Étude des modes de perturbation et susceptibilité des circuits numériques aux collisions de particules et aux attaques laser

Damien Leroy

Laboratoire Interfaces Capteurs et Microélectronique

UNIVERSITE DE METZ

École Doctorale IAEM -Lorraine
Département de Formation Doctorale Électronique - Électrotechnique

THÈSE DE DOCTORAT

Discipline: ÉLECTRONIQUE

ÉTUDE DES MODES DE PERTURBATION ET DE SUSCEPTIBILITÉ DES CIRCUITS NUMÉRIQUES AUX COLLISIONS DE PARTICULES ET AUX ATTAQUES LASER

Par

Damien LEROY

Soutenance réalisée le 1er décembre 2006 devant le jury composé de:

Rapporteurs

Patrick GIRARD	Directeur de Recherche au CNRS, LIRM Montpellier
Régis LEVEUGLE	Professeur à l'Institut National Polytechnique de Grenoble

Directeur de thèse

Abbas DANDACHE	Professeur à l'Université Paul Verlaine - Metz

Examinateurs

Fabrice MONTEIRO	Maître de Conférence HDR, à l'Université Paul Verlaine - Metz
Michael NICOLAIDIS	Directeur de Recherche au CNRS, TIMA, INPG

LICM – 07 Rue Marconi, Technopôle, 57070 Metz, France

A mes parents,

REMERCIEMENTS :

Je tiens à remercier tout spécialement le professeur Abbas Dandache qui a été un soutient très important tant au point de vue psychologique que scientifique et administratif. Il n'est pas facile de piloter un thésard à distance comme ce fut le cas mais il a encadré cette thèse d'une main de maître.

Je remercie aussi mes encadrants, Fabrice Monteiro et Stanislaw Piestrak pour leurs conseils et les semaines passées à revoir mes copies.

Les rapporteurs Regis Leveugle et Patrick Girard qui, par leur lecture critique et leurs conseils avisés m'ont permis de transformer un essai en travail scientifique digne de ce nom.

Michael Nicolaidis sans qui les voyages en conférence seraient malheureusement beaucoup plus formels et qui m'a permis de débuter cette thèse chez iRoC.

Lorena Anghel pour m'avoir donné goût au test en ligne (et aux études par la même occasion), Eric Dupont pour m'avoir présenté les « soft errors », et le directeur de l'ENSERG de l'époque M. Baribaud pour m'avoir tiré de l'oisiveté de la cafétéria et m'avoir envoyé assister à la conférence donnée par M. Dupont.

Je tiens aussi à remercier toutes les personnes d'iRoC que j'ai connues depuis mars 2002, et qui ont travaillé avec moi, m'ont encouragé, voire facilité mes démarches administratives. Je pense particulièrement à Moez Cherif, Stephane Rossignol, Renaud Perez et Jocelyne Baudoin, merci beaucoup pour tout.

Mes amis thésards grenoblois tout comme moi, qu'ils soient chez iRoC ou au CEA pour les bons moments partagés, et pour cette compassion dans les moments difficiles.

A mon amie Christiana Molfeta, qu'elle sache que tout ceci aurait été beaucoup plus dur sans elle, et que son soutien dans les dernières phases de rédaction m'a aidé à clore ce chapitre de ma vie.

A ma mère, j'espère que la fin de cette thèse sera un autre rayon de soleil dans une période difficile. Je te soutiens de tout mon coeur.

Table des matières

Index des illustrations

Index des tables

Introduction

Depuis qu'il a été prouvé dans les années 70 qu'un rayonnement intense (particules du vent solaire) pouvait affecter des circuits présents en orbite terrestre [PIC78], les concepteurs de circuits intégrés ont réalisé que l'estimation de la fiabilité des transistors devait prendre en compte ce phénomène. Il est de plus apparu que cette sensibilité au rayonnement progressait avec l'évolution des technologies, et si dans les années 80 ce problème restait confiné au domaine des circuits militaires et spatiaux, la perturbation des circuits intégrés est aujourd'hui un sujet qui préoccupe le monde de la micro-électronique dans son ensemble. En effet, ces dernières années, ce problème de fiabilité est devenu tellement important que les fournisseurs de circuits intégrés se doivent d'intégrer des parades dans leur flot de conception de circuits pour satisfaire les exigences de leurs clients. L'évolution des technologies modifiant les paramètres des transistors (réduction de la taille et de la charge), la sensibilité de ces derniers aux perturbations infimes provoquées par l'impact d'une particule énergétique augmente dans une telle mesure que ce problème ne concerne plus seulement les circuits utilisés en orbite terrestre ou en aéronautique, mais aussi ceux utilisés dans les applications quotidiennes au sol.

Des études extensives ont été menées pour comprendre ces phénomènes et pour y remédier. Les termes de SET (événement singulier transitoire ou Single Event Transient) et SEU (événement singulier d'inversion ou Single Event Upset) sont apparus pour désigner respectivement les perturbations apparaissant dans la logique combinatoire et dans les élément mémorisants. Ces perturbations ont la propriété d'être des altérations ponctuelles (pour les SET) ou durables (pour les SEU) de l'état logique d'une structure semi-conductrice. Des chercheurs ont étudié ce phénomène sur des structures élémentaires pour mieux l'appréhender, et ils se sont attachés à reproduire les effets d'impacts de particules en utilisant des sources de rayonnement énergétique comme les accélérateurs de particules, les lasers ou bien des sources radioactives. Leur travail a contribué à la compréhension des effets de ces perturbations et ont permis la mise en place de protocoles d'injection de perturbations pour étudier leur influence sur le comportement de circuits complexes. Ces protocoles ont permis, suivant la précision de la source de perturbation utilisée, d'étudier de manière plus ou moins reproductible le comportement de circuits intégrés soumis à tout type de perturbation. Des documents grand public ont ainsi mis à disposition des

méthodologies, relativement simples à mettre en place et à contrôler, d'injection de fautes dans un circuit intégré complexe. Ces méthodologies étaient cependant basées sur des sources de perturbation difficiles à obtenir à l'époque.

Avec l'évolution des technologies de semiconducteur, les moyens à mettre en oeuvre pour obtenir des perturbations significatives ont cependant considérablement diminué au point que des chercheurs britanniques ont prouvé qu'il était possible de perturber un circuit mémorisant à l'aide d'un simple flash d'appareil photo. La conjonction de méthodologies d'injection de fautes dans les circuits et de moyens de perturbation faciles à mettre en oeuvre a donc été un signal pour les concepteurs de circuits électroniques sécuritaires qui ont investit de plus en plus d'argent dans les contre mesures embarquées. Ces concepteurs, poussés par le système bancaire qui voyait dans le traitement électronique de l'argent un moyen de s'affranchir d'un argent liquide ayant toujours attiré les convoitises, avaient en parallèle proposé des solutions de paiement par circuit intégré (les cartes bancaires à puce). Ce nouveau type de cible a donc créé une nouvelle génération de pirates électroniques qui ont détourné les moyens à leur disposition pour perturber le fonctionnement des circuits intégrés des cartes bancaires et ainsi frauder le système bancaire. Ils ont mis en place des techniques d'attaque dédiées à la récupération de codes secrets et autres clés de cryptage. Ceci a conduit à réorienter la recherche de techniques de protection des circuits intégrés vers le domaine public alors que celles-ci restaient jusqu'ici l'apanage des militaires et du domaine spatial.

Aujourd'hui cette problématique dépasse le système bancaire car nous utilisons de plus en plus de circuits intégrés pour stocker et traiter des informations confidentielles, que ce soient des codes d'accès, des clefs de cryptage sécurisant des informations confidentielles ou bientôt des papiers d'identité. Ces informations sont une cible privilégiée pour des personnes malintentionnées, et garantir la confidentialité de ces données est un prérequis à l'utilisation de ces supports. L'industrie de la carte à puce est bien placée dans ce domaine de par son rôle historique de fournisseur de circuits intégrés à vocation sécuritaire. C'est pourquoi elle étudie les modes d'attaque utilisés contre ses circuits pour proposer des ripostes et ainsi garantir à ses clients un maximum de protection de leurs moyens de paiement.

Des attaques de plus en plus complexes ont vu le jour pour contourner les protections mises en place, elles mêmes en évolution constante. À la base, simples modifications des pistes du circuit

intégré, les attaques utilisent maintenant tout un arsenal de méthodes statistiques et mathématiques complexes qui explorent la cohérence d'un flot de données pour en extraire les informations utiles. Les attaques utilisent même les fruits de recherches portant sur les erreurs transitoires dans les circuits intégrés. L'utilisation de sources de perturbation comme les flash lumineux, voire les laser, permettent d'injecter des fautes de manière très précise dans des circuits intégrés complexes et construits dans les technologies les plus modernes.

Les domaines de la conception sécuritaire et de la tolérance aux fautes se sont rencontrés avec l'apparition d'un type d'attaque nommé attaque par injection de faute. Celle-ci consiste à perturber le fonctionnement normal d'un circuit pour le faire entrer dans un état erroné qui facilite la récupération des informations confidentielles contenues dans le circuit. Les erreurs produites ne doivent cependant pas détruire le circuit sous peine de rendre l'attaque inutile, et les diverses approches utilisent des sources d'erreur non destructrices comme la lumière.

Le principal problème de la lutte permanente des concepteurs de circuits sécuritaires contre les attaques est de diminuer les coûts de la mise en oeuvre d'une protection tout en obtenant les meilleurs résultats. En effet un concepteur doit fournir un produit peu onéreux tout en assurant un maximum de fiabilité pour satisfaire aux exigences d'un marché de masse hautement concurrentiel. Dans ces conditions, proposer des parades efficaces s'intégrant facilement dans un flot de conception standard est le cheval de bataille des concepteurs, et à ce niveau s'impose encore la similitude avec la conception de circuits résistant aux perturbations transitoires.

Les techniques d'injection de fautes les plus avancées utilisent une source lumineuse très focalisée pour provoquer des erreurs par effet photoélectrique. Cette source peut être un simple flash d'appareil photographique ou un rayon laser. Ce dernier ayant l'avantage d'avoir une grande souplesse d'utilisation et une grande précision, il est l'arme ultime des attaquants pour pénétrer les protections mises en place par les concepteurs. Il est donc indispensable de rassembler des informations sur ce nouveau mode d'attaque pour proposer des parades appropriées.

Dans les années 1980, des chercheurs ont mis en évidence la similitude entre l'impact d'une particule chargée et le tir d'un rayon laser sur un circuit intégré [BUC87]. En effet, dans les deux cas l'impact crée des paires électrons-trous dans le silicium dopé ce qui entraîne une

perturbation de l'état logique de la structure frappée. Ces similitudes nous permettent d'étudier les techniques en vigueur dans la protection des circuits face aux attaques de particules et de les rapporter au domaine des attaques laser.

C'est donc pour explorer les liens entre conception sécuritaire et tolérance aux fautes que ce travail a été entrepris. Cette thèse s'est réalisée dans le cadre d'une convention CIFRE entre la société iRoC Technologies de Grenoble et le laboratoire LICM de l'université Paul Verlaine de Metz. Le but est d'apporter une approche structurée et de construire des compétences académiques pour prendre en main le projet Duracell. Ce projet financé par le ministère de la recherche et de l'industrie a été mis en place avec l'objectif de rapprocher le domaine de la conception de circuits sécuritaires, représenté par Gemplus et Thalès, avec celui de la recherche sur des architectures tolérantes aux fautes (TIMA et iRoC Technologies) dans le but d'étudier les attaques laser sur des circuits à vocation sécuritaire.

Ce travail propose une approche duale du problème : en intégrant la problématique des perturbations transitoires provoquées par un rayonnement au domaine de la conception de circuits sécuritaires nous recherchons une approche faible coût permettant de quantifier l'impact d'une attaque dans un circuit intégré moderne, et nous étendons cette approche pour proposer un moyen peu onéreux de tester la sensibilité d'une technologie face au rayonnement. En association avec un concepteur de circuits sécuritaires, nous avons choisi de réaliser des prototypes de circuits basés sur une bibliothèque standard de cellules combinatoires et séquentielles conformément à la réalité du marché des cartes à puces. Le premier prototype est dédié à la mesure de la durée d'impulsion générées dans une bibliothèque standard de cellules combinatoire par un tir laser et le second est conçu pour quantifier la sensibilité d'une bibliothèque de cellules standard aux faisceaux de particules. Enfin nous réalisons une campagne de tirs laser sur le premier circuit, et nous analysons les résultats pour proposer des moyens de diminuer la sensibilité d'un circuit sécuritaire aux attaques par injection de faute.

L'environnement opératoire des circuits électroniques peut être très divers et les sources de rayonnement existantes sont très variées. Le chapitre 1 introduit les divers environnements radiatifs ainsi que les sources qui peuvent y être attachées. Chaque type de radiation interagit de manière spécifique avec les matériaux entrant dans la conception des circuits électroniques et le risque de fautes lié à cette interaction dépend à la fois des caractéristiques propres à la particule

et au matériau. Les erreurs logiques provoquées par une interaction peuvent générer plusieurs types d'effets, permanents ou transitoires, réversibles ou irréversibles. Nous passons ces effets en revue dans ce premier chapitre avant de nous focaliser sur les spécificités de la source laser que nous avons utilisons dans ce travail. Nous présentons ensuite les bases de l'interaction laser-silicium qui nous aident à comprendre le phénomène d'injection de faute. Nous expliquons enfin pourquoi le laser vert de 532 nm de longueur d'onde peut être utilisé pour provoquer des perturbations dans les circuits intégrés.

Dans le deuxième chapitre nous étudions les conséquences de la réduction du facteur d'échelle des technologies sur le comportement des circuits exposés à ces environnements radiatifs. Ensuite nous passons en revue des différentes méthodes de perturbation des circuits à la disposition d'éventuels attaquants, de la perturbation de l'horloge ou de l'alimentation à l'altération de l'état des points mémoires, structures logiques et séquentielles. Une exploration plus spécifique du domaine de l'attaque de circuits sécuritaires est proposée, en étudiant diverses attaques par injection de fautes documentées à ce jour. Cette exploration pose les bases de la conception de circuits sécuritaires et les différentes réponses aux attaques à la disposition des concepteurs. Nous finissons ce chapitre en présentant les différents moyens de protection utilisés dans l'industrie pour protéger les circuits contre les perturbations transitoires et nous présentons les outils développés par la société iRoC Technologies pour protéger ces circuits.

Le domaine de la conception de protections efficaces contre les perturbations se doit d'utiliser des méthodologies adaptées aux spécificités des attaques. C'est pourquoi nous nous proposons dans le chapitre 3 de mettre au point un circuit dédié à la mesure de la durée des impulsions générées par une source laser. Nous utilisons les spécificités de cette source pour mettre au point une architecture optimisant la surface et la précision des mesures. Nous proposons aussi une méthodologie de conception de circuit réduisant au maximum les coûts de conception tout en permettant une excellent maîtrise des paramètres physiques du circuit. Forts de cette méthodologie, nous utilisons ses avantages pour l'étendre à d'autres types de sources et pour mettre au point un circuit mesurant la sensibilité d'une technologie aux perturbations d'origine radiative en général, et plus spécifiquement adapté à la mesure des perturbations provoquées par l'impact de neutrons sur le circuit. Nous finissons ce chapitre en étudiant par simulation les seuils de sensibilité de ces structures de détection et proposons une étude de la charge critique des portes de la technologie utilisée.

Je consacre le quatrième chapitre aux expériences réalisées sur le circuit de mesure de durée des impulsions générées par laser. Je présente tout d'abord le banc de test et le mode opératoire utilisé, puis évalue les performances du circuit de mesure. Je décris les expériences portant sur l'étude de la propagation d'impulsions générées en interne pour mettre en évidence les différents types de comportement des portes de la technologie et leur influence sur la durée des impulsions qui les traversent, puis j'analyse résultats d'expérience de tirs laser sur les surfaces sensibles du circuit. La fin de ce chapitre est l'occasion de revenir sur les faiblesses des techniques de protection habituelles contre les fautes transitoires face aux attaques laser et de proposer des astuces de conception ainsi qu'une stratégie globale de protection à même de rendre les circuits sécuritaires plus résistants face à ces attaques.

Chapitre 1 : Étude des différentes sources de perturbation

1.1 Introduction

Les circuits intégrés sont sensibles à de multiples sources de perturbation, et l'évolution technologique les rend de plus en plus sensibles en diminuant leur immunité au bruit. L'étude de ces sources est indispensable car la compréhension de leurs effets est un pré requis à la conception de solutions efficaces pour les contrecarrer. Nous étudierons en particulier dans ce document les effets des particules ionisantes et du rayonnement laser, en partant des perturbations physiques pour monter jusqu'aux effets logiques d'un tir laser sur un circuit intégré.

Dans ce chapitre nous décrivons en détail la provenance et l'effet des différents phénomènes radiatifs pouvant perturber un circuit intégré. Dans un premier temps, nous étudions les sources possibles de ces phénomènes, puis nous intéressons à leurs modes d'action sur le silicium, et enfin nous décrivons les conséquences de ces interactions sur un circuit électronique.

1.2 Environnement radiatif

Une radiation est une énergie rayonnée sous forme d'ondes ou de particules. Ces ondes ou ces particules deviennent dangereuses pour l'électronique dès lors que l'énergie qu'elles apportent est suffisante pour perturber directement ou indirectement le fonctionnement des systèmes.

1.2.1 Sources de radiations naturelles

Les radiations naturelles proviennent principalement du soleil (vent solaire) et des étoiles en général. Ces sources cosmiques (quasars, noyaux galactiques, pulsars) produisent les *rayons cosmiques primaires* (pour les distinguer des *rayons cosmiques secondaires* issus des interactions avec l'atmosphère terrestre).

1.2.1.1 Rayonnement cosmique primaire

Ces rayonnements cosmiques primaires sont constitués à 85% de protons et à 14% de particules alpha. Le reste est constitué d'ions lourds (Z > 2). Le flux moyen de particules est de 1800 part.m^{-2}.s^{-1} dans l'espace, mais tombe à 360 part.m^{-2}.s^{-1} au niveau de la mer. L'énergie moyenne de ce flux est de 500 MeV, pouvant croître au delà de 1 GeV. Les particules cosmiques interagissant avec le vent solaire, le flux reçu par la Terre est fonction de l'activité du soleil [ZIE96b] [CRE96].

1.2.1.2 Rayonnement solaire

Le soleil rayonne constamment les produits des réactions thermonucléaires qui se produisent en son sein. Il est ainsi une source de lumière, de chaleur, mais aussi de particules sous la forme d'un gaz, le vent solaire, essentiellement composé d'électrons et d'ions positifs d'hydrogène et d'hélium (protons et particules α) et dans une moindre mesure d'ions lourds . Ce vent solaire s'étend depuis sa source dans toutes les directions de l'espace.

Le flux de particules provenant du soleil varie selon l'activité de ce dernier. En particulier l'activité du soleil connaît un cycle de 11 ans qui contient 2 phases : une phase calme et une phase d'activité intense. Lors des phases d'activité, le flux augmente considérablement, autant en densité de particules qu'en énergie. Cependant, les particules générées par le soleil s'approchent rarement à moins de 60 000 km de la terre grâce aux ceintures de radiation qui entourent celle-ci.

Ces ceintures de radiation, aussi appelées ceintures de Van Allen, sont situées dans la magnétosphère et constituent *un lieu de piégeage des particules à haute énergie* venues du rayonnement cosmique et des rayonnements solaires. Le champ magnétique terrestre se comporte comme un bouclier de protection qui piège certaines particules tentant soit d'atteindre le niveau du sol, soit de s'en échapper et les contraint à tourner autour de l'équateur magnétique en décrivant des ceintures en forme de tores (voir figure 1). La ceinture la plus proche de la terre, dite intérieure, est située à environ 5000 km d'altitude et est principalement constituée de protons à haute énergie (plusieurs dizaines de MeV). La ceinture extérieure, beaucoup plus large, s'étire entre 20000 km et 36000 km d'altitude et est principalement constituée d'électrons à haute énergie (autour de 1MeV).

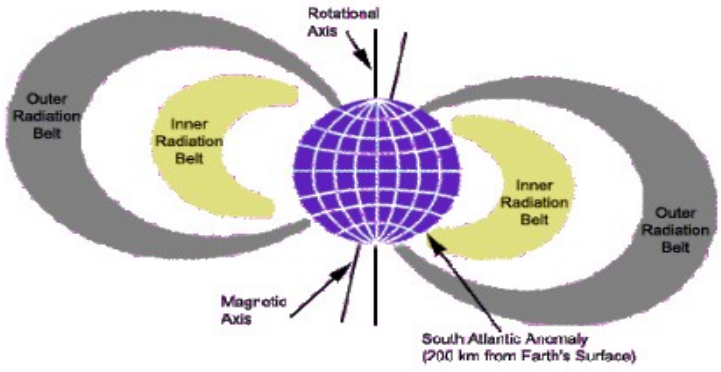


Figure 1: Ceintures de Van Allen.

Lors des périodes d'activité solaire importantes, la pression du rayonnement solaire crée une troisième ceinture de particules autour de l'atmosphère [NIE01] qui a pour effet de diminuer l'ensemble du rayonnement cosmique de 30% au niveau du sol [ZIE96b].

1.2.1.3 Rayonnement cosmique secondaire

Le flux de particules entrant dans l'atmosphère est d'environ 1000 part.m^{-2}.s^{-1}. Ces particules, principalement des protons et des particules α vont interagir par interaction nucléaire forte avec les noyaux d'oxygène et d'azote présents dans celle-ci. Sous l'effet de ces réactions, les noyaux se brisent faisant apparaître une succession de cascades de particules. L'effet immédiat de ces interactions est d'accroître le flux de particules (cf. figure 2). Celui-ci pourra atteindre une valeur dépassant 10^6 part.m^{-2}.s^{-1} (1 part.mm^{-2}.s^{-1}) autour de 15 km d'altitude.

Les noyaux sont constitués de nucléons (protons et neutrons) qui forment avec les mésons (dont fait partie le pion ou méson π) une famille de particules appelées hadrons. Les hadrons interagissent entre eux grâce à la force nucléaire forte. Ces réactions, à très haute énergie, produisent des jets hadroniques dont les particules résultantes sont aussi des hadrons et dans la plupart des cas des mésons π et K (kaons). Les pions ont une durée de vie de l'ordre de la nanoseconde. Si les pions chargés ne sont pas rapidement absorbés dans une nouvelle interaction forte, ils se désintègrent en donnant naissance à un muon et au neutrino associé. Le muon ainsi généré ne participera plus au phénomène de cascades. De plus, dans chaque interaction entre hadrons, une partie de l'énergie n'est pas transmise aux hadrons résultants Le nombre d'interactions fortes va donc vite s'amenuiser et laisser la place aux interactions faibles

qui causeront la désintégration des pions chargés en muons et neutrinos. Les pions neutres se désintégreront par interaction électromagnétique et généreront des *photons* γ. Enfin, les produits de ces deux derniers types d'interaction feront apparaître par la suite, soit *des électrons et des neutrinos* dans le cas de la désintégration des muons soit *des électrons et des positrons* dans le cas de la désintégration des photons gamma.

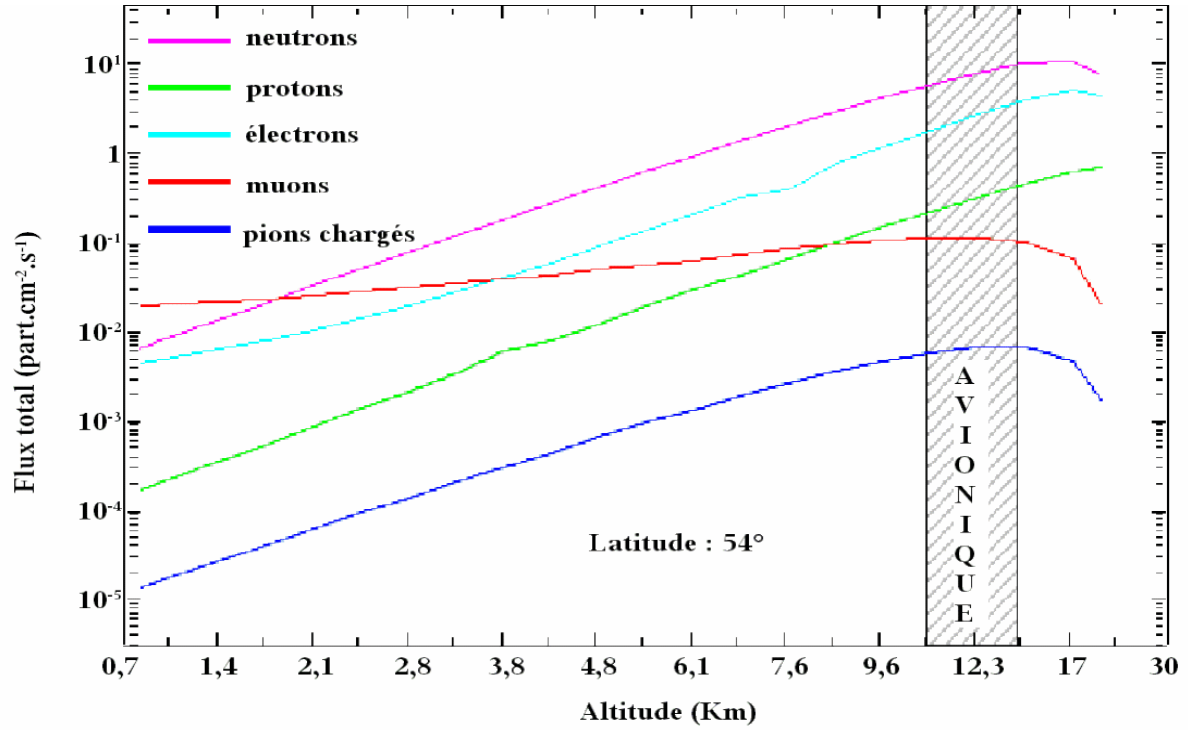


Figure 2: Flux de différentes particules dans l'atmosphère en fonction de l'altitude.

Finalement le flux de particules qui atteint la surface de la terre est environ 3000 fois plus faible et chute jusqu'à environ 360 part.m^{-2}.s^{-1} (voir figure 3).

Les quelques réactions que nous venons d'examiner ne représentent pas la totalité des réactions se produisant dans l'atmosphère mais en sont une approximation suffisante. Ce bref aperçu permet de comprendre comment un flux primaire de protons peut, par interaction, créer de nouvelles particules qui seront présentes dans l'atmosphère.

Seulement 1% de ces particules primaires peut créer une cascade susceptible d'atteindre le niveau de la mer. En effet la majorité des particules générées seront absorbées par l'atmosphère

soit par interaction soit car elles sont instables. Parmi celles-ci, les pions se désintègrent en muons après environ 1 ns et ces muons se transforment en électrons en quelques µs. Les électrons et les protons chargés électriquement perdent de l'énergie par interaction électromagnétique avec les atomes atmosphériques, tandis que l'absence de charge électrique des neutrons, leur confère un pouvoir de pénétration important les rendant ainsi plus dangereux pour l'électronique terrestre [ZIE96b] [ZIE98] [JAC01] [BAU00] [HUA02] [DES01].

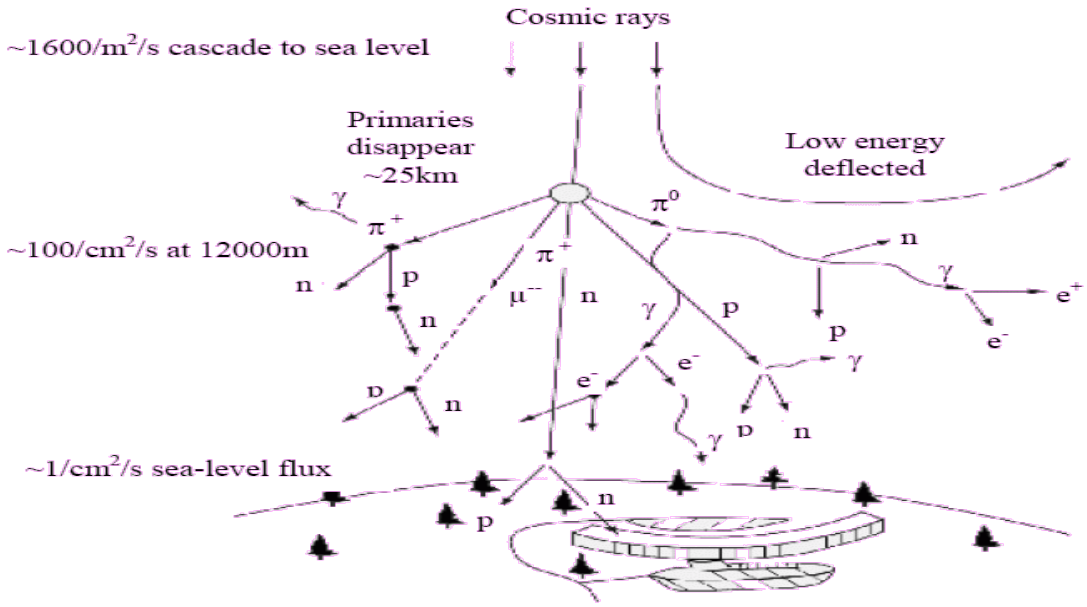


Figure 3: Cascades de particules à travers l'atmosphère terrestre [ZIE96b].

1.2.2 Sources de radiations artificielles

Parallèlement aux radiations naturelles, qui sont issues d'événements très énergétiques, l'humanité possède plusieurs moyens de créer des particules pouvant affecter les circuits électroniques. Nous présenterons ici les accélérateurs de particules, les flash lumière et les lasers.

1.2.2.1 Accélérateur de particules

Les accélérateurs de particules peuvent être utilisés pour bombarder des circuits de test, comme par exemple à Los Alamos avec un faisceau de neutrons dont le spectre est équivalent à celui des neutrons atmosphériques (voir figure 4). Ces tests servent à simuler en accéléré le

comportement d'un circuit en utilisation normale. Comme le flux est très important, les données statistiques sur la fiabilité du composant peuvent être récupérées rapidement. Le faisceau a en général un diamètre de quelques centimètres.

