeur à mesure que les démonstrations et les exemples de vulnérabilités exploitées se multiplient. Le fonctionnement de l'objet mais aussi les données privées sont susceptibles d'être compromis, et par conséquent la sécurité des systèmes et des personnes qui en dépendent. La sécurisation de l'IoT fait toutefois face à plusieurs difficultés. La grande diversité des technologies et acteurs du domaine limite les solutions de sécurité génériques. Les protections doivent aussi respecter les contraintes de ressources et d'usage des dispositifs. De plus, au cours de leur cycle de vie, les objets IoT sont soumis à des besoins de sécurité spécifiques.

La thèse recherche des solutions pour gérer la sécurité du dispositif tout au long de son cycle de vie. Cela implique de définir le cycle de vie ainsi que les atouts et menaces associées pendant celui-ci. Le terme *cycle de vie* réfère à l'ensemble des processus et états qui caractérisent un objet durant sa vie, de la création à la fin de vie (*End of Life* : EoL). La Figure 1 montre un schéma classique de celui-ci : spécification technique du dispositif, production des éléments matériels et logiciels, déploiement de l'appareil, utilisation et fin de vie. Une phase d'intervention (mise à jour logicielle, maintenance, réparation…) peut aboutir à une reconfiguration ou à un redéploiement du dispositif. Idéalement la fin de vie consiste selon les usages soit à la destruction des composants de l'objet, soit à leur recyclage. Toutefois l'absence de règlements ou d'assistance mène parfois à l'abandon de l'objet, le devenir de ses composants et des données qui y sont stockées est alors une inconnue.

Plusieurs atouts sensibles intègrent et composent le système au cours de ce cycle : le système sur puce (*System-on-Chip* : SoC) et ses éléments matériels, les micrologiciels (firmware), le système d'exploitation, les logiciels embarqués ainsi que des composants ou des sous-systèmes de tierces parties. Le concept de *cycle de vie* est initialement utilisé dans l'étude d'impact environnementale d'un produit (*Life Cycle Assessment* : LCA) *:* évaluer les interactions d'un produit sur l'environnement extérieur en prenant compte de toutes les étapes amont et aval à son utilisation. La démarche est similaire pour les enjeux de sécurité : analyser et réduire les risques sur l'ensemble du cycle de vie. Toutes les opérations qui induisent une interaction avec le dispositif cyber-physique, où ses atouts, sont considérées.

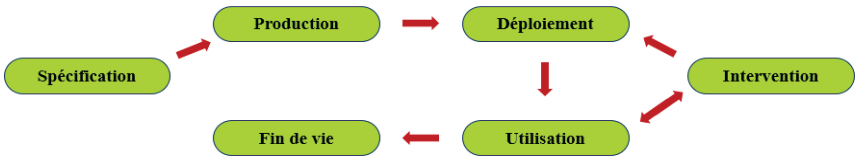

Figure 1: Phases principales du cycle de vie IoT

La première section de cette partie introduit des généralités sur le cycle de vie d'un objet connecté, en considérant les besoins spécifiques à la phase de production. L'élément central de l'objet, le système sur puce, se compose de divers éléments matériels et logiciels. Nous listons les opérations et les interactions qui exposent ces composants ; nous constatons des exigences techniques qui imposent des accès au dispositif. Cela complexifie la sécurisation de l'objet au cours du cycle de vie, et ce d'autant plus que l'IoT est sujet à une grande diversité des usages, des acteurs et des atouts à protéger.

La deuxième section approfondit les besoins de sécurité, grandissant avec l'accroissement des vulnérabilités et des menaces. La surface d'attaque croît avec l'ajout de nouvelles fonctionnalités et l'apparition de tierces parties au cours du cycle de vie. Cela suit la progression du nombre de cyber-attaques dans l'actualité, y compris pour les failles exploitées dans les couches matérielles de l'IoT.

La troisième section résume les avancées de la recherche en sécurité matérielle ; en priorité sur les travaux prenant compte du cycle de vie. Nous soulignons les enjeux cruciaux sur la conception de primitives efficaces pouvant assurer des propriétés de sécurité dès les premières phases du cycle de vie.

La quatrième et dernière partie détaille l'orientation et l'organisation du mémoire.

1.1 Complexité du cycle de vie IoT

1.1.1 Développement et miniaturisation des architectures des systèmes sur puce

Les performances des circuits intégrés se sont accrues exponentiellement avec l'amélioration des procédés de fabrication et d'intégration. Le niveau de miniaturisation et de performance obtenu permet aujourd'hui la conception de *système sur puce (SoC)* complexes et diversifiés.

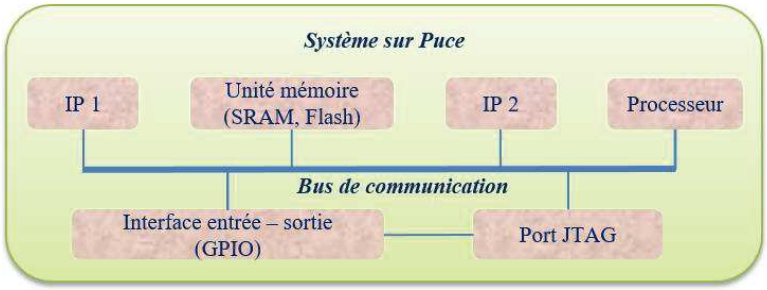

Figure 2: Architecture d'un système sur puce

Un système sur puce est une architecture matérielle - logicielle intégrée sur une puce et déployant l'ensemble des fonctionnalités nécessaires pour le dispositif [1]**.** L'architecture d'un SoC, présentée dans la figure 2, comprend des blocs essentiels tels que le processeur de calcul, les unités mémoires, le contrôleur et les interfaces d'échanges tant interne (bus de communication) qu'externe (GPIO). Toutefois, le SoC peut inclure des composants supplémentaires propriétés de tierces parties, intégrés pour des motifs spécifiques. La conception de telles architectures, couplant des composants de diverses origines et avec des technologies de fabrication hautement avancées, implique des contraintes de tests et de vérifications. Les fabricants doivent évaluer le succès de la production des puces et de l'intégration des composants tierces (test), valider le fonctionnement et les exigences spécifiés (vérification). Cela est d'autant plus complexe avec des niveaux de miniaturisation et d'intégration élevés.

La figure 3 schématise le flot d'étapes qui composent la chaine de production d'un SoC, tant la fabrication et l'intégration d'IP (*Intellectual Property*) matérielles que le développement des couches logicielles tierces. Au cours de cette phase du cycle de vie des tests structurels valident les sorties de productions, détectant la présence de défauts dans les interconnections électriques ou dans les transistors. Parmi les fautes craintes par les fabricants nous trouvons le blocage du signal en entrée ou sortie d'une porte logique, les connections non prévues entre des pistes électriques, les retards dans les temps de proposition de signaux ou encore des court-circuits et circuits ouverts dans les transistors [2]. Trois grandes familles de composants nécessitent des tests : circuits numériques, unités mémoires et circuits analogiques. Cela implique pour les acteurs des semi-conducteurs de prévoir et déployer des opérations et des mécanismes de tests. Des tests fonctionnels sont requis pour valider le comportement du circuit par rapport à la description donnée en spécification. Une des solutions connues se base sur des mécanismes de tests embarqués (*Built-in-Self Test*) : un circuit de stimulation, accessible par une interface externe, permet de soumettre une série de messages d'entrée aux composants électroniques ; et de lire les états internes de la logique. L'acteur en charge de l'opération peut ainsi vérifier si les états logiques correspondent à ceux attendus. Ces dernières décennies les acteurs de la microélectronique favorisent ainsi le *Design-for-testability (DsT).* Ce type d'approche implique l'intégration d'éléments matériels spécifiques, ainsi que les interfaces et accès nécessaires à leur utilisation.

Après la phase de production le système sur puce est assemblé sur le PCB (*Printed Circuit Board*) avec d'autres composants; unité de communication, batterie ou écran. Les phases d'assemblage sur PCB requièrent aussi des tests vérifiant l'intégration des composants. Des modules tierces plus spécifique peuvent aussi se coupler avec la carte, formant un objet cyber-physique complet qui réponds à un besoin particulier. Par exemple, des modules mécaniques pour actionner des pompes dans le cas d'un système d'infusion automatisé.

Outre une diversité de composants matériels, un système sur puce se caractérise aussi par plusieurs couches logicielles :

- *Micrologiciel (firmware),* couche basse responsable des accès aux composants et ressources matériels, propriété du fabricant du SoC.
- *Système d'exploitation* qui fournit une abstraction et une gestion des ressources matérielles.
- *Logiciel applicatif embarqué,* couche supérieur qui définit et gère les fonctionnalités du dispositif : traitements et calculs spécifiques, communications et éventuellement des fonctions de sécurité…

Le système dépend de ces couches logicielles pour l'exécution de ses fonctions de base, celle-ci peuvent être développées et intégrées par des tierces parties, à différents moments du cycle de vie du SoC, et suivant diverses méthodes de programmation et d'approvisionnement de code. Les processus de déploiement des modules logiciels changent selon le type de logiciel, le type de matériel ciblé et les techniques de débogage utilisées pour vérifier la bonne programmation de ces modules.

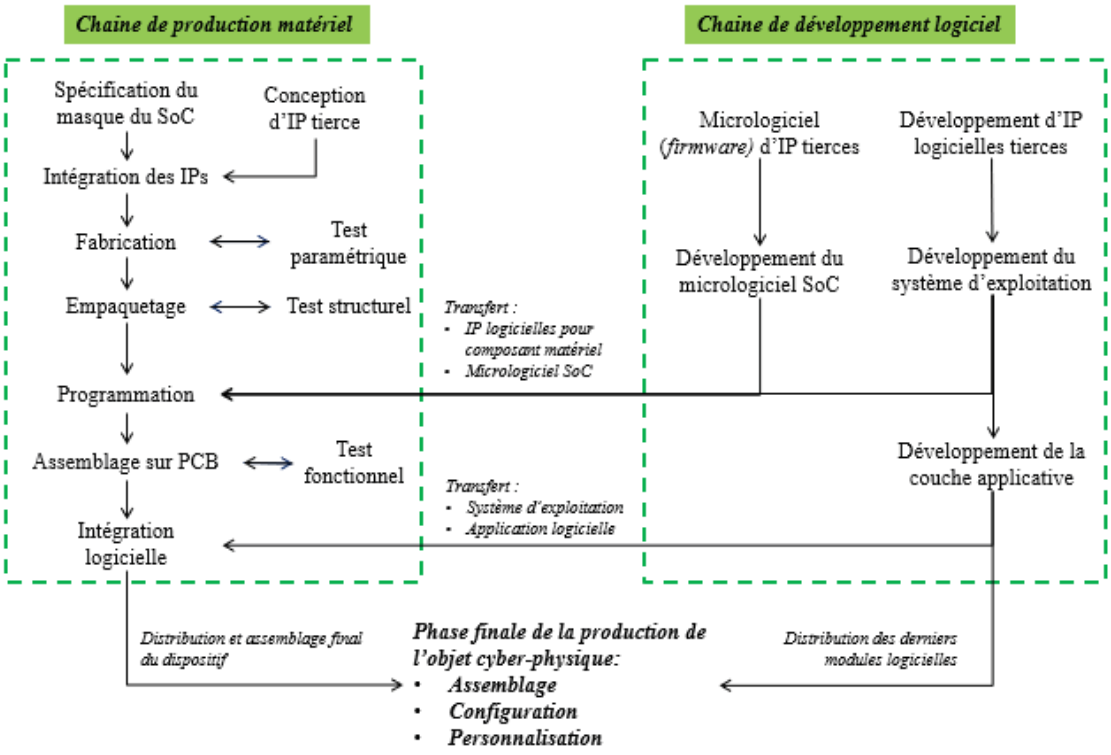

Figure 3: Phases de production d'un système sur puce

1.1.2 Extension et segmentation du cycle de vie

La complexité et diversité croissantes des composants électroniques se répercutent sur le cycle de vie des objets cyber-physiques. Les flots de production s'étendent avec la multiplication des opérations d'intégration, vérification et assemblage; cela oblige les compagnies à de lourds investissements dans les équipements et compétences nécessaires pour ces étapes. Certaines entreprises se concentrent parfois entièrement pour une seule opération, phénomène accrut par la spécialisation économique. En outre la mondialisation favorise les échanges de matériels et de services à grandes échelle. Ainsi l'ensemble des phases de production et de développements des composants des SoCs se mondialisent, incluant des tierces parties délocalisées. Le cycle de vie est ainsi aujourd'hui segmenté entre différents fabricants et sous-traitants en charge de services techniques spécifiques (test, emballage, assemblage…). Cette distribution non standardisée des rôles varie selon la capacité (en termes de ressource et de compétence) des acteurs à réaliser les opérations.

La figure 4 détaille les principaux acteurs de la chaine d'approvisionnement des systèmes ; tant pour les couches logicielles que pour les IP matérielles. Les grandes familles d'acteurs sont :

- *Les acteurs de la chaine d'approvisionnement des SoC :*
  - Les concepteurs qui élaborent les masques des puces et incorporent souvent des IPs de tierces parties. Après la conception les dessins des masques sont transmis aux usines de production.
  - Les fondeurs en charge de la fabrication des puces.
  - Les *OSATs (Outsources Semiconductor Assembly and Test Services)*, sous-traitants qui effectuent les étapes de tests et d'emballage des puces.
- *Original Component Manufacturer (OCM):* entreprise qui produit un composant qui sera intégré dans le système, un semi-conducteur complet avec un micrologiciel spécifique. Plusieurs modèles sont proposés en vente, libre au fabricant du SOC de sélectionner celui à sa convenance. La fabrication du composant de l'OCM est souvent sous-traitée à des fondeurs et des OSATs.
- *Original Equipment Manufacturer (OEM):* le fabricant de l'objet final, incorporant le système sur puce et tous les composants tierces. L'OEM définit les spécifications de son système et charge des tiers de la fabrication, distribution, déploiement et fin de vie des dispositifs. Selon ses besoin l'OEM choisit tel ou tel SoC disponible auprès des fournisseurs.
- *Electronic Manufacturing Service (EMS):* sous-traitant qui réalise l'assemblage du SoC et des composants sur le PCB, ainsi que l'emballage et l'intégration logiciel final du dispositif produit.

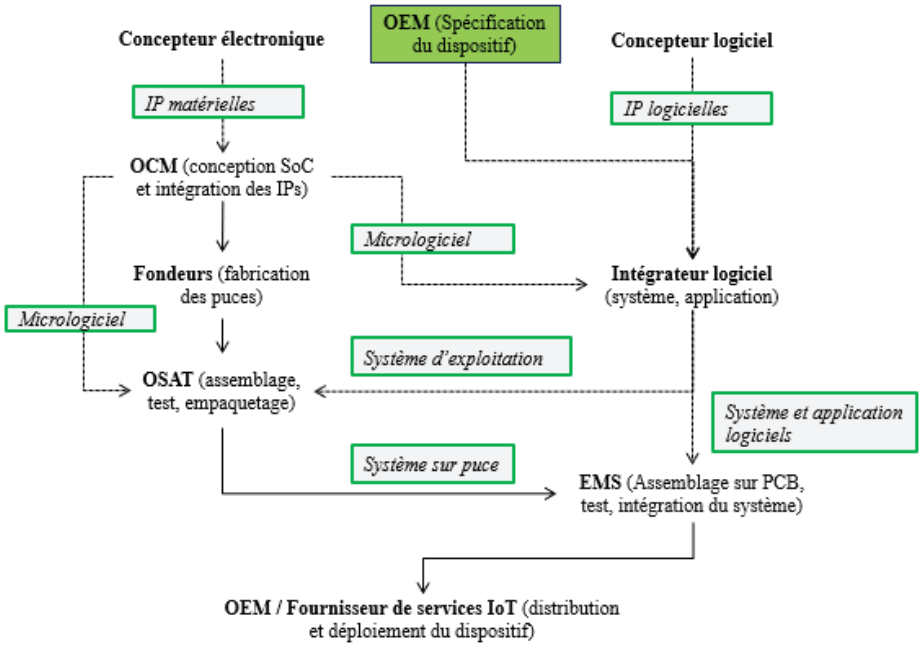

Figure 4: Acteurs et atouts de la chaine de production IoT

Nous constatons une multiplicité des acteurs et des interactions. Certaines étapes impliquent l'échange d'atouts sensibles : transfert de micrologiciels spécifiques au système sur puce, intégration d'application logiciel tierce, assemblage matériel par des sous-traitants…

1.1.3 Diversité des applications

La grande diversité des architectures, des modèles et des acteurs du cycle de vie IoT va de pair avec l'immensité des applications émergentes dans ce domaine. Les usages en lien avec l'IoT se multiplient dans tous les domaines et dans de nombreux pays y compris la France [3]. Divers secteurs voient de nouveaux dispositifs émergés. La domotique connectée et automatisée émerge : thermostat, lampe, serrure… Les objets du quotidien se dotent d'électronique et de capacité de communication et de

calcul perfectionné. Il en est de même pour une partie des dispositifs médicaux tels que les pompes à insuline, ou les stimulateurs cardiaques (*pacemaker)*. Ce développement des objets connectés se constate aussi dans les milieux industriels, militaires et aéronautiques. La liste des applications et des métiers potentiellement concernés est longue. Cette multiplicité des usages s'appuie sur la création et l'amélioration des fonctionnalités des systèmes sur puce. Les capacités de calcul et de communication accrues offrent de nouveaux potentiels pour des applications inédites et performantes ; alliant connectivité et automatisation. Les atouts se multiplient et se diversifient. Cela génère des risques au cours du cycle de vie ainsi que de nouvelles exigences de sécurité, dépendantes du cas d'usage.

Selon l'usage destiné à l'objet connecté les phases de déploiement, d'utilisation, de maintenance mais aussi de fin de vie font intervenir des acteurs et des métiers différents. Les modes opératoires et les cadres légaux ne sont pas identiques ; ainsi que la nature des données et fonctions manipulées par le système. Ces spécificités, variables selon les usages et applications ciblées par l'objet cyber-physique, influencent nécessairement les objectifs et exigences de sécurité. Les exigences de sécurité dépendront entre autre du niveau de confidentialité requis pour les données générées et stockées par le circuit. De plus, selon l'application et l'interaction avec l'extérieur des objets connectés, le détournement ou l'interruption de leurs fonctionnements n'auront pas le même impact. De même les contraintes de coûts et performances varient selon les besoins des utilisateurs et des fabricants. Les objectifs peuvent porter sur le coût de fabrication et la surface *silicium* du circuit, sur sa durée de vie, sur la vitesse et précision des calculs ou sur l'autonomie énergétique. Ainsi chaque cas d'usage d'un dispositif IoT présente des exigences de coûts, de performances et de sécurité qui lui sont spécifiques. Etudier le cycle de vie IoT pour un cas prédéfini est moins complexe que d'établir un modèle générique.

1.2 Besoins pour la sécurité au cours du cycle de vie

1.2.1 Accroissement de la surface d'attaque

Quel que soit le cas d'usage étudié, des problématiques génériques sont établies. L'évolution des technologies et de l'écosystème de l'IoT – complexification et segmentation du cycle de vie, multiplication des atouts et des acteurs – aboutit à de nouveaux enjeux de sécurité pour le cycle de vie.

Criticité des fonctionnalités *:* Les objets connectés disposent de fonctionnalités de plus en plus étendues : automatisation, inter-connectivité, calcul embarqué. Si cela améliore leurs capacités, cela implique aussi une augmentation du nombre de fonctions et de données à protéger. Les dispositifs accumulent et traitent des données privées des utilisateurs (géolocalisation, données de santé) de plus en plus sensible et en plus grande quantité. Le règlement général sur la protection des données [4] impose que la confidentialité et l'intégrité de celles-ci soient assurées. En outre, dans certains domaines (industriel, médical, aéronautique…) les conséquences d'une compromission de l'application IoT sont fortes : un détournement d'une fonction de calcul ou de commande menace directement l'intégrité physique du système ou de l'utilisateur : un dispositif médical peut commander une mauvaise infusion, un thermostat connecté dérégler la température de sa zone industriel…

Multiplication des interactions acteurs - système *:* De nouveaux acteurs sont impliqués, la liste établie en section 1.1.2 est longue et diversifiée : développeurs logiciels, fournisseurs de composants matériels, services prestataires pour la maintenance et l'assistance techniques… Les objets connectés subissent de plus en plus d'interaction avec des tierces parties qui peuvent élever leurs privilèges et réaliser des opérations non-autorisées, notamment via les interfaces de débogage JTAG ([5], [6]). Un acteur qui intervient sur le dispositif au cours d'une opération d'assemblage des composant matériels, ou pendant une maintenance, peut exploiter les fuites d'informations ou introduire des éléments malveillants tant logiciels que matériels (aussi dits *Chevaux de Troie* [7]). Ces menaces exposent les atouts, telles que les IPs (propriétés intellectuelles) intégrées dans le dispositif. Cela génère un fort besoin en authentification et en sécurisation des accès. Les interactions à distance sont aussi une source de menace. Une mise à jour logicielle développée par un tiers peut contenir un virus ; par ailleurs les autres dispositifs communicants sur le réseau peuvent être compromis et être un vecteur d'attaque contre l'objet ([8], [9]). Dans ces situations, non-exhaustives, la confidentialité et l'intégrité des atouts sont menacées.

***Confiance matérielle des SoC** :* Aujourd'hui, les SoCs nécessitent la fabrication, l'intégration et l'assemblage de divers composants matériels. L'ensemble de ces phases est aujourd'hui mondialisé, segmenté entre différents acteurs. La confiance n'est pas assurée aisément. Il y'a un risque que ces tiers éléments matériels soient compromis au cours de leur fabrication ou de leur distribution ([10], [11]). Les micrologiciels des systèmes sur puces, ainsi même que leurs composants matériels, sont désormais susceptibles d'être compromis ; incorporant des fonctions malveillantes ou des fuites d'informations.

En conséquence, un accroissement de la surface d'attaque est constaté. Les dispositifs comportent de plus en plus de composants matériels et logiciels. Ceux-ci sont de nature diverse et présentent des vulnérabilités qui leur sont propres. Les points d'entrées dans le système et les éléments sensibles se multiplient. Par ailleurs leur intégration implique des interactions et des accès physiques, parfois intrusifs, avec différents acteurs. Ces interactions peuvent être détournées, ou les acteurs usurpés. L'objet est exposé tout le long du cycle de vie, vulnérable face à des attaques d'origines multiples.

1.2.2 Accroissement des menaces et modèles d'adversaires

Les motivations des attaquants se multiplient : l'IoT concerne de plus en plus de données, parfois sensibles et sources de gain financier, et ce sans que la sécurité soit sérieusement prise en compte. De plus, l'IoT induit aussi une mise en réseau et des communications entre les systèmes et les utilisateurs, potentiellement un dispositif compromis peut ainsi fournir des accès ou données supplémentaires. L'exploitation des faiblesses de la sécurité des paramètres sensibles (mots de passe, clef de sécurité) fait notamment l'objet de nombreuses démonstrations. L'attaque de caméras connectées contre Dyn en 2016 [9] a provoqué des dégâts considérables. Les caméras, rattachées à un *botnet,* furent utilisées pour un DDoS de grande ampleur. La gestion des clefs d'authentication des caméras n'était pas assurée au cours du cycle de vie, aucune personnalisation des clefs et aucune vérification des accès. La sécurité de tels atouts doit être assurée tout au long du cycle de vie. Outre ces menaces qui s'appuient sur des failles logicielles, voir sur un simple manque d'hygiène en sécurité, la protection du matériel inquiète : les rapports d'étude sur les circuits intégrés et l'approvisionnement des composants électroniques pointent le nombre croissant des contrefaçons ainsi que le vol de propriétés intellectuels. Cela concerne y compris des domaines critiques (aéronautiques, militaires, médicales…)

Aujourd'hui les menaces se multiplient et se diversifient. Les scénarios d'attaques varient selon la capacité des attaquants et selon l'exposition du dispositif. La définition d'un modèle d'adversaires pour une étude sécurité peut s'avérer délicate. Nous relevons un modèle pertinent, établi par Bhunia et Ray [12], où les adversaires se classent selon le niveau d'accès aux interfaces logicielles et matérielles. Le tri se fait de l'accès le plus restreint (à distance, avec droit utilisateur seulement) à l'accès le plus intrusif (opération physique directe réalisée sur l'objet) :

- Adversaire à distance exploitant des failles logicielles et matérielles :
  - *Adversaire sans privilèges* qui attaque le système via l'application embarquée sur le SoC, et possède des droits utilisateurs restreints. Des failles logicielles ou matérielles sont exploitées pour élever les privilèges.
  - *Adversaire avec privilèges* qui a des accès au système d'exploitation ; et peut interagir avec les communications et opérations internes du système. Les protections doivent intervenir aux couches basses du système (*firmware* ou matérielles).
  - *Adversaire avec privilèges et accès aux canaux auxiliaires* qui, outre les accès classiques, dispose d'informations supplémentaires telles que la consommation d'énergie ou l'horloge.
- Adversaire avec un accès physique au dispositif :
  - *Adversaire limité (dit naïf)* qui utilise des équipements basiques (et peu cher) pour interagir avec le SoC via des accès usuels, type interface de débogage ou port JTAG.
  - *Adversaire avec équipement de rétro-ingénierie* qui dispose des équipements et des compétences suffisantes pour extraire les micrologiciels ou les designs matériels du SoC, y compris les paramètres de sécurité sensibles (clefs cryptographiques ou DRM).

- *Adversaire hautement intrusif* qui compromet le SoC par l'intégration de fonctionnalités ou de composants malveillants (*Trojan*). Cela suppose des accès à des composants matériels pendant les premières phases de production du SoC.

Ces modèles d'adversaires ne sont pas pris en compte avec la même importance selon le cas d'usage et les enjeux de sécurité. Une analyse spécifique doit être menée pour définir les besoins du cas étudié. Il apparaît toutefois aujourd'hui obligatoire de considérer les menaces matérielles et de déployer des contremesures adéquates.

1.3 Sécurité matérielle et cycle de vie

1.3.1 Contremesures pour les menaces matérielles : état de l'art et limites de l'existant pour la sécurité du cycle de vie

Un ensemble de contremesures existent dans l'industrie et dans la littérature scientifique pour atténuer les menaces et les risques que font peser les différents adversaires sur le cycle de vie. Les travaux sur ces protections, parfois très différents, entremêlent plusieurs disciplines – cryptographie, électronique, physique. Dans l'état de l'art, des études pertinentes balayent les vulnérabilités des systèmes sur puces et les solutions existantes : [11] pour les contrefaçons, [7] pour les chevaux de Troie, ou encore [10] qui couvre un ensemble plus larges des menaces connues. Ces études intègrent le cycle de vie des puces électroniques dans les modèles d'adversaires, en particulier au niveau des phases de production. Plusieurs solutions atténuent les failles de sécurité sans toutefois répondre à tous les besoins et exigences du cycle.

Protection spécifique pour les IPs matérielles : Comme décrit en 1.1.1et 1.1.2 un système sur puce intègre des IPs d'origines diverses. La confidentialité peut être exigée tant pour certaines de ces IPs que pour le design du SoC dans son ensemble. Diverses approches sont listées dans l'état de l'art [10] pour la sécurité IPs :

- *Marquage de filigrane :* la signature du concepteur de l'IP est marquée dans le circuit et utilisée au cours du cycle de vie pour authentifier l'IP.
- *Caractérisation d'empreinte physique :* la signature du circuit est extraite à partir d'un ou plusieurs paramètres choisis. Cette signature assure l'authenticité du circuit au cours du cycle de vie. Une forme aboutit de cette contremesure est l'intégration de primitive *PUF (Physical Unclonable Function)* dans le design du circuit. Un *PUF* génère une réponse en fonction de l'état physique du circuit et d'un challenge fournit par un acteur (utilisateur, intégrateur, auditeur…). Stockés dans une base de donnée, ces couples challenge-réponses permettent d'établir un protocole d'authentification pour les acteurs du cycle de vie.
- *Offuscation de design :* Des éléments logiques additionnels – type portes logiques (XOR/XNOR) ou éléments mémoires – couplés avec les fonctions et les IPs du circuit complexifient le design. Dans certains cas, les fonctions / IPs ne s'activent que si les éléments d'offuscations sont soumis à un vecteur d'entrée spécifique. Cela rend plus difficile la rétro-ingénierie et l'extraction des IPs.
- *Segmentation des masques de gravures :* Le design du circuit est divisé et répartie entre différentes fonderies, généralement entre les couches silicium arrière (*back-end*) et avant (*front-end*). Cela dépend du nombre de ligne de métal, une référence prend la quatrième ligne de métal comme séparateur. L'assemblage et le test du circuit sont réalisés par la suite par un tiers acteur.

Ces solutions apportent authenticité et confidentialité des IPs, toutefois elles ne répondent pas à tous les besoins du cycle de vie. Elles concernent la protection de l'IP d'un acteur, et non pas de l'ensemble des atouts du système. Les exigences de sécurité impliquent aussi les données privées de l'utilisateur, les fonctionnalités de l'objet et ses interactions avec l'extérieur. En outre, les solutions énumérées ne permettent pas l'usage ou la protection de clefs de sécurité, nécessaires pour les protocoles de chiffrement et d'authentification. Seule exception les PUFs, dont certaines implémentations remplissent les critères des primitives de sécurité pour la génération et stockage de clefs cryptographiques.

Réduction de la fuite d'information : Les attaques par canaux auxiliaires sont une des menaces redoutées. L'analyse de variations des paramètres physiques (consommation énergétique, temps de calcul, émanation électromagnétique) permet d'extraire des informations sensibles tels que les clefs de chiffrement. L'accès non sécurisé des chaines de scan interne (utilisé pour du débogage) sont une faille par laquelle les clefs peuvent être extraites. Plusieurs solutions réduisent ces fuites d'informations:

- *Injection de bruit aléatoire:* Ajout d'opération pour introduire de l'aléa dans la consommation d'énergie du circuit, ou dans les temps de calcul, faisant ainsi échouer les analyses de corrélation.
- *Mise à jour des clefs de sécurité et restriction de leur usage :* Cette contremesure se concentre sur le protocole de sécurité. La clé est restreinte à un nombre limité d'utilisation ; l'attaquant doit alors réussir l'analyse avec peu de trace. Aussi la clef est modifiée régulièrement au cours du cycle de vie ; l'attaquant doit réitérer l'analyse pour chaque nouvelle clef.
- *Sécurisation des chaines de scan :* L'accès aux chaines internes pour le débogage peut être protégé par diverses méthodes. Un filtrage par des mécanismes d'authentification peut limiter l'accès aux informations sensibles [13], ou une désorganisation aléatoire de la chaine en sous-chaines.

Ces protections sont nécessaires car une compromission des clefs de sécurité à un impact grave sur le système. Les exigences de sécurité concernant ces modèles d'attaques sont parfois sévères, notamment dans le domaine des cartes à puce bancaire : des normes strictes imposent l'intégration et l'étude de contremesures robustes. Toutefois ces protections concernent uniquement la protection du stockage des clefs de sécurité, elles ne répondent pas aux autres besoins de sécurité : authenticité des IPs, génération des clefs de sécurité, répudiation des clefs corrompues ou obsolètes et confidentialité du design.

Lutte contre la contrefaçon : Dans les solutions décrites précédemment plusieurs d'entre elles assurent l'authenticité du matériel : le marquage de filigrane pour authentifier le concepteur, l'empreinte physique pour authentifier le circuit ou en particulier les PUFs qui potentiellement offrent un large espace de signature. En outre, les clefs de sécurité sont aussi un moyen de vérifier l'authenticité du circuit sous réserve que la génération, la programmation et le stockage de ces clefs soient sûre. Ici, une approche idéale est l'implémentation légère et sures d'un PUF vérifiant des critères de sécurité élevés, preuve de l'authenticité et de l'unicité des clefs de sécurité générés.

Une autre gamme de contremesures se base sur des techniques d'inspection [11] :

- *Les tests électriques classiques :* Tests paramétriques, tests fonctionnels ou tests structurels ; initialement utilisés pour valider la bonne fabrication et la fonctionnalité des puces sont ici mis en œuvre pour vérifier l'authenticité et l'intégrité du circuit
- *Les inspections physiques extérieures :* Analyse de l'état du circuit sans décapsulation.
- *Les inspections physiques internes :* Intervention sur l'emballage du circuit pour exposer sa structure et réaliser une observation approfondie.
- *Les analyses de matériaux* : Observations du circuit et de ses couches internes par des équipements optiques ou physiques qui détaillent leur composition.

Si ces inspections offrent une authenticité forte du circuit, elles sont aussi couteuses, fastidieuses et ne couvrent que les premières phases du cycle. Elles ne sont réalisables que au cours de la production et ne répondent pas non plus aux autres besoins de sécurité du cycle de vie : génération et stockage des clefs de sécurité, sécurisation des accès physiques aux atouts sensibles ou mise à jour logicielle.

1.3.2 Solutions de sécurité complètes pour les besoins de sécurité du cycle de vie

La plupart des contremesures se limitent à répondre à un ou deux besoins de sécurité spécifiques, sans considérer l'ensemble du cycle de vie. Certains articles proposent toutefois des solutions de sécurité pour le cycle de vie, des supports matériels pour une gestion sûre et flexible des atouts du cycle de vie. Elles répondent aux besoins spécifiques du cycle de vie, décris en 1.1.2 et 1.2.1: authentification des acteurs et gestion sécurisée des accès, et ce pour diverses opérations du cycle.

Architecture et protocole pour des mécanismes de débogage sécurisé et flexible [13]**:** Les auteurs détaillent une architecture personnalisée de l'interface de débogage de SoC. Elle assure la confidentialité des atouts et la sécurité des accès au SoC. Un mécanisme de filtre est intégré en amont du bus de débogage, les données qui y transitent sont chiffrées (AES). Cela inclut les micrologiciels propriétaires des concepteurs. Les identifiants des acteurs du cycle de vie (nommés en 1.1.2, *OEM, OSAT*…) sont stockés dans un table. La solution impose pour tout accès au SoC une authentification des acteurs avec ces identifiants. Le filtre peut chiffrer les données pour lesquelles l'acteur n'a aucun droit d'interaction. Pour contrer une extraction malveillante des clefs d'authentification (stockées en ROM) les auteurs suggèrent de substituer les clefs par un PUF. En l'occurrence, l'article [14] inclut l'intégration et l'utilisation d'un TERO-PUF dans l'architecture sécurisée de débogage. Une évaluation indique un surplus de surface qui ne dépasse pas 7 % du total initial requis pour le circuit de l'étude.

Plateforme de gestion sécurisée du cycle de vie du SoC et de ses IPs [15] **:** les auteurs proposent d'intégrer dans le SoC une IP matériel, un contrôleur qui d'une part stocke des informations de sécurité (code d'autorisation, identifiant, empreinte d'authentification) et qui par ailleurs contient des primitives de sécurité (implémentation matérielle cryptographique pour chiffrement ou authentification). Selon un ensemble de spécifications protocolaires ce contrôleur permet de sécuriser la communication et les interactions avec le SoC ; assurant l'authenticité des actions et la confidentialité des IPs. Un élément clef de l'architecture est la SRAM-PUF, un modèle PUF basé sur le comportement aléatoire des cellules mémoires pour générer la clef maîtresse assurant la confiance dans le SoC (*Root of Trust)*

Ces références sont les premiers travaux pertinents offrant une réponse aux besoins de sécurité du cycle de vie IoT. Dans les deux cas cités, nous constatons que les primitives PUFs jouent un rôle primordial. Ces fonctions matérielles sont un socle pour l'architecture de sécurité ; mécanismes de génération et de stockage des paramètres (clefs, signatures) sur lesquelles reposent les propriétés de sécurité.

1.4 Objectifs

1.4.1 Premier bilan sur la sécurité du cycle de vie IoT

L'accroissement de la surface d'attaque et des menaces (section 1.2) génère des besoins de sécurité importants tout au long du cycle de vie ; la sécurisation ne peut se faire sans prise en compte des menaces en amont ou en aval. Une étude approfondie de la sécurité du dispositif sur l'ensemble des phases de production et d'utilisation est nécessaire. Il existe des approches pour instaurer la confiance au cours du cycle de vie mais les schémas sont difficiles à mettre en place et leurs apports parfois limités. De plus les besoins en vérifications et surveillance décris en 1.1.1 nécessitent des accès flexibles. Chaque acteur requiert en effet des accès aux fonctionnalités et aux atouts du système pour performer les tâches spécifiques qui lui sont attribuées.

Comment assurer qu'une partie prenante dispose d'un accès uniquement aux atouts qui lui sont autorisées et nécessaires, et cela à travers les multiples phases du cycle de vie dotées de politiques d'accès distinctes ?

La sécurisation et la gestion de ces accès mène naturellement à la mise en œuvre de chiffrement pour assurer la confidentialité des données et de protocole d'authentification pour authentifier les acteurs. De telles primitives reposent sur des paramètres de sécurité: clefs de chiffrement, signature d'authentification… Ces éléments sont stockés et manipulés par le matériel (au niveau du SoC) et cela oblige de prendre en compte des besoins en sécurité matérielle. Une première conclusion souligne les considérations suivantes :

- Des mécanismes matériels doivent être intégrés pour sécuriser le cycle de vie, gérer et filtrer les accès et actions réalisés dès les premières phases de production des puces.
- Ces mécanismes doivent être flexibles, c.à.d. permettre les accès et interactions nécessaires aux opérations d'intégration, programmation ou vérification au cours du cycle.

- Ces mécanismes doivent assurer une certaine robustesse contre les menaces matérielles, c.à.d. être sujet à une fuite d'information par canal auxiliaire limitée, offrir une certaine résistance à la rétro-ingénierie ou à la contrefaçon…
- Pour terminer ces mécanismes doivent offrir des possibilités de compromis, respectant les contraintes de ressources et d'usage du dispositif IoT.

1.4.2 Organisation du mémoire

La section 2 présente l'étude théorique de la sécurité d'un cas d'usage et ce avec l'appui d'une méthodologie de référence. Les objectifs sont d'acquérir un formalisme pour les analyses de sécurité, dégager les vulnérabilités induites par le cycle vie sur un cas concret et identifier les exigences à respecter pour une solution de sécurité efficace. En ce qui concerne le cas d'usage il a été retenu l'exemple des dispositifs médicaux (DM) connectés. Si les DMs apportent des bénéfices importants pour le secteur médical, leurs brèches de sécurité provoquent aussi des inquiétudes couramment relayées par les chercheurs du domaine lors des conférences. Une approche rationnelle est privilégiée pour estimer correctement les risques, une analyse de sécurité avec une vision globale du cycle de vie IoT. Cette étude révèle des vulnérabilités pernicieuses, toutefois l'intégration de protection se répercute sur le coût de fabrication, les performances de l'appareil ainsi que sur les contraintes d'utilisation et de maintenance. Nous concluons sur l'impératif de concevoir des mécanismes de sécurité flexibles et efficients qui répondent aux contraintes de coût et d'usage. Nous décidons par la suite de restreindre le périmètre de la thèse à la conception d'un nouveau modèle de Fonction Physique Non-clonable.

La section 3 offre un état de l'art des recherches sur les PUFs, avec pour intérêt premier la catégorie *digital PUF*. Cette gamme d'implémentations s'appuie sur un aléa de nature structurelle et se caractérise par une robustesse forte. Cela assure la reproductibilité des réponses de tels PUFs ; réduisant les risques de faux rejets et le besoin en code correcteur d'erreur. Le chapitre introduit d'abord des généralités sur les PUFs : définition, critères de classification, métriques de sécurité et avancement de la recherche. Nous détaillons ensuite les *digital PUFs* existants, les processus de fabrication à l'origine de l'aléa structurelle mais également les modèles de circuits logiques pour la génération des réponses et les résultats des évaluations de sécurité de ces PUFs. Dans le contexte du cycle de vie le PUF doit répondre à des besoins d'authentification au cours de multiples interactions impliquant divers acteurs. En conséquence nous nous focalisons sur les propriétés et contraintes pour concevoir un modèle *strong digital PUF*. Le qualificatif *strong* d'un PUF se caractérisant par un mécanisme de challenge-réponse offrant un « large » espace de réponses. Cela permettra de déployer un protocole d'authentification basé sur les multiples réponses du *strong PUF*

La section 4 introduit notre proposition de modèle de circuit logique pour construire un modèle *strong digital PUF* assurant une forte entropie. Le circuit doit extraire une réponse de l'aléa structurel et permettre un compromis sécurité-coût. Nous spécifions un mécanisme challenge-réponse basé sur un réseau d'opération mathématiques de type substitution-permutation. Ce type de réseau (nommé SPN) offre une forte entropie et respecte des propriétés de sécurité adéquates. Pour la conception de ce circuit nous faisons l'hypothèse de la faisabilité d'une grille d'interconnections aléatoires par un procédé de fabrication *DPUF* quel qu'il soit. Nous définissons un modèle d'étude comportant plusieurs paramètres (en lien avec les aspects physiques de la grille aléatoire du *DPUF* mais aussi avec le schéma mathématique *SPN*). L'architecture obtenue est nommée *SPN-DPUF*. Par la suite, nous proposons une approche pour optimiser le design *SPN-DPUF*, limitant les coûts de surface du circuit *DPUF* et les contraintes sur le procédé de fabrication.

La section 5 présente l'analyse de sécurité du modèle *SPN-DPUF* ainsi que d'autres variantes incluant une des propositions de circuit existante dans la littérature. Nous présentons la méthodologie et les outils développés pour la modélisation et l'évaluation. La plateforme réalisée permet de générer une base de challenge-réponse pour les modèles *DPUF* étudiés et les jeux de paramètres choisis. Parmi les paramètres de configuration nous étudions l'impact de la probabilité de fermeture des connections, la taille de la grille (nombre de colonnes et de rangées) et le niveau de séquencement des opérations dans le réseau *SPN*. Une étude statistique approfondie l'influence de la configuration sur les métriques de

sécurité des PUFs. Cette évaluation a permis d'identifier des jeux de paramètre pour optimiser le compromis entre la sécurité du DPUF et les contraintes de taille et d'entropie.

La section 6 complète l'étude précédente par des travaux de simulation et synthèse numériques des circuits; cela afin d'estimer des coûts d'implémentation des modèles proposés. Des codes descriptifs VHDL des modèles *SPN-DPUFs* sont développés et synthétisés pour les jeux de paramètres identifiés pour des compromis sécurit-cout. Une 1ère phase porte sur l'implémentation des circuits et la vérification des respects des contraintes de délais. Par la suite une 2ème phase analyse les indicateurs de performance fournis par les outils de synthèse. Les métriques ciblées sont la surface, l'énergie consommée et la vitesse de traitement ; elles sont relevées en fonction des paramètres des circuits SPN-DPUFs. Un bilan des résultats est réalisé sur l'ensemble des métriques: surface, fréquence, puissance mises en jeu par le circuit mais également énergie consommée par bit, latence et débit.

La section 7 conclut les travaux sur deux perspectives qui doivent être approfondies. La première concerne l'évaluation du coût globale et des contraintes pour la fabrication d'un circuit *SPN-DPUF* complet et performant. La deuxième porte sur les problématiques d'intégration du *SPN-DPUF* dans le cycle de vie et sur le déploiement des protocoles d'authentification exploitation la primitive.

2 Sécurité du cycle de vie d'un dispositif médical

Nous étudions un cas concret dans le but d'illustrer les enjeux de sécurité liés au cycle de vie. Notre objectif est aussi de formaliser les exigences de sécurité qui découlent des multiples interactions et vulnérabilités induites par le cycle. Le cas d'étude (pompe à perfusion connectée) est un système cyber-physique doté de fonctions spécifiques pour un usage médical et classifié en tant que *dispositif médical (DM)*. Ce type de dispositif subit des contraintes réglementaires fortes, cadré par des règles de classification qui sont détaillées dans cette première section. L'analyse de sécurité sur ce dispositif nous permet d'établir les conséquences graves qui découlent des vulnérabilités de son cycle de vie et la nécessité de déployer des contremesures du fait des risques et exigences identifiés.

La première section introduit les dispositifs médicaux et le règlement 2017/745 de l'Union Européenne [16] qui définit les termes employés dans l'électronique médicale. Il distingue les dispositifs réglementés des applications de bien-être. Nous abordons quelles sont les exigences spécifiques pour les fabricants de DM au cours du cycle de vie. Nous précisons les contraintes et procédures qui doivent être respectées selon la classe du DM. Ces exigences portent sur la performance des dispositifs ainsi que sur leur sécurité. Nous détaillons nos motivations pour ce sujet, les craintes pour la sécurité et finalement le besoin d'établir un compromis avec les contraintes exigées pour les DMs.

La deuxième partie introduit le cas d'étude de sécurité des systèmes de perfusion ; avec comme modèle d'exemple le pancréas artificiel : un système avec pompe à insuline connectée et automatisée. Nous présentons la méthodologie EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) qui cadre, formalise et dirige l'étude de sécurité. La section détaille ensuite l'architecture de ce type de DM, les éléments qui le composent et les interactions auxquelles ils participent. Cela est déterminant pour la compréhension des risques et des besoins de sécurité. Nous réalisons un inventaire détaillé des composants du DM et des acteurs qui interviennent au cours du cycle de vie. Nous décrivons les accès et interactions qui exposent les éléments sensibles du DM (données, logiciels…). Cela éclaire un premier bilan sur les risques menaçant la sécurité du DM. Ce cas d'étude est représentatif des enjeux de sécurité l'IoT médical : concevoir des dispositifs portables performants et sures ; respectant à la fois les contraintes du médical et de flexibilité des accès au cours du cycle de vie.

La troisième et dernière section synthétise l'analyse de risque réalisée pour le dispositif médical. Le niveau de risque s'établit en fonction de de la vraisemblance des scénarios des menaces et de leur impact sur le dispositif. Le bilan de l'analyse aboutit à l'identification des risques les plus significatifs ; notamment la faible sécurisation des interfaces physiques et le manque d'assurance pour l'authenticité des composants. Des contremesures sont nécessaires pour atténuer ces risques. Au terme de cette étude, les besoins de sécurité du dispositif sont établis, ainsi que les exigences auxquelles doivent répondre les contremesures. Nous concluons sur notre intérêt pour la conception de primitive d'authentification de type PUF (Physical Unclonable Function) afin de répondre à ces besoins.

2.1 Dispositifs médicaux

2.1.1 Terminologie et classification des dispositifs médicaux

Les dispositifs électroniques à usages médicaux sont l'objet d'un cadre réglementaire rigoureux en particulier vis-à-vis des risques de défaillances et des exigences de traçabilité au cours du cycle de vie. Les récentes évolutions apportent une plus grande considération pour les aspects sécuritaires, et ce d'autant que dans certains cas d'usage la compromission de l'objet peut avoir un impact grave sur le patient ou les atouts sensibles du cycle de vie (données privées, logiciel médical…). Le règlement 2017/745 de l'Union Européenne [16] définit les termes employés dans l'électronique médicale ainsi que les critères qui déterminent le statut d'un objet en tant que dispositif médical (DM). Nous détaillons en annexe 10.1 cette partie du règlement, ainsi que des exemples de classifications de DM.

En résumé, il convient de distinguer les dispositifs médicaux certifiés et les produits de « bien-être ou de confort », aussi appelés produits ou applications de santé mobile. Un dispositif a donc le qualificatif « médical » s'il répond à un état de santé défaillant, et non pas un besoin de bien-être, confort ou de diagnostic physiologique à finalités sportive. Le règlement [16] considère qu'un produit relève du statut dispositif médical (DM) pour « tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour des fins médicales précises, (notamment traitement ou diagnostic) et dont l'action principale n'est pas obtenue par des moyens pharmacologiques. ». Les usages en médecine sont aujourd'hui multiples, diversifiés et ont des incidences variables en termes de risques. Il faut noter que le niveau de risque associé à un produit ne justifie pas le statut de celui-ci en tant que DM ; il intervient par contre dans les règles de classification des DMs

Le règlement de l'U.E. – article 51 – stipule que « Les dispositifs sont répartis dans quatre classes (I, IIa, IIb, III) en fonction de la destination (usage) des dispositifs et des risques qui leur sont inhérents. La classification est effectuée conformément à l'annexe VIII. » La dangerosité du dispositif pour le patient est prise en compte dans les règles de classification. Tous les critères interviennent, tels que la nature de l'usage, la durée d'utilisation du DM, le caractère ou encore la localisation du DM.

Chaque classe se voit attribuer des contraintes réglementaires spécifiques, des exigences de plus grande sévérité à mesure que la criticité du dispositif augmente. Nous décrivons des exemples de DM pour chaque classe avec une brève interprétation des règles de classifications dans l'annexe 10.1. Le cas d'usage que nous étudions, la pompe à perfusion, se positionne en classe IIb. Le dispositif administre des médicaments potentiellement dangereux, telle que l'insuline, et peut être reconfigurer à distance. Une compromission de cet objet impacte la santé du patient, face à un tel risque les aspects sécuritaires doivent être traités et ce tout au long du cycle de vie. Cela impose des contraintes au cours du cycle de vie, notamment des opérations de vérification et de suivi avant et après la mise sur le marché.

2.1.2 Contraintes réglementaires au cours du cycle de vie

Des organismes notifiés (« ON »), laboratoires ou groupes d'expertises certifiés, interviennent pendant le cycle de vie pour évaluer les DMs et valider le marquage CE (« Conformité Européenne »). Le fabricant justifie avec ce marquage la conformité technique de son DM auprès de ses utilisateurs ou partenaires ; obligatoire pour une mise sur le marché ([17]). Cela nécessite des accès et des opérations de tests ou de vérification par les ONs à divers moments du cycle.

Deux exigences sont communes à toutes les classes : la réalisation d'un dossier technique (spécifications, analyse de risque, rapport d'évaluation …) et le déploiement de procédure de suivi au cours du cycle de vie (service d'assistance, surveillance des incidents). Dans la Figure 5, décrivant les exigences pour la classe IIb qui correspond à notre cas d'étude (pompe médicale connectée), le fabricant a le choix entre différentes procédures. Il peut déployer une assurance qualité, notamment avec l'application de la norme ISO 13485 (Dispositifs médicaux — Systèmes de management de la qualité — Exigences à des fins réglementaires). Ces procédures d'assurance seront évaluées par un ON. L'autre option est la délégation à l'ON de certaines étapes du cycle de vie. Au final plusieurs démarches réglementaires sont offertes : le fabricant peut ainsi sélectionner ce qui convient le plus à sa situation.

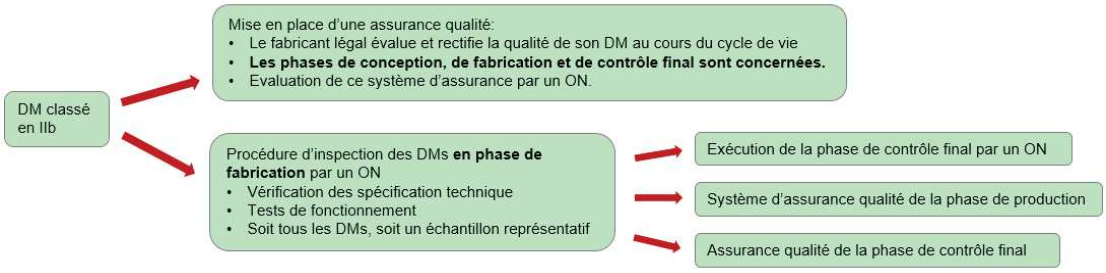

Figure 5: : Les procédures de contrôles des DMs de classe IIb

Après obtention du marquage CE le fabricant légal peut commercialiser le DM. Des procédures de surveillance et de maintenance, exigées par le règlement, « sécurisent » le cycle de vie du DM :

- ***Les protocoles de matériovigilance :*** Déploiement d'un service qui collecte les déclarations d'incidents par les utilisateurs et analyse ces données. Le service doit opérer toute maintenance préventive ou corrective pour assurer la qualité des DMs.
- ***Surveillance post-marché (PMS) :*** Le fabricant doit veiller à l'évolution des DMs sur le terrain ; réévaluer périodiquement les risques et le niveau de qualité. Cela inclut des revues de la littérature et un suivi clinique. Des mises à jour logicielles sont prévues pour améliorer les performances ou rectifier les fonctionnalités.
- ***Mise à jour d'un dossier post-marché :*** Le fabricant doit entretenir et mettre à disposition au cours d'un éventuel audit un dossier sur son DM. Le dossier contient les données de surveillance sur la qualité et les risques des DMs au cours de leur utilisation.
- ***Maintenance matérielle :*** Le fabricant légal doit assurer la « maintenance matériel » du DM au cours de la phase d'utilisation. Ce service d'assistance réalise les remplacements et les reconfigurations, tel que cela est spécifié d'après les protocoles de matériovigilances. Il faut noter que le fabricant doit maintenir sa capacité à produire et distribuer tout composant matériel nécessaire au fonctionnement ou à la réparation des dispositifs encore présent sur le marché.
- ***Audit de surveillance annuelle*** *:* L'organisme notifié réalise des contrôles annuels, vérifiant la bonne mise en œuvre des assurances de qualité. Cela se programme à des périodes prédéfinies mais intervient aussi de manière « inopinés ».
- ***La phase de fin de vie :*** Le fabricant est responsable de la spécification, évaluation et mise en place des procédures d'élimination des DMs. Le recyclage des objets est autorisé ; l'opérateur qui recycle a par contre le statut de fabricant et doit respecter toutes les exigences décrites précédemment.

2.1.3 Motivation et enjeu pour la sécurité de l'IoT médical

Des dispositifs électroniques légers et portables embarquent aujourd'hui des logiciels médicaux performants avec les fonctions nécessaires pour des diagnostics ou des analyses. Cela a un intérêt sociétal fort : amélioration des traitements médicaux, hospitalisations à domicile et meilleure qualité de vie pour les patients. Les apports des DMs sont toutefois contrebalancés par les risques qu'ils induisent pour la sécurité des patient, en particulier au regards des cyber menaces. Des failles peuvent être exploités pour compromettre le dispositif, les chercheurs en font la démonstration régulièrement. Un état de l'art conséquent existe sur la sécurité des objets médicaux, [18] répertorie les vulnérabilités des dispositifs médicaux et les contremesures potentielles, [19] présente une étude plus holistique avec la considération pour l'environnement, « l'écosystème », qui interagit avec ces appareils. Les dispositifs IoT sont interconnectés, et ce avec des protocoles de communication comportant potentiellement des failles de sécurité : il y'a une exposition aux menaces par le réseau, en provenance de tierces parties criminelles ou d'autres dispositifs qui seraient compromis. Outre les démonstrations et les études de vulnérabilité nous constatons aussi que le secteur médical est régulièrement ciblé par des cyber-attaques ; vol de données médicales privées, exécution de rançongiciel sur les services informatiques. Cela ouvre par contre la question d'une « convergence » entre les risques induits par les failles des DMs et les menaces contre le médical. Cette question se répercute sur les exigences de sécurité définies par le cadre réglementaire, celui-ci est contraignant mais peut encore se durcir à l'avenir.

La chronologie [20] synthétise les événements marquants dans la recherche des vulnérabilités des dispositifs médicaux connectés, ainsi que les actions entreprises par les institutions, telle que la FDA (Food Drug and Administration), pour atténuer les risques. Les exigences de conformité techniques imposent des contraintes de sécurité du patient. L'accroissement des enjeux « cybersécurité » a provoqué l'édition de recommandations fortes et de règlement sur la sécurisation des DMs. La FDA (Food and Drug Administration) fournit des guides pour la cybersécurité, en amont [21] et aval [22] de la commercialisation d'un dispositif. Le nouveau règlement acté par l'Union Européenne a de plus fortes exigences sur la cybersécurité [16]. Le fabricant se confronte ainsi aux contraintes de sécurité de DMs ; il doit théoriquement concevoir un dispositif qui présente un niveau de sécurité élevé. La problématique

s'aggrave avec le développement des dispositifs. Les interactions avec et autour d'un DM se complexifient, s'accroissent et impactent son utilisation, et ce tout au long du cycle de vie. Les avertissements listés en section 1.2.1 concernent aussi les DMs : le nombre et la criticité des fonctions à protéger augmentent, le cycle de vie intègre des composants de tierces parties et induit de nouvelles interactions. Le fabricant légal doit inclure ces vulnérabilités liées à la cybersécurité dans son analyse de risque ; et par la suite démontrer l'efficacité des contremesures intégrées dans le DM. Les protections sont proportionnelles à la classe de criticité du DM, et doivent considérer les menaces de tiers parties, et ce dans le contexte d'un cycle de vie à interactions multiples. Cette situation nécessite une étude approfondie de la sécurité du dispositif, et ce en considérant l'ensemble du cycle de vie. Au vue de ces enjeux, l'étude de sécurité du cycle de vie des DMs apparait donc aujourd'hui primordiale.

2.1.4 Besoin d'un compromis entré sécurité et contraintes des DMs

Les dispositifs médicaux sont des systèmes isolés, embarquant une application logicielle exploitée sur le long terme. Cela correspond notamment au cas des pompes médical portables pour patients diabétiques. De tels dispositifs doivent respecter un certain niveau de performances :

- Faible consommation. Il s'agit d'un objet portable, sans canal d'alimentation, et avec le besoin de fonctionner sur de longue période.
- Disponibilité et fiabilité. Le dispositif doit réaliser avec succès ses fonctions pour le traitement médical. Cela implique une efficacité des opérations (vitesse, précision …).
- Coût de fabrication réduit. Le produit concerne des utilisateurs (patients ou institut médical) ayant des contraintes financières fortes. Il doit rester accessible.

Le fabricant se confronte donc à la fois aux questions de sécurité et de performances : cela mène au besoin d'un compromis optimal entre ces contraintes. Il s'agit d'une problématique courante dans la sécurité des systèmes embarqués, et qui est prise en compte dans la suite des recherches.

De plus, au cours du cycle de vie le fabricant doit accéder, ou autoriser l'accès à des tiers, aux dispositifs. Cela se fait à divers moments et pour diverses raisons : contrôle de la qualité, maintenance, ou audit. Par exemple, au cours du contrôle final, l'inspection d'un DMs consiste à vérifier si leurs performances, leurs niveaux de sécurité et de sûreté, et leurs fonctions médicales correspondent aux spécifications. Cela implique l'autorisation d'effectuer des tests sur le DM, d'exécuter ses fonctions et d'accéder à des données techniques. Certaines contraintes portent aussi sur l'usage des données :

- Usage médical pour l'observation du patient, avec collecte des données par l'objet et transmission à un serveur agrégé.
- Usage technique également, communication de données concernant le statut du dispositif. Le fabricant réalise un suivi de ses DMs évaluant performances et fonctionnalités.

Cela nécessite des droits d'accès à certaines données des DMs et la mise en œuvre d'une communication sécurisée. En outre, des opérations telles que les maintenances ou les mises à jour logicielles impliquent un accès à des composants critiques de l'objet. Cela ajoute un besoin d'accès flexible à des éléments internes du DM. Pour finir les utilisateurs requièrent dans certains cas, tels que des situations d'urgence, d'accéder à des fonctions de l'objet pour rectifier le traitement ou vérifier le fonctionnement du DM. Cela peut exiger une flexibilité des droits d'accès.

Cela justifie le besoin de sécuriser la gestion des interactions et des accès de manière flexible :; il faut intégrer des protections pour protéger les éléments critiques du DM, démontrer leur efficacité au cours du cycle de vie mais sans compromettre les autres contraintes (règlementation, couts, usages…).

2.2 Contexte de l'étude de sécurité de la pompe à insuline

2.2.1 Méthodologie EBIOS pour l'analyse de sécurité

Nous appliquons la méthodologie EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) sur le cas d'étude de pompe médicale connectée. Elle a été élaboré en 1995 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qui fournit plusieurs documents de références, le guide détaillé [23] ainsi que [24], une base de connaissance pour l'énumération des types de menaces. EBIOS est une méthode générique qui s'adapte au contexte, le « bien » à protéger peut-être une infrastructure, un service interne d'une entreprise ou une application logicielle. Les objectifs de sécurité varient : cartographie des risques, mise en œuvre d'une politique de sécurité ou évaluation plus technique et précise des protections. La figure 11 présente les cinq modules de la méthode EBIOS. : l'étude de contexte, l'estimation des événements redoutés et de leur impact, la description des scénarios de menaces, la synthèse des risques et l'évaluation des contremesures.

Comme décrit par la figure 11 la synthèse des risques consiste à coupler les événements redoutés avec les scénarios de menaces. Ces deux modules s'appuient respectivement sur les cotations suivantes : un niveau d'impact (quels dégâts occasionnent l'événement) et un niveau de vraisemblance (crédibilité de la mise en œuvre du scénario de menaces par un adversaire). Le cinquième et dernier module n'est pas nécessaire dans le cas où l'étude se limites à l'établissement d'une cartographie des risques.

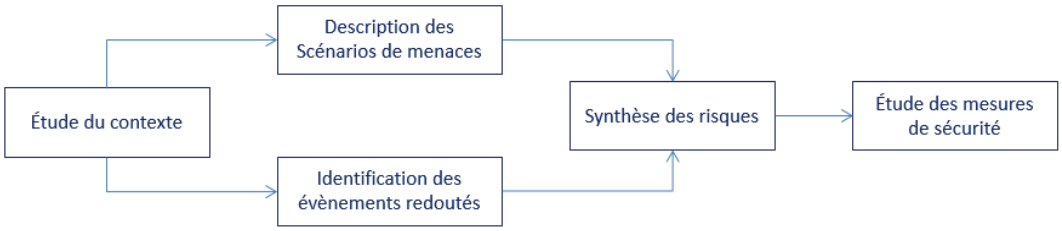

Figure 6: Modules de la méthodologie EBIOS

Objectifs : Notre étude de sécurité se focalise sur les risques induits par le cycle de vie du DM et par les problématiques d'authentification et de gestion des accès au cours des diverses opérations :

- Authentification des acteurs et des biens, impliqués dans plusieurs phases du cycle de vie.
- Multiplication des accès et des interactions qui requièrent un certain niveau de sécurité.
- Gestion des autorisations, avec une flexibilité requise pour l'exploitation du DM.

Ces questions impactent la sécurité du DM au cours du cycle de vie et accroissent le niveau de risque. Le premier objectif est l'identification des exigences de sécurité qui découlent de ces enjeux ; cela est établi au cours du module 4 qui étudie les risques significatifs. Le deuxième objectif est l'identification de contremesures adéquates qui répondent à ces besoins de sécurité.

L'ensemble de l'analyse de risque est résumée en annexe 10.2. La suite de la section décrit toutefois en détaille le contexte de l'étude : l'architecture et le cycle de vie du DM, avec des précisions sur les acteurs, les composants matériels du DM, les communications et les interactions au cours du cycle. Cela est déterminant pour la compréhension des risques et des besoins de sécurité qui en résultent.

2.2.2 Architecture de la pompe à insuline connectée

Des systèmes de pompe à perfusion portables et automatisés se développent grâce au perfectionnement des composants matériels et logiciels. Parmi les applications récentes et représentatives des bénéfices pour les patients nous trouvons le cas du **Pancréas Artificiel (PA).** Ce dispositif est destiné au traitement du diabète : déficience du pancréas qui provoque un défaut dans la génération d'insuline [25]. Le pancréas artificiel est un système cyber-physique qui consiste à automatiser l'administration de l'insuline et ce avec un contrôle régulier de l'état du patient (c.à.d. dans notre le taux de glucose). Le système pali ainsi les défauts de régulation. Une des architectures couramment proposées se forme de trois sous-dispositifs. La Figure 7 présente cette boucle de régulation qui comporte un dispositif d'observation (DO), un dispositif de contrôle (DC) et un dispositif d'injection (DI). Le DO mesure et transmet le taux du glucose du patient au DC. Le DC analyse les données médicales et commande au DI l'injection d'insuline nécessaire pour réguler l'état du patient. Le DO est aussi connu sous le nom de CGM (« Continuous Glucose Monitoring »).

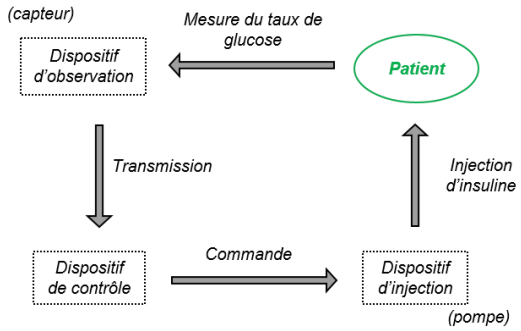

Figure 7: Système de pancréas artificiel pour réguler l'insuline

Certaines architectures intègrent le système de contrôle dans la pompe à perfusion. Cela réduit la boucle au couple capteur / pompe. La section 2.2 de la publication [26] compare et présente ces deux configurations possibles. Le cas étudié dans la thèse est celui de la Figure 7 , plus fréquemment étudié en recherche médicale. Cela permet en plus d'aborder les questions d'interactions inter-dispositif. L'institution IEEE publie et met à jours des normes concernant les dispositifs d'injections et d'observations : [27] et [28] pour les premiers rapports de 2018, qui décrivent les exigences génériques en termes d'architecture, de fonctionnalité et de communication. Dans le cas d'étude le système comporte donc un dispositif de contrôle qui réalise l'analyse des données du patient. La dose d'insuline est déterminée en fonction de la mesure du glucose et du profil du patient. Cela implique la configuration du DM par le médecin. En outre, l'utilisateur peut renseigner des informations complémentaires. Ainsi plusieurs personnes ont un accès physique direct au système au cours de la phase d'utilisation :

- Personnel médical, qui configure le dispositif, le traitement médical et le profil du patient.
- Patient, qui informe le dispositif de certains événements (repas, activités sportives.), ou effectue des actions spécifique (modification du traitement, mise en pause…).
- Opérateurs techniques qui interviennent pour la maintenance du système.

La Figure 8 complète le schéma précédent avec les interactions au cours de la phase d'utilisation entre le DM et les acteurs extérieurs. Le schéma montre aussi les interactions avec des serveurs à distances. Un serveur dédié aux données de santé réceptionne (communication à sens unique) des données privées concernant l'état de santé du patient. Un serveur « métier » recueille des données techniques sur l'état du DM, l'historique de son fonctionnement logiciel et l'évolution des performances. Cela sert de base de données pour un diagnostic technique. Cela n'exclut pas la transmission de données logicielles en direction du DM, en particulier pour les mises à jour de l'application ou des *firmwares.*

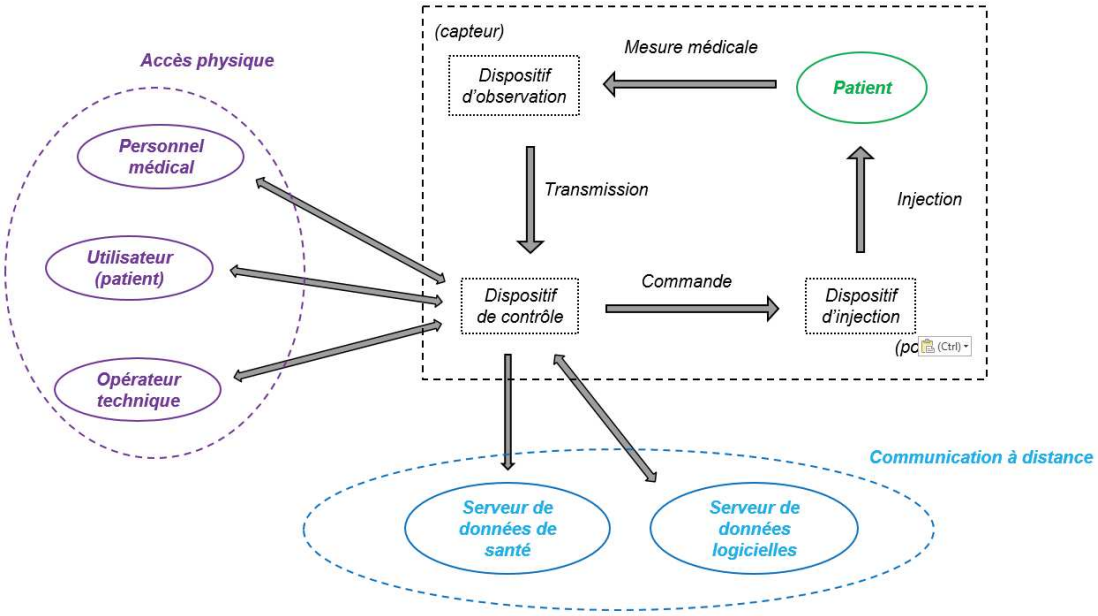

Figure 8: Modèle d'un dispositif pancréas artificiel en phase d'utilisation

2.2.3 Cycle de vie et identification des acteurs.

Nous investiguons les spécificités du cycle de vie d'un tel dispositif médical. Nous nous inspirons des présentations fournies par la fédération française des diabétiques. La Figure 9 résume les phases de déploiement et d'utilisation de ce DM [29]. Il s'agit là uniquement du schéma « post-production », de l'étape de distribution du DM qui déjà conçus et fonctionnel jusqu'à sa fin de vie. La phase d'utilisation inclut plusieurs opérations et situations typiques des DMs.

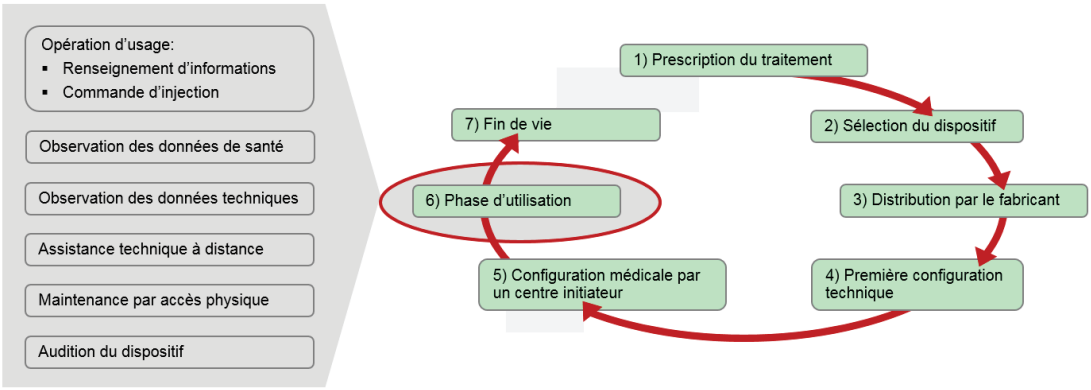

Figure 9: Cycle de vie « post-production » d'une pompe à insuline

Plusieurs acteurs interviennent au cours de cette partie du cycle de vie:

- Le docteur référent qui prescrit l'usage d'un dispositif médical et effectue un suivi médical du traitement par une observation des données de santé
- Le centre initiateur qui sélectionne avec le patient le dispositif et réalise la configuration « médicale » : paramétrage du traitement médical, formation du patient et test du dispositif

- Le fabricant légal, ou OEM, responsable de plusieurs opérations : la distribution du DM, la première configuration technique, les assistances techniques à distance, les maintenances logicielles ou matérielles et également la fin de vie.
- Le patient qui communique au cours du cycle de vie avec tous les acteurs précédents et qui interagit avec le DM.

La **Figure** 10 inclut ces acteurs dans le cycle de vie, ainsi que des opérations supplémentaires : le centre initiateur peut réaliser des audits annuels du DM, et rectifier le paramétrage du dispositif. Il faut également considérer la possibilité de procédures de recyclage au cours de la fin de vie.

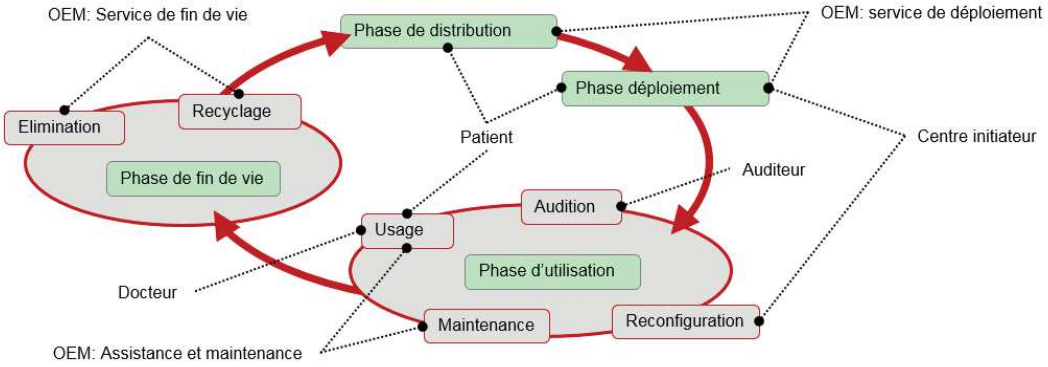

Figure 10: Acteurs au cours du cycle de vie « post-production »

Nous intégrons ensuite dans le cycle de vie les phases de fabrication du DM qui comportent notamment les intégrations logicielles, l'assemblage de composants et les premières étapes de fonderies des puces électroniques tels que préalablement étudiées au cours de l'Introduction du mémoire ; notamment dans les sections 1.1.1 et 1.1.2. La Figure 11 décrit ces étapes qui impliquent les concepteurs, les sous-traitants fabricants, mais aussi les tierces parties qui auditent les systèmes en sortie de la chaine de fabrication. La Figure inclue aussi les éléments provenant de tierces parties et intégrés dans le système : IP (sous-circuits spécifiques, firmware MCU), matériels (batterie, capteur…), logiciels (module de communication). L'assemblage des composants forme notre dispositif médical final, qui par la suite entre dans la phase de déploiement et d'exploitation décrite précédemment. La table 1 liste en outre l'intégralité des acteurs et des opérations notables du cycle de vie du DM.

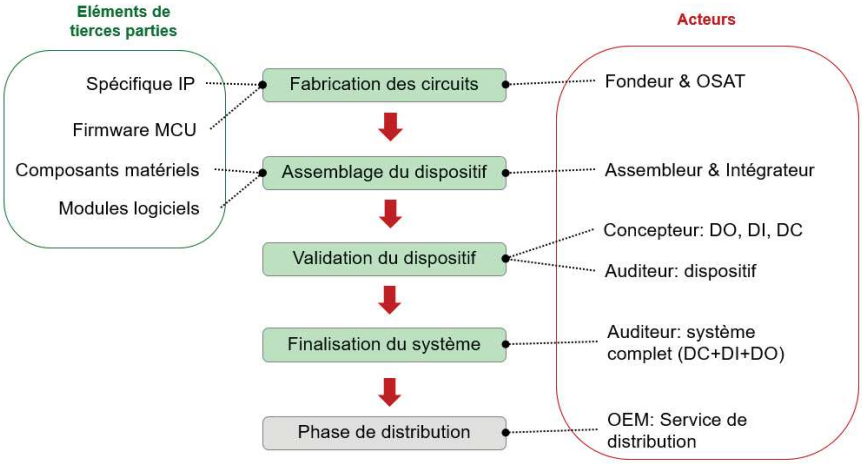

Figure 11: Acteurs et éléments étrangers au cours de la fabrication du DM

Tableau 1 : Acteurs impliqués dans le cycle de vie du DM

Cycle de vie		***Acteurs concernés***
Phase de fabrication	Fabrication des composants matériels	▪ Concepteur des dispositifs (OCM) ▪ Sous-traitants o Fondeur o OSAT
	Assemblage des composants matériels	▪ Sous-traitant assembleur, type EMS o Fournisseur de PCB o Assembleur de composant sur PCB o Testeur PCB
	Intégration logiciels	▪ Intégrateur système
	Audit pour certification	▪ Auditeur agrégé
Phase de déploiement	Distribution et configuration technique	▪ Patient ▪ OEM o Service de distribution o Service d'assistance « démarrage »
	Paramétrage du traitement	▪ Patient ▪ Center initiateur o Médecin o Technicien
Phase d'exploitation	Usage courant	▪ Patient ▪ Docteur ▪ OEM o Service d'observation o Service d'assistance technique
	Intervention : audit, reconfiguration, maintenance	▪ Centre initiateur ▪ Auditeur : Organisme Notifié (ON) ▪ OEM o Service de maintenance o Service d'assistance technique à distance o Service de mise à jour logicielle o Service d'observation (dossier post-marché)
Phase de fin de vie	Recyclage et élimination	▪ Patient ▪ OEM o Service de recyclage o Service d'élimination

2.2.4 Caractéristiques détaillées des composants de l'architecture et des communications

Au cours du cycle nous devons considérer l'ensemble du système qui comporte trois sous-dispositifs (tels que décrits dans la Figure 7 en section 2.2.4) : le dispositif d'observation en continu (DO), le dispositif d'injection (DI) et le dispositif de contrôle (DC). Chacun d'eux présentent des architectures matérielles et logicielles différentes. La plus complexe est celle du dispositif de contrôle, qualifié de « smartphone » dédié au médical. La composition des architectures varie selon les constructeurs et les fournisseurs des pièces internes. L'article [30] décrit un exemple de pompe à insuline (architecture matérielle et fonctions logicielles requises) et [31] réalise un état de l'art des capteurs. Nous listons dans la table suivante les éléments principaux chargés des fonctions de traitement ou de communication.

Tableau 2: Composants matériels et logiciels du dispositif médical

	Eléments matériels	*Eléments logiciels*
Dispositif d'observation (DO)	▪ Capteur ▪ Transmetteur ▪ Microcontrôleur (MCU*) ▪ Unité mémoire ▪ Batterie	▪ Micrologiciel du MCU ▪ Module de communication ▪ Module de gestion des mesures
Dispositif d'injection (DI)	▪ Réservoir de médicament ▪ Actionneur (type turbine) ▪ Transmetteur ▪ Unité mémoire ▪ Microcontrôleur (MCU) ▪ Batterie	▪ Firmware du MCU ▪ Module de communication ▪ Module de contrôle de la pompe
Dispositif de contrôle (DC)	▪ Système sur puce o Microprocesseur o Bloc de port entrée / sortie - USB, SPI, UART o Circuiterie JTAG o Unité mémoire - ROM, Flash o Superviseur de batterie - Watchdog ▪ Batterie ▪ Interface physique o Clavier o Ecran ▪ Transmetteur ▪ Alarme o Haut-parleur o Vibreur	▪ Système d'exploitation ▪ Firmware du système sur puce ▪ Modules de communication o Capteur o Pompe o Serveurs o Interface physique ▪ Modules de traitement o Fonctions médicales o Collecte et stockage de données ▪ Module de contrôle ▪ Module de sûreté

*MCU : Microcontroller unit.

Le système se caractérise aussi par des communications de diverses natures et impliquant des entités différentes. Nous identifions trois catégories : les communications inter-dispositifs, la communication par accès physique (via les interfaces clavier ou écran), les communications à distances avec les serveurs. Une quatrième catégorie potentielle : interaction à distance avec des tierces parties spécifiques (assistance technique, médecin…). Nous décrivons les éléments concernés, la nature des données et les usages associés à ces différents échanges.

Communication interne entre les dispositifs du système *:* Le système régule l'état du patient en s'appuyant sur une boucle de contrôle : le capteur mesure les valeurs physiologiques, et la pompe reçoit les ordres d'injection. Généralement cela s'appuie sur des technologies sans-fil telle que le Bluetooth ; le Wi-Fi ou encore 6LoWPAN. Cela concerne les modules de communication RF listés dans 2.2.2**.** Chaque échange peut inclure des acquittements, comportant alors des transmissions bidirectionnelles.

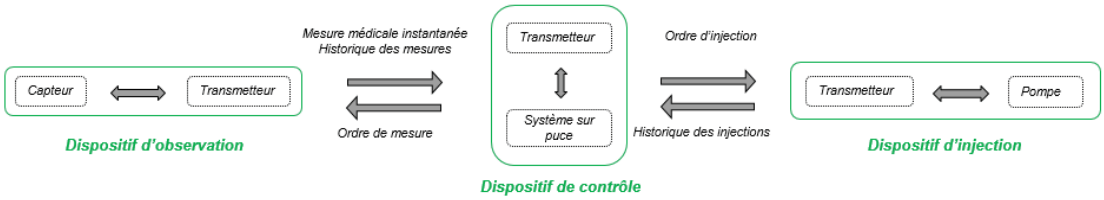

Figure 12: Communication inter-dispositifs

Communication externe avec les serveurs *:* Le dispositif de contrôle échange deux catégories de données. Il transmet des informations médicales sur le patient à un serveur agrégé pour l'hébergement de données de santé. Nous supposons cette communication restreinte en sens sortant. Une deuxième communication concerne les données dites « métiers » : envoie des informations techniques, ou de performances au serveur du fabricant. Ces échanges utilisent le protocole IP implémenté dans le module de communication du DC. Des composants matériels (carte Wi-Fi) peuvent être intégrés pour permettre la communication sans-fil.

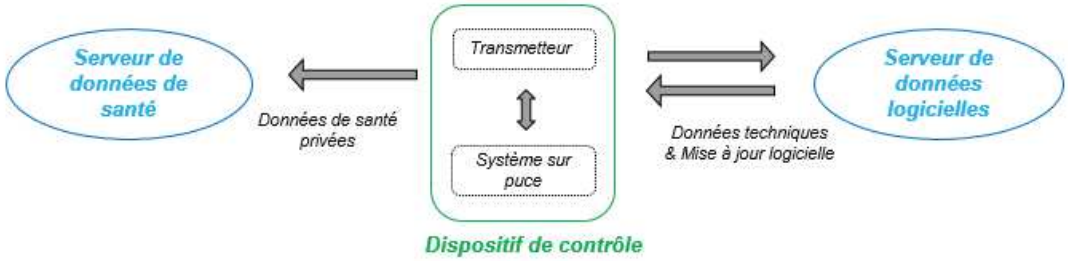

Figure 13: : Communication avec les serveurs externes

Communication par accès physique direct : Interaction entre les utilisateurs (patient, médecin ou installateur) et le dispositif par les interfaces physiques : écran, clavier. Cela concerne la configuration de la pompe, la définition du profil du patient et aussi des opérations quotidiennes telles que le renseignement d'événements particuliers, modification du dosage…

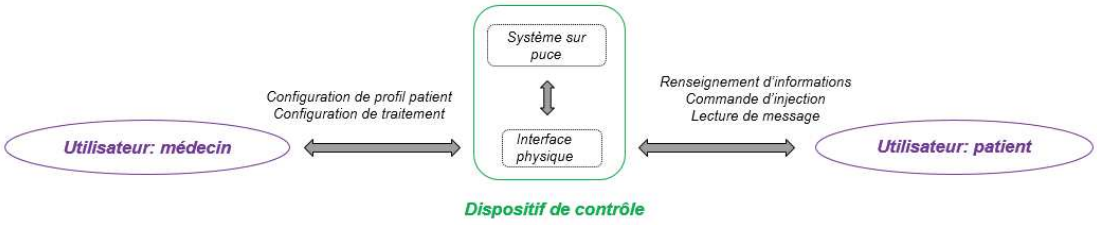

Figure 14: Communication par les interfaces physiques

2.2.5 Caractéristiques des fonctions de sûreté

Les fabricants de DMs doivent assurer la sécurité du patient, leurs produits sont soumis à des exigences de sécurité « au sens sûreté » : protéger le système des événements accidentel et des mésusages non intentionnels, et ce tout au long du cycle de vie. Les dispositifs médicaux à forte criticité

embarquent des mécanismes pour la sûreté de leur fonctionnement, tels que décrits dans [26] ou [30]. Nous listons les problématiques qui concernent notre cas d'étude.

- ***Disponibilité et intégrité matérielle*:** Les dispositifs contiennent des éléments qui surveillent les niveaux d'énergie des batteries et le réservoir de médicament. Ces capteurs ou circuits supplémentaires transmettent les informations au module de sûreté principal. Une fonction logicielle déclenche des alertes en cas de dépassement de seuil critique.
- ***Disponibilité et intégrité logicielle des processeurs*:** Le système possède des fonctions d'observation de l'occupation mémoire et de la charge de calcul. Elles transmettent au module de sûreté l'état de ces composants.
- ***Disponibilité et intégrité des communications* :** Les modules de communications inter-dispositifs implémentent des vérifications d'intégrité des messages échangés, notamment par « checksum » (somme des trames de données d'un protocole, cela permet de détecter les erreurs). Le module de communication du dispositif de contrôle surveille également la perte de connexion.
- ***Intégrité du traitement médical :*** Plusieurs fonctions renforce l'intégrité des actions. Des demandes de confirmation pour le renseignement d'informations, les configurations et les ordres d'injections. La pompe embarque une fonction logicielle qui enregistre dans une unité mémoire l'historique des injections. Le module de sûreté vérifie régulièrement l'historique et émet des avertissements si les doses ne correspondent pas.
- ***Procédure d'avertissement utilisateur*** : Le DM embarque des alarmes sonores et vibrantes. Le module de sûreté, en cas de détection d'état ou de réception d'information qui témoigne d'une perte de disponibilité ou d'intégrité des fonctions essentielles, active les alarmes et transmet également des notifications par l'interface physique.

Les fonctions de sûreté décrites précédemment apportent des propriétés requises pour les exigences de sécurité : disponibilité et intégrité du système. Cela reste toutefois à un niveau limité, ces protections ne prenant pas en compte les menaces criminelles, et par ailleurs les deux autres propriétés de sécurité courantes, confidentialité et authentification, ne s'obtiennent pas avec ces fonctions. Il faut noter pour certains dispositifs l'absence de fonctions de sécurité assurant ces propriétés. Dans l'article [8] les auteurs démontrent la vulnérabilité d'une pompe à insuline au niveau des communications sans-fil, tant pour la confidentialité que pour l'authentification.

2.2.6 Interactions entre les acteurs et les biens du dispositif.

Nous qualifions de « biens » les éléments qui composent l'objet et qui sont essentiels au regard de son fonctionnement ou de sa sécurité. Cela peut-être des informations sensibles telles que les mots de passe, mais également des modules logiciels embarqués ou des composants matériels qui assurent les fonctions de base du traitement médical. Le cycle de vie des DMs induit des interactions entre les biens du DM et les différents acteurs. Outre les opérations techniques couramment effectuées dans le cas de la production et du déploiement d'un objet IoT (tel que listées dans l'introduction, section 1.1.1) diverses interactions caractérisent un DM. Elles impliquent des contraintes et des besoins spécifiques. En vue du marquage CE le fabricant est soumis aux contraintes du règlement [16], présentées dans la section 2.1.2. Elles comportent des auditions, ou des contrôles internes du fabricant. Cela implique des tests en sortie de production, avec accès physique au DM, qui peuvent être séparés ou regroupés :

- Tests de fonctionnalités pour exécuter les fonctions du DM et vérifier le respect des spécifications fonctionnelles définies.
- Tests de performances qui relèvent les données techniques relatives aux performances (vitesse, précision, consommation…)
- Test de sûreté qui évalue le module de sûreté du DM et vérifie son comportement face à des situations de défaillances.

Tableau 3 : Description des accès au cours du cycle de vie du DM

Cycle de vie	*Acteurs*	*Biens essentiels*	*Nature et contraintes des accès*
Phase de fabrication			
Fabrication des puces	Fondeur	IP des concepteurs Circuit (MCU / SoC)	Exploitation des masques et des IPs pour les processus de fabrication Tests de production
Encapsulation des puces	OSAT	Circuit (MCU / SoC)	Tests fonctionnels Accès à des données techniques et des interfaces spécifiques pour les tests
Assemblage des PCB	Assembleur	Circuit (MCU / SoC) Composants matériel	Manipulation des composants pour l'assemblage sur PCB Tests d'assemblage
Intégration logicielle	Intégrateur	PCB du dispositif Modules logiciels	Accès à des éléments logiciels Accès aux interfaces de programmation Vérification fonctionnelle du dispositif
Finalisation	Préparateur	Dispositifs assemblés	Empaquetage des dispositifs Distribution à l'OEM
Audit pour certification	Auditeur	Dispositifs complets	Exécution des fonctions logicielles Lecture des données techniques
Phase de déploiement			
Distribution	OEM : Service de distribution	Dispositifs complets	Accès physique pour le transport, pas d'interaction spécifique,
Initialisation	OEM : Service d'assistance pour le démarrage	Données techniques	Lecture des données techniques
	Patient	Interface physique du DM	Démarrage et test de fonctionnement Exécution des fonctions d'appareillage et d'initialisation
Paramétrage du traitement	Centre initiateur	Interface physique du DM Données de santé privées Données de paramétrage	Exécution des fonctions médicales Lecture et modification de paramètres techniques et médicaux

Phase d'exploitation			
Usage courant	Patient	Interface physique Données de santé privées Données de paramétrage	Opération d'usage Lecture des messages techniques Lecture des données de santé
Suivi médical	Docteur	Données de santé privées	Accès à distance Lecture uniquement
Suivi technique	OEM : Service d'assistance technique	Données techniques « métier »	Accès à distance
Mise à jour	OEM : Service de développement logiciel	Modules logiciels	Développement et déploiement d'une mise à jour logicielle à distance
Maintenance	OEM : Service de maintenance	Dispositifs complets Modules logiciels Données de paramétrage	Accès physique spécifique Exécution des protocoles d'appareillage
Reconfiguration	Centre initiateur	Interface physique du DM Données de santé privées Données de paramétrage	Exécution des fonctions médicales Lecture et modification de paramètres techniques et médicaux
Audit pour révision	Auditeur	Interface physique du DM	Exécution des fonctions Lecture des données techniques
Phase de fin de vie			
Retour du DM	Patient	Dispositif Données de santé	Renvoi du DM Effacement des données privées
Recyclage	OEM : Service de recyclage	Composants matériels	Diagnostic de l'état des composants Extraction des composants réutilisables
Elimination	OEM : Service d'élimination	Composants matériels et logiciels	Procédure de destruction des composants

Par la suite la phase de déploiement nécessite une mise en communication entre les différentes entités et les acteurs, ainsi que des opérations techniques pour l'initialisation et le paramétrage du DM : exécution d'un protocole d'appareillage entre les dispositifs du système, établissement de communication avec les serveurs externes, paramétrage du profil du patient et de son traitement. Au cours de l'exploitation plusieurs interactions ont lieu, entre autres les communications décrites dans la section 2.2.2. Des interventions au niveau logiciel ou matériel peuvent avoir lieu : des mises à jour de l'application logicielle, préventives ou correctives, nécessitant une réception sécurisée et fiable des données externes ; des maintenances matérielles, exigeant un accès physique au DM et éventuellement

un redéploiement et une reconfiguration du système. Le personnel médical (médecin référent ou technicien du centre initiateur) peut aussi interagir, et requiert des accès à des fonctions ou des données du dispositif. Des audits annuels sont à prévoir, impliquant des opérations similaires à celles décrites en section 2.1.2.

Les interactions décrites impliquent des accès, par divers acteurs et tiers composants, à des fonctions et des données du DM. Nous présentons dans la table 3 les acteurs qui doivent être authentifiés, les biens avec lesquels ils interagissent, et la nature et les contraintes de ces interactions. Certaines des étapes induisent des accès physiques au DM et aux biens qui sont conçus et/ou intégrés au cours de ces étapes. La nature des accès peut varier : interface de débogage, interface de programmation, interface physique (écran, clavier…).

2.2.7 Gestion et sécurité des accès au DM

Au cours de ces opérations des tierces parties accèdent aux biens du DM et cela impose leur authentification pour sécuriser ces biens. Cela est aussi réciproque : l'authentification des biens est requise également dans certains cas (assurance de l'origine des composants matériels, des mises à jours logicielles, des dispositifs…). La gestion des droits d'accès et des authentifications apparaît complexe: la précédente étude montre que les accès sont de natures diverses selon les phases du cycle de vie, et n'impliquent pas les mêmes biens. Plusieurs problématiques de sécurité sont établies :

- ***Interventions des sous-traitants et intégration de tiers composants :*** La phase de fabrication des circuits et d'assemblages des dispositifs est segmentée, différents fournisseurs ou sous-traitants prennent en charge certaines opérations techniques. Cela induit des interactions multiples et variables. Un ensemble de normes strictes – contrôle et auditions – permet, à défaut de sécuriser les interactions, d'assurer un certain niveau de confiance dans le fonctionnement et les performances des DMs. Des règles de contrôles d'accès peuvent être déployées au cours de cette phase : la mise en œuvre est complexe du fait des nombreuses exigences d'accès. Cela concerne les composants matériels du dispositif, ainsi que les éléments logiciels.
- ***Exécution des protocoles de déploiement et d'appareillage :*** Au cours du déploiement des données sensibles sont concernées : les identifiants des dispositifs et des acteurs (patients, docteurs…), les données de paramétrage du DM**.** Le service du fabricant doit établir et gérer les différents niveaux d'autorisations, et assurer en outre l'initialisation du DM. Cela concerne les données de paramétrage du système, ainsi que des éléments de sécurité (mot de passe, identifiants…).
- ***Authentification des utilisateurs et tierces parties au cours de la phase d'exploitation :*** Généralement les dispositifs médicaux embarquent une fonction pour des règles de droits d'accès utilisateurs et administrateurs. Le module de contrôle exécute un protocole d'authentification, et selon le communicant (patient, médecin…) autorise des accès de différents niveaux à des fonctions ou des données du système. Cela se couple avec une base de mots de passe. Cela sécurise dans un premier temps les modifications du traitement médical ainsi que la lecture de données sensibles (historique médical ou données d'exploitation technique du système). Le système présente une gestion des autorisations complexe : utilisateur, docteur, technicien, ou auditeur n'ont pas les mêmes besoins d'accès. Certains interagissent par l'interface physique, et d'autre par des accès à distance. Dans le cadre d'un dispositif médical se pose notamment la contrainte de collecter, stocker et retourner les historiques d'activités (mesure médicale, ordre d'injection...) Une dernière contrainte concerne la nécessité d'un suivi technique et le déploiement de mises à jour logicielles. Cela implique des données sensibles ainsi qu'un accès à distance aux modules logiciels du DM.
- ***Gestion de la fin de vie de l'objet :*** La fin de vie nécessite des procédures pour l'effacement des données utilisateurs (données de santé privé, mot de passe…), et le recyclage est possible sous réserve d'un contrôle adéquat. Le fabricant du dispositif pouvant diagnostiquer l'état des différents composants, et les réutiliser pour un autre usage ; potentiellement le DM en intégralité. Il faut alors assurer la suppression des données privées, et tracer le dispositif et ses composants.

Ce cas d'étude montre la complexité du cycle de vie et l'exposition des biens au cours des différentes phases. Des interactions de diverses natures sont nécessaires pour produire et exploiter le dispositif. Celui-ci présente en plus de nombreux points d'entrées vulnérables. La fabrication comporte des opérations sous-traitées, réalisées par de tierces parties, qui nécessitent des accès physiques aux composants. Ces accès peuvent être détournés de leur usage, ou bien réutiliser par des acteurs non autorisés. Il faut aussi considérer l'intégration d'éléments matériels et logiciels de tierces parties, ayant des interactions fortes avec les biens du DM. Cela pose des exigences d'authentifications pour protéger le DM mais aussi les tiers éléments (dont les propriétaires peuvent également définir des exigences de sécurité). L'utilisation du DM implique des informations sensibles, et des communications avec plusieurs acteurs. Les contraintes réglementaires imposent des exigences de sécurité pour ces échanges mais aussi un suivi, et donc une disponibilité, de certaines données. Au cours de cette exploitation les biens du DM – données, composants matériels, logiciels – peuvent être compromis via des accès physiques vulnérables, une authentification mal assurée ou une communication non sécurisée.

Un premier bilan souligne l'exposition des biens face aux situations suivantes :

- Détournement des accès par des tiers partis au cours de leur intervention, soit non sécurisation de la gestion des droits d'accès.
- Utilisation des accès par des acteurs extérieurs, soit non sécurisation des accès.
- Compromission des communications non sécurisées.
- Usurpation d'un acteur, ou d'un tiers composant pour interagir avec les biens.

Cela peut survenir à divers moments du cycle de vie et nous craignons des scénarios d'attaques qui se déroulent sur plusieurs phases. Cela rend d'autant plus complexe l'évaluation et la sécurisation du DM, ainsi que l'établissement de la responsabilité des divers acteurs.

2.3 Bilan de l'analyse de risques

2.3.1 Synthèse des modules de l'analyse EBIOS

L'intégralité de l'analyse de risque est inclut en annexe 10.2. Nous synthétisons dans cette section les trois premiers modules : l'établissement des biens essentiels du DM et des propriétés de sécurité qui doivent être assurées (module 1), l'estimation des évènements les plus redoutés (module 2) et l'étude des scénarios de menaces les plus crédibles (module 3).

Module 1 – étude de contexte : Les quatre propriétés de sécurité retenues sont : confidentialité, intégrité, disponibilité et authenticité. Nous considérons comme biens essentiels l'ensemble des éléments du DM qui se présentent au cours du cycle de vie et pour lesquels une compromission impacte le fonctionnement du dispositif ou les acteurs associés. Nous nous appuyons sur les descriptifs du DM réalisés dans la section précédente. Tous les biens essentiels requièrent par défaut une exigence maximale pour l'intégrité, la disponibilité et l'authenticité (respectivement – intégrité complète – disponibilité permanente – authenticité assurée). Seule la confidentialité varie selon les restrictions d'accès exigés ; nous constatons déjà des besoins : les acteurs n'ont pas les même droits d'accès aux éléments du système. Il apparaît nécessaire de disposer de mécanismes d'authentification pour les acteurs et ce dès le début du cycle de vie du DM.

Module 2 – évènements redoutés : Nous décrivons dans ce module les événements redoutés en cas de perte de telle ou telle propriété pour les biens essentiels. Nous évaluons l'impact sur plusieurs axes : santé du patient et conséquences pour le fabricant. Cette échelle est subjective et dépends du contexte précis dans lequel s'inscrit l'analyse : cadre réglementaire, objectifs et besoins du fabricant, conscience des acteurs vis-à-vis de la sécurité. Le *Medical Device Privacy Consortium* [32] a réalisé un rapport sur l'étude de sécurité des DMs. Il est fourni dans ses annexes un exemple précis et détaillé d'une échelle d'impact, présentée une fois par niveau de gravité, une fois par propriété de sécurité. La table 4 s'inspire de cette étude et résume les différents niveaux d'impact. Outre les conséquences sur les patients, une

appréciation est également fournie pour celles qui concernent le fabricant (en terme de sanction judiciaire ou de perte économique). Nous classons les événements redoutés pour le patient selon le danger pour son état de santé.

Tableau 4: Echelle du niveau d'impact des événement redoutés

Impact de l'événement	1 : faible	2 : sérieux	3 : critique	4 : catastrophique
Patient	Faible impact sur la santé du patient, presque négligeable Vol de données privées faiblement exploitable	Dégradation de la santé du patient mais guérison possible Vol de données privées partiel (une partie seulement des données médicales, mot de passe)	Mise en danger du patient Vol de données privées important (historique complet, mot de passe et clef de chiffrement)	Mort du patient : cela est probable en cas de surdosage élevé du médicament
Fabricant OEM	Faible coût d'intervention Contraintes légales et commerciales faiblement impactées	Perte de 1 à 5% du chiffre d'affaire Contraintes légales et commerciales renforcées	Perte de 5 à 20% du chiffre d'affaire Contraintes légales et commerciales fortement renforcées. Impact sur plusieurs années.	Fermeture de l'entreprise Poursuite judiciaire

Par la suite nous relevons le niveau d'impact dans le cas de la compromission d'un bien ; les tables fournies dans l'annexe résument ces craintes. Nous y présentons les biens ciblés en quatre catégories, une pour chaque sous-dispositif du système (pompe, capteur et dispositif de contrôle), et une dernière pour les biens spécifiques aux mesures de sécurité et sûreté. Nous fournissons une brève justification de notre appréciation pour chaque évènement redouté.

Module 3 – Scénarios de menaces : La recherche de scénarios de menaces est complexe : la surface d'attaque est importante et les scénarios doivent être cotés en termes de vraisemblance. Nous définissons quatre niveaux de vraisemblance : **1 – faible, 2 – moyenne, 3 – forte, 4 – certaine**. Plusieurs catégories d'attaques sont identifiées dans le guide EBIOS [24] ; les plus pertinentes pour l'analyse de risques du DM sont notamment les attaques matérielles, les menaces contre les communications (interception ou malversation des échanges entre le DM et des tiers parties) et les exploitations de failles logicielles. Ces menaces sont nombreuses et diverses, l'annexe résume les scénarios les plus critiques. Afin d'apprécier plus finement la nature et la vraisemblance des menace nous classons les scénarios en fonction des modèles d'adversaires listés dans la section 1.2.2 :

- A distance et sans privilèges, qui possède seulement des droits utilisateurs restreints.
- A distance et avec privilèges qui a des accès au système d'exploitation à distance.
- A distance, avec privilèges et accès aux canaux auxiliaires.
- Avec un accès physique limité qui utilise des équipements basiques (et peu cher).
- Avec accès physique et capacité avancée, qui dispose d'équipements de rétro-ingénierie.
- Hautement intrusif qui compromet le SoC par l'intégration de composants malveillants.

2.3.2 Bilan du module 4 : évaluation des risques significatifs

Le « risque » est un événement redouté (perte de propriété de sécurité d'un bien du dispositif) qui se réalise suite à un scénario de menace. Plus le scénario est vraisemblable et l'événement impactant, plus le risque est significatif. Cette pertinence s'obtient ainsi par croisement des niveaux d'impact et de vraisemblance déterminés au cours des modules 2 et 3. Il faut toutefois noter que les niveaux de gravité et de crédibilité qui détermine un niveau de risque sont arbitraires. L'évaluateur a la charge de définir dans l'évaluation des risques la signification de ceux-ci par rapport aux objectifs de sécurité. Nous synthétisons dans le tableau 5 la pertinence des risques identifiés selon cinq niveaux de signification : **0 – négligeable, 1 – faible, 2 – moyen, 3 – fort, 4 – critique, 5 – hautement critique**.

Tableau 5: Evaluation des risques significatifs

Gravité \ Vraisemblance	1 : Faible	2 : Moyenne	3 : Forte	4 - Certaine
1 : Faible			Interception de données de mesure ou injection par écoute passive.	
2 : Sérieux			Interception des historiques médicaux des DO et DI.	
3 : Critique	Perte d'intégrité et de disponibilité des circuits matériels du capteur par insertion de cheval de Troie. Dévoilement des clés de chiffrement par brute force.	Perte d'intégrité des clés de sécurité par injection de faute semi-invasive	Perte d'intégrité et d'authenticité du capteur par contrefaçon. Perte d'authenticité de la mesure du capteur par injection de faux message. Non-disponibilité du capteur ou de la pompe par déni de service. Dévoilement des données de santé par abus des droits d'accès. Perte d'intégrité des données de paramétrage par abus des droits d'accès.	Dévoilement des données de santé par intrusion via interface de débogage. Perte d'intégrité des données de paramétrage par intrusion via interface de débogage
4 : Catastrophique	Perte d'intégrité et de disponibilité des circuits de la pompe et du dispositif de contrôle par insertion de cheval de Troie. Dévoilement ou perte d'intégrité des clés de sécurité par injection de faute invasive	Perte de confidentialité des clefs de sécurité par attaques sur les canaux cachés ou par injection de faute semi-invasive Perte d'intégrité des logiciels, confidentialité des données privée ou des clés par une exploitation de vulnérabilité logicielle.	Perte d'intégrité et d'authenticité des circuits du DM par contrefaçon. Perte d'authenticité des commandes d'insuline par injection de faux message. Dévoilement des mots de passe par brute force. Dévoilement des mots de passes et de perte d'intégrité des logiciels et firmwares par non-respect des droits d'accès.	Perte d'intégrité des modules logiciels ; risque de dévoilement des clefs de sécurité par intrusion via interface de débogage Perte de l'authenticité de l'ordre d'injection de la pompe par rejeu.

La synthèse de l'analyse révèle des risques critiques qui doivent être traités pour sécuriser les biens du dispositif médical. Les failles sont de natures diverses : non sécurisation de l'accès physique (risques liés à des intrusions via les interfaces de débogage) qui est exploitée pour accéder à des biens, défauts dans l'authentification des composants électroniques (contrefaçons), manque de sécurisation des communications, mauvaise gestion des droits d'accès.

Les attaques matérielles les plus craintes sont celles mises en œuvre par des adversaires limités ou moyennement équipés ; les attaques hautement intrusives réalisées par des adversaires ayant de fortes ressources sont moins vraisemblables. Les attaques à distance qui doivent être considérées sont celles

concernant la compromission des communications non-sécurisées, ainsi que les attaques exploitant des faiblesses dans la gestion des droits d'accès (mot de passe ou clef d'authentification mal-sécurisé, niveau d'autorisation mal défini).

Au vue de ces risques identifiés nous pouvons établir des exigences de sécurité, celles-ci peuvent être complémentaires, mais peuvent également générer de nouvelles problématiques :

- Etablir des protocoles de sécurité pour authentifier les acteurs et le dispositif au cours des communications, assurer l'intégrité des messages et chiffrer les données.
    - Cela implique l'utilisation de clefs de sécurité (clef cryptographique pour le chiffrement, signature pour authentification).
- Intégrer une solution de sécurité qui assure l'authenticité des composants du dispositif et des acteurs face aux scénarios d'attaques matérielles (contrefaçons et intrusion physique).
    - Idéalement, cette solution est embarquée dans le circuit du dispositif et permet de prouver l'authenticité du circuit et des acteurs au cours du cycle de vie.
    - Cela suppose, à priori, une intégration de ce mécanisme dès les premières phases.
- Déployer une politique de sécurité qui distribue et assure les droits d'accès au cours du cycle de vie sans compromettre le dispositif.
    - Cela implique des protocoles d'authentifications sures, ceux-ci pourraient s'appuyer sur les mécanismes qui assure l'authenticité.
    - Cela impose aussi une flexibilité, répudier ou ouvrir des accès au cours du cycle de vie.