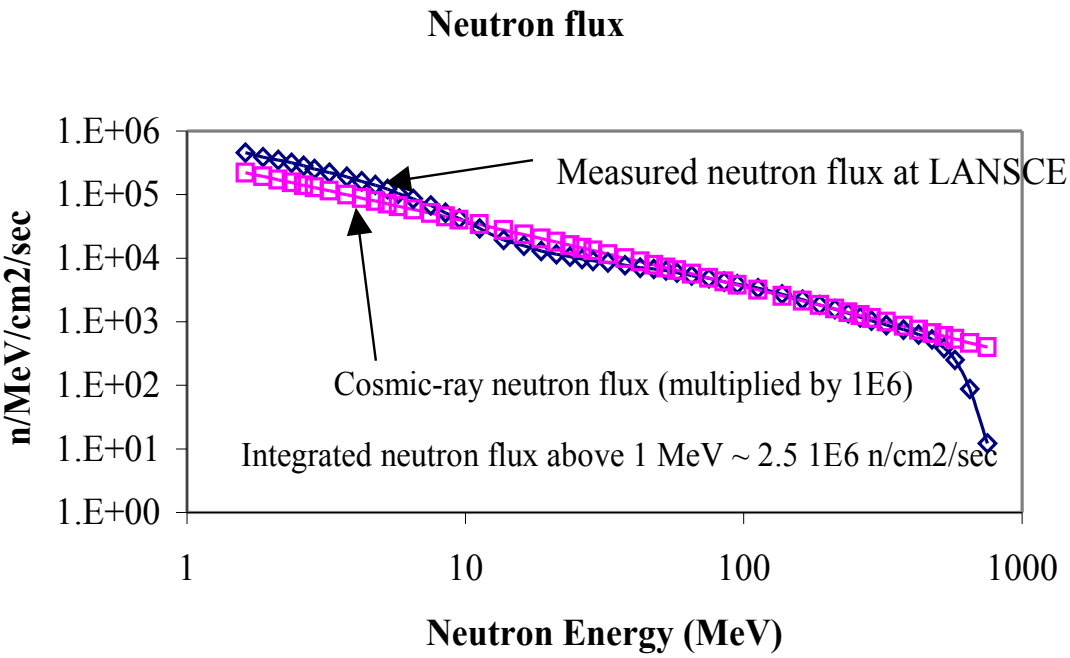


Figure 4: Spectre du flux de neutron disponible au laboratoire de Los Alamos.

Différentes sources existent à travers le monde, concernant aussi bien les protons, les électrons, les neutrons, certains ions lourds etc. Toutes ces sources peuvent théoriquement être utilisées pour simuler le comportement de dispositifs dans l'environnement spatial. Cependant leur accès est réglementé et n'est pas à disposition du grand public.

1.2.2.2 Flash

La simple lumière visible peut faire réagir un composant électronique par effet photo-électrique. Un flash assez intense (quelques watts) peut être utilisé pour perturber un circuit électronique [AND97]. Ces perturbations sont souvent intenses, mais nécessitent la décapsulation du circuit pour affecter directement le silicium. En outre on ne peut irradier très précisément une faible surface car une lumière polychromatique (voir figure 5) a tendance à

diffracter et est difficile à focaliser. De plus, on ne maîtrise absolument pas l'énergie rayonnée sur le silicium.

Une telle source de perturbations est facile à mettre en oeuvre, mais ses caractéristiques en font un outil trop grossier pour une étude quantitative précise de la sensibilité d'un circuit.

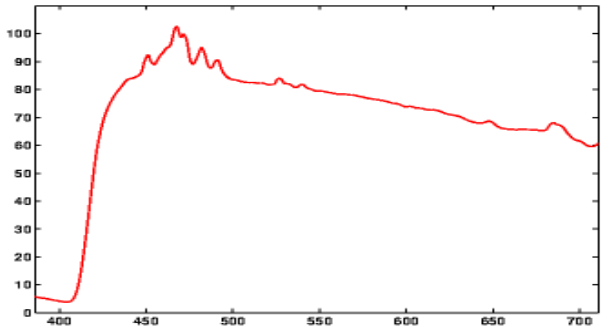


Figure 5: Spectre d'un flash au xénon Nikon SB-16.

1.2.2.3 Laser

Un laser (pour Light Amplification by Stimulated Emission of Radiation) est une source de lumière cohérente et monochromatique. Parmi les sources lumineuses, les laser constituent une solution particulièrement idoine pour la photo excitation d'un circuit électronique. Le faible rayon de leur faisceau, après focalisation par un microscope optique (possible grâce à sa cohérence), permet d'exciter l'échantillon sur une surface proche du micromètre carré. De plus, leur monochromaticité permet de bien contrôler la profondeur de pénétration des photons dans l'échantillon. Quand la longueur d'onde est suffisamment faible, l'essentiel de l'injection a lieu au voisinage de la surface. Au contraire, quand la longueur d'onde est suffisamment importante, l'absorption de photons s'effectue sur toute la profondeur de l'échantillon.

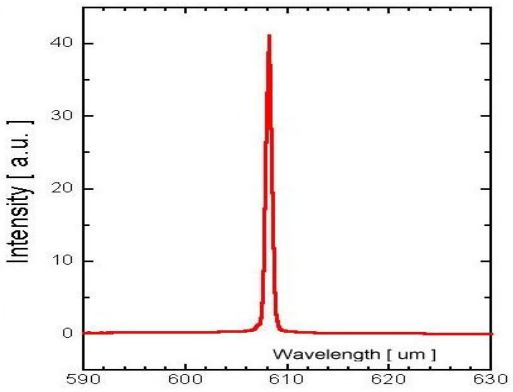


Figure 6: Spectre d'un laser de longueur d'onde 608 µm.

1.2.3 Étude de la densité radiative de l'atmosphère

On distingue trois grands types de milieux radiatifs liés à l'existence de l'atmosphère terrestre: le milieu extra atmosphérique (ou l'espace), le milieu atmosphérique et l'environnement terrestre.

1.2.3.1 Milieu extra-atmosphérique (au delà de 1000 km d'altitude)

Le milieu extra-atmosphérique est le plus étendu et le plus contraignant en matière de radiations. Parce qu'il est très vaste, les phénomènes modifiant la nature de cet environnement sont nombreux et les sources de radiations y sont variées. Certaines de ces sources sont connues et globalement prévisibles tandis que d'autres proviennent d'événements occasionnels et sont totalement imprévisibles. Les sources de radiation les plus importantes recensées dans cet environnement sont les *rayonnements solaires*, le *rayonnement cosmique* et les c*eintures de radiations*. Chacune d'entre elles est à l'origine de l'émission de flots de particules variées pouvant interagir et générer ainsi l'émission de *particules secondaires*.

Les cas de défaillances d'engins spatiaux et de satellites imputables aux particules ne manquent pas dans la littérature[BAR95] [ONE94].

1.2.3.2 Milieu atmosphérique (jusqu'à 1000 km d'altitude)

La terre et son environnement sont protégés par l'atmosphère qui constitue un véritable écran vis-à-vis du rayonnement issus de l'espace. La plupart des radiations issues de ce rayonnement,

perdent une grande partie de leur énergie initiale dans l'atmosphère durant leur parcours vers la terre. Cette perte d'énergie est la conséquence d'interactions et de collisions avec les atomes présents dans l'atmosphère (principalement l'oxygène et l'azote). Cependant, ces interactions produisent des cascades de particules secondaires qui vont à leur tour engendrer de nouvelles cascades, jusqu'à ce que la dernière génération atteigne le niveau du sol (voir figure 3) [ZIE96b]. Cette succession de cascades tend à accroître la densité de particules dans l'atmosphère. Cependant le nombre de cascades ne croît pas indéfiniment car les particules soit subissent une désintégration rapide imputable à leur courte durée de vie, soit perdent leur énergie jusqu'à avoir un niveau trop faible pour provoquer une nouvelle cascade.

Par conséquent quand le niveau de pénétration dans l'atmosphère augmente, c'est-à-dire au fur et à mesure que l'altitude diminue, la présence des éléments primaires appartenant au rayonnement cosmique se raréfie tandis que la quantité de particules secondaires progresse. Il résulte de ces différents phénomènes l'existence d'une altitude où la densité de radiations est *maximale*. Cette altitude a été repérée pour la première fois en 1936 à l'aide d'un ballon sonde autour de 18 km. Elle a été confirmée par la suite par plusieurs mesures, et le flux de particules à cette altitude est d'environ 10^6 part./(m^2.s). Cette altitude est connue sous le nom de « maximum de Pfotzer » du nom du scientifique l'ayant découverte. Cette altitude est proche de l'altitude de croisière de la majorité des vols commerciaux [TAB93] [NOR93] [ZIE96a] [OLS93].

1.2.3.3 Environnement terrestre (niveau du sol)

Même si l'on met de coté certains systèmes électroniques évoluant dans des environnements particuliers comme les centrales nucléaires ou au voisinage des accélérateurs de particules, les circuits sont en permanence soumis à un *environnement radiatif ambiant*.

Les radiations rencontrées au niveau du sol proviennent non seulement des cascades de particules d'origine cosmique vues dans la section précédente mais encore de la désintégration radioactive d'atomes lourds présents en faible quantité dans tous les matériaux et plus particulièrement dans les métaux. La présence de ces atomes provoque une contamination radioactive des circuits notamment par les eaux de lavage au cours du « process » ou encore par les boîtiers contenant ces mêmes circuits [ZIE96a]. Enfin, il existe une radioactivité naturelle

provenant de la croûte et du manteau terrestre ou piégée dans certaines roches (granit) ainsi que des émanations gazeuses radioactives provenant du centre de la terre et remontant à la surface. Les éléments issus de ces dernières sources et leurs sous produits radioactifs sont aussi présents à l'état de traces dans les sols et dans les matériaux de construction (pierre, brique, béton, plâtre…).

1.3 Modes d'interaction des rayonnements considérés

Après nous être intéressés aux différentes sources de radiations existantes, nous allons considérer les interactions possibles entre ces rayonnements et le silicium. Tout d'abord nous parlerons des effets généraux des rayonnements sur le silicium, puis nous approfondirons les effets des électrons, des neutrons et des photons.

1.3.1 Considérations générales

La principale cause de fautes dans les circuits intégrés est identifiée comme étant l'ionisation du semi-conducteur. Elle est imputable à la génération de paires électron-trou par une particule ionisante. Dans le cas ou elle est provoquée par des particules chargées, cette ionisation peut être directe. Mais pour des particules incidentes neutres, elle a pour origine les particules secondaires émises lors de la collision entre la particule primaire et les noyaux des matériaux internes.

L'énergie et *la masse* de la particule ne sont donc pas les seuls facteurs à considérer pour évaluer la probabilité des particules à générer des événements singuliers. L'identification du mode d'interaction devient donc prépondérante dans cette analyse.

1.3.2 Ions (ions lourds, particules Alpha)

Les particules chargées ont un pouvoir d'ionisation direct. Au cours de leur passage au travers du matériau semi-conducteur, ces particules vont échanger de l'énergie avec le milieu par interaction électromagnétique. Cette interaction appelée aussi interaction coulombienne est équivalente à une *collision inélastique* de l'ion incident avec les électrons atomiques de la matière. L'énergie injectée dans le silicium est caractérisée par deux paramètres : le LET et la profondeur de pénétration.

- Le LET (Linear energy transfert) ou transfert d'énergie linéique, correspond à la quantité d'énergie que la particule dépose le long de sa trace par unité de longueur (dE/dx).

- La profondeur de pénétration, correspond à la distance que parcourt la particule avant d'avoir perdu son énergie initiale.

Le produit de ces 2 paramètres fournit l'énergie déposée dans le matériau. Les tables de Ziegler fournissent pour chaque type d'ions les valeurs du LET et de la profondeur en fonction du matériau traversé. Ces tables sont aussi disponibles au travers d'un outil logiciel appelé SRIM qui a été créé par l'équipe de J.F. Ziegler. La figure 7 représente les valeurs de LET pour différents ions. Elle est tracée à partir des données de SRIM. [DUT01].

Les ions lourds peuvent aussi interagir dans des *collisions élastiques* avec les noyaux du silicium. Dans ce cas, une très faible quantité d'énergie est transférée car la masse des noyaux de la matière est en général grande comparée à la masse de la particule incidente.

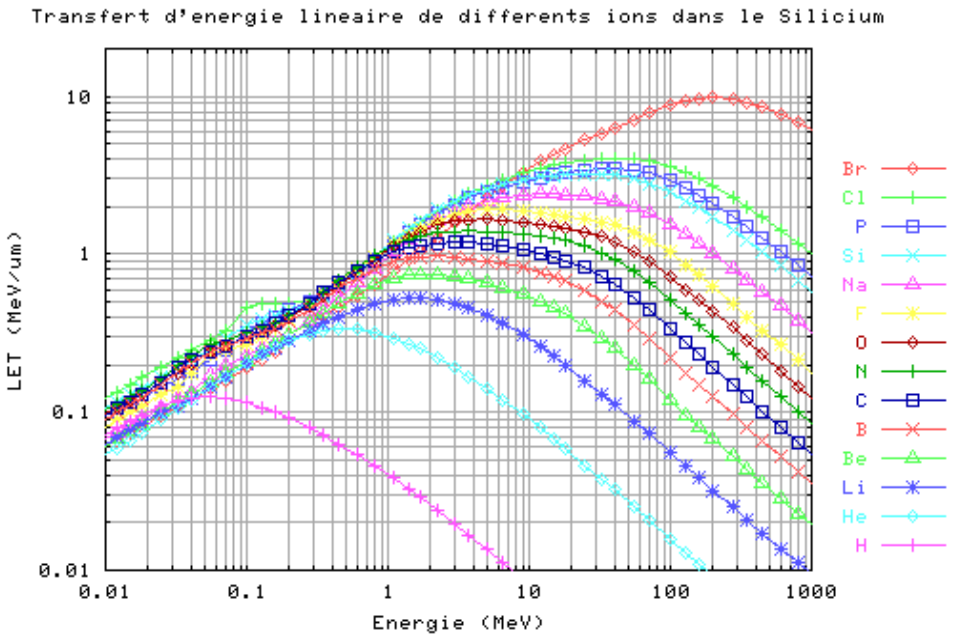


Figure 7: Transfert d'énergie linéique (LET) de différents ions dans le silicium.

1.3.3 Neutrons (rayonnement Bêta)

Les neutrons ne possèdent pas de charge électrique et ne sont donc pas sensibles à l'interaction coulombienne avec les électrons ou les noyaux. Leur principale interaction avec la matière se produit au travers d'interactions fortes avec le noyau. Le noyau étant beaucoup plus petit que l'atome, ce type de réaction est donc beaucoup plus rare. Lorsqu'un neutron interagit avec la matière, il y a soit collision élastique soit collision inélastique. Dans les 2 cas, l'énergie du neutron incident va être répartie entre les produits de la réaction. La majeure partie sera emportée par les noyaux légers tandis que les noyaux de recul issus des réactions élastiques n'obtiendront qu'une faible partie de l'énergie. Avec l'élimination ou la purification des couches de passivation en verre de borophosphosilicate (BPSG) dans les technologies récentes, les interactions neutron-silicium sont devenues la cause première des erreurs dues aux neutrons car elles peuvent générer des produits secondaires allant de l'hydrogène au phosphore. En effet, les couches de passivation à base de bore contiennent un isotope, le B^{10} possédant une grande section efficace d'interaction avec les neutrons de faible énergie. La section efficace prépondérante de ce choc est une réaction de type $^{28}Si(n,a)^{7}Li$ et les produits résultants un noyau de lithium 7 et une particule alpha sont tous deux ionisants. Dans les technologies récentes, un effort particulier a été réalisé afin d'éliminer cette cause d'erreur et les couches de passivation utilisant du PSG ou du ^{11}BPSG se sont généralisées. Néanmoins, la réduction d'échelle des technologies conduit à une augmentation des concentrations en produits dopants dont le bore. L'ordre de grandeur de la concentration en bore actuellement utilisée se situe autour de 10^{19} atomes.cm^{-3} dans la zone active et la probabilité d'interaction neutron-bore redevient prédominante sur l'interaction neutron-silicium à partir d'une concentration en bore de 10^{20} cm^{-3}. Ce type d'interaction, n'étant plus négligeable vis-à-vis de l'interaction neutron-silicium, la probabilité d'erreurs imputables aux neutrons augmente. [BAU95] [BAU01] [WRO02] [CAS02]

1.3.4 Photons

Ces rayonnements électromagnétiques particuliers peuvent interagir de différentes façons avec les matériaux en fonction de leur énergie. L'interaction avec des électrons s'effectue soit par effet photo-électrique, soit par effet Compton. Pour des énergies élevées, l'interaction avec la

matière s'accompagne d'une production de paires électron- positron. Les 3 effets principaux de ces rayonnements sont résumés ci-après.

- L'absorption par effet photo-électrique domine pour des photons d'une énergie inférieure à 60keV. Elle consiste en l'absorption complète de l'énergie du photon incident par l'émission instantanée d'électrons à très grande vitesse. L'atome s'ionise.

- L'effet Compton est prédominant dans le silicium quand les photons ont une énergie comprise entre 60keV et 15MeV. Dans ce type d'effet, le photon incident ne perd qu'une faible partie de son énergie dans l'interaction avec l'atome. Il en résulte un nouveau rayonnement γ qui pourra à nouveau interagir avec les électrons du silicium jusqu'à ce que son énergie devienne insuffisante.

- La création de paires électron-trou devient majoritaire lorsque les photons ont une énergie supérieure à 15MeV. Cette réaction se produit lorsque le photon incident passe dans le champ d'une particule chargée. Il se désintègre alors en une paire électron-positron. Le positron à une durée de vie très courte, sa capture par un électron entraîne leur annihilation et génère 2 photons, chacun d'une énergie de 0,51MeV. Ces 2 photons pourront alors à leur tour générer des effets Compton ou photoélectrique.

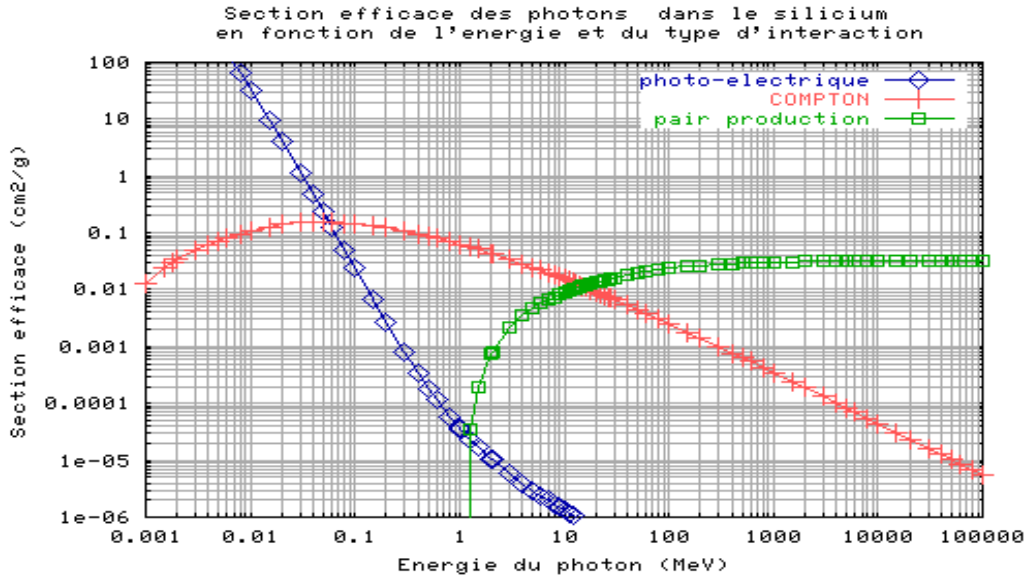


Figure 8: Section efficace des photons dans le silicium en fonction de l'énergie et du type d'interaction.

1.3.4.1 Rayons X et Gamma

Ces rayonnements sont très énergétiques (longueur d'onde inférieure à 100 nm). Pour ces valeurs d'énergie (supérieures à 12 eV), l'effet Compton et la création de paires électron-trou prédominent.

1.3.4.2 Lumière visible

La lumière visible (comprise entre 400 et 700 nm) est constituée de photons peu énergétiques (de 1,8 à 3,1 eV). Dans ce cas l'absorption photo-électrique prédomine. Par contre, les sources classiques de lumière visible sont polychromatiques, ce qui signifie que l'on ne peut connaître avec précision l'énergie des photons qui frappent le silicium.

1.3.4.3 Cas particulier du laser

Dans le cas d'un laser, tous les photons ont la même énergie et la même phase. Cela permet de faire des simplifications théoriques sur l'énergie déposée par chaque photon et de supposer que les photons ont tous le même vecteur vitesse. Le laser est donc une source très stable de photons. Si le laser a une longueur d'onde relativement grande (c'est-à-dire une énergie faible), son impact sur du silicium produit une source stable d'électrons pendant le régime permanent (avant la déplétion complète des zones de valence du matériau). C'est le cas des lasers visibles et infrarouges (énergie comprise entre 0,52 et 3,1 eV).

1.4 Effet sur les technologies CMOS des interactions radiation-silicium

Le dépôt d'énergie d'une particule ionisante dans un matériau se matérialise par la création de paires électron-trou. Selon que le matériau est isolant, semiconducteur ou conducteur, les porteurs libérés n'ont pas la même capacité de retour à l'équilibre thermodynamique. Cette capacité dépend directement de la densité et de la mobilité des porteurs libres dans le matériau considéré :

- Dans les éléments conducteurs, la mobilité et la densité des porteurs libres étant très importantes, l'énergie déposée n'entraîne aucune perturbation.

- Dans les semiconducteurs, les porteurs libérés peuvent soit revenir à l'équilibre par recombinaison avec les autres porteurs libres du semiconducteur soit progresser rapidement vers les électrodes de potentiel électrique créant ainsi des perturbations de très courte durée (quelques ps) appelées événements singuliers.

- Les matériaux isolants ne possèdent pratiquement pas de porteurs libres et leur mobilité y est très limitée, donc les charges créées ne peuvent pas se combiner avec celles du milieu. De ce fait, si les porteurs négatifs sont suffisamment séparés des porteurs positifs (sous l'effet d'un fort champ électrique par exemple), les porteurs ne contribuent pas à un processus de recombinaison ni de conduction. Ces centres de charge, en grande majorité des atomes ionisés apparaissant au sein du matériau et aux interfaces participent à l'effet de dose.

1.4.1 Effet de dose

Tous les matériaux isolants présents dans les circuits intégrés sont soumis à une accumulation de charge par effet de dose. Cet effet est dominant au niveau de la structure active, l'oxyde de grille (volume et interface). Actuellement, la dégradation du composant entraînée par la dose cumulée est principalement attribué à l'interface Si-SiO_2 des transistors.

Dans des matériaux isolants, une grande partie des charges générées par le passage de particules ionisantes se retrouve piégée dans le milieu. En effet, elles ne peuvent pas participer au phénomène de recombinaison initial ni se combiner avec des porteurs libres inexistants. Cette phase est extrêmement rapide, de l'ordre de la picoseconde. L'étape qui suit celle de recombinaison consiste en un déplacement des charges. La mobilité des électrons dans le SiO_2 reste suffisamment importante et ceux-ci sont tout de même assez rapidement évacués de l'oxyde. De mobilité beaucoup plus réduite, les trous ne pourront se déplacer que très lentement vers l'interface Si/SiO_2 sous l'action du champ électrique. La vitesse de transport des trous dépend de la température, du champ électrique et du processus de fabrication.

Au cours de leur migration vers l'interface, certains trous peuvent rencontrer des centres de défaut et être piégés dans l'oxyde. Une fois parvenue au niveau de l'interface, une partie des trous peut se recombiner en dehors de l'isolant. Dans le cas où les trous se retrouvent piégés au

niveau de l'interface, la tension aux bornes de l'isolant augmente. Si les charges parviennent à se combiner hors de l'isolant, la tension diminue. La quantité des trous piégés varie entre 1% et 80% en fonction des paramètres évoqués précédemment. Une fois la migration des trous terminée, il reste dans l'oxyde une charge quasi permanente qui va évoluer très lentement. Le phénomène de guérison, caractérisé par la recombinaison des porteurs à l'interface et par la migration des charges piégées vers les électrodes est donc très lent (figure 9).

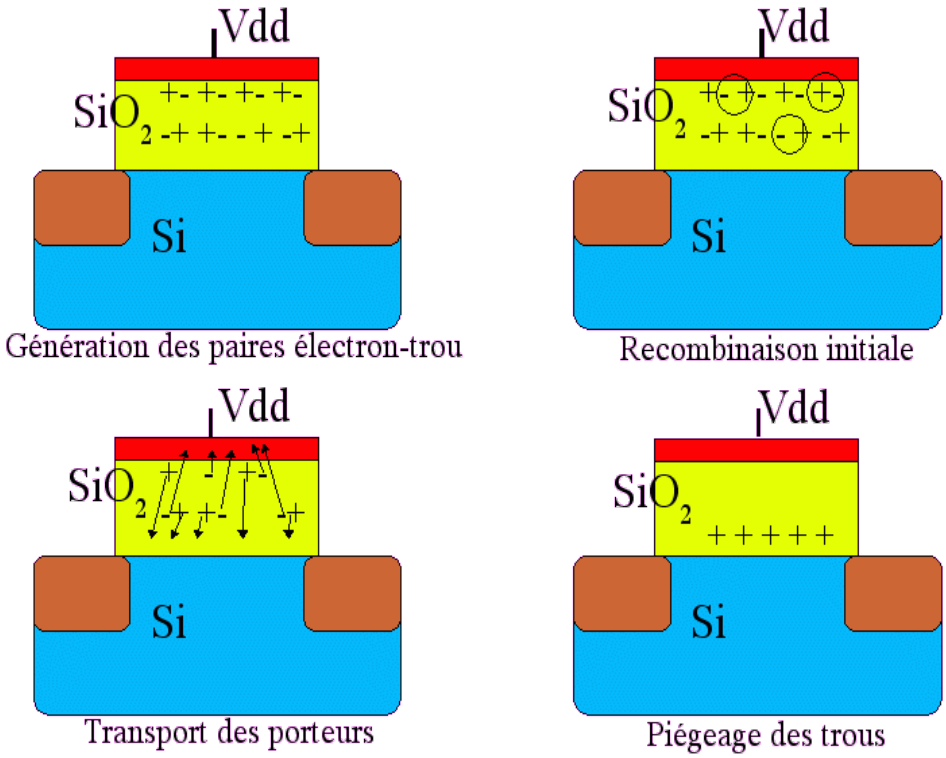


Figure 9: Piégeage des trous par effet de dose.

De manière pratique l'effet de dose induit par le piégeage des trous se traduit par une dérive de la tension de seuil du composant, pouvant l'entraîner vers un état permanent passant ou bloqué [SAI98] [ANE00].

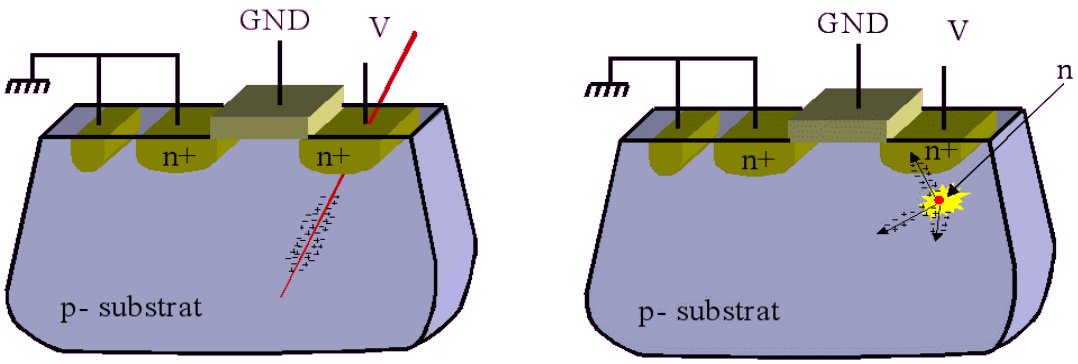
1.4.2 Événements singuliers

Les événements singuliers (Single Event Effects, SEEs) sont instantanés et peuvent provoquer des défaillances soit temporaires soit permanentes. C'est pourquoi ils sont généralement classés en deux sous catégories :

- Les événements réversibles c'est-à-dire non destructifs appelés aléas logiques ou "Soft Errors".

- Les événements irréversibles c'est-à-dire destructifs appelés "Hard Errors".

Ces événements sont dus au courant induit par la collection de charge à l'intérieur ou au voisinage de la zone active d'un transistor. Les charges à l'origine de ces phénomènes sont générées soit directement par une particule chargée (figure 10 (a)) soit indirectement par les particules secondaires issues des interactions entre les nucléons et les noyaux du matériau semiconducteur (figure 10 (b)).



(a) Ionisation directe *(b) Ionisation indirecte*

Figure 10: Modes d'interaction des particules impactant un transistor.

1.4.2.1 Événements singuliers irréversibles (hard errors)

Single Event Latch up (SEL)

La proximité des transistors NMOS et PMOS dans les technologies CMOS induit la présence d'une structure parasite de type NPNP appelée thyristor. La mise en conduction de cette structure conduit à une amplification du courant avec un gain infini qui se traduit par un court-circuit entre les bornes d'alimentation. Le verrouillage de cette structure peut conduire à la destruction du circuit si l'alimentation n'est pas immédiatement coupée.

Le principe de durcissement le plus utilisé contre le SEL consiste à surveiller le courant d'alimentation du circuit et à mettre le circuit hors tension lorsque celui-ci franchi un seuil préalablement déterminé. Cette solution entraîne donc une réinitialisation du circuit. Le phénomène de SEL n'affecte pas les circuits conçus dans certaines technologies comme la technologie SOI (Silicon On Insulator) ou la technologie DNW (Deep N Well) car celles-ci ne présentent pas de structure parasite de type NPNP [POU00] [BRU96] [JOH96].

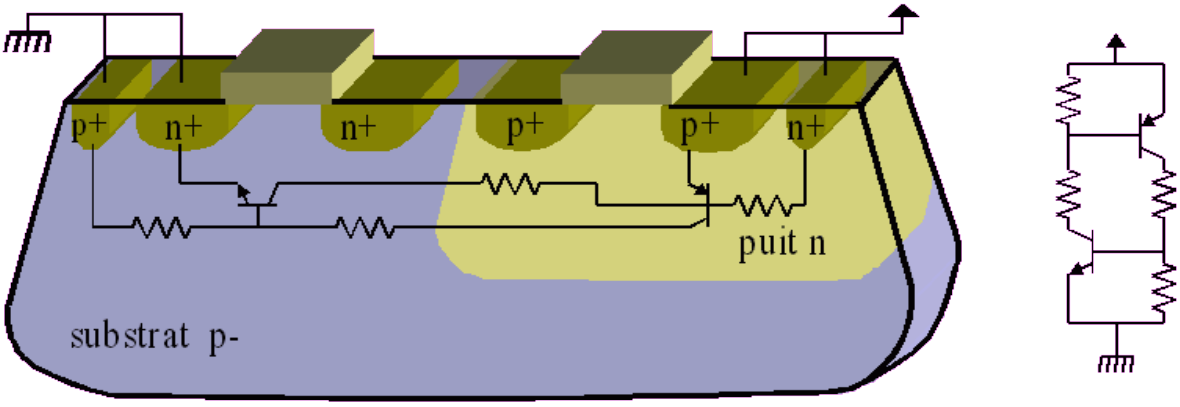


Figure 11: Déclenchement de la structure NPNP lors du phénomène de Latch-up.

Single Event Snap back (SES)

Cet événement produit les mêmes effets qu'un SEL, c'est-à-dire un courant élevé et une surchauffe locale pouvant mener à la destruction du composant. Contrairement au SEL, il ne nécessite pas la mise en conduction de la structure NPNP. Dans le cas du snapback, c'est le transistor bipolaire inhérent à la structure NMOS qui est à l'origine du phénomène. La zone sensible au snapback correspond à la partie sous-jacente à la zone déplétée du drain d'un

transistor NMOS bloqué. A la suite d'un dépôt de charge dans cette région, les porteurs se déplacent le long des lignes de champ. La majorité des électrons gagne le drain alors au potentiel haut tandis que les trous se déplacent principalement à travers la région P (substrat ou puits) reliée au potentiel bas. Le transistor NPN dit "parasite", correspondant aux jonctions source/substrat/drain peut alors se mettre à conduire sous l'effet de l'augmentation du potentiel de substrat. Il s'en suit l'apparition d'un courant de conduction drain/source à travers la structure bipolaire. La zone déplétée sous la jonction drain/substrat étant considérablement diminuée, le potentiel de la base du transistor bipolaire est positif et contribue à l'entretien de sa polarisation.