Ces exigences imposent la mise en œuvre d'une solution de génération, stockage et gestion de clefs de sécurité (chiffrement et / ou authentification). Cela nécessite l'exploitation d'une source d'aléa sûre, ou d'une fonction de génération, qui respecte les propriétés de sécurité (notamment en termes d'aléa, de niveau d'entropie et de non-prédictibilité) ; et qui par ailleurs résiste aux attaques matérielles.

2.3.3 Bilan général sur l'analyse de risques et les exigences de sécurité identifiées

Des solutions adéquates existent pour sécuriser les communications, la publication [8] présente des solutions cryptographique pour une pompe à insuline connectée et évalue l'impact sur le système en termes de performances. L'analyse détaille le coût additionnel pour la mise en œuvre d'une chiffrement AES et d'un protocole MAC pour assurer la confidentialité et l'authenticité des échanges. Ces protocoles de sécurité sont une brique essentielle pour atténuer les risques menaçant les communications et la confidentialité des données du dispositif médical. En outre, ces protocoles sont définis par des normes strictes qui respectent des critères de sécurité. Cela nous assure de la justesse de leur efficience. De fait, cela nécessite une solution pour la gestion des clefs de chiffrement et d'authentification ; il faut un mécanisme pour générer et stocker les clefs, mais également la répudiation des clefs au cours du cycle de vie : cela peut subvenir en cas de changement d'opérateur médical, d'utilisateur, ou d'intervention ponctuelle par un auditeur.

Des contremesures supplémentaires sont toutefois requises pour les autres exigences du cycle de vie : la gestion sûre des clefs de sécurité, une solution d'authentification pour les acteurs du cycle de vie et la protection contre les attaques dites « matérielles ». Certaines des solutions énumérées en introduction dans la section 1.3 répondent à ces besoins. Ces contremesures sont contraignantes, et n'offrent parfois qu'une assurance limitée au regard des besoins de sécurité que nous avons ciblés. Entre autre, les tests et inspections contre la contrefaçon sont lourds et couteux, et n'assurent seulement que l'authenticité du matériel. L'offuscation de design et le marquage de filigrane se limitent à la sécurité d'une IP, tandis que les contremesures pour les attaques par canaux cachés ne protègent que les clefs de sécurité. L'intégration de toutes ces protections sécurisent le cycle de vie mais cela à un surcoût tant financier qu'en termes de performances. Cela compromettrait le développement et la commercialisation d'un dispositif médical : cette application concerne des utilisateurs ou services qui peuvent être limités

en capacité de production et d'achat, et de plus les contraintes réglementaires imposent un niveau de performance minimum.

Généralement chaque contremesure apporte l'assurance d'une ou deux propriétés de sécurité, sans répondre à tous les besoins de sécurité du cycle de vie, et sans offrir non plus une flexibilité en terme de gestion des droits d'accès. Il nous faut investiguer une solution qui couvre plus globalement ces exigences de sécurité. La multiplicité des acteurs et des interactions au cours du cycle impose de disposer d'une solution efficace qui permette de générer, répudier et manipuler des paramètres de sécurité pour gérer les accès aux atouts du dispositif, et ce tout en ayant une certaine résistence aux attaques matérielles.

Parmi les solutions, les PUFs *(Physical Unclonable Function)* peuvent potentiellement répondre à l'ensemble des exigences de sécurité : elles assurent l'authenticité du matériel par leurs propriétés, elles sont sources d'aléa pour générer des clefs de chiffrement ou des signatures d'authentification, et elles peuvent être intégrées en amont du cycle de vie. Les propositions plus spécifiques pour la sécurité du cycle de vie, en section 1.3.2, s'appuient notamment sur des primitives PUFs. Des architectures complètes sont détaillées, intégrant des protocoles d'authentification pour le cycle de vie. Ces solutions assurent les propriétés d'authentifications et permettent une gestion sure des droits d'accès aux circuits.

Dans ce contexte nous voyons un intérêt fort à rechercher des briques matérielles de sécurité type PUF, à la fois efficaces et souples en termes de compromis**.** La suite des recherches se focalise sur la conception de primitives de sécurité PUF capable de répondre aux besoins d'authentification, et d'efficience induit par le cycle de vie. La primitive servira de socle pour des fonctions de sécurité protégeant les interactions entre les acteurs et les biens du dispositif au cours du cycle de vie ; offrant une gestion sûre des droits d'accès aux biens du système.

Le PUF apportera une assurance pour les exigences de sécurité identifiées par l'analyse EBIOS : l'authenticité du matériel, la gestion sûre des clefs de sécurité (génération, stockage et répudiation) et l'atténuation des risques face aux menaces matérielles les plus vraisemblables.

3 Etat de l'art sur les Fonctions Physiques Nonclonables

PUF is an expression of an inherent and unclonable instance-specific feature of a physical object.

Roel Maes

Le terme *Physical(ly) Unclonable Function* (PUF), fonction physique(ment) nonclonable, apparait au début de notre millénaire. Nombreuses sont les définitions, les propositions et les critiques des PUFs dans la littérature. Roel Maes [33], chercheur en sécurité matérielle, définit une PUF comme l'instance d'une fonction d'un objet physique ; instance inhérente et spécifique audit objet, et physiquement non-clonable. Dans les cas où l'objet est un circuit intégré, la conception du PUF repose généralement sur un paramètre électrique ou analogique. Au cours de la fabrication, un aléa imprédictible et non-maitrisable produit des variations distinctes de circuit en circuit et mesurables. Les mesures du paramètre par le PUF, uniques et spécifiques à chaque instance du circuit, sont utilisées pour générer des signatures uniques. Cela mène aux applications suivantes : identification des circuits, protocoles d'authentification, génération et stockage de clefs cryptographiques.

La première section introduit le concept général et les premiers modèles de PUFs traditionnelles. Nous rappelons dans un premier temps les origines et le concept de la sécurité basée sur le désordre physique. Nous formalisons les aspects importants de la conception des PUFs et nous établissons via des références de l'état de l'art les critères de classification des PUFs. Nous présentons deux architectures, l'Arbiter PUF et le SRAM-PUF, qui illustrent les classes *weak PUF* et *strong PUF.*

La deuxième section détaille les critères d'évaluations et caractérisation des PUFs. Deux propriétés sont déterminantes, l'unicité et la reproductibilité : le modèle PUF implémenté doit permettre de distinguer avec certitude un PUF d'un autre (unicité) et le comportement du PUF doit être stable au cours du cycle de vie (reproductible). Cette dernière exigence impose des post-traitements pour corriger les éventuelles réponses erronées. La sécurité du PUF repose en outre sur la non-prédictibilité des réponses, une propriété qui peut être requise selon les applications. Afin de juger de l'efficacité des PUFs, nous reformulons l'ensemble des métriques de sécurité et de coût connues dans la littérature.

La troisième section argumente les apports et limites des PUFs pour la sécurité du cycle de vie. Nous abordons le cas du SRAM-PUF pour lequel existent des études détaillées. Le SRAM-PUF fait l'objet d'une industrialisation avancée et certains travaux proposent des schémas pour répondre aux besoins du cycle de vie. Toutefois, les contraintes de robustesse et de sécurité (en particulier la qualité de l'aléa des réponses) limitent les performances et induisent un coût supplémentaire.

La quatrième section introduit les modèles *digital PUFs*, des PUFs fortement robustes. Ces architectures exploitent un paramètre stable, figé après fabrication du circuit : les états ouverts / fermés des nœuds de connexion. Cela nécessite une personnalisation des masques du circuit ou une intervention supplémentaire au cours de la production. Nous formalisions dans cette partie la définition des *digital PUFs,* ainsi que leur classification. Nous exprimons notre motivation pour ce modèle de PUF assurant une haute stabilité des réponses, primordiale pour répondre aux besoins du cycle de vie. Nous terminons par les problématiques de conception, concluant sur l'importance d'étudier une configuration adéquate de ces modèles qui respecter les critères de coût et de sécurité.

La cinquième section présente les *digital PUFs* de la littérature. Pour chacun nous établissons les principes sur lesquels reposent leur conception, les méthodes de fabrication des structures aléatoires et les modèles de circuits d'extraction. Nous présentons aussi tous les résultats existants en termes de sécurité et de coûts de surfaces.

La sixième et dernière section conclut sur les perspectives pour la littérature des *digital PUFs.* Nous établissons des objectifs pour la suite de nos recherches : la conception d'une couche logique (circuit d'extraction) performante permettant de déployer un modèle strong PUF à partir des structures aléatoires. Ce circuit devra respecter les critères de sécurité et de coût établi précédemment.

3.1 Fonctions Physiques Nonclonables Traditionnelles

3.1.1 Introduction sur le désordre physique

Les primitives PUFs font aujourd'hui parties de la littérature scientifique en sécurité matérielle, décrites dans des plusieurs ouvrages de chercheurs du domaine : *Introduction to Hardware Security and Trust* de Mark Tehranipoor et Cliff Wang [34], ou encore *Fundamentals of IP and SoC Security* de Swarup Bhunia, Sandip Ray et Susmita Sur-Kolay [35]. Embarqués dans le circuit, les PUFs exploitent le *désordre physique* de celui-ci pour générer des signatures d'authentification. Le *désordre physique* fut utilisé dès les années 80 pour l'authentification ; un mécanisme physique, présenté Figure 15, permet d'authentifier les équipements militaires lors d'une inspection. Une couche de particules diffusantes, appliquée sur la surface des armes, sert d'empreinte unique et non-falsifiable. Le désordre de ces particules induit une relation unique entre les angles de réflexions des rayons lumineux d'entrée et de sorties, réfléchis sur l'empreinte de l'arme inspectée. Sur la Figure 15, les angles de sorties **y1** et **y2** sont déterminés par les angles d'entrée (**x1, x2**) et les caractéristiques de la couche diffusante. Cela illustre un principe fondamental de la sécurité basée sur le désordre physique, primordial pour les PUFs : l'implémentation dans un « système » (objet, circuit, ou autre…) d'une fonction dont la sortie, mathématiquement, dépend d'une entrée choisie par un acteur externe et du désordre physique dudit système. Ce type de fonction est aussi couramment nommé *mécanisme challenge réponse.*

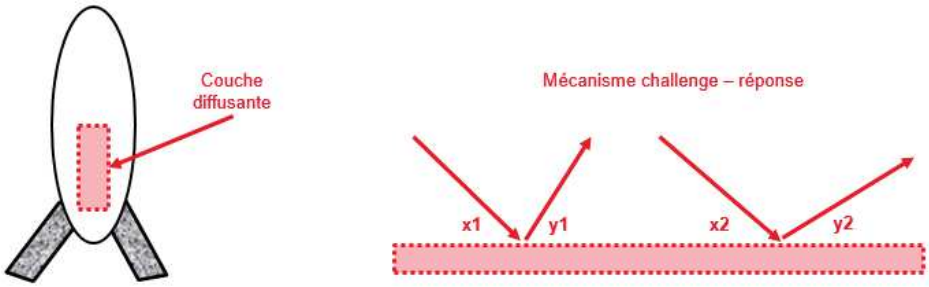

Figure 15: Mécanisme physique pour l'authentification des équipements militaires [34]

Depuis 2000, de nouveaux mécanismes basés sur le désordre physique se développent. En 2001, Pappu [36] implémente une fonction physique à sortie non-réversible *(physical one-way function*). Le mécanisme, similaire à l'exemple précédent, se base sur une couche de diffraction. Les angles en entrée et sortie de la couche forment la paire challenge - réponse de la fonction. En 2002, Gassend [37] propose une fonction physique aléatoire *(physical random function)* pour les circuits intégrés. Une architecture à oscillateurs en anneaux mesure les différences de fréquence dans le circuit. Les écarts, induits par le désordre physique, apportent un aléa non-prédictible. Pour ces deux primitives, la reproduction à l'identique d'une instance est irréalisable, elles sont *physiquement non-clonable*. L'expression *physical unclonable function (PUF)* est adoptée dans la littérature les années suivantes. Les modèles de Pappu et Gassend sont respectivement renommés *Optical PUF* et *Ring-Oscillator PUF (RO-PUF).* Par la suite, de nombreux articles proposent des *silicon PUFs,* des modèles spécifiques aux circuits intégrés. Basel Halak [38] détaille les phénomènes sources de désordre physique dans les circuits intégrés, bases des *silicon PUFs*. Ce désordre se situe dans les dimensions et la structure des composants internes :

- La géométrie du transistor, notamment l'épaisseur de la couche d'oxyde et les dimensions latérales du canal (largeur et hauteur) de la grille.
- La composition physique du transistor, par variation du dopage et ajout de matériaux non prévus.
- La géométrie des connections (dimension des lignes, épaisseur du métal, hauteur de la couche diélectrique).
- Les propriétés physiques des connections (la résistance du métal et du contact électrique, la constante diélectrique)

Le comportement de ces variables ne peut être contrôlé et prédit avec certitude au cours de la fabrication. Cela provoque des variations imprédictibles dans les paramètres électriques des circuits : la vitesse de propagation des signaux électriques, les différences de tensions ou toutes autres variables existantes. Dans la Figure 16, chaque puce produite aura ainsi une *empreinte physique* unique, la mesure de celle-ci permettra d'identifier la puce parmi les lots de *wafer.* Ce concept est parfois comparé à l'ADN de l'humain : la variabilité du désordre physique a la particularité d'être spécifique à chaque instance de circuit, affectant de manière unique la mesure de l'empreinte. Concrètement, un *silicon PUF* se présente sous la forme d'un bloc matériel intégré dans le circuit et qui extrait une signature à partir d'un des paramètres cités. Aucune personnalisation du masque de gravure dudit circuit n'est requise pour obtenir cette *unicité*, un seul et unique masque est exploité au cours de la fabrication. Un avantage fort à la vue des coûts prohibitifs de conception, ou modification des masques de circuits. De plus, à une échelle de mesure suffisamment fine, les variabilités de cet état physique ne sont pas reproductibles, assurant sa *non-clonabilité.* Ainsi, théoriquement, pour chaque puce produite un état physique unique et nonclonable lui est associé ; preuve de l'authenticité de ces puces au cours de leur cycle de vie.

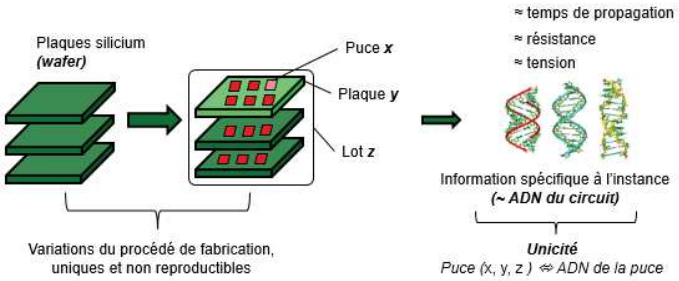

Figure 16: Désordre physique dans les circuits intégrés

3.1.2 Enjeux pour la conception des PUFs

Sans perturber l'état matériel du circuit, les facteurs environnants – la puissance, la tension d'alimentation, la température et le vieillissement – influencent aussi les paramètres électriques. Cela déstabilise les mesures des paramètres électriques, modifiant les réponses des PUFs au cours du cycle de vie. La reproductibilité des réponses est ainsi un critère décisif pour l'évaluation d'un PUF. En outre, certains aspects sécuritaires doivent être respectés et vérifiés, tels que l'unicité et l'imprédictibilité des réponses. Cela impose des contraintes sur la conception d'un PUF et le choix de ses deux composantes essentielles: le paramètre électrique choisi comme « stimulus » de transmission du désordre physique et le circuit qui extrait une réponse de ce paramètre. L'architecture générique d'un PUF en Figure 17 inclus ses composantes ainsi que d'éventuels blocs supplémentaires exigés.

Le choix du paramètre est arbitraire, sans contraintes ou limites, du moment qu'il soit possible d'en mesurer les variations. *Idéalement*, celui-ci doit être insensible aux facteurs environnants et seulement déterminé par le désordre physique (c.à.d. les variables citées précédemment, géométrie et composition physique des circuits). Le circuit d'extraction influence aussi les mesures et dicte la nature et les spécificités techniques des réponses du PUF, notamment la taille de réponse. Certains circuits incluent des combinaisons et des comparaisons des variations du paramètre afin d'améliorer la qualité de l'aléa. *Idéalement*, la réponse qui est extraite doit être imprédictible et unique (aspect sécuritaire) et reproductible au cours du cycle de vie (robustesse). Les applications de sécurité auxquelles sont destiné les PUFs imposent des contraintes et des exigences fortes ; en pratique une architecture PUF telle que présentée en Figure 17 doit souvent intégrer des blocs de post-traitement avec le circuit d'extraction, incluant selon les besoins :

1) Un code correcteur d'erreur (ECC) qui rectifie les réponses erronées
2) Une fonction de renforcement d'entropie pour améliorer l'aléa des réponses

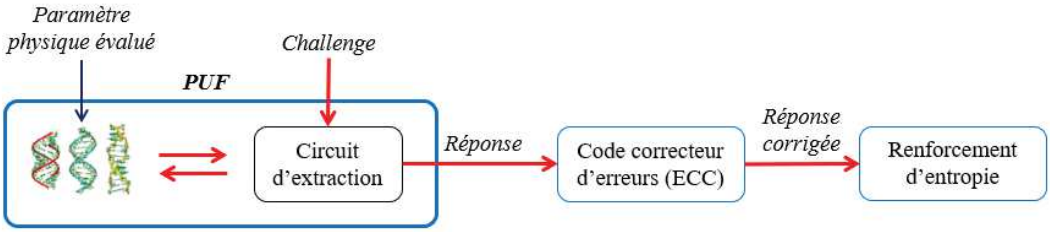

Figure 17: Architecture générique d'une primitive PUF

Ces fonctions supplémentaires impactent le coût et performances des PUFs. Ces enjeux – robustesse, coût, qualité de l'aléa – complexifient l'utilisation et l'évaluation des solutions de sécurité basées sur les PUFs. En l'occurrence, l'état de l'art comporte une multitude de modèles PUF de natures diverses ; tant par rapport au choix du paramètre que pour le circuit d'extraction. Parmi l'existant, certains PUFs ont des niveaux de sécurité et de fiabilité élevés. Roel Maes [33] détaille avec précision plusieurs *silicon PUFs*, leurs classifications et propriétés ; mais aussi leur évaluation par rapports aux applications de sécurité: authentification et génération de clefs cryptographiques. Deux états de l'art récents parcourent la littérature, un réalisé par des chercheurs de Singapore [39] , un autre par ceux de l'université de Lancaster (Royaume-Uni) titré « *A PUF Taxonomy* » [40]. Ce dernier approfondit la terminologie et la classification des PUFs, complexe à appréhender. Nous abordons ce point dans les sections suivantes.

3.1.3 Arbiter PUF et SRAM-PUF, illustrations des modèles *Weak* et *Strong*

La littérature distingue deux grandes catégories : les strong PUFs et les weak PUFs. Ce critère de « force » ne désigne pas le niveau de sécurité du PUF mais la taille et la capacité d'extension de son espace de challenges – réponses. Cet aspect détermine l'usage et les contraintes du PUF ; un nombre réduit de réponses limite l'utilisation directe de celles-ci. *A PUF Taxonomy* [40] détaille la distinction entre les modèles et les usages des weak PUFs et strong PUFs, ils sont schématisés dans la Figure 18.

Un strong PUF a un espace CRP (*challenge response pairs)* large, *idéalement* non énumérable et ainsi résistant aux attaques par brute-force En outre, cet espace s'accroit exponentiellement avec la taille du circuit PUF. Cela permet de concevoir à un coût raisonnable un PUF qui génère une multitude de signatures et ce avec un risque négligeable de collision (faible probabilité de paires identiques). Le protocole d'authentification déployé avec le strong PUF peut ainsi faire un usage unique de ces signatures ; elles sont « jetables ».

L'espace CRP d'un weak PUF est restreint, le nombre de signatures générées est faible. Parfois une seule et unique réponse est extraite comme schématisé dans la Figure 18. L'accroissement entre les dimensions du modèle et de son espace CRP est linéaire : doubler la taille de la réponse ou générer une 2ème réponse nécessite l'accroissement d'un facteur de deux de la taille du PUF. Par conséquent la réponse d'un weak PUF est à usage restreint, l'accès doit être protégé. Dans la Figure 18, des fonctions de dérivations de clefs sont nécessaires pour déployer un protocole de sécurité. Concrètement, l'usage d'un weak PUF se rapproche à celui d'une clef maitresse utilisé comme « racine de confiance » (*Root of Trust*) et source de dérivation de clefs cryptographiques.

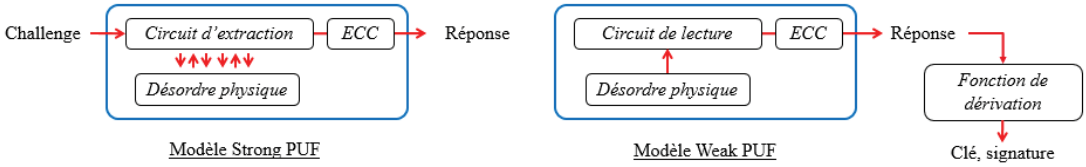

Figure 18: Les modèles strong PUF et weak PUF

Le SRAM-PUF est le modèle weak PUF le plus étudié dans la littérature et le plus avancé au niveau industriel. L'architecture repose simplement sur un bloc de cellules SRAM (Static Random Access Memory) ; une cellule se compose de six transistors formant un couple d'inverseurs croisés [41]. Cela permet de stocker un bit d'information (1 ou 0) ; deux transistors supplémentaires sont utilisés pour la lecture et l'écriture. Même si aucun bit n'a été « écrit », à la mise sous tension les transistors basculent nécessairement vers un des deux états logiques : un état initial déterminé aléatoirement selon le « point d'équilibre » des inverseurs. Ainsi, au démarrage d'un bloc SRAM (mis sous tension), une séquence binaire aléatoire peut en être extraite ; sa taille correspond au nombre de cellules, chacune d'elle retournant un bit d'information. Un modèle SRAM-PUF en fut dérivé en 2007 [42], [43]. Le challenge est l'adresse du bloc SRAM ; la réponse la séquence binaire qui en est extraite, la seule et unique. Cette architecture représente typiquement la faiblesse des weak PUFs en capacité de génération de paires challenge-réponse. Pour obtenir une nouvelle paire de même taille, ou doubler la longueur de la réponse extraite, un deuxième bloc SRAM doit être intégré dans le circuit.

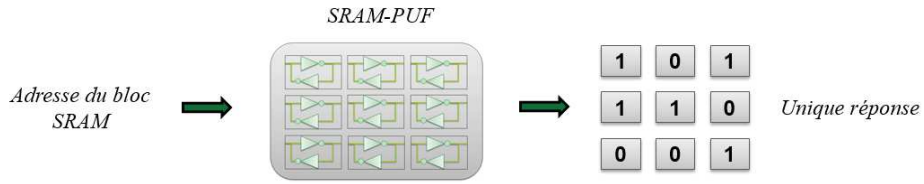

Figure 19: SRAM-PUF 3x3

En opposition, le modèle Arbiter PUF offre un espace de challenges plus large et qui s'accroit exponentiellement. Ce strong PUF, introduit en 2004 [44], a été étudié et amélioré à plusieurs reprises dans la littérature. Le PUF exploite les temps de propagation dans le circuit. Deux signaux se propagent par deux chemins symétriques, théoriquement identiques en longueur. En fin de parcours un composant logique arbitre « la course » des signaux, retournant 1 ou 0. Afin de varier le résultat, des commutateurs inversent la position des signaux entre les deux pistes électriques. Cette inversion dépend d'une séquence de bits fournie en entrée du PUF ; chaque bit détermine l'état d'un commutateur, influant le résultat de la course. Cette séquence est le challenge, le bit de résultat de la course la réponse. Avec ce PUF, le nombre de challenge est égal à la puissance deux du nombre de commutateurs. Doubler les commutateurs élève d'une puissance deux la dimension de l'espace CRPs. L'accroissement est exponentiel.

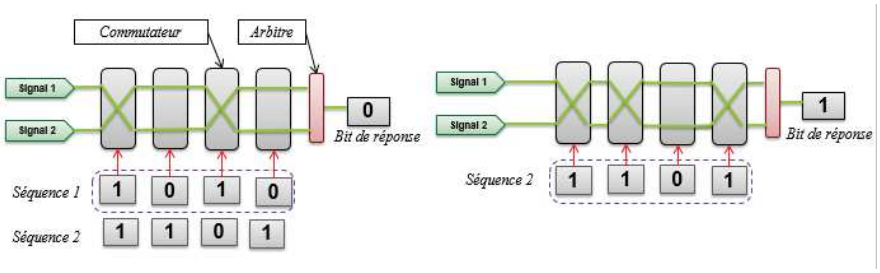

Figure 20: Arbiter PUF

L'usage et les contraintes varient sensiblement entre weak PUF et strong PUF ; nous apprécions le modèle strong PUF comme plus adéquat pour répondre aux exigences de sécurité du cycle de vie. En effet, la sortie d'un weak PUF doit être protégée, si la réponse est révélée au cours du cycle de vie cela peut compromette toute la sécurité des protocoles et des fonctions qui en sont tributaires. Un strong PUF offre plus de souplesse avec un large espace de réponses ; la compromission d'une réponse impacte seulement la sécurité des actions et des données assurées par celle-ci ; la multitude de signatures permet, en outre, de faciliter la répudiation ou l'ajout des acteurs dans la politique de sécurité.

3.1.4 Critère de classification des PUFs

La capacité de génération de réponse du PUF, *weak* ou *strong*, apparait comme un critère déterminant qui guide l'évaluation et la classification de tout nouveau modèle de PUF. Les architectures PUFs se distinguent aussi par d'autres aspects techniques, le choix du paramètre mesuré, la nature du mécanisme d'extraction ou encore l'origine de l'aléa (c.à.d. les spécificités du processus qui caractérise le désordre physique). Roel Maes [45], ainsi que l'article sur la taxonomie [40], fournissent les grands critères et concepts de base qui classent les PUFs.

La nature technologique du PUF – hybride, électronique, *silicium* : Les PUFs ne sont pas restreints à une technologie prédéfinie : une des première primitives, l'Optical PUF, utilise un matériau de diffraction optique ; une autre, récente, exploite des caractéristiques « biologiques » [46]. Toutefois, une majorité de la littérature se concentre sur les PUF dits « électroniques », constitués uniquement de composants analogiques ou numériques. Un PUF électronique est classifié *silicon PUF* s'il est embarqué dans un circuit intégré et se présente sous la forme d'un circuit numérique standard.

L'origine de l'aléa physique – intrinsèque ou extrinsèque : Si la chaine de conception et production du circuit conserve un flot standard, le désordre physique provient seulement de la variabilité de l'étape de fabrication. L'aléa est inhérent au circuit, le PUF est dit *intrinsèque.* C'est le cas des modèles Arbiter PUF et SRAM-PUF. Une procédure peut aussi être déployée en supplément pour apporter de l'aléa, auquel celui-ci est d'origine « externe ». Le PUF est dit *extrinsèque* ; tel que le modèle Optical PUF.

La nature du paramètre mesuré : Tout paramètre est susceptible de servir de source de mesure. L'article sur la taxonomie [40] fournit une classification des modèles selon le paramètre exploité. Cette étude liste trois catégories de variables pour les PUFs électroniques : les variables de « temps », comme la fréquence des circuits ou le temps de propagation des signaux (Arbiter PUF), les constantes physiques telles que les seuils de tensions électriques et les éléments matériels présentant des états binaires telles que les PUFs mémoires (SRAM-PUF). Cette dernière famille de PUF inclut un modèle récent et spécifique : les PUFs basés sur la « connectivité binaire » ; exploitant les états aléatoires – ouverts / fermés – des connections électriques dans les circuits.

L'intégration du mécanisme de mesure : Il faut noter un dernier point de classification**,** la mesure du paramètre peut être réalisée en interne ou en externe par un équipement. La majorité des *silicon PUFs* ont un circuit d'extraction qui génère la réponse au sein même du circuit intégré.

3.2 Critères d'évaluation des PUFs

3.2.1 Critère d'évaluation des PUFs : propriétés requises

Les critères précédents caractérisent une solution PUF nous permettant de la positionner et de la comparer à des modèles préexistants. En outre, certaines propriétés doivent être respectées pour que la primitive soit considérée comme PUF. Roel Maes détaille les propriétés requises dans [47] ; Van der Berg [48] en fournit un résumé synthétique que nous reformulons ci-dessous :

Physiquement non clonable : Un adversaire ne peut reproduire un objet physique identique au PUF – un clone – présentant les mêmes spécificités physiques et les mêmes paires de challenge-réponse. Cette propriété se mesure en fonction des ressources et de l'équipement de l'attaquant considéré. De plus, si même les fabricants (fondeur, concepteur…) ne peuvent réaliser une contrefaçon à un coût raisonnable le PUF est dit résistant aux fabricant – *manufacturer resistant.*

Identifiable : L'instance d'un PUF – pour un modèle et une implémentation définis – est identifiable au cours du cycle de vie et distinguable de toutes les autres instances. Cela induit deux contraintes :

- Unicité des réponses : Les réponses générées par des instances PUFs – pour un même modèle et une même implémentation – sont distinctes les unes des autres, associées à une seule et unique instance.

- Reproductibilité des réponses : Le modèle PUF permet de régénérer sur demande (soumission d'un même challenge) les réponses au cours du cycle de vie et les mesures sont suffisamment stables pour reproduire les réponses, à minima avec un post-traitement correctif abordable en termes de coût et de performance. *Cette propriété est « à l'opposé » de celle exigée pour un TRNG : les nombres aléatoires générés ne doivent pas être reproductible. Ceci est l'aspect fondamental qui distingue ces deux classes de primitives.*

Faisable : La construction et l'évaluation du PUF sont faisables à un coût abordable ; et la génération des réponses ne nécessite pas un temps excessif.

Outre ces exigences, une série de propriétés dites « secondaires » caractérisent la qualité du PUF, non nécessaires, elles déterminent toutefois la résistance du PUF face à certaines attaques et sont des critères supplémentaires pour évaluer une solution :

Mathématiquement non clonable : Un adversaire ne peut pas simuler le comportement d'un PUF à un coût et temps raisonnables ; c.à.d. incapable de créer un modèle théorique – quelle que soit l'implémentation logicielle – qui reproduit les mêmes paires de challenge réponse. Il s'agit là d'un clone « mathématique », non pas physique. Cela implique une contrainte :

- Non prédictibilité des réponses : Les réponses du PUF ne peuvent être anticipés ; cette propriété est induite par la non clonabilité mathématique (cela n'est pas réciproque).

Mathématiquement non réversible : Un adversaire ne peut déterminer à un coût et temps raisonnables le challenge utilisé pour générer une réponse du PUF ; propriété des fonctions non-réversibles.

Sensible à l'altération physique : Un adversaire ne peut altérer physiquement le PUF sans que ladite altération ne modifie les réponses du PUF ; et ce suffisamment pour être détecter ou non corrigible.

3.2.2 Critère d'évaluation des PUFs : métriques de sécurité

Une part importante de la littérature des PUFs étudie la sécurité et les performances des solutions existantes, ainsi que les méthodologies d'évaluation. Cela inclut des discussions et des critiques sur les métriques et modèles de sécurité pour les PUFs et leurs protocoles applicatif. Des métriques fondamentales furent définies dès les premières architectures PUFs ; notamment pour la capacité d'identification. Deux indicateurs, basées sur la distance de Hamming, permettent de vérifier respectivement l'unicité et la reproductibilité des réponses ([49], [50], [51]). La distance de Hamming quantifie la différence entre deux séquences de symboles ; généralement un simple OU exclusif suffit. Pour deux réponses binaires, il faut calculer le nombre de bits différents à chaque position.

La distance de Hamming inter-PUF évalue l'unicité des réponses. La métrique s'appuie sur la distance entre des réponses générées par des PUFs différents pour un même challenge ; calculant le nombre de bits différents. Cela indique la similarité entre des réponses. *Idéalement*, si les bits des réponses sont réellement aléatoirement différents, la distance converge vers une distribution binomiale avec espérance de 50% et déviation standard inférieur à 25% ([52], [53]).

Pour k PUFs retournant des réponses de n bits notées Ri, où i est l'identifiant du PUF, la distance de Hamming inter-PUF pour un challenge donné est :

$$HDinter = \frac{2}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} \sum_{l=1}^{n} \frac{R_i(l) \otimes R_j(l))}{n}$$

La distance de Hamming intra-PUF évalue la reproductibilité des réponses. La métrique s'appuie sur la distance entre des réponses générées pour un même PUF et même challenge, calculant et détectant le cas échéant les bits erronés. *Idéalement* la métrique se calcule en faisant varier, pour un même PUF et même challenge, les conditions environnementales : température, tension d'alimentation, humidité ou encore la pression. Les plages d'étude de températures sont parfois larges, pour l'implémentation

SRAM-PUF par l'entreprise *Intrinsic ID* les bornes sont - 50°C et + 150°C [54]. *Idéalement*, la métrique doit s'approcher de 0, preuve d'une forte robustesse du PUF. *Idéalement,* les conditions de tests peuvent être définis selon des standards reconnus, notamment les normes JESD22 du consortium JEDEC (*Joint Electron Device Engineering Council).*

Soit un modèle PUF définit, pour k PUFs retournant deux réponses de n bits à deux instants différents soumis à des conditions externes différentes, notées Ri et Ri', où i est l'identifiant du PUF, la distance de Hamming intra-PUF pour un challenge donné est :

$$HDintra = \frac{1}{K}\sum_{i=1}^{K}\sum_{l=1}^{n}\frac{R_i(l) \otimes R'_i(l))}{n}$$

Ces deux métriques jaugent l'unicité et la reproductibilité des réponses, et donc la capacité du PUF à être identifié. Roel Maes [55] détaille aussi la méthodologie pour évaluer un PUF dans le cas d'un protocole d'identification. La fiabilité du protocole est évaluée par les taux de faux rejet et de fausse acceptation ; respectivement abrégés FRR *(false rejection rate)* et FAR *(false acceptation rate)*. FRR et FAR sont déterminés par l'unicité et la reproductibilité des réponses, mais aussi par le seuil d'erreurs accepté et la capacité de correction d'un éventuel post-traitement. Selon le cas d'usage les exigences sont fortes, jusqu'à 10^{-12} pour les FAR et FRR des systèmes critiques.

L'uniformité est la dernière métrique régulièrement calculée. Aussi nommé « poids de Hamming », la métrique calcule le ratio 1 / 0 dans la réponse du PUF. C'est le premier indicateur pour estimer la qualité de l'aléa des réponses. *Idéalement,* l'uniformité doit être de 50 % (ratio équilibré entre les 1s et les 0s).

Soit un modèle PUF définit, pour k PUFs retournant des réponses de n bits notées Ri, où i est l'identifiant du PUF et Ri(l) le bit en position l, l'uniformité pour un challenge donné est :

$$Uniformité = \frac{1}{K}\sum_{i=1}^{K}\sum_{l=1}^{n}\frac{R_i(l)}{n}$$

Outre ces indicateurs, nécessaires pour valider un nouveau modèle PUF, des métriques plus sophistiquées sont étudiées pour les autres propriétés. Cela concerne notamment l'estimation de la qualité de l'aléa des réponses, ainsi que la non-prédictibilité de celles-ci.

La diffusion de l'information du challenge à la réponse extraite est un facteur important pour la non-prédictibilité. Définie par Shannon [56], cette propriété est notamment considérée pour les primitives cryptographiques ; où des schémas introduisent ***l'effet avalanche :*** les modifications en entrée de la fonction sont amplifiés pour la sortie. Dans le cas d'entrées / sorties binaires, ***le coefficient d'avalanche*** est le taux de modification entre deux sorties pour un bit modifié en entrée de la fonction. Pour une primitive de sécurité, chiffrement ou hachage, *idéalement* ce coefficient doit être de 50 %. La métrique est primordiale pour les strong PUFs, une forte diffusion est nécessaire entre challenges et réponses, pour éviter des réponses similaires à des challenges similaires. En cas de faible diffusion, des acteurs ayant accès à une partie des paires de challenge-réponse pourraient forger une nouvelle paire, ou prédire la réponse du challenge d'un autre acteur. Plusieurs chercheurs soulignent l'importance de la diffusion :

- Maiti & al [57] font une synthèse des métriques existantes (2011). Apparaissent les indicateurs classiques – unicité, reproductibilité et uniformité – ainsi que la diffusion. Les auteurs estiment cette propriété nécessaire pour les strong PUFs utilisé dans un protocole d'authentification.
- Van Herreweghe [58] introduit la diffusion sous le terme *self-similarity*, le niveau de similarité des réponses d'un même PUF pour différents challenges. L'auteur estime cette métrique pertinente dans les cas où le PUF doit générer de multiples réponses ; cas où elles sont susceptibles d'être analysées par un adversaire (tel que l'usage des réponses comme clefs cryptographiques).
- Le livre d'Halak [59] cite des métriques et des méthodes supplémentaires pour une évaluation approfondie. La section concernant la non prédictibilité présente le *test de distance de Hamming*, formalisant la métrique de diffusion [60]. La métrique utilise la distance entre deux réponses de

deux challenges de distance prédéfinit. Cela estime l'impact du taux de différence en entrée du PUF sur sa sortie. Le coefficient d'avalanche est ainsi le cas extrême où la distance prédéfinie est 1 ; l'auteur considère ce cas d'étude comme nécessaire pour évaluer la non prédictibilité.

Soit un modèle PUF définit, pour k PUF retournant, pour deux challenges distant de t, des réponses de n bits notées respectivement Ri et Ri', où i est l'identifiant du challenge, la distance de test est

$$HDtest(t) = \frac{1}{K}\sum_{i=1}^{K}\sum_{l=1}^{n}\frac{R_i(l) \otimes R_i'(l))}{n}$$

Le coefficient d'avalanche est le résultat pour t=1. Dans ce cas-là, idéalement, le coefficient doit être de 50 % et avec une déviation faible, inférieure à 15 %.

L'entropie est un indicateur primordial pour l'évaluation des fonctions cryptographique. L'entropie représente le niveau d'imprévisibilité (ou chaos) dans l'information. Plus l'entropie de la sortie de la fonction est haute, plus son imprévisibilité est forte c.à.d. moins elle donne d'information sur la fonction ou l'entrée. Une forte entropie des réponses du PUF assure l'imprévisibilité de celles-ci et la difficulté pour un adversaire de prédire les réponses ou de modéliser le PUF. Plusieurs formules existent, la métrique mise en avant est ***min-entropie*** ([61], [62], [63]), plus conservatrice : la formule conserve pour chaque bit l'imprévisibilité la plus faible ; cela permet d'estimer l'imprévisibilité minimale obtenu pour la réponse. *Idéalement,* la min-entropie doit s'approcher de la longueur de la réponse, soit une entropie de 1 pour chaque bit ; les standards préconisent 0.998 ; soit 127.744 pour une clef de 128 bits.

Soit un modèle PUF définit, pour plusieurs instances PUF soumises à différents challenges et retournant des réponses de n bits, pour lesquelles nous notons $P_0(l)$ et $P_1(l)$ la probabilité pour que le bit en position l soit égal à 0 ou 1, l'entropie minimale est

$$entropie_{min} = \sum_{l=1}^{n} -log_2(\max(P_1(l), 1 - P_1(l))$$

Pour terminer nous citons, sans entrer dans le détail, des méthodologies et des références supplémentaires sur l'évaluation de la sécurité des PUFs :

- Le taux de succès du PUF aux examens qualitatifs des nombres aléatoires, tel que les suites de tests de l'institut du NIST [64], Die Hard [65] ou AIS [66]. Un aléa « élevé » est requis pour les réponses du PUFs, notamment pour certaines applications (clefs cryptographiques).
- La résistance du PUF aux méthodes d'apprentissage, dites *machine learning attacks*. Rührmair & al ([67], [68]) évaluent en détails des attaques contre plusieurs modèles de PUFs, Noor & al [69] font une revue complète de la littérature sur ce sujet. Ces méthodes permettent de modéliser le PUF, créer un clone mathématique qui prédit les réponses. Cela suppose que l'adversaire a accès à des détails sur l'architecture du PUF et à une partie de ses challenge-réponses pour construire le modèle.
  - Des paires challenge – réponse sont transmises à un modèle d'apprentissage, le succès du modèle se mesure par sa capacité de prédiction sur les bits de sortie. Un coefficient de prédiction à 100 % par bit signifie que le PUF a été mathématiquement cloné
  - *Idéalement* pour un PUF résistent la prédiction de l'adversaire doit se limiter à 50 %.
  - Aussi, la résistance du PUF est évalué par le nombre de paires nécessaire aux modèles d'apprentissage pour créer le clone mathématique ; *idéalement* pour l'adversaire ce nombre doit être suffisamment bas pour un temps de traitement raisonnable.
- Armknecht & al [70] définissent un modèle de sécurité « unifié » synthétisant les précédents travaux sur la sécurité des PUFs. L'étude s'appuie sur cadre rigoureux issus du domaine de la cryptographie, comprenant les propriétés suivantes « *l'entropie minimum, la non-réversibilité, la non-forgeabilité, la non clonabilité, l'indiscernabilité, la qualité de pseudo-aléa, la sensibilité à l'altération ».*
- Un processus de normalisation est en cours (ISO/IEC 20897) sur les exigences de sécurité et les méthodes d'évaluation des PUFs. Des articles publiés par des membres du comité [71] pointe les contraintes sur les données évaluées. Cela peut se restreindre à une analyse du design, nécessiter des données de circuits simulés ou bien exiger des données de mesures réelles.

3.2.3 Métriques de performances

Les critères de coût sont déterminants pour l'implémentation des PUFs. Une faible performance peut être un facteur éliminatoire dans le cas de ressource ou d'environnement contraint. Des indicateurs essentiels permettent de vérifier la faisabilité du PUF : la surface requise par le circuit d'extraction, l'énergie consommée et la vitesse de traitement. La priorité est accordée à l'un ou l'autre selon les cas d'usage. L'université de Singapour tient à jour une base de données des PUFs existantes [72], incluant l'équivalent « normalisé » de ces métriques, c.à.d. l'énergie consommé par bit ou la surface de silicium requise par bit. Le standard ISO/IEC 29192 [73] indique aussi ces indicateurs pour les mécanismes de sécurité matériels. Si le rapport se focalise sur les crypto-primitives de chiffrement ou hachage, le contexte est similaire aux cas d'usage des PUFs. Ces deux références nous permettent d'établir un ensemble d'exigences et de métriques pour estimer la performance et le coût d'un PUF.

Surface requise par le PUF : Généralement l'occupation des ressources du circuit se mesure en μm^2, unité de surface. L'aire requise varie selon les modèles PUFs et le type d'implémentation. La technologie joue un rôle majeur ; des niveaux de gravure et de taille de transistors plus fins réduiront la surface.

- Le couple « aire requise en μm^2 » et « nœud technologique » de l'implémentation est l'indicateur le plus précis pour comparer les surfaces de PUFs intégrés dans les circuits ASICs. Idéalement, les surfaces de deux primitives PUFs doivent se comparer pour des nœuds technologiques identiques, à défaut les mesures de surface d'un PUF sont converties pour avoir une estimation – mais théorique seulement – pour la technologie utilisée pour le deuxième PUF.
- Le nombre de portes équivalentes (*GE pour Gate Equivalent*) de la primitive de sécurité est aussi une métrique couramment utilisée. Une GE correspond à une porte logique NAND à deux entrée, l'unité logique élémentaire dans laquelle peut se décomposer une implémentation matérielle. Le décompte des GEs nécessaires peut être convertis en surface réelle ; par exemple pour un nœud technologique à 65nm, une GE occupe $1.44\ um^2$. Cette métrique reste limitée pour une implémentation sur ASIC, elle ne prend pas en compte tous les paramètres, notamment les contraintes et optimisations au cours du placement-routage.

Vitesse de traitement du PUF : Les métriques et les objectifs en terme de vitesse peuvent diverger selon les applications, selon si les besoins portent sur la réactivé, ou plutôt sur le débit de sortie.

- La latence du PUF, exprimée en unité de temps, désigne la durée nécessaire pour générer une réponse complète après réception du challenge. Une latence réduite est imposée dans certaines applications en temps réel où la réactivité est vitale (automobile ou aéronautique).
- Le débit, mesuré en bit/seconde, désigne la quantité d'information fournie dans un temps donné. Cela s'applique aux réponses en sortie du PUF. Le débit est pertinent en cas de fonctionnement continu du PUF ; avec des appels successifs pour générer une série de réponse.
- La fréquence opérationnelle du PUF est le dernier indicateur pertinent, exprimée en hertz Hz. Pour une implémentation matériel synchrone elle désigne la fréquence du signal d'horloge du circuit, caractérisant sa vitesse de fonctionnement interne.

Energie requise pour le PUF : Plusieurs métriques caractérisent les flux d'énergie requis pour le fonctionnement d'un circuit.

- La mesure de la puissance nécessaire pour le fonctionnement du PUF, exprimée en Watt, permet une première appréciation des besoins énergétique du PUF.
- L'énergie consommée en Joule est l'indicateur le plus pertinent pour un cas d'usage soumis à des contraintes de durabilité. La consommation globale du PUF doit être réduite pour éviter une fin de vie prématurée de la batterie.
- L'énergie consommé par bit est aussi une métrique pertinente, en Joule / bit. Cette normalisation permet de comparer l'efficacité de PUFs de tailles différentes.

3.3 Apports et limites des PUFs traditionnels pour le cycle de vie

3.3.1 Sécurisation du cycle de vie, le cas du SRAM-PUF

L'étude de Roel Maes [33] évalue plusieurs modèles *silicon PUFs ;* notamment via des critères définis précédemment pour juger de leur l'efficacité. Pour un cas d'usage simple du PUF, l'identification du circuit, l'exigence porte sur la capacité d'identification : les taux de faux rejet et de fausse acceptation, respectivement abrégés FRR *(false rejection rate)* et FAR *(false acceptation rate)* en section 3.2.2, dépendant de l'unicité et de la reproductibilité des réponses. Les résultats démontrent la nécessité, pour compenser les taux d'échecs, d'accroitre la taille des réponses et donc la surface des PUFs. Les surfaces des implémentations SRAM-PUFs avec une technologie 65nm sont 75, 116 et 159 μm^2 pour des taux d'erreurs respectifs de 10^{-6}, 10^{-9} et 10^{-12}. Dans le cas d'un protocole d'authentification des contraintes s'ajoutent : l'obligation d'intégrer un code correcteur d'erreur et un taux d'entropie supérieur à 128 bits. Un point crucial, non approfondi dans cette section, est le coût en surface du code correcteur de la structure qui s'accroit avec celle de la réponse corrigée. Or, une entropie plus forte implique une réponse PUF plus longue ; la surface du circuit augmente en conséquence. L'étude de Roel Maes [33] démontre que la plupart des modèles *silicon PUFs* (RO-PUF, Arbiter PUF, Latch PUF ou Buskeeper PUF) ne respectent les exigences de stabilité et de sécurité qu'à un coût intolérable. L'Arbiter PUF atteint par exemple des taux d'erreurs de 10^{-6}, 10^{-9} et 10^{-12} avec des coûts de surfaces respectifs de 5100, 11800 et 240000 μm^2 ; bien trop élevés en comparaison du modèle SRAM-PUF. Celui-ci est le seul à fournir des performances acceptables : les surfaces sont estimées à 600, 1600 et 4200 μm^2 pour des taux d'erreurs respectifs de 10^{-6}, 10^{-9} et 10^{-12} ; et des entropies de 80, 128 et 256 bits. Deux références complètent l'évaluation du SRAM-PUF, témoignant en outre de son rôle de support pour la sécurisation du cycle de vie des systèmes sur puce *Intrinsic ID* [54] et Skuldlarek & al [15].

L'entreprise *Intrinsic ID* commercialise un SRAM-PUF pour générer de clefs cryptographiques au cours du cycle de vie [54], [74]. *Intrinsic ID* a évalué la stabilité du SRAM-PUF sous des conditions fortes [54] : températures de 150°C, humidité à 80 %, exposition à champ électromagnétique de 3V/m. L'instabilité monte jusqu'à 15 % ; un code correcteur et une fonction d'amplification d'entropie sont intégrés en conséquent pour assurer la génération, à 10^{-9} près, d'une clef de sécurité de 256 bits. La clef est utilisée comme *racine de confiance (Root of Trust)* qui assure l'authenticité des circuits fournit par le fondeur. Des fonctions de dérivations sont intégrées pour générer des clefs cryptographiques destinés à divers usages. Au cours du cycle de vie des certificats sont signés avec ces clefs [74], cela permet l'approvisionnement de codes logiciels tierces et d'applications utilisateurs. Les bénéfices sont forts : réduction du coût de personnalisation, protection contre la contrefaçon, suppression des risques de détournement des clefs et des certificats de sécurité qui ne sont plus transférés entre les acteurs contrairement aux schémas classiques. Deux produits sont proposés par *Intrinsic ID* : QUIDDKEY une implémentation matérielle sous la forme d'une *netlist* (description du circuit au niveau porte logique, interconnexions inclues) et BROADKEY une version logicielle développée en langage C.

L'article de Skuldlarek & al [15] (Mentor Graphics) détaille une plateforme complète pour les besoins d'authentifications du SoC. Ces travaux rappellent les enjeux de de sécurité lors des échanges et opérations impliquant les divers acteurs de production des circuits (OSAT, OEM, Fondeur...).La plateforme inclut un protocole d'authentification mutuel – authentifiant le circuit et l'utilisateur – et un bloc matériel de sécurité. Des fonctionnalités pour les besoins du cycle de vie sont implémentées : gestions de *logs* et paramétrage pendant les opérations de tests et d'encapsulation de puces, approvisionnement des fichiers de configurations et des IPs logicielles pendant le débogage, gestions des autorisations d'accès pendant l'assemblage et protocole pour les mises à jour logicielles. Le bloc de sécurité verrouille les accès au SoC, des fonctions et données supplémentaires sont intégrées : crypto-primitives et code d'autorisation pour les IPs. Le SRAM-PUF est l'élément central et critique : il génère la clef maitresse utilisée dans le protocole d'authentification. Cela illustre l'apport d'un PUF pour le cycle de vie : une confiance matérielle assurant l'authenticité et la capacité de génération de clefs, support sûr et efficace pour un protocole de sécurité.

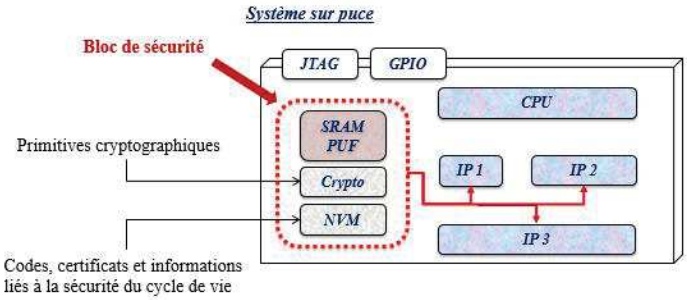

Figure 21: Architecture de Mentor Graphics avec SRAM-PUF pour la sécurité du cycle de vie [15]

3.3.2 Considération pour les aspects protocolaires

Un point crucial et limitant concerne l'aspect protocolaire : les communications du PUF doivent être protégées contre l'observation et les attaques d'interception type *man in the middle*. Cela peut nécessiter des fonctions de hachage et des générateurs de nombres aléatoires pour une sécurisation complète des échanges telle que schématisé dans le Figure 22. Les travaux de Delvaux & al ([75], [76]) offrent un état de l'art complet sur le sujet, ainsi que des critères précis pour évaluer les protocoles existants : robustesse et correction des erreurs, résistance aux attaques par modélisation, prévention contre le déni de service, scalabilité… Cela permet d'argumenter en faveur d'un schéma ou d'un autre selon les besoins et les contraintes de sécurité. Pour les protocoles d'authentification basés sur les strong PUFs, l'étude écarte des propositions – celles dépourvus de bloc de correction et de protection contre les *machine learning attack* – et fait ressortir du lot certains protocoles plus performants. Les conclusions pointent toutefois l'absence de strong PUFs robustes et offrant de propriété cryptographiques fortes. De fait, la majorité des protocoles dépensent des ressources pour compenser ces faiblesses. Le besoin en strong PUF sûr et efficace est critique.