Le phénomène peut être détecté en surveillant la consommation. Il existe 2 manières de stopper l'auto-entretien du phénomène. La première consiste à couper l'alimentation puis à remettre le dispositif sous tension exactement comme dans le cas du SEL. La seconde, applicable aux technologies CMOS, consiste à modifier la polarisation en entrée de la paire NMOS/PMOS afin d'inverser la valeur du potentiel de drain. Cette modification a pour effet de stopper le flux de courant entre le drain et la source du transistor NMOS, et donc d'annihiler le phénomène.

Cet événement peut être important dans le cas des MOS de puissance mais est très peu probable dans les technologies actuelles qui fonctionnent sous faible tension. Ces événements sont aussi limités dans les circuits en fonctionnement du fait des changements rapides et permanents des potentiels de drain [KOG89] [POU00].

Single Event Burnout (SEB)

Cet effet est initié par le passage d'un ion lourd à travers un transistor MOSFET de puissance polarisé en inverse. La mise en conduction de la structure bipolaire PNP dans le cas du PMOS ou NPN dans le cas des transistors NMOS est à l'origine des SEB. Lorsque la structure bipolaire est mise en conduction, il peut apparaître un régime de fort courant. Au delà de ce régime, si le courant dépasse un certain seuil, la tension collecteur/émetteur, correspondant respectivement au drain et la source du transistor NMOS, chute tandis que le courant collecteur-émetteur augmente fortement. Il s'en suit, dans le transistor bipolaire, un phénomène thermique local très rapide appelé "second claquage". L'élévation de la température lors de cet événement peut localement atteindre le point de fusion du silicium et entraîner inévitablement la destruction du composant [HOH87] [DAC95] [ALL96].

Single Event Gate Rupture (SEGR)

Le phénomène de SEGR est provoqué par le passage d'un ion lourd à travers la grille d'un transistor MOS et correspond au claquage de l'oxyde de grille. Il affecte principalement les transistors de puissance. Cependant, la réduction des épaisseurs d'oxyde de grille dans les technologies récentes fortement intégrées semble être à l'origine d'une augmentation des SEGR dans les circuits nanométriques.

Ce phénomène est dû à la manifestation combinée du passage d'une particule et du champ électrique appliqué. Lorsqu'un ion lourd traverse le diélectrique, il se forme un filament de plasma entre le silicium et la grille qui va permettre aux charges déposées de diffuser vers l'interface Si/SiO2. L'accumulation de charges à cette interface entraîne l'augmentation du champ électrique dans l'oxyde. Lorsque ce champ est suffisamment important, il peut entraîner la rupture locale de l'oxyde de grille. Les charges sont alors collectées à travers l'oxyde, occasionnant une surchauffe locale de la structure. Sous l'effet de la température le diélectrique peut fondre localement créant un court circuit permanent à travers l'oxyde de grille [ALL94] [WHE94] [ALL96] [SEX97].

1.4.2.2 Événements singuliers réversibles (soft errors)

Single Event Upset (SEU)

Le terme de SEU est associé au phénomène entraînant le changement d'état d'un point mémoire en son état inverse sous l'effet d'une particule ionisante. Lorsque la particule ionisante traverse la jonction bloquée d'un transistor MOS, elle ionise le composant par interaction coulombienne le long de son parcours laissant derrière elle une colonne de charges sous la forme de paires électron-trou. Parmi les charges déposées, une partie va se recombiner sans participer au phénomène de SEU. L'autre partie sera collectée sous l'effet du champ électrique. Les porteurs négatifs seront collectés par la cathode de la jonction tandis que les porteurs positifs migreront vers l'anode. Ce déplacement de charge crée un courant de conduction entre les 2 électrodes qui se comportent comme un court-circuit entraînant la valeur du potentiel de drain vers celle du potentiel de substrat. La variation de potentiel sur le drain heurté modifie alors la polarisation du deuxième inverseur faisant basculer sa sortie vers l'état inverse. Enfin, le changement en

sortie du deuxième inverseur conclut le phénomène en modifiant la polarisation en entrée de l'inverseur affecté. Le basculement est alors définitif et la valeur du point mémoire modifié.

La sensibilité d'un point mémoire est caractérisée par sa *charge critique*. Elle correspond à la quantité de charge tolérée par le nœud de mémorisation. Si la charge collectée après impact est supérieure à la charge critique, l'état logique du point mémoire sera modifié. La valeur de cette charge critique est fortement dépendante de la capacité du nœud heurté ainsi que de la tension d'alimentation, donc de la technologie et des conditions de fonctionnement.

Les mémoires de type SRAM en technologie CMOS sont plus sensibles à ce phénomène que les mémoires de types DRAM qui possèdent une capacité plus élevée. De même, le parcours réduit des particules dans les mémoires SOI limite la quantité de charges déposées rendant ce type de technologie moins sensible aux SEU [DET97] [FAC98] [DOD98] [DOD97] [DOD96].

Single Event Transient (SET)

Cet effet concerne plus particulièrement la logique combinatoire. Un SET ou aléa transitoire est initié lorsqu'une charge est déposée sur un noeud d'un transistor MOSFET, entraînant une impulsion de tension qui se propage dans le circuit.

Un aléa transitoire peut devenir la cause d'une erreur s'il parvient à l'entrée d'un registre en synchronisme avec le signal d'écriture ou encore s'il se manifeste en amont sur la logique d'écriture (arbre d'horloge, logique de décodage etc.).

Trois conditions doivent être réunies pour qu'un aléa transitoire puisse être mémorisé dans un registre:

- l'impulsion doit présenter une amplitude et une largeur suffisantes pour être propagées à travers la logique combinatoire sans atténuation importante,
- le chemin logique entre la porte affectée et le prochain registre doit permettre la propagation de l'impulsion,
- l'impulsion parvenue à l'entrée d'un registre doit satisfaire à ses conditions d'écriture, c'est-à-dire, dans le cas des registres synchrones respecter des temps de "set-up" et de "hold" et dans

le cas des registres asynchrones respecter le temps de commutation de l'entrée [BAZ97] [NGU03] [ALE02].

Multiple Bit Upset (MBU)

Un MBU est défini comme un aléa unique provoquant un ensemble d'erreurs logiques en différents points mémoire. Dans les circuits dynamiques, la propagation d'un événement transitoire (SET) peut induire des erreurs multiples lorsqu'il parvient à l'entrée de plusieurs points de mémorisation en satisfaisant leurs conditions d'écriture. Un cas similaire survient lorsqu'un SET affecte la logique de décodage des mots ou des adresses d'une mémoire. Dans les mémoires, les erreurs multiples peuvent aussi résulter de l'interaction d'une particule unique avec plusieurs régions sensibles. Par exemple, lorsque les charges induites par la perturbation diffusent sur plusieurs jonctions voisines ou encore lorsque l'angle d'incidence de la particule lui permet de traverser les jonctions de différentes cellules en déposant de l'énergie [MUS96] [MAI03] [ZOU89].

Single Event Functional Interrupt (SEFI)

Le terme SEFI désigne les événements causés par une perturbation et menant à une perte de fonctionnalité temporaire du circuit (ou à l'interruption de l'opération en cours). Les SEFI qui ne concernent que des événements n'endommageant pas le circuit, peuvent durer jusqu'à la coupure d'alimentation dans certains cas ou un temps fini dans d'autres cas. Ils désignent en général un événement qui dure longtemps [KOG98] [JES96].

1.5 Étude de l'interaction laser-silicium

Dans cette section nous allons présenter les caractéristiques d'une source laser. Des références à cette source seront utilisées dans la suite du document quand nous parlerons des expériences réalisées dans le cadre du projet Duracell.

1.5.1 Source laser

Une source laser est une source lumineuse particulière dans le sens où elle produit notamment un rayonnement entre autres monochromatique et polarisé de manière rectiligne. Ce rayonnement est issu d'un milieu amplificateur, d'une cavité optique, puis le rayonnement passe dans un modulateur optique qui permet de réguler son intensité à la demande. Ce faisceau laser est ensuite focalisé sur le circuit à tester par un microscope optique. Nous nous sommes appuyés sur la thèse de Hervé Lapuyade [LAP96] pour des données quantitatives sur le rayonnement laser.

1.5.1.1 Caractéristiques principales

La principale caractéristique du laser que nous allons utiliser dans ce travail est sa monochromaticité qui assure que les photons produits ont tous la même énergie. De plus un faisceau laser peut être focalisé dans son intégralité sur une surface proche de sa longueur d'onde sans craindre les phénomènes classiques de diffraction des rayonnements polychromatiques.

La source est un laser pulsé qui permet d'envoyer des impulsions de 6 ns de durée à une fréquence de 60 Hz.

1.5.1.2 Énergie transmise par le laser

La longueur d'onde d'un faisceau laser nous donne l'énergie transportée par les photons qui le composent grâce à l'équation

$$E = h * \nu \qquad \text{(Eq. 1)}$$

avec E l'énergie en eV, h la constante de Planck, et ν la fréquence considérée.

En travaillant avec un laser vert Nd:YAG de longueur d'onde 532 nm, et avec la formule

$$\nu = c / \lambda \qquad \text{(Eq. 2)}$$

(c la vitesse de la lumière, et λ la longueur d'onde), on trouve une énergie des photons émis égale à 2,33 eV. Comme le gap du silicium est de 1.2 eV, les photons sont susceptibles de créer des paires électrons-trous par photo excitation [VER89]. Par contre la bande interdite de l'oxyde de silicium (SiO_2) étant de 9 eV, le laser n'affectera pas du tout ce matériau.

La source a une puissance réglable qui peut monter jusqu'à 0,4 W sur une durée de 6 ns. L'énergie maximale déposée est donc de 2,4 nJ. D'après nos premières expérimentations nous avons constaté des perturbations dans les circuits CMOS de dernière génération à moins de 1% de cette puissance.

1.5.1.3 Dépôt de charges dans le silicium

L'impact d'un faisceau laser dans le silicium provoque par effet photoélectrique une création de porteurs (des paires électron-trou). Cette création de porteurs n'est effective que si l'énergie des photons impactant le circuit est supérieure au gap du silicium pour faire passer des électrons de la bande de valence vers la bande de conduction [LAL94].

La régulation de la population de ces porteurs s'effectue de plusieurs manières [MAR93] :

- thermalisation des porteurs qui abandonnent toute énergie supérieure à l'énergie de gap,
- relaxation diélectrique,
- recombinaison ambipolaire [ROO53].

Les deux premiers phénomènes ont un temps caractéristique de quelques picosecondes alors que le troisième a une durée de l'ordre de la nanoseconde. On considérera les deux premiers phénomènes comme instantanés par rapport à la durée de l'expérience.

Cette accumulation de charges provoque un courant lors de la collection, courant qui s'évacue par les chemins classiques de propagation (figure 12).

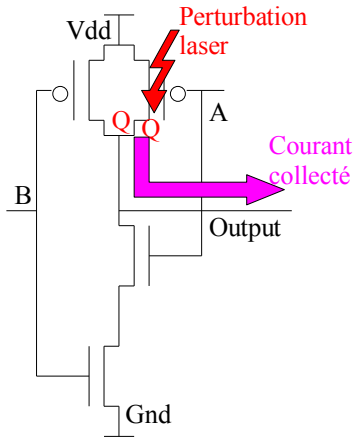


Figure 12: Chemin de collection des charges (Q) dans une porte NAND attaquée par un tir laser.

1.5.2 Influence des paramètres du laser sur l'interaction avec le silicium

1.5.2.1 Longueur d'onde et pénétration

À la longueur d'onde de 532 nm (lumière verte), le coefficient d'absorption optique α est égal à 1,3 μm^{-1} [BUC88]. L'énergie du laser est donc très rapidement absorbée par le silicium. Au contraire, un laser d'une longueur d'onde de 1064 nm (rayonnement infrarouge) a un coefficient d'absorption de 800 μm^{-1} qui permet une pénétration profonde de l'énergie lumineuse dans le substrat. La densité d'énergie dans les couches supérieures du circuit sera donc beaucoup plus élevée avec un laser vert, et elle est concentrée dans les zones supérieures du circuit (zones de métallisation et grille par exemple) [LER05], [BUC87].

Cependant le laser infrarouge est très efficace pour tirer à travers le circuit (par la face arrière) pour éviter de décaper le circuit, ou pour éviter les multiples niveaux de métallisation qui caractérisent les technologies de fabrication actuelles.

1.5.2.2 Impulsion laser et courant généré

Comme la génération de porteurs est active durant toute l'illumination du semiconducteur, on peut maîtriser la durée pendant laquelle les paires électron-trou sont produites, et donc la quantité totale de charge déposée dans le circuit. Il est donc possible de maîtriser le profil de

l'impulsion de courant ainsi créée car sa durée dépend de la durée de l'impulsion laser, et son intensité dépend de la densité d'énergie du rayonnement laser.

Dans la figure 13 on peut voir la relation entre les paramètres du tir laser et ceux de l'impulsion de courant générée. Le pic de courant est entretenu pendant la durée du tir et son intensité dépend de celle du laser. La décroissance du courant dépend des paramètres du circuit, à savoir les capacités connectées au noeud frappé.

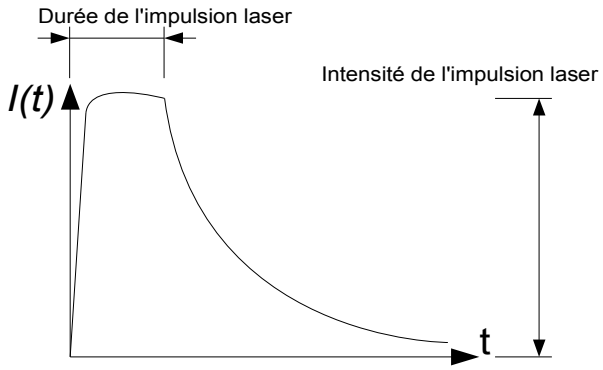


Figure 13: Profil de l'impulsion de courant générée par un rayon laser.

1.6 Conclusion

Malgré leurs modes d'action très différents, toutes ces sources de perturbation provoquent les mêmes effets, à savoir la génération de charges dans un noeud d'une structure MOS, charge qui provoque un courant pendant sa collection, et qui *in fine* génère une impulsion de tension qui se propage suivant les chemins électriques réguliers du circuit. Les paramètres de cette impulsion de tension sont déterminés par les spécificités de la source physique de la perturbation, mais dans le cadre de circuits numériques nous pourrons modéliser cette impulsion par une impulsion carrée de tension entre le niveau logique haut et le niveau logique bas. Le seul paramètre inconnu de cette impulsion restant donc sa durée. En nous basant sur ce modèle d'impulsion nous allons être capables de discriminer les perturbations affectant un circuit numérique d'après ce seul paramètre, paramètre que nous sommes capables de mesurer.

Nous allons utiliser l'exemple du laser vert décrit dans ce chapitre comme instrument d'injection de référence dans la suite de ce travail pour ses qualités de précision et de souplesse d'utilisation.

Chapitre 2 : Technologies nanométriques et composants sécuritaires

2.1 Introduction

Dans ce chapitre nous nous intéressons à l'évolution des technologies de conception des circuits intégrés et à son impact sur la conception des circuits sécuritaires. Il apparaît que l'évolution des techniques de fabrication des circuits tend à diminuer au maximum les marges de bruit des composants physiques des circuits intégrés. Il devient donc de plus en plus facile de perturber le fonctionnement d'un circuit. De plus la banalisation de ces circuits dans la vie de tous les jours les amène à conserver dans leurs mémoires de plus en plus d'informations confidentielles qui peuvent devenir la cible de personnes malintentionnées.

Ces facteurs s'additionnent pour provoquer une situation dans laquelle les circuits dits sécuritaires deviennent l'enjeu majeur d'une lutte opposant les pirates voulant obtenir les informations confidentielles stockées dans ces circuits et les concepteurs qui doivent à tout prix les en empêcher en intégrant des mesures de protection dans leur flot de conception. Les technologies et les protections s'améliorant, la difficulté des attaques augmente et cela motive l'adoption de sources toujours plus précises, la plus précise étant la source laser.

Nous allons tout d'abord étudier l'impact de l'évolution des composants sur leur sensibilité, puis nous présenterons différentes attaques disponibles dans la littérature pour finir par présenter les moyens à disposition des concepteurs pour s'en protéger.

2.2 Loi de Moore et planning de l'industrie du semiconducteur

La loi de Moore, omniprésente dans l'industrie du semiconducteur, est un défi pour tous les acteurs de l'évolution des circuits intégrés. Cette loi prévoit en moyenne un doublement de la densité d'intégration tous les 18 mois. Depuis son premier énoncé en 1965 par G.E. Moore (co-

fondateur de la société Intel), les divers intervenants dans la fabrication des circuits intégrés s'efforcent en permanence d'innover dans le but de la perpétuer, voire de la devancer.

L'intégration de plus en plus poussée et la miniaturisation constante des circuits intégrés entraînent des problèmes nouveaux quasiment à chaque génération de processus technologiques. C'est dans ce cadre que nous avons vu apparaître des problèmes liés à l'intégrité des signaux tel ceux de couplages capacitifs ou de bruit sur la masse. De nombreux autres problèmes sont aussi apparus comme l'augmentation des courants de fuites, les retards dans les lignes d'interconnexion, l'augmentation de la consommation de puissance et bien d'autres. Cette énumération n'a pas pour objectif de dresser une liste exhaustive mais de rendre compte de la complexité nouvellement apparue pour continuer à suivre la loi de Moore.

Ces problèmes concernent tous les acteurs associés à la réalisation des circuits, à savoir les technologues, les fabricants, les concepteurs de circuits, les concepteurs d'outils de CAO, les spécialistes du test et les concepteurs de systèmes. C'est pourquoi l'innovation et la recherche en électronique sont en majorité portées par la prévision, l'examen et la résolution des problèmes futurs.

Le problème nous concernant est lié au phénomène de réduction des dimensions des transistors qui entraîne la diminution de la charge contenue dans les portes logiques, et donc à l'augmentation de la sensibilité des dernières technologies semi-conductrices.

Avant de rentrer dans le vif du sujet, il nous semble important de voir comment l'évolution des différents paramètres entraînés par la miniaturisation peut influencer la fréquence d'apparition des dysfonctionnements liés aux phénomènes qui nous préoccupent.

Pour cela nous avons décidé de nous appuyer sur les prévisions de L'ITRS (International Technology Roadmap for Semiconductors) en examinant comment la variation des paramètres peut affecter les taux d'erreurs dues aux interactions des particules-circuits [ANG00][ITR05] [MOO65].

2.3 Évolution des paramètres électriques et de la sensibilité des structures HCMOS en fonction de la technologie

La table 1 rassemble les paramètres importants liés à la variation des règles de conception dans les semiconducteurs pour les prochaines années jusqu'en 2010.

Table 1: Carte de la tendance technologique pour les années à venir.

année de production	2003	2004	2005	2006	2007	2010
largeur de grille MPU (nm)	65	53	45	40	35	25
ASICs						
largeur de grille ASIC (nm)	90	75	65	53	45	32
épaisseur d'oxyde (nm)	1,1-1,4	0,9-1,4	0,8-1,3	0,7-1,2	0,6-1,1	<1
tension d'alimentation (V)	1-1,2	0,9-1,2	0,9-1,1	0,9-1,1	0,8-1,1	0,7-1,0
tension de seuil (V)	0.27-0.36	0.24-0.33	0.21-0.30	0.18-0.27	0.17-0.23	???
fréquence d'horloge (GHz)	3	4	5	7	9	15
densité combinatoire (Transistors/cm²)	61M	77M	97M	122M	154M	309M
densité SRAM (Transistors/cm²)	305M	393M	504M	646M	827M	1.7G
DRAMs						
taille mémoire	1G	1G	1G	2G	2G	4G
dimension cellule (µm²)	0,08	0,07	0,05	0,04	0,03	0,01
dimension circuit (mm²)	139	110	82	122	97	83
GBits/cm²	0,77	0,97	1,31	1,76	2,22	5,19

2.3.1 Dimension de l'oxyde

Toutes les dimensions liées à l'oxyde diminuent avec les avancées technologiques (voir figure 14). La capacité de l'oxyde de grille est un paramètre important car il joue un rôle déterminant dans la sensibilité des composants aux particules ionisantes. En effet, plus la capacité de la grille est faible, plus la quantité de charge nécessaire pour changer l'état du transistor est faible, et donc plus la structure est sensible aux perturbations.

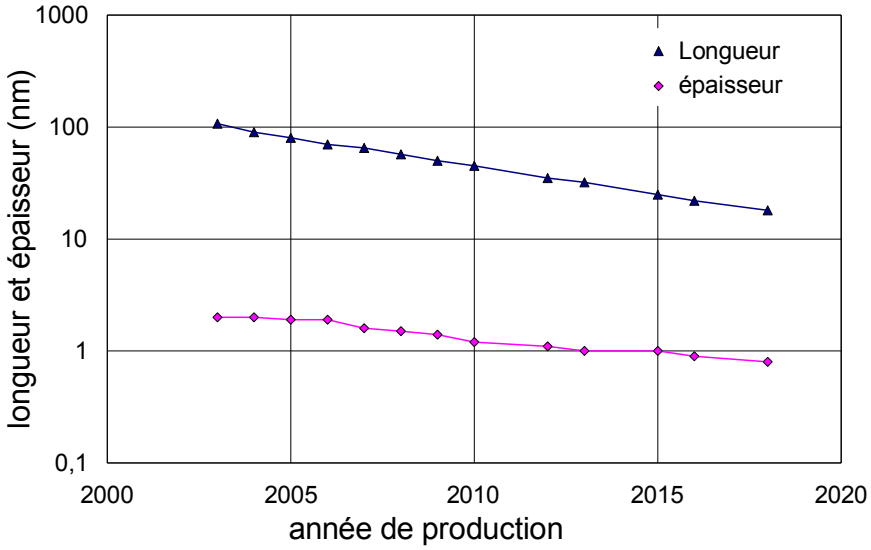


Figure 14: Évolution des dimensions d'oxyde de grille.

D'après la "roadmap", l'épaisseur de l'oxyde de grille devrait atteindre 1nm dès 2006. La diminution de l'épaisseur d'oxyde en dessous de ce seuil critique ne permettra plus de répondre aux exigences concernant les courants de fuite dans certaines applications. Par conséquent, des matériaux à haute constante diélectrique (high K) tels le HfO2 (dioxyde de Hafnium) prendront très certainement la relève dans les applications à faible consommation en veille dès 2006, suivi par les micro-processeurs dès 2007. C'est pourquoi, nous considérerons avec prudence les évolutions indiquées pour les valeurs de capacité d'oxyde après 2007. Ces valeurs sont calculées à partir de la constante diélectrique du SiO2 et de ses dimensions (voir figure 15).

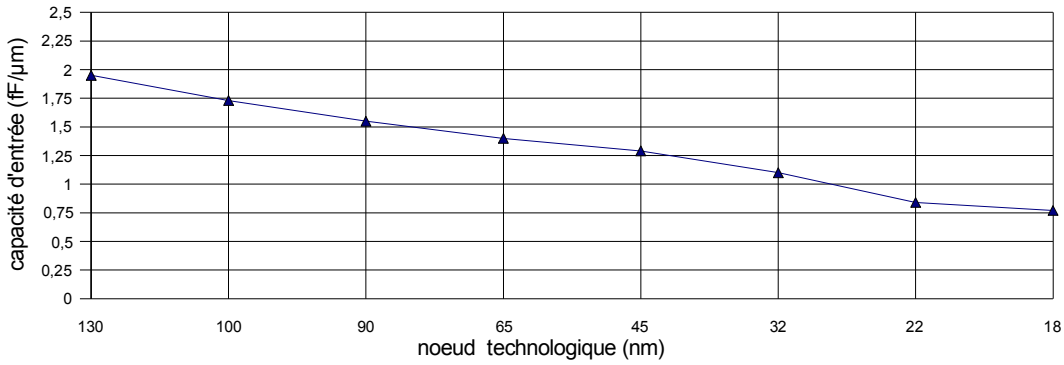


Figure 15: Évolution de la capacité d'oxyde de grille par unité de largeur.

En technologie CMOS, l'évolution de la capacité du diélectrique est en rapport direct avec la charge perturbatrice que peuvent tolérer les dispositifs. Lorsque cette capacité diminue, la charge tolérée, plus couramment appelée charge critique, diminue et la sensibilité de la technologie augmente.

2.3.2 Tensions d'alimentation et de seuil

On sait que la consommation de puissance dynamique d'un dispositif à transistors MOS évolue proportionnellement au carré de la tension d'alimentation V_{DD} car elle suit la loi

$$P_{dyn} = CV_{DD}^2 \qquad \text{(Eq. 3)}$$

Le meilleur moyen pour diminuer la consommation de puissance, consiste donc à réduire la tension d'alimentation. Cette réduction entraîne une diminution du potentiel aux bornes du diélectrique et permet de conserver un champ électrique acceptable dans l'isolant malgré la diminution de son épaisseur. Il en résulte une diminution de la charge critique et par conséquent une augmentation de la sensibilité (voir figure 16).

La charge critique d'un point de mémorisation est la quantité de charge qu'il faut injecter dans une structure pour faire basculer son état. Dans les mémoires de type SRAM, elle est considérée comme étant le produit du potentiel par la capacité d'un nœud de mémorisation. Pour cela nous considérons que la somme des largeurs de canal des transistors N et P est approximativement égale à 4 fois leur longueur (tendance vérifiée sur la plupart des technologies actuelles). La

quantité de charge tolérée pour la logique combinatoire est évaluée en tenant compte de la propagation d'un événement transitoire à travers un inverseur chargé par une porte identique. Le rapport W/L utilisé dans cette évaluation est de 10 pour le transistor NMOS et de 20 pour le transistor PMOS (voir figure 17).

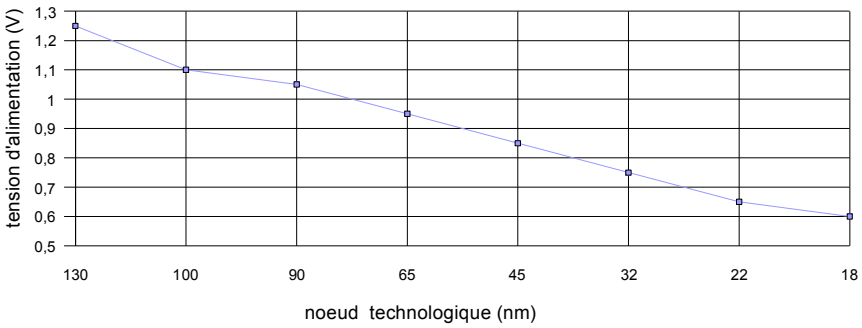


Figure 16: Évolution de la tension d'alimentation.

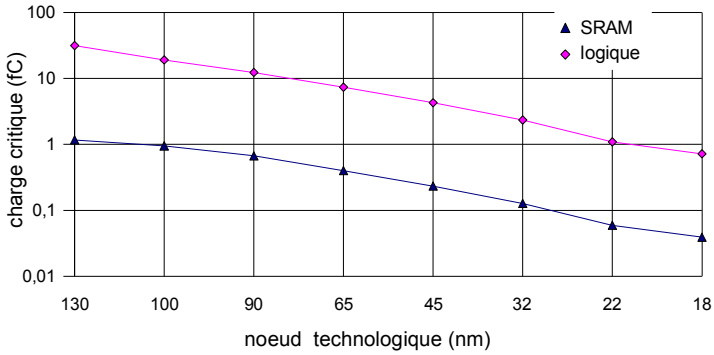


Figure 17: Évolution de la charge critique dans la logique et les mémoires de type SRAM.

2.3.3 Fréquence d'horloge

Les générations récentes de circuits se concentrent sur l'augmentation des fréquences d'horloges rendues possibles par l'évolution des technologies, mais la vitesse de fonctionnement joue un rôle dans la sensibilité des circuits aux événements transitoires. Cette sensibilité peut être évaluée en fonction de la fenêtre de vulnérabilité liée à la fois à la fréquence d'horloge et à la durée des événements transitoires. En logique séquentielle, la fenêtre de vulnérabilité d'un élément est définie comme le rapport entre la durée de l'événement transitoire mesuré à l'entrée

d'un registre et la période d'horloge. En réalité, ce rapport n'est valable que si l'impulsion transitoire est correctement synchronisée avec les temps de stabilisation et de maintien de l'élément séquentiel mais dans les autres cas de figure, il reste proportionnel à ce même rapport. Si nous ne considérons que les événements transitoires provoqués par l'impact de particules ionisantes, nous pouvons raisonnablement penser que non seulement les événements transitoires doivent augmenter en nombre mais aussi en durée puisque la sensibilité générale de la logique combinatoire augmente. Cette double augmentation des caractéristiques des événements transitoires couplée à la diminution de la période d'horloge ne peut qu'entraîner une augmentation de la sensibilité générale des circuits.

2.3.4 Dimension des zones actives

Une réduction des dimensions liée au facteur d'échelle accompagne les avancées technologiques et la *dimension des zones actives* obéit également à cette évolution. Il s'agit peut être là du seul paramètre susceptible d'apporter une réduction de la sensibilité des composants, tant dans la logique séquentielle que dans la logique combinatoire et dans les points mémoire. En effet la surface d'une porte ou d'un point mémoire sensible à une particule est fonction de la surface des zones actives. Cette surface diminuant, la probabilité que cette structure soit perturbée diminue mécaniquement.

Cette tendance est vraie si l'on regarde les composants élémentaires un à un, ou si l'on compare 2 circuits sensibles identiques réalisés dans deux générations de technologie différentes. Cependant la réduction a pour but de réaliser des circuits de plus en plus complexes comportant toujours plus d'éléments et finalement la section efficace d'interaction doit être étudiée dans son ensemble ou dans son rapport avec la surface totale. Ce rapport est défini comme quasi-constant par la carte d'évolution technologique de L'ITRS. Ainsi, le rapport de la surface efficace d'une structure sur la surface totale peut quasiment être défini comme une constante n'influençant pas la sensibilité des circuits.

En revanche la diminution générale des règles de lithographie implique un rapprochement des zones sensibles entre elles. Cette conséquence peut se répercuter fortement sur l'augmentation des erreurs multiples (MBU) et finalement accroître la sensibilité des circuits [MUS96].

La diminution de la profondeur du puits ou du substrat n'intervient qu'indirectement sur la sensibilité du composant, elle ne participe pas à la diminution de la charge critique. En revanche, elle permet une réduction du trajet des particules dans celui-ci. Donc à LET identique, la charge déposée sera inférieure si la particule traverse le puits en intégralité. Cette réduction s'accompagne aussi d'une réduction du volume de silicium sensible. L'avantage d'un puits ou d'un substrat peu profond sur la réduction des SER est donc certain et peut s'observer sur certaines technologies telles que les technologies SOI ou les technologies sur substrat épitaxié.