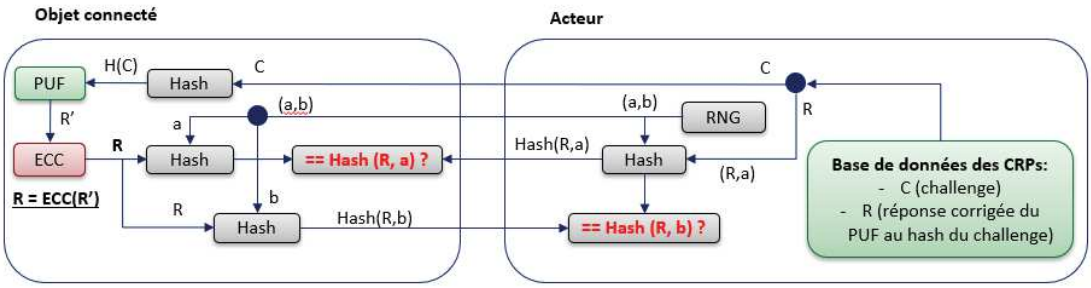

Figure 22: Protocole d'authentification mutuelle sécurisé avec fonction de hachage

Plusieurs points restent en suspens : la question de la gouvernance et des menaces au moment de la fabrication et de l'enregistrement du PUF ; la protection des bases du stockage des paires challenge réponse ; les stratégies de résilience (en cas d'attaque réussie il faut prévoir la répudiation des réponses et la possibilité d'une phase de réenregistrement). Cela ajoute une étude conséquente sur la sécurité au niveau système et organisationnel. Nous arguons ici d'une limite induite par un weak PUF : la compromission de sa sortie – seule et unique réponse – met en défaillance l'intégralité du système. A contrario, un strong PUF, avec forte entropie fournit une multitude de réponses aisément répudiables et dont la compromission à un impact limité à la fonctionnalité et à l'acteur qui les concernent.

3.3.3 Problématique de la robustesse des PUFs

La littérature propose des architectures strong PUFs avec de fortes entropies et des couts raisonnables. Toutefois les contraintes de robustesse contrebalancent ces résultats et limitent l'usage de ces modèles. Des procédés pour la correction des erreurs existent. Nous avons déjà cité les codes correcteur (de type BCH dans les travaux de Maes [33]). Halak [77] détaille des solutions supplémentaires, les prétraitements (consistant généralement à du vieillissement artificiel), la détection en amont des réponses les plus stables – éliminant les autres de la base de CRPs – et surtout le déploiement de méthode de reconstruction avec les *helper data.* Aussi, Halak prends en exemple les codes BCH pour l'étude du coût des corrections et démontre une évolution linéaire entre le niveau de correction exigé et la surface de circuit nécessaire pour le code correction. La Figure 23 illustre l'impact sur la surface requise (en nombre de porte logique – *Gate Equivalent)* pour corriger des réponses de tailles 128 et 256 bits. L'étude constate un facteur proche de deux entre surface et capacité de correction. Pour limiter le taux d'erreurs et le coût de surface qui en résulte pour l'ECC Halak recommande d'intégrer les méthodes supplémentaires, prétraitement et présélection des réponses.

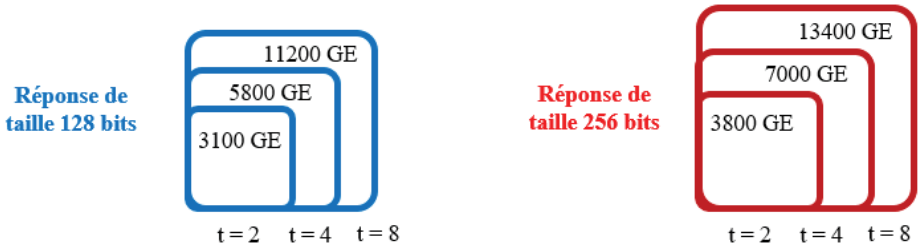

Figure 23: Evolution de la surface des ECCs en fonction de la capacité de correction et de la taille de réponse (t : capacité de correction, GE : Gate Equivalent – nombre porte logique requise) [77]

Outre le coût de surface, les schémas de corrections augmentent aussi les vulnérabilités. Delvaux présente les méthodes d'exploitation des *helper data* pour découvrir les réponses PUFs [78]. Une autre étude précise les *pertes d'entropie* dues à un protocole de correction [79]. La robustesse exigée implique donc la recherche d'un compromis entre coût, performance et sécurité du PUF. Des travaux se focalisent sur la conception de PUFs robustes, notamment via des paramètres moins sensibles aux perturbations extérieures ou en améliorant le circuit d'extraction. L'étude de l'université de Singapore montre toutefois une tendance au désintéressement pour ce sujet [72]. Les derniers modèles ont des taux d'erreurs plus fort. Les auteurs argumentent que même avec une forte robustesse, des codes correcteurs et un post-traitement sont nécessaires ; par conséquent les recherches se tournent sur l'amélioration des autres métriques. Toutefois, les PUFs à connectivité binaire – ainsi définis dans *« A PUF Taxonomy »* - offrent théoriquement une robustesse parfaite. Nous nommons aussi ce modèle *digital PUF*, en référence au caractère *numérique* du paramètre, Cela exclurait la nécessité d'intégrer des blocs correcteurs.

3.3.4 Conclusion

Dans une certaine mesure, les PUFs traditionnelles répondent aux besoins de sécurité du cycle de vie (2.3.1). Une primitive PUF respectant les critères de conception assure l'authenticité du circuit. Sous réserve d'une forte entropie, les modèles strong PUFs offrent aussi un large espace de réponse. Cela permet de construire des protocoles d'authentification ou de générer des clefs cryptographiques. Avec le déploiement d'un protocole adéquat et d'une gestion sûre de la base de réponses PUF, une politique de droit d'accès peut être déployé au cours du cycle de vie.

En terme de coût, la question est ouverte. Les PUFs sont moins chères que les composants mémoires et plus sûres de par leurs propriétés physiques. Un intérêt majeur est de limiter l'étape de personnalisation et d'intégration des paramètres de sécurité ; des gains en coût et simplification sont possibles. Cependant,

des difficultés demeurent, comme la correction des erreurs et le renforcement de l'entropie. Elles doivent être résolues avant le déploiement des fonctions de sécurité du cycle de vie. La reproductibilité est un critère décisif, or même avec un post-traitement de haute qualité une erreur n'est pas exclue. En particulier si le circuit est soumis à de fortes perturbations ; notamment pour certains usages avec des conditions extérieures influentes. De plus, le vieillissement a un effet inévitable sur le circuit. Une réponse erronée est toutefois incompatible avec des fonctions de sécurité de type chiffrement ou hachage. La conception d'un PUF sûr et efficace est donc astreinte à respecter le critère de robustesse.

3.4 Motivation et problématique pour la conception des *digital PUFs*

3.4.1 Introduction des *digital PUFs*

Récemment, des recherches s'intéressent aux *digital PUFs* (DPUF), basés sur des paramètres non analogiques : des structures aléatoires instanciées à la fabrication, composées de connections électriques ou lignes métalliques aléatoirement coupées. Un circuit d'extraction convertit ces discontinuités électriques en séquences binaires, utilisées comme réponse. La réponse se génère ainsi via un aléa de nature structurelle, statique, fortement résistant au bruit et au vieillissement. La robustesse inhérente à la structure matérielle assure une forte reproductibilité. Nous modélisons dans la Figure 24 un DPUF sous la forme d'un bloc électronique cohérent, intégrant avec une structure aléatoire le circuit logique qui extrait la réponse.

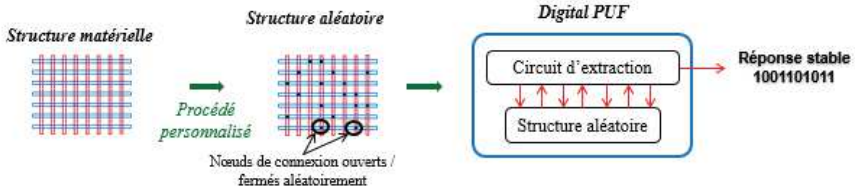

Figure 24: Le modèle digital PUF

Divers procédés de fabrication existent pour fabriquer ces structures aléatoires, tout comme il existe différents modèles de circuits logiques pour générer la réponse finale du DPUF. Plusieurs travaux démontrent la faisabilité et l'intérêt des DPUFs :

- SD-PUF ([80], [81])
- VIA-PUF ([82], [83], [84])
- LED-PUF ([85], [86])
- CNT-PUF ([87], [88], [89]).

Les structures aléatoires sont générées en agissant sur les distances limites de formation de contact électrique : positionnement rapproché des lignes d'interconnections du masque de gravure du circuit pour produire des discontinuités électriques au cours de la lithographie (SD-PUF [81]) ; VIAs (*Vertical Interconnect Access*) avec une taille d'orifice à la limite de celle requise pour que la jonction soit effective (VIA-PUF [84]) ; densité spécifique de copolymère conducteur pour produite un contact électrique aléatoire (LED-PUF 94]) ; projection aléatoire de nanotubes de carbone (CNT-PUF [87]).

La nomination des modèles par les auteurs varie en fonction du procédé de fabrication – *self-assembly PUF* pour le LED-PUF ou le CNT-PUF (auto assemblage), *physical-based PUF* pour le VIA-PUF. L'article *« A PUF Taxonomy »* catégorise ce modèle sous le terme « PUF basé sur un état de connexion binaire » : une terminologie adéquate pour l'ensemble des paramètres des modèles DPUFs. Nous employons dans notre recherche l'adjectif *digital* pour qualifier ces PUFs. Introduit pour le SD-PUF [81], ce terme désigne judicieusement la nature de l'entropie statique obtenu après fabrication et utilisée pour générer les réponses. Nous précisons les exigences qui classifient un PUF en DPUF :

- Le paramètre évalué est de nature structurelle, caractérisé comme source d'aléa *numérique,* résistant au bruit et au vieillissement tel que le besoin en correction d'erreur soit négligeable.
- La génération de la réponse, de l'évaluation du paramètre à la séquence binaire finale, est un processus strictement *numérique.*
- Le bloc PUF est un circuit logique fonctionnel et robuste, son implémentation respecte le flot de conception standard d'un circuit intégré et supporte notamment les contraintes de temps.

Les DPUFs, intrinsèquement robustes, offrent une forte reproductibilité des réponses contrairement aux PUFs traditionnelles. Cela avantage les DPUFs pour des cas d'usage soumis à des conditions extérieures dures, à une longue durée de vie et à des exigences élevées sur la stabilité des réponses.

3.4.2 Classification et propriétés des DPUFs

Similaire sur certains aspects, les DPUFs se différencient des modèles traditionnels par certaines propriétés. Nous détaillons les particularités des modèles DPUFs en nous appuyant sur les critères de classification (3.1.4) et les propriétés (3.2.1) définis précédemment.

Nature technologique :

Les DPUFs sont des silicon PUFs, implémentés sous la forme de circuits numériques standards.

Origine de l'aléa :

Ce point est sujet à caution. Nous considérons l'aléa extrinsèque quand un DPUF nécessite une opération explicite, ou une personnalisation, pour fabriquer la structure aléatoire. Des DPUFs s'appuient toutefois uniquement sur une spécification particulière des masques (SD-PUF & VIA-PUF) ; auquel cas l'aléa peut être dit intrinsèque. Ces exemples sont détaillés en section 3.5.

Nature du paramètre mesuré :

Le paramètre est structurel, modélisé comme un ensemble de nœuds de connections aléatoirement fermées ou ouvertes ; concept fondamental des DPUFs.

Intégration du mécanisme de mesure :

La mesure est interne ; le circuit d'extraction, intégré dans le circuit silicium, génère la réponse par une conversion des nœuds de connections.

➔ *Un DPUF est un silicon PUF avec un circuit interne qui génère les réponses en exploitant un paramètre structurel qui est d'origine intrinsèque ou extrinsèque selon le procédé de fabrication.*

Physiquement non clonable :

Cloner un DPUF implique de fabriquer une structure aléatoire identique, disposant spécifiquement des mêmes nœuds de connections que celle du DPUF ciblé. Une extraction du statut des connexions est faisable, toutefois reproduire la structure du DPUF impose de réaliser un processus de fabrication complet avec une spécification précise des connections pour le masque de la contrefaçon. Cela demande un coût et un temps élevés ; de plus, cela ne permet d'usurper qu'un seul DPUF. Une telle contrefaçon est donc couteuse et limité en gain.

Identifiable :

(1) La reproductibilité des réponses est assurée par la robustesse inhérente des DPUFs.

(2) L'unicité dépend des caractéristiques de la structure aléatoire et du circuit d'extraction. Sous réserve d'un modèle DPUF correctement définit, les métriques de sécurité peuvent être assurées.

Faisabilité : Deux aspects de la faisabilité sont considérés.

(1) Un DPUF dit fonctionnel est faisable ; des démonstrateurs validant les contraintes physiques et électriques sont décrits dans la littérature ([81], [84], [87]). Il faut toutefois noter la nécessité d'intégrer des cellules logiques pour la conversion des nœuds de connexions. En outre, les méthodes de fabrication du DPUF implique une adaptation du flot de conception standard. Cela doit être compatible avec les contraintes et coûts de conception. Cela dépend de la nature et des contraintes du procédé.
(2) Un DPUF dit performant est faisable. Les coûts et les performances varient selon les cas. Des études concluent sur des résultats corrects ; les estimations de surface dans les dernières articles du LED-PUF [86] et SD-PUF [81] concurrencent ceux du SRAM-PUF. La section 3.5 détaillent les résultats et performances de ces modèles.

Les DPUFs respectent, dans une certaine mesure, les propriétés fondamentales des PUFs.
- *Ils se caractérisent par une robustesse forte, théoriquement parfaite.*
- *Les implémentations existantes dans la littérature prouvent leur faisabilité*
- *La non-clonabilité physique est élevée et est compromise uniquement face à adversaires disposants de moyens importants et de connaissances avancées.*
- *L'obtention de propriétés mathématiques, telle que l'unicité, ainsi que des performances convenables, notamment en terme de surface, est faisable mais impliquent un effort de conception.*

Mathématiquement nonclonable : La sensibilité des DPUFs aux méthodes d'apprentissage ou à des algorithmes de prédictions dépend du modèle d'implémentation. Selon le type d'architecture – strong PUF ou weak PUF – les problématiques de sécurité diffèrent. L'étude du SD-PUF [81] montre un certain niveau de résistance à la modélisation pour les strong DPUFs, sous réserve d'une configuration adéquate du DPUF. Un point critique est la vulnérabilité à l'imagerie, ou plus généralement aux attaques invasives qui pourraient extraire le statut des nœuds de connexions. Ces menaces sont crédibles pour certains cas d'usages qui requièrent un très haut niveau de sécurité ou à forte valeur ajoutée. Cette faiblesse varie selon la technologie d'implémentation du DPUF ; la question est abordée dans les travaux du VIA-PUF [82], LED-PUF [86] et des CNT-PUFs , [88].

Mathématiquement non-réversible : Cette propriété dépend essentiellement du modèle d'implémentation et du circuit d'extraction.

Sensible à l'altération physique : Les structures matérielles DPUFs sont peu sensibles à une altération physique classique, une injection de faute ou une attaque invasive non destructive ne laissent aucune trace sur les nœuds de connexion. Par conséquent ces attaques peuvent ne pas être détectées, mais en ayant toutefois un impact sur les signaux logiques en sortie du DPUF et la sécurité du protocole. Des mécanismes supplémentaires peuvent être requis pour détecter et atténuer ces menaces.

Les DPUFs ont des propriétés secondaires particulières, en comparaison des PUFs traditionnelles :
- *Non-clonabilité mathématique variable selon l'architecture et la configuration du DPUF.*
- *Sensibilité variable à l'imagerie selon la technologue d'implémentation et vulnérable face à certains modèles d'adversaire considérés.*
- *Insensibilité à l'altération physique, avantage ou non selon le modèle d'adversaire.*

3.4.3 Problématique et modélisation pour la conception des DPUFs

Une question critique de la conception des DPUFs porte sur l'optimisation du modèle : réussir l'implémentation d'un DPUF à la fois sûr et efficace. Les réponses générées doivent assurer des propriétés de sécurité et le circuit respecter des contraintes de coût et de performances. Ces aspects dépendent à la fois des caractéristiques de la structure matérielle – l'ensemble des nœuds de connexion aléatoire source d'entropie – et du circuit logique spécifié pour extraire les réponses. La Figure 25 illustre la couche matérielle du DPUF – la structure aléatoire – se caractérise par deux paramètres : le dimensionnement de la structure et l'aléa des nœuds de connexions.

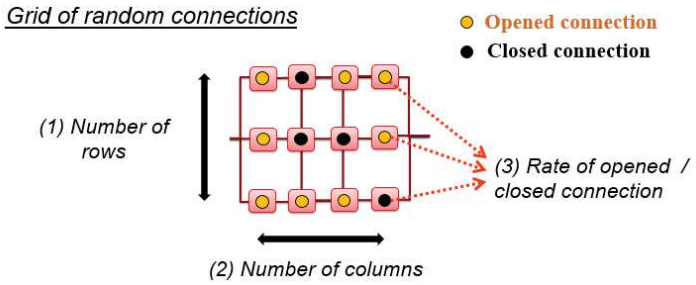

Figure 25: Modélisation de la structure matérielle d'un DPUF

Une première contrainte s'impose : la probabilité de collision entre deux structures fabriquées doit être faible, à minima quasi nulle. Cela implique une quantité suffisante de nœuds de connexion pour multiplier le nombre de combinaisons d'états fermés / ouverts de ces nœuds. Cela se répercute sur la taille de la structure ; elle augmente avec la quantité de nœuds de connexion implémentés. De plus, *idéalement*, la probabilité de déconnection doit être de 50 % pour maximiser le nombre de combinaisons. La configuration de ces paramètres, ainsi que leur incertitude et leur impact sur le coût et la performance du DPUF, dépendent du procédé de fabrication choisi.

Toutefois, le circuit d'extraction joue aussi un rôle majeur : les opérations logiques supplémentaires accroissent la surface silicium du bloc DPUF et influencent les propriétés mathématiques des réponses. Cette couche logique introduit des paramètres supplémentaires, spécifiques au circuit d'extraction. Les configurations diffèrent fortement selon la catégorie weak ou strong du modèle PUF implémenté.

Une étude est requise pour identifier la configuration adéquate des couches matérielles et logiques qui forment le modèle DPUF. La conception s'avère délicate car les deux couches peuvent être spécifiées indépendamment : divers procédés de fabrication sont compatibles pour le même type de circuit d'extraction et vice-versa. Or, les contraintes varient en fonction des solutions choisis pour les deux couches ; et celles-ci s'influencent l'une l'autre, modifiant les performances finales du modèle implémenté. Cela offre une large gamme d'architectures DPUF diverses, hétérogènes et flexibles.

Cette problématique de conception est essentielle pour les besoins du cycle de vie ; la primitive matérielle PUF doit respecter les exigences de coûts, de sécurité et de flexibilité identifiées précédemment dans l'analyse de sécurité.

Plusieurs approches sont possibles pour répondre aux objectifs de compromis surface / sécurité ; et peuvent s'appuyer sur les propositions existantes dans la littérature des DPUF.

3.5 Etat de l'art des implémentations DPUFs : analyse et classification

3.5.1 VIA-PUF

Introduction

Le VIA-PUF, introduit en 2014 [82] par des chercheurs sud-coréens, tire son nom des points de contacts entre deux lignes de métaux d'un circuit : les *VIAs* ou *Vertical Interconnect Access*. Une première phase de recherche ([83], [90]) analyse les métriques de base ; stabilité et unicité. L'évaluation porte sur une série de 119 VIA-PUFs produits en nœud technologique 180 nm. Une publication en 2019 [84] étudie des métriques de robustesse et de sécurité supplémentaires pour des VIA-PUFs produits en 130 nm. Cette étude complète en détail les performances et les contraintes. Plusieurs brevets ont été déposés ; le VIA-PUF est aujourd'hui industrialisé et commercialisé par l'entreprise ICTK [91].

Fabrication des structures aléatoires

Le VIA-PUF consiste en l'établissement aléatoire de VIAs, les canaux connectant les lignes de métaux du circuit. Ces VIAs se forment durant la photolithographie, leur taille et position sont spécifiées sur le masque par les concepteurs. Au cours du processus de fabrication, un diamètre minimal est nécessaire pour « remplir » le VIA. En deçà, les lignes ne se connectent pas, au-delà le VIA est formé. Les auteurs ont étudié plusieurs tailles de VIAs, identifiant les intervalles pour lesquelles la probabilité de formation se rapproche de 50 %, la valeur idéale pour les structures aléatoires DPUFs. Dans la Figure 26, la taille spécifiée dans le masque du circuit induit une formation aléatoire des VIAs. Avec ce procédé de fabrication le DPUF a un aléa *intrinsèque*, aucune intervention n'est requise sur les équipements, seulement une personnalisation du masque de gravure au moment de la conception.

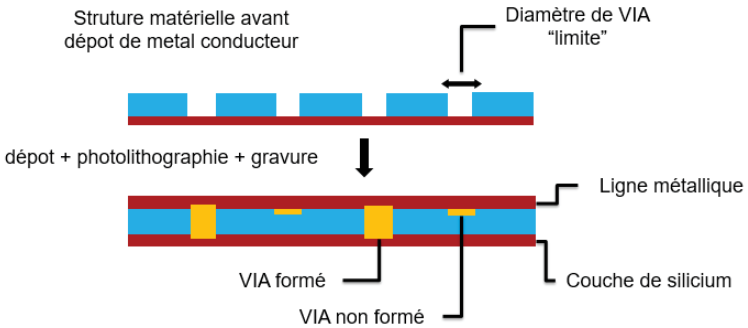

Figure 26: Formation aléatoire des VIAs [91]

Circuit d'extraction de réponse

Un circuit de lecture simple est proposé pour extraire une réponse. Dans la Figure 27 une cellule composée d'une charge résistive et d'un transistor de lecture convertit le statut du VIA ; un VIA formé sera traduit par un bit 1, 0 sinon. Les VIAs alignés régulièrement forment une grille sur laquelle se superpose la grille de cellules qui génèrent les bits de statut. Il s'agit d'un modèle *weak-DPUF,* semblable au SRAM-PUF, avec un espace challenge-réponses réduit : en entrée l'adresse de la rangée dans la grille de lecture, en sortie la séquence binaire correspondant aux statuts des VIAs. En complément, les auteurs proposent dans plusieurs brevets un protocole de dérivation pour générer des clefs de sécurité à partir de cette unique réponse. Avec ce circuit d'extraction, les propriétés et les performances du DPUF dépendent essentiellement de la configuration de la structure aléatoire, c.à.d. sa taille et son entropie. Dans l'optique de renforcer les propriétés de sécurité – uniformité et unicité – une couche logique supplémentaire est intégrée ; détaillée dans les sections suivantes.

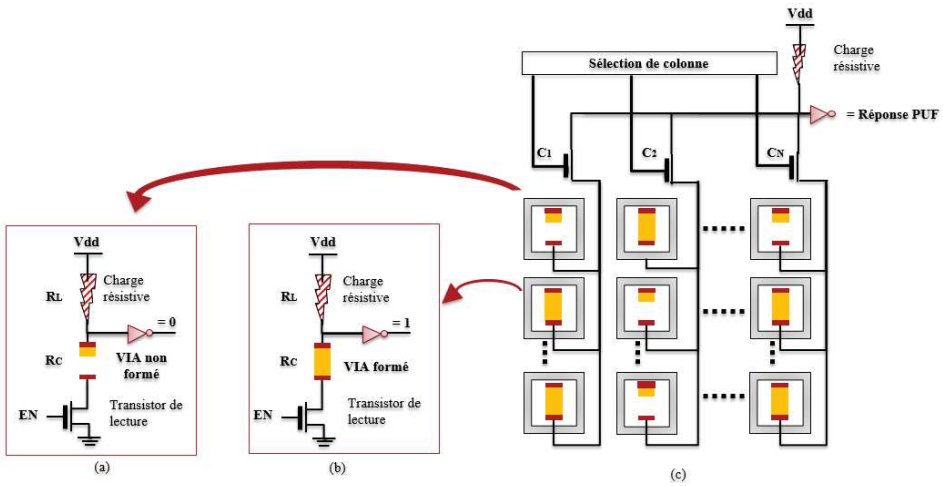

Figure 27: Circuit d'extraction du VIA-PUF [83]
(a) Réponse de la cellule pour un VIA non formé (b) Réponse de la cellule pour un VIA formé (c) Grille de lecture des VIAs

Robustesse du VIA-PUF

Le statut des VIAs, fermé / ouvert, dépend de la formation de la liaison métallique. Cet état physique est insensible au vieillissement ou aux perturbations ; ceux-ci ne peuvent modifier la présence, ou l'absence, de matériau métallique conducteur. La 1ère étude démontre une reproductibilité parfaite des réponses sous des variations de températures de 25°C à 125°C et des seuils de tensions de 1.6 à 2V.

Toutefois, la dernière publication [84] nuance ces assertions et approfondit l'évaluation. Les auteurs précisent que sous conditions extrêmes les contacts changent : un champ électrique fort peut produire un claquage (un arc électrique) connectant les deux couches de métaux, ou une densité élevée de courant générer une électro-migration coupant le contact. Une deuxième question problématique et spécifique au VIA-PUF, est abordée ; bien que la probabilité soit très faible, certains VIAs peuvent être « partiellement » formés. La Figure 28 montre ces deux cas :

- Dans un cas, le conducteur (du tungstène pour le VIA-PUF) ne complète pas entièrement le VIA dans la longueur, la fin du VIA plus étroite ne permet qu'un contact limité.
- Dans un autre cas, le conducteur n'est posé que sur les bordures du VIA, formant une ligne de vide plus ou moins large dans le VIA.

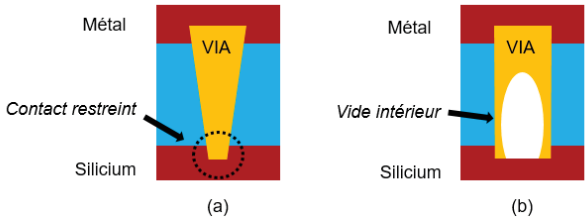

Figure 28: Formation partielle des VIAs
(a) formation incomplète en longueur (b) formation incomplète en largeur

Dans ces deux situations, le contact est établi entre les métaux, mais ces imperfections produisent un état instable. Selon le niveau de résistance dans les pistes électriques le signal sera transmis ou non. 405 puces sont produites, contenant chacune 122 880 VIAs. Environ 10 % (~ 42 puces) présentent des VIAs problématiques. La robustesse des VIA-PUFs bien formés est cette fois-ci analysée en suivant la

normes JEDEC (*Joint Electron Device Engineering Council) : JESD22-A108, A103, A19A, A104E, A101, A118B et A113H.* Les réponses sont générées sous des conditions extrêmes, maintenus pendant un intervalle de plusieurs heures. Les températures varient de -55°C à 150°C, la tension d'alimentation jusqu'au maximum (1.7V) et les taux d'humidité montent à 85 %. Le taux d'erreurs des réponses est de 0 % ; validant ainsi la robustesse du PUF. Il faut toutefois noter, en incluant les 42 DPUFs erronés, un taux d'erreur de 2.3 x 10^{-8}.

Sécurité du VIA-PUF

La sécurité du VIA-PUF, l'unicité et l'imprédictibilité des réponses, repose sur la configuration de la structure aléatoire c.à.d. la taille de la grille de VIAs et la densité de formation de ceux-ci. Les auteurs se confrontent à des difficultés pour obtenir l'uniformité idéale, soit 50 % de VIAs formés. Les équipements et outils de conception ne permettent pas de spécifier au nanomètre près la taille des VIAs ; un pas prédéfini doit être respecté. En outre, de plaque à plaque et de lot à lot, des variabilités non contrôlables influent sur la probabilité de formation. En conséquent, la probabilité de formation des VIAs n'est pas uniforme, les réponses ont un biais dans le ratio de 1 et 0. Les auteurs proposent un post-traitement, basé sur une procédure de comparaison sur 8 bits, pour améliorer l'aléa. Ce post-traitement ajoute un surcoût d'un facteur 8 en terme de surface nécessaire pour générer un bit de réponse. Dans la dernière étude [84] ce traitement est accru : 12 XORs sont effectués sur 16 bits chacun suivi d'une dernière opération XOR pour renforcer l'aléa. Au total il faut 192 VIAs pour générer un bit de réponse.

L'évaluation du 1er modèle VIA-PUF [83], effectuée sur 119 puces, générant des réponses de 2 560 bits, conclut sur les résultats suivant pour les métriques basiques (unicité et uniformité) incluant la déviation standard :

- Uniformité de 51,12 % avec une déviation de 8,07 %
- Unicité de 49,64 % avec une déviation de 1,95 %

Ces premières performances atteignent les objectifs de sécurité des PUFs établis en section 3.2.2. L'analyse du 2ème modèle en 2019 [84], effectué sur 405 puces, conforte ces résultats. Celle-ci inclut des métriques supplémentaires, les tests du NIST et l'estimation de l'entropie :

- Uniformité de 49.72 % avec une déviation de 2,05 %
- Unicité de 49.99 % avec une déviation de 0,99 %
- Entropie de 0.99973 par bit
- Tests du NIST validés

Coût et performance du VIA-PUF

Les deux modèles VIA-PUFs sont produits en technologie CMOS avec respectivement des nœuds de 180 nm et 130 nm. Les études indiquent la surface silicium requise ainsi que des estimations pour le débit de sortie et la consommation d'énergie. Les résultats du 1er modèle sont les suivants :

- 47 um^2 pour un bit de réponse, 6 016 um^2 pour une clef taille 128.
- Débit de sortie supérieur à 1 Mbit/s

Le 2ème modèle nécessite une surface plus importante à cause du post-traitement supplémentaire :

- 8 225 um^2 pour un bit de réponse, 1 053 800 um^2 pour une clef taille 128.
- Latence de 30 ms pour générer la réponse, soit dans le cas étudié un débit de 21 kbit/s
- Une énergie de 0.645 pJ/bit

Conclusion

Le VIA-PUF est le 1er modèle DPUF proposé dans la littérature et aussi le plus avancé en termes d'industrialisation et d'expérimentation. Des évaluations ont démontré une robustesse élevée et certifiée

par des standards de tests. Par contre, les structures aléatoires produites ont un aléa de faible qualité du fait des contraintes technologiques : les tailles de VIAs ne peuvent pas être configurées avec suffisamment de précision et la probabilité de formation des VIAs varie de puce en puce. Par conséquent, un post-traitement est nécessaire, alourdissant le coût d'implémentation du circuit d'extraction.

3.5.2 LED-PUF

Introduction

Le LED-PUF est introduit en 2016 [85] par des chercheurs de l'université de Californie (Los Angeles) et se base sur des blocs de copolymères qui s'assemblent aléatoirement selon leur proximité. Ce procédé – aussi nommée *Direct Self-Assembly* (DSA) – est utilisé pour générer des défauts locaux dans les connections du circuit, d'où le terme désignant le PUF : LED, pour *Locally Enhanced Defectivity*. Les auteurs proposent deux modèles de circuit d'extraction. Le premier est similaire au VIA-PUF avec une lecture simple de l'état des connexions. Le deuxième intègre une fonction de hachage avec la structure aléatoire et instancie un modèle strong DPUF. Une deuxième contribution [86] complète ces travaux avec une méthodologie supplémentaire pour évaluer la sécurité des circuits PUFs.

Fabrication des structures aléatoires

Des blocs de copolymères conducteurs déposés sur les couches de silicium permettent de créer des connexions électriques. Ces nœuds de connexion, similaire à un VIA, sont appelés *DSA-VIA* par les auteurs. Un aléa est provoqué dans l'assemblage des blocs par une configuration adéquate de la température, de la composition des blocs et en particulier des distances définies par le *masque de guidage*. Les auteurs fournissent les références et les contraintes nécessaires pour générer une structure aléatoire [86] ; et ce avec une configuration qui équilibre la probabilité de formation des DSA-VIAs.

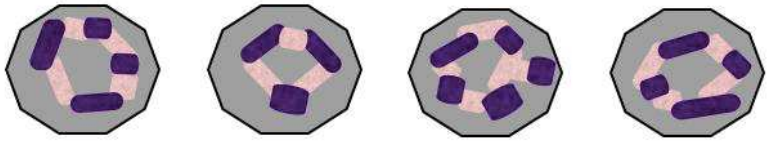

Figure 29: Formation aléatoire des DSA-VIAs selon divers masque de guidage [85]

Circuit d'extraction des réponses

Un 1er circuit instancie un modèle weak DPUF comparable au VIA-PUF : en entrée l'adresse de la rangée de la grille de lecture, en sortie la séquence binaire correspondante à l'état des VIAs. Dans la Figure 30, le bloc logique qui interprète le statut de la DSA-VIA est composé d'un total de 3 transistors ; moins couteux qu'une cellule SRAM (6 transistors).

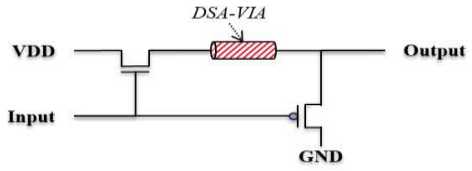

Figure 30: Cellule logique de lecture du statut des DSA-VIAs

Par la suite, les auteurs proposent un modèle strong PUF, ils intègrent en sortie du weak DPUF une fonction de hachage à deux entrées. Dans la Figure 31, la 1ère entrée est réservée à une clé de sécurité permanente – en l'occurrence la seule et unique réponse du LED-PUF – la 2ème entrée pour un challenge. Des standards existent, notamment la version HMAC (*keyed hash message authentication code)* de la primitive SHA-3. Avec ce schéma, la sécurité et la performance du strong DPUF dépendent de celles du weak DPUF et de celles du hachage sélectionné. Du fait des propriétés de hachage – notamment l'effet

avalanche – toute erreur en entrée de cette fonction sera répercutée sur l'ensemble de la réponse finale. Ce modèle se construit uniquement à partir de weak PUF parfaitement robuste.

Figure 31: Modèle strong DPUF avec fonction de hachage

Robustesse du LED-PUF

Théoriquement, la reproductibilité des réponses est assurée par l'état permanent des DSA-VIAs. La construction de structure par mécanisme DSA fait l'objet d'une littérature et de démonstrations avancées qui offrent une certaine assurance dans la faisabilité de cette méthode. Les études du LED-PUF ne fournissent toutefois aucun résultat d'expérimentation réelle. Du fait de la similarité de ce procédé avec celui du VIA-PUF, nous considérons un risque faible d'être confronté à des DSA-VIAs partiellement formés. Des travaux et analyses supplémentaires sont nécessaires.

Sécurité du LED-PUF

Mille weak LED-PUFs ont été simulés, chacune avec une réponse de 512 bits. La publication [86] indique les métriques basiques pour les deux modèles (weak et strong). Une évaluation supplémentaire introduit le *guesswork*, un coefficient estimant la probabilité pour l'adversaire de prédire les bits de sortie. Cela se rapproche de l'estimation de l'entropie ; en l'occurrence les auteurs pondèrent la taille de réponse avec le *guesswork* pour déduire la taille de clef de sécurité équivalente. Les résultats obtenus par les auteurs sur les weak LED-PUFs simulées sont :

- Uniformité de 46,26 % (déviation non indiquée)
- Unicité de 50,3 % avec une déviation standard de 2 %
- *Guesswork* de 0.998 par bit

Le modèle strong DPUF est construit avec le hachage SHA-256, couplé avec les LED-PUFs simulés :

- Unicité de 50 % avec une déviation de 3 %
- *Guesswork* de 0.91 par bit

Coût et performance du LED-PUF

L'étude se focalise sur la surface, le circuit est synthétisé pour une technologie CMOS 65 nm :

- 3,24 μm^2 pour un bit de réponse (coût de surface de la cellule de lecture d'un DSA-VIA)
- 415 μm^2 pour générer une clef de 128 bits

La surface n'est pas évaluée pour le strong LED-PUF ; les auteurs indiquent toutefois leurs motivations pour une implémentation SHA-256 de 5 000 GE (portes logiques équivalentes) nécessitant deux entrées de 256 bits pour les vecteurs initiaux. Cela impose l'intégration d'un LED-PUF de 512 bits de sortie. Nous estimons les surfaces requises en technologie 65 nm :

- 1 660 μm^2 pour la partie weak LED-PUF
- 7 200 μm^2 pour le hachage (1 GE est approximée à 1,44 um^2 en technologie 65 nm)
- 8 860 μm^2 au total pour générer une clef de 256 bits
- 34,61 μm^2 par bit de réponse

Conclusion

Le procédé de fabrication est innovant et compatible pour des technologies avancées (65 nm). Les travaux du LED-PUF se limitant à des simulations, une étude supplémentaire est cependant requise pour estimer la robustesse et la faisabilité. Le modèle weak LED-PUF offre en théorie un niveau de sécurité acceptable et un coût de surface réduit. Selon les auteurs la surface requise est inférieure aux PUFs concurrents : 415 μm^2 au lieu de 600 pour l'implémentation la plus légère du SRAM-PUF. L'intégration de fonctions de hachage pour le modèle strong LED-PUF nécessite un coût supplémentaire ; la surface est multipliée par un facteur 10. Il faut 34,61 μm^2 par bit de réponse au lieu de 3,24. En outre, nous pouvons argumenter que cette proposition se rapproche d'un modèle weak PUF classique, complété par des fonctions de sécurité en aval pour des clefs secondaires à partir de la clef maitresse. Le strong LED-PUF se confronte ainsi aux problématiques similaires : la fonction de hachage couplée avec le DPUF doit être sécurisée et si la réponse « weak DPUF » initiale est dévoilée l'ensemble du cycle de vie est compromis.

3.5.3 CNT-PUF

Introduction

Les CNT-PUFs se construisent avec des nanotubes de carbone (*CNT pour Carbon Nanotubes)*. Ces dernières années (2016 à 2019) des publications ([87], [88], [89]) de différentes équipes démontrent la faisabilité de structures aléatoires avec des nanotubes de carbones. Les articles présentent une estimation de l'aléa obtenus et proposent des circuits d'extraction pour implémenter des modèles DPUFs. Des variantes *weak* et s*trong* sont proposées et partiellement évaluées.

Fabrication des structures aléatoires

Le procédé de fabrication des structures en nanotube de carbone se catégorise aussi en mécanisme DSA (auto assemblage). Les tubes sont projetés sur la couche de silicium et établissent un contact électrique après l'opération d'isolation. La 1ère étude [95] identifie la configuration adéquate pour provoquer une fermeture aléatoire des contacts. Le comportement des tubes est simulé en fonction de la densité, du diamètre et de l'alignement géométrique. Les résultats aboutissent à un paramétrage permettant la fabrication de structure aléatoire, il faut toutefois noter un état intermédiaire pour les points de contact, nommé *semi-conducting*. Les publications [95] et [89] proposent des mécanismes basés sur des dépassement de seuils de tensions pour exploiter ces états intermédiaires ; et construire un modèle DPUF plus complexe, disposant d'une entropie plus forte.

Circuit d'extraction des réponses

Les trois études référencées développent diverses gammes de circuits. Le premier cas [95] est un modèle weak DPUF classique avec un circuit de lecture simple de la grille de connexions. L'article le plus récent [89], datant de 2019, spécifie un mécanisme de sélection de tension. Les auteurs nomment ce modèle CNT-FET (*Field Effect Transistor*). L'état de la connexion varie selon cette tension et selon l'état du point de contact du tube de nano-carbone. Le choix de tension est considéré comme un « challenge » qui influe sur la connectivité de la structure et donc sur la réponse extraite par le circuit. Cela reste toutefois limité, le nombre de tensions possible est réduit (entre 4 et 6).

Les chercheurs de l'université du Michigan [88] proposent un modèle strong DPUF, composé de deux modules. Premièrement, un circuit de lecture simple est intégré avec un CNT-PUF classique. En entrée un challenge indique l'adresse des rangées de contacts qui seront lues. Un système de Lorenz est ensuite ajouté en aval du circuit : un système mathématique chaotique avec des opérations qui renforcent l'aléa et la diffusion des informations. L'article détaille les propriétés et les paramètres de ce modèle. L'architecture reste toutefois similaire à un modèle *weak PUF étendu*. Un circuit est implémenté, en complément de la structure aléatoire, pour dériver un espace de réponses plus larges.

Robustesse des CNT-PUFs

Les études supposent une forte robustesse des CNT-PUFs sans toutefois réaliser une évaluation approfondie tel que pour le VIA-PUF. La structure évaluée dans la 1ère étude, (qui comporte environ 200 points de contact), reste stable sous température de 85°C ; des tests additionnels sont requis pour assurer la robustesse. Nous exprimons aussi des craintes pour les mécanismes à sélection de tension en entrée du circuit. L'étude se limite à des simulations ; or les tensions internes du circuit peuvent être fortement sensibles aux conditions environnementales.

Sécurité des CNT-PUFs

La 1ère expérimentation [95] porte sur un échantillon réduit, une structure weak CNT-PUF de dimension 64x40, soit 2560 bits. L'analyse de sécurité fournit des résultats corrects :

- Uniformité de 49,53 %
- Unicité de 50 % avec déviation de 0.39 % pour une segmentation de la structure en clés de 64 bits.
- Succès des tests du NIST

Pour le strong CNT-PUF avec le système de Lorenz, l'évaluation se réserve à l'estimation de la résistance du modèle à des méthodes d'apprentissage. Les résultats valident l'intérêt de la couche supplémentaire : avec le système de Lorenz le coefficient de prédiction de l'adversaire se réduit à 53,45% par bit. A contrario, pour un CNT-PUF sans protection, ce coefficient est estimé à 100% : le modèle d'apprentissage réussit à déterminer l'état des connexions de l'ensemble de la structure CNT.

Coût et performances des CNT-PUFs

La publication [88] indique des coûts de surface pour les deux modèles étudiés ; la variante weak DPUF simple et la variante avec sélection des tensions d'entrée (CNT-FET). Dans le 2ème cas, plusieurs bits sont générés au niveau du nœud de connexion. Les surfaces déclarées par les auteurs sont :

- 18,6 μm^2 par bit pour le weak CNT-PUF
- 6,36 μm^2 par bit pour le CNT-FET

Conclusion

Les CNT-PUFs présentent un fort potentiel au regard des résultats et recherches actuelles concernant la fabrication des structures aléatoires. Outre les études référencés plusieurs autres travaux se concentrent sur le sujet. Toutefois, nous notons un manque d'évaluation et d'assurance pour la robustesse.

Autre point bloquant, les études sont peu précises sur les coûts de surface. Cela limite les comparaisons avec les autres modèles DPUF. Par ailleurs l'appréciation du strong CNT-PUF avec système de Lorenz est délicate sans évaluation de surface.

3.5.4 SD-PUF

Introduction

Les chercheurs J. Miao, M. Li, S. Roy et B. Yu proposent le 1er modèle DPUF qualifiable en « strong DPUF » [88]. L'architecture superpose avec la structure aléatoire matérielle un réseau logique qui interconnecte les nœuds de connexion, formant un bloc logique où une séquence de bit, appliquée en entrée de la structure, qui se diffuse à travers la structure. Les auteurs introduisent le terme « digital » pour caractériser ce modèle. Une évaluation approfondie les métriques de sécurité ainsi que les coûts de surface. Une 2ème publication [81] détaille une intervention supplémentaire dans l'étape de fabrication : une opération de permutation de structures DPUF pour répondre à des menaces du cycle de vie.

Fabrication des structures aléatoires

Le procédé exploite les variations locales induites dans la projection du masque sur la couche de silicium. Les lignes d'interconnections du masque de gravure sont positionnées à la limite de la distance lithographique nécessaire pour former la continuité électrique. Au cours de la lithographie les jonctions seront formées entre les pistes électriques selon divers paramètres (écart des pistes, valeur de dosage). Une étude approfondie est réalisée pour établir la probabilité de connexion en fonction de ces paramètres.

Les auteurs spécifient une cellule logique composée d'un double inverseur. Dans la Figure 32, un des inverseurs est volontairement biaisé pour forcer la sortie de la cellule si la connexion est coupée. Dans le cas contraire, le signal en entrée est transmis et son état logique simplement inversé. Cette structure permet de convertir le statut des nœuds de connexion en information binaire.

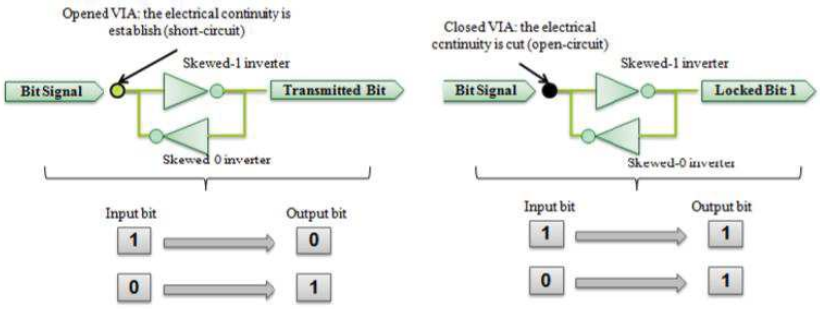

Figure 32: Double inverseurs biaisé pour le traitement des nœuds de connexion [88]

Circuit d'extraction des réponses

Le circuit d'extraction est constitué d'un réseau de fonctions logiques XOR qui mixe une séquence de bit avec les cellules logiques à doubles inverseurs. Chaque cellule logique se couple avec des portes XOR. Dans la Figure 33, cette porte XOR prend en entrée la sortie des inverseurs et un bit d'information de la séquence. La sortie des inverseurs dépend elle-même d'un autre bit d'information de la séquence, transmis ou non selon l'établissement de la connexion (cf Figure 32).

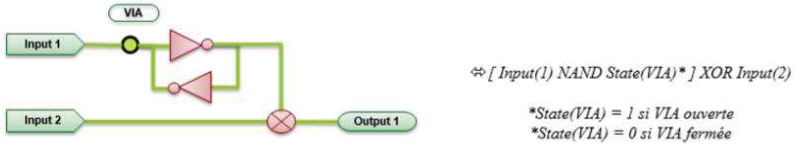

Figure 33: Représentation logique de la combinaison entre une porte XOR et la cellule double inverseur

L'architecture globale se présente sous la forme d'une grille organisée en colonne de cellules ; une configuration simple, de dimension 4 x 4 (4 colonnes, composées de 4 cellules) est schématisée dans la Figure 34. La séquence de bits en entrée du réseau est transmise de colonne en colonne. Chaque colonne mixe la séquence à son entrée avec l'état des nœuds de connexion. La séquence en entrée du réseau est alors considérée comme un challenge dont les bits se diffusent à travers la grille ; en sortie une séquence sous le même format peut être lue comme réponse du *digital PUF*. Avec cette architecture, la taille des paires challenge réponse est égale à la hauteur de la grille. Cela implémente ainsi un modèle *strong DPUF* : le réseau logique offre un espace challenge réponse qui s'accroit exponentiellement avec la

hauteur de grille. Dans la Figure 34, avec une hauteur de colonne à 4 cellules l'espace CRP est de taille 2^4 . Doubler la hauteur de colonne augmente exponentiellement l'espace CRP à 2^8.

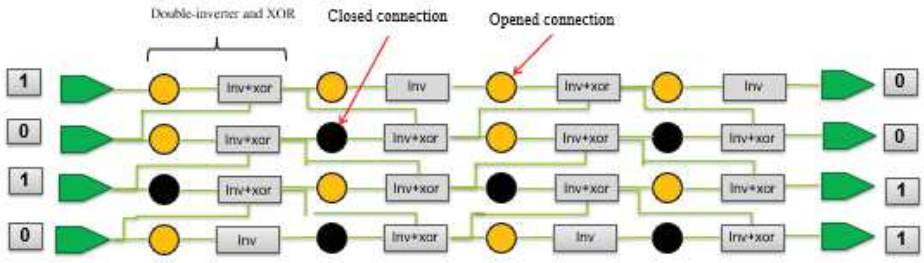

Figure 34: Réseau logique XOR pour un modèle strong DPUF

Les publications ([80], [81]) détaillent les propriétés de cette architecture ainsi que l'expression des opérations logiques. Les auteurs énumèrent quatre affirmations :

1. *Le modèle DPUF – réseau logique XOR combiné avec la structure matérielle de connexion aléatoire – est non-linéaire.*
2. *L'unicité des structures matérielles est aisément assurée avec une taille adéquate, y compris en cas de probabilité de connexion déséquilibrée.*
3. *L'accroissement du nombre de colonne augmente la résistance du modèle contre les méthodes d'apprentissage.*
4. *Toute modification de l'état des connexions se répercute sur la sortie du DPUF, c.à.d. le modèle assure une bonne diffusion.*

Extension du modèle : le Spliced Digital PUF

Dans la deuxième publication [81] les auteurs proposent une intervention supplémentaire au cours de la fabrication. Au lieu d'instancier une seule structure DPUF, un ensemble de *N* structures est généré par un masque puis réarrangé par une opération de permutation. L'objectif est de réduire les effets de corrélations : les auteurs craignent que pour un masque donné les variations qui influent sur l'état des connexions se reproduisent de plaque en plaque. Des structures pourraient ainsi présenter des similarités. Le mécanisme de permutation permet de réduire cet effet.

Robustesse du SD- DPUF

Les structures DPUFs ont été simulées avec le logiciel SPICE [81] avec une configuration adéquate pour générer des connexions aléatoires pour deux probabilités : 20% et 90%. Des conditions environnementales sont testées par le simulateur, des variations de températures de -20°C à 100°C et des variations de tensions de 0.7V à 1.2V. La distance IntraPUF est estimée à 0%.

Sécurité du modèle strong DPUF

Les auteurs fournissent une évaluation des métriques de base pour les deux modèles, le strong DPUF classique avec réseau logique XOR et la variante avec le mécanisme de permutation de structure. Ils étudient aussi la résistance des DPUFs à des méthodes par apprentissage : les machines à vecteur de support, les réseaux de neurones artificiels et les forêts aléatoires. L'analyse montre que la configuration de la structure aléatoire influe fortement sur les métriques. L'unicité baisse pour des grilles de tailles réduites, ainsi que pour des probabilités de connexion plus faible. La même conclusion est établie pour la résistance aux méthodes d'apprentissage. Les auteurs évaluent le modèle strong DPUF avec des grilles de dimensions 8 x 8 et 64 x 64. Pour la $2^{ème}$ dimension (64 x 64), le DPUF obtient :

- Uniformité de 50% avec déviation de 6,25%.
- Unicité de 50% avec déviation de 0,1%.

- Coefficient de prédiction entre 48 et 50% pour les méthodes type forêts aléatoires et type réseau de neurone artificiel.
- Coefficient de prédiction entre 48 et 50% pour les méthodes type machine à vecteur de support, si la probabilité de connexion est supérieure à 20%.
- Coefficient de prédiction supérieur à 60 % pour les méthodes type machine à vecteur de support, si la probabilité de connexion est inférieure à 20% ; la performance de l'attaque s'élève à 95% de prédiction pour une faible probabilité de connexion (1%).

Le modèle strong DPUF, avec mécanisme de permutation des structures, présente des résultats similaires pour l'unicité et l'uniformité ; le coefficient de prédiction des méthodes SVM reste faible (inférieur à 60%) sous réserve d'un dimensionnement suffisamment élevé de l'ensemble de l'architecture.

Cette approche souffre d'une limite en terme de diffusion. Les opérations logiques combinent uniquement des bits d'information voisins dans la grille. La diffusion se réduit encore plus si la probabilité de connexion est faible ; un nœud de connexion fermé ne transmet pas le bit de la séquence à la colonne suivante. Les auteurs argumentent que le DPUF avec une grille 8 x 8 présente un effet d'avalanche correct, sous réserve d'une probabilité de connexion de 90%. Toutefois, aucune évaluation de la diffusion n'est réalisée pour les dimensions plus élevées (64 x 64). Une analyse supplémentaire est requise pour estimer les contraintes de configuration à respecter pour obtenir une diffusion suffisante.

Coût et performance

La surface nécessaire pour le réseau logique XOR a été estimée pour une structure de taille 64 x 64. Les auteurs ont implémenté l'architecture avec la librairie en accès libre *NanGate*, en nœud 45 nm.

- 13 034 µm2 de surface pour un DPUF 64 x 64, retournant des réponses de 64 bits.
- 204 µm2 par bit de réponse.

Conclusion

L'analyse du modèle SD-PUF montre des performances élevées pour les métriques de sécurité basique – unicité et uniformité – et également une résistance face à certaines attaques par méthodes d'apprentissage, sous réserve d'une configuration de structure adéquate (en terme de dimension et de probabilité de connexion).

L'évaluation ne considère toutefois qu'un seul dimensionnement du circuit, sans approfondir le compromis entre les coûts d'implémentation des fonctions logiques et les métriques de sécurité. En outre, une faiblesse subsiste en terme de diffusion pour le modèle, du moins pour les paramètres de configuration évalués.

3.6 Bilan et perspective des recherches sur les DPUFs

La littérature offre des modèles DPUFs variés, dont la construction et les propriétés reposent sur des procédés divers. La primitive VIA-PUF est la plus avancée ; l'architecture a été complètement intégrée et la robustesse évaluée selon des métriques standardisées. Cela nous assure une reproductibilité forte des réponses, que ce soit face à des conditions extérieures dures, ou face aux vieillissement des circuits. Nous constatons des limites à l'exploitation du VIA-PUF. Le procédé de fabrication des structures aléatoires souffre d'une incertitude, des écarts dans la probabilité de connexion se répercutent sur la qualité de l'aléa. Le circuit d'extraction compense cette défaillance, mais accroit le coût en surface. Le VIA-PUF nécessite 8 225 μm^2 par bit de réponse pour un nœud technologique de 135 nm. Pour les autres modèles DPUFs, les coûts de surfaces estimés sont bien plus réduits, 204 μm^2 par bit de réponse pour le SD-PUF (45 nm), 34 μm^2 pour le LED-PUF (65 nm) et 18 μm^2 pour les CNT-PUFs. Les études sur ces architectures concurrentes ne vérifient pas la robustesse avec des critères aussi stricts que pour le VIA-PUF. La stabilité des structures matérielles devrait être évaluée pour les même contraintes.

Globalement, la probabilité de connexion est un enjeu déterminant de la conception d'un modèle DPUF. Un déséquilibre de la répartition des états ouverts / fermés des nœuds de connexion doit être compensé soit par le circuit d'extraction (cas du VIA-PUF), soit par un accroissement de la taille de la structure (cas du SD-PUF). Ces premières publications montrent la nécessité d'évaluer les configurations de structures et de circuits d'extraction ensemble.

Les modèles DPUFs se catégorisent essentiellement en *weak PUF,* les circuits extraient une seule et unique réponse de la structure aléatoire. Cela inclut aussi le « strong » LED-PUF, la fonction de hachage exploite en fait l'unique réponse obtenue par la lecture des états des DSA-VIAs. Nous portons notre attention sur l'architecture du SD-PUF, où la structure de connexions aléatoires se superpose avec une grille de cellules logiques interconnectées. Une séquence de bits appliquée en entrée de la grille peut se diffuser à travers la structure. Cela forme un bloc logique cohérent, compact et répondant aux critères d'un modèle strong PUF classique : accroissement exponentiel de l'espace de réponse par une augmentation linéaire de la structure. Dans ce modèle, les fonctions logiques intégrées dans le réseau ont un rôle primordial, influant sur les propriétés mathématiques des réponses. Cela alourdit toutefois le coût d'implémentation et la surface requise. Optimiser l'architecture et déterminer un compromis entre surface et sécurité, est une question clé de la conception d'un strong DPUF efficace et sécurisé.

Tableau 6 : Bilan des résultats de la littérature DPUF

	VIA-PUF [84]	**LED-PUF** [92]	**CNT-PUF** [89]	**SD-PUF** [93]
Modèle	Weak	Strong	Weak	Strong
Nœud technologique	130 nm	65 nm	X	65 nm
Métriques de sécurité				
Uniformité moyenne (0.50) *Déviation standard (<0.15)*	**49.72 %** *2.05 %*	**X** *(supposée correcte ~ 50 %)*	**49.53 %** *X*	**50 %** *6.25 %*
Unicité moyenne (0.50) *Déviation standard (<0.15)*	**49.99 %** *2.05 %*	**50 %** *3 %*	**50 %** *0.39 %*	**50 %** *0.1 %*
Diffusion	X	X	X	X
Métrique de performance				
Aire pour générer une réponse (μm^2) *Aire par bit (* $\mu m^2/bit$)	**1 053 800** *8 225*	**4 430** *34,61*	**2380.8** *18,6*	**13 034** *204*
Latence	30 ms	X	X	X
Energie consommée	0.645 pJ/bit	X	X	X

4 Circuit d'extraction pour un *strong PUF :* proposition et description du modèle SPN (Substitution-Permutation-Network)

Comme vu précédemment, les DPUFs sont de bons candidats pour sécuriser à faible coût un système au long du cycle de vie. Il est toutefois nécessaire de coupler ces primitives avec des circuits d'extraction permettant d'optimiser leurs performances et d'assurer leurs propriétés de sécurité.

La première section formalise les motivations pour la conception d'un strong DPUF, motivations préalablement abordées au cours de l'état de l'art en section 3.4.3. En particulier, un strong DPUF répond au besoin d'authentification induit par la multiplicité des interactions et des acteurs au cours du cycle de vie. En outre, la robustesse inhérente d'un *digital PUF* assure aussi une fiabilité qui est impérative. Cette partie formalise aussi les objectifs en termes de sécurité et de coût de surface. Ce compromis coût / sécurité impose des contraintes sur la configuration du circuit.

La deuxième section approfondit les contraintes de sécurité pour le circuit d'extraction ; présentant les réflexions et les arguments pour concevoir un DPUF efficace. Nous rappelons les faiblesses du réseau XOR utilisé dans le premier modèle de strong DPUF (SD-PUF [81]), déjà discutées dans la section 3.5.4. La diffusion de l'information transmise dans ce circuit est restreinte et n'atteint le niveau exigé que par une configuration contraignante du modèle. Cela amène à rechercher des schémas mathématiques renforçant les propriétés de diffusion du mécanisme challenge-réponse du strong DPUF. Un intérêt particulier est porté sur les travaux de cryptographie légère, notamment les schémas *SPN (Substitution-Permutation Network)* de la primitive PRESENT [94]. La section se termine par une discussion de l'impact de l'intégration des SBOXs dans le circuit.

Dans la troisième section, une architecture basée sur un schéma SPN est proposée comme candidate pour un circuit d'extraction sécurisé et efficace. Ce modèle, issu des réflexions de la section précédente, couple la structure aléatoire avec un réseau logique constitué d'opérations XOR, substitution et permutation. Les opérations de substitution et permutation réalisées entre les colonnes de nœuds de connexions, accroissent les propriétés de diffusion et de confusion du circuit. L'architecture est nommée SPN-DPUF (Substitution-Permutation Network for Digital PUF). Plusieurs configurations sont possibles pour la couche de diffusion du circuit, notamment des variantes sans substitution afin d'apprécier l'intérêt de cette opération pour le compromis coût / sécurité. Ce modèle de circuit instancie un strong DPUF, le réseau diffuse un challenge dans la structure matérielle aléatoire et retourne une réponse dépendant dudit challenge et de l'état des nœuds de connexion.

La quatrième section termine le chapitre par des remarques sur les enjeux et les difficultés de la conception d'un strong DPUF. En particulier, il est nécessaire de réaliser une optimisation de la configuration des paramètres du SPN-DPUF pour valider les métriques de sécurité tout en limitant la surface du circuit d'extraction et les contraintes sur le process de fabrication.

4.1 Motivations et Objectifs

4.1.1 Motivations pour un Strong DPUF intégré

Le modèle strong PUF est un support matériel efficace pour un protocole d'authentification au cours de cycle de vie (1.3.2, 2.3.3). Le PUF assure l'authenticité du matériel et l'unicité des signatures utilisées dans le protocole. Ces propriétés sécurisent le protocole contre l'usurpation ou la contrefaçon. Dans le cas d'un strong PUF, la taille et la capacité d'extension de l'espace de réponses offre en plus la possibilité de distribuer un nombre conséquent de clés de sécurité. Chaque acteur peut ainsi disposer de clés qui lui sont réservées. Avec une conception adéquate, les risques de collisions ou de similarités entre les clés sont faibles. Des fonctions additionnelles sont envisageables pour la suppression ou la création des accès au circuit : la révocabilité des clés ou la génération d'une base supplémentaire au cours du cycle de vie. Cela permet une gestion sûre et efficace des droits d'accès, flexible selon les requêtes des acteurs.

L'utilisation d'un *weak DPUF,* tel que le modèle VIA-PUF (section 3.5.1), nécessite un couplage avec des fonctions de dérivation de clés ou des fonctions de hachage. Cela alourdit le coût et complexifie le protocole. Par ailleurs, cela implique de considérer certains besoins de sécurité spécifique. En effet, le circuit du weak DPUF génère une seule et unique réponse, utilisée pour dériver des clés de sécurité au cours du cycle de vie. Le circuit réalise une extraction directe du statut des nœuds de connexions de la structure aléatoire. L'information détaillée sur les statuts de connexions transite dans le circuit et est transférée au bloc matériel qui dérive les clés de sécurité. Une attaque invasive ou une analyse de canaux auxiliaires, en sortie du weak DPUF ou en entrée du bloc de dérivation, peut extraire cette information. Cela pourrait compromettre la sécurité de l'ensemble cycle de vie ; car celle-ci repose entièrement sur l'unique réponse du DPUF. A l'opposé, un strong DPUF génère de multiples clés, gage de la sécurité de différentes opérations au cours du cycle de vie et liées à différents acteurs. L'impact de la compromission d'une clé peut être limité à l'opération et l'acteur associés. Nous notons toutefois que par effet rebond cela peut impacter les biens d'autres acteurs ou perturber les phases suivantes du cycle.

A contrario, pour compromettre complètement le strong DPUF, un attaquant doit extraire les statuts de connexions, information qui dans ce modèle n'est présente qu'à l'intérieur du bloc matériel DPUF et est mixée avec le réseau logique. L'accès à cette information est restreint – « camouflée » dans le circuit logique qui extrait les réponses – et nécessite une intrusion ou une analyse fine de la couche matérielle. C'est un bénéfice supplémentaire pour la sécurité du cycle de vie dans le contexte de notre cas d'usage.

La première motivation pour un strong DPUF porte sur sa capacité à répondre aux besoins d'authentification (par la génération de multiples clés) et ce avec un niveau de sécurité élevé.

Le PUF doit aussi assurer la sécurité tout au long du cycle de vie et ce sous diverses conditions environnementales. Cela impose des contraintes de robustesse : les réponses doivent être reproductibles malgré les effets du vieillissement sur le circuit ou malgré les perturbations induites par les variations de températures, d'humidité ou du bruit électromagnétique. Une pompe à insuline est utilisée jusqu'à cinq ans, voir plus dans certains cas (huit ans pour les produits de *Medtronic* [95]). A minima, une contrainte de durée de vie de six ans peut être imposée. Il est donc nécessaire de prendre en compte les effets du vieillissement pour la conception du PUF. A titre d'exemple, les SRAM-PUFs proposés par *Intrinsic ID* subissent des tests simulant des vieillissements de quatre ans [96]. Malgré des performances honorables, le modèle SRAM-PUF nécessite néanmoins un post-traitement pour corriger les réponses.

Un strong digital PUF offre une robustesse inhérente qui, potentiellement, soustrait le PUF à l'impératif d'intégrer des blocs correcteurs. La reproductibilité des réponses est assurée à un très haut niveau (jusqu'à un taux d'erreur abaissé à 10^{-8} et sous conditions extrêmes pour le VIA-PUF [84]). Un tel modèle répond aux contraintes de fiabilité du cycle de vie du dispositif, tout en assurant les propriétés de sécurité des PUFs traditionnels.

La deuxième motivation pour un strong DPUF porte sur sa robustesse inhérence qui assure la fiabilité du protocole d'authentification qui sera déployé au cours du cycle de vie.

L'état de l'art (section 3.5) démontre la faisabilité et le succès de ces primitives. Des études complémentaires indiquent aussi une résistance des strong DPUFs aux attaques par apprentissage [80]. Cela motive nos travaux pour proposer une nouvelle architecture performante et optimisée, notamment en termes de dimension et de schéma d'extraction. Cela permettrait de répondre de façon optimale au compromis sécurité / coût.

4.1.2 Objectifs pour la conception du circuit d'extraction

Les travaux portent sur la conception d'un circuit d'extraction efficace et sécurisé pour un strong DPUF. La littérature prouve a faisabilité et la robustesse de structures aléatoires et ce par l'exploitation

de l'un des procédés de fabrications identifiés (section 3.5). Dans ce contexte, les objectifs concernent l'optimisation du circuit d'extraction et de ses propriétés de sécurité; avec la nécessité de considérer diverses configurations de structures aléatoires (en termes de tailles et de distributions des nœuds de connexions). Le circuit conçu doit respecter les exigences de sécurité établies en section 3.2.2 et un certain niveau de performances (3.2.3). Des cibles sont définies pour ces métriques, tant vis-à-vis des exigences générales discutées pour les PUFs traditionnels que vis-à-vis des évaluations des DPUFs existants. L'objectif final est de proposer des modèles de DPUFs assurant de meilleurs résultats que ceux de la littérature. Les exigences de sécurité pour la conception du strong DPUF incluent les métriques de base : uniformité et unicité, auxquelles nous ajoutons la diffusion (requise pour un partage de réponses entre de multiples acteurs), la min-entropie et le taux de succès aux tests d'aléa (type NIST). Cet ensemble de métriques couvre les propriétés de sécurité essentielles des PUFs, établissant une première assurance de leur capacité à générer des signatures ou des clés cryptographiques correctes. Les critères seront évalués sur les réponses générées en sortie du strong DPUF et ciblent *idéalement* :

- Uniformité à 0.50 (+/- 0.001) avec déviation inférieure à 0. 15.
    - Pour rappel, le SD-PUF atteint ces objectifs, pour une taille de structure 64x64.
    - L'uniformité est plus faible pour les autres DPUFs (jusqu'à 0.51 pour le VIA-PUF) Il faut toutefois noter que cela suffit pour valider le premier test d'aléa du NIST.
- Unicité à 0.50 (+/- 0.001) avec déviation inférieure à 0. 15.
    - La plupart des DPUFs respectent cette exigence, avec des déviations parfois extrêmement basses (< 0.01).
- Coefficient d'avalanche (diffusion) à 0.50 (+/- 0.001) avec déviation inférieure à 0. 15.
    - La métrique est peu évaluée dans la littérature, notamment car une partie des propositions sont des weak DPUFs qui ne génèrent qu'une seule réponse.
- Min-entropie de 128 bits à 0,998 près par bit.
    - Cette exigence est respectée par les modèles weak DPUFs du VIA-PUF et LED-PUF.

Une min-entropie de 128 bits implique de facto une taille de réponses, à minima, de 128 bits et contraint le dimensionnement du strong DPUF. Ces exigences de taille et de qualité d'aléa sont imposées pour les clés de sécurité. Il faut noter que certains standards cryptographiques acceptent des clés de 96 bits, voir 64 bits, pour les cas d'usage fortement contraints en ressources. Toutefois, ce compromis abaisse le niveau de sécurité et est fortement contre-indiqué pour des applications sensibles.

Après ces exigences de sécurité, le deuxième objectif est l'optimisation des performances du circuit d'extraction, en particulier la réduction des coûts de surface. Cet enjeu est délicat à apprécier car il est spécifique à chaque cas d'usage et aux contraintes de ressources auxquelles ce cas se confronte. Un cadre comparatif peut être établis avec les DPUFs de la littérature, ainsi qu'avec les références proposant des supports matériels pour la sécurité du cycle de vie. Toutefois, la comparaison avec les surfaces des weak DPUFs manquent de pertinence. En effet, leur usage diffère, une seule réponse est générée et des fonctions de dérivations doivent être intégrée accroissant la surface. Les comparatifs retenus sont :

- Le SD-PUF avec un circuit d'extraction à base d'un réseau XOR, dont la surface est estimée pour une technologie en 45nm (avec *NanGate,* librairie libre d'accès)
    - 204 μm^2 par bit soit 26 000 μm^2 pour générer des réponses de 128 bits
- Le LED-PUF avec un circuit d'extraction intégrant une fonction de hachage, la surface est calculée en 65 nm avec une estimation du coût du hachage.
    - 34 μm^2 par bit soit 4 352 μm^2 pour générer des réponses de 128 bits
    - Il faut toutefois noter que ce modèle dérive d'un weak DPUF et expose l'information des nœuds de connexion en entrée du hachage
- La solution de sécurité [14] basée sur une plateforme de débogage personnalisée intègre un strong PUF dont la surface est estimée avec une librairie technologique 45 nm (*NanGate)*
    - 22 335 μm^2 pour un *Arbiter PUF* avec des réponses de 64 bits, soit potentiellement 44 670 μm^2 pour des réponses de 128 bits.

Idéalement, le coût de surface obtenu doit être en dessous des comparatifs identifiés.

4.2 Schémas mathématiques pour un circuit d'extraction sécurisé

4.2.1 Avantage et limite de l'existant : le réseau XOR du SD-PUF

Le premier modèle strong DPUF s'appuie sur un réseau XOR superposé à la structure aléatoire [93] que nous avons détaillé au préalable en section 3.5.4. Ce réseau se compose de cellules élémentaires représentées dans la Figure 35 (a) qui mixent les sorties de nœuds de connexions et les bits d'un challenge – soumis en entrée de la structure - par des opérations XORs. Dans la Figure 35 (b) le modèle générique se présente comme une grille de nœuds de connexions, organisée en rangées et colonnes, où la couche logique XOR s'intercale entre chaque colonne. Cela déploie ainsi un mécanisme challenge-réponse et instancie un modèle « strong » tel que défini par les critères de classification. L'architecture XOR génère un large espace de réponses et celui-ci s'accroit exponentiellement avec le nombre de rangées.

Le réseau XOR apporte plusieurs avantages forts pour la sécurité, argumentés par ses auteurs [93]. La cellule élémentaire permet de conserver l'uniformité (c.à.d. une répartition idéale entre les états « 1 » et « 0 » des bits d'informations transmis dans le circuit). Précisément, dans la Figure 33 (a), si une des deux entrées du XOR est uniforme, alors la sortie l'est aussi. De fait, si le challenge en entrée est uniforme, le réseau assure l'uniformité en sortie et ce quel que soit le taux de connectivité de la structure. Aussi, avec le couplage des doubles inverseurs, l'équivalent logique est une opération NAND entre le bit d'entrée et le statut de la connexion. Cela établit une opération non-linéaire et renforce le circuit d'extraction comme les méthodes d'analyses linéaires.

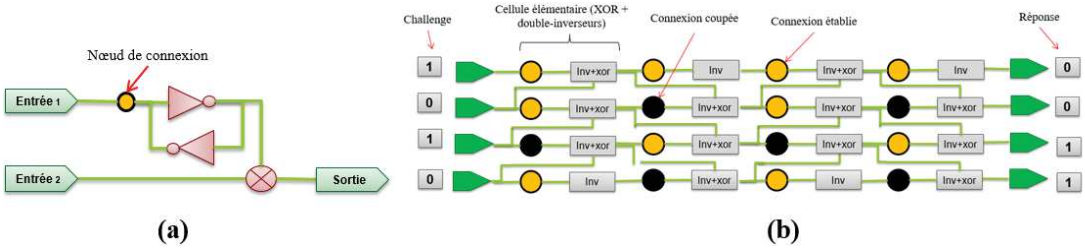

Figure 35: Réseau XOR pour un strong DPUF (a) Opération élémentaire (b) Architecture complète

Les études publiées [93] pointent l'influence de la configuration sur les métriques de sécurité : la diffusion s'accroit avec le taux de connectivité ; la résistance à la prédiction (par méthode d'apprentissage) augmente pour des tailles de structures plus élevées. Sans que cela soit énoncé par les auteurs, les résultats montrent que la diffusion s'accroit aussi avec le nombre de colonnes de la structure : chaque colonne supplémentaire permettant une diffusion à une rangée de plus.

Une faiblesse est toutefois constatée dans ce type de réseau: la diffusion est restreinte. L'information n'est transmise qu'à une rangée d'écart au plus à chaque colonne et ce sous réserve que la connexion soit établie. Un constat évident porte sur la contrainte de taille, la distance maximale de diffusion est définie par le nombre de colonne : une modification d'un bit de challenge en position i se répercute sur les bits qui sont à moins de X positions de celui-ci dans la réponse, où X est le nombre de colonnes. L'étude existante n'estime la diffusion que pour un cas extrême, une grille 8x8 et un taux de connectivité élevé. Le coefficient d'avalanche n'est pas évalué pour les dimensions supérieures.

Ces affirmations sont approfondies dans l'évaluation des circuits, où nous estimons la diffusion du réseau XOR pour diverses configurations. Cette question est primordiale, une forte diffusion doit être assurée pour atténuer le risque de prédiction de réponses et de constructions de fausses paires par un acteur ou un adversaire ayant accès à une partie de la base de réponses. Au vue de l'architecture XOR,

la diffusion peut être augmentée mais cela a un coût : l'augmentation de la structure en nombre de colonne (et donc une surface supplémentaire) et l'accroissement du taux de connectivité.

4.2.2 Apport des travaux en cryptographie légère pour le renforcement de la diffusion

Nous estimons l'architecture XOR comme un modèle pertinent qui peut potentiellement remplir les objectifs de sécurité et de performances. Nous recherchons toutefois une amélioration ou une rectification pour ce schéma mathématique afin de respecter les exigences de diffusion. En cryptographie la diffusion est considérée comme une propriété fondamentale. Plusieurs travaux étudient les opérations mathématiques et les algorithmes qui renforcent cette propriété. De nombreuses évaluations, notamment pour les primitives de cryptographie légère, tiennent comptent spécifiquement des contraintes de ressources et de performances ([97], [98] et [99]). On peut rapprocher ces travaux des enjeux de conception du strong PDUF où un compromis sécurité / coûts est impératif.

L'article [98]présente et évalue les opérations élémentaires qui améliorent la confusion et la diffusion dans les schémas de chiffrement. La confusion est une autre propriété requise pour les primitives de sécurité, tout aussi importante pour un strong PUF. Elle traduit la complexité de la relation entre l'entrée et la sortie de la primitive, c.à.d. celle entre un challenge et la réponse pour un strong PUF.

- La diffusion est apportée par des opérations soit à l'échelle du *bit,* soit à l'échelle du *nibble* (bloc de quatre bits). Au niveau du bit nous avons les rotations et les permutations, à l'échelle du niddle nous avons les décalages de colonnes et les mixages de colonnes. La plus pertinente est la permutation, au niveau matériel il s'agit d'un simple réarrangement des lignes métalliques.
- La confusion se renforce avec l'opération arithmétique ADD (addition), l'opérateur booléen AND ou avec des SBOXs (table de substitution) de dimensionnement 4x4 (quatre bits en entrée, quatre bits en sortie). Nous portons un intérêt sur les SBOXs car ces tables améliorent aussi la diffusion ; leur conception respecte notamment l'effet d'avalanche ([100], [101])

La combinaison de permutations et substitutions est présente dans plusieurs schémas cryptographiques, notamment pour le chiffrement ; la dénomination courante emploie l'expression *Substitution-Permutation-Network (SPN)* – réseau de substitutions et de permutations. L'algorithme de chiffrement PRESENT [94], employé aujourd'hui, se base sur un schéma SPN avec des SBOXs 4x4. La primitive est conçue pour chiffrer des blocs de données de 64 bits et ce avec des clés de sécurité de 80 bits ou 128 bits. Cela réduit la surface de silicium requise pour l'implémentation et permet de respecter les exigences de cas d'usage contraints en ressources. Pour PRESENT le schéma inclut 31 itérations de la couche SP, représentée dans la Figure 36, celle-ci se constitue d'une substitution 4 bits par 4 bits et d'une permutation sur 64 bits. La permutation échange des bits jusqu'à une « distance » de 48 positions dans le bloc de données traité. Ainsi, la couche SP, intercalée entre deux séquences d'opérations XORs, diffuse efficacement toute modification en entrée de la primitive. L'approche pour renforcer la diffusion du réseau strong DPUF est d'intégrer une couche similaire entre les colonnes de cellules élémentaires. Cette couche de diffusion est adaptée au dimensionnement de la grille de connexion, et peut comporter une permutation et / ou une substitution.

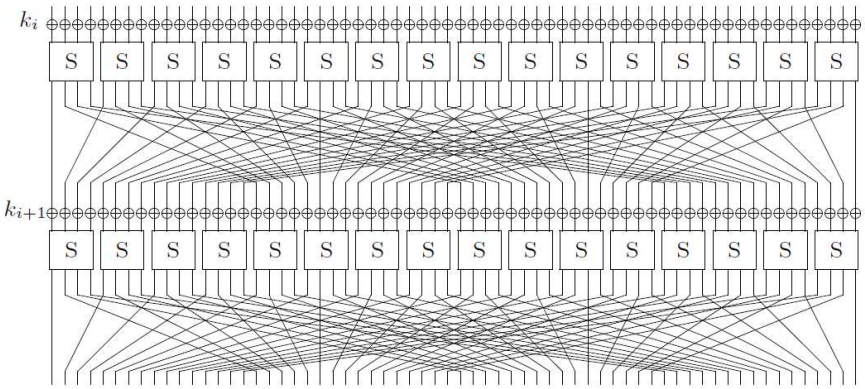

Figure 36: Couche Substitution - Permutation de PRESENT [94]

4.2.3 Problématique de l'intégration des SBOXs

La couche logique proposée pour renforcer la diffusion comporte une opération de substitution. Celle-ci substitue un nombre par des valeurs de références fixées et prédéterminées ; généralement stockées dans des tables appelés SBOXs. Ces valeurs résultent d'étude mathématiques et visent à respecter des propriétés tel que la diffusion. Une des premières description des SBOXs [101] en 1970 rappelle deux objectifs fondamentaux pour les primitives cryptographiques : la complétude et l'effet d'avalanche. La complétude traduit le fait que chaque bit de sortie dépend de tous les bits d'entrée. L'effet d'avalanche consiste en l'assurance que la modification d'un bit en entrée modifie (en moyenne) la moitié des bits de sortie. L'étude de 1970 [101] présente la combinaison de ces deux propriétés comme l'effet d'avalanche stricte : chaque bit de sortie est modifié avec une probabilité de 50 % si un seul bit d'entrée est modifié quel qu'il soit. Les SBOXs sont élaborées de manière à obtenir cette propriété ; en l'occurrence pour cette étude [101] les auteurs déterminent les SBOXs de taille 4x4 qui respectent cette contrainte et la réversibilité (nécessaire pour permettre le déchiffrement). Une analyse détaillée plus récente [102] classifie toutes les SBOXs selon des critères de sécurité avancés tel que la résistance à la cryptanalyse linéaire et différentielle. Ce sont ces SBOXs prédéterminées qui intègrent les schémas SPNs, la Figure 37 montre les valeurs de substitutions de la SBOX 4x4 de PRESENT.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Figure 37: SBOX 4x4 de PRESENT

Toutefois, utiliser cette opération de substitution dans la couche de diffusion du circuit DPUF nécessite l'intégration de SBOXs et implique un coût supplémentaire en surface. Les concepteurs de PRESENT [94] avertissent que la substitution occupe une part importante des ressources dans les implémentations matérielles cryptographiques. Plusieurs études ([102], [103]) optimisent ce coût pour les SBOXs de dimension 8x8, notamment pour l'algorithme de chiffrement AES. La version simple consiste à intégrer des LUTs (*Look-Up-Table*), des registres contenant les valeurs de substitution. Des variantes existent ; l'implémentation de la substitution peut être réalisée avec de la logique combinatoire. Une des intégration de SBOX 8x8 les plus légères [104] aboutit à un coût final de 228 portes logiques (ou *GE pour Gate Equivalent,* la métrique généralement utilisée pour chiffrer le coût d'implémentation). Toutefois cette surface est trop élevée pour des cas d'usage contraints en ressources. Pour PRESENT les concepteurs s'orientent vers les SBOXs 4x4 pour abaisser les coûts ; leur étude [94] indique un chiffre de 28 portes logiques pour une SBOX 4x4. Nous privilégions ainsi une couche de diffusion basée sur les SBOXs 4x4 pour le circuit d'extraction du DPUF .

Un des enjeux de conception du circuit d'extraction est l'estimation du coût supplémentaire induit par les SBOXs 4x4 et de leur intérêt pour la sécurité du strong DPUF. Si la substitution renforce la diffusion dans le circuit cela pourrait être toutefois trop coûteux pour certains cas d'usage. Il apparaît judicieux de modéliser et évaluer différentes configurations, avec ou sans SBOXs. Cela permettra de choisir les paramètres optimums pour concevoir un strong DPUF adapté au cas d'usage. En fonction des besoins de sécurité ou des contraintes de coûts, les jeux de paramètres adéquats pour le circuit d'extraction du DPUF seront déjà prédéterminés, ainsi que les estimations de coûts associés.

En vue d'identifier la configuration idéale du circuit d'extraction, nos propositions de schémas mathématiques sont élargies à plusieurs variantes pour la couche de diffusion. Cela amène à étudier ainsi plusieurs configurations possibles pour la couche de diffusion.

4.3 SPN-DPUF : réseau de substitutions et permutations pour un strong DPUF

4.3.1 Schéma et équation logique de la couche de diffusion

Le circuit d'extraction proposé est inspiré du réseau logique XOR [93], avec des cellules élémentaires composés d'une structure à double inverseurs et d'une porte XOR, tel que décrites en section 4.2.1. Nous intégrons dans le circuit une couche de diffusion constitué d'une opération permutation et d'une opération substitution avec SBOXs 4x4. La Figure 38 schématise l'intégration de cette couche entre deux colonnes de nœuds de connexion. Des SBOXs 4x4 substituent la sortie des XORs, puis une permutation réarrange en sortie des SBOXs la séquence binaire.

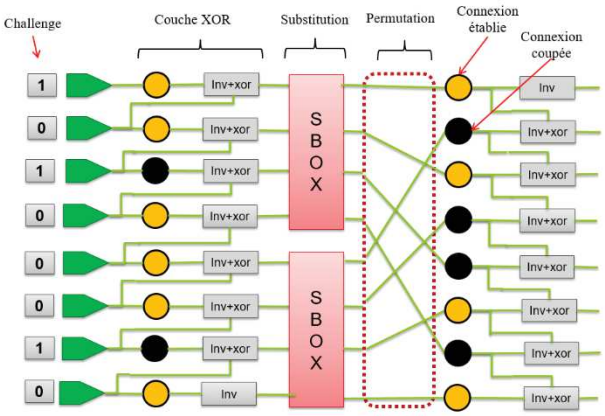

Figure 38: Couche de diffusion dans le réseau SPN

La couche de diffusion se compose ainsi de trois sous-couches logiques distinctes : la « colonne » XOR, la substitution et la permutation. Ces couches sont respectivement nommées X_{layer}, S_{layer} et P_{layer}. La couche X_{layer} alterne le sens de diffusion des bits transmis, selon la parité de la colonne la structure est reliée en entrée soit avec le bit de rangée supérieure soit avec celui de rangée inférieure. En bordure de grille la structure ne reçoit qu'un seul signal d'entrée et est simplifiée (pas de XOR). La couche S_{layer} se compose des tables SBOXs 4x4 utilisées pour substituer les bits transmis en sortie des portes XORs. La dernière couche, P_{layer}, implique simplement le réarrangement des lignes métalliques pour permuter les signaux. Les bits sont alors transmis à la colonne logique suivante dans le réseau du DPUF.

Par la suite, nous étudions un réseau SPN basé sur ces trois couches logiques. Il existe plusieurs modèles de SBOX 4x4 ou de permutations. Nos choix se portent sur les modèles utilisés pour PRESENT car ceux-ci sont conçus pour assurer des propriétés de sécurité. La SBOX 4x4 de PRESENT (figure 35)

est définie et évaluée pour respecter les critères de confusion et de diffusion. En ce qui concerne la permutation celle-ci disperse les 4 bits de sorties des SBOXs 4x4 « équitablement » sur l'ensemble de la séquence de bit transmis. La couche de diffusion ainsi composée est intégrée entre chaque colonne des nœuds de connexion.

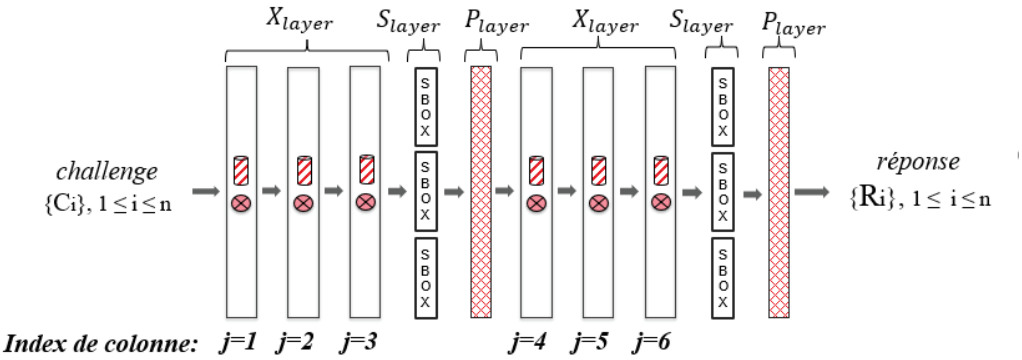

Figure 39: Schéma des couches logiques du circuit d'extraction SPN-DPUF

Soit un DPUF avec une grille de nœuds de connexion répartis en *m* colonnes et *n* rangées, nous formalisons les expressions logiques des couches avec les notations suivantes :

- l'état des nœuds de connexion est noté $v_{i,j}$ avec *i* indiquant la rangée et *j* la colonne.
- $v_{i,j} = 0$ si la connexion est coupée, $v_{i,j} = 1$ si la connexion est établie.
- Les *n* bits du challenge soumis au DPUF sont notés c_i avec *i* la position du bit.
- Les bits transmis dans le circuit SPN, en sortie des couches logiques, sont notés $r_{i,j}$ avec *i* indiquant la rangée et *j* la colonne ; $r_{*,j}$ désigne la séquence complète des bits transmis en sortie des couches.

A chaque colonne de nœuds de connexion l'expression des bits transmis est :

$$(1)\quad r_{*,j} = P_{layer}(S_{layer}(X_{layer}(r_{*,j-1}))$$

La couche X_{layer} est définie, avec $x_{i,j}$ le bit en sortie de la couche, par l'expression suivante:

$$(2)\quad x_{i,j} = \begin{cases} (v_{i,j} \text{ NAND } r_{i-1,j-1}) \text{XOR } r_{i,j-1}\,, & \text{si } j \text{ impair} \\ (v_{i,j} \text{ NAND } r_{i+1,j-1}) \text{XOR } r_{i,j-1}\,, & \text{si } j \text{ pair} \end{cases}$$

$$\text{avec } r_{i.0} = c_i \text{ et } r_{0.i} = r_{n+1.i} = 0$$

La couche P_{layer} est définie, avec $p_{k,j}$ le bit en sortie de la couche, par l'expression suivante :

$$(3)\quad p_{k,j} = s_{i,j}$$

$$\text{avec } k = (i-1) mod[4] * \frac{n}{4} + trunc(\frac{i-1}{4}) + 1 \text{ ; } \textit{(« trunc » opérateur de troncature)}$$

La couche S_{layer} est définie, à l'échelle du *niddle* (bloc de 4 bits) avec $s_{i,j}$ le bit en sortie de la couche et $SBOX_4$ la table de qui substitue le *niddle*, par l'expression suivante :

$$(4)\quad s_{i,j} = SBOX_4\,(x_{[i-i\ mod[4]+1, i-i\ mod[4]+4],j})_{i\ mod[4]+1}$$

$$\textit{avec la contrainte de taille } n = 0\ mod[4], \textit{c.à.d. le challenge doit être un multiple de } 4$$

Les couches de diffusion intégrées successivement entre chaque colonne de la grille de nœuds de connexion forment un réseau SPN. Cette couche logique implémente un mécanisme challenge-réponse, un challenge peut être soumis à ce circuit, et une réponse retournée dépendant de l'état des connexions de la structure matérielle, instanciant un strong DPUF.

Ce modèle de couche de diffusion impose des contraintes sur la taille de la colonne de nœuds de connexion, c.à.d. aussi sur le nombre de rangées de la grille de nœuds de connexion. Cela est induit par les spécificités des opérations logiques sur lesquelles reposent le réseau SPN :

- Le nombre de rangées doit être égal à la taille des paires de challenge-réponse (CRP), en l'occurrence pour 128 bits (taille des clés de sécurité) cela impose 128 rangées.
- Le nombre de rangées (et donc la taille des CRPs) doit être un multiple de la taille des SBOXs, en l'occurrence un multiple de 4 pour des SBOXs 4x4.
- Le modèle de permutation choisi impose aussi un nombre de rangées multiple de 4, cela peut toutefois être adapté.

En ce qui concerne le nombre de colonnes ou le taux de connectivité ce modèle n'implique pas de contraintes particulières.

Plusieurs configurations restent toutefois possibles pour le nombre de colonnes, il est également envisageable de réduire la couche de diffusion pour limiter le coût de surface supplémentaire. D'une part la couche de diffusion peut être réduite en terme d'opération, et éventuellement n'être intégrée que pour un nombre réduit de colonnes.

4.3.2 Architecture SPN: Modélisation du réseau et paramètres de configuration

Le réseau logique SPN combiné avec la grille de nœuds de connexion aléatoire forme un strong DPUF, nous nommons cette primitive SPN-DPUF. Dans l'architecture SPN-DPUF plusieurs paramètres sont variables. La Figure 39 indique notamment les paramètres physiques de la structure matérielle aléatoire, la taille de la grille ainsi que la probabilité d'établissement de la connexion (ceux-ci ont déjà étaient énoncés en section 3.4.3 et en Figure 25: Modélisation de la structure matérielle d'un DPUF) :

- Le nombre de rangées de nœuds de connexion dans la grille
- Le nombre de colonnes de nœuds de connexion
- La répartition des connexions ouvertes et fermées (éventuellement simplifiée en « taux de connectivité »)

Les dimensions de la grille sont aisément configurables au cours de la spécification des masques de gravure. Les concepteurs doivent simplement tenir compte des contraintes sur le nombre de rangées énoncées en 4.3.1 : multiple de quatre pour être compatible avec l'opération de substitution, suffisamment grand pour obtenir une taille adéquate de paires de challenge-réponse. La probabilité d'établissement de la connexion dépend de la méthode de fabrication choisie, elle est parfois sujette à une variabilité peu maitrisable. Plusieurs paramètres physico-chimiques interviennent en effet selon le processus de fabrication. La loi de probabilité obtenue peut être complexe ; dans notre travail de modélisation du circuit SPN nous simplifions cette problématique en considérant une probabilité de connexion uniforme. Cette variable est assimilable à un simple taux de connectivité.

En ce qui concerne le circuit d'extraction, nous disposons d'une marge de manœuvre sur la spécification et l'intégration de la couche de diffusion substitution-permutation. Premièrement nous considérons la possibilité de limiter le mécanisme de diffusion à une des deux opérations seulement. Cela offre trois configuration distinctes pour la couche de diffusion :

- substitution et permutation combinées (modèle **SPN**)
- restreinte à la substitution (modèle **SN**)
- restreinte à la permutation (modèle **PN**)

Deuxièmement, nous introduisons la notion d'itération pour la couche de diffusion, c.à.d. la fréquence des opérations substitution-permutation dans la grille. L'intégration de celles-ci peut être limitée à un certain nombre de colonnes. Nous considérons une itération régulière des opérations entre les colonnes et nous nommons ce paramètre d'itération « sp ». Nous conservons les opérations XORs à chaque colonne, nécessaires pour mixer l'aléa de la structure matérielle avec les bits diffusés dans le réseau. Nous précisons l'expression logique des bits transmis entre chaque colonne du DPUF, dans le cas d'une couche substitution-permutation :

Soit une architecture SPN-DPUF, avec couche de diffusion substitution-permutation, $r_{*,j}$ désignant la séquence complète de bits transmis en sortie des couches à la colonne *j* et *sp* le paramètre d'itération:

$$(5)\quad r_{*,j} = \begin{cases} X_{layer}(r_{*,j-1}), & \text{si } j \bmod [sp] \neq 0 \\ P_{layer}(S_{layer}(X_{layer}(r_{*,j-1}))), & \text{si } j \bmod [sp] = 0 \end{cases}$$

La Figure 39 indique ces deux paramètres supplémentaires, spécifiques au circuit d'extraction sont configurables indépendamment de la grille de connexions. Cela nous amène à un total de cinq paramètres configurables pour le modèle de strong DPUF :

1) nombre de rangées de la grille de nœud de connexion
2) nombre de colonnes de la grille de nœuds de connexion
3) taux de connectivité de la grille
4) niveau d'itération de la couche de diffusion (paramètre nommé ***sp***)
5) type de couche de diffusion (SPN, SN ou PN)

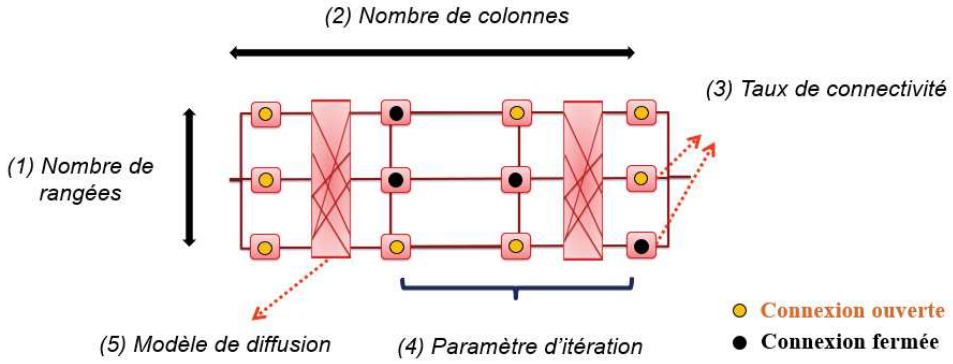

Figure 40: Architecture SPN-DPUF et paramètres variables

4.4 Enjeu et difficultés de la configuration du circuit d'extraction du SPN-DPUF

En vue de respecter les objectifs de sécurité (aléatoire, unicité, diffusion…) il est nécessaire d'intégrer un circuit d'extraction avec une configuration adéquate. L'étude des paramètres énoncés précédemment est primordiale, ceux-ci ont un impact direct sur le coût du DPUF. La taille de la grille et l'ajout d'opérations logiques accroissent la surface requise pour le circuit. La question critique porte notamment sur la nécessité d'intégrer ou non l'opération de susbtitution, les SBOXs ayant un coût conséquent (point abordé en section 4.2.3). Toutefois le circuit doit respecter les critères de sécurité définis en section 4.1.2, une confusion et une diffusion suffisante, ainsi que des dimensions minimums pour générer des réponses de 128 bis d'entropie. Le schéma SPN permet d'atteindre ces objectifs, toutefois une évaluation et une étude d'optimisation sont nécessaires pour identifier une configuration idéale offrant un compromis sécurité-coût-performance.

En ce qui concerne le taux de connectivité, la conception du DPUF se confronte à deux problématiques : la flexibilité de ce paramètre et les contraintes à respecter vis-à-vis des besoins de sécurité. La flexibilité dépend essentiellement de la méthode de fabrication choisie. Dans le cas du VIA-PUF (section 3.5.1, [84]), la probabilité de connexion varie de nœud en nœud ; pour une même dimension de VIA la probabilité de formation est fortement instable, variant de 40 à 60 %. De fait, le taux de connectivité sur l'ensemble de la grille est difficile à maitriser. Cela implique d'évaluer la marge de manœuvre disponible pour configurer le processus de fabrication. En l'occurrence, des contraintes, ou à minima des objectifs, sont à considérer pour le taux de connectivité. L'étude du modèle SD-PUF souligne par exemple le besoin d'augmenter le taux de connectivité, cela accroit le coefficient d'avalanche (métrique de diffusion). Un taux à 90 % assure une forte diffusion ainsi qu'une résistance aux méthodes par apprentissages, et ce sans compromettre les autres métriques de sécurité (uniformité, unicité, aléa). Une conséquence du faible contrôle sur ce paramètre est la nécessité de prévoir une configuration adéquate. Celle-ci compensera les éventuels biais dans les bits d'informations extraits des nœuds de connexion ; assurant ainsi les objectifs liés aux métriques de sécurité.

Une étude préalable de la configuration du SPN-DPUF est essentielle pour répondre aux contraintes de coûts des circuits intégrés. Le prochain chapitre se focalise sur l'évaluation des paramètres du SPN-DPUF pour identifier la solution optimale.

5 Evaluation Sécuritaire des Circuits d'Extraction

L'objectif de ce chapitre est l'identification d'une solution optimale pour la configuration du circuit d'extraction des « strong digital PUFs ». Cela implique premièrement de vérifier que les configurations étudiées répondent aux exigences de sécurités des PUFs. Entre autres, l'évaluation doit estimer les métriques de base : unicité, uniformité et diffusion (définies dans la section 3.2.2). Ce bilan de sécurité peut être complété par des indicateurs supplémentaires, notamment ceux définis par les suites de tests du NIST pour les nombres aléatoires. Aussi, la solution doit permettre de limiter le coût en surface du « strong digital PUF ». Diverses configurations doivent être évaluées et comparées selon les différents paramètres du « strong digital PUF ». Cela implique la comparaison des métriques de sécurité entre chaque configuration de paramètre.

Ce chapitre présente l'évaluation et l'analyse des métriques de sécurité pour les modèles *substitution-permutation* (SPN) proposés précédemment comme circuit d'extraction pour un « *Strong Digital PUF »*. L'étude s'appuie sur une plateforme de modélisation développée à cet effet, permettant d'estimer les métriques de sécurité des PUFs pour différentes configuration de circuit d'extraction.

La première section décrit les outils de modélisation et d'analyse développés pour l'évaluation des circuits d'extraction. Ces outils simulent des challenges-réponses de *Strong Digital PUF* pour diverses configurations de circuits. Le cadre méthodologique est précisé, détaillant les fonctions de calcul des métriques mais aussi les intervalles d'études des paramètres du circuit. L'étude indique les hypothèses acceptées, notamment celle sur la probabilité de l'état ouvert / fermé des nœuds de connexions des Digital PUFs.

Les deuxième et troisième sections présentent les résultats des calculs des indicateurs de base – uniformité et unicité – réalisés grâce à la plateforme de simulation et d'évaluation. L'étude pointe l'influence des paramètres sur les métriques de sécurité. Les métriques sont estimées à la fois pour les modèles SPN *(Substitution-Permutation-Network)* mais aussi pour le premier schéma *Strong Digital PUF* à base de réseau de XORs. Une première conclusion confirme le niveau de sécurité de ces modèles en terme d'unicité et d'uniformité, validant les travaux de la littérature sur les strong digital PUFs.

La quatrième section se focalise sur la problématique de diffusion, détaillant l'incidence de la configuration sur le coefficient d'avalanche. Cette troisième métrique est déterminante, son évaluation pointe la sensibilité de la diffusion aux choix de configuration. L'analyse du niveau de diffusion est complexe, les paramètres du modèle ont tous une influence sur les résultats. Une première phase d'étude déroule étape par étape l'impact du choix du modèle, du taux de connectivité et du nombre de colonne. Cela discrimine les effets de la variation de chaque paramètre sur les réponses générées. Les résultats valident le constat, déjà argumenté en section 3.5.4, de l'inefficacité du modèle XN pour assurer une bonne diffusion. En outre, l'étude montre la capacité des nouveaux modèles proposés (SPN, SN et PN) à renforcer la diffusion ; justifiant l'intérêt d'optimiser et d'implémenter ces modèles pour une extraction sure et efficace des réponses DPUFs.

La cinquième section approfondit l'analyse des métriques de diffusion pour les modèles PN et SPN, notamment en vue de réduire le nombre de colonnes de la primitive PUF. Le paramétrage spécifié de chaque configuration est étudié et évalué. Des compromis entre taux de connectivité et niveau d'itération des opérations substitution-permutation sont identifiés, permettant de respecter efficacement les objectifs de diffusion.

5.1 Méthodologie de l'évaluation de sécurité

5.1.1 Hypothèse pour la modélisation des DPUFs

Les structures aléatoires des DPUFs – les grilles de nœuds de connexions ouverts / fermés – dépendent de la technologie de semi-conducteur et du procédé de fabrication choisis. Ceux-ci impactent les spécificités des structures notamment en termes de coût et d'aléa des structures. Comme argumentés dans les sections précédentes (4.1.2 et 4.4) cela se répercute sur le coût et la sécurité du circuit d'extraction. L'évaluation du circuit doit donc prendre en compte les paramètres des structures aléatoires. Pour notre étude, nous acceptons la simplification suivante : *il existe un procédé de fabrication qui permet de produire des structures aléatoires dont l'état des nœuds de connexions respecte une loi de probabilité uniforme.* L'étude considère ainsi comme seul paramètre un taux de connectivité identique pour chaque nœud de connexion des structures aléatoires.

Ces grilles de nœuds de connexions peuvent être assimilées à des matrices d'états. Dans ces matrices l'état de la connexion serait noté 1 pour une connexion établie, 0 pour une connexion interrompue. Les schémas logiques du circuit d'extraction et les matrices d'états représentants les structures aléatoires peuvent être aisément implémentés par des outils de modélisation mathématique. Cela permet de simuler les réponses d'un strong digital PUF pour diverses configurations et ainsi rechercher la solution optimale répondant aux objectifs d'évaluation.

5.1.2 Plateforme de modélisation et d'évaluation

Une plateforme de modélisation et d'évaluation a été réalisée pour identifier les jeux de paramètres les plus pertinents pour le circuit d'extraction des DPUFs. Les figures 41 et 42 schématisent deux premières chaines de traitement, une pour la simulation de l'extraction des réponses, une autre pour l'évaluation des métriques d'uniformité et d'unicité. La chaine de simulation se compose de trois fonctions qui génèrent les espaces de chalenge-réponse associés à telle ou telle configuration de DPUF :

- Une fonction de génération de challenge prenant en entrée l'effectif et la taille de challenge souhaités
- Une fonction de génération de matrices d'états **1** et **0** représentants les grilles de nœuds de connexion. Cette fonction prend en entrée la dimension des grilles (nombre de colonnes et de rangées), le taux de connectivité, et l'effectif de grilles souhaité.
- Une fonction de simulation qui prend en entrée des espaces de challenges et de grilles préalablement générés, ainsi qu'une configuration de strong digital PUF complètement définie (nombre de colonnes et de rangées de la grille de nœud, taux de connectivité des nœuds, modèle de diffusion pour le circuit d'extraction et niveau d'itération de la couche de diffusion), et génère les réponses associées à cette configurations et à ces challenges.

Cette fonction de simulation s'appuie sur une librairie contenant des implémentations, purement mathématiques, des schémas d'extraction : modèle **SPN,** modèle **SN,** modèle **PN** et modèle **XOR.** Au cours de la simulation les contraintes (définies en section 4.3.1 sont vérifiées : l'égalité entre le nombre de rangée et la taille des paires de challenge réponses, et l'exigence que le nombre de rangée soit un multiple de quatre pour les modèles **SPN, PN et SN.** En outre, les fonctions de génération s'appuient sur les fonctions internes *rand()* pour produire des séquences de bits ayant un aléa suffisant.

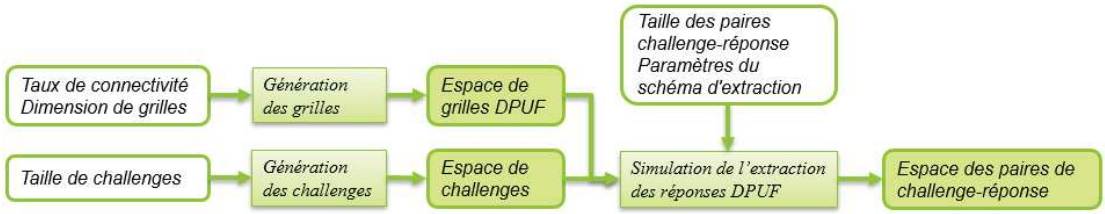

Figure** 41**: Chaine de simulation de l'extraction des réponses DPUF

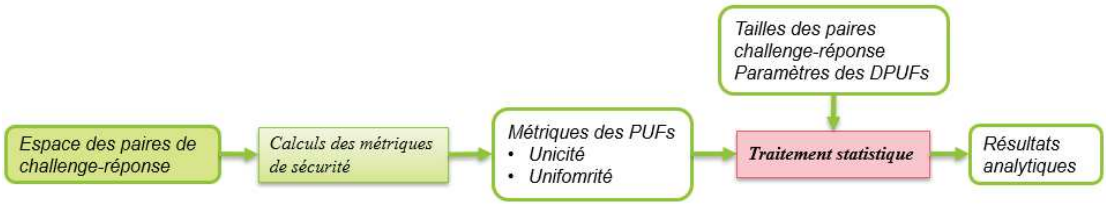

Figure 42: Chaine d'évaluation des métriques de sécurité (uniformité et unicité)

La chaine d'évaluation en Figure 42 se compose de deux modules pour produire les résultats finaux estimant la performance des configurations des circuits d'extraction :

- Un calculateur de métriques de sécurité, prenant en entrée les paires challenge-réponse, et déterminant pour chacune l'uniformité et l'unicité, selon les formules en section 3.2.2 :
  - Calcul de la distance inter-PUF pour chaque challenge, (c'est à dire des distances entre les réponses, pour un même challenge, par paire de PUF)
  - Calcul du ratio de 1 et 0 pour chaque réponse de chaque PUF à chaque challenge
- Un traitement statistique, avec estimation des moyennes et des coefficients de variance pour les deux métriques, et comparaison entre les paramètres de configurations.