2.4 Techniques de perturbation et conception de circuits sécuritaires

2.4.1 Contexte

Les circuits intégrés ont de multiples applications dans la vie de tous les jours, et en particulier pour des applications dites « sensibles » qui gèrent des informations confidentielles comme des informations bancaires ou d'identification (clés de cryptage par exemple). La confidentialité de ces informations stockées dans un circuit intégré est donc une priorité pour les concepteurs, et les techniques utilisées doivent évoluer en fonction des menaces potentielles au fur et à mesure qu'elles apparaissent. Ainsi, alors que les premières cartes à puces (cartes téléphoniques) pouvaient être mises en échec par des techniques très basiques comme l'isolation d'une entrée de la puce, les circuits actuels doivent être attaqués par de s techniques très avancées, par exemple l'utilisation de pointes pour sonder directement l'état des composants logiques du circuit (probing), l'utilisation de failles dans les algorithmes du circuit ou l'injection de fautes dans le circuit pour provoquer un état non désirée à la conception. Comme les concepteurs ont appris à sécuriser les différents modes de fonctionnement de leurs circuits pour éviter une diffusion accidentelle des informations confidentielles, et que les technologies actuelles demandent énormément d'effort pour permettre un probing efficace, les pirates ont appris à perturber le fonctionnement normal du circuit pour le faire rentrer dans un état non prévu par le concepteur [BIH96A], [JOY97] et [AND97], [BAR04], [BID01]. Les techniques de piratage qui nous intéressent ici relèvent donc principalement de l'injection de fautes dans un circuit intégré.

2.4.2 Injection de fautes

Historiquement, perturber des circuits par injection de fautes a d'abord été effectué via les signaux externes tels que l'alimentation ou l'horloge, puis sur des blocs mémoire qui sont facile à repérer. À mesure que ces méthodes ont été connues et que les concepteurs ont protégé leurs circuits contre ces attaques, l'injection de fautes a commencé à apparaître dans la logique séquentielle et enfin dans la logique combinatoire.

2.4.2.1 Perturbation de l'alimentation

Les portes logiques sont des composants actifs qui doivent être alimentés. En effet les transistors CMOS sont utilisés en tant qu'interrupteurs et consomment une quantité substantielle de courant quand ils commutent. L'intégralité des composants d'un circuit dépend donc du bon fonctionnement de l'alimentation, perturber cette dernière conduisant très souvent à une interruption de la fonctionnalité du circuit.

Le corollaire de cette observation est donc que l'alimentation d'un circuit (principalement la consommation de courant, mais aussi les variations de tension dans les rails d'alimentation) est en elle-même une source d'information. On peut déduire de son observation les périodes d'activité majeures du circuit (comme les moments où le coprocesseur mathématique se met en route dans un circuit cryptographique [KOC99]). Ces informations permettent au pirate de cibler ses attaques pour augmenter ses chances de récupérer les données qu'il cherche.

2.4.2.2 Perturbation de l'horloge

Dans un circuit synchrone, le signal d'horloge contrôle l'ensemble des éléments séquentiels du circuit. Il peut y avoir un ou plusieurs signaux d'horloge définissant autant de domaines d'horloge. Ces signaux sont en général dénués de logique (mis à part un arbre d'amplification), même si certaines architectures recourent à des arbres d'horloge contenant des couches logiques.

La perturbation de l'horloge a des effets dévastateurs sur le fonctionnement d'un circuit car elle perturbe le fonctionnement de toute la couche séquentielle du circuit. Si la fréquence d'horloge est accélérée, l'intégrité du signal n'est plus garantie et génère une grande quantité d'erreurs car les signaux n'ont pas le temps de se propager et de se stabiliser entre deux fronts montants. Si

l'horloge n'est plus active, le circuit ne fonctionne tout simplement pas car l'information ne peut franchir les verrous que sont devenues les bascules. Par contre dans le cas où l'horloge est ralentie, l'observabilité du circuit augmente car l'information reste plus longtemps stable dans les bascules pour l'observation (par probing par exemple).

Par exemple, dans une architecture où une information confidentielle transite par un registre, un pirate connaissant un minimum l'architecture du circuit pourra couper l'horloge pendant le stockage de cette information et disposera ainsi du temps nécessaire pour récupérer cette information. Il pourra ensuite suivre pas à pas la progression de cette information dans le circuit pour affiner sa connaissance de l'architecture et détecter les moments propices à la récupération de l'information.

De manière plus générale, tous les signaux globaux (reset, signaux de contrôle) ont le même type de comportement face aux attaques et génèrent des résultats similaires. Par contre l'horloge est souvent générée par un bloc externe à la fonction ciblée (comprenant les informations confidentielles) ce qui permet de l'isoler rapidement après une brève analyse du circuit. Le contrôle de l'horloge est donc un atout majeur pour le pirate dans sa quête de l'information confidentielle.

2.4.2.3 Perturbation des mémoires

L'injection de fautes dans une mémoire consiste à modifier le contenu des cellules contenant l'information. Ces cellules contiennent un élément mémorisant qui stocke l'information sous la forme d'une charge électrique. Une perturbation de cette charge électrique permet donc d'altérer l'information contenue dans la mémoire.

Les mémoires étant en général à la pointe de la technologie en matière d'intégration, la charge qu'elles contiennent est très faible ce qui rend d'autant plus facile leur perturbation. Par contre la diminution de leurs dimensions rend d'autant plus difficile l'isolation d'une cellule précise afin de la perturber. La technologie nécessaire pour injecter une erreur dans un point mémoire précis demande de pouvoir affecter une zone de l'ordre de 1 um^2.

En contrepartie, les mémoires sont des éléments particulièrement sensibles en technologie CMOS de par leur densité et la faible charge qui matérialise le contenu informatif (voir

figure 17). De plus, leur présence importante dans les circuits intégrés modernes participe à l'augmentation de la sensibilité globale d'un circuit [MIT05].

Si l'on considère uniquement la capacité d'injection de faute dans une mémoire, il suffit d'attaquer la mémoire par le biais d'un simple flash d'appareil photo pour provoquer des erreurs comme cela est montré dans [SKO03].

2.4.2.4 Perturbation de la logique séquentielle

La logique séquentielle comporte des bascules et des verrous. Ces composants sont des points de mémorisation utilisés en technologie CMOS synchrone (pour les bascules) permettant de découper le domaine temporel en intervalles de temps délimitées par deux fronts actifs consécutifs d'horloge. Le principe de fonctionnement d'un circuit synchrone repose sur cette séparation pour garantir l'intégrité du signal transitant dans la logique combinatoire située entre deux éléments séquentiels.

En effet, les éléments séquentiels stockent un état stable des données entre deux fronts actif d'horloge. Pendant cette durée de stockage, les signaux sont propagés dans la logique combinatoire. Quand le front actif d'horloge arrive, les signaux se sont stabilisés ce qui permet de garantir l'intégrité de l'information transitant dans le circuit.

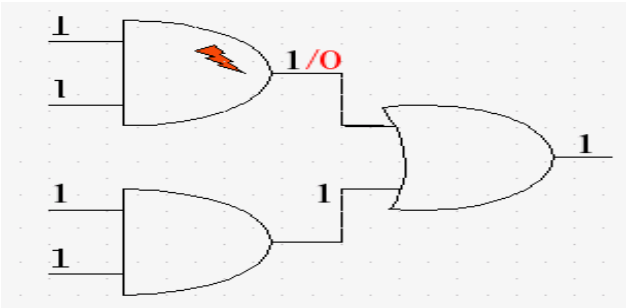


Figure 18: Exemple de masquage de faute dans la logique combinatoire.

Les éléments séquentiels contiennent donc une information stable pendant une bonne partie du cycle d'horloge (t_{setup} + t_{hold}) ce qui est un gros avantage quand on veut maîtriser la perturbation du circuit. De plus la perturbation d'un élément séquentiel garantit (si les temps de propagation

sont respectés) que l'erreur sera propagée comme un signal valide (s'il n'y a pas de masquage logique cf. figure 18) dans le circuit.

2.4.2.5 Perturbation de la logique combinatoire

La logique combinatoire est constituée de portes logiques qui appliquent une fonction logique aux données en provenance des entrées, et restituent le résultat aux éléments séquentiels en sortie. Toute perturbation dans la logique combinatoire est susceptible de se propager vers la sortie du bloc combinatoire pour être capturée par un élément séquentiel.

Cependant, les temps de propagation font que le signal perturbé n'est pas forcément disponible en entrée des éléments séquentiels au moment où le verrou est passant (c'est-à-dire aux alentours du front montant d'horloge), ce qui peut masquer la faute pour la suite du fonctionnement du circuit. De plus, les chemins de propagation « actifs » dans la logique combinatoire peuvent conduire à un masquage du chemin correspondant au signal erroné, ce qui élimine l'erreur de fonctionnement du circuit.

Ces facteurs font qu'une injection de faute dans un bloc combinatoire donne des résultats difficiles à analyser car la propagation de l'erreur induite est assujettie à de nombreux facteurs. En outre, l'injection d'une erreur localisée peut provoquer de multiples erreurs dans les registres grâce aux chemins divergents ce qui rend difficile la restauration de l'information [KOM99].

2.4.3 La récupération d'informations confidentielles

2.4.3.1 But d'une attaque

Quand un pirate s'attaque à un circuit, son but peut être multiple :

- suspendre le fonctionnement du circuit,

- récupérer des informations contenues dans le circuit.

Pour perturber une transaction il suffit d'interrompre le service (encryptage, transmission), mais l'utilité de ces attaques pour le pirate est limitée. En effet, il est bien plus intéressant de prendre le contrôle de la fonctionnalité en question pour l'utiliser à ses propres fins, comme par exemple

pour récupérer le code d'une carte de crédit, l'identifiant d'un usager sur un réseau de communication etc.

2.4.3.2 Quelques attaques

- **Analyse de la consommation du circuit**

Les dernières techniques d'attaque sur les circuits sécuritaires (en particuliers les crypto-systèmes) mettent en valeur l'information qui peut être extraite d'une étude de la courbe de consommation de courant d'un circuit [KOC99].

En effet les technologies CMOS ne consomment du courant (en dehors des courants de fuites statiques) que lors de la commutation de transistors. La consommation globale d'un circuit est donc fonction du nombre de transistors qui commutent à chaque coup d'horloge. Quand on analyse la consommation d'un circuit cryptographique sur la même opération (mais avec des opérandes différents), on peut éliminer la consommation de l'architecture (par recherche de corrélation) et ne garder que la consommation propre au changement des données. Ainsi on dispose d'une information sur les données traitées dans le circuit.

Si on connaît l'algorithme de cryptage utilisé et les opérandes (le texte à crypter et le résultat) on peut donc reconstituer la clef de cryptage avec un minimum d'itérations. Cette technique est connue sous le nom de « Simple Power Analysis » ou SPA.

Une amélioration substantielle de la SPA a aussi été proposée dans [KOC99]. Cette technique de « Differential Power Analysis » ou DPA permet de s'affranchir de la connaissance du texte à encrypter. En effet si on observe suffisamment d'opérations d'un algorithme crytpographique, on observe une corrélation due au processus de cryptage qui permet de récupérer des informations sur les clefs utilisées. Une analyse statistique permet de mettre en valeur ces informations et de deviner la clef.

- **Autres attaques par canaux cachés**

Comme les concepteurs ont appris à protéger l'architecture de leurs circuits contre les attaques « classiques », les pirates ont appris à exploiter toutes les possibilités pour récupérer de l'information à partir du fonctionnement du circuit. Par exemple, le circuit en fonctionnement

dégage de l'énergie électro-magnétique, consomme du courant, requiert un temps de calcul, et toutes ces informations sont corrélées d'une façon ou d'une autre aux données traitées. Une analyse statistique permet d'éliminer certains facteurs constants ainsi que le bruit et de magnifier l'effet des données sensibles. Comme ces données sont émises de en parallèle du fonctionnement du circuit, il est très difficile de protéger le circuit. L'ajout de signaux aléatoires ou non corrélés aux données peut être une solution, mais en augmentant le nombre d'échantillons il est théoriquement possible de filtrer ce bruit [BIH96B]. Par contre au delà d'un certain point, l'exploitation des données devient trop coûteuse (en temps et/ou en ressources informatiques) pour être réaliste.

- **Attaque du software**

Un pirate peut aussi profiter des failles du programme qui gère le module cryptographique [BON01]. En effet, les programmeurs incluent souvent un mode de test avec un accès étendu aux données internes du circuit, ce qui peut permettre la récupération facile des clefs de cryptage normalement protégées d'un accès externe. Ces modes de test sont souvent protégés par des fusibles grillés dès que la phase de validation est terminée. Un pirate peut court-circuiter les fusibles pour basculer dans ce mode de test et récupérer les données sensibles.

- **Attaque par injection de faute**

Un circuit peut être attaqué en provoquant des erreurs pendant son fonctionnement. Il en résulte une perturbation de l'algorithme qui entre alors dans un mode non prévu par les concepteurs. Si par exemple une attaque arrive à modifier le registre où est stocké le compteur du nombre de cycles d'un algorithme de type DES, il peut faire croire à l'algorithme que l'encryptage des données est terminé à un moment où il est facile de récupérer les données de la clef de cryptage (1ère ou dernière ronde de l'algorithme, selon que l'on a accès au texte en clair ou au texte crypté) [BIH96A]. Le circuit va donc sortir des données qui n'ont pas été correctement encryptées et qui sont très fortement corrélées avec la clef de cryptage.

Un autre type d'attaque a été étudiée théoriquement dans [BON90] et une première application pratique proposée par Biham et Shamir dans [BIH97]. Cette attaque est basée sur un résultat incorrect dans un processus cryptographique. Si une erreur apparaît dans les calculs, on obtient une donnée fausse dont les propriétés de corrélation avec le message initial et la clef de

cryptage sont suffisamment fortes pour nous permettre de retrouver cette dernière. Ces attaques nécessitent la connaissance de l'algorithme cryptographique utilisé et la possibilité d'injecter des fautes dans le module de calcul. Tous les algorithmes ne se sont pas avérés sensibles à ce genre de fautes, mais les algorithmes RSA (Rivest, Shamir and Adleman), DES (Data Encryption Standard) et ECC (Elliptic Curve Cryptography) ont été reconnus sensibles à ces attaques [BIH96A][JOY97].

- **Probing**

Les mémoires sont des composants très sensibles car elles peuvent contenir des informations confidentielles (code software, clés de cryptage, informations bancaires), et leur structure régulière permet l'identification facile des zones contenant des informations sensibles [SAM02]. En effet, une matrice de points mémoire est constituée de lignes et de colonnes qui constituent un point de repère pour le pirate. Plus généralement, tous les éléments séquentiels d'un circuit sont susceptibles de renfermer une information confidentielle persistant au moins pendant un cycle d'horloge. Cette stabilité de l'information en fait une cible privilégiée pour l'observation, même si cette observation est soumise à des contraintes temporelles et spatiales très strictes. Le pirate doit en effet posséder des informations très précises sur la structure et le mode de fonctionnement du circuit pour espérer pouvoir récupérer des informations utiles par la méthode du probing, car les technologies actuelles ont une grande densité à la fois temporelle (augmentation de la fréquence d'horloge), et spatiale (augmentation de la densité de composants au mm^2).

Les techniques modernes de probing n'utilisent plus des pointes pour se connecter au circuit mais des sondes à effet Hall qui permettent, avec une résolution toujours plus élevée, de sonder le rayonnement électromagnétique émanant d'un composant à haute fréquence [AND01].

2.4.3.3 Utilité du laser vert dans la problématique de l'injection de fautes

Le laser vert de longueur d'onde 532 nm est un outil de choix pour réaliser des attaques par injection de fautes car c'est un laser utilisé à la base dans l'industrie pour modifier les pistes électriques des composants électroniques. Ce laser est donc disponible à des prix raisonnables dans le cadre d'une attaque d'envergure.

Comme cette source est monochromatique, il est facile de la focaliser sur une surface d'1 μm^2 [LAP96], et sa longueur d'onde permet de déposer l'énergie dans les premiers micromètres de l'épaisseur du circuit. Il est suffisamment puissant pour traverser les premières couches du circuit et atteindre les zones actives des transistors. En réglant sa puissance on peut provoquer des perturbations électriques dans le circuit sans toutefois le détruire. On peut aussi le faire fonctionner dans un mode ou la longueur d'onde est doublée à 1064 nm, dans l'infrarouge. A cette longueur d'onde le laser traverse le silicium et rend possible les attaques par face arrière qui évitent les couches supérieures protectrices du circuit.

La source laser peut en outre être commandée très précisément à la fois au niveau temporel grâce à sa grande réactivité, et au niveau spatial en utilisant une table motorisée adéquate. L'un intervalle minimum de 1 seconde entre deux tirs successifs du laser est suffisamment court pour que l'on puisse se préoccuper de l'échauffement du circuit.

2.5 Stratégies sécuritaires

Les concepteurs de circuits sécurisés doivent donc certifier que leurs circuits sont capables de résister aux attaques décrites ci-dessus. Bien sûr, on ne protège pas un circuit cryptographique militaire comme on protège une carte à puces car les moyens mis en oeuvre ne sont pas les mêmes, mais les pirates actuels ont accès à un nombre croissant de ressources informatiques, électroniques et techniques. De plus, de nombreuses attaques sont documentées dans le domaine public et accessibles à un pirate persévérant. Les concepteurs ont donc des règles très strictes à respecter quand ils conçoivent un circuit.

2.5.1 Circuits concernés

Dans le cadre de ce travail, nous avons principalement étudié l'architecture et l'utilisation des cartes à puces car ce sont des architectures génériques pouvant comporter de nombreux types de fonctionnalité, en majorité des algorithmes de cryptage. Grâce à ces algorithmes, on peut crypter des communications, authentifier un tiers, sécuriser une transaction bancaire etc.

Le cartes à puces modernes sont constituées en général d'un micro-contrôleur, d'un ou plusieurs modules dédiés aux calculs cryptographiques, et de mémoires. Les entrées/sorties de la carte

sont formatées ISO-7816. Ces cartes sont en outre des objets de grande consommation car on les retrouve dans les téléphones portables, les cartes bancaires, certaines cartes d'identité etc.

2.5.2 Problématique de la conception de circuits sécuritaires

Les fonctions logiques sécuritaires sont généralement conçues autour d'un algorithme provenant du domaine public, avec des technologies standards. Ces caractéristiques servent à réduire les coûts de conception du circuit (par diminution du temps de conception), à optimiser les performances (en utilisant un algorithme déjà optimisé) et enfin à diminuer les coûts de production (en utilisant des technologies standards), le tout dans une optique de production de masse. En effet, là où dans le passé les circuits sécuritaires étaient ciblés pour les applications militaires et bénéficiaient de technologies ad hoc et où les algorithmes n'étaient pas dans le domaine public, on assiste à une démocratisation de ces applications à l'heure où un nombre croissant de personnes dans le monde utilise l'authentification numérique sous toutes ses formes (signature e-mail, cartes bancaires, réseaux non câblés etc.).

Ces propriétés nouvelles des applications sécuritaires font ressortir une question cruciale : comment protéger une application dont les caractéristiques principales sont à disposition des pirates et dont les coûts doivent être les plus bas possibles ?

2.5.3 Méthodologies utilisées pour sécuriser un circuit

Sécuriser un circuit revient à diminuer son observabilité et sa contrôlabilité par un tiers non autorisé. On peut sécuriser le circuit en agissant à plusieurs niveaux de sa conception : dans la conception des algorithmes utilisés par le circuit, dans l'implantation physique de ces algorithmes, et enfin dans la conception du logiciel d'exploitation.

2.5.3.1 Réponse hardware (technologique)

Au niveau technologique, les réponses possibles concernent la manière dont est agencé le circuit pendant sa fabrication. On peut utiliser des couches de métal recouvrant le circuit pour faire bouclier contre le probing, utiliser des cellules logiques résistantes à l'injection de fautes, implanter des détecteurs de variation de tension, de fréquence d'horloge ou encore disperser au

maximum l'implantation des fonctions logiques sur la surface du silicium pour reduire toute corrélation entre la géographie et l'architecture du circuit.

Malheureusement, ces techniques ont des coûts importants en surface et en temps de conception (cellules full-custom). En outre, en tant que modules analogiques (détecteurs de courant, détecteurs de lumière, circuits de brouillage), ils sont très dépendants de la technologie utilisée et doivent être conçus à nouveau pour chaque nouveau type de circuit. Les concepteurs de circuits sécuritaires utilisant de plus en plus des flots de conception standardisés, ces structures leur imposent des contraintes difficiles à gérer. De plus, s'agissant de composants physiques, un pirate bien informé peut les mettre hors d'usage avant de s'attaquer au circuit.

2.5.3.2 Réponse architecturale

La problématique architecturale comprend la conception de l'algorithme utilisé dans le circuit (choix de l'algorithme de cryptage), son implantation physique (choix du module de calcul), le choix de l'architecture du circuit (synchrone ou non, à base de processeur générique ou de logique câblée) et enfin la définition des protocoles d'échange de données.

La conception sécuritaire devra proposer des solutions différentes selon que les blocs fonctionnels traitent les données sensibles (blocs de calculs) où qu'ils assurent simplement le routage des données (interfaces de communication, microprocesseur). Par exemple, un bloc d'exponentiation (communément utilisé dans les algorithmes de cryptage à clefs asymétriques) aura un accès direct aux clefs de cryptage et devra donc être totalement coupé du monde extérieur en plus d'être protégé contre des erreurs éventuelles (la détection d'une erreur entraînant le reset du bloc). D'autre part, un microprocesseur devra être en mesure de dialoguer avec l'extérieur (pour gérer les flux de données et les instructions) et de lancer les algorithmes de cryptage, mais ne doit pas donner accès aux clefs secrètes ou aux résultats intermédiaires. Pour le protéger, le concepteur devra s'assurer que le fonctionnement normal ne comprend pas de mode d'accès étendu, et qu'une perturbation du fonctionnement de ce processeur ne peut pas provoquer de fuite de données confidentielles.

En fait, la conception d'une architecture sécuritaire doit se faire par bloc, en respectant des spécifications strictes, hiérarchisées selon les informations que le bloc fonctionnel manipule. En effet, s'il existe une barrière physique entre la zone où les clefs sont stockées (et manipulées) et

les zones ayant accès à l'extérieur, l'architecture peut être considérée comme sécurisée. Si de plus un mécanisme de détection d'erreur est implanté pour contrer les attaques par injection de faute, le circuit est fonctionnellement sûr.

Malheureusement, le circuit reste sensible aux attaques par canaux cachés [CLA00] qui exploitent la corrélation entre les clefs utilisées et les données disponibles en sortie du circuit pour récupérer ces clefs. Il utilisent pour ce faire toute la gamme des émissions du circuit (consommation de courant, radiations électromagnétiques, temps de calcul) combinées à des analyses statistiques pour magnifier l'apparition des clefs dans le bruit récolté. Même si les concepteurs cryptent les données confidentielles à l'intérieur du circuit en les combinant avec des données inutiles, l'analyse statistique permet de mettre en évidence cette part de bruit comme ne faisant pas partie du flot de données et permet donc de l'éliminer. L'insertion de bruit dans le processus de calcul rend au final la récupération de données confidentielles plus difficile mais pas impossible, et un choix doit être fait entre la robustesse de l'architecture et le coût de ces contre mesures, à la fois en temps de conception et en temps de calcul.

2.5.3.3 Réponse logicielle

La couche logicielle d'un circuit sécuritaire fait aussi l'objet d'une réflexion pour le rendre plus sûr. Les principales failles de cette couche proviennent en général d'un accès possible aux données non encryptées par le biais d'un mode de test du logiciel ou grâce à des failles dans le protocole de transmission des données [BON01].

Comme les techniques actuelles d'injection de fautes permettent d'affecter un registre précis d'un circuit, il est nécessaire de protéger les parties critiques d'un algorithme logiciel. Cela peut être réalisé en utilisant par exemple la redondance de code, ou des codes correcteurs pour assurer que les données circulant dans le circuit n'ont pas été affectées.

Ce type de contre mesures a été la première réponse des concepteurs aux attaques sur les circuits sécuritaires, et des contraintes très fortes sont appliquées sur les logiciels destinés à de tels circuits. Par contre, ces logiciels ne peuvent efficacement diagnostiquer les perturbations subies par leur substrat physique, ce qui oblige à durcir les circuits contre les attaques au niveau du composant.

2.6 Protéger les circuits intégrés face aux erreurs transitoires

Dans le cadre des études portant sur les erreurs transitoires générées par des particules comme les neutrons, des méthodologies et des outils ont été développés pour détecter ces erreurs et les corriger. Cette section va présenter différents modes de protection à la disposition des concepteurs. Ces techniques sont adaptées à la protection des circuits contre des perturbations très courtes (~ 100 ps) et apparaissant avec parcimonie dans le circuit.

2.6.1 Redondance temporelle

La redondance temporelle est un concept dans lequel les informations sont stockées et traitées plusieurs fois d'affilée. On retrouve ce type de protection dans certains processeurs pouvant être programmés pour traiter les informations plusieurs fois et comparer leurs résultats, ceci sans modification architecturale.

Cette méthode a un coût quasiment nul en surface, mais elle ralentit énormément les calculs, d'un facteur proche de 2. Elle est préconisée dans les applications où la surface de silicium prime sur la vitesse de calcul ou la consommation.

L'outil L-RoCKIT d'iRoC Technologies propose une implantation automatisée d'une technique de redondance temporelle adaptée aux erreurs transitoires. Cette technique propose d'utiliser le front descendant de l'horloge pour détecter les erreurs transitoires, mais la longueur des impulsions ne doit alors pas dépasser la moitié de la période d'horloge sous peine de ne pas être détectée.

2.6.2 Redondance spatiale (matérielle)

Les techniques de redondance spatiale se basent sur plusieurs modules de calcul effectuant simultanément le même calcul sur les mêmes données. On retrouve cette technique dans les systèmes incluant des modules spécifiques devant effectuer un traitement complexe des données en un temps très court.

Cette technique est donc gourmande en surface de silicium et en consommation car les modules de calculs sont dupliqués (voire plus) et fonctionnent en parallèle. Par contre la vitesse de traitement des informations n'est que peu affectée dans une architecture de ce type.

2.6.3 Redondance d'information

La redondance d'information consiste à augmenter la cohérence des données grâce à un codage judicieux des états du circuit. C'est une technique largement utilisée (souvent en combinaison avec les deux précédentes) car elle englobe les codes détecteurs et correcteurs d'erreurs (code de parité, code de Hamming…). Ces codes correcteurs sont en effet utilisés dans la majorité des applications nécessitant une certaine intégrité de l'information comme les systèmes de communication. La mise en œuvre d'un code correcteur peut être très simple (code de parité) avec une faible surface supplémentaire, ou très complexe (codage Reed-Solomon). Dans beaucoup de cas cependant, ces codes sont développés pour une architecture précise et peuvent être relativement inefficaces dans un autre environnement.

Ces codes ont une capacité fixe de traitement des erreurs et peuvent être mis en défaut dès que ce seuil est dépassé. Leur consommation et leur coût en surface et en temps de calcul sont fonction de leur complexité.

On voit dans la figure 19 un type d'architecture exploitant la redondance d'information à l'aide d'un code de parité.

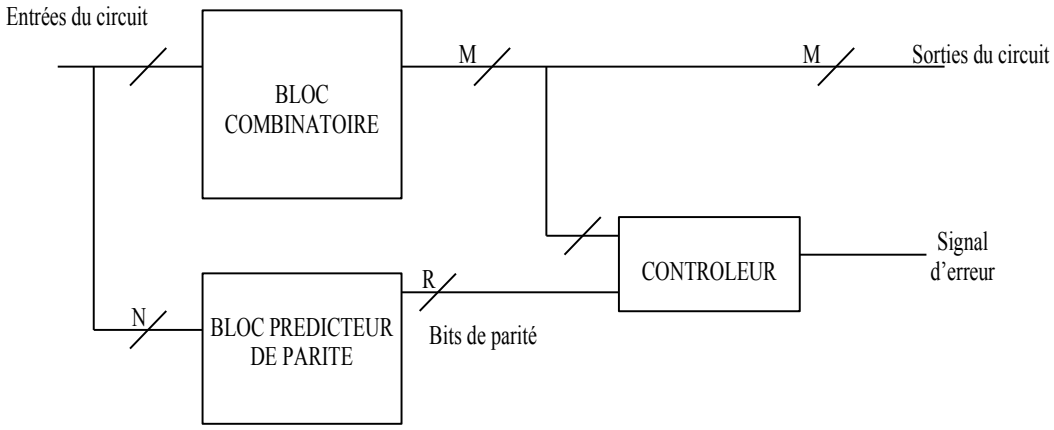


Figure 19: Architecture protégeant un circuit à l'aide de la redondance d'information.

L'outil L-RoCKIT d'iRoC Technologies permet de protéger un circuit intégré contre les erreurs transitoires selon cette méthode. La contrainte principale étant qu'une erreur ne doit pas affecter à la fois le bloc combinatoire et le bloc prédicteur de parité.

Cette protection est efficace contre les erreurs longues de la source laser. Cependant cette dernière peut provoquer des erreurs multiples sur une grande surface du circuit, en nombre suffisant pour que le bloc détecteur d'erreur soit saturé. Il y a alors conflit entre le besoin du pirate de contourner le dispositif de protection et l'injection d'un trop grand nombre d'erreurs qui gêne l'observation des données.

Pour craquer ce type de protection les erreurs injectées doivent provoquer des codes de contrôle identiques dans le bloc combinatoire et le bloc prédicteur de parité pour leurrer le controleur, cf. figure 19.

L'outil M-RoCKIT d'iRoC Technologies permet de protéger les mémoires contre les SEU dans les mémoires à l'aide d'un code correcteur d'erreurs, le code de Hamming. La mémoire ainsi protégée peut corriger une unique erreur sur chaque groupe de mot, ou détecter 2 erreurs sans pouvoir les corriger. La source laser pouvant provoquer des erreurs sur l'ensemble d'une mémoire cette méthode de protection n'est pas toujours suffisante.

2.7 Conclusion

On a pu voir dans ce chapitre que les pirates ont accès à un nombre impressionnant de techniques pour récupérer des informations confidentielles dans un circuit moderne. Les contre mesures développées par les concepteurs sont toujours sujettes à des failles par rapport aux attaques par canaux cachés qui exploitent la seule cohérence des données du système sécurisé et les attaques par injection de fautes pourront toujours théoriquement saturer un système de correction. Il est donc impossible de protéger à 100% un circuit à la disposition d'un pirate possédant de moyens et de temps illimités, la seule réponse possible des concepteurs étant d'augmenter au maximum le coût d'une attaque pour le pirate.

C'est dans ce cadre que les techniques habituellement utilisées dans la protection des circuits face aux erreurs transitoires rentrent en jeu. Cependant le coût non négligeable et la difficulté d'implantation réduisent leur utilisation à quelques modules seulement dans un circuit. j'ai

utilisé durant ces travaux les outils développés par iRoC Technologies pour me familiariser avec ces techniques de protection et évaluer leur efficacité. Il apparaît que ces outils conçus pour protéger les circuits contre les erreurs transitoires provoquées par rayonnement ne sont pas adaptés aux spécificités de la source laser verte. Il convient donc de proposer d'autres méthodes de protection.

Quand les investissements nécessaires pour attaquer avec succès un circuit dépassent les bénéfices obtenus, il est évident que très peu de personnes s'intéressent à cette problématique. Le fait est qu'actuellement une personne disposant de connaissances techniques raisonnables et d'un outillage disponible dans le domaine public peut mettre en oeuvre des attaques efficaces comme la DPA et certaines techniques par injection de fautes, tout en restant discret et en récoltant beaucoup d'argent. Le choix d'une source laser verte à 532 nm a été présenté pour représenter un outil d'injection de fautes puissant potentiellement à la disposition d'un attaquant potentiel. J'utilise d'ailleurs un dispositif basé sur cette source dans la suite de ce travail.

Pour contrer les attaques par injection de fautes, il faut donc étudier l'impact des sources sur le silicium. Pour ce faire, j'ai proposé une métrique (la durée des impulsions), et dois maintenant mettre au point un instrument de mesure adapté à notre problématique. C'est ce qui va être développé dans le chapitre 3.

Chapitre 3 : Techniques de quantification du bruit d'origine radiative

3.1 Introduction

Après avoir modélisé les perturbations dans les circuits intégrés, il faut pouvoir les caractériser pour étudier leur impact dans les circuits intégrés modernes. Notre objectif est ici d'étudier la sensibilité d'une technologie donnée face aux attaques laser d'une part, et plus généralement face aux perturbations d'origine radiative.

Pour ce faire je mets en place une méthodologie de conception d'un circuit de mesure adapté aux spécificités de la source laser, puis je propose une autre architecture destinée à caractériser une technologie face à des sources moins souples que le laser.

La première architecture a été réalisée et est confrontée à des attaques laser (dont les résultats sont disponibles dans le chapitre 4), alors que la deuxième n'est pas encore été testée. C'est pourquoi nous nous attachons à étudier les performances de cette dernière architecture grâce aux outils de simulation à notre disposition.

3.2 Vers un circuit de qualification d'une bibliothèque de cellules standards face aux attaques laser

3.2.1 Contexte

Dans le cadre du projet Duracell, les premières discussions ont porté sur la proposition d'un modèle approprié pour représenter l'effet d'une injection de fautes par laser dans un circuit intégré. Nous avons donc décidé de rechercher un moyen de quantifier ces effets à l'aide d'un circuit de cellules standards en technologie HCMOS9GP 0.13 µm STM. Le circuit devait être capable de mesurer les impulsions transitoires générées dans plusieurs types de cellules de cette technologie. De plus, une étude devait être faite sur la génération d'impulsions simultanées dans plusieurs cellules.

3.2.2 Contraintes

Après analyse des spécifications, plusieurs contraintes fortes sont apparues, particulièrement au niveau de l'architecture du circuit, mais aussi autour des coûts de la réalisation du circuit et de la méthodologie à appliquer.

3.2.2.1 Timing

Dans le cadre d'impulsions générées par un tir laser, les paramètres de longueur à mesurer se sont montrés problématiques. En effet, l'impulsion laser que nous utilisons dure entre 500 ps et 10 ns ce qui, pour une mesure précise comprenant au minimum une dizaine de points, nous donne une période d'échantillonnage de 50 ps. Le temps de transition d'un inverseur étant donné par l'équation 4 :

$$T_{pr} = -0.01 + 0.236 * T_{tr-1} + 2.047 * C \qquad \text{(Eq. 4)}$$

avec la charge C d'un inverseur (quelques pF) et un temps de transition $T_{tr\text{-}1}$ du signal de 100 ps, on obtient T_{pr} = 23,6 ps.

Ces calculs s'appliquent au cas idéal où les connexions entre les cellules sont parfaites et ne chargent pas la cellule étudiée. Si on rajoute la connexion la plus directe, on arrive à des temps de propagation de l'ordre de 50 ps.

De plus dans le cas d'un circuit synchrone, les arbres d'horloge doivent être capables de propager le signal sur toutes les bascules du circuit en un temps très bref par rapport à la période d'horloge.

3.2.2.2 Coûts

Les consignes pour réaliser ce circuit étaient claires : minimiser le coût externe de conception. Comme l'entreprise ne possède pas des outils nécessaires au back-end (phase physique de la conception), cette opération devait être confiée à un contractant externe.

D'autre part, les caractéristiques du circuit (équilibrage des temps de propagation entre les différents éléments) nous ont montré que les techniques habituelles de placement et de routage

(à l'aide d'outils automatisés) sont inadaptées à notre projet. Nous avons donc du prévoir des moyens de réduire les coûts de back-end en modifiant le flot de conception pour l'adapter aux spécificités du circuit.

3.2.2.3 Performance

Comme le circuit fonctionne aux limites des capacités de la technologie, les temps de propagation entre les cellules doivent être minimisés ou tout du moins équilibrés pour ne pas induire d'erreur dans le calcul de la durée de l'impulsion. Un placement automatique des cellules ne garantira que difficilement des chemins équilibrés, et les contraintes de délais de propagation draconiennes rendront cette phase très longue.

3.2.3 Solutions

Pour répondre aux contraintes posées par la conception du circuit, nous avons du élaborer des solutions spécifiques qui s'écartent du flot de conception habituel des circuits synchrones. Cette section décrit les techniques utilisées.

3.2.3.1 Cellules standards

Pour pouvoir réduire les coûts de conception du circuit (temps de conception et outils nécessaires) et pour des raisons de disponibilité nous avons choisi d'utiliser des cellules standards. Ces cellules ont l'avantage d'être conçues de manière uniformes, c'est-à-dire qu'elles ont toutes la même hauteur pour pouvoir être placées dans des rails d'alimentation communs. Elles épargnent de plus au concepteur d'avoir à construire ses propres éléments électriques, mais imposent un mode non analogique (travail avec les niveaux logiques 0 et 1).

Les bibliothèques disponibles sont en outre très bien documentées et contiennent tous les éléments nécessaires à la simulation du circuit comme des informations de délais, de consommation etc.

3.2.3.2 Élaboration d'un flot de conception dédié

Pour mesurer un signal analogique comme les impulsion transitoires dans un circuit, nous avons pensé à réaliser un échantillonneur à l'aide de bascules placées régulièrement sur une ligne où se propage l'impulsion à mesurer. L'objectif de cette structure est dedéclencher simultanément toutes les bascules de la ligne pour capturer une image de l'état électrique de l'ensemble de la ligne. Comme nous devons déclencher les bascules via le signal d'horloge, ce signal doit être propagé à toutes les bascules de la ligne avec le moins de délai.

De plus, nous cherchons à mesurer des impulsions de très courte durée et les contraintes de conception vont nécessairement être très fortes. Par exemple si nous cherchons à échantillonner un signal, le décalage (désynchronisation) des signaux entre les différentes bascules d'échantillonnage (cf. figure 20) va introduire des erreurs dans la mesure. Pour information, les outils actuels de placement et routage automatiques permettent d'atteindre à grand peine une précision de l'ordre de la centaine de picosecondes dans la gestion des désynchronisation d'horloge.

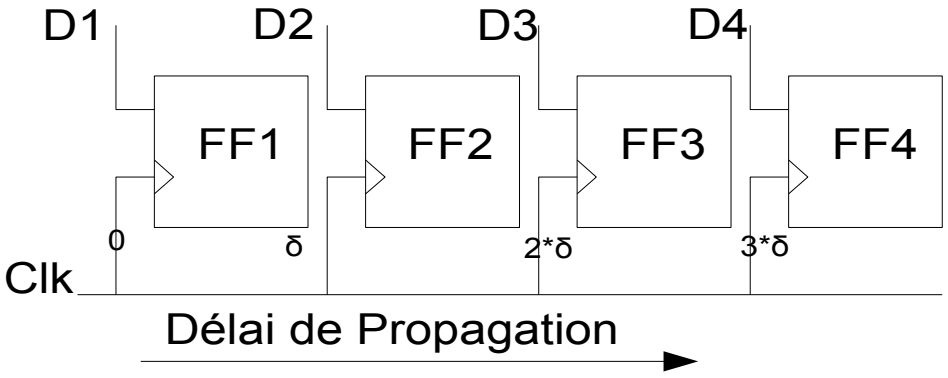


*Figure 20: Exemple de désynchronisation pour le signal Clk : FF4 recevra le signal d'horloge avec un retard mesurable (3*δ) par rapport à FF1 dû au temps de propagation sur l'arbre d'horloge.*

Le moyen que nous avons trouvé pour contourner ce problème est de recourir à une structure en H équilibrée pour router nos signaux. Dans la figure 21, on voit que le chemin de propagation des signaux D et Clk sont les mêmes pour chaque bascule. On peut en conclure qu'en plaçant judicieusement les cellules, les chemins les plus directs de routage entre les connecteurs seront aussi les chemins les plus équilibrés. On gagne ainsi en performance du circuit, tout en réalisant

un gain de temps sur les contraintes à imposer à l'outil de routage automatique. De plus, le temps de calcul de la phase de routage automatique en sera très nettement diminué.

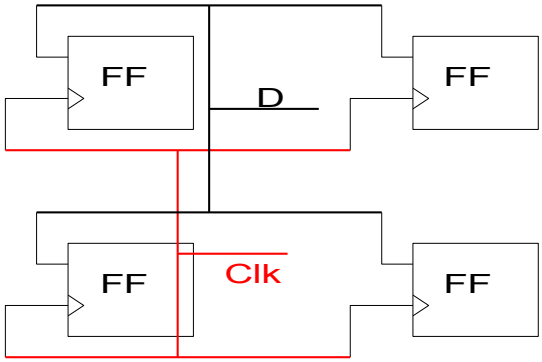


Figure 21: Structure en H visant à équilibrer les chemins de propagation.

Dans ce projet nous allons utiliser cette méthode de routage des signaux pour éliminer au maximum les désynchronisations dues à la propagation des signaux.

3.3 Conception du circuit PROBES Laser

Le projet de circuit PROBES Laser vise à concevoir un circuit capable de détecter et de mesurer la durée d'impulsions générées dans des cellules logiques par un tir laser. Le circuit se compose donc d'une partie « cible » qui contient les cellules allant être illuminées par le laser, et d'une partie « capture » qui contient le détecteur d'impulsion et l'outil de mesure de durée. Dans cette section nous allons décrire la phase de conception de ce circuit.

3.3.1 Spécifications

3.3.1.1 Contraintes génériques

Les contraintes du circuit PROBES face aux attaques laser sont assez minimes car d'une part, seules les surfaces sensibles sont touchées grâce à l'étroitesse du faisceau, et d'autre part les impulsions peuvent être contrôlées pour apparaître au moment désié. Nous n'avons donc pas à protéger la partie de capture des impulsions contre le bruit radiatif (SET ou SEU) et le fonctionnement du circuit peut donc être contrôlé de l'extérieur.

3.3.1.2 Échantillonneur

L'échantillonneur (figure 22) est conçu pour capturer et mesurer des impulsions d'une longueur de quelques nanosecondes. Ce module est totalement autonome pendant la phase de détection et de capture des données, car les informations de synchronisation sont difficiles à échanger entre le circuit et son environnement dans des intervalles de temps réduits. Les bases de fonctionnement de cet échantillonneur sont tirées de [NIC03].

Le fonctionnement de l'échantillonneur est le suivant :

- un tir laser crée des impulsions dans des cellules logiques reliées à l'entrée de l'échantillonneur,
- des impulsions arrivent dans la chaîne d'inverseurs de l'échantillonneur et se propagent,
- un détecteur d'impulsion active l'horloge des bascules pour capturer le front d'onde de la chaîne d'inverseurs,
- une fois le front d'onde capturé, un système de « scan » extrait les informations des bascules et l'échantillonneur est prêt pour un nouveau tir laser.

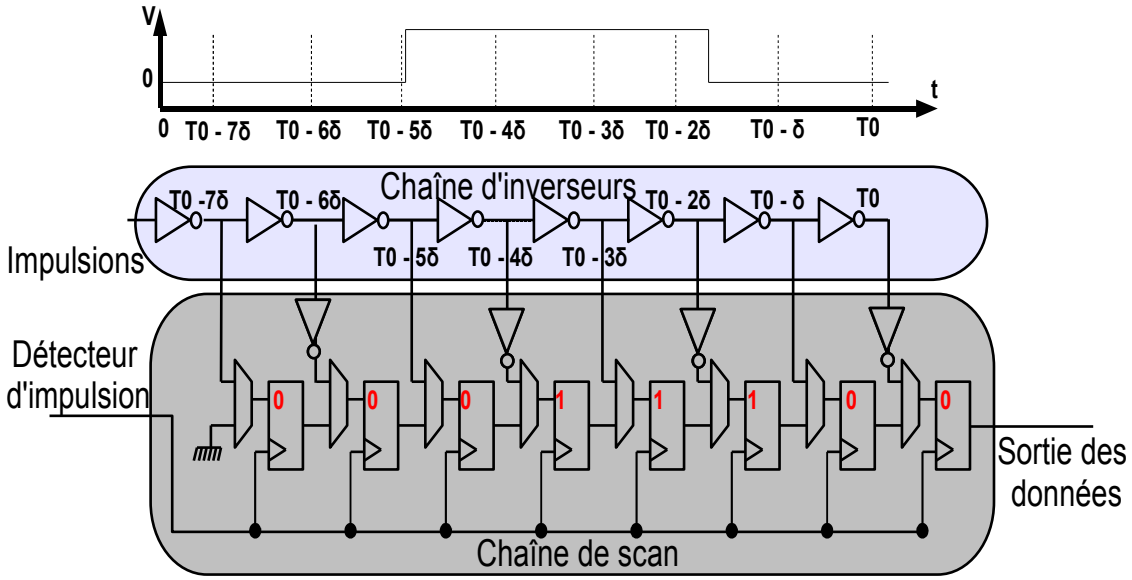


Figure 22: Schéma de l'échantillonneur du circuit PROBES.

Dans la figure 22, on voit une impulsion se propager dans la chaîne d'inverseurs de l'échantillonneur. Cette impulsion se propage à travers chaque inverseur avec un délai de propagation δ. Quand le front montant de l'impulsion arrive au point de détection de la chaîne (instant T0), le système de détection déclenche simultanément toutes les bascules de l'échantillonneur, bascules qui vont capturer l'état de la ligne de propagation en sortie de chaque inverseur. On observe donc dans chaque bascule l'état de la ligne à différents instants de la propagation, ce qui permet de reconstituer de manière discrète l'évolution temporelle de la ligne de propagation avec une base de temps correspondant au temps de propagation d'un inverseur.

En sortie de l'échantillonneur on obtient donc une représentation numérique de la forme d'onde de l'impulsion créée par la perturbation dans les surfaces sensibles.

3.3.1.3 Conception des surfaces sensibles

Les surfaces sensibles (le pas de tir) doivent être conçues de sorte à donner de bonnes indications de la sensibilité des portes combinatoires de la librairie de cellules standards HCMOS9 0.13 µm STM. On se contentera des cellules les plus utilisées pour ensuite faire une extrapolation vers les autres cellules. En outre, les différentes tailles de cellules devront aussi être étudiées.

Pour pouvoir étudier la sensibilité de chaque cellule indépendamment, nous avons décidé de former des cibles composées uniquement d'un seul type de cellule liées entre elles pour former une chaîne propageant le signal électrique (figure 23). Ces groupes de cellules sont décrites après comme les surfaces sensibles du circuit.

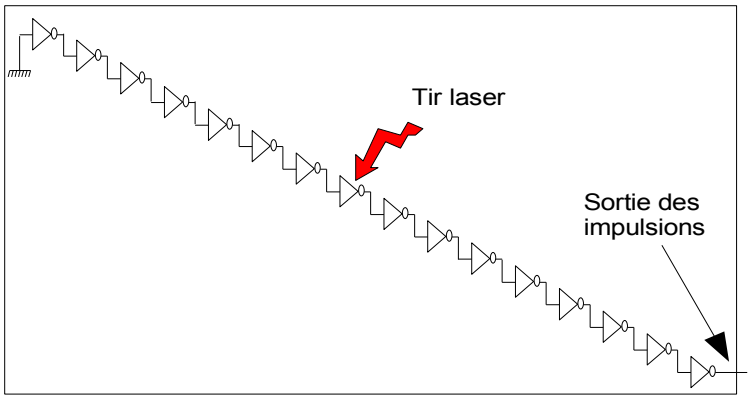


Figure 23: Schéma d'implémentation d'une surface sensible composée de cellules IVLL basée sur le motif D16.

La figure 24 résume le contenu des surfaces sensibles décrites dans la table 2.

Table 2: Récapitulatif du contenu des surfaces sensibles du circuit PROBES

Référence	***Nom***	***Type de cellule***	***Sortance***	***motif***	***Formule logique***
0	DC	N/A	N/A	N/A	Z = A
1	IVLL	Inverseur basse consommation	1	D64	Z = -A
2	IVLL		1	C64	
3	IVHS	Inverseur haute vitesse	1	D16	Z = -A
4	IVHS		1	D64	
5	IVHS		1	C64	
6	IVLLP	Inverseur basse consommation	2	D16	Z = -A
7	IVLLP		2	D64	
8	IVLLP		2	C64	
9	BFLL	Amplificateur basse consommation	1	D16	Z = A
10	BFLLP		2	D16	
11	ND2LL	NAND 2 entrées basse consommation	1	D16	Z = -(A.B)
12	ND2LLP		2	D16	
13	NR2LL	NOR 2 entrées basse consommation	1	D16	Z = -(A+B)
14	NR2LLP		2	D16	
15	AN2LL	AND 2 entrées basse consommation	1	D16	Z = A.B
16	OR2LL	OR 2 entrées basse consommation	1	D16	Z = A+B
17	IVLLX4	Inverseur basse consommation	4	D16	Z = -A
18	BFLLX4	Amplificateur basse consommation	4	D16	Z = A
19	EOLL	EXOR 2 entrées basse consommation	1	D16	Z = A XOR B
20	EOLLP		2	D16	
21	AO6LL	Porte composée basse consommation	1	D16	Z = -(A.B + C)
22	AO6LLP		2	D16	
23	AO7LL	Porte composée basse consommation	1	D16	Z = -((A+B).C)

Référence	***Nom***	***Type de cellule***	***Sortance***	***motif***	***Formule logique***
24	MUX21LL	Multiplexeur 2 entrées basse consommation	1	D16	Z = A.(-S) + B.S
25	MUX21LLP		2	D16	
26	ND3LL	NAND 3 entrées basse consommation	1	D16	Z = -(A.B.C)
27	ND3LLP		2	D16	
28	NR3LL	NOR 3 entrées basse consommation	1	D16	Z = -(A+B+C)
29	NR3LLP		2	D16	
30	IVHSP	Inverseur haute vitesse	2	D64	Z = -A
31	IVLL	Inverseur basse consommation	1	D16	Z = -A

Le choix des types de cellule à tester a été fait d'après la structure interne des cellules. Par exemple, l'inverseur permet d'étudier la structure de base à deux transistors, tandis que les portes NAND apportent des structures à 4 transistors (figure 25). On étudie ainsi l'ensemble des structures de portes de la bibliothèque HCMOS9 avec les EXOR, les MUX et autres portes complexes définies dans la table 2.

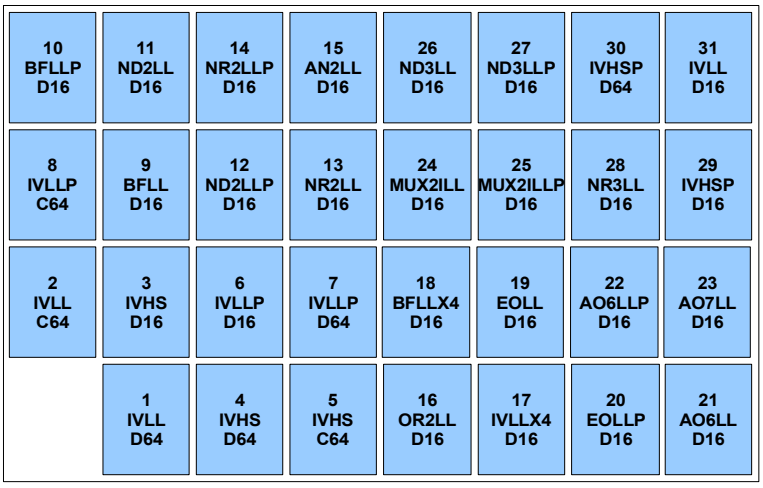
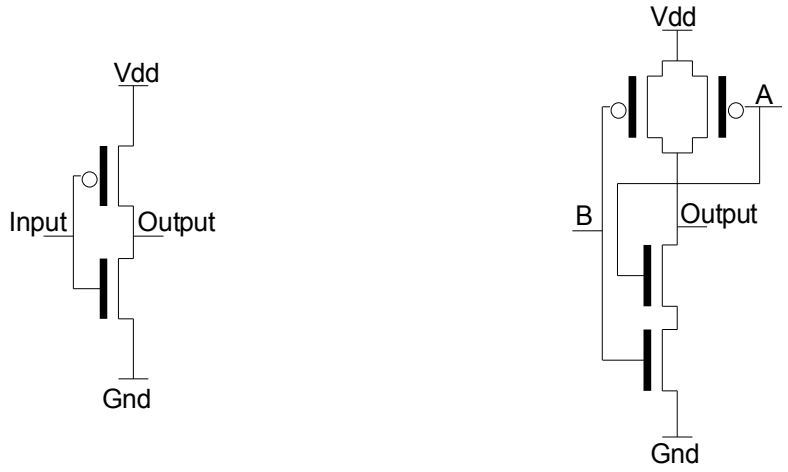


Figure 24: Contenu des différentes surfaces de tir du circuit PROBES Duracell.



(a) : Implémentation d'un inverseur à 2 transistors *(b) : Implémentation d'un NAND à 4 transistors*

Figure 25: Exemple d'implémentation de portes logiques en technologie CMOS.

L'organisation des cellules dans les surfaces sensibles a été choisie pour mettre en évidence les phénomènes de recombinaison d'impulsion et pour profiter de la taille variable du faisceau laser. Nous avons implémenté 3 types de motifs, le motif D16 (figure 23), le motif D64 (figure 26) et enfin le motif C64 (figure 27).

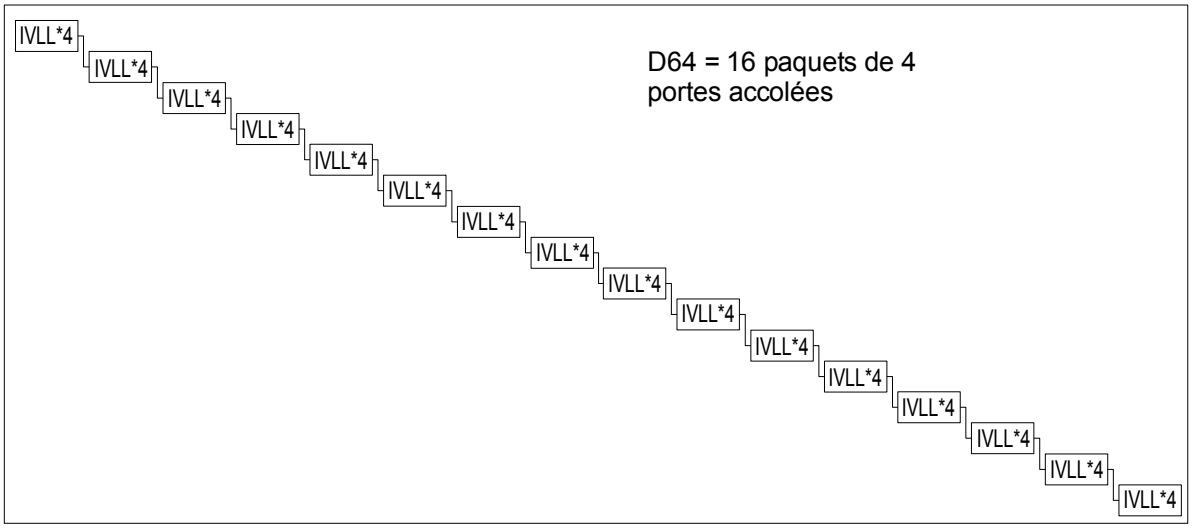


Figure 26: Exemple d'une surface sensible implémentée selon le motif D64.

Ces surfaces sensibles sont chacune inscrites dans un carré de 80 µm de côté.

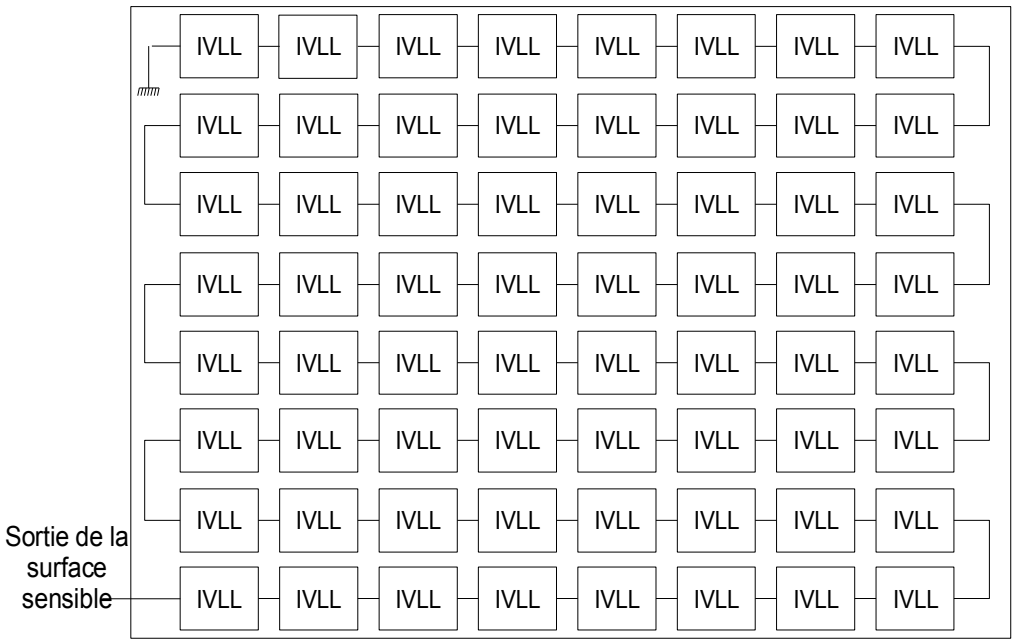


Figure 27: Exemple d'une surface sensible implémentée selon le motif C64.

3.3.2 Choix du flot de conception

3.3.2.1 Abandon de la spécification comportementale

Le flot de conception classique utilisé dans la conception de circuits complexes repose sur la description comportementale des différents modules du circuit (figure 28), puis sur la transformation de ces informations en un fichier décrivant la liste des cellules et leurs interconnexions (netlist). Cette approche est efficace pour la description de circuits comportant des fonctions complexes pouvant être décrites sans faire référence à la technologie silicium utilisée, comme par exemple un processeur ou un registre à décalage.

Dans le cadre du circuit PROBES, la technologie utilisée est primordiale dans le choix des portes logiques qui serviront à créer le circuit, ce qui rend la phase de compilation très délicate pour les outils habituels. En effet, une architecture massivement redondante comme celle du circuit PROBES ne sera pas considérée par le compilateur comme optimale ce qui entraînera des erreurs d'implantation auxquelles il sera difficile de remédier.

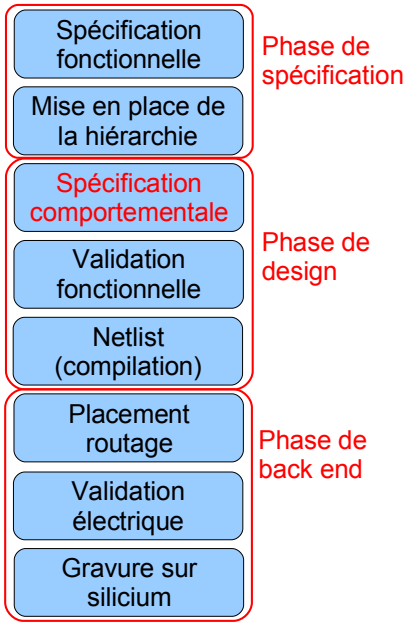


Figure 28: Flot de conception classique envisagé pour le circuit PROBES.

La solution que nous avons utilisé est de décrire le circuit au niveau portes dès le début du flot de conception. Nous nous assurons ainsi que l'implantation des portes logiques est bien conforme aux spécifications, à la fois en ce qui concerne les interconnexions entre portes et le placement des portes. Ce procédé permet de décrire des modules contenant au plus une centaine de portes, et comme notre circuit est très redondant nous pouvons écrire le module une fois puis l'instancier un grand nombre de fois.

Cette méthodologie est donc adaptée aux spécificités de notre circuit, sous réserve de respecter certaines contraintes de taille maximale pour les modules hiérarchiques.

3.3.2.2 Abandon des techniques de placement automatique

Une autre contrainte majeure dans la conception du circuit PROBES est la fugacité des événements à détecter et la précision désirée dans la mesure de leur durée. En effet, les impulsions transitoires générées par un tir laser sur une porte logiques sont de l'ordre de la nanoseconde et la précision désirée est de l'ordre de 50 picosecondes.

Pour obtenir par des méthodes classiques une telle précision, il faut des contraintes très fortes concernant les délais de propagation dans les parties critiques du circuit, à savoir les zones de tir et le module de capture. On ne parle pas seulement ici de réduire les délais de propagation au minimum, mais aussi d'équilibrer ces délais pour qu'ils puissent être pris en compte comme des constantes dans les équations des temps de propagation. De cette manière, il est facile de les éliminer de manière statistique. Le problème est que les outils de placement automatique ne peuvent garantir de telles propriétés.

Comme nous avons décidé de construire le circuit directement au niveau portes, nous pouvons en profiter pour placer chaque porte en même temps que nous les connectons. Cette décision nous permet de maîtriser facilement les temps de propagation des parties critiques du circuit tout en relâchant complètement les contraintes sur les modules de contrôle. En particulier, le module échantillonneur fera l'objet de toute notre attention en vue d'équilibrer et minimiser au maximum les délais de propagation pour avoir une précision maximale sur nos mesures. Pour obtenir des délais de propagation les plus faibles possibles nous avons donc rapproché au maximum les portes interconnectées.

Notre design étant très redondant, nous laisserons le soin à un script automatique de transformer les informations de placement relatives en coordonnées XY absolues. Cela nous permet de construire le placement du circuit de manière hiérarchique et donc de réaliser cette tache parallèlement à l'implantation de la netlist. Les scripts serviront à éliminer la hiérarchie pour obtenir le placement final du circuit à plat.

3.3.3 Validation

Une fois la netlist et les informations de placement générées, nous entrons dans la phase de validation du design. Durant cette phase nous allons vérifier que le design est conforme aux spécifications. Cette phase comporte deux étapes, la validation fonctionnelle pendant laquelle nous vérifions le comportement au niveau logique (par les tables de vérité) et la validation électrique pendant laquelle nous vérifions l'intégrité électrique des signaux générés dans le circuit.

3.3.3.1 Validation fonctionnelle

La validation fonctionnelle consiste pour le circuit PROBES à vérifier que l'initialisation du circuit est conforme aux spécifications (par exemple, que la phase de reset fait entrer le circuit dans l'état sensible). Cette étape permet aussi de valider le mode opératoire de test du circuit. Nous utilisons un simulateur fonctionnel classique pour cette étape. Il est préférable de commencer par valider les modules du niveau hiérarchique le plus bas au fur et à mesure de leur implantation pour détecter le plus en amont possible d'éventuelles erreurs de conception.