Pour évaluer les propriétés de diffusion des DPUFs, notamment avec les métriques de coefficient d'avalanche définies en section 3.2.2, il est nécessaire de soumettre des challenges spécifiques en entrée des DPUFs simulés. Pour rappel, le coefficient d'avalanche est la distance de Hamming entre des réponses du DPUF pour des paires de challenges *distants de 1 bit*. Un mode dit *diffusion* est intégré pour les fonctions de génération et d'évaluation de la plateforme. Sous ce mode, pour chaque challenge généré, un deuxième est généré différent d'un seul bit dont l'index est spécifié en entrée de la fonction de génération. Cela implique les modifications suivantes :

- Ajout du paramètre *index du bit de diffusion* pour la fonction de génération des challenges.
- Ajout de la commande d'activation du mode *diffusion* pour la fonction de génération de challenges et de simulations des réponses.

La fonction de calcul du coefficient d'avalanche évalue les deux formes de la métrique :

- La version dite *simple*, la distance de Hamming par paire de réponses sur l'ensemble de leur séquence de bits retournés, analysée ensuite au cours du traitement statistique par sa moyenne et son coefficient de variance.
- La version dite *stricte*, énoncée en section 4.2.2, qui consiste à estimer la probabilité pour chaque bit de sortie d'être modifié pour la modification d'un seul bit en entrée. Idéalement cette probabilité doit tendre vers 50 %. Pour cela la fonction calcule la fréquence de modification des bits de sortie à chaque position de bit des réponses.

Cette plateforme permet d'analyser les performances des configurations de DPUFs. La figure 43 illustre la mise en œuvre de celle-ci pour générer des paires de challenge-réponse de DPUF pour plusieurs valeurs de taux de connectivité et analyser son influence sur les métriques de sécurité. Trois

espaces de paires challenge-réponse sont générés pour un schéma d'extraction **SPN** (substitution-permutation), chacun des trois espaces est associé à des grilles de nœuds de connexion ayant un taux de connectivité différent : 25 %, 50 % et 75 %. La dimension des gilles (128x64) et le niveau d'itération de la couche de diffusion sont fixés. Seul l'influence du taux de connectivité sur les métriques de sécurité est évaluée.

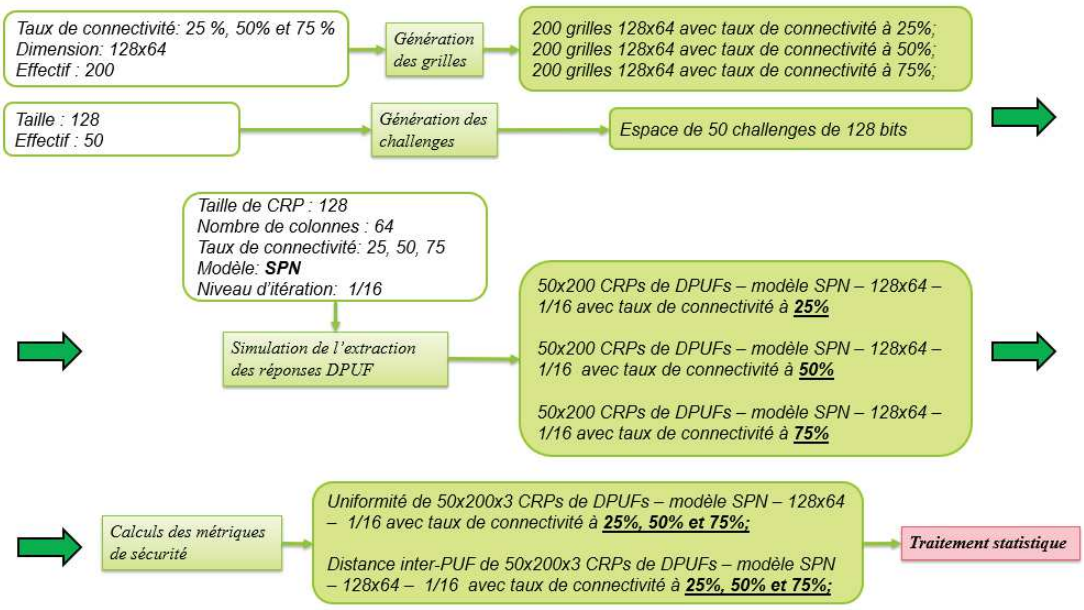

***Figure* 43*: Exemple d'évalua*tion pour un modèle SPN**

5.1.3 Estimation de l'effectif nécessaire pour le traitement statistique

Tout traitement statistique requiert des échantillons de test suffisamment importants en effectif. Ces contraintes d'effectif varient selon le contexte d'étude et la confiance exigée. En préambule des analyses sur l'influence des paramètres du circuit d'extraction, une première évaluation porte donc sur l'estimation des effectifs nécessaires. Ces contraintes concernent à la fois les effectifs des DPUFs modélisés et les effectifs des challenges générés. Des métriques de sécurité ont été calculées pour plusieurs niveaux d'effectifs. Un niveau minimum requis a été identifié : 30 challenges et 50 DPUFs. Au-dessus de cet effectif les résultants ne varient pas au-delà de 0.001, l'exigence d'approximation définie pour les objectifs de sécurité.

La Figure 44 illustre l'impact des effectifs sur la distance inter-PUF moyenne. Dans le cas présenté la configuration du circuit est un modèle XN avec une grille de 128 rangée et 64 colonnes ; l'espace de challenge est fixé à un effectif de 30. Seul le taux de connectivité varie afin de vérifier si celui-ci influe sur le résultat du modèle XN. En l'occurrence, la métrique converge vers la valeur idéale – 0.50 – quel que soit le taux de connectivité et ce dès un effectif de quelques dizaines de DPUFs. Pour un effectif de 50 la métrique approche 0.50 à 0.001 près et 0.50 à 0.0002 près pour 100 DPUFs. Soumettre 30 challenges à des effectifs de 50 et de 100 DPUFs implique respectivement des espaces de 36750 et 148500 paires de challenges réponses. Ces effectifs dépassent ceux de la littérature DPUF :

- Pour le VIA-PUF ([83], [84]) les effectifs des deux études sont respectivement 119 et 405 puces, pour des réponses uniques de 128 bits.
- Pour le LED-PUF 1000 structures ont été simulées, générant des réponses uniques de 256 bits.
- La 1ère expérimentation d'un CNT-PUF [95] porte sur un échantillon réduit, une structure de dimension 64x40 générant 2560 bits, soit 20 réponses de 128 bits.

- Seule l'étude du SD-PUF, le modèle de référence pour un strong DPUF [81], se base sur un espace plus important, 100 000 paires de challenge réponse.

La plupart des analyses se basent par la suite sur des espaces de 30 challenges et de 50 DPUFs.

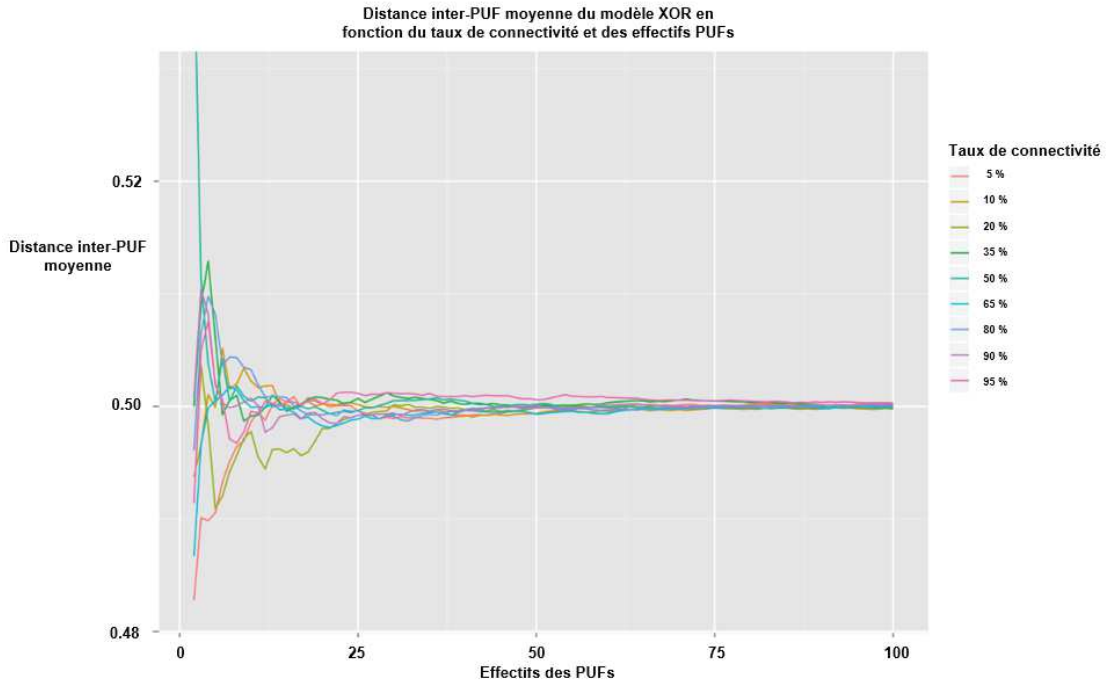

Figure 44: Distance inter-PUF du modèle XN en fonction des effectifs PUFs

5.1.4 Intervalle d'étude des paramètres DPUFs

L'étude a estimé les métriques de sécurité (unicité, uniformité, diffusion…) en priorité pour les intervalles de paramètres suivants :

- Nombre de rangées de la grille de nœuds de connexion : fixé à 128
- Nombre de colonnes de la grille de nœuds de connexion : 16, 32, 64, 128, 256
- Niveau d'itération : 1/2, 1/4, 1/8, 1/16, 1/32
- Taux de connectivité : 25 %, 50 % et 75 %

Nous fixons le nombre de rangées à 128, imposant une taille de challenge-réponse de 128 bits, la longueur minimale requise pour les clés de sécurité (exigence définie en section 4.3.1). Le nombre de colonnes spécifié est une puissance de deux, pour plusieurs raisons. D'une part, la première étude de strong DPUF dans la littérature s'appuie sur cette échelle (puissance de deux pour les colonnes), ainsi calculer les métriques de sécurité avec les mêmes configurations de grille permet une comparaison plus aisée des résultats. De plus, en cryptographie les tailles standardisées sont régulièrement en puissance de deux. Cela semble plus judicieux en vue d'anticiper des processus de standardisation ou d'évaluation qui imposeraient ce type d'échelle.

Une échelle avec puissance deux est aussi définie pour le paramètre d'itération de la couche de diffusion, cela permet d'échelonner avec cohérence les opérations de diffusion entre les colonnes.

5.2 Evaluation de l'uniformité

Une première étude évalue les moyennes et les déviations standard de l'uniformité des réponses des modèles DPUFs. Cette métrique représente les rations de 1 et 0 dans la séquence binaire extraite. Cette métrique permet de discriminer et éliminer des nombres non-aléatoires. Les standards du NIST pour les générateurs de nombres aléatoires [64] intègrent cette métrique dès le premier test (nommé *frequency monobit test*) et recommandent d'exclure tout nombre qui ne présente pas un ratio à minima de 47 %.

Dans le cadre de l'évaluation de sécurité des modèles DPUFs, des objectifs précis et plus élevés ont été définis en section 4.1.2 : idéalement l'uniformité des réponses doit avoir une moyenne proche de 0.50 à 0.001 près et une déviation standard inférieure à 0.15. Ces valeurs idéales sont rappelées par le tableau 7 présentant les calculs de l'uniformité des réponses simulées pour certaines configurations. Ces exigences pour le modèle DPUF correspondent aux résultats fournis dans la littérature DPUF.

Les moyennes et déviations standard ont été calculées à 0.0001 près pour les différents intervalles d'études de paramètres définis en section 5.1.4. Les effectifs des DPUFs simulées et des challenges générés sont respectivement de 50 et 30 tels que requis en section 5.1.3. La majorité des configurations fournissent des réponses caractérisées par un niveau d'uniformité correct. Les moyennes se situent entre 0.4980 et 0.5020, les déviations standard sont inférieures à 0.005. Le tableau 7 illustre cette bonne performance des modèles, il regroupe la série de résultats pour des grilles de 128 rangées et 16 colonnes, et un niveau d'itération de couche diffusion de 1/4 pour les modèles SPN, PN et SN. L'uniformité des réponses du modèle XN a des moyennes de 0.5000, 0.5002 et 0.4996 pour des taux de connectivité respectifs de 25, 50 et 75 %. Cela valide les études sur l'uniformité du schéma « XOR » du strong digital PUF de la littérature (SD-PUF). Le modèle PN se caractérise aussi par une forte uniformité, entre 0.4996 et 0.5001. Cela argumente en faveur de la capacité de ces schémas à extraire un aléa de qualité des grilles de nœuds de connexion, y compris pour des dimensions faibles (seulement 16 colonnes), et ce pour les trois taux de connectivités de référence.

Les modèles SPN et SN présentent des moyennes d'uniformité plus faibles, proche des contraintes : jusqu'à 0.4990 pour un circuit SPN et jusqu'à 0.4992 pour un modèle SN avec une connectivité de 50 %. Cela respecte toutefois les exigences requises, ces deux modèles conviennent également pour extraire l'aléa des grilles de nœuds de connexion.

Tableau 7 : Uniformité des modèles DPUFs avec des grilles 128x16 (et niveau d'itération ¼ pour les SPNs)

Métrique (idéale) \ Modèle • **Uniformité moyenne (0.50)** • *Déviation standard (<0.15)*	**Modèle XN**	**Modèle SPN**	**Modèle PN**	**Modèle SN**
Taux de connectivité = 25 %	**0.5000** *0.0039*	**0.5003** *0.0039*	**0.5001** *0.0039*	**0.5007** *0.0039*
Taux de connectivité = 50 %	**0.5002** *0.0039*	**0.4990** *0.0039*	**0.4996** *0.0039*	**0.4992** *0.0039*
Taux de connectivité = 75 %	**0.4996** *0.0039*	**0.5006** *0.0039*	**0.5001** *0.0039*	**0.5002** *0.0039*

5.3 Evaluation de l'unicité

Une deuxième étude se focalise ensuite sur les moyennes et les déviations standard de la distance inter-PUF des réponses simulées. Cette métrique est l'indicateur essentiel qui caractérise l'unicité des réponses et estimer la capacité du DPUF à assurer des propriétés d'authentification (3.2.2). Les calculs sont réalisés sur les mêmes espaces de paires challenges-réponses que pour l'analyse de l'uniformité de la section précédente. Les objectifs définis pour l'unicité des modèles DPUFs en section 4.1.2 sont identiques à ceux pour l'uniformité : idéalement la métrique – la distance inter-PUF – des réponses doit avoir une moyenne de 0.50 à 0.001 près et une déviation standard inférieur à 0.15. La présentation des distances inter-PUF dans le tableau 8 suit la même méthodologie que pour l'uniformité :

- Les valeurs idéales sont rappelées (moyenne de 0.5000 et déviation inférieure à 0.15)
- Les moyennes et déviations standard sont calculées à 0.0001 près
- Les effectifs sont de 50 grilles simulées et 30 challenges soumis en entrée.
- Les configurations prisent en exemple concernent des grilles de 16 colonnes, et un niveau d'itération de couche de diffusion de ¼ pour les modèles SPN, SN et PN.

Dans le tableau 8 la métrique pour le modèle XN a des moyennes de 0.4947, 0.5000 et 0.4997 pour des taux de connectivité respectifs de 25, 50 et 75 %. Cela témoigne de l'influence d'un faible taux de connectivité, dans le cas étudié (25 %) une baisse de la distance inter-PUF est constatée : moyenne estimée à 0.4947. L'unicité du modèle XN est vérifiée pour des nombres de colonnes différents. Pour 64 colonnes les moyenne se situent entre 0.4995 et 0.5005 ; pour 8 colonnes des différences sont constatées :

- 0.4687 pour une connectivité de 25 %.
- 0.4982 pour une connectivité de 50 %
- 0.5002 pour une connectivité de 75 %.

Cela conclut sur la nécessite pour un modèle XN de respecter des contraintes sur les paramètres physiques pour fournir une unicité convenable. A partir d'un faible nombre de colonnes il faut augmenter le taux de connectivité : 50 % pour 16 colonnes, 75 % pour 8 colonnes. En comparaison, les résultats dans le tableau 8 attestent d'un niveau d'unicité élevé plus stable pour les modèles SPN, SN et PN. Les moyennes se situent entre 0.4994 et 0.5005, les déviations standard estimées sont inférieures à 0.0445, et ce quel que soit le taux de connectivité. Les modèles SPN, PN et SN présentent des moyennes acceptables pour cette métriques pour des dimensions de grilles plus faibles (8 colonnes). Cela confirme la capacité de ces nouveaux schémas à extraire des réponses DPUFs uniques. Les résultats dans les tableaux 7 et 8 démontrent que – pour des configurations avec des grilles 128x16 et un niveau d'itération de 1/4 pour la couche de diffusion – les modèles SPN, PN et SN remplissent les objectifs d'uniformité et d'unicité.

Tableau 8 : Unicité des modèles DPUFs avec des grilles 128x16 (et niveau d'itération ¼ pour les SPNs)

Métrique \ Modèle • **Distance inter-PUF moyenne (0.50)** • *Déviation standard (<0.15)*	**Modèle XN**	**Modèle SPN**	**Modèle PN**	**Modèle SN**
Taux de connectivité = 25 %	**0.4947** *0.0444*	**0.5003** *0.0443*	**0.4994** *0.0440*	**0.5005** *0.0442*
Taux de connectivité = 50 %	**0.5000** 0.*0441*	**0.5005** 0.*0441*	**0.4998** 0.*0441*	**0.5000** 0.*0443*
Taux de connectivité = 75 %	**0.4997** *0.0444*	**0.4999** *0.0442*	**0.5001** *0.0445*	**0.4997** *0.0441*

5.4 Évaluation de la diffusion

5.4.1 Impact du choix du modèle

Cette partie détaille l'évaluation du coefficient d'avalanche des modèles d'extraction. Cette métrique caractérise la propriété de diffusion exigée pour les modèles *strong DPUFs*. La section 3.2.2 explicite la formulation de la métrique ainsi que les références scientifiques décrivant son usage et argumentant son intérêt. La section 4.2.3 rappelle le concept de la complétude, propriété de sécurité évaluée par le calcul de la variante stricte du coefficient d'avalanche : l'ensemble des probabilités de chaque bit de sortie d'être modifié pour la modification d'un seul bit en entrée. De même que pour l'uniformité et l'unicité les objectifs ciblent une moyenne du coefficient d'avalanche de 0.5000 à 0.001 près.

Une première série de résultat permet d'analyser l'impact du choix du modèle. Le coefficient d'avalanche des quatre modèles est calculé dans la Figure 45 pour une configuration fixée selon les paramètres suivants :

- Des espaces de 50 grilles et 30 paires de challenges.
- Les challenges de chacune des paires ont un bit de différence *(bit de diffusion)* dont l'index est spécifié en amont de la génération (*mode diffusion* voir la section 5.1.2)
- L'index du bit de diffusion est fixé à 64
- La dimension des grilles simulée est fixée à 128x64, le niveau d'itération pour les couches diffusion à 1/8 et le taux de connectivité à 50 %. Ce paramétrage a été privilégié car correspondant à la médiane des intervalles définis pour les paramètres.

Dans la figure 45 les nuages de points correspondent aux taux de modification pour chacun des bits de réponses, en fonction de leur position dans la réponse et en fonction du modèle choisi.

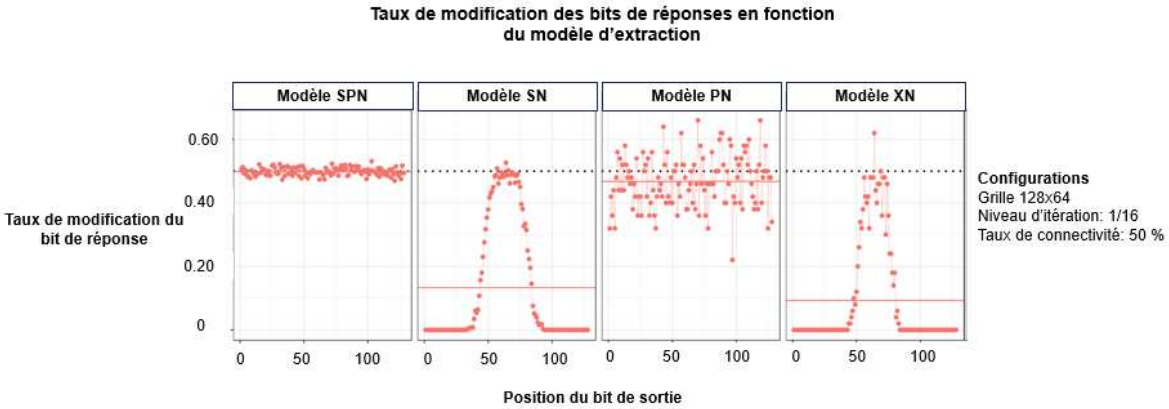

Figure 45: Coefficient d'avalanche strict selon les modèles de circuits

Le bit de diffusion (bit de challenge modifié) est en position 64. Un effet de faible diffusion est observé pour les modèles SN et XN sur la figure 45. Le taux de modification des bits s'effondre à mesure que les bits de réponses évalués sont éloignés de la position 64. Cela illustre une restriction de la diffusion de l'information dans ces deux modèles.

Sur cette même figure l'effet de diffusion est équitablement réparti sur les bits de réponses pour les modèles SPN et PN. Sans la SBOX il faut toutefois noter des écarts moyens plus fort avec la valeur idéale (0.50). Les taux de modifications varient entre 0.25 et 0.70 pour le modèle PN contre 0.45 et 0.55 pour le modèle SPN. Ces écarts se traduisent par des performances inégales dans la déviation standard de la métrique, ce point est abordé dans la sous-section suivante.

5.4.2 Impact du taux de connectivité

Le précédent résultat montre que le choix du modèle a un impact fort sur la diffusion. Pour compléter cette analyse, les calculs intégrant des variations de paramètre sont présentés. Le tableau 9 croise les moyennes des coefficients d'avalanche en fonction du choix modèle et du taux de connectivité. Les calculs sont effectués sur les mêmes espaces de réponses que pour la figure 45 et pour une configuration similaire. Cette fois-ci, sont aussi pris en compte les taux de connectivité à 25 et 75 %. Dans ce tableau de résultat, la moyenne du coefficient d'avalanche suffit à discriminer les modèles.

Pour les modèles XN et SN, la moyenne du coefficient d'avalanche est inférieure à 0.22, loin des objectifs souhaités pour la diffusion. La SBOX 4-bits améliore l'effet d'avalanche mais cela reste insuffisant et ce pour les trois taux de connectivité étudiés. Le modèle PN présente par contre une diffusion au-dessus de 0.45 dès le taux de connectivité à 25 %. La permutation a un apport bien plus élevé pour le coefficient d'avalanche en comparaison à la substitution. D'une part cela argumente pour considérer la permutation comme l'opération essentielle qui permet au circuit d'extraction d'accroitre sa propriété de diffusion. D'autre part cela suggère que le choix du modèle prévaut en terme d'impact sur le niveau de diffusion par rapport au taux de connectivité, du moins pour les configurations étudiées.

Dans le tableau 9, le coefficient d'avalanche du modèle PN reste toutefois en-dessous des exigences (0.4990), la meilleure moyenne est de 0.4968 pour le taux de connectivité à 75 %. Le modèle SPN se rapproche, quant à lui, de la valeur idéale, avec une moyenne haute de 0.5002 pour un taux de connectivité de 50 %. L'opération de substitution supplémentaire ajoutée dans le circuit compense le manque diffusion.

Ces premiers résultats pointent l'efficacité des modèles PN et SPN par rapport aux modèles XN et SN, avec toutefois un léger désavantage au modèle PN par rapport au modèle SN. Afin de mieux apprécier cette différence, des calculs supplémentaires de la métrique sont effectués pour d'autres configurations, notamment dans le cas de niveau d'itération de couche de diffusion inférieure à 1/8. Cela permet d'observer si les tendances constatées précédemment se confirment.

Cette deuxième série de résultats est présentée dans le tableau 10 et dans les figures 46 et 47. Les figures montrent le taux de modification des bits de réponses, cette fois-ci avec un niveau d'itération inférieure, 1/16. Les nuages de points illustrent des écarts à la moyenne plus fort pour le modèle PN. Ceci se traduit par des déviations standards des coefficients d'avalanche déséquilibrées entre les deux catégories de modèles. Le tableau 10 précise les moyennes et déviations observées dans les figures.

Tableau 9: Coefficient d'avalanche moyen des réponses selon le modèle DPUF
Grille 128x64 – Niveau d'itération 1/8

Paramètre \ Modèle	Modèle XN	Modèle SN	Modèle PN	Modèle SPN
Taux de connectivité = 25 %	0,0480	0.1106	0.4540	0.5019
Taux de connectivité = 50 %	0.0980	0.1645	0.4915	0.5002
Taux de connectivité = 75 %	0.1668	0.2173	0.4968	0.4991

Tableau 10: Moyennes et déviations standards du coefficient d'avalanche des modèles PN et SPN
Grille 128x64, niveau d'itération 1/16

Paramètre \ Modèle	**Coefficient d'avalanche du modèle PN**		**Coefficient d'avalanche du modèle SPN**	
	Moyenne	*Déviation standard*	Moyenne	*Déviation standard*
Taux de connectivité = 25 %	0,2631	*0.0591*	0.4725	*0.0158*
Taux de connectivité = 50 %	0.4678	*0.0818*	0.4985	*0.0126*
Taux de connectivité = 75 %	0.4903	*0.0656*	0.4996	*0.0130*

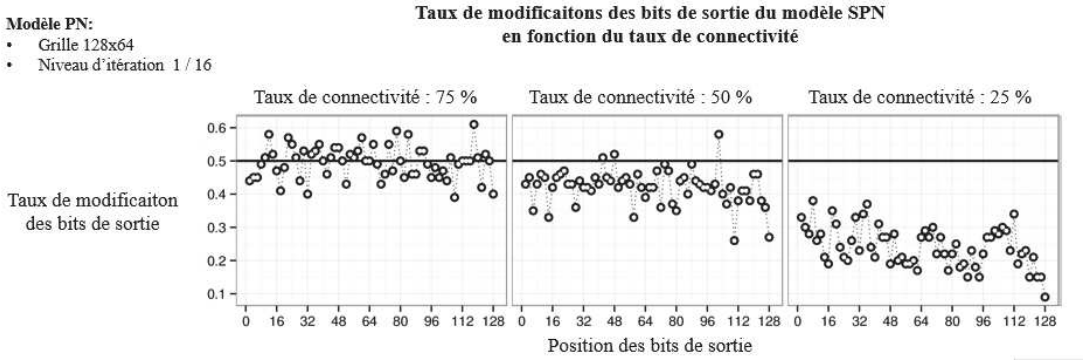

Figure 46 : Coefficient d'avalanche strict du modèle PN en fonction du taux de connectivité

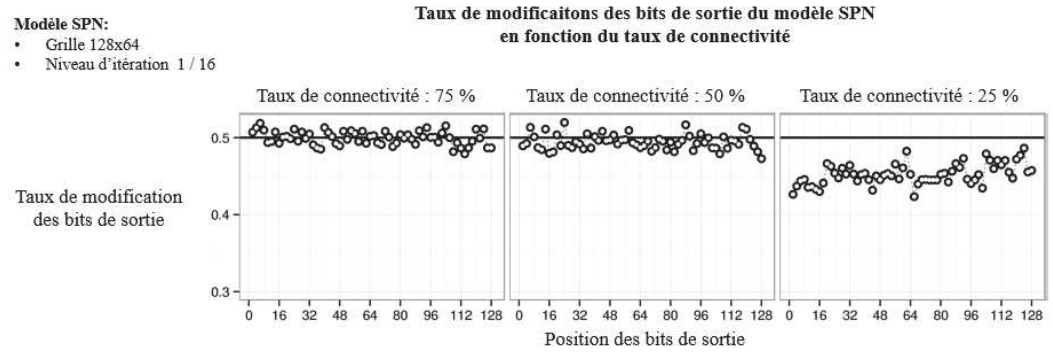

Figure 47 : Coefficient d'avalanche strict du modèle SPN en fonction du taux de connectivité

Les déviations standard du coefficient d'avalanche pour le modèle PN sont entre 5% et 9 % dans le tableau 10 et entre 1.2 % et 1.6 % pour le modèle SPN. La SBOX permet une forte homogénéisation du taux de modification des bits de réponses. La déviation pour le modèle PN respecte toutefois la contrainte, qui pour rappel doit être inférieure à 15 %.

Avec ce niveau d'itération plus faible (1/16 pour 64 colonnes), le modèle PN est bien plus impacté par le taux de connectivité. La moyenne du coefficient d'avalanche tombe à 0.2631 dans le tableau 10 pour une connectivité à 25 %. L'effet de baisse de diffusion due à une connectivité réduite est amoindrie par la SBOX (0.4725 pour la même connectivité). Cela dénote la capacité du modèle SPN à assurer une diffusion malgré de fortes contraintes sur la connectivité. Toutefois, seul un modèle SPN avec une connectivité à 75 % permet de respecter l'exigence d'une moyenne à 0.4990 pour la métrique.

Cela démontre la nécessité d'établir un équilibre entre ces deux paramètres – taux de connectivité de grille et niveau d'itération des opérations substitution-permutation – pour accroitre la diffusion. Cela permettra de réduire la dimension de la grille et donc le coût de surface. En l'occurrence, le nombre de colonne de la grille impacte aussi fortement le niveau de diffusion dans certaines configurations.

5.4.3 Impact du nombre de colonne sur les modèles XN et SN

En section 4.2.1, nous avons argumenté que le manque de diffusion du modèle XN peut être compensé en augmentant la taille de la structure et le taux de connectivité. En l'occurrence, la Figure 48 permet d'observer l'effet de diffusion en fonction du nombre de colonne. A la différence de la figure 45, le bit de diffusion est en première position et seul le modèle XN est présenté avec un taux de connectivité à 50 %. Comme observé en figure 45, le taux de modification diminue à mesure que les bits évalués se distancent de la position du bit de diffusion. Un nombre de colonne plus élevé améliore effectivement le taux de modifications. Toutefois, l'effet de diffusion reste bien trop faible, y compris avec 256 colonnes ; le coefficient d'avalanche moyen est estimé à 0.1794.

La figure 49 illustre l'effet d'un taux de connectivité supérieur (75 %), cela améliore l'effet d'avalanche. Il faut toutefois encore un accroissement conséquent de la taille de la structure pour répondre aux objectifs de diffusion : au vu de ces résultats, il faudrait un nombre de colonne supérieur à 256. Avec une configuration de 256 colonnes et une connectivité à 75 %, la moyenne de la métrique reste en effet nettement insuffisante.

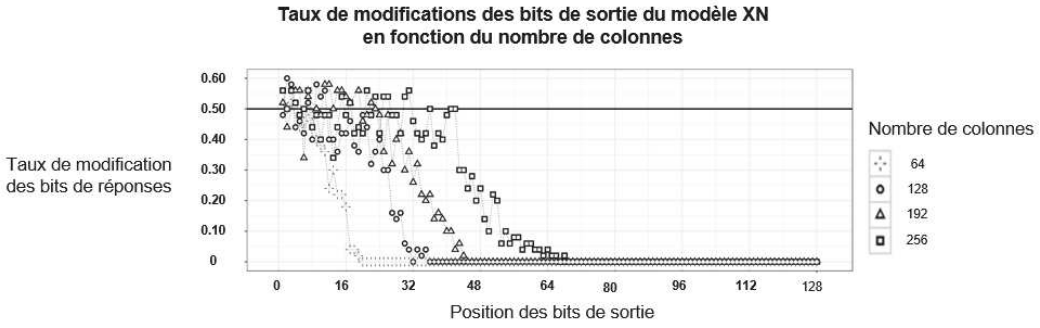

Figure 48 : Coefficient d'avalanche strict pour le modèle XN avec connectivité à 50 %

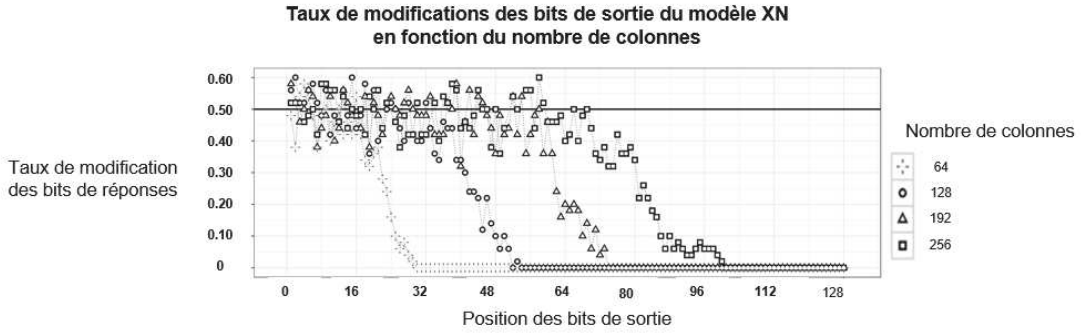

Figure 49 : Coefficient d'avalanche strict du modèle XN avec connectivité à 75 %

Le modèle SN souffre du même constat, la figure 50 montre le coefficient d'avalanche strict qui décroit en fonction du nombre de colonne. Le taux de connectivité est fixé à 50 % et le niveau d'itération de la SBOX à 1/8. L'effet de diffusion diminue à mesure que le bit de réponse est à une position distante de celle du bit modifié en entrée de la grille. Une dimension supérieure accroit la métrique, la moyenne du coefficient d'avalanche est estimée à 0.4465 pour 256 colonnes. Pour rappel, dans le tableau 10, pour un même niveau d'itération et de connectivité, les modèles PN et SPN affichaient des coefficients d'avalanche respectivement de 0.4915 et 0.5002 pour seulement 64 colonnes.

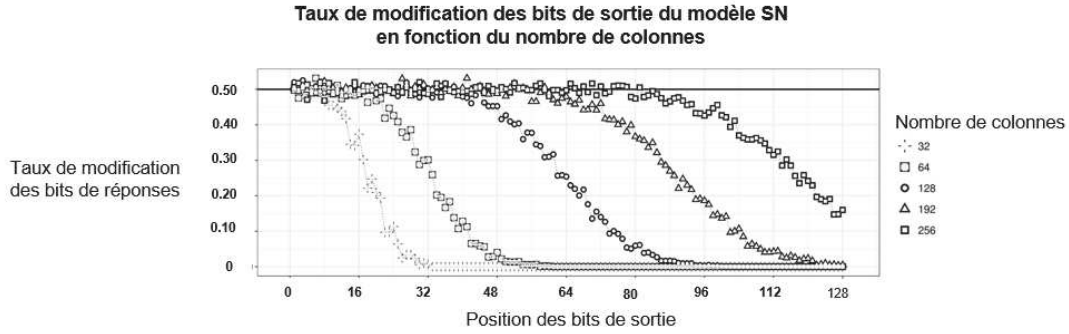

Figure 50 : Coefficient d'avalanche strict du modèle SN en fonction du nombre de colonne

Ces résultats montrent la nécessité pour les modèles XN et SN d'accroitre fortement la taille de la grille et la connectivité. Cela permet de maximiser la transmission des bits d'informations à l'ensemble des rangées de nœuds de connexion et ainsi de diffuser toute modification sur l'ensemble de la séquence binaire extraite en sortie par le circuit. Les contraintes sur ces deux paramètres apparaissent toutefois excessives et couteuses. Il est estimé qu'un nombre de colonne supérieur à 256 est requis tout en imposant des taux de connectivité élevés (plus de 75 %). Cela aura des conséquences lourdes sur le procédé de fabrication des grilles DPUFs, celui-ci devra être optimisé pour maximiser les connexions.

Cela valide l'exclusion des modèles XN et SN des choix de conception pour un modèle de circuit d'extraction des strong DPUF. La phase d'analyse suivante se concentre ainsi sur les modèles PN/SPN, argumente en faveur de leur efficacité et approfondit la recherche de configurations PN/SPN optimales.

5.5 Evaluation de la diffusion : optimisation des configurations SPN et PN

5.5.1 Impact et réduction du nombre de colonnes

Après exclusion des modèles XN et SN, des calculs supplémentaires sont menés pour analyser la propriété de diffusion des modèles SPN et PN avec des grilles de tailles réduites. Les précédents résultats du tableau 10 (section 5.4.2) pour 64 colonnes soulignent une diffusion performante pour le modèle SPN mais plus faible pour le modèle PN. Selon ces résultats le modèle PN a une connectivité plus élevée.

Le tableau 11 détaille les moyennes et déviations standard des coefficients d'avalanche des deux modèles avec une réduction des colonnes. Le taux de connectivité est à 50 % et le niveau d'itération fixé à 1/8, identique au tableau 10. La perte de diffusion est constatée dès 32 colonnes, les coefficients d'avalanche moyens sont respectivement 0.4834 et 0.3433 pour les modèles SPN et PN. Une grille réduite à 16 colonnes est rédhibitoire y compris pour le modèle SPN : la moyenne des coefficients d'avalanche est estimée à 0.2166 pour ces configurations.

Il est constaté que les tendances des écarts aux moyennes sont conservées, les déviations sont autour de 1.2 % pour les réponses SPN et supérieures à 7 % pour celles du modèle PN. Cela confirme l'effet de la SBOX, quel que soit les paramètres de configurations celle-ci homogénéise les taux de modifications.

Ces résultats pointent l'obligation de contraindre les taux de connectivité et les niveaux d'itération pour compenser la réduction du nombre de colonnes. Pour les configurations évaluées – 50 % de connectivité et une couche de de substitution-permutation itérée à 1/8 – la diffusion est limitée. Ce paramétrage ne peut respecter les exigences de sécurité que par un nombre de colonnes élevé. Cela impacte directement la surface du circuit DPUF. Afin de limiter la taille requise, un accroissement de la diffusion des modèles SPN et PN doit être réalisé par un paramétrage spécifique des deux autres paramètres. En effet, le taux de connectivité, tout comme le niveau d'itération plus élevé, influe sur la diffusion.

Des nouvelles mesures sont réalisées pour des grilles de dimension réduites à 16 et 8 colonnes. avec des niveaux d'itération supérieurs.

Tableau 11 : Coefficient d'avalanche des modèles SPN et PN en fonction du nombre de colonnes
Taux de connectivité : 50 %. Niveau d'itération : 1/8

Paramètre \ Modèle	**Coefficient d'avalanche du modèle SPN**		**Coefficient d'avalanche du modèle PN**	
	Moyenne	*Déviation standard*	Moyenne	*Déviation standard*
Nombre de colonnes : 64	0,5002	*0.0126*	0.4915	*0.0746*
Nombre de colonnes : 32	0.4834	*0.0149*	0.3433	*0.0706*
Nombre de colonnes : 16	0.2166	*0.0102*	0.0756	*0.1044*

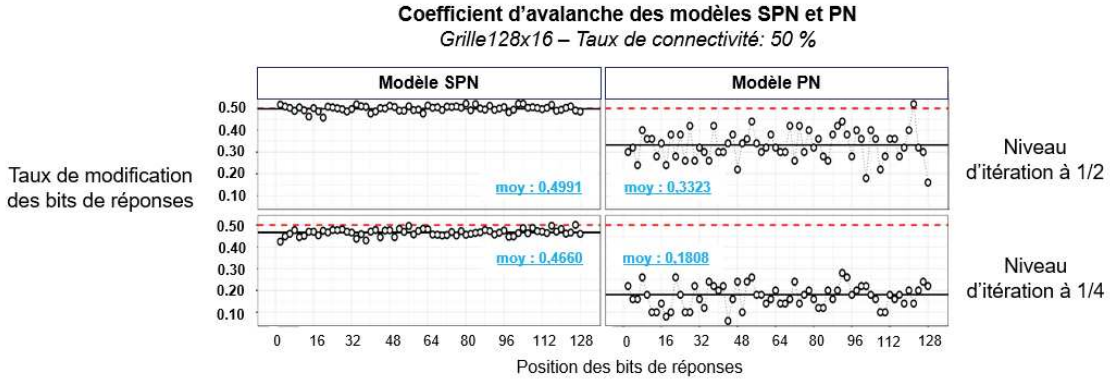

Figure 51 : Coefficient d'avalanche des modèles SPN et PN – 16 colonnes

La figure 51 montre les coefficients d'avalanche pour 16 colonnes et une connectivité à 50 % pour des niveaux d'itération de 1/2 et 1/4. Les moyennes pour chaque configuration sont indiquées sur les nuages de points. Une amélioration effective est constatée par rapport au tableau 11, où pour 16 colonnes les moyennes étaient de 0.2166 et 0.0756. Pour un niveau d'itération à 1/2 les moyennes respectives des circuits SPN et PN sont 0.4991 et 0.3323. Une itération supplémentaire renforce efficacement la diffusion, cela est observé aussi dès les niveaux 1/4. Toutefois, parmi ces résultats, seul le modèle SPN avec itération à 1/2 valide les objectifs (moyenne à 0.4991).

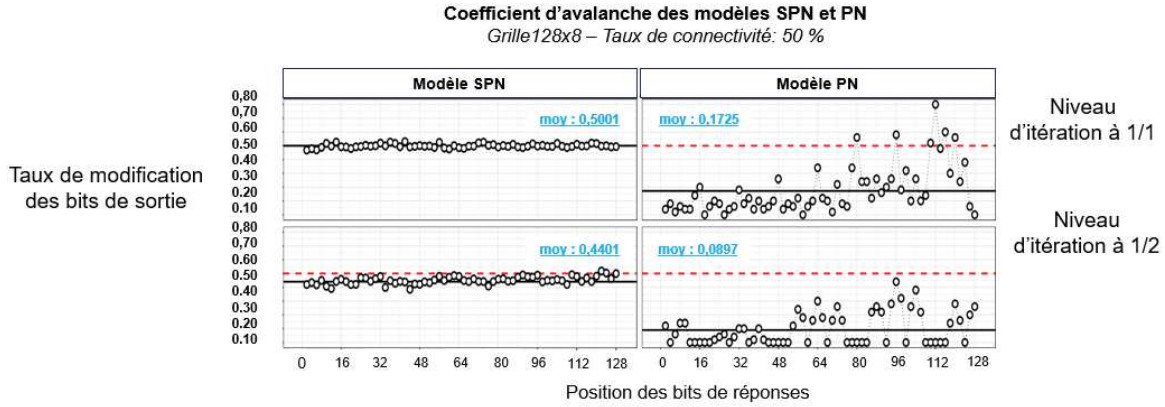

Figure 52: Coefficient d'avalanche des modèles SPN et PN - 8 colonnes

La figure 52 complète le constat précédent avec une estimation de la diffusion pour des grilles de 8 colonnes avec connectivité de 50 %. Malgré un niveau d'itération élevé, la métrique est fortement limitée pour le modèle PN (0.1725 en moyenne) ; un modèle SPN avec une itération entre chaque colonne de grille atteint par contre les exigences : 0.5001 en moyenne.

Il est observé que le niveau d'itération seul ne permet pas de maximiser la diffusion, une connectivité accrue est nécessaire. Un paramétrage spécifique de la configuration est requis pour obtenir un compromis entre la taille de la grille et le niveau de diffusion exigé pour le circuit d'extraction.

5.5.2 Optimisation du compromis entre les paramètres des modèles SPN et PN

Les tableaux 12 et 13 détaillent les moyennes et déviations standard des coefficients d'avalanche des deux catégories de modèles SPN et PN, avec des configurations qui croisent les intervalles d'études paramètres. Les résultats des figures 51 et 52, avec les configurations de grilles à 8 colonnes et 16 colonnes et connectivité à 50 %, sont inclus. Dans ces tableaux, la moyenne des coefficients discrimine les configurations, seul un ensemble restreint de configuration respecte les exigences de diffusion (moyenne à 0.50 à 0.001 près). Les résultats validant les objectifs sont indiqués en fond vert. Les résultats approchant la valeur idéale à 0.01 près sont aussi précisés à titre indicatif en bleu.

Le modèle SPN, en tableau 12, respecte les exigences de diffusion pour les configurations suivantes :

- *32 colonnes, itération à 1/4, taux de connectivité 25 à 75 %*
- *16 colonnes, itération à 1/2, taux de connectivité 25 à 75 %*
- *8 colonnes, itération à 1/1, taux de connectivité supérieur à 50 %*

Le modèle PN n'atteint, en tableau 13, le niveau de diffusion que pour une seule configuration :

- *32 colonnes, itération à 1/1, taux de connectivité supérieur à 75 %.*

Il faut noter que certaines configurations du modèle PN approchent les exigences :

- *32 colonnes, itération à 1/2 et 1/1, taux de connectivité à 50 %*
- *16 colonnes, itération à 1/2, taux de connectivité 25 à 75 %*

Tableau 12: Coefficients d'avalanches du modèle SPN avec croisement des paramètres

Paramètre \ Modèle	**8 colonnes**		**16 colonnes**		**32 colonnes**
	Itération 1/2	***Itération 1/1***	***Itération 1/4***	***Itération 1/2***	***Itération 1/4***
Taux de connectivité = 25 %	**0.4063** *0.0530*	**0.4984** *0.0125*	**0.4276** *0.0332*	**0.5005** *0.0133*	**0.4994** *0.0158*
Taux de connectivité = 50 %	**0.4402** *0.0315*	**0.5001** *0.0125*	**0.4660** *0.0158*	**0.4991** *0.0127*	**0.5000** *0.0137*
Taux de connectivité = 75 %	**0.4757** *0.0179*	**0.5003** *0.0139*	**0.4906** *0.0135*	**0.5005** *0.0129*	**0.4993** *0.0131*

Tableau 13: Coefficients d'avalanches du modèle PN avec croisement des paramètres

Paramètre \ Modèle	**8 colonnes**	**16 colonnes**		**32 colonnes**	
	Itération 1/1	***Itération 1/2***	***Itération 1/1***	***Itération 1/2***	***Itération 1/1***
Taux de connectivité = 25 %	**0.04671** *0.1080*	**0.1309** *0.0936*	**0.1661** *0.0894*	**0.4005** *0.0684*	**0.4572** *0.0723*
Taux de connectivité = 50 %	**0.1725** *0.1477*	**0.3323** *0.0633*	**0.4645** *0.0719*	**0.5063** *0.0727*	**0.4986** *0.0705*
Taux de connectivité = 75 %	**0.4166** *0.1215*	**0.4642** *0.0179*	**0.4969** *0.0720*	**0.5013** *0.0685*	**0.4996** *0.0626*

5.6 Bilan de l'évaluation

Les calculs de métriques de sécurité, réalisés avec la plateforme de simulation et d'évaluation, sur des effectifs de 50 DPUFs et 30 paires de challenges (soit 1500 réponses par configuration), fournissent des indications sur les performances de sécurité des modèles. Pour l'ensemble des espaces de challenge-réponse étudiés, les résultats en termes d'uniformité et d'unicité sont corrects (5.2), confortant des études de la littérature. Toutefois, les analyses sur le coefficient d'avalanche et la métrique de diffusion, aboutissent à des conclusions discriminant les modèles et les choix des configurations.

- Premièrement, les analyses excluent les modèles XN et SN, ceux-ci souffrant d'une diffusion restreinte qui ne peut être compensée que par un nombre excessif de colonnes (section 5.4.3).
- Deuxièmement, un compromis entre les choix de paramètres est nécessaire pour les modèles SPN et PN. Des configurations sont identifiées en section 5.5.2 et précisées dans le tableau 14, afin d'atteindre les exigences de diffusion. Les moyennes et déviations standard obtenues pour ces configurations respectent les objectifs : moyenne de 0.50 à 0.001 près et déviation inférieure à 0.15.
- Troisièmement, au vu des configurations SPN et PN proposées, plusieurs enjeux vis-à-vis des contraintes de fabrication et de surface apparaissent. Si le procédé de fabrication le permet, un haut taux de connectivité peut être favorisé, cela procure au modèle PN un niveau de diffusion acceptable. Il est ainsi envisageable de soustraire l'opération de substitution. Par ailleurs, plusieurs jeux de paramètres, entre nombre de colonnes et niveau d'itération, sont valables pour maximiser la diffusion d'un circuit SPN.

Sous réserve que les hypothèse de modélisation soient valides (notamment la densité de répartition des connexions, section 5.1.1), cette évaluation des métriques est « universelle » vis-à-vis de la technologie d'implémentation. Celle-ci s'applique à un circuit d'extraction DPUF quel que soit le procédé de fabrication utilisé pour générer la structure aléatoire (la grille de nœud de connexion). Cela en fait un outil et une étude pertinent pour toute démarche de conception de DPUF. L'analyse de sécurité peut toutefois être affinée par des métriques supplémentaires ou se focaliser sur de nouveaux modèles.

En outre, la conception complète d'un DPUF implique aussi des analyses sur les paramètres en amont et en aval de la spécification du circuit d'extraction. En amont, des paramètres doivent être pris en compte selon la méthode de fabrication, notamment ceux qui déterminent la densité de répartitions des connexions. Cela précise les contraintes et variabilités auxquelles est soumis le taux de connectivité. En aval, les configurations identifiées pour un modèle DPUF optimal doivent aussi faire le sujet d'une étude de leur coût d'implémentation. Des estimations de surface sont requises, d'une part pour discriminer les configurations SPN identifiées et d'autre part pour évaluer l'efficacité des modèles. En l'occurrence, la surface du circuit est variable selon le nombre de colonnes mais aussi si des SBOXs sont intégrées. Le chapitre suivant adresse cette problématique : l'évaluation des coûts de surfaces des circuits d'extraction, plus particulièrement pour les configurations identifiées dans le tableau 14.

Tableau 14: Configurations identifiées pour les modèles SPN et PN et niveau de diffusion associé

Paramètre \ Modèle	**PN 128x32**	**SPN 128x8**	**SPN 128x16**	**SPN 128x32**
	Itération 1/1	***Itération 1/1***	***Itération 1/2***	***Itération 1/4***
Taux de connectivité = 25 %	**0.4572** *0.0723*	**0.4984** *0.0125*	**0.5005** *0.0133*	**0.4994** *0.0158*
Taux de connectivité = 50 %	**0.4986** *0.0705*	**0.5001** *0.0125*	**0.4991** *0.0127*	**0.5000** *0.0137*
Taux de connectivité = 75 %	**0.4996** *0.0626*	**0.5003** *0.0139*	**0.5005** *0.0129*	**0.4993** *0.0131*

6 Coûts d'implémentation des Circuits SPN pour un *Strong DPUF*

6.1 Flot de la conception et de l'évaluation des circuits

6.1.1 Conception et simulation comportementale

L'évaluation des performances des circuits d'extraction s'appuie sur le développement et la synthèse de codes descriptifs VHDL des circuits d'extraction SPN (*VHSIC Hardware Description Language*). Cela correspond aux deux premières étapes du flot de conception d'un circuit intégré décrite dans la figure 53: la simulation comportementale et la synthèse logique. Les descriptions VHDL des circuits incluent le calibrage du réseau selon les paramètres souhaités (colonne, niveau d'itération de la couche de diffusion…). Les circuits sont simulés et synthétisés avec les configurations identifiées dans le chapitre précédent. La synthèse aboutit à une première estimation sur les coûts en surface, ainsi que sur certains indicateurs de performances tels que la fréquence et l'énergie consommée.

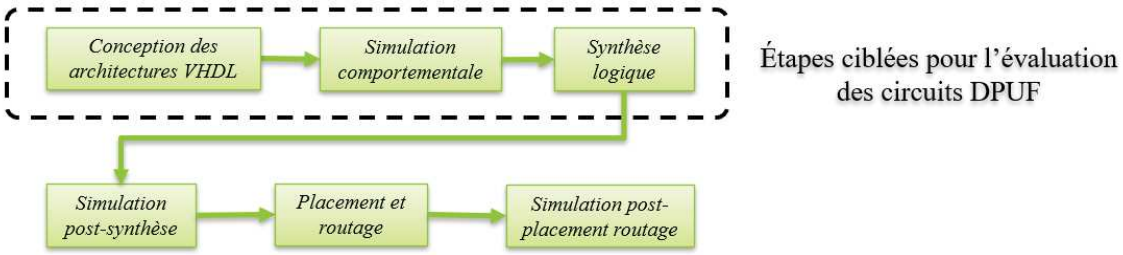

Figure 53: Flot de conception d'un circuit intégré

L'étude n'inclut pas les coûts de la structure matérielle aléatoire : la grille de nœud de connexion n'est pas synthétisable. Sa surface pourrait être estimée sous réserve de connaitre le nœud et les spécificités de la technologie et du procédé de fabrication choisie. Au cours de la synthèse seul le schéma d'extraction est spécifié : le réseau logique, composé des colonnes de XORs et des opérations substitution et permutation. Nous considérons le circuit d'extraction comme un bloc logique englobant la structure matérielle. Si la grille peut occuper une surface non négligeable, nous estimons que la surface du circuit, composée du réseau logique, est un facteur important du coût d'implémentation du strong digital PUF. La surface des circuits d'extraction implémentés est déterminante pour évaluer et optimiser le strong digital PUF.