Cette phase de validation s'achève par la simulation de la version finale du design (ou d'une sous partie représentative) et par la vérification de sa conformité aux spécifications fonctionnelles.

3.3.3.2 Validation électrique

La validation électrique consiste à simuler le comportement électrique du circuit. Cette validation demande des informations très précises sur la topographie du circuit pour avoir un maximum de précision et ne peut se faire qu'après la phase de placement routage. De plus la complexité des algorithmes de calcul fait que cette simulation est extrêmement lourde à mettre en place sur un circuit complet.

On se contentera donc de simuler certaines parties critiques comportant quelques dizaine de portes au maximum. Ces simulations permettent de valider les comportements transitoires du circuit, par exemple au moment de la capture du SET. On arrivera donc à corréler les résultats expérimentaux et les données issues de la simulation pour modéliser efficacement le phénomène étudié.

3.3.4 Méthodologie de back end

Le back end (implantation physique) d'un circuit consiste à passer de la netlist d'un circuit au dessin des masques qui seront utilisés pour concevoir le circuit en fonderie. Cette phase comprend également la validation des règles de conception du circuit au niveau électrique, comme l'intégrité des signaux électriques.

La phase de back end se compose de plusieurs étapes :

1. Placement,
2. Routage,
3. Dessin des masques,
4. Validation (Layout versus Schematics LVS),
5. Vérification des règles de design (Design Rule Checking DRC),
6. Extraction d'une netlist Spice (niveau transistor) à partir des masques pour la validation électrique.

3.3.4.1 Minimisation des coûts de back end

Notre méthode de description du circuit au niveau portes nous permet d'agir sur les deux premières phases du flot de back end. En effet, les portes ont été placées lors de leur implantation dans le circuit ce qui élimine les problèmes liés au placement automatique. De plus, les portes ont été conçues et placées de telle sorte que le routage se fasse en ligne droite, en minimisant les changements de couche sur le chemin de propagation (vias).

Nous éliminons donc des étapes les plus gourmandes en temps de calcul et en expertise pour passer directement à la conception des masques.

3.3.4.2 Maximisation des performances

- **Désynchronisation d'horloge**

L'équilibrage des temps de propagation des bascules connectées à l'arbre d'horloge est primordial dans le circuit PROBES. En particulier dans l'échantillonneur on cherche à équilibrer au maximum la propagation du signal d'horloge vers toutes les bascules de la chaîne. On utilise le placement de la figure 29. Dans celle-ci, le signal Clk provient d'un arbre en H (comme figure 21) et le seul déséquilibre dans l'arbre d'horloge vient donc de la partie placée après les

cellules « buffclk ». Dans cette configuration, même avec 1536 bascules le déséquilibre maximal est limité au délai de propagation du signal sur 3 hauteurs de cellule.

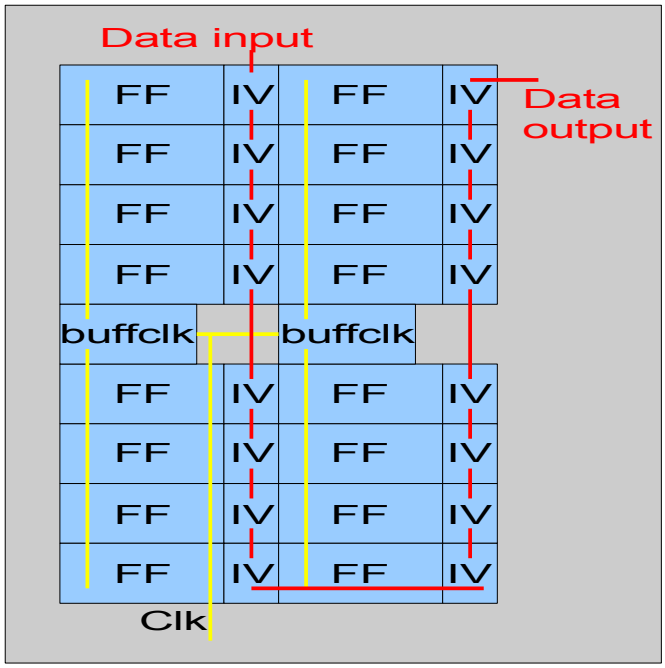


Figure 29: Modèle de placement des cellules dans le module échantillonneur.

➢**Chemins critiques**

Les parties du circuit denses en portes sont placées de sorte que les chemins critiques au niveau délais soient physiquement très courts (les portes partageant des connexions sont placées les unes à coté des autres) et peuvent être routés en métal 2 et 3 (ce sont les noms des premières couches d'interconnexions entre portes). De plus ce sont les niveaux de connexion les plus rapides disponibles ce qui assure de très faibles temps de propagation.

Dans la figure 29, on a un exemple de placement d'une zone dense (l'échantillonneur). On y distingue deux colonnes de bascules séparées par les inverseurs de la chaîne de propagation, toutes ces cellules étant collées les unes aux autres pour minimiser la longueur des interconnexions (chemins Data et Clk). Les amplificateurs buffclk situés au milieu du schéma préservent l'intégrité du signal d'horloge et minimisent les déséquilibres d'horloge. Cette horloge (chemin Clk) arrive dans les amplificateurs et rayonne ensuite vers chaque bascule. Les amplificateurs buffclk sont placés au milieu de chaque colonne pour un maximum d'efficacité.

Le chemin data input qui forme la chaîne de propagation des impulsions bénéficie des interconnexions les plus courtes possibles pour profiter de la meilleure résolution possible sur les résultats.

3.3.5 Architecture du circuit PROBES Laser

Le circuit PROBES comprend un module de surfaces sensibles, un module échantillonneur et un module de génération d'impulsion. Les surfaces sensibles sont les zones de tir laser. Sur ces zones sont implantées des portes suivant les motifs D16, D64 ou C64 (cf. 3.3.1.3). Ces zones peuvent être activées grâce à un sélecteur. Le générateur d'impulsion peut se substituer à un tir laser pour injecter des impulsions de longueur définie dans les surfaces sensibles. La longueur de cette impulsion peut être paramétrée au moyen d'un autre sélecteur (PW). Enfin le module échantillonneur numérise une impulsion issue des surfaces sensibles en 1536 bits qu'il peut sortir par sa chaîne de scan (Scan out).

Le schéma bloc est disponible figure 30.

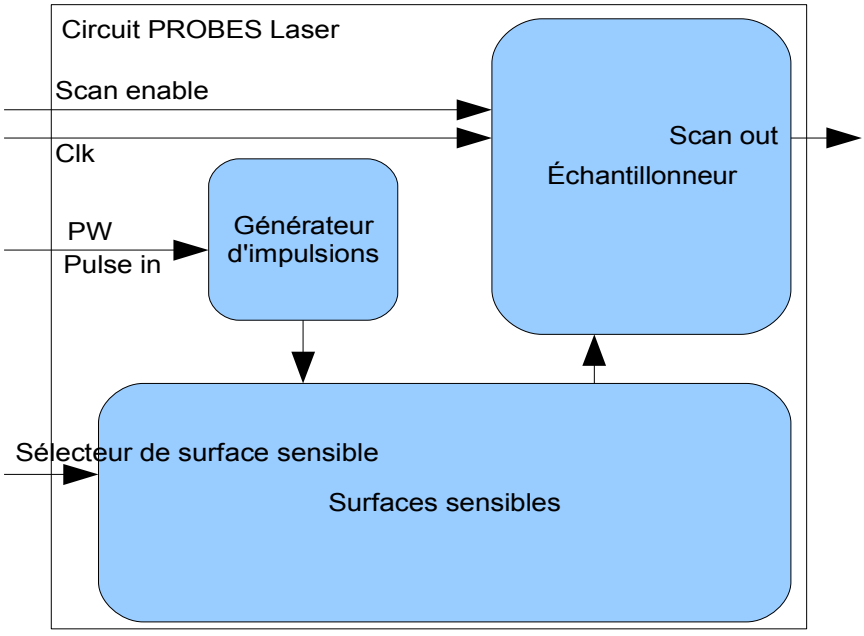


Figure 30: Schéma bloc du circuit PROBES Laser.

Le placement final du circuit et les chemins de données sont montrés figure 31, en particulier en bas sont les 31 surfaces sensibles, en haut a droite l'échantillonneur et en haut a gauche on voit le bloc de génération d'impulsion.

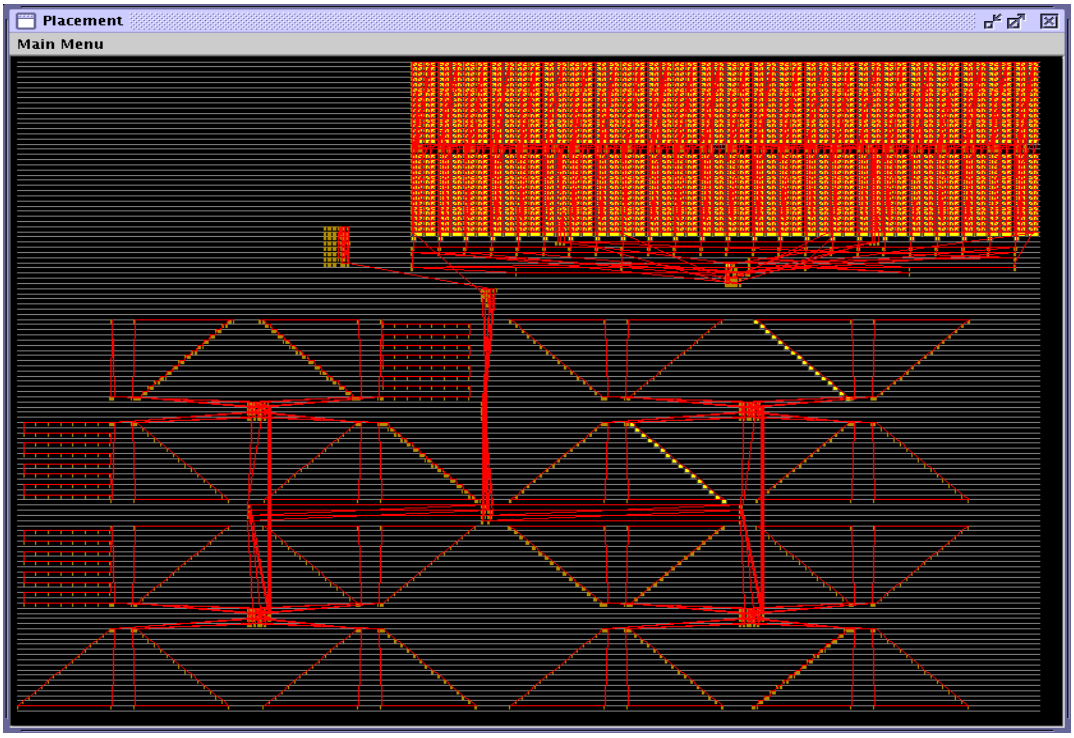


Figure 31: Placement final du circuit PROBES Laser.

3.4 Conception d'un circuit PROBES détectant les perturbations produites par des neutrons

Après avoir conçu les PROBES Laser, nous avons envisagé de concevoir un circuit adapté à la capture d'impulsions transitoires générées par des neutrons basé sur le même flot de conception. Cette section décrit les spécificités de ce projet par rapport aux PROBES Laser.

3.4.1 Objectifs

La mesure de sensibilité aux neutrons des cellules logiques est une préoccupation croissante des industriels après la caractérisation des mémoires. En effet, si les mémoires implantées dans les circuits actuels sont protégées par des codes correcteurs, la logique ne l'est que rarement du fait de sa faible sensibilité. Cependant, dans les technologies les plus récentes le besoin est présent

de caractériser cette sensibilité, et surtout la capacité des perturbations produites à se propager dans l'arbre logique.

Le but de ce circuit est de mesurer la sensibilité des cellules logiques de la librairie standard par rapport à des neutrons. En effet, l'impact d'un neutron sur un transistor MOS peut provoquer une impulsion transitoire qui va se propager à travers le circuit. En utilisant des cellules inverseuses connectées sous forme de point mémoire, nous capturons cette impulsion transitoire et nous transformons donc ce SET en SEU. Ceci nous permet de remonter une information stable vers l'utilisateur.

3.4.2 Spécifications

3.4.2.1 Contraintes

- **Sensibilité des structures de détection**

Comme les faisceaux de particules à notre disposition sont relativement larges (quelques centimètres de diamètre) tout le coeur du circuit est irradié. Cela entraîne que la logique de détection des erreurs (qui ne fait pas partie de la zone sensible) est elle aussi affectée par le phénomène de SEU/SET. Nous devons donc protéger les zones de détection ou au moins pouvoir détecter spécifiquement ces erreurs pour éviter de polluer les statistiques d'apparition d'erreurs transitoires dans les cellules cibles.

- **Taille des surfaces sensibles**

La sensibilité aux neutrons des technologies 90nm est faible, avec en particulier une « cross section » inférieure à 10^{-14} cm^2 (source iRoC). Une porte logique soumise à un flux de $3*10^6$ $neutrons.cm^{-2}.s^{-1}$ comme à TRIUMF (Vancouver, Canada), qui est le plus puissant faisceau de neutrons à notre disposition devra donc être irradiée en moyenne pendant $3,3*10^7$ secondes pour que nous obtenions une perturbation.

Comme le temps d'irradiation est une contrainte forte, nous devons augmenter le nombre de cellules testées simultanément pour obtenir un nombre d'erreurs significatif. Pour obtenir 100 erreurs avec une irradiation de 3 heures nous devons donc avoir approximativement

$3*10^5$ cellules sensibles dans notre circuit. Cet ordre de grandeur nous impose donc une densité de portes importante pour notre circuit.

3.4.2.2 Solutions

- **Densité de portes sensibles élevée**

Pour répondre aux contraintes concernant la taille du silicium et le temps d'irradiation disponible pour nos expériences, nous devons augmenter au maximum le rapport (portes sensibles) sur(logique de contrôle). Nous avons donc décidé d'abandonner la séparation physique entre zone sensible et zone de mesure. La logique de détection devra être à la fois la plus petite possible et la moins sensible aux particules.

- **Capture des impulsions dans une structure mémorisante**

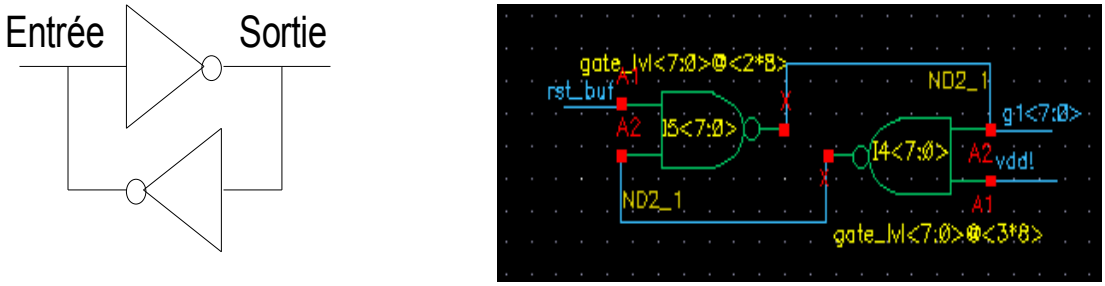
Pour pouvoir capturer des impulsions transitoires comme les SET qui sont très fugitives, le modèle choisi dans les PROBES Laser était basé sur un échantillonneur. Dans le cas des PROBES Neutron, nous avons choisi de capturer les transitoires au coeur de la zone sensible.

Nous somme partis du fait que les SEU proviennent à l'origine d'un SET apparaissant dans un point mémoire et arrivant à modifier l'état électrique de ce dernier. Si on connecte deux portes inverseuses comme un point mémoire, on peut assumer qu'un SET se produisant dans une de ces portes va se propager et modifier l'état électrique du point mémoire. Nous aurons donc réussi à détecter de manière stable (information stockée et disponible) un SET apparaissant dans la porte cible. Il nous suffit de réinitialiser le point mémoire pour remettre le détecteur en action après capture d'un transitoire.

3.4.3 Implémentation de la structure de détection

3.4.3.1 Principe de capture des impulsions transitoires

La capture des impulsions transitoires se fait dans une structure mémorisante. Cette structure est basée sur la forme classique du point mémoire SRAM présentée figure 32. Dans cette configuration, les transistors sont dans un état stable et mémorisent donc cet état électrique.



(a) : Point de mémorisation basé sur des inverseurs *(b) : Point de mémorisation basé sur des NAND*

Figure 32: Exemples de points de mémorisation standard.

On peut forcer une valeur au point mémoire par l'entrée inversée (initialisation), la sortie restant stable jusqu'à la prochaine initialisation.

On peut facilement étendre cette définition de point mémoire à tout type de porte combinatoire inverseuse, comme les NAND de la figure 32. Dans le cas de portes à plusieurs entrées, il suffit de placer les entrées supplémentaires dans un état neutre, comme le niveau logique haut pour un NAND, ou le niveau bas pour un NOR.

L'intérêt de cette structure est qu'en cas d'apparition d'un SET sur une des portes de la structure mémorisante, le point mémoire est susceptible de basculer et donc de stocker un état logique différent de celui initialement stocké. Nous pouvons donc utiliser cette structure pour détecter un SET apparaissant dans l'une des portes composant la structure mémorisante.

3.4.3.2 Validation du principe par simulation électrique

Pour vérifier l'efficacité de cette structure de détection, nous avons procédé à une série de simulations électriques (SPICE). Ces simulations ont permis de déterminer la sensibilité de la structure mémorisante. La structure utilisée dans chaque cas est basée sur celle de la figure 33. On y retrouve la structure tête-bêche à deux portes inverseuses chargée par un NAND4. Ce NAND4 correspond au premier étage de l'arbre de détection de changement d'état du point mémoire. L'entrée A de la porte NAND2_0 sert à initialiser l'état du point mémoire.

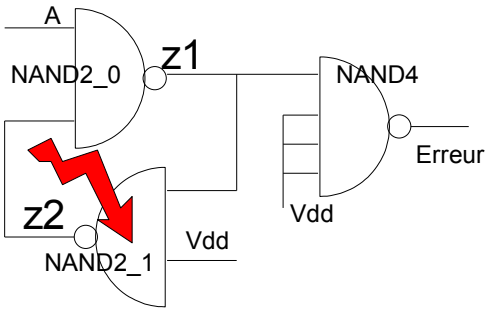


Figure 33: Schéma d'une structure mémorisante à base de NAND2.

Nous avons transformé la porte NAND2_1 pour lui ajouter une source de courant (figure 34). Cette source de courant simule l'effet d'une particule frappant un des transistors de la porte [PER04]. Dans le cas de la structure simulée, l'entrée B de cette porte est connectée au Vdd.

Toutes les autres structures simulées dans cette section utilisent le principe de la boucle à deux portes inverseuses pour créer une structure mémorisante, et ne diffèrent que par le type de porte inverseuse utilisé.

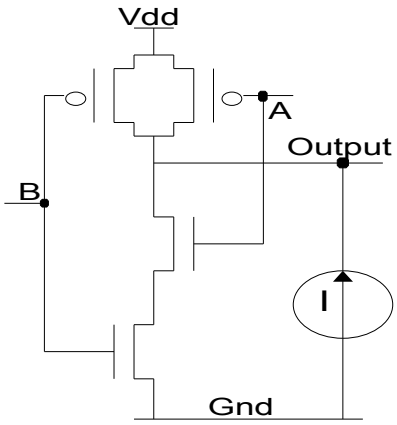
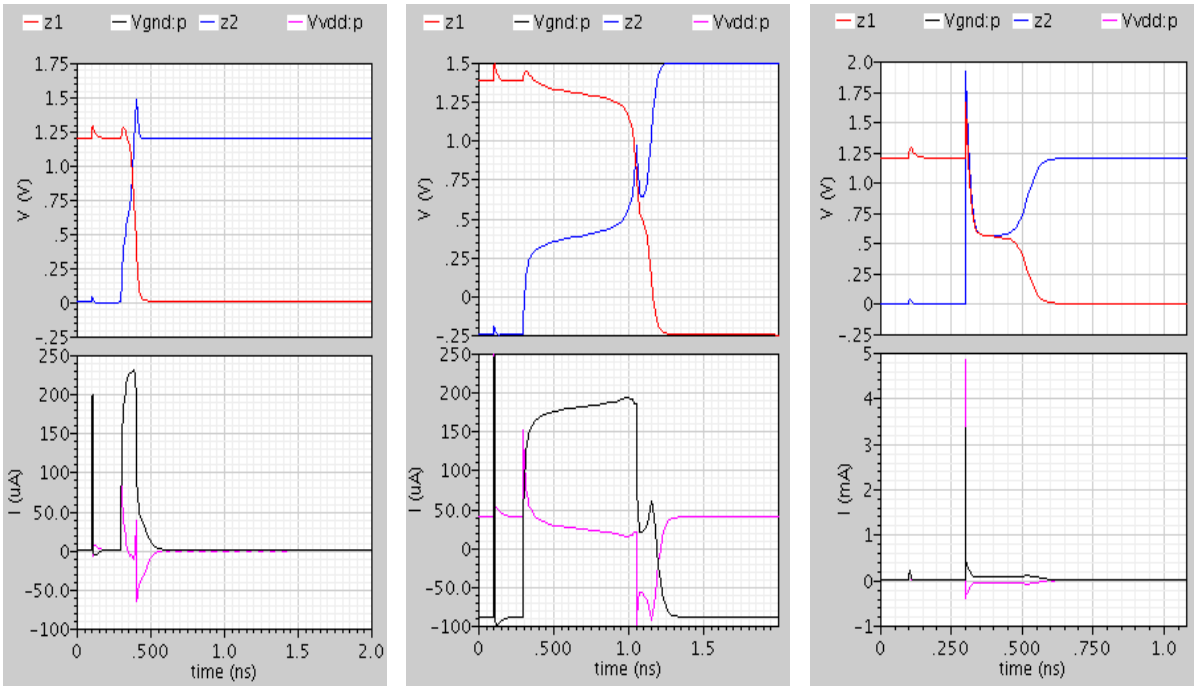


Figure 34: Porte NAND modifiée par ajout d'une source de courant.

Les simulations ont servi à déterminer la courbe de sensibilité de ces structures [PER04]. Cette courbe permet de mettre en évidence les deux composantes déterminant le point d'inversion de l'état du point mémoire. Les courbes ci-dessous montrent les courbes de tension des noeuds z1 et z2, et le courant tiré de l'alimentation. Nous voyons trois cas d'inversion de l'état du point mémoire Figure 35, un cas moyen en (a), le cas de courant minimal en (b) et enfin le cas de durée d'impulsion minimale en (c).



(a) I = 218 µA pendant T = 80 ps *(b) I = 149 µA pendant T = 757 ps* *(c) I = 9044 µA pendant T = 1 ps*

Figure 35: Simulations d'impulsions de courant dans un point mémoire suivant différents paramètres.

On observe le mode d'inversion du point mémoire très clairement sur la partie (b) de la figure 35 : le courant est d'abord collecté dans la porte NAND2_1 dont la tension de sortie commence à évoluer, puis la tension d'inversion de l'entrée de la porte NAND2_0 est atteinte et cette dernière change aussi d'état. Le point mémoire a ainsi achevé son changement d'état et nous avons donc capturé l'impulsion transitoire.

3.4.4 Architecture du circuit PROBES Neutrons

Dans ce circuit, nous avons réutilisé le flot de conception des PROBES Laser pour obtenir un circuit très dense et minimisant les délais sur les interconnexions. Le circuit étant très redondant, nous l'avons hiérarchisé en partant d'un bloc élémentaire contenant 28 cellules mémorisantes ainsi que la logique de détection associée (module BLOCK), comme montré dans la figure 36. Nous avons ensuite instancié ce bloc plusieurs fois dans un module GROUP en rajoutant la logique associée de propagation des signaux d'entrée-sortie (drivers). Le nombre d'instances du module BLOCK dans un module GROUP dépend de la taille des structures mémorisantes, de telle sorte que tous les modules GROUP du circuit PROBES Neutron ont une taille similaire.

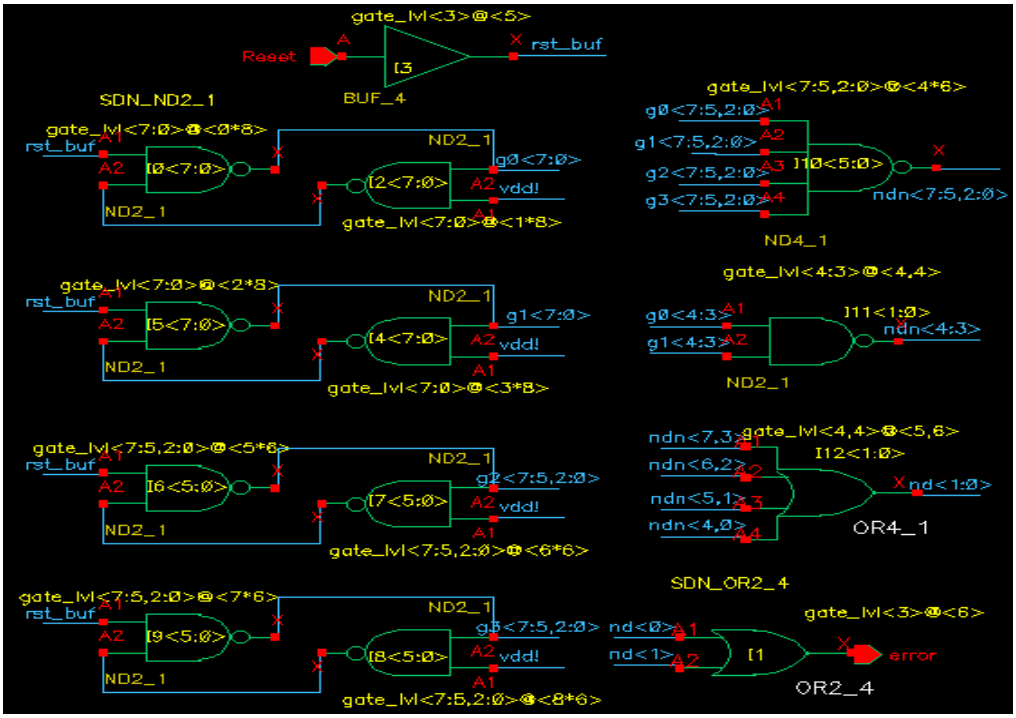


Figure 36: Vue d'un module BLOCK contenant 28 structures mémorisantes basées sur des portes NAND.

Dans la figure 36, nous voyons les 4 groupes de structures mémorisantes sur la gauche et la structure de détection d'erreur sur la droite. Comme il est très important de minimiser les capacités parasites dues aux interconnexions entre les deux NAND de la structure mémorisante, nous les avons placées côte à côte. Le plan de masse du module BLOCK est montré figure 37. On y voit les 28 structures mémorisantes (MEM) ainsi que la logique d'amplification et de détection d'erreurs.

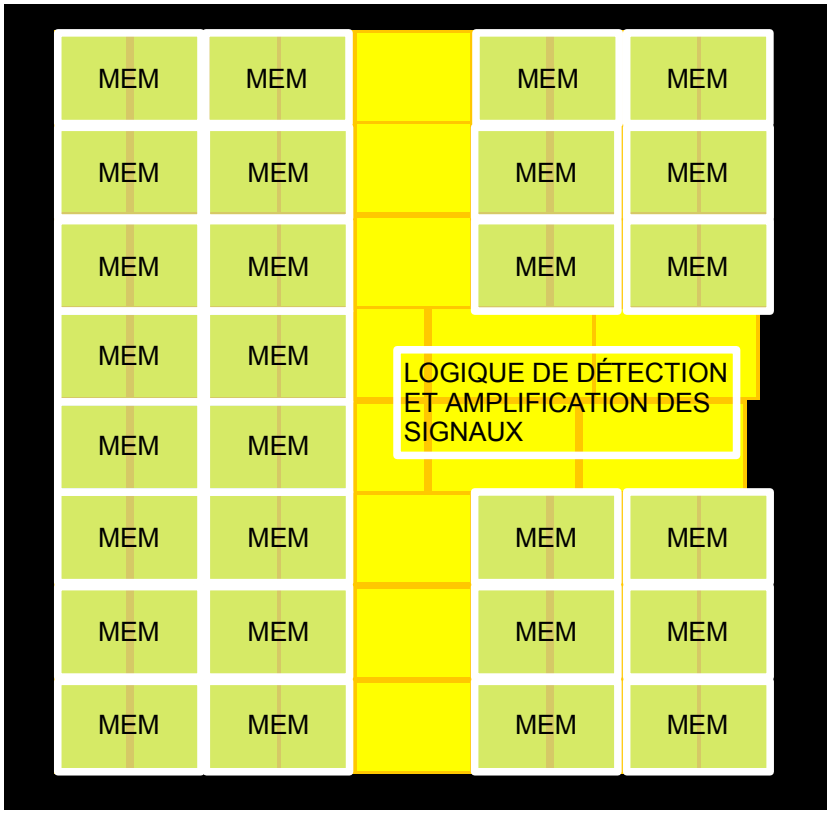


Figure 37: Plan de masse du module BLOCK.

La figure 38 montre la hiérarchie complète du circuit PROBES Neutrons. Au niveau du module BLOCK, nous n'avons qu'un seul signal d'erreur correspondant à toutes les structures du module, ce signal étant remonté au niveau du module GROUP qui représente environ 1000 bits de données. Chaque GROUP remonte son propre signal d'erreur au module SA qui possède un additionneur (figure 39) pour compter le nombre de modules GROUP défectueux. Chaque module SA contient 128 instances GROUP.

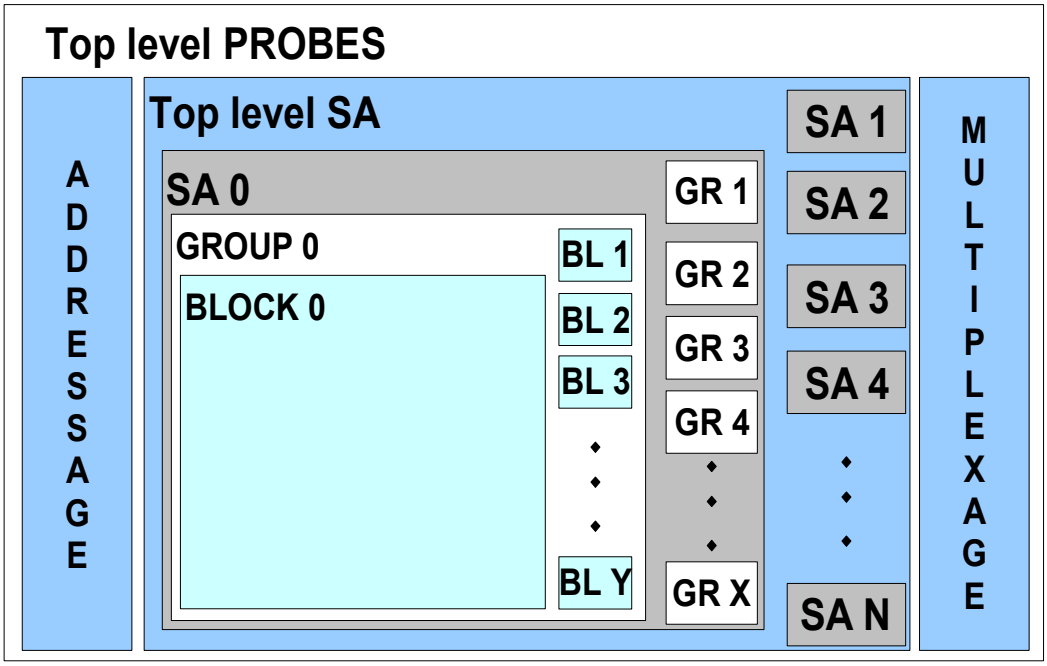


Figure 38: Hiérarchie du circuit PROBES Neutrons.

Grâce à un système d'adressage des entrées et de multiplexage des sorties du circuit, le circuit PROBES Neutron est capable de remonter le nombre de modules GROUP défectueux dans chaque surface sensible à volonté. La résolution maximale de ce circuit est donc le niveau GROUP, ce qui correspond environ à 1k bit de données.

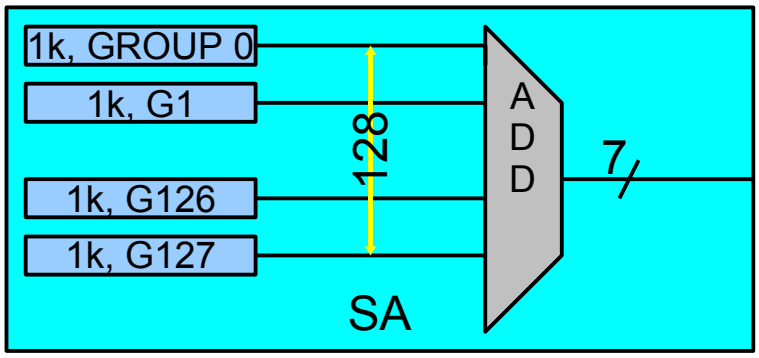


Figure 39: Architecture d'un module SA.

3.4.5 Traitement des données issues du circuit PROBES Neutron

Pendant l'irradiation du circuit, le système de test associé va scanner les différentes surfaces sensibles à la recherche du nombre d'erreurs remontées par le système de détection. Les éléments mémorisants n'appartenant pas aux structures de détection sont triplés, ce qui permet

d'éliminer les perturbations parasites apparaissant dans les structures de contrôle en lisant 3 fois consécutives les données sortant du circuit.

3.5 Conclusion

Dans ce chapitre un flot de conception spécifique adapté à nos contraintes est proposé, puis est utilisé pour concevoir deux circuits. Le premier est orienté vers la mesure de la durée d'impulsions provoquées par un tir laser sur des portes combinatoires, l'autre est dédié à la mesure de la sensibilité de cellules combinatoires et séquentielles face à des perturbations d'origine radiatives non directionnelles.

Avec cette méthodologie et ces circuits à notre disposition il est maintenant possible d'attaquer la phase d'expérimentation qui fait l'objet du chapitre 4.

Chapitre 4 : Analyse des impulsions transitoires provoquées par l'attaque d'un laser vert sur une technologie ST HCMOS9GP 0.13 µm

4.1 Introduction

Après fabrication du circuit PROBES Laser, j'ai conçu une interface me permettant d'insérer l'expérience dans le banc de test laser de la société GemPlus. J'ai donc réalisé plusieurs campagnes de tir sur les cellules implantées dans le circuit. Ces campagnes de mesure vont me permettre de vérifier l'efficacité de la méthodologie de conception proposée dans le chapitre précédent.

Ce chapitre décrit les expérimentations menées sur le circuit PROBES Laser. Dans la suite sont décrites l'expérimentation mise en place, puis le mode opératoire utilisé. Enfin les résultats et une analyse de la sensibilité de la technologie ST HCMOS9GP 0.13 µm sont présentés.

4.2 Étude du matériel

4.2.1 Source laser

La source laser utilisée dans nos expériences est un laser Nd:YAG (pour neodymium-doped Yttrium Aluminium Garnet Nd:$Y_3Al_5O_{12}$), ou laser à grenat dopé. Ce laser à état solide émet dans l'infrarouge (1064 nm) avec possibilité de doubler la fréquence pour atteindre 532 nm (lumière verte). Cette source laser est utilisée pour modifier des circuits silicium en coupant certaines pistes électriques par fusion. Dans le cadre de cette étude nous allons travailler en lumière verte.

Un rayon laser de cette longueur d'onde possède un facteur d'absorption dans le silicium de 1.3 μm^{-1} [BUC88] ce qui signifie qu'il sera très rapidement absorbé par les premières couches du circuit. Cependant, la puissance de notre source laser garantit (0.6 mJ au maximum pendant 6

ns, soit 10 kW) l'apparition de perturbations dans le circuit. La première étape des expérimentations sera d'ailleurs de détecter le seuil de destruction du silicium pour éviter de détruire les circuits testés ou de provoquer des erreurs permanentes comme les latch-ups [SKO03]. La surface illuminée par le laser est réglable et peut varier de 1*1 μm^2 à 200*200 μm^2.

4.2.2 Pas de tir

Le système d'expérimentation (figure 40) consiste en une source laser, une table motorisée d'une précision micrométrique commandée par ordinateur permettant de placer le circuit suivant les coordonnées XY, un oscilloscope pour vérifier les signaux électriques, ainsi qu'une interface de test entre le circuit PROBES et l'ordinateur commandant le pas de tir. Ce pas de tir est conçu pour permettre d'automatiser au maximum les séquences de tir laser, seule la mise en place de l'expérience demandant une intervention humaine.

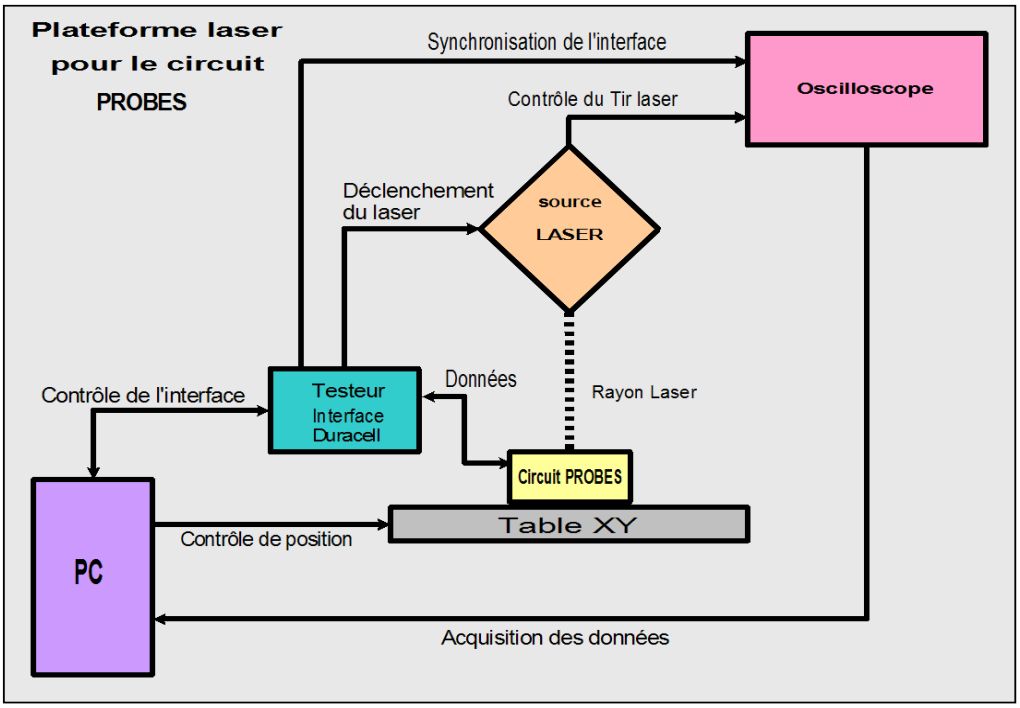


Figure 40: Pas de tir laser pour le circuit PROBES.

4.2.3 Interface de contrôle

L'interface de contrôle entre le circuit PROBES et l'ordinateur commandant l'expérience est basée sur le testeur iRoC SMARTESTBED. Ce testeur permet, via une interface Ethernet et une bibliothèque de fonctions simples, de commander directement le circuit PROBES.

Les entrées de l'interface sont les fonctions C d'une bibliothèque spécialisée. Elles fournissent toutes les fonctionnalités possibles, tant pour la gestion du circuit PROBES (gestion des entrées-sorties du circuit) que pour la gestion de l'interface elle-même.

Les informations en sortie sont de deux types : d'une part, des variables d'état qui permettent à l'utilisateur et au programme commandant le pas de tir de connaître l'évolution de l'expérience, et d'autre part, un fichier de résultats contenant les résultats de l'expérience en cours avec tous les paramètres d'environnement utiles.

Le fichier de résultats contient des données sur chaque tir laser sous forme de 14 lignes (figure 41) :

- la première ligne contient le numéro de la surface sensible ciblée ainsi que les coordonnées XY du tir;
- les 12 lignes suivantes commençant par « **>E** » contiennent les données de sortie du circuit PROBES (1536 bits sous la forme de 384 chiffres hexadécimaux);
- la dernière ligne contient les paramètres utilisés par le circuit PROBES.

```
Area: 01 , X = 125.0, Y = 286.0
>E  Nov-09  03:13:26.891   7  01  00000000000000000000000000000000
>E  Nov-09  03:13:26.891   7  02  00000000000000000000000000000000
>E  Nov-09  03:13:26.891   7  03  000000000007FFFFFF800000000000000
>E  Nov-09  03:13:26.891   7  04  00000000000000000000000000000000
>E  Nov-09  03:13:26.891   7  05  0000000000000000FFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  06  FFFFFFFFFFFFFF8000000000000000000
>E  Nov-09  03:13:26.891   7  07  0000000000000000FFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  08  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  09  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  10  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  11  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
>E  Nov-09  03:13:26.891   7  12  FFFFFFFFFFFFFFFFFFFFFFFFFFFE00000
>E  Nov-09  03:13:26.891   7  13  1UUUUUUUUUUUUUUC1U111CUUUU1C111
```

Figure 41: Exemple de log d'un tir laser.

Dans le « log » de la figure 41, le rectangle délimite les 1536 bits (écrits sous forme hexadécimale) sortant de l'échantillonneur. Ils représentent une capture du signal électrique issu du tir laser sur les cellules cibles. Par défaut, tous les bits sont à l'état logique « 0 », et un bit à « 1 » est synonyme d'une perturbation.

Dans l'exemple proposé, on observe 3 groupes de perturbations :

- « 7FFFFFF8 » correspondant à 28 bits erronés consécutifs;
- « FFFFFFFFFFFFFFFFFFFFFFFFFFF8 » pour 109 bits erronés;
- 679 bits erronés consécutifs.

Ces 3 groupes peuvent être identifiés comme 3 erreurs distinctes résultant du tir laser sur la surface 01. En connaissant le délai de propagation d'un inverseur de la chaîne de capture on peut calculer la longueur de chaque erreur.

4.3 Mode opératoire de l'expérience

Une session de tirs laser consiste en 3 étapes successives : la calibration, la génération interne d'impulsions et enfin les tirs laser proprement dits.

4.3.1 Calibration

Calibrer le circuit revient à calculer le délai moyen de propagation des inverseurs de l'échantillonneur. Cette donnée nous donnera la précision de nos mesures. Pour ce faire, nous avons placé un chemin de propagation équilibré en 4 points régulièrement espacés de l'échantillonneur qui sont propagés vers 4 sorties adjacentes du circuit. Quand nous envoyons un front dans la chaîne de capture, nous pouvons mesurer avec une bonne précision le temps séparant chaque front. Ce temps nous donne la durée de propagation à travers 512 inverseurs.

4.3.2 Tests internes

Le circuit PROBES contient un générateur d'impulsion implanté selon l'architecture décrite Figure 42.

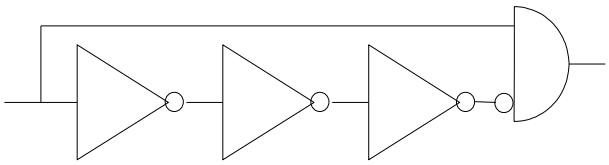


Figure 42: schéma d'un générateur d'impulsion à 3 inverseurs dans le circuit PROBES.

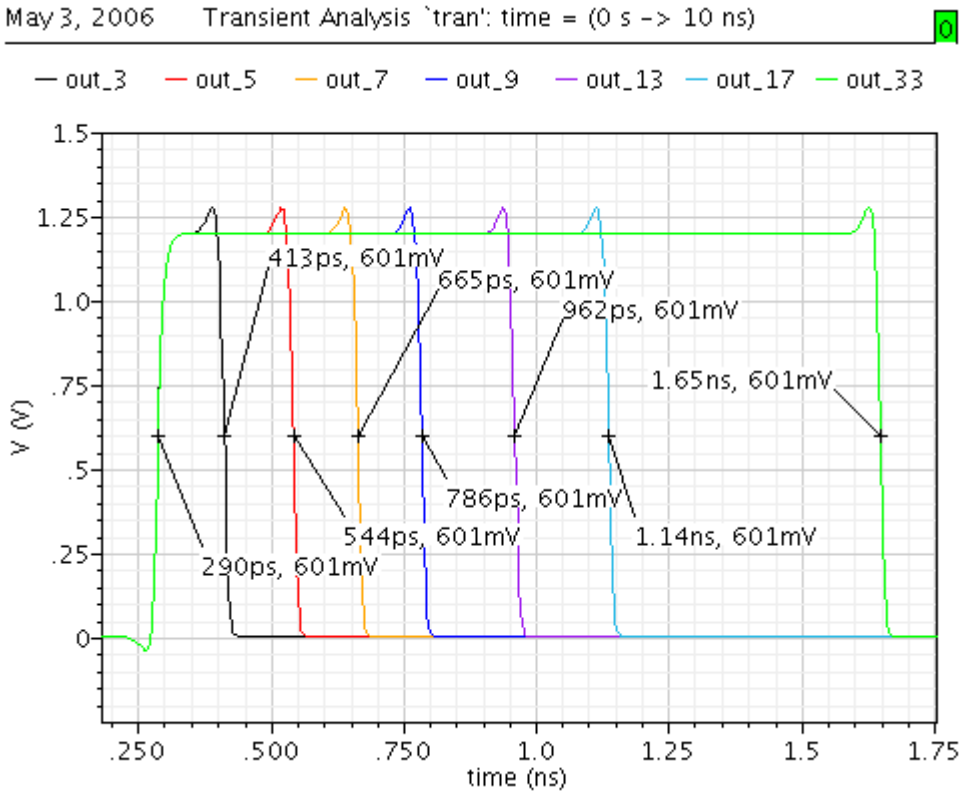


Figure 43: Simulations de la durée des impulsions générées par le module internal_pulse.

Le principe de ce module est de générer une impulsion dont la longueur est commandée par le temps de propagation des inverseurs présents sur le chemin du signal. Dans le circuit PROBES nous avons placé 7 générateurs avec un nombre différent d'inverseurs, respectivement 3, 5, 7, 9, 13, 17 et 33. Cette fonctionnalité nous permet de vérifier la répétabilité de notre mode

opératoire grâce à la relative constance des impulsions générées. Nous nous servons aussi de ce système pour comparer les performances de nos différents circuits.

Nous avons simulé cette partie du circuit pour évaluer les performances du générateur (figure 43) ce qui nous a permis de construire la table 3.

Nombre d'inverseurs	Durée de l'impulsion (ps)
3	123
5	254
7	375
9	496
13	672
17	850
33	1360

Table 3: Durée des impulsions générées par le module internal pulse d'après simulation électrique.

Ces durées ne sont que le produit de simulations électriques et ne peuvent prendre en compte l'intégralité des paramètres du circuit, comme les capacités parasites engendrées par les interconnexions.

4.3.3 Tirs laser

Dans le mode principal, après initialisation, le circuit PROBES est capable de capturer la réponse transitoire de portes logiques atteintes par un tir laser. Il détecte l'arrivée d'un front dans l'échantillonneur et déclenche le processus de capture. Le front d'onde véhiculé dans l'échantillonneur est ainsi capturé dans des bascules et une chaîne de bascules de scan permet de récupérer les informations en sortie du circuit. L'échantillon capturé par le circuit est disponible sous la forme de 3 trames de 512 bits mises bout à bout. Le tir laser dure 6 ns et frappe une surface rectangulaire réglable de 5*5 μm^2 à 200*200 μm^2.

4.3.4 Précision de l'échantillonneur

Pour calculer la précision de l'échantillonneur nous avons mesuré le temps de propagation d'un front sur 512 inverseurs de la chaîne d'inverseurs du circuit. Nous en avons extrait la table 4 [LER06] :

Table 4: Mesure de la précision de l'échantillonneur du circuit PROBES.

	1ere partie de la chaîne d'inverseurs	2e partie de la chaîne d'inverseurs	3e partie de la chaîne d'inverseurs
Chip1 (ns)	12,5	12,44	11,67
Chip2 (ns)	12,28	12,39	11,39
Chip3 (ns)	12,39	12,56	11,61
Chip4 (ns)	12,67	12,61	12
Chip5 (ns)	12,06	12,44	11,61
Moyenne (ns)	**12,38**	**12,49**	**11,66**
Temps de propagation moyen par inverseur (ps)			**23,78**

On remarque une diminution du temps de propagation d'environ 1ns sur la dernière tranche de l'échantillonneur ce qui peut être dû au fait que la patte correspondant à la sortie de fin de chaîne soit de l'autre côté du boîtier. Le câblage réalisé n'assure donc pas l'équilibre des longueurs de fil (ce dernier est plus court d'environ 5 cm que les autres). Comme la conception de l'échantillonneur est régulière jusqu'aux pattes de sortie, il ne devrait pas y avoir de divergence majeure dans les temps de propagation, ce qui est suggéré par les deux premières valeurs de la table 4.

Nous avons aussi fait des tests sur les durées des impulsions produites par le générateur interne, et nous avons obtenu les données de la figure 44 (à comparer avec celles de la table 3).

Le générateur d'impulsion a un comportement similaire (à un « offset » près) pour un faible nombre d'inverseur, mais en fait il y a une divergence de pente qui devient visible pour un grand nombre d'inverseurs. Les divergence observées comme l'offset peuvent provenir de certains paramètres comme les interconnexions qui n'ont pas été prises en compte dans nos simulations. La différence de pente peut provenir des écarts entre le processus de fabrication et les données utilisées pour les simulations.

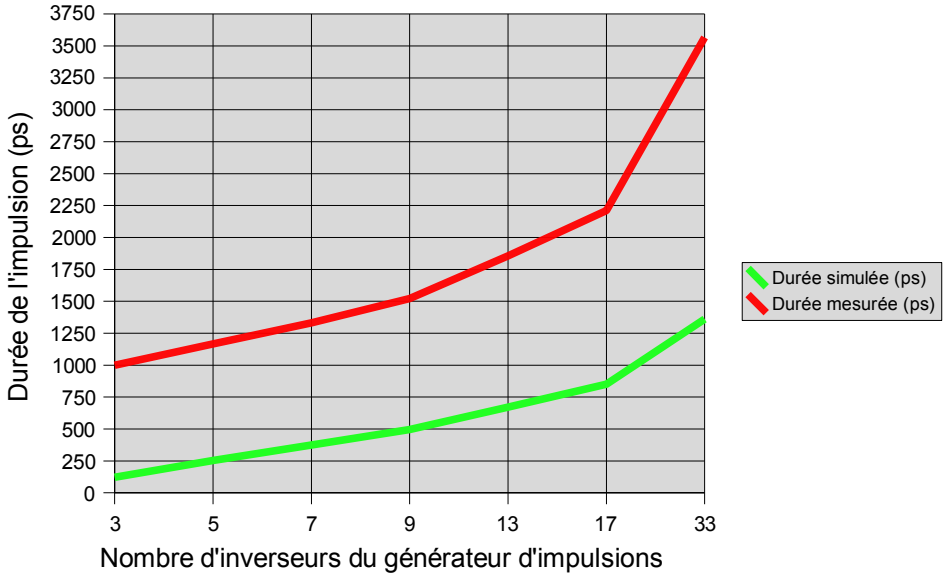


Figure 44: Écarts entre les durées simulées et mesurées du générateur d'impulsion.

4.3.5 Stabilité de l'échantillonneur

Grâce au générateur d'impulsion du circuit PROBES, nous avons fait des tests de stabilité de l'échantillonneur. Ces tests ont consisté en la génération d'impulsions de longueur fixe (issues du générateur d'impulsion interne) capturées et échantillonnées par le système de mesure. Nous en avons extrait des données statistiques représentant les performances de notre circuit.

Nous avons réalisé 200 expériences pour chaque longueur d'impulsion et pour chaque surface sensible. Nous avons remarqué une bonne cohérence dans les résultats comme le montre la figure 45. En effet la variance et l'écart-type ont une moyenne respective de 1,34 et de 1,16 bits et dépendent peu de la valeur mesurée, tandis que l'incertitude reste quasiment constante entre 4 et 5 bits (en moyenne 4,71). En outre la précision des résultats ne dépend que très peu du type de porte traversé par les impulsions.

Selon les mesures effectuées ci-dessus, nous pouvons donc nous attendre à une erreur d'environ 1 à 2 bits, ce qui nous donne une incertitude sur la stabilité de nos mesures comprise entre 25 et 50 ps. L'expérience montre que les plus faibles valeurs sont obtenues en début d'expérience (circuit froid) et qu'elles augmentent au cours de l'utilisation du circuit (notre expérience a duré 2 heures 16 minutes).

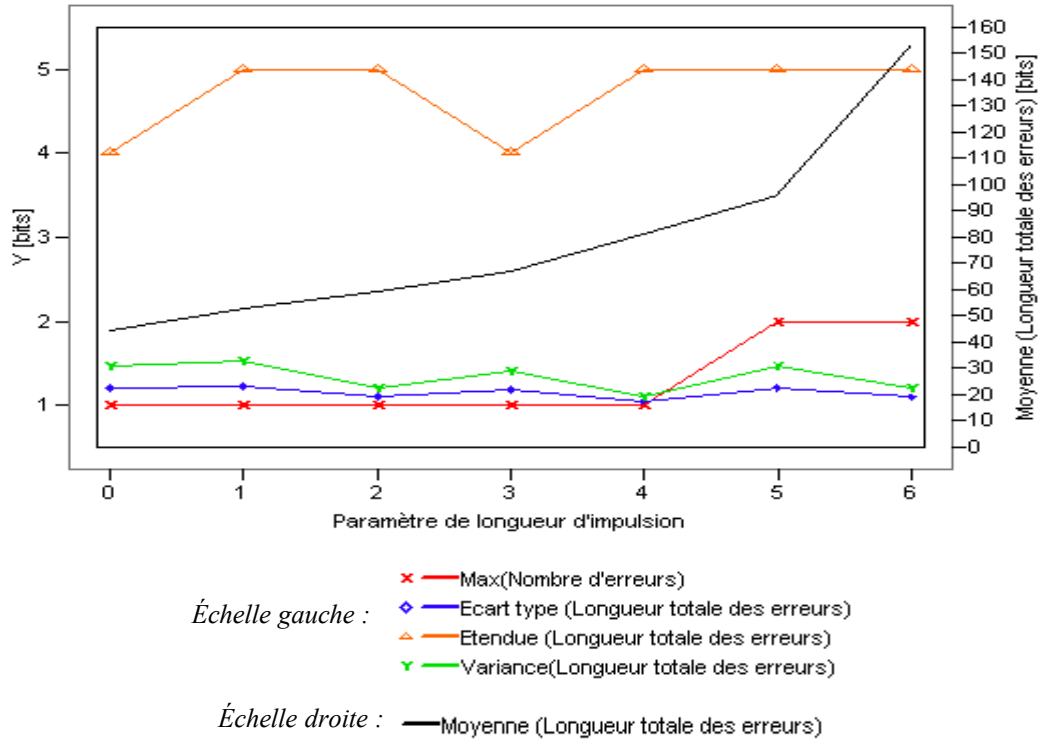


Figure 45: Résultats de stabilité du module de capture d'impulsion.

Sur une période plus courte (expérience de 4 minutes 16 secondes) nous observons une réduction de l'écart entre les valeurs min et max, écart qui passe à 2 bits au maximum sur les impulsions les plus courtes. On obtient même des écarts nuls dans le cas de certaines longueurs d'impulsions. Les résultats de cette expériences sont visibles dans la figure 46.

Nous pouvons donc affirmer que la précision de notre échantillonneur est au maximum de l'ordre de 2 bits pour des expériences courtes.

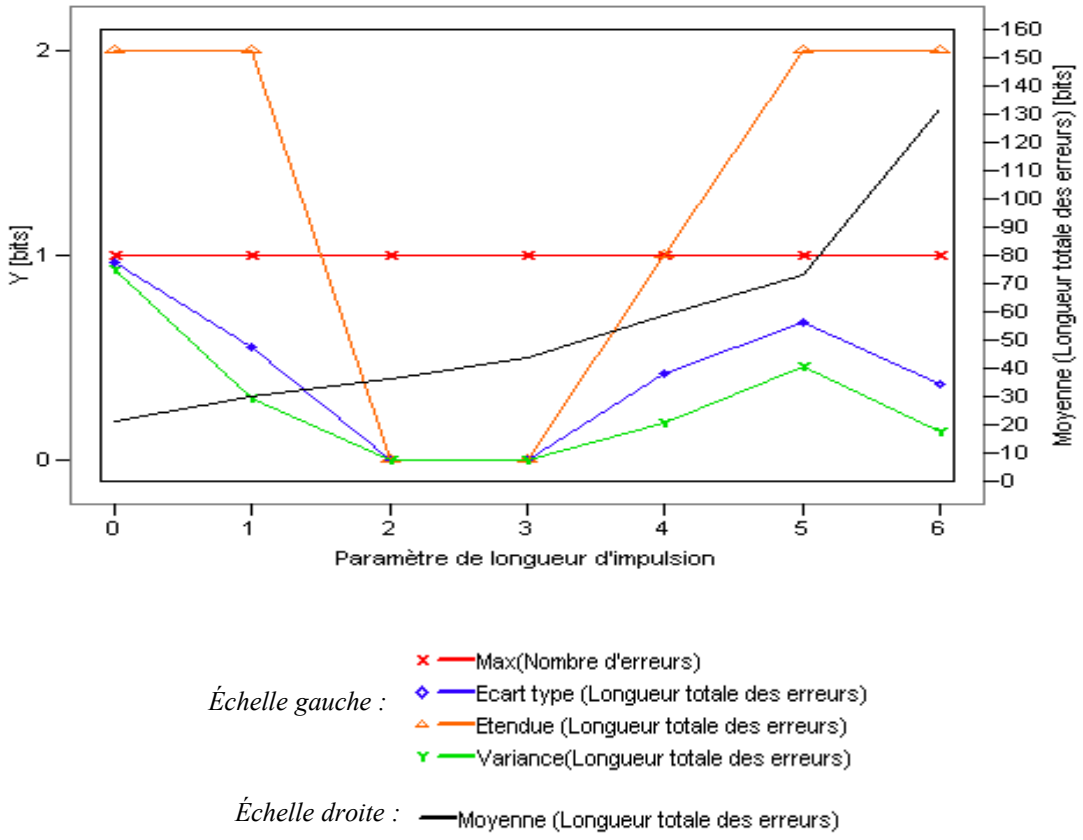


Figure 46: Précision des mesures de longueur d'impulsion sur une expérience courte (T < 5 minutes).

4.4 Étude d'une impulsion se propageant dans des cellules standard ST

4.4.1 Altération de la durée d'impulsions dans une chaîne de portes

4.4.1.1 Étude des résultats du générateur d'impulsions

Dans la figure 47, nous voyons les résultats de capture d'impulsions internes au circuit PROBES. La durée de l'impulsion initiale étant fixée, nous allons observer l'effet de la propagation de cette impulsion à travers les cellules des différentes surfaces sensibles. Nous observons très clairement deux groupes de résultats, c'est-à-dire d'une part les résultats proches de la référence (NONE_DC), d'autre part les résultats plus élevés que celle-ci. On remarque de plus que le premier groupe est constitué de portes inverseuses, alors que le deuxième groupe est constitué de portes non inverseuses. Ce phénomène vient du fait que les portes logiques n'ont

pas les mêmes caractéristiques de durée de propagation entre un front positif et un front négatif. Il s'ensuit une altération de la durée d'une impulsion après le passage à travers une porte logique [PER04].

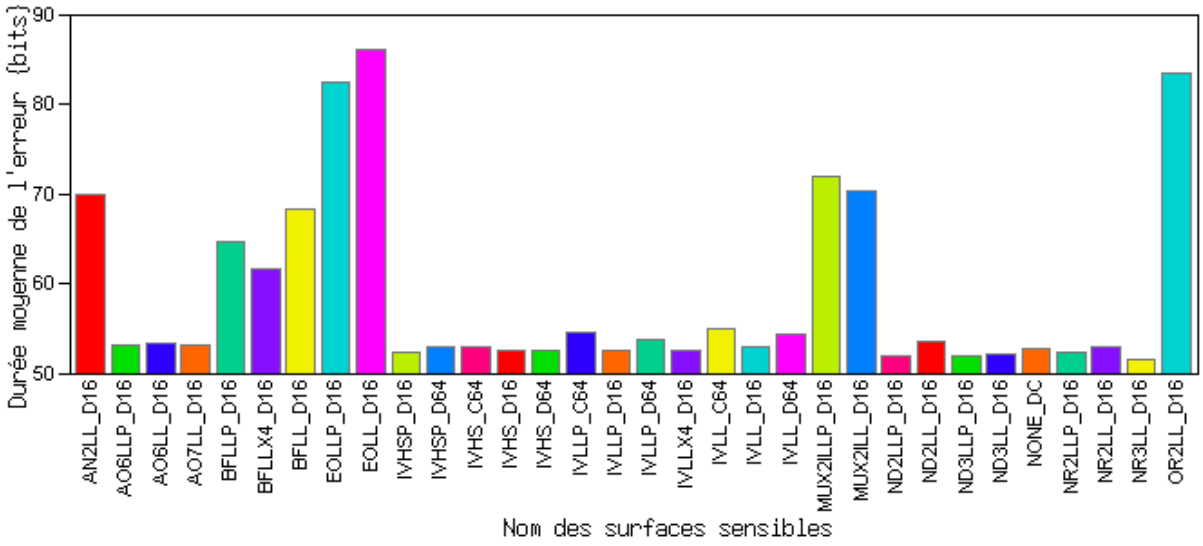


Figure 47: Durées moyennes des impulsions générées par le circuit PROBES mesurées après propagation dans les surfaces sensibles (générateur d'impulsion réglé sur 5 inverseurs).

Les portes non-inverseuses sont les seules à exhiber cette déformation de l'impulsion initiale car une porte inverseuse va transformer une impulsion positive en impulsion négative, et la formule générique d'altération de durée d'une impulsion positive (figure 48)

$$D_1 = D_0 + t_{fall} - t_{rise} \qquad \text{(Eq. 5)}$$

où D_0 est la durée initiale de l'impulsion et D_1 la durée finale, devient dans le cas de deux portes non-inverseuses successives :

$$D_2 = D_1 + t_{fall} - t_{rise} = D_0 + 2*(t_{fall} - t_{rise}) \qquad \text{(Eq. 6)}$$

ou devient dans le cas de deux portes inverseuses successives :

$$D_2 = D_1 - t_{fall} + t_{rise} = D_0 \qquad \text{(Eq. 7)}$$

On voit donc que les portes non-inverseuses cumulent leurs effets quand elles sont enchaînées alors que les portes inverseuses ont tendance à stabiliser la durée de l'impulsion qu'elles transmettent.