Conception des architectures VHDL

La première phase se concentre sur le développement et la simulation comportementale des architectures VHDL des schémas d'extraction. Cette conception implique des choix d'implémentation : chaque modèle de circuit d'extraction peut être implémenté sous une forme entièrement combinatoire, ou sous une forme incluant une logique séquentielle.

Dans le cas d'une fonction implémentée par un circuit combinatoire, la sortie de la fonction à un instant donné dépend uniquement des valeurs en entrée de la fonction à ce même instant et de la logique du circuit. En théorie, avec cette forme d'implémentation, après la réception du challenge, le circuit d'extraction implémenté retourne directement la réponse DPUF. Le temps minimale pour générer la réponse dépends du chemin critique, et détermine la période d'horloge requise pour le circuit implémenté. L'étude des coûts en surface des circuits d'extraction se focalise en premier lieu à ce modèle d'implémentation.

Dans le cas d'une implémentation avec logique séquentielle, les registres mémoires sont inclus entre les colonnes du réseau logique. L'horloge du circuit cadence la propagation des séquences de bits à travers le réseau. La quantité de registres intégrés est variable, augmentant la surface requise pour l'implémentation de circuit. L'horloge de cadencement est aussi paramétrable et directement liée à la fréquence de fonctionnement du circuit.

Ces deux formes d'implémentations sont détaillées dans la section suivante (6.2).

Simulation comportementale

Les architectures VHDL sont conçues pour les différents modèles et configurations, avec les deux formes d'implémentation possibles. Le comportement des architectures est simulé avec le logiciel *QuestaSim* de MentorGraphic [105]. Une phase de simulation de et vérification, présentée dans la figure 54, valide les développements des circuits ainsi que le comportement attendu. Des suites de test (*testbenchs*) accompagnent les codes VHDL et spécifient des entrées pour les circuits testés.

Le comportement induit par la grille de nœuds de connexions est simulé : une séquence est envoyée en entrée de chaque colonne du réseau logique, représentant les états ouvert/ fermé des nœuds. Un registre est intégré entre chaque colonne du réseau pour mémoriser les états. Le réseau du schéma d'extraction interagit avec ces états selon l'expression logique définie précédemment dans la partie 4.3.

Les challenges et séquences d'états des connexions injectés au cours de la simulation sont les mêmes que ceux générés pour la phase d'évaluation des métriques de sécurité. Ainsi, cela doit aboutir à des espaces de paires challenges-réponses identiques. Les réponses obtenues au cours de la simulation comportementale sont comparées avec les réponses générées par la plateforme de modélisation. Une correspondance exacte valide le comportement des schémas d'extraction implémentés en VHDL.

Une fois validées, les architectures peuvent être synthétisées.

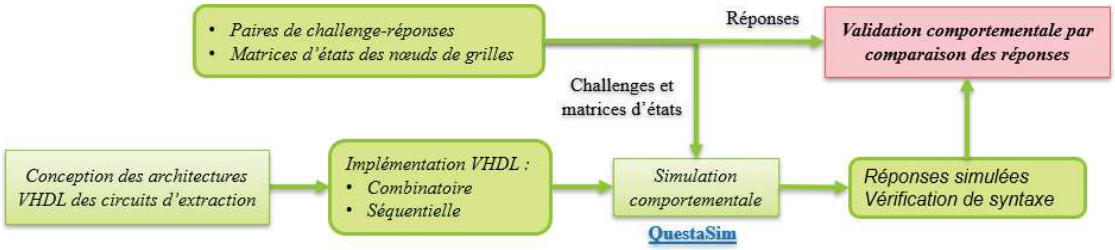

Figure 54: Démarche pour la simulation comportementale des circuits DPUF

6.1.2 Phase de synthèse logique

Par la suite, une deuxième phase étudie la synthèse des circuits d'extraction et les indicateurs de performances qui en résultent. L'analyse est réalisée avec le logiciel de synthèse *Design Compiler* de Synopsys [106] et le kit de développement libre d'accès *NanGate 45nm* [107], aussi désigné comme une librairie de cellule standards.

Design compiler est un outil de synthèse logique, il génère à partir d'une architecture VHDL, la description détaillée du circuit logique correspondant : la *Netlist* qui énumère l'ensemble des portes logiques du circuits et les interconnexions entre ces portes. La synthèse peut être configurée pour une puissance ou une fréquence de fonctionnement ciblées et des limites de surface peuvent être définies. Pour la synthèse logique, une libraire de cellule standard doit être choisie.

La librairie de cellule standards décrit les spécificités physiques des cellules logiques élémentaires pour un nœud technologique, parfois elle est spécifique à une entreprise *fondeur* donnée, parfois elle est transverse. La librairie, telle que *NanGate*, définit les propriétés physiques, structures et comportement

des cellules : surface et puissance, mais aussi les contraintes de délais et les contraintes géométriques. L'outil de synthèse logique utilise ces informations pour estimer les performances du circuit synthétisé.

Nous choisissons la librairie *NanGate* qui a l'avantage d'être libre d'accès. Il s'agit d'une référence pour la recherche en conception de circuit intégré. Cette librairie a aussi été utilisée pour la proposition du SD-PUF [93]. Cela permet une comparaison pertinente entre les couts de surface du SD-PUF et ceux résultant de l'étude de nos modèles. En outre, le nœud technologique associé (45 nm) est suffisant avancé pour que les estimations soient pertinentes pour des applications futures.

Les architectures VHDL des circuits d'extractions sont synthétisées avec les différentes configurations possibles, mais aussi selon diverses fréquences de fonctionnement. Au cours de cette évaluation les plages de fréquences s'étendent de 5 Mhz à 200 MHz. Pour les dimensions de circuits étudiées les délais de propagation ne sont pas respectés au-dessus d'une fréquence de 200 MHz. Cette phase de synthèse logique est présentée dans la figure 55.

Design Compiler génère des rapports de synthèse contenant des estimations des performances : surface, fréquence maximale, énergie consommée et contraintes de délais. Cela permet d'évaluer et comparer les performances des modèles de circuits d'extraction en fonction des configurations choisies et des types d'implémentation (combinatoire ou séquentielle).

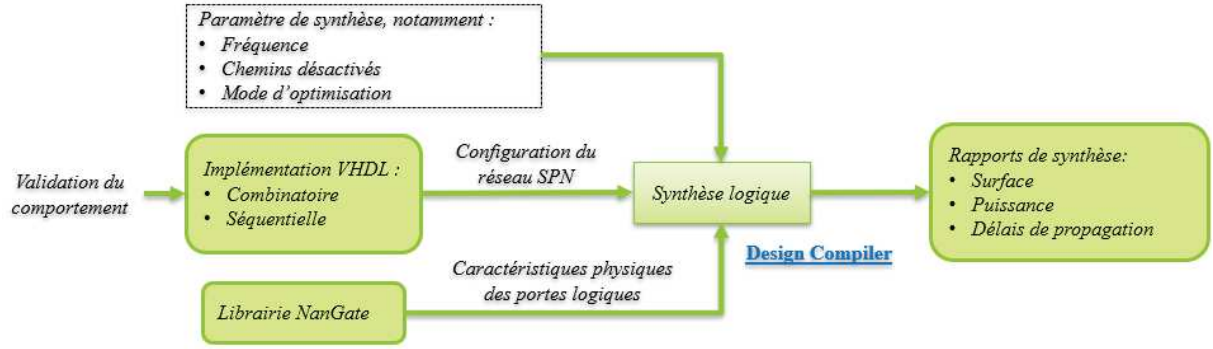

Figure 55: Phase de synthèse logique

6.1.3 Phase d'évaluation des performances

Le rapport sur les surfaces détaille l'aire requise par les différents blocs logiques du circuit :

- La surface totale du circuit synthétisé *(design area)* composée de deux blocs :
  - L'aire dites combinatoire *(combinational area)*
  - L'aire dites non-combinatoire *(noncombinational area)*
- La surfaces des blocs composés de « buffers » et d'inverseurs *(Buf/Inv area).*

Ces surfaces, exprimées en um^2, dépendent des configurations du schéma d'extraction, du niveau de logique séquentielle mais également des paramètres de synthèse, tel que la fréquence souhaitée. L'évaluation des performances se focalise sur la surface totale du circuit *(design area)*, l'indicateur prioritaire pour juger du coût d'implémentation du circuit d'extraction du Strong Digital DPUF.

Le rapport sur les estimations de puissance contient :

- Une estimation de la puissance dynamique du circuit en cours de fonctionnement, en deux parts :
  - La puissance interne aux cellules logiques *(cell internal power),* dissipée par les charges et les décharges des capacités internes aux cellules logiques.

  - La puissance de commutation des interconnexions *(net switching power)*, dissipée par le chargement et le déchargement des capacités en sortie des cellules logiques.
- Une estimation de la puissance statique *(cell leakage power)*, dissipée en permanence par le circuit.

Ces indicateurs de puissances sont exprimés dans le rapport d'évaluation en *Watts* (*mW* ou *uW* selon les ordres de grandeurs). Ils permettent une première estimation de la puissance requise pour les circuits implémentés et de l'énergie consommée. Toutefois, dans le cadre de ces synthèses logiques, ce critère ne témoigne que d'une tendance générale de l'influence des paramètres. Une estimation fine des puissances et de l'énergie requise nécessite une précision des caractéristiques technologiques et des paramètres de fonctionnement du circuit implémenté.

Plusieurs rapports fournissent aussi des informations sur les temps de propagation. Ils indiquent les éventuels chemins pour lesquels les délais ne sont pas respectés.

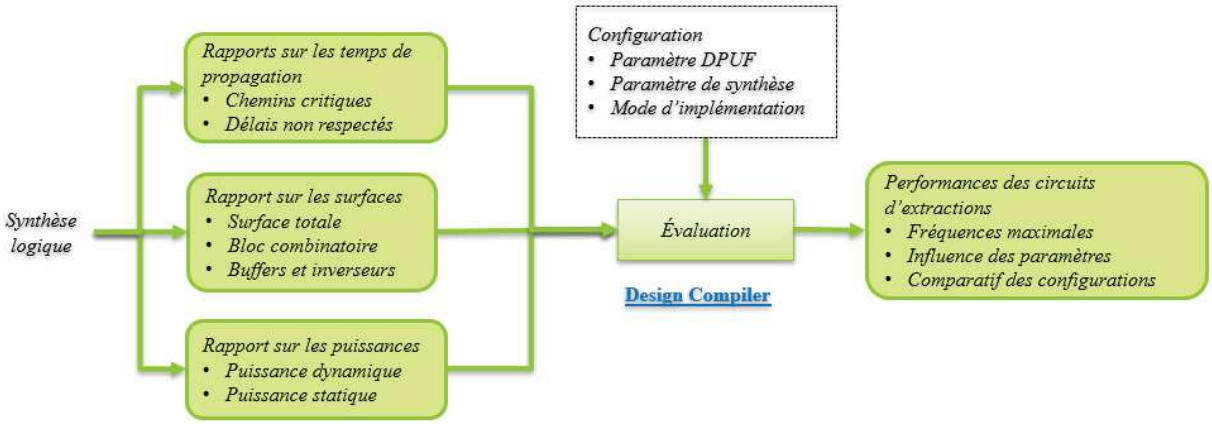

Figure 56: Phase d'évaluation des résultats de synthèse

L'évaluation se base sur ces indicateurs pour estimer les performances des circuits implémentés, notamment comparer les coûts de surfaces entre les configurations et identifier les fréquences maximales de fonctionnement. La fréquence influe entre autres sur le débit en sortie du circuit et la latence (voir section 3.2.3). Surface et fréquence sont toutefois les indicateurs essentiels de cette étude pour identifier la configuration optimale (les paramètres du circuit et le mode d'implémentation).

6.2 Implémentation des circuits d'extractions

6.2.1 Présentation générale des architectures

Les architectures VHDL développées instancient les modèles **PN et SPN** des circuits d'extractions pour strong DPUF. La conception des architectures s'appuie sur la description des modèles en section 4.3, précisant notamment les expressions logiques des réseaux **SPN**. En l'occurrence, ces réseaux se décomposent en opérations élémentaires : les opérations XOR, substitution et permutation. Celles-ci sont itérées entre les colonnes du DPUF et appliquées – en rangée – à la sortie des nœuds de colonnes.

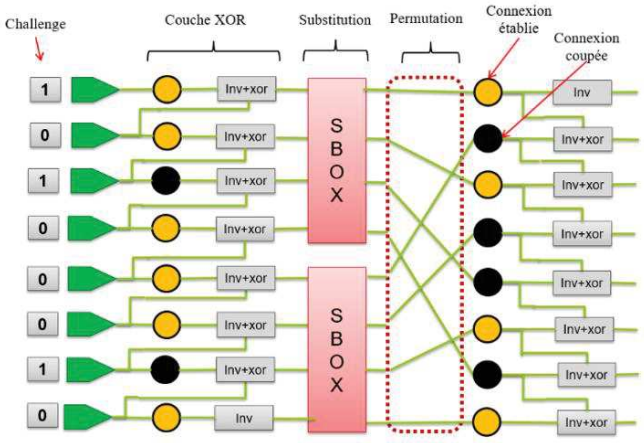

Figure 57: Rappel de la schématique des réseaux SPN

Cette décomposition en opérations élémentaires détermine la structure des architectures VHDL des circuits. Des composant sont spécifiés pour chacune des opérations élémentaires et sont ensuite connectés pour former l'ensemble du réseau. Les implémentations peuvent se découper en trois niveaux de hiérarchies :

- Les opérations élémentaires (XOR, substitution, permutation).
- Des composants « colonnes » qui forment une couche logique appliquée entre les colonnes.
- L'ensemble de l'architecture avec l'itération des « colonnes »

L'architecture du réseau peut être entièrement combinatoire ou séquentielle. Dans le cas combinatoire, les composants sont simplement connectés entre eux de telle sorte à respecter les expressions logiques du réseau (section 4.3). Dans le cas d'une implémentation séquentielle, la différence architecturale est l'ajout de registres mémoire entre les composants « colonnes » du réseau logique. Le changement d'état de ces registres est cadencé par l'horloge (donc la fréquence de fonctionnement choisie). Cela induit des coûts de surface et des performances différents. La section suivante approfondit ces enjeux et détaille les schémas des architectures VHDL.

6.2.2 Schématique des implémentations

La schématique de l'implémentation combinatoire est similaire aux figures descriptives des circuits d'extractions. Dans la figure 58, l'entité de plus haut niveau (qualifiée « top ») est nommée *DPUF_circuit* et forme le réseau logique. Elle est constituée de colonnes logiques appliquant les opérations de diffusions (XOR, S-P) et de deux registres, un pour les variables d'entrée, un pour les variables de sortie. Les composants colonnes *Col_in* et *Col_down* diffèrent pour l'opération XOR : l'entrée logique du XOR est connectée à la rangée supérieure ou inférieure en fonction de la parité.

Le circuit « top » a comme variable d'entrée le challenge (Puf_in), la matrice d'état (node_in), l'horloge (Clk) et le signal de reset. L'horloge cadence la transmission du challenge – stocké dans Reg_in – au réseau logique. Les signaux internes (m_puf_X) transfèrent les états logiques de chaque composant colonne au suivant. La réponse est récupérée dans Reg_out au coup d'horloge suivant. Une période d'horloge minimale est requise pour que la transmission des bits respecte les délais de propagation. Dans le cas contraire, les rapports de synthèse indiquent les chemins pour lesquels une transgression est détectée.

Dans les rapports de surface, l'aire combinatoire estimée correspond à la surface de l'ensemble des composants « colonnes » et de leurs interconnexions, l'aire non-combinatoire à la surface occupée par les registres d'entrée et de sortie. Avec cette approche chaque colonne supplémentaire accroit la taille

de chemin et donc le temps nécessaire pour que les bits soient transmis. Ainsi un réseau de plus grande dimension impliquera une contrainte plus forte sur la période d'horloge.

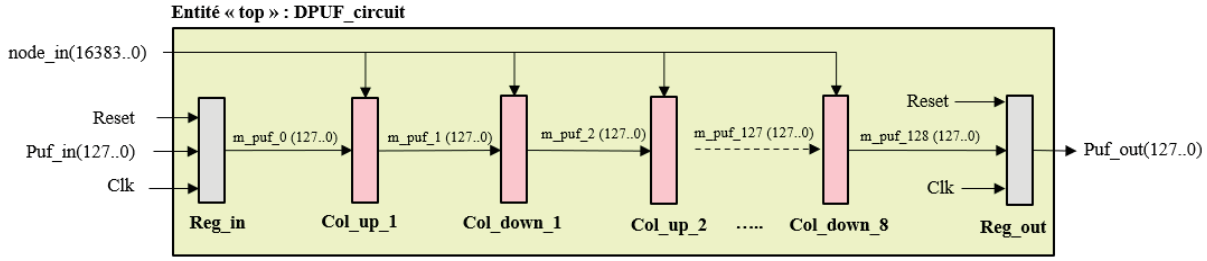

Figure 58: Implémentation combinatoire du réseau SPN

La deuxième approche, séquentielle, consiste à intégrer des registres stockant les états intermédiaires entre les composants colonnes. Le « niveau » de registre est variable, dans la schématique en figure 59, des registres intermédiaires sont spécifiés toutes les deux « colonnes » : pour une dimension de réseau 128x16 cela implique l'intégration de 8 colonnes de registres. Nous nommons niveaux de registres le nombres de colonnes de registres intégrées dans le circuit.

Ces registrent prennent en entrée la sortie logique de la colonne précédente et l'horloge qui cadence la transition des états à travers le circuit. Cela permet de réduire les contraintes sur les temps de propagation et ainsi d'augmenter la fréquence de circuit en comparaison du mode combinatoire.

En théorie, la latence est similaire entre les deux implémentations car les longueurs de chemin sont peu différentes. Toutefois, si des challenges sont soumis en flux continu, la fréquence plus élevée de l'implémentation séquentielle permet des débits plus importants : après le remplissage de tous les registres d'états intermédiaires, une réponse sera générée à chaque coup d'horloge. L'intérêt de ce mode d'implémentation dépend donc du cas d'usage et des contraintes de débit.

En contrepartie, les registres supplémentaires accroissent la surface occupée par le circuit d'extraction.

Cela fait l'objet de l'étude de la section suivante, déterminant les paramétrages optimaux pour maximiser les performances de ces circuits.

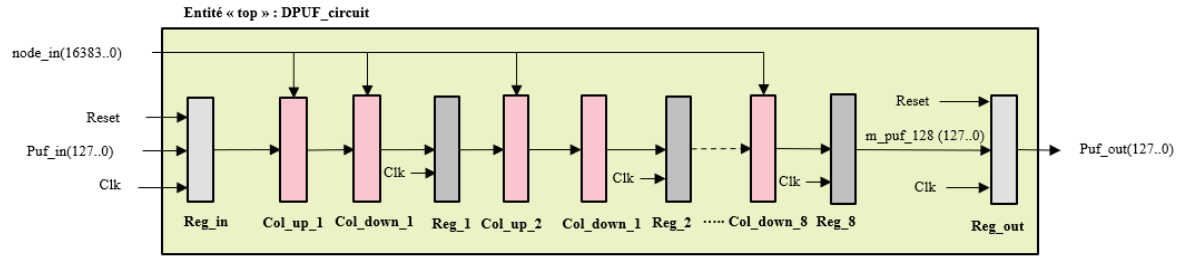

Figure 59: Implémentation séquentielle des réseaux SPN

6.3 Analyses et Réduction des Coûts d'Implémentation

6.3.1 Résultats pour les implémentations combinatoires

Les architectures combinatoires et séquentielles des circuits d'extraction sont synthétisées et évaluées, notamment avec les configurations identifiées en section 5.5 (tableau 14), respectant les exigences de diffusion. Pour rappel, les configurations adéquates sont les suivantes :

Tableau 15 : Configurations adéquates pour les modèles SPN et PN et niveau de diffusion associé

Paramètre \ Modèle	PN 128x32 *Itération 1/1*	SPN 128x8 *Itération 1/1*	SPN 128x16 *Itération 1/2*	SPN 128x32 *Itération 1/4*
Connectivité = 25 %	0.4572	0.498	0.5005	0.499
Connectivité = 50 %	0.4986	0.5001	0.4991	0.5000
Connectivité = 75 %	0.499	0.5003	0.5005	0.4993

La première évaluation concerne les résultats en termes de surface et de fréquence pour les implémentations combinatoires. La figure 60 montre l'évolution de la surface en fonction de la fréquence, pour une dimension de réseau 128x32 et des niveaux d'itération 1/4, 1/8 et 1/16. Sur l'ensemble des résultats, les surfaces estimées se situent entre 10 000 um^2 et 35 000 um^2, variant selon les fréquences et les configurations choisies. Cela illustre les tendances générales ; notamment ce constat : à partir d'un certain seuil de fréquences les graphes montrent un accroissement rapide de la surface occupée. En deçà de ces fréquences, la surface estimée reste stable. Nous nommons cette indicateur « la fréquence de seuil » (*frequency threshold : Fth*).

Au-delà des fréquences de seuil, l'outil de synthèse doit optimiser les chemins des interconnexions pour respecter les délais. Cela explique l'accroissement de surface des circuits synthétisés. Pour chaque courbe, les résultats pour lesquels des violations de délais étaient détectées ont été retirés. Les extrémités des courbes indiquent ainsi une estimation des fréquences maximales pour les configurations correspondantes. Le paramétrage des circuits d'extraction est donc restreint en deçà de ces fréquences.

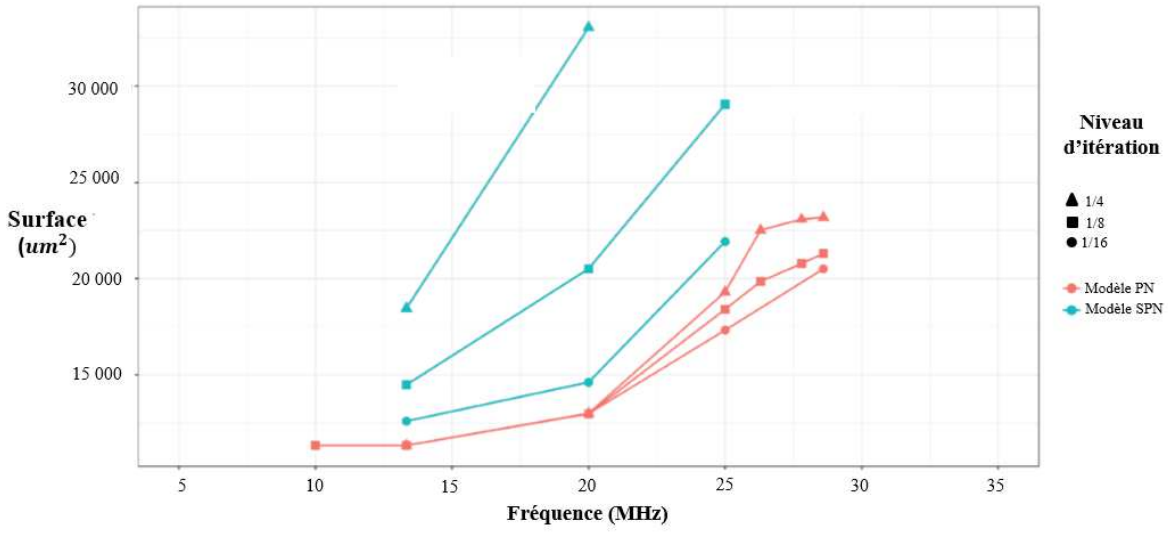

Figure 60: Surfaces des implémentations combinatoires PN et SPN - 128x32

Le choix de configuration a aussi une incidence, les synthèses pour des dimensions 128x8 et 128x16 montrent que la surface occupée s'accroit avec le nombre de colonnes. De plus, comme argumentée dans le chapitre 4, des SBOXs supplémentaires augmentent le coût de surface. Des écarts de surfaces sont ainsi constatés pour le modèle SPN selon le niveau d'itération. Le tableau 16 détaille plus précisément les surface et fréquences pour l'ensemble des configurations candidates.

Le modèle PN en dimension 128x32 a la plus haute fréquence maximale, 30 MHz, avec une surface de 25 300 et 28 300 um^2 (respectivement pour 1/1 et 1/2 en niveau d'itération). Cette configuration favorise une latence plus faible au détriment de la surface. Pour un compromis minimisant le cout de surface, le modèle SPN avec une dimension restreinte, 128x8, occupe seulement 9 200 um^2.

Tableau 16: Résultats pour les implémentation combinatoires PN et SPN à configuration optimale

Configuration du réseau (modèle – dimension – niveau d'itération)	Synthèse à la fréquence de seuil (Fth)		Synthèse la fréquence maximale (Fmax)	
	Surface total (um^2)	Fth (MHz)	Surface total (um^2)	Fmax (MHz)
PN - 128x32 - 1/1 (& 1/2)*	11 300	15	28 300	30
PN - 128x32- 1/2*	11 300	15	25 300	30
SPN - 128x32 - 1/4	16 500	15	33 000	20
SPN - 128x16 - 1/2	11 750	15	16 200	25
SPN - 128x8 - 1/1	9 200	15	14 500	25

Le choix de configuration pour le circuit d'extraction dépend ainsi des objectifs et des contraintes du cas d'usage du DPUF. Selon ces premiers résultats, le modèle PN doit être intégré en priorité si une fréquence élevée est requise ; dans le cas contraire, le modèle SPN en dimension 128x8 permet une surface plus réduite. Toutefois, le choix peut différer selon les contraintes. En dimension 128x8, le modèle SPN requière en effet un taux de connectivité supérieure à 25 % (selon les résultats d'évaluation, section 5.6). Si non, des dimensions supérieures doivent être privilégiées. De même, un réseau PN en dimension 128x32 requière un taux de connectivité supérieure à 50 %.

En ce qui concerne cette étude sur les implémentations combinatoires, les conclusions pour les compromis entre les différents paramètres et objectifs de conception sont les suivantes :

- *Modèle PN, dimension 128x32 (itération à 1/1), pour maximiser la fréquence ; avec un taux de connectivité supérieure à 50 %.*
- *Modèle SPN, dimension 128x8 (itération 1/1), pour réduire la surface ; avec un taux de connectivité supérieure à 25 %.*
- *Modèle SPN dimension 128x16 (itération 1/2)), dans le cas où la connectivité est limitée.*

6.3.2 Résultats des implémentations séquentielles

L'étude complémentaire des implémentations séquentielles montre l'amélioration des fréquences de circuits grâce aux registres d'états intermédiaires. Le graphe en figure 61 montre les résultats de surface pour deux configurations : un réseau PN de dimension 128x32 avec itération à 1/1 et un réseau SPN de dimension 128x32 avec itération à 1/2. La surface est exprimée en fonction de la fréquence, comme précédemment les résultats avec des violations de délais ne sont pas affichés. L'évaluation porte sur des niveaux de registres 4 et 8. Pour le modèle PN à 8 registres, la fréquence maximale acceptée monte jusqu'à 170 MHz, en restant en dessous des 25 000 um2. La fréquence de seuil se situe autour de 110 MHz ; pour laquelle la surface estimée est de 21 000 um^2.

La logique séquentielle accroit effectivement la fréquence de fonctionnement du circuit mais implique une surface d'occupation minimum plus élevée en comparaison: 21 000 um^2 contre 11 300 pour la même implémentation en combinatoire.

Cet écart correspond dans les rapports de surface à l'accroissement de l'aire non-combinatoire, de 1 200 um^2 à 10 900 um^2 due à l'intégration des 8 colonnes de registres.

Ces gains en fréquence sont d'un fort intérêt pour certains cas d'usage spécifiques du DPUF. En l'occurrence, si des contraintes de débits en sortie du DPUF doivent être respectées, l'équivalent d'une fréquence de 170 Mhz en débit, pour un circuit générant des réponses de 128 bits à chaque coup d'horloge est de 21.2 Gbits/s. Pour une fréquence de 30 MHz (meilleur résultat des implémentations combinatoires) le débit pour ces mêmes réponses est de 4.8 Gbits/s. L'apport du mode séquentiel est conséquent.

Toutefois, plusieurs cycles d'horloge sont nécessaires avant de retourner la réponse (pour le modèle PN 128x32, un niveau de 8 registres nécessite 8 cycles d'horloge). Cela augmente finalement la latence du circuit. Le réseau PN fonctionnant à fréquence de 170 MHz cela correspond à une latence approximative de 47 ns. Pour un réseau PN en combinatoire, à fréquence de 30 MHz, la latence est de 33 ns. Finalement, cela restreint l'intérêt de l'implémentation séquentielle à aux usages contraintes en débits et ce au détriment du coût en surface.

Les résultats sont similaires avec le modèle SPN, les tendances montrent un fort accroissement de fréquence proportionnel au niveau de registres intégrés entre les colonnes.

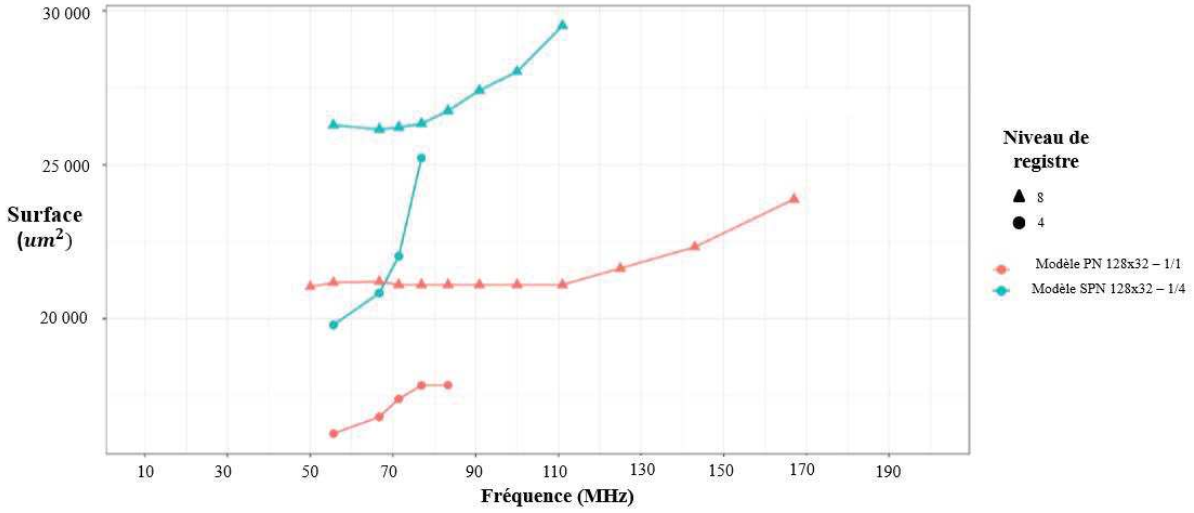

Figure 61: Résultats des implémentations séquentielles PN et SPN - 128x32

En conséquent, dans le cadre plus général d'une primitive d'authentification pour des circuits à bas coût, l'intérêt se porte avant tout sur les implémentations combinatoires.

6.4 Bilan et configuration finale pour le circuit SPN-DPUF

Pour les implémentations combinatoires, plusieurs configurations sont identifiées selon le compromis recherché. Le modèle SPN en dimension 128x16, itération à 1/2, se démarque avec des résultats de surfaces réduits, proche de la configuration inférieure en coût : respectivement 11 700 um^2 et 9 200 um^2 (surface pour un modèle SPN 128x8).

Nous considérons cette configuration finale de circuit d'extraction la plus adéquate pour répondre au compromis coûts – sécurité exigé pour une primitive strong DPUF. Nous conservons dans le bilan final les performances de différentes implémentations identifiées, l'implémentation minimisant la surface occupée (modèle SPN – 128x8 en combinatoire) et l'implémentation maximisant la fréquence (modèle PN – 128x32 en séquentiel avec 8 niveau de registre).

Les rapports de puissance de l'outil de synthèse permettent de compléter le bilan de cette configuration en fournissant une estimation de la puissance requise par le circuit implémenté. Dans ce bilan présenté dans le tableau 21, les indicateurs de surface, fréquence et de puissance sont utilisés pour déterminer les indicateurs normalisés (par bit).

Tableau 17 : Bilan de performances de la configuration finale du circuit d'extraction implémenté

Modèle	**SPN –128x16 – itération ½ - mode combinatoire**	**SPN –128x8 – itération 1/1 – mode combinatoire**	**PN –128x32 – itération 1/1 – mode séquentiel 8**
Contrainte sur le taux de connectivité	X	> 25 %	> 50 %
Unicité	0.4997 ~ 0.5001	0.4997 ~ 0.5001	0.4997 ~ 0.5001
Uniformité	0.4990 ~ 0.5010	0.4990 ~ 0.5010	0.4990 ~ 0.5010
Diffusion	0.4991 ~ 0.5005	0.4991 ~ 0.5005	0.4991 ~ 0.5005
Aire totale du circuit	11750 um^2	9200 um^2	21000 um^2
Aire normalisée	91.8 um^2 / bit	71.9 um^2 / bit	164 um^2 / bit
Fréquence de seuil (Fth)	15 MHz	15 MHz	110 MHz
Fréquence maximale (Fmax)	25 MHz	25 MHz	170 MHz
Débit (à Fth)	2,4 Gbits / s (Fth)	2,4 Gbits / s (Fth)	17.6 Gbits / s (Fth)
Latence (à Fth)	16 ns	16 ns	17.45 ns
Puissance total (à Fth)	0.4984 mW	0.4262 mW	3.313 mW
Énergie normalisée (à Fth)	0.0735 pJ / bit	0.0667 pJ / bit	4.836 pJ / bit

Les objectifs de conception définis en section 4.1.2 ciblaient à minima une surface inférieure à celles des primitives PUF identifiés dans la littérature, le SD-PUF (26000 um^2) et l'Arbiter PUF (22000 um^2) utilisé pour un mécanisme d'authentification au cours du cycle de vie [14]. La synthèse des configuration finales du circuit SPN-DPNF aboutit à des surfaces estimées inférieures, 11750 um^2 pour la configuration « équilibrée » (SPN – 128x16), à technologie d'intégration identique.

L'implémentation séquentielle du modèle PN permet des débits élevés, mais à des couts de surface et d'énergie supplémentaires. Ce choix de conception se restreint à des cas d'usages spécifiques.

Les performances du circuit SPN-DPUF, obtenues dans cette évaluation, valident les objectifs de conception de strong digital PUF, en termes de surface et de métriques de sécurité.

7 Conclusion et perspectives générales

7.1 Contributions pour la sécurité du cycle de vie

Les recherches menées au cours de la thèse apportent deux contributions au domaine de la sécurité matérielle : la formalisation des exigences de sécurité du cycle de vie des objets cyber-physiques et une proposition de primitive matérielle de type *digital PUF*, permettant d'adresser ces exigences et offrant un compromis sécurité-coût-robustesse.

L'analyse de sécurité du cas d'usage (dispositif médical, section 2) identifie les risques et les besoins de sécurité (2.3.3) au cours du cycle de vie. Le bilan argumente en faveur de solutions PUF, des briques matérielles qui implémentent des fonctions d'authentification pertinentes pour le cycle de vie et atténuent les risques induits par certaines menaces identifiées dans l'analyse. Un PUF assure une authenticité des circuits dès la fabrication et permet de déployer des clés d'authentification pour les différents acteurs du cycle de vie. Des contraintes spécifiques sont aussi établies : le PUF doit générer un large espace de réponses, respectant une qualité d'aléa élevée, et conserver une stabilité tout au cours du cycle de vie.

L'état de l'art sur la littérature PUF (section 3.3) pointe la nécessité de renforcer la stabilité des modèles classiques, sensibles au vieillissement ou aux perturbations extérieures. Certains modèles assurent toutefois une forte robustesse, notamment celui dit *digital PUF* (DPUF), basé sur des structures matérielles d'interconnexions aléatoires. L'étude des DPUFs existants conclue sur leur faisabilité et leur robustesse mais aussi sur le besoin de concevoir des circuits d'extraction (le circuit de lecture générant la réponse du DPUF à partir de la structure matérielle) plus performants.

La contribution spécifique pour ce besoin est la proposition d'un nouveau modèle d'extractions (section 4), dont le schéma logique se base sur les réseaux dits SPN (*substitution-permutation-network)*. Cela renforce les propriétés de sécurité, en particulier la diffusion, et assure la non prédictibilité des réponses du DPUF. Par la suite, le développement et l'évaluation de circuits modélisés permet de vérifier les métriques de sécurité et identifier le cas échéant les configurations requises, pour la taille et l'entropie de la structure matérielle mais aussi pour les paramètres du réseau SPN (section 5). La dernière partie de la thèse contribue en estimant les coûts de surfaces des implémentations VHDL de ces réseaux SPN pour les configurations identifiées (section 6). L'étude fournie un bilan détaillé pour concevoir un *digital PUF* performant répondant aux exigences de sécurité du cycle de vie. Des configurations optimales sont identifiées pour un compromis entre la surface occupée par le circuit, la fréquence et les métriques de sécurité. Ces premières estimations justifient que ces modèles SPN permettent la conception d'un strong digital PUF efficace.

Nous nommons cette primitive SPN-DPUF (*Substitution-Permutation Network based Digital PUF*). Cette primitive intégrée à la fabrication des puces électroniques, en amont de leur cycle de vie, constitue une brique matérielle pour la sécurité du cycle de vie. Elle sert ainsi de base pour déployer un protocole de sécurité, sécurisant les étapes suivantes du cycle de vie.

Le SPN-DPUF répond aux besoins de sécurité établis en section 2, contrairement à la majorité des autres contremesures qui ne couvrent pas toutes les exigences de sécurité. Elle apporte propriétés et fonctionnalités : la preuve d'authenticité du circuit et des acteurs, la capacité de générer des clefs de sécurité, la résistance à la contrefaçon et aussi la flexibilité des accès. Les propriétés d'aléa, notamment en termes d'unicité et de diffusion, permettent l'établissement d'un espace de réponses aléatoires large. Les réponses sont aisément distribuables et révocables pour les acteurs à divers moments du cycle de vie. Et ce, sans le risque d'instabilité des PUFs traditionnels.

7.2 Bénéfices du SPN-DPUF pour le compromis sécurité-coût

Les configurations de paramètres qui ont été identifiées offrent un compromis équilibré entre sécurité et surface occupée par le circuit (section 5.6 et section 6.4). L'évaluation de sécurité valide les métriques d'unicité, uniformité et diffusion, des indicateurs essentiels de la qualité de l'aléa extrait pour générer les réponses. La phase d'implémentation des circuits a permis d'affiner les choix de configurations pour une surface d'occupation réduite. Les résultats de surface atteignent les objectifs définis par rapport à la littérature des PUFs, notamment dans les études de solutions de sécurité pour le cycle de vie. Dans le modèle digital PUF précisé en figure 62, outre le coût du circuit d'extraction, il faut tenir compte de celui du procédé de fabrication de la structure matérielle aléatoire et de la surface occupée par celle-ci.

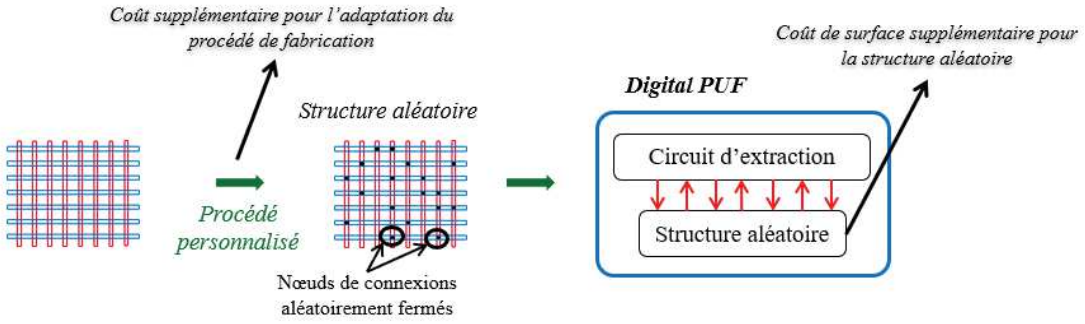

Figure 62: Modèle digital PUF et coût supplémentaire pour l'intégration

Le bilan final du SPN-DPUF montre que cette primitive répond à la nécessité de respecter les contraintes de ressources au cours du cycle de vie de l'objet cyber-physique dans lequel serait intégré le PUF. L'optimisation du circuit d'extraction est l'apport principal de la thèse pour la sécurité du cycle de vie, parmi les différents enjeux d'intégration et d'usage du SPN-DPUF présentés dans la figure 63.

Toutefois, la surface requise pour un strong digital PUF dépend aussi du choix du procédé de fabrication de la structure matérielle aléatoire. En fonction des choix technologiques, la structure matérielle pourrait accroitre l'aire totale de la primitive. Des recherches additionnelles doivent approfondir les coûts de fabrication de cette primitive, tenant compte des contraintes d'intégration et objectifs de coûts – performances. Entre autre, l'ajout du procédé personnalisé pour la génération de la structure impose une modification ou une adaptation de la phase de fabrication de la puce électronique. Cela implique, selon le procédé, un réglage spécifique des équipements de lithographie. Ces contraintes techniques, et leurs coûts associés, doivent donc être spécifiquement étudiés. Dans la figure 63, l'optimisation des implémentations technologiques de la structure matérielle est l'enjeu majeur pour la conception et l'intégration d'un SPN-DPUF efficace.

La bibliographie des DPUFs contient des solutions technologiques (section 3.5) prometteuses. La plus avancée, la technologie du VIA-PUF [84], respecte des normes de fiabilité fortes qui répondent à l'objectif de robustesse des PUFs. Des solutions innovantes récentes, telle que celle étudiée au CEA-Leti [108], pourraient aussi assurer une forte stabilité des nœuds de connexion ainsi qu'un aléa de qualité dans la répartition des états ouverts / fermés. Couplée avec les configurations optimales pour le circuit d'extraction SPN-DPUF, cela permettrait la conception d'une primitive de sécurité efficace et sure.

Pour conclure, notre étude apporte une base solide pour concevoir un strong *digital PUF,* intégrable dès le début du cycle de vie et assurant les propriétés de sécurité et le niveau de performances requis. Cela répond au besoin de sécuriser le cycle de vie en amont des phases de déploiement et d'utilisation, et ce en respectant des exigences de coûts. Le déploiement de protocoles de sécurité basés sur le DPUF permettra de répondre ensuite aux besoins d'usage, tel que l'authentification des acteurs du cycle de vie.

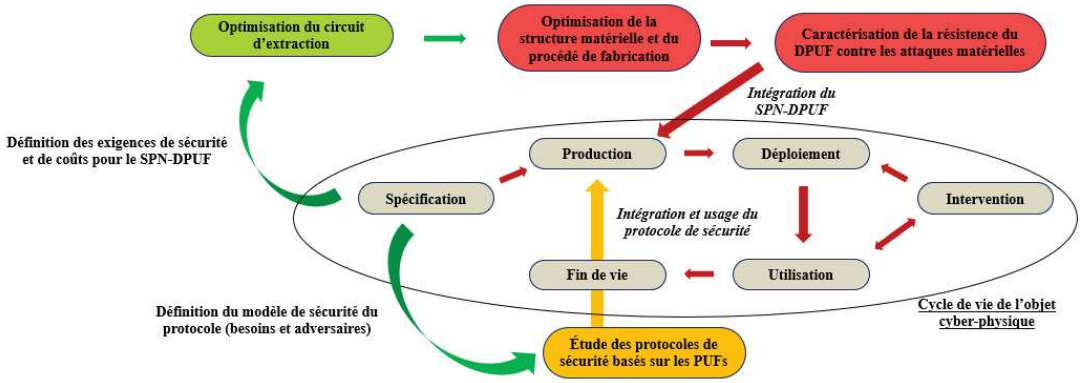

Figure 63: Enjeux et perspectives pour l'intégration et l'usage du SPN-DPUF pour la sécurité du cycle de vie

7.3 Perspectives générales

Intégré dès la fabrication, une primitive SPN-DPUF apporte des propriétés d'identification et d'authentification fortes. Les paires de challenge-réponse générées servent de sources d'information sûres pour déployer des protocoles de sécurité. La poursuite des études est toutefois nécessaire, au niveau de la conception matérielle, de l'évaluation de la sécurité et d'autre part au niveau protocolaire et intégration de la primitive.

Une étude complémentaire doit affiner les coûts de fabrication et de surface liés à la structure matérielle, mais aussi caractériser l'entropie spécifique à celle-ci c'est à dire déterminer précisément les lois de répartition des états ouverts et fermés des nœuds de connexion. Une phase d'optimisation doit identifier les paramètres de fabrication idéales pour réduire les coûts et respecter les contraintes liées à l'entropie de la structure matérielle.

Selon le cas d'usage considéré il sera nécessaire de caractériser la résistance du DPUF face à certains types de menaces. La primitive assure un niveau de sécurité face aux risques de contrefaçons ou d'accès matériel malveillants via les ports de communications classiques (type JTAG). Toutefois, des menaces subsistent : les attaques par canaux cachés et les intrusions matérielles avancées. Les risques induits par ces menaces dépendent de plusieurs facteurs : la sensibilité du cas d'usage (quels sont les moyens et motivations des adversaires) mais aussi les choix technologiques pour la conception du DPUF. La sécurité du SPN-DPUF varie toutefois selon les caractéristiques de la structure aléatoire et du circuit d'extraction. La fuite d'information en termes de canaux auxiliaires (consommation, émanations électromagnétiques) et de rétro-ingénierie de la structure dépendent entre-autres de l'accessibilité des nœuds de connexion, de leur taille et de leur modèle de consommation.

La dernière problématique complexe pour la solution DPUF concerne l'intégration de celle-ci dans l'architecture d'un système sur puce (SoC). L'intégration doit tenir compte des contraintes et des spécificités du système. Il faut ainsi définir une architecture permettant d'intégrer facilement ce type de structures dans les SoCs et permettre son utilisation de façon sécurisée par les autres éléments du circuits. Par exemple, ce type de primitives devraient permettre de sécuriser des mécanismes de débogage implémentés dans le SoC et gérer l'authentification des différents utilisateurs du mécanisme de débogage. Cela impose une étude conséquente pour proposer un SoC sécurisé avec le DPUF, tenant compte des modèles de sécurité et des contraintes du cycle de vie du SoC.

Le DPUF nécessite aussi le déploiement de protocole pour l'authentification au cours du cycle de vie. Ce dernier aspect est toutefois traité dans la littérature. Jeroen Delvaux offre un état de l'art complet et précis des solutions existantes [75]. Le choix d'un tel protocole se fait en fonction des besoins et des modèles de sécurité. Par exemple la solution peut tenir compte des risques d'interception des échanges protocolaires et intégrer des fonctions de hachages en amont et en aval du DPUF pour sécuriser

ces échanges. Des protocoles peuvent aussi être développés pour des usages spécifiques, tels que les mises à jour sécurisées ou la vérification de l'intégrité des micrologiciels et des données du SoC.

Une fois le protocole déployé, des enjeux de sécurité de plus haut niveaux sont aussi à considérer tels que les questions de gouvernance vis-à-vis de l'étape de génération des paires de challenge-réponse et la protection des bases de challenges-réponses. Cela impose la sécurisation de l'administration des accès à cet base mais aussi la mise en place de procédures de révocation et d'attribution de paires de challenge-réponse. Cela permet d'adapter les autorisations d'accès au SoC par les différents acteurs via des ensembles de paires challenge-réponse, attribuables et révocables au cours du cycle de vie.

8 Listes des publications

Publications soumises et acceptées en conférences

J. Marconot, D. Hély et F. Pebay-Peyroula, « IoT Components LifeCycle based Security Analysis », *Digital System Design (DSD),* Vienne, 2017

J. Marconot, D. Hély et F. Pebay-Peyroula, « SPN-DPUF: Substitution-Permutation Network based Secure Circuit for Digital PUF », *IEEE Symposium on VLSI (ISVLSI),* Miami, 2019

Publication soumise et acceptée en journal

J. Marconot, D. Hély et F. Pebay-Peyroula, « Conception and Evaluation of Secure Circuits for Strong Digital PUF », pour l'appel à publication "Special Issue : Hardware-Assisted Security Solutions for Electronic Systems" du journal *Spring Nature Computer Science Journal,* 2020

Posters présentés en séminaires et conférences

J. Marconot, D. Hély et F. Pebay-Peyroula, « IoT Components LifeCycle based Security Analysis », *Digital System Design (DSD),*Vienne, 2017

J. Marconot, D. Hély et F. Pebay-Peyroula, « Implementation and Evaluation of Digital PUF Primitive for Chip Lifecycle Hardware Security », à l'école d'été *Cyber In Occitanie* du LIRMM, Montpellier, 2018

9 Bibliographie

[1] S. Ray, S. Sur-Kolay et S. Bhnia, «The Landscape of SoC and IP Security,» dans *Fundamentals of IP and SoC Security*, Springer International Publishing, 2017.

[2] J. Ma et M. Tehranipoor, «Background on VLSI Testing,» dans *Introduction to Hardware Security and Trust*, Springer New York, 2012.

[3] C. Ehrel et L. La Raudière, «Rapport d'information par la commission des affaires éconoomqiesu sur les objets connectés,» Assemblée Nationale Française, 2017.

[4] Parlement Européen, «Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,» 2016.

[5] K. Rosenfeld et R. Karri, «Attacks and Defenses for JTAG,» *IEEE Design &Test of Computers,* vol. 27, pp. 36-47, 2010.

[6] P. Rajput et M. Maniatakos, «JTAG: A Multifaceted Tool for Cyber Security,» *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS),* 2019.

[7] M. Tehranipoor et F. Koushanfar, «A Survey of Hardware Trojan Taxonomy and Detection,» *IEEE Design and Tests of Computers,* 2010.

[8] E. Marin, D. Singelee, B. Yang, I. Verbauwhede et B. Preneel, «On the Feasability of Cryptography for a Wireless Insulin Pump System,» *CODASPY' 16, ACM.*

[9] Wikipedia, the frre encyclopedia, «2016 Dyn cyberattack,» Wikipedia, 2016. [En ligne]. Disponible: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack. [Accès le 2016].

[10] M. Rostami, F. Koushanfar et R. Karri, «A Primer on Hardware Security,» *Proceedings of the IEEE 102(8),* pp. 1283-1295, 2014.

[11] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor et Y. Makris, «Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,» *Proceedings of the IEEE,* 2014.

[12] S. Ray, S. Bhunia et P. Mishra, «2.4 Adversaries in SoC Security,» dans *Fundamentals of IP and SoC Security*, Springer International Publishing, 2017.

[13] J. Backer, d. Hely et R. karri, «Secure and Flexible Trace-Based Debugging of Systems-on-Chip,» *ACM Transactions on Design Automation of Electronic Systems,* 2015.

[14] J. Backer, D. Hely et R. Karri, «Secure Design-for-Debug for System-on-Chip,» *International Test Conference,* 2015.

[15] J. Skudlarek, T. Katsioulas et M. Chen, «A Platform Solution for Secure Supply-Chain and Chip Life-Cycle Management,» *IEEE Computer Society,* 2016.

[16] P. E. e. C. d. l. Européenne, «Règlement (UE) 2017/745 relatif aux dispositifs médicaux,» 2017.

[17] Agence National de Sécurité du Médicament et des Produit de Santé, «Mise sur le marché des dispositifs médicaux et dispositifs médicaux de diagnostic in vitro (DM/DMIA/DMDIV),» [En ligne]. Disponible: http://ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/(offset)/0. [Accès le 12 03 2018].

[18] M. Zhang, A. Raghunathan et N. Jha, «Trustworthiness of Medical Devices and Body Area Networks,» *Proceedings of the IEE 102(8),* 2014.

[19] P. Williams et A. Woodward, «Cybersecurity Vulnerabilities in Medical Devices: a Complex Environment and Multifaceted Problem,» *Medical Devices: Evidence and Research,* 2015.

[20] A. Burns, M. Johnson et P. Honeyman, «A Brief Chronology of Medical Device Security,» *Communication of the ACM,* vol. 50, 2016.

[21] Food and Drug Administration, «Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,» 2014.

[22] Fond and Drug Administration, «Postmarket Management of Cybersecurity in Medical Devices,» 2016.

[23] ANSSI, «Expression of Needs and Identification of Security Objectives: Methodology Guidance,» 2010.

[24] ANSSI, «Expression of Needs and Identification of Security Objectives: Base of Knowledge,» 2010.

[25] Fédération Française des Diabétiques, «Qu'est ce que le diabète,» [En ligne]. Disponible: https://www.federationdesdiabetiques.org/information/diabete . [Accès le 09 02 2017].

[26] S. Zavitsanou, A. Chakrabarty, E. Dassau et F. Doyle, «Embedded Control in Wearable Medical Devices: Application to the Artificial Pancreas,» *Processes,* vol. 4, 2016.

[27] IEEE, «Health informatics--Personal health device communication-Part 10419: Device Specialization--Insulin Pump,» 2018.

[28] IEEE, «Health informatics--Personal health device communication - Part 10425: Device Specialization--Continuous Glucose Monitor (CGM)».

[29] Fédération Française des Diabétiques, «Les étapes du traitement,» [En ligne]. Disponible: https://pompeainsuline.federationdesdiabetiques.org/comment-ca-marche/les-etapes-du-traitement/. [Accès le 28 02 2018].

[30] John Mossman, «Insulin Pumps: design basics and tradeoffs,» 05 17 2010. [En ligne]. Disponible: https://www.eetimes.com/document.asp?doc_id=1278073 . [Accès le 02 03 2018].

[31] Giacomo Cappon, «Wearable Continuous Glucose Monitoring Sensors: A Revolution in Diabetes Treatment,» *Electronics 2017,* 2017.

[32] Medical Device Privacy Consortium, «Security Risk Assessment Framework for Medical Device».

[33] R. Maes, «Physically Unclonable Functions : Constructions, Properties and Applications,» Th, Arenberg Doctoral School of Science, Engineering & Technology, 2012.

[34] U. Rührmair, S. Devadas et F. Koushanfar, «Security based on Physical Unclonability and Disorder,» dans *Introduction to Hardware Security and Trust*, Springer, 2012.

[35] J. Plusquellic, «PUF based authentication,» dans *Fundamentals of IP and SoC Security*, Springer, 2017.

[36] R. Pappu, «Physical One-Way Functions,» Th, MIT, 2001.

[37] B. Gassend, D. Clarke, M. Van Dijk et S. Devadas, «Controlled Physical Random Functions,» 2002.

[38] B. Halak, «Chapitre 2.4 : The Origins Physical Disorder in Integrated Circuits,» dans *Physically Unclonable Functions*, Southampton, UK, Springer, 2018.

[39] C. H. Chang, Y. Zheng et L. Zhang, «A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement,» *IEEE Circuits and Systems Magazine,* pp. 32 - 62, 2017.

[40] T. McGrath, I. Bagci, Z. Wang, U. Roedig et R. Young, «A PUF Taxonomy,» *Applied Physics Review,* 2019.

[41] R. Maes, «Section 2.4.4 : SRAM-PUF,»*Physically Unclonable Functions : Construction, Properties and Applications*, Th, Arenberg Doctoral School of Science, Engineering & Technology, 2012.

[42] J. Guajardo, S. Kumar, G. Schrijen et P. Tuylis, «FPGA Intrinsics PUFs and Their Use for IP Protection,» *Workshop on Cryptographic Hardware and Embedded Systems - CHES,* pp. 63 - 80, 2007.

[43] D. Holcomb, W. Burleson et K. Fu, «Initial SRAM State as a Fingerprint and Source of a True Random Numbers for RFID Tags,» *Workshop on RFID Security and Privacy - RFIDSec,* 2007.

[44] J. Lee, D. Lim, B. Gassend, G. Suh, M. Dijk et S. Devadas, «A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications,» *Symposium on VLSI,* 2004.

[45] R. Maes, «Section 2.3 : Terminology and Classification,» dans *Physically Unclonable Functions : Constructions, Properties and Applications*, Th, Arenberg Doctoral School of Engineering, 2012.

[46] A. Wali, a. Dodda, Y. Wu, A. Pannone, L. Usthili, S. Ozdemir, I. Ozbolat et S. Das, «Biological Physically Unclonable Function,» *Communications Physics,* 2019.

[47] R. Maes, «Section 3.2 : A Discussion on the Properties of PUFs,» dans *Phyically Unclonable Functions : Constructions, Properties and Applications*, Th, Arenberg Doctoral School of Engineering, 2012.

[48] R. Van der Berg, «Section 3.1 : Properties,» dans *Entropy Analysis of Physical Unclonable Function*, Th, Eindhoven University of Technology, Master, Department of Mathematics and Computer Science, 2012.

[49] B. Halak, «Section 2.9 : Evaluation Metrics of PUF Devices,» dans *Physically Unclonable Functions*, Springer, 2018.

[50] A. Van herrewege, «Section 2.6 : Quality Metrics,» *Lightweight PUF-based Key and Random Number Generation*, Th, KU Leuven, Arenberg Doctoral School, 2015.

[51] U. Mureddu, «Evaluation de la sécurité des PUFs,» *Génération d'aléa dans les circuits électroniques numériques exploitant des cellules oscillantes*, Th, Laboratoire Hubert Curien, Université de Lyon, 2019.

[52] U. Mureddu, «Section 1.1.2.2 : Unicité,» *Génération d'aléa dans les circuits électroniques numériques exploitant des cellules oscillantes*, Th, Laboratoire Hubert Curien, Université de Lyon, 2019.

[53] A. Van Herrewege, «Section 2.6.3 : Inter-device distance,» dans *Lightweight PUF-based Key and Random Number Generation*, Th, KU Leuven, Arenberg Doctoral School, 2015.

[54] Intrinsic ID, «White Paper - SRAM-PUF: The Secure Silicon Fingerprint,» Eindhoven, 2017.

[55] R. Maes, «Section 5.2.2 : Fuzzy Identification,» dans *Physically Unclonable Functions : Constructions, Properties and Applications*, Th, Arenberg Doctoral School of Engineering, 2012.

[56] C. Shannon, «Communication Theory of Secrecy Systems,» *Bell System Technical Journal,* vol. 28, n° 14, pp. 656-715, 1949.

[57] A. Maiti, V. Gunreddy et P. Schaumont, «A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions,» dans *Embedded Systems Design with FPGAs*, vol. 9781461413622, 1 November 2013, pp. 245-267.

[58] A. Van Herrewege, «Section 2.6.5 : Self-similarity,» dans *Lightweight PUF-based Key and Random Number Generation*, Th, KU Leuven, Arenberg Doctoral School, 2015.

[59] B. Halak, «Section 5.4 Security Evaluation Metrics for PUF,» dans *Physically Unclonable Functions*, Springer, 2018.

[60] B. Halak, «Section 5.4.4 : Unpredictability,» dans *Physically Unclonable Functions*, Springer, 2018.

[61] A. Van Herrewege, «Section 2.6.7: Entropy,» dans *Lightweight PUF-based Key and Random Number Generation*, Th, KU Leuven, Arenberg Doctoral School, 2015..

[62] B. Halak, «Section 5.42 :Randomness,» dans *Physically Unclonable Functions*, Springer, 2018.

[63] U. Mureddu, «Section 1.1.2.2: Méthode d'évaluation moderne,» *Génération d'aléa dans les circuits électroniques numériques exploitant des cellules oscillantes*, Th, Laboratoire Hubert Curien, Université de Lyon, 2019.

[64] NIST - National Institute of Standards and Technology, «A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,» Technology Administration and U.S. Department of Commerce , 2010.

[65] Wikipedia , «Diehard tests,» 10 12 2019. [En ligne]. Disponible: https://en.wikipedia.org/wiki/Diehard_tests. [Accès le 08 01 2020].

[66] W. Killmann et W. Schindler, «A proposal for: Functionality classes for random number generators,» German Federal Officle for Information Security, 2011.

[67] U. Rührmair et e. al, «PUF Modeling Attacks on Simulated and Silicon Data,», *IEEE Transactions on Information Forensics and Security*, *V*ol 8, 2013.

[68] U. Rührmair et J. Sölter, «PUF Modeling Attacks: An Introduction and Overview,» Design, Automation & Test in Europe Conference & Exhibition (DATE) 2014.

[69] N. Q. Noor, S. Daud, N. A. Ahmad, N. Maarop, N. Sa'at et N. Aziz, «Defense Mechanisms against Machine Learning Modeling Attacks on Strong PHysical Unclonable Functions for IOT Authantication: A Review,» *Internation Journal of Advanced Computer Science and Applications,* vol. 8, n° 110, pp. 128-137, 2017.

[70] F. Armknecht, D. Moriyama, A.-R. Sadeghi et M. Yung, «Towards a unified security model for physically unclonable functions,» dans *Cryptographers' Track at the RSA Conference*, 2016.

[71] J.-L. Danger, S. Guilley, P. Nguyen et O. Rioul, «PUFs: Standardization and Evaluation,» *Mobile Systems Technologies Workshop,* pp. 12 - 18, 2016.

[72] National University of Singapore, Department of Electrical and Computer Engineering, «Database of Physically Unclonable Functions,» [En ligne]. [Accès le 14 11 2018].

[73] International Standard ISO/IEC, «Information Technology - Security Techniques - Lightweight Cryptography,» 2012.

[74] Intrinsic ID, «White Paper: Flexible Key Provioning with SRAM PUF,» 2017.

[75] J. Delvaux, «Section 5: A Survey on PUF-Based Entity Authentication,» dans *Security Analysis of PUF-based Key Generation and Entity Authentication*, Th, KU Leuven & Shangai Jiao Tong University, 2017.

[76] J. Delvaux, D. Gu, D. Schellekens et I. Verbauwhede, «Secure Lightweight Entity Authentication with Strong PUFs», CHES 2014

[77] B. Halak, «Section 4 : Reliability Enhancement Techniques for Physically Unclonable Functions,» dans *Physically Unclonable Functions*, Springer, 2018.

[78] J. Delvaux et I. Verbauwhede, «Attacking Puf-based pattern matching key generators via helper data manipulation,» dans *Conference on Cryptographer's Track at the RSA*, San Francisco, 2014.

[79] B. Colombier, L. Bossuet, V. Fischer et D. Hely, «Key reconcialiation Protocols for Error Correction of Silicon PUF Responses,» *IEEE Transactions on Information Forensics and Security,* vol. 12, n° 18, 2017.

[80] J. Miao, M. Li, S. Roy et B. Yu, «Learning Resilient and Reliable Digital Physical Unclonable Function,» *IEEE/ACM International Conference on Computer-Aided Design,* 2016.

[81] J. Miao, M. Li, S. Roy, Y. Ma et B. Yu, «SD-PUF: Spliced Digital Physical Unclonable Function,» *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2017.

[82] T. W. Kim, B. D. Choi et D. K. Kim, «Zero bit error rate ID generation circuit using VIA formation probability in 0.18 um CMOS process,» *Electronics Letters,* vol. 50, n° 112, pp. 876-877, 2014.

[83] D. Jeon, J. H. Baek, D. K. Kim et B. D. Choi, «Toward Zero Bit-Error-Rate Physical Unclonable Function: Mismatch-Based vs. Physical-Based Approaches in Standard CMOS Technology,» dans *Euromicro Conference on Digital System Design*, 2015.

[84] D. Jeon, Y. D. Kim et D. K. Kim, «A Physical Unclonable Function With Bit Error Rate < 2.3 × 10−8 Based on Contact Formation Probability Without Error Correction Code,» *IEEE Journal of Solid-State Circuits,* 2019.

[85] W.-C. Wang, Y. Yona, S. Diggave et P. Gupta, «LEDPUF: Stability-guaranteed physical unclonable function through locally enhanced defectivity,» *IEEE HOST,* pp. 25-30, 2016.

[86] W.-C. Wang, Y. Yona, S. Diggavi et P. Gupta, «Design and Analysis of Stability-Guaranteed PUFs,» *IEEE Transactions on Information Forensics and Security,* vol. 13, n° 14, 2018.

[87] Z. Hu, J. M. Lobez Comeras, H. Park, J. Tang, A. Afzali, G. Tulesvski, J. Hannon, M. Liehr et S.-J. Han, «Physically Unclonable Cryptographic Primitives using Self-assembled Carbon Nanotubes,» *Nature Nanotechnology,* vol. 11, pp. 559-566, 2016.

[88] L. Lio, H. Huang et S. Hu, «Lorenz Chaotic System-Based Carbon Nanotube Physical Unclonable Functions,» *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 37, n° 17, pp. 1408-1421, 2018.

[89] N. Kumar, J. Chen, M. Kar, S. Sitaraman, S. Mukhopadhyay et S. Kumar, «Multigated Carbon Nanotube Field Effect Transistors-Based Physically Unclonable Functions As Security Keys,» *IEEE Internet of Things Journal,* vol. 6, n° 11, pp. 325-334, 2019.

[90] D. Jeon et B.-D. Choi, «Circuit Design of Physical Unclonable Function for Security Applications in Standard CMOS Technology,» *IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC),* 2016.

[91] ICTK, «Our Technology: a Provably Secure Root of Trust,» [En ligne]. Disponible: https://ictk-puf.com/puf-technology/. [Accès le 21 01 2020].

[92] W.-C. Wang, Y. Yona, S. Diggavi et P. Gupta, «Design and Analysis of Stability-Guaranteed PUFs,» *IEEE Transactions on Information Forensics and Security,* vol. 13, n° 14, pp. 978-992, 2018.

[93] J. Miao, M. Li, S. Roy, Y. Ma et B. Yu, «SD-PUF: Spliced Digital Physical Unclonable Function,» 2017.

[94] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin et C. Vikkelsoe, «PRESENT: An Ultra-Lightweight Block Cipher,» *Cryptographic Hardware and Embedded Systems - CHES,* 2007.

[95] Europe1.fr avec AFP, «Charente-Maritime : des élus et des diabétiques s'inquiètent de l'arrêt d'un dispositif médical,» Europe 1, 07 08 2019. [En ligne]. Disponible: https://www.europe1.fr/sante/charente-maritime-des-elus-et-des-diabetiques-sinquietent-de-larret-dun-dispositif-medical-3913306. [Accès le 10 02 2020].

[96] Intrinsic ID, «Accelerated Lifetime Test,» dans *White Paper - The reliability of SRAM-PUF*, 2017.

[97] P. Chao, X. Yang, L. Wei et H. Xiaojia, «Trade-off of Security and Performance of Lightweight Block Ciphers in Industrial Wireless sensor Networks,» *EURASIP Journal on Wireless Communications and Networking,* 2018.

[98] S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne et R. Tourki, «Performance Evaluation and Design Considerations of Lightweight Block Cipher for Low-Cost Embedded Devices,» *IEEE/ACS 13th International Conference of Computer Systems and Applications,* 2016.

[99] P. Peter et H. Michael, «Pushing the Limits of SHA-3 Hardware Implmentations to Fit on RFID,» *International Conference on Cryptographic Hardware and Embedded Systems,* pp. 126-141, 2013.

[100] H. Shi, Y. Deng, T. Xie, D. Xu et J. Gong, «Study and Comparison on the Avalanche Property of the AES and the Camellia,» *International Conference on Electrical and Control Engineering,* 2011.

[101] A. Webster et S. Tavares, «On the Design of SBOXES,» *Lecture notes in Computer Sciences; 218 on Advances in Cryptology - CRYPTO 85,* 1970.

[102] G. Leander et A. Poschmann, «On the Classification of 4 Bit S-Boxes,» *International Workshop on the Arithmetic of Finite Fields,* 2007.

[103] M. Wong, M. L. D. Wong, I. Hijazin et A. K. Nandi, «Composite field GF(((2^2)^2)^2) AES S-Box with direct computation in GF(2^4) inversion,» *7th International Conference on Information Technology in Asia,* 2011.

[104] M. Wong, M. Wong, I. Hijazin et A. Nandi, «Composite Field GF(((2)^2)^2)^2) AES S-Box with Direct Computation in GF(2)^4) Inversion,» *7th International Conference on Information Technology in Asia,* 2011.

[105] Mentor Graphics, «Questa Advanced Simulator,» [En ligne]. Disponible: https://www.mentor.com/products/fv/questa/. [Accès le 05 2020].

[106] Synopsys, «Design Compiler Graphical, Create a Better Starting Point for Faster Physical Implementation,» 05 2020. [En ligne]. Disponible: https://www.synopsys.com/implementation-and-signoff/rtl-synthesis-test/design-compiler-graphical.html.

[107] Silvaco, «PDK 45nm Open Cell Library,» 05 2020. [En ligne]. Disponible: https://www.silvaco.com/products/nangate/FreePDK45_Open_Cell_Library/.

[108] F. Pebay-Peyroula et M. May, «METHOD OF SECURING AN INTEGRATED CIRCUIT DURING MANUFACTURING». France Brevet US20180358310, 13 12 2018.

10 Annexes

10.1 Complément sur la terminologie et classification des dispositifs médicaux

Application de « bien-être » : Les produits de « bien-être ou de confort », aussi appelés produits ou applications de santé mobile, sont à distinguer des dispositifs médicaux. Le règlement [16] considère : « […] que les logiciels destinés à des usages généraux, même lorsqu'ils sont utilisés dans un environnement de soins, ou les logiciels destinés à des usages ayant trait au mode de vie ou au bien-être, ne constituent pas des dispositifs médicaux ».

Dispositif médical : Selon l'article 2.1 du règlement un produit relève du statut dispositif médical (DM) pour « tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes:

- […] traitement d'une maladie,
- […] traitement d'une blessure ou d'un handicap ou compensation de ceux-ci,
- Investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique,
- Communication d'informations au moyen d'un examen in vitro […],

Et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques […]

Accessoire de dispositif médical : « Tout article qui, sans être lui-même un dispositif médical, est destiné […] à être utilisé avec un ou plusieurs dispositifs médicaux données pour permettre une utilisation […] contribuer spécifiquement à la fonction médicale […]

Ces définitions précisent le périmètre du domaine médical : un dispositif a le qualificatif « médical » s'il répond à un état de santé défaillant, et non pas un besoin de bien-être, confort ou de diagnostic physiologique à finalités sportive. ». Des applications mobiles pour le suivi du rythme cardiaque lors de l'activité sportive ne rentrent pas dans le champ d'application du règlement. Par contre la définition d'accessoire inclut des systèmes complémentaires des DMs, assurant son fonctionnement ou son usage, par exemple les chargeurs de batterie. Le règlement de l'U.E. en 1.4, précise que ces accessoires sont soumis aux mêmes contraintes. Il faut noter que le niveau de risque associé à un produit ne justifie pas le statut de celui-ci en tant que DM ; il intervient par contre dans les règles de classification des DMs

Classification des dispositifs : Le règlement de l'U.E. – article 51 – stipule que « Les dispositifs sont répartis dans quatre classes (I, IIa, IIb, III) en fonction de la destination (usage) des dispositifs et des risques qui leur sont inhérents. La classification est effectuée conformément à l'annexe VIII. » La dangerosité du dispositif pour le patient et le personnel médical est donc prise en compte dans les règles de classification. Tous les critères interviennent, tels que :

- La nature de l'usage (diagnostic, mesure, injection, stimulation…)
- La durée d'utilisation du DM
- Le caractère invasif (est-ce un dispositif implanté ? de type chirurgical ?)
- La localisation du DM (le DM est-il en contact avec des parties sensibles du corps ?)

Chaque classe se voit attribuer des contraintes réglementaires spécifiques, des exigences de plus grande sévérité à mesure que la criticité du dispositif augmente. Nous décrivons des exemples de DM pour chaque classe avec une brève interprétation des règles de classifications. (Voir l'annexe VIII du règlement) Le niveau de criticité des DMs augmente s'ils ont un caractère actif, un caractère invasif, une longue durée d'utilisation, ou un usage critique tel que l'injection de médicament ou une interaction avec des organes vitaux du patient.

- *Classe I - Electrodes pour électrocardiographie (ECG) :* L'électrocardiographie mesure et affiche l'activité cardiaque d'un patient. L'opération nécessite l'utilisation d'électrodes posées sur le torse du patient pour recueillir la fréquence cardiaque. Ces dispositifs présentent les caractéristiques suivantes : non-invasifs, durée d'utilisation courte, pas de contact avec une partie sensible du corps, pas de modification biologique ou corporel. De plus une mesure médicale sera réalisée avec plusieurs électrodes offrant une redondance de l'information. Dans ce cas-là l'interaction est limitée et l'impact en cas de défaillance est faible : le dispositif se classe dans la catégorie la moins critique.
- *Classe IIa – Tensiomètre :* Le tensiomètre mesure la tension artérielle pour diagnostiquer les cas d'hypertension ou d'hypotension. Du fait qu'il soit non-invasif, isolé d'autres équipements médicaux, utilisé dans des situations « non-urgentes » (c'est-à-dire au cours d'examens routiniers où la vie du patient n'est pas en danger) le dispositif a un niveau de criticité faible. Une compromission de l'objet risque toutefois de fausser le diagnostic. Cela le qualifie à minima dans la classe IIa.
- *Classe IIb - Pompe à perfusion :* Dans la classe IIb nous pouvons retrouver les dispositifs actifs destinés à administrer des médicaments potentiellement dangereux. (Règle 12 sur les DMs actifs). Par exemple une pompe à perfusion : un système avec un mécanisme d'injection.
- *Classe III - Stimulateur cardiaque (pacemaker) :* Ce dispositif est implanté dans la cage thoracique des patients. Il génère des impulsions électriques pour stimuler des muscles cardiaques défaillants. Il a un caractère invasif et soutient l'activité cardiaque du malade. Ces deux points, quel que soit le temps d'utilisation, positionne le DM en classe III. (Voir les règles 6, 7 et 8)

10.2 Analyses EBIOS détaillée

10.2.1 Méthodologie EBIOS

La méthodologie EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été élaboré en 1995 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qui fournit

plusieurs documents de références, le guide détaillé [23] ainsi que [24], une base de connaissance pour l'énumération des types de menaces. EBIOS est une méthode générique qui s'adapte au contexte, le « bien » à protéger peut-être une infrastructure, un service interne d'une entreprise ou une application logicielle. Les objectifs de sécurité varient : cartographie des risques, mise en œuvre d'une politique de sécurité ou évaluation plus technique et précise des protections. La figure 11 présente les cinq modules de la méthode EBIOS. : l'étude de contexte, l'estimation des événements redoutés et de leur impact, la description des scénarios de menaces, la synthèse des risques et l'évaluation des contremesures.

Comme décrit par la figure 64 la synthèse des risques consiste à coupler les événements redoutés avec les scénarios de menaces. Ces deux modules s'appuient respectivement sur les cotations suivantes : un niveau d'impact (quels dégâts occasionnent l'événement) et un niveau de vraisemblance (crédibilité de la mise en œuvre du scénario de menaces par un adversaire). Le cinquième et dernier module n'est pas nécessaire dans le cas où l'étude se limites à l'établissement d'une cartographie des risques.

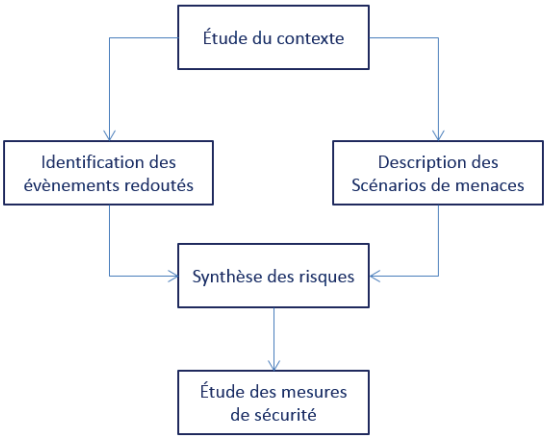

Figure 64: Modules de la méthodologie EBIOS

Objectifs : Notre étude de sécurité se focalise sur les risques induits par le cycle de vie du DM et par les problématiques d'authentification et de gestion des accès au cours des diverses opérations :

- Authentification des acteurs et des biens, impliqués dans plusieurs phases du cycle de vie.
- Multiplication des accès et des interactions qui requièrent un certain niveau de sécurité.
- Gestion des autorisations, avec une flexibilité requise pour l'exploitation du DM.

Ces questions impactent la sécurité du DM au cours du cycle de vie et accroissent le niveau de risque. Le premier objectif est l'identification des exigences de sécurité qui découlent de ces enjeux ; cela est établi au cours du module 4 qui étudie les risques significatifs. Le deuxième objectif est l'identification de contremesures adéquates qui répondent à ces besoins de sécurité.

10.2.2 Module 1 – étude de contexte

Notre cas d'étude concerne le dispositif médical *Pancréas Artificiel*, composé des trois sous-dispositifs (dispositif d'injection, dispositif d'observation, dispositif de contrôle). L'analyse considère les composants du DM au cours de l'ensemble du cycle de vie, pas uniquement au cours de l'exploitation. Le module nous amène à définir les biens essentiels et les exigences de base des propriétés de sécurité. Les biens essentiels de notre sujet d'étude sont les éléments pour lesquels une compromission aurait un impact sur la santé du patient, la vie des utilisateurs et la situation du fabricant légal (OEM). Le périmètre de l'étude et le choix des biens essentiels dépends du niveau d'abstraction et de détail exigé. Le périmètre

peut être large ou fortement restreint. Une première approche serait par exemple de considérer comme biens essentiels à protéger uniquement la commande d'injection (le traitement final du DM) et la clef de sécurité du fabricant. Dans notre étude nous prenons un cadre élargi qui englobe les différents modules logiciels, les diverses catégories de données exploitées et les informations d'authentification des acteurs. Nous souhaitons mettre en avant les problématiques de sécurisation des interactions ; nous restons à un niveau relativement abstrait pouvant inclure les biens associés à l'ensemble du cycle de vie du DM.

Les quatre propriétés retenues sont : ***confidentialité, intégrité, disponibilité et authenticité.*** D'autres propriétés peuvent être considérées ; la fraîcheur, la non-répudiation. Nous gardons uniquement les quatre premières qui sont les plus importantes. La méthode nous mène à définir des niveaux d'exigences pour les propriétés de sécurité. Les niveaux d'exigences sont décrits dans la table 18, variant de 1 à 4, avec les codes couleurs suivants : **blanc jaune, orange rouge**.

Nous listons ensuite les biens essentiels du dispositif, pour lesquels une compromission impacte le fonctionnement du dispositif et les acteurs associés. Cela implique de considérer les biens à protéger sur l'ensemble du cycle de vie, pour tous les acteurs. Nous nous appuyons sur les descriptifs du DM réalisés dans la section précédente. Outre les biens liés au traitement médical, nous considérons aussi les mesures de sûreté et de sécurité incorporées dans le DM. En termes de sûreté nous retrouvons les fonctions de surveillance décrites en section 2.2.5 : nous synthétisons cela par un bien essentiel appelé « fonctions de surveillance » incluant les fonctionnalités d'avertissement (sonore ou par message) d'une défaillance ou d'une erreur. En outre nous supposons l'existence des fonctions de sécurité de base : gestion des droits d'accès par couple [identifiant / mot de passe] que nous appelons « données d'authentification », chiffrement des communications avec utilisation des clefs cryptographiques.

Tous les biens essentiels requièrent par défaut une exigence maximale pour l'intégrité, la disponibilité et l'authenticité ; respectivement – intégrité complète – disponibilité permanent – authenticité assurée. Seule la confidentialité varie selon les restrictions d'accès exigés ; la table 19 présente le niveau de confidentialité supposé pour tel ou tel biens essentiels. Nous constatons déjà des besoins : les acteurs n'ont pas les même droits d'accès aux éléments du système. Il apparaît nécessaire de disposer de mécanismes d'authentification pour les acteurs et ce dès le début du cycle de vie du DM.

Tableau 18: Echelle des exigences pour les propriétés de sécurité

Propriétés de sécurité \ Exigence	1	2	3	4
Confidentialité	Publique	Limité ▪ 4 acteurs ou plus	Restreinte ▪ 2 ou 3 acteurs	Hautement restreinte ▪ 1 seul acteur
Intégrité	Aucune contrainte	Partielle ▪ Altération forte ▪ Longue durée	Maitrisée ▪ Altération faible ▪ Courte durée	Complète et permanente
Disponibilité	Aucune contrainte	Partielle	Maitrisée	Permanente
Authenticité	Aucune contrainte	Moyenne confiance	Forte confiance	Confiance parfaite

Tableau 19: Exigence de confidentialité pour les biens essentiels du DM

Biens essentiels	Exigence sur la confidentialité et acteurs ayant droit d'accès
Circuit matériel et firmware des microcontrôleurs et microprocesseurs du DM	Hautement restreinte : concepteurs des circuits
Modules logiciels des DMs	Restreinte : OEM, opérateurs techniques, auditeurs…
Données de mesures du DO, données d'injections du DI	Restreinte : patients, docteurs, dispositif de contrôle, opérateurs médicaux

Historique médical du DO et du DI	Restreinte : patients, docteurs, dispositif de contrôle, opérateurs médicaux…
Données de paramétrage du DC	Restreinte : docteurs, opérateurs du centre d'initiation
Données de santé privées	Restreinte : patient, docteurs…
Données pour suivi technique OEM	Hautement restreinte : OEM, auditeur
Mise à jour logicielle	Restreinte : OEM, auditeur, opérateur technique
Fonctions de surveillance	Partagée : Patient, docteurs, dispositif de contrôle, OEM, opérateurs médicaux, opérateurs techniques…
Eléments de sécurité : mot de passe, clés de chiffrement, clés d'authentification	Hautement restreinte : acteurs ou entité (circuit, DM, données…) associés à l'élément de sécurité

10.2.3 Module 2 – événements redoutés

Nous décrivons dans ce module les événements redoutés en cas de perte de telle ou telle propriété pour les biens essentiels. Nous évaluons l'impact sur plusieurs axes : santé du patient et conséquences pour le fabricant. Cette échelle est subjective et dépends du contexte précis dans lequel s'inscrit l'analyse : cadre réglementaire, objectifs et besoins du fabricant, conscience des acteurs vis-à-vis de la sécurité. Le *Medical Device Privacy Consortium* [32] a réalisé un rapport sur l'étude de sécurité des DMs. Il est fourni dans ses annexes un exemple précis et détaillé d'une échelle d'impact, présentée une fois par niveau de gravité, une fois par propriété de sécurité. La table 20 s'inspire de cette étude et résume les différents niveaux d'impact. Outre les conséquences sur les patients, une appréciation est également fournie pour celles qui concernent le fabricant (en terme de sanction judiciaire ou de perte économique). Nous classons les événements redoutés pour le patient selon le danger pour son état de santé.

Tableau 20: Echelle du niveau d'impact des événement redoutés

Impact de l'événement	1 : faible	2 : sérieux	3 : critique	4 : catastrophique
Patient	Faible impact sur la santé du patient, presque négligeable Vol de données privées faiblement exploitable	Dégradation de la santé du patient mais guérison possible Vol de données privées partiel (une partie seulement des données médicales, mot de passe)	Mise en danger du patient Vol de données privées important (historique complet, mot de passe et clef de chiffrement)	Mort du patient : cela est probable en cas de surdosage élevé du médicament
Fabricant OEM	Faible coût d'intervention Contraintes légales et commerciales faiblement impactées	Perte de 1 à 5% du chiffre d'affaire Contraintes légales et commerciales renforcées	Perte de 5 à 20% du chiffre d'affaire Contraintes légales et commerciales fortement renforcées. Impact sur plusieurs années.	Fermeture de l'entreprise Poursuite judiciaire

Par la suite nous relevons le niveau d'impact dans le cas de la compromission d'un bien ; les tables suivantes résument ces craintes. Nous présentons les biens ciblés en quatre catégories, une pour chaque sous-dispositif du système (pompe, capteur et dispositif de contrôle), et une dernière pour les biens spécifiques aux mesures de sécurité et sûreté. Nous fournissons une brève justification de notre appréciation. La table 21 liste les événements redoutés pour le dispositif d'observation (le capteur). La plus grande crainte est la modification non détectée du matériel ou du logiciel de mesure du taux de glucose. Cela correspond à la perte d'intégrité ou d'authenticité, et a un impact grave **(niveau 3).** Cela fausse l'observation de l'état du patient ; le dispositif de contrôle calculera un dosage incorrect. Un autre événement craint est la perte de disponibilité du matériel ou du logiciel, ce qui interrompt l'observation. Toutefois cela devrait être détecté par les fonctions de surveillance ; d'où un impact moindre que pour

l'intégrité. Pour terminer une malversation, ou la perte de confidentialité, de l'historique de mesure est embarrassant mais cela n'impacte pas gravement l'état du patient.

- ***Tableau 21: Evènement redoutés pour le dispositif d'observation***

Biens essentiels \ Propriétés	Confidentialité	Intégrité	Disponibilité	Authenticité
Microcontrôleur	0	3	2	3
Firmware	0	3	2	3
Module logiciel	0	3	2	3
Mesure du capteur	1	3	2	3
Historique des mesures	2	1	1	1

La table 22 liste les craintes pour la pompe, similaires à celles du capteur. La plus redoutée est la perte d'intégrité ou d'authenticité du matériel, du logiciel ou des données d'injection. Cela peut entrainer un surdosage d'insuline et la mort du patient **(niveau 4)**. De même l'autre crainte est la perte de disponibilité du matériel ou du logiciel, ce qui interrompt injection. Cela devrait être détecté par les fonctions de surveillance ; d'où un impact moindre. Pour terminer une malversation ou la perte de confidentialité de l'historique de mesure doit être évitée mais n'impacte pas gravement l'état du patient.

Tableau 22: Evènement redoutés pour le dispositif d'injection

Biens essentiels \ Propriétés	Confidentialité	Intégrité	Disponibilité	Authenticité
Microcontrôleur	0	4	2	4
Firmware	0	4	2	4
Module logiciel	0	4	2	4
Ordre d'injection	1	4	2	4
Historique des injections	2	1	1	1

La table 23 présente les impacts pour les éléments du dispositif de contrôle. La plus grande crainte est une modification, une perte de contrôle des éléments matériels et logiciels. Cela inclut le circuit, les logiciels embarqués et les données de mise à jour. Un surdosage mortel est envisageable **(niveau 4).** Parmi les autres craintes nous listons le vol des données de santé privées **(niveau 3)**, et la modification des données de paramétrage. Dans ce cas le dosage de l'injection ne correspond plus au profil du patient ce qui compromet sa santé **(niveau 3)**. D'autres événements sont redoutés mais avec un impact plus faible. Les données techniques peuvent être exploitées pour récupérer des informations sur l'usage de l'objet. La perte des données de santé ou des données de suivi techniques, la non-disponibilité des biens, peut entrainer une mauvaise gestion du traitement médical et du suivi technique du DM. Cela n'a aucune conséquence rapide sur le traitement médical, et la perte sera probablement détectée par les opérateurs.

Tableau 23: Evènements redoutés pour le dispositif de contrôle

Biens essentiels \ Propriétés	Confidentialité	Intégrité	Disponibilité	Authenticité
Système sur puce	0	4	2	4
Firmware	0	4	2	4
Système d'exploitation	0	4	2	4
Module logiciel	0	4	2	4
Données de paramétrages	2	3	2	3
Données de santé privée	3	2	1	2

Données techniques pour le suivi par l'OEM	1	2	1	2
Données logicielles pour les mises à jour	0	4	2	4

Pour terminer, la table 24 donne les craintes pour la dernière catégorie de biens essentiels, ceux relatifs aux mesures de sécurité ou sûreté.

- Le plus grand danger est le vol des données d'authentification. Un adversaire pourrait alors usurper un acteur ou un dispositif ; et potentiellement forcé une injection mortelle **(niveau 4).**
- Le vol des clés de chiffrements permet de voler les données de santé privées **(niveau 3).**
- Les fonctions de surveillances deviennent problématiques en cas de non authenticité. Elles pourraient ne pas correspondre aux spécifications requises **(niveau 3).**
- La perte d'intégrité et de disponibilité des fonctions de surveillance est grave. Le DM pourrait ne plus détecter des erreurs de fonctionnement un mésusage médical **(niveau 3).**

Tableau 24: Evènements redoutés pour les biens essentiels relatifs à la sécurité

Biens essentiels \ Propriétés	Confidentialité	Intégrité	Disponibilité	Authenticité
Fonctions de surveillance	1	3	3	3
Données d'authentification des patients	4	2	2	4
Données d'authentifications des opérateurs médicaux	4	2	2	4
Données d'authentification des administrateurs	4	2	2	4
Données d'authentifications des opérateurs OEM à distance	4	2	2	4
Données d'authentification du DO	3	2	2	3
Données d'authentification du DI	3	2	2	3
Données d'authentification du DC	4	2	2	4
Clés de chiffrement pour les données de santé	3	1	1	3
Clés de chiffrement pour les données techniques	2	1	1	2
Clés de sécurité des mises à jour	4	2	2	4

10.2.4 Module 3 – Scénarios de menaces

La recherche de scénarios de menaces est complexe : la surface d'attaque est importante et les scénarios doivent être cotés en termes de vraisemblance. Nous définissons quatre niveaux de vraisemblance : **1 – faible 2 – moyenne 3 – forte 4 – certaine** Plusieurs catégories d'attaques sont identifiées dans le guide EBIOS [24] ; les plus pertinentes pour l'analyse de risques du DM sont notamment les attaques matérielles, les menaces contre les communications (interception ou malversation des échanges entre le DM et des tiers parties) et les exploitations de failles logicielles. Ces menaces sont nombreuses et diverses, notre synthèse résume brièvement les scénarios les plus critiques.

Afin d'apprécier plus finement la nature et la vraisemblance de la menace nous classons les scénarios en fonction des modèles d'adversaires listés dans la section 1.2.2 :

- Adversaire à distance exploitant des failles logicielles et matérielles :

  - *Adversaire sans privilèges* qui attaque le système via l'application embarquée sur le SoC, et possède des droits utilisateurs restreints.
  - *Adversaire avec privilèges* qui a des accès au système d'exploitation ; et peut interagir avec les communications et opérations internes du système.
  - *Adversaire avec privilèges et accès aux canaux auxiliaires* qui, outre les accès classiques, dispose d'informations supplémentaire tels que la consommation d'énergie ou l'horloge.
- Adversaire avec un accès physique au dispositif :
  - *Adversaire limité (dit naïf)* qui utilise des équipements basiques (et peu cher) pour interagir avec le SoC via des accès usuels, type interface de débogage ou port JTAG.
  - *Adversaire avec capacité avancée :* qui dispose des équipements de rétro-ingénierie et des compétences suffisantes pour extraire les micrologiciels ou les designs matériels du SoC.
  - *Adversaire hautement intrusif* qui compromet le SoC par l'intégration de fonctionnalités ou de composants malveillants (*Trojan*). Cela suppose des accès à des composants matériels pendant les premières phases de production du SoC.

Les tables 25, 26 et 27 listent les scénarios d'attaques matérielles, du modèle d'adversaire le plus « naïf » au plus intrusif. Les tables incluent le niveau de vraisemblance, les biens ciblés et les propriétés de sécurité qui sont perdues en cas de réussite de l'attaque.

Scénarios d'attaques matérielles dites « naïves » :

L'attaque naïve la plus crainte est *l'intrusion par les interfaces de programmation et débogage :* Des adversaires extérieures peuvent exploiter des accès spécifiques (JTAG par exemple) pour atteindre des *firmwares* logiciels ou des données privées stockés dans les dispositifs ([5], [6]). Cela est possible au cours des phases pour lesquelles les ports sont accessibles, et où les interactions et les accès ne sont pas sécurisés : assemblages, intégration logicielle, distribution, maintenance, fin de vie… Cela remet en cause l'intégrité et la confidentialité de biens critiques : les fonctions sensibles (calcul et commande de l'injection) ou bien la surveillance du système. La vraisemblance est élevée : plusieurs acteurs utilisent ces interfaces ; celles-ci sont aussi exposées à l'extérieur. Des menaces similaires pèsent sur d'autres interfaces utilisateurs (accès périphériques, carté réseau) [109]. Ces scénarios sont moins répandus que les attaques via le JTAG ; moins intéressants pour l'adversaire car ces interfaces n'offrent pas le même niveau d'accès au système. La table 25 regroupe les deux scénarios :

Tableau 25: Scénarios d'attaques matérielles dites « naïves »

Scénarios de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Intrusion par l'interface de programmation et débogage [5], [6]	Modules logiciels des dispositifs Données de santé privées Données d'authentification Clés de sécurité	Confidentialité, intégrité	4
Attaques par des interfaces utilisateurs (USB, GPIO, carte réseau) [109]	Données de santé privées Données d'authentification Clés de sécurité	Confidentialité, intégrité	3

Scénarios d'attaques matérielles avec capacités avancées

La table 26 liste plusieurs catégories d'attaques matérielles. Pour certaines l'adversaire dispose des équipements et compétences nécessaires pour une intrusion et une analyse plus approfondie. Cela concerne notamment les attaques par canaux cachés [110] ou les injections de faute. Des acteurs externes ou internes exploitant les canaux auxiliaires (température, émission électromagnétique…) peuvent déduire des clés de chiffrement privé. Cela peut se passer au cours de la phase d'exploitation ou des étapes de maintenance et de fin de vie. Ces clés peuvent être réutilisées pour déchiffrer des données

privées. Certaines méthodes d'injection de fautes, celles semi-invasives et à faible coût, sont à craindre également [111]. Parmi elle, les impulsions électromagnétiques ou les *glitch* (décalage forcé) d'horloge sont des menaces vraisemblables. La mise en œuvre de ces attaques (injection de faute et exploitation de canaux auxiliaires) supposent toutefois, outre un accès aux circuits, un certain niveau de compétence et d'équipement. La vraisemblance des scénarios est plus faible mais ceux-ci doivent être pris en compte.

Les contrefaçons de circuits sont à craindre également ; au cours de la phase de fabrication ou d'assemblage des fournisseurs ou sous-traitants avec des motivations financières peuvent intégrer des composants contrefaits, ayant des performances moindres. Cela réduit l'intégrité et la disponibilité des circuits. Un autre scénario est l'extraction des IPs du circuit et leur duplication : ainsi des contrefaçons du dispositif médical peuvent circuler sur des marchés non surveillés. Les contrefaçons font l'objet d'un état de l'art dans [11]. Ces scénarios ont à priori, comme attaquant, des acteurs propres au cycle de vie, des tierces parties qui ont accès au circuit lors d'une opération. Réaliser une contrefaçon peut être couteux en temps et ressources mais les gains sont importants ; les motivations financières rendent ce scénario vraisemblable. Aujourd'hui les contrefaçons sont répandues dans le milieu de l'électronique.

Tableau 26 : Scénarios d'attaques avec rétro-ingénierie et accès physique semi-invasif

Scénarios de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Contrefaçon [11]	Circuit des dispositifs	Authenticité	3
Attaque par canaux cachés [110]	Clés de sécurité	Confidentialité	2
Injection de faute semi-invasive, type *glitch* ou *impulsion EM* [111]	Clés de sécurité	Confidentialité, intégrité	2

Scénarios d'attaques matérielles hautement intrusives

La table 27 liste les scénarios mis en œuvre par des adversaires hautement intrusifs. En premier lieu *l'insertion de cheval de Troie dans les circuits matériels ou dans les micrologiciels*: Des tiers parties insèrent des fonctionnalités malveillantes dans les circuits en amont des phases d'assemblages. Le circuit ciblé perd en confidentialité, intégrité et disponibilité. Les chevaux de Troie font l'objet d'un état de l'art dans [7], plusieurs phases du cycle de vie sont susceptibles d'être compromises. Cela suppose par contre un adversaire avec des privilèges élevés : accès direct au circuit et haute compétence pour modifier le circuit. Deuxièmement il y'a le risque des injections de fautes invasives avec laser ou rayon X. Celles-ci, plus couteuses, sont peu vraisemblables. D'autres méthodes existent, telles que la provocation de tension sur le substrat d'un transistor (*glitch sur le substrat, appelé aussi forward by body biasing*). Cette approche invasive est délicate à mettre en œuvre. Nous distinguons ainsi ces méthodes d'injection de faute de celles listées précédemment ; notamment en terme de vraisemblance.

Tableau 27: Scénarios d'attaques matérielles avec adversaires hautement intrusifs

Scénarios de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Cheval de Troie [7]	Circuits des dispositifs	Intégrité, disponibilité	1
Injection de faute invasive [111], type *rayon* ou *laser X*	Clés de sécurité	Confidentialité, intégrité	1

Par la suite les tables 28, 29 et 30 énumèrent les scénarios avec des adversaires « à distance ». Il s'agit essentiellement d'attaques exploitant des vulnérabilités logicielles, des failles dans les protocoles ou une mauvaise gestion des droits d'accès.

Scénarios d'attaques sur les communications par un adversaire sans privilèges

Parmi les menaces mises en œuvre par des adversaires sans privilèges nous trouvons l'interception ou la malversation des communications inter dispositifs. Cela est notamment présenté dans l'article [8] qui décrit l'interception, l'analyse et la modification des communications d'une pompe médicale connectée. L'événement le plus redouté est envisageable : la modification de la commande d'injection. Ces attaques sont vraisemblables si aucun protocole de sécurité n'est mis en place pour chiffrer et authentifier les communications. Auquel cas l'attaque est envisageable sans privilèges et avec des ressources limitées. La table 28 présente les divers scénarios possibles :

- *Rejeu de commande* : Un adversaire intercepte et réémet des échanges à destination du DM, forçant l'exécution de commandes non souhaitées et non authentiques.
- *Interception passive :* Un adversaire écoute les messages échanges et brise leur confidentialité.
- *Man in The Middle* : Interception puis émission de messages falsifiés, cela produit des messages non authentiques ou non intègres.
- *Déni de services :* Emission massive de messages pour mettre en défaut de fonctionnement les transmetteurs des dispositifs, voir provoquer un épuisement de la batterie.

Tableau 28: Scénarios de menaces contre les communications par un adversaire sans privilèges

Scénarios de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Rejeu de commande [112] [112]	Ordre d'injection	Authenticité	4
Interception passive des échanges DO-DC et DI-DC [112]	Mesure du capteur, ordre d'injection, historique médical	Confidentialité	3
« Man in the Middle » [112]	Mesure du capteur, ordre d'injection, historique médical	Authenticité	3
Déni de service [113]	Module de communication	Intégrité, disponibilité	3

Scénarios d'attaques à distance par un adversaire sans privilèges

Les autres menaces avec adversaire sans privilèges concernent les brèches logicielles dans le système, ou la faiblesse des protocoles de sécurité contre un « brute-force ». Si les clés de sécurité et les mots de passe ne dérivent pas d'une entropie (ou source d'aléa) de qualité suffisante, ceux-ci sont sensibles au brute-force ou à une cryptanalyse. Au niveau logiciel diverses attaques existent pour contourner la sécurité du système et élever ses privilèges ; l'adversaire gagne ainsi des accès non autorisés. En [114] les auteurs présentent les grandes vulnérabilités connues : le dépassement non contrôlé de tampons mémoires, les pointeurs invalides ou le détournement de flot de contrôle. Ces failles sont source de risque, elles peuvent être atténuées par une application stricte des normes de sécurité logicielles et par des processus de vérification. Le scénario est vraisemblable, il faut toutefois un adversaire ayant les connaissances nécessaires tant sur la mise en œuvre et sur le fonctionnement du système ciblé.

Tableau 29: Scénarios de menaces avec adversaires sans privilèges

Scénario de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Brute force	Mot de passe	Confidentialité	3
	Clés de sécurité	Confidentialité	1
Exploitation de vulnérabilités logicielles, dépassement mémoire, pointeurs invalides…	Module logiciel et données du dispositif de contrôle	Confidentialité, intégrité	2

Scénarios d'attaques à distance par un adversaire avec privilèges

Pour terminer, les dispositifs sont susceptibles de subir des attaques d'adversaires ayant des privilèges déjà établis. Un acteur ou un dispositif extérieur peut abuser de ses droits d'accès pour atteindre et interagir avec des biens pour lesquels il n'a pas autorisation d'accès. Cela peut se produire au cours de phases d'utilisation ou de déploiement où un manque de sécurité dans la gestion des droits d'accès permet des interactions non autorisées. Ce scénario est vraisemblable, au cours du cycle de vie plusieurs acteurs disposent d'accès au système ou à ces données.

Tableau 30: Scénarios de menaces avec adversaires disposant de privilèges

Scénarios de menace	Biens essentiels ciblés	Perte de propriétés :	Vraisemblance
Abus des droits d'accès pour atteindre des biens essentiels	Données médicales, données de paramétrage, modules logiciels	Confidentialité ; intégrité	3
	Firmware	Confidentialité ; intégrité	

10.2.5 Module 4 : Evaluation des risques significatifs

Le « risque » est un événement redouté (perte de propriété de sécurité d'un bien du dispositif) qui se réalise suite à un scénario de menace. Plus le scénario est vraisemblable et l'événement impactant, plus le risque est pertinent. Cette pertinence s'obtient ainsi par croisement des niveaux d'impact et de vraisemblance. Nous synthétisons dans le tableau 31 la pertinence des risques identifiés, cinq niveaux sont établis : **0 – négligeable, 1 – faible, 2 – moyen, 3 – fort, 4 – critique, 5 – hautement critique**

Tableau 31: Evaluation des risques significatifs

Gravité \ Vraisemblance	1 : Faible	2 : Moyenne	3 : Forte	4 - Certaine
1 : Faible			Interception de données de mesure ou injection par écoute passive.	
2 : Sérieux			Interception des historiques médicaux des DO et DI.	
3 : Critique	Perte d'intégrité et de disponibilité des circuits matériels du capteur par insertion de cheval de Troie. Dévoilement des clés de chiffrement par brute force.	Perte d'intégrité des clés de sécurité par injection de faute semi-invasive	Perte d'intégrité et d'authenticité du capteur par contrefaçon. Perte d'authenticité de la mesure du capteur par injection de faux message. Non-disponibilité du capteur ou de la pompe par déni de service. Dévoilement des données de santé par abus des droits d'accès. Perte d'intégrité des données de paramétrage par abus des droits d'accès.	Dévoilement des données de santé par intrusion via interface de débogage. Perte d'intégrité des données de paramétrage par intrusion via interface de débogage

4 : Catastrophique	Perte d'intégrité et de disponibilité des circuits de la pompe et du dispositif de contrôle par insertion de cheval de Troie. Dévoilement ou perte d'intégrité des clés de sécurité par injection de faute invasive	Perte de confidentialité des clefs de sécurité par attaques sur les canaux cachés ou par injection de faute semi-invasive Perte d'intégrité des logiciels, confidentialité des données privée ou des clés par une exploitation de vulnérabilité logicielle.	Perte d'intégrité et d'authenticité des circuits du DM par contrefaçon. Perte d'authenticité des commandes d'insuline par injection de faux message. Dévoilement des mots de passe par brute force. Dévoilement des mots de passes et de perte d'intégrité des logiciels et firmwares par non-respect des droits d'accès.	Perte d'intégrité des modules logiciels ; risque de dévoilement des clefs de sécurité par intrusion via interface de débogage Perte de l'authenticité de l'ordre d'injection de la pompe par rejeu.

La synthèse de l'analyse révèle des risques critiques qui doivent être traités pour sécuriser les biens du dispositif médical. Les failles sont de natures diverses : non sécurisation de l'accès physique (risques liés à des intrusions via les interfaces de débogage) qui est exploitée pour accéder à des biens, défauts dans l'authentification des composants électroniques (contrefaçons), manque de sécurisation des communications, mauvaise gestion des droits d'accès.

Les attaques matérielles les plus craintes sont celles mises en œuvre par des adversaires limités ou moyennement équipés ; les attaques hautement intrusives réalisées par des adversaires ayant de fortes ressources sont moins vraisemblables. Les attaques à distance qui doivent être considérées sont celles concernant la compromission des communications non-sécurisées, ainsi que les attaques exploitant des faiblesses dans la gestion des droits d'accès (mot de passe ou clef d'authentification mal-sécurisé, niveau d'autorisation mal défini).

Au vue de ces risques identifiés nous pouvons établir des exigences de sécurité, celles-ci peuvent être complémentaires, mais peuvent également générer de nouvelles problématiques :

- Etablir des protocoles de sécurité pour authentifier les acteurs et le dispositif au cours des communications, assurer l'intégrité des messages et chiffrer les données.
    - Cela implique l'utilisation de clefs de sécurité (clef cryptographique pour le chiffrement, signature pour authentification).
- Intégrer une solution de sécurité qui assure l'authenticité des composants du dispositif et des acteurs face aux scénarios d'attaques matérielles (contrefaçons et intrusion physique).
    - Idéalement, cette solution est embarquée dans le circuit du dispositif et permet de prouver l'authenticité du circuit et des acteurs au cours du cycle de vie.
    - Cela suppose, à priori, une intégration de ce mécanisme dès les premières phases.
- Déployer une politique de sécurité qui distribue et assure les droits d'accès au cours du cycle de vie sans compromettre le dispositif.
    - Cela implique des protocoles d'authentifications sures, ceux-ci pourraient s'appuyer sur les mécanismes qui assure l'authenticité.
    - Cela impose aussi une flexibilité, répudier ou ouvrir des accès au cours du cycle de vie.

Ces exigences imposent la mise en œuvre d'une solution de génération, stockage et gestion de clefs de sécurité (chiffrement et / ou authentification). Cela nécessite l'exploitation d'une source d'aléa sûre, ou d'une fonction de génération, qui respecte les propriétés de sécurité (notamment en termes d'aléa, de niveau d'entropie et de non-prédictibilité) ; et qui par ailleurs résiste aux attaques matérielles.