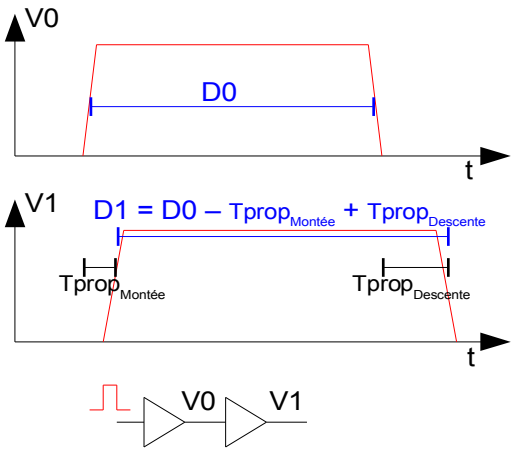


Figure 48: Altération d'une impulsion positive dans une porte logique non-inverseuse

Ces résultats sont complétés par la figure 49 qui montre le même phénomène pour différentes longueurs d'impulsion. On remarque que l'altération de la longueur n'est pas affectée par la longueur initiale de l'impulsion (paramètre PW0, ..., PW6). Les seules exceptions à cette règle proviennent des portes ND3LL et NR3LL qui filtrent les impulsions les plus courtes.

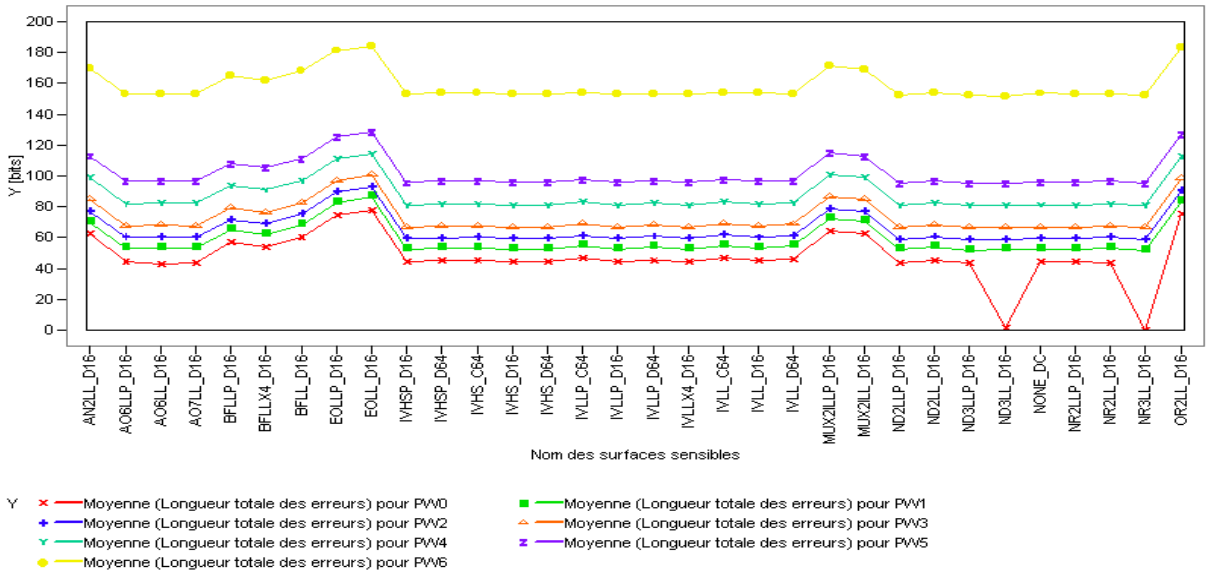


Figure 49: Altérations provoquées par les différentes surfaces sensibles du circuit PROBES selon la longueur initiale de l'impulsion.

Ces altérations semblent surprenantes au premier abord car une porte non-inverseuse en technologie CMOS est une porte inverseuse suivie d'un inverseur. Cependant, les caractéristiques de propagation des portes montrent clairement que chaque porte altère les impulsions qui les traversent. Les paramètres des transistors utilisés (N et P) influent en effet sur la vitesse de propagation des fronts du signal électrique (respectivement descendants et montants).

4.4.1.2 Étude Spice d'une chaîne de portes

Nous pouvons corréler les résultats ci-dessus avec une étude des caractéristiques de la bibliothèque de portes logiques que nous utilisons (table 5) et par la simulation Spice de la figure 50. Sur cette figure on voit qu'une porte AND augmente la durée d'une impulsion de 19 ps alors qu'une porte OR l'augmente de 29 ps.

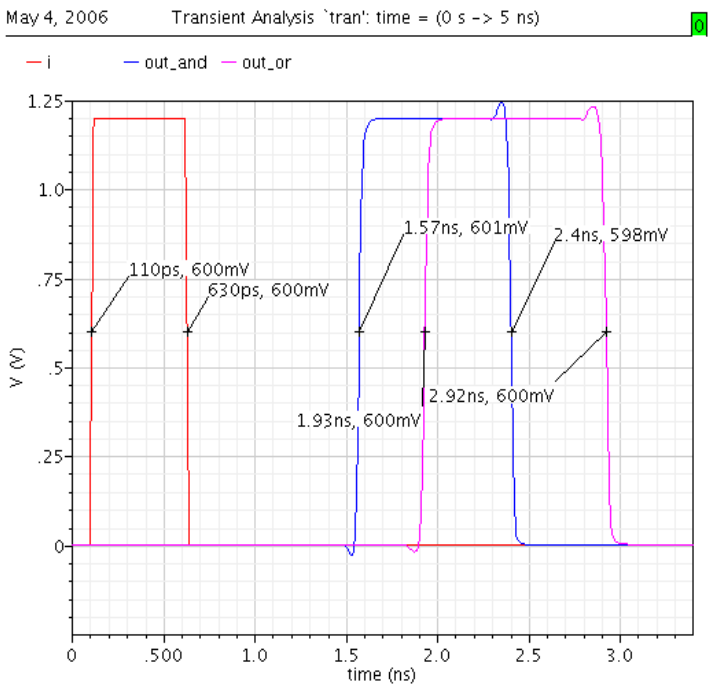


Figure 50: Simulation électrique de l'altération de la longueur d'une impulsion propagée à travers 16 portes AND et 16 portes OR.

La table 5 propose un récapitulatif des altérations de longueur d'une impulsion positive dans les différentes portes utilisées dans le circuit PROBES selon les caractéristiques de la bibliothèque. Les valeurs sont différentes des simulations à cause des paramètres utilisés, mais on voit que

toutes les portes non inverseuses augmentent la durée des impulsions positives qui leurs sont transmises.

Portes inverseuses	Altération (ps)	Portes non inverseuses	Altération (ps)
IVLL	-09,90	BFLL	17,83
IVLLP	-03,88	BFLLP	13,34
IVLLX4	-03,44	BFLLX4	12,47
IVHS	-03,70	AN2LL	20,80
IVHSP	-03,30	OR2LL	25,88
ND2LL	-05,11	EOLL	06,39
ND2LLP	-02,95	EOLLP	04,26
NR2LL	-21,99	MUX21LL	18,77
NR2LLP	-15,98	MUX21LLP	19,73
AO6LL	-10,69		
AO6LLP	-06,61		
AO7LL	-16,44		
ND3LL	-06,37		
ND3LLP	-03,04		
NR3LL	-33,23		

Table 5: Caractéristiques des portes logiques utilisées dans le circuit PROBES.

La mise en évidence d'une corrélation entre les résultats obtenus par simulation ou à partir de la littérature avec ceux obtenus expérimentalement n'est pas facile car les ordres de grandeur ne sont pas respectés (par exemple les portes EOLL et EOLLP ont les taux d'altération les plus faibles parmi les portes non inverseuses mais produisent quand même les impulsions les plus longues dans les résultats expérimentaux, figure 47 et figure 49).

4.4.2 Corrélation entre la longueur du tir laser et le SET créé

Pour les expériences sous faisceau laser, nous avons illuminé l'ensemble des surfaces sensibles par une série de tirs laser délimitant chacun un carré de 5 µm de côté. Les tirs ayant conduit à la création d'impulsions dans les cellules ciblées ont été répertoriés et la longueur moyennes des erreurs capturées a été compilée dans la figure 51. Les temps sont à comparer avec la longueur initiale de l'impulsion laser qui correspond à 252 inverseurs (trait épais gris).

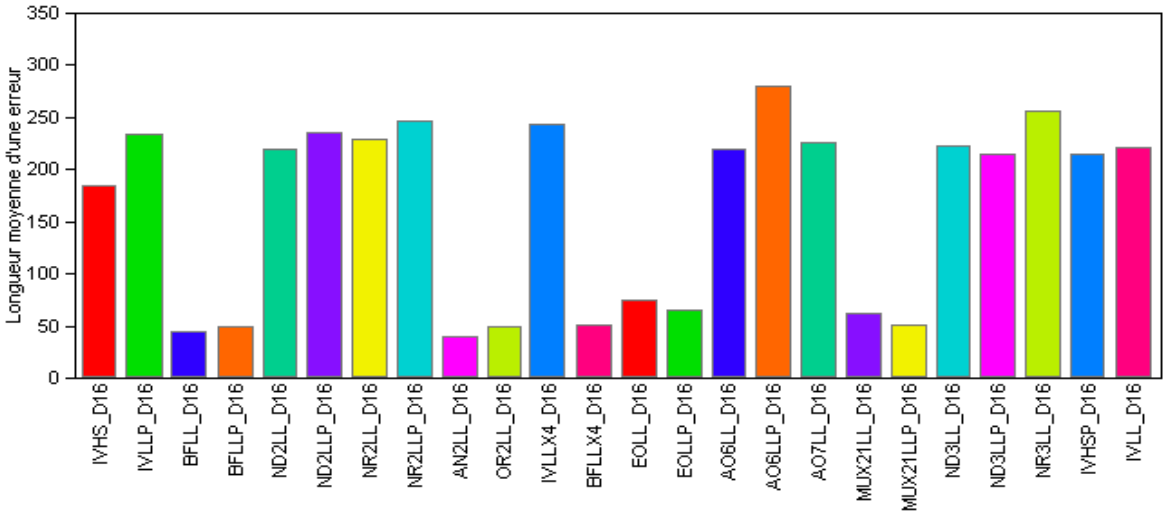


Figure 51: Longueurs moyennes en bits des impulsions générées par un tir laser.

4.4.2.1 Durée des impulsions dans les cellules non-inverseuses

Une explication plausible à ce phénomène peut être proposée. Dans le cas d'un tir laser sur une porte logique, si l'ouverture du faisceau est plus grande que la porte elle-même le laser va affecter l'intégralité des transistors de la porte. Ceci est le contraire du modèle d'injection de faute utilisé dans le cas des impacts de particule où l'approche classique consiste à injecter une impulsion de courant sur le drain d'un seul transistor de la cellule étudiée.

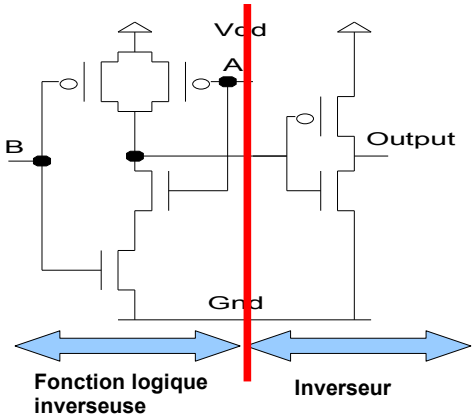


Figure 52: Schéma électrique d'une porte AND.

Dans le cas d'une fonction logique inverseuse, tous les transistors sont susceptibles d'être affectés et l'impulsion résultante est propagée en sortie. Les portes non-inverseuses quant à elles sont construites à partir d'une fonction logique inverseuse (pour la fonction AND, la base est une porte NAND) à laquelle est branchée un inverseur en sortie, comme sur la figure 52. Ce type de schéma électrique donne aux transistors du même type (respectivement P et N) une polarisation opposée durant le fonctionnement normal de la porte. Une perturbation identique introduite dans tous les transistors de même type à l'intérieur de la porte va donc entraîner des effets antagonistes sur l'état logique de la sortie.

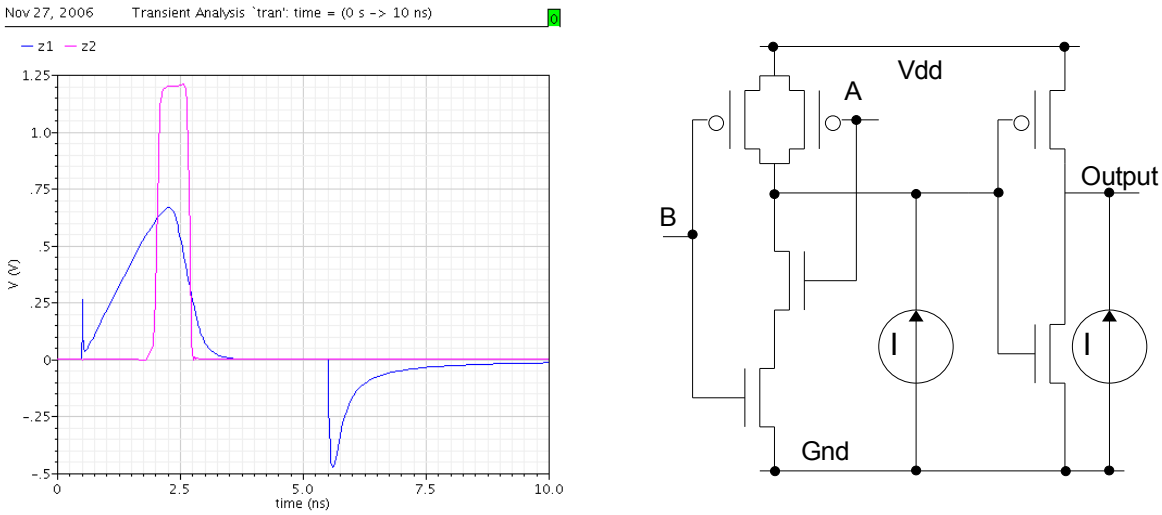


Figure 53: Simulation Spice de l'injection d'un courant dans tous les transistors P d'un porte logique AND.

Nous avons réalisé des simulations Spice de ce type d'injection (figure 53) qui montrent que la tension résultante au point de sortie de la porte est constituée d'impulsions parasites relativement courtes devant la durée de la perturbation. Ceci est à comparer avec une impulsion résultant de l'injection d'une perturbation sur un seul transistor de la porte, dont la longueur suit la durée d'injection du courant.

Les effets antagonistes sur la sortie de la porte non-inverseuse devraient être plus à même de provoquer une instabilité dans l'état de la sortie de la porte, ce qui peut amener un tir laser à provoquer plus d'une erreur en même temps. On peut en effet remarquer sur la figure 54 que le nombre moyen d'erreurs mesurées dans les cellules non-inverseuses (1.8 erreur par tir) est plus élevé que celui mesuré dans les cellules inverseuses (1.5 erreur par tir).

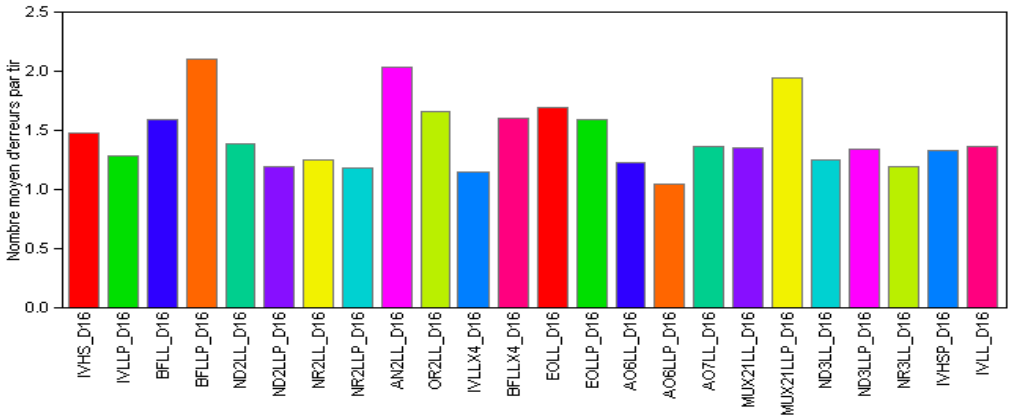


Figure 54: Nombre moyen d'erreurs par tir pour des motifs D16.

4.4.2.2 Sensibilité relative des cellules de la technologies ST

La figure 55 nous montre le rapport entre la longueur cumulée des impulsions mesurées par le circuit PROBES et le nombre total de tirs efficaces sur des cibles à 16 cellules. On retrouve la séparation entre cellules inverseuses et non inverseuses. On remarque aussi que les différences de performance entre portes du même type (inverseuses et non-inverseuses) sont beaucoup moins marquées que dans la figure 51. Les cellules non-inverseuses sont donc en moyenne 3 fois moins sensibles aux perturbations provoquant une impulsion positive en sortie de la porte logique.

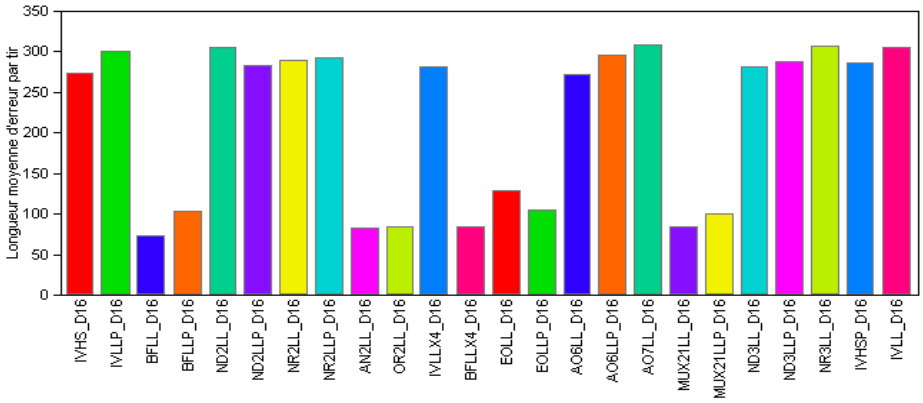
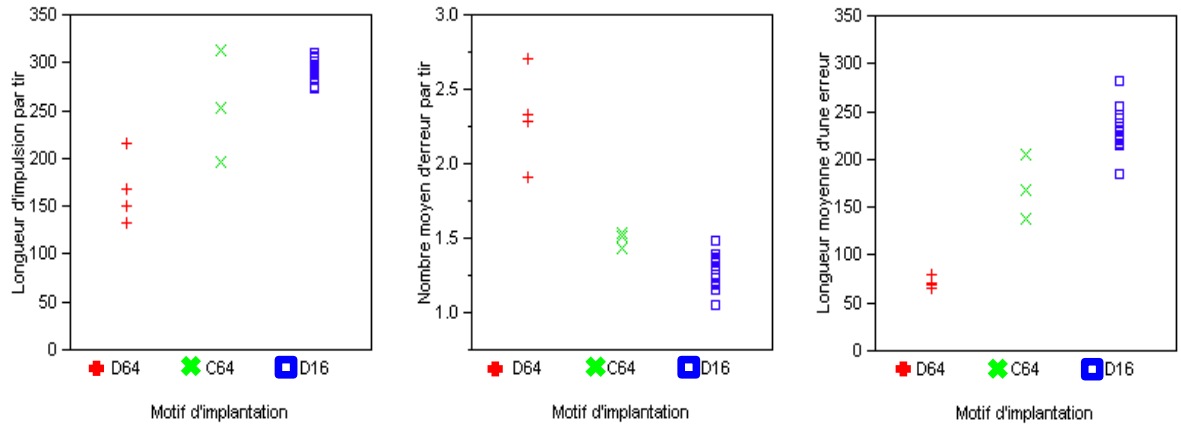


Figure 55: Rapport de la longueur en bits des impulsions sur le nombre d'expériences efficaces pour des tirs laser sur des surfaces sensibles à 16 cellules.

4.4.2.3 Influence du motif des surfaces sensibles sur la durée des impulsions

La figure 56 montre la répartition des caractéristiques des impulsions générées dans les cellules sensibles en fonction du motif d'implantation. Nous prenons pour référence le motif D16 qui a été analysé ci-dessus. Seules des portes inverseuses ont été implantées dans les structures à 64 portes.



(a) Sensibilité globale *(b) Nombre d'erreurs par tir* *(c) Durée moyenne des erreurs*

Figure 56: Caractéristiques des impulsions mesurées sur des portes inverseuses selon le motif d'implantation.

On remarque que les structures C64 provoquent des erreurs un peu moins longues mais légèrement plus nombreuses que les structures D16. Nous n'assistons donc pas aux recombinaisons prévues lors de la conception de cette structure. Les erreurs ne sont ni plus longues ni plus nombreuses que dans des structures plus dispersées telles que les D16.

Les structures D64 provoquent des erreurs très courtes comparativement aux autres structures. Leur durée est semblable à celle des portes non-inverseuses des structures D16. De plus, le nombre d'erreurs par tir est très important. Au final, la sensibilité des structures D64 est légèrement inférieure à celle des structures D16, pourtant moins denses en portes. On peut expliquer ce phénomène par le fait que les portes sont groupées 4 par 4 en îlots plus denses que les structures D16. Ceci génère plus d'interactions entre les cellules touchées par le tir laser. Par ailleurs, tous les groupes D64 observables au microscope sont partiellement masqués par les rails d'alimentation (opaques au rayonnement laser), ce qui peut conduire deux portes

consécutives sur le chemin de données à réagir très différemment (par exemple, l'une étant illuminée, l'autre masquée).

4.4.2.4 Influence du paramètre de sortance des portes sur la durée des impulsions

Plusieurs fonctions logiques ont été implantées avec des sortances différentes, les sortances 2 et 4 étant repérées par les suffixe P et X4 respectivement. La figure 57 montre les résultats des tests menés sur ces portes. Il est difficile de se prononcer sur l'influence de ce facteur, tant les résultats divergent d'une fonction logique à une autre.

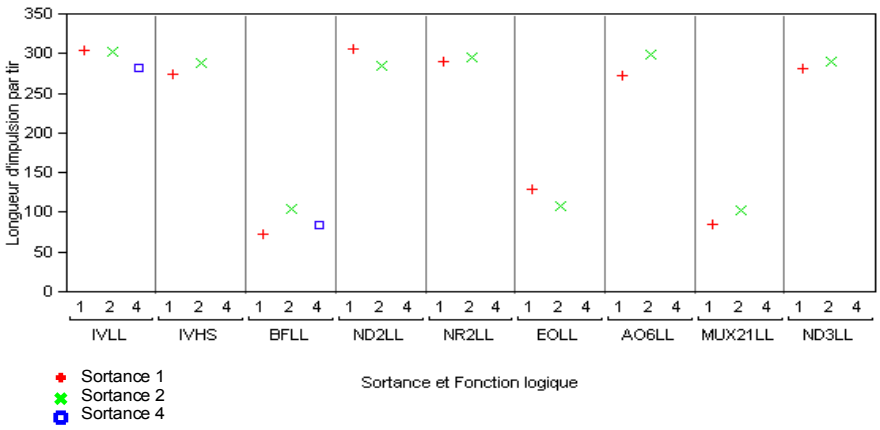


Figure 57: Sensibilité des portes logiques par rapport à leur sortance

4.4.2.5 Influence des paramètres technologiques des portes sur la durée des impulsions

Nous avons placé dans l'une des surfaces sensibles, des portes en technologie haute vitesse (HS), et des portes en technologie basse consommation (LL) dans toutes les autres. La figure 58 montre que l'inverseur HS est moins sensible en moyenne que l'inverseur LL. Les règles de dessin semblent donc influer sur la sensibilité d'une cellule aux perturbations laser.

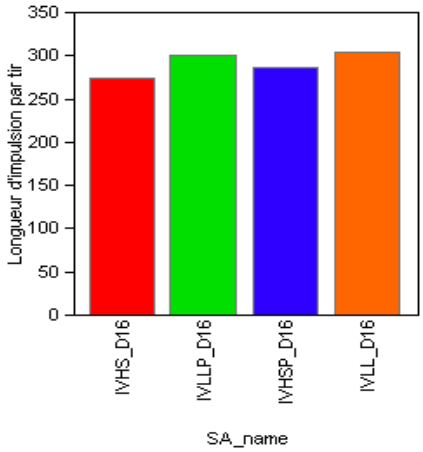


Figure 58: Sensibilité des portes IVHS et IVLL.

Nous n'avons cependant pas collecté assez de données pour pouvoir affiner cette analyse, vu que nous n'avons implanté qu'un seul type de porte dans la technologies HS.

4.4.3 Vers une nouvelle architecture des surfaces sensibles

Les surfaces sensibles ont été conçues sur la base d'un modèle qui s'avère être insuffisant pour décrire l'intégralité des phénomènes expérimentaux observés. Les nouvelles hypothèses introduites au paragraphe 4.4.2 ne peuvent pas être validées avec les fonctionnalités du circuit actuel. Elles nécessitent donc une nouvelle architecture des surfaces sensibles capable de mettre en évidence d'autres phénomènes.

Nous avons observé des disparités de comportement entre les portes inverseuses et non-inverseuses, mais nous n'avons pas été en mesure de mesurer la part due à la polarisation des portes dans leur sensibilité car toutes nos surfaces sensibles ont été conçues avec une polarisation identique configurée pendant la conception. Il est intéressant d'explorer cette voie car les transistors sensibles de la porte logique changent suivant sa polarisation. Implanter un moyen de reconfigurer les polarisations des portes pendant le fonctionnement du circuit est une fonctionnalité majeure à insérer dans les spécifications du prochain circuit.

Nous avons aussi noté que les paramètres technologiques avaient une influence sur la sensibilité des portes, mais avec une seule surface sensible dédiée à un autre procédé de fabrication nous n'avons pas assez de données pour valider cette observation. Il serait intéressant d'étendre de

prochaines expériences en implantant plusieurs surfaces sensibles différentes pour chaque procédé.

Enfin, nous n'avons pas été en mesure de déterminer avec précision le nombre de portes frappées par le tir laser car les ouvertures pratiquées dans les dummy cells ne couvraient pas l'intégralité de la surface sensible et la grille d'alimentation couvrait certaines cellules. Dans l'optique d'un futur circuit il est impératif de placer les cellules dans les trous de cette grille d'alimentation pour éviter ces phénomènes de bouclier. En outre, les caractéristiques du laser doivent guider l'écartement des cellules dans une même surface sensible pour pouvoir choisir avec précision le nombre de cellules illuminées. En effet, les résultats obtenus sur le circuit PROBES Laser sont teintés d'une imprécision due au fait que la fenêtre de tir la plus petite disponible (25 μm^2) touche plusieurs portes en même temps.

En conclusion il est nécessaire de concevoir un nouveau circuit PROBES Laser sur la base de ces observations pour clarifier les points ci-dessus.

4.4.4 Influence des couches parasites du flot de conception

Dans les technologies actuelles, il est impératif de respecter une certaine densité de matière pour chaque couche par unité de surface car les couches successives de métaux et d'oxyde doivent être déposées de manière très précise. En effet, de petits défauts de planarité au moment de la lithogravure peuvent entraîner par parallaxe une déformation des motifs à graver. Il est donc obligatoire de remplir les couches non utilisées avec des motifs factices (dummy cells) pour respecter les règles de conception. De plus, les technologies modernes possèdent de plus en plus de possibilité d'interconnexion (les niveaux de métallisation) qui s'empilent au dessus des couches de silicium actives (la technologie ST que nous avons utilisé pour le circuit PROBES en comporte 6).

Ces contraintes techniques entraînent une dissimulation des couches sensibles du circuit par des couches parasites en théorie opaques au rayonnement laser. Pour évaluer l'effet de ces couches parasites, nous avons placé sur les surfaces sensibles du circuit PROBES des zones libres de toute protection et d'autres conservant toutes les couches parasites associées à la technologie utilisée. On peut voir la une photographie d'une surface sensible prise au microscope sur la

figure 59. L'intérieur de l'image est semé de petites stries verticales qui délimitent les rangées de placement des cellules et leur alimentation. On voit de plus au dessus un quadrillage épais qui correspond à la grille d'alimentation du circuit et un motif fin en escalier qui correspond aux interconnexions entre cellules ponctué par un carré à l'emplacement de la cellule. Enfin à l'extérieur de cette zone on voit les zones qui correspondent aux cellules factices. Le trou dans les couches parasites ne couvre pas la totalité de la surface sensible.

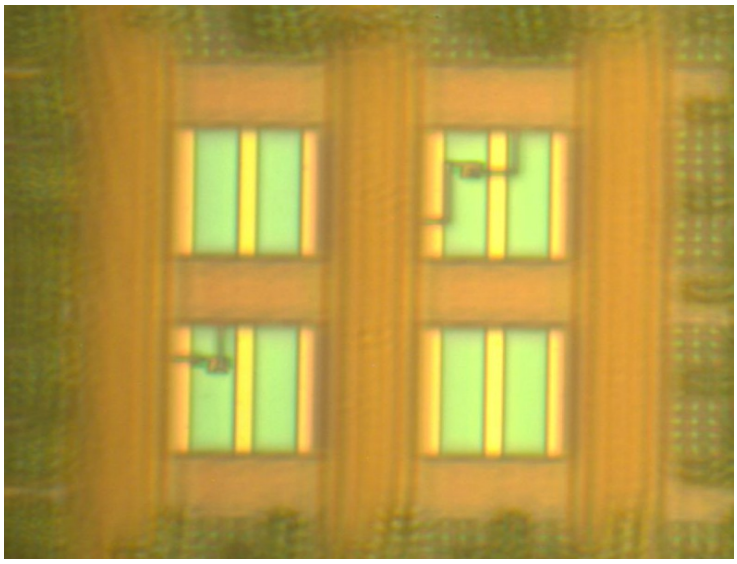


Figure 59: Exemple d'ouverture dans les couches parasites pour une surface sensible du circuit PROBES.

En regardant l'ensemble du circuit (figure 60) on voit les 31 trous dans les couches parasites que nous avons placé au dessus des surfaces sensibles. Sur chaque surface sensible nous avons donc une partie se trouvant sous le trou, et une partie encore protégée. La figure 61 montre les effets de ces couches parasites dans la sensibilité d'une zone de tir face à des impulsions laser. Chaque tir prend pour cible un carré de 5 µm de côté et nous balayons un carré de 100 µm de côté.

Sur le schéma, la zone comportant des cellules logiques est un carré de 80 µm de côté représentée par le carré externe, alors que le trou ouvert dans les couches parasites est représenté par le petit carré aux coordonnées (30,120) et (75,160)). On voit que le circuit ne réagit aux tirs laser que sur la zone découverte. On distingue aussi facilement le quadrillage de la grille d'alimentation qui offre une très bonne protection aux cellules se trouvant en dessous.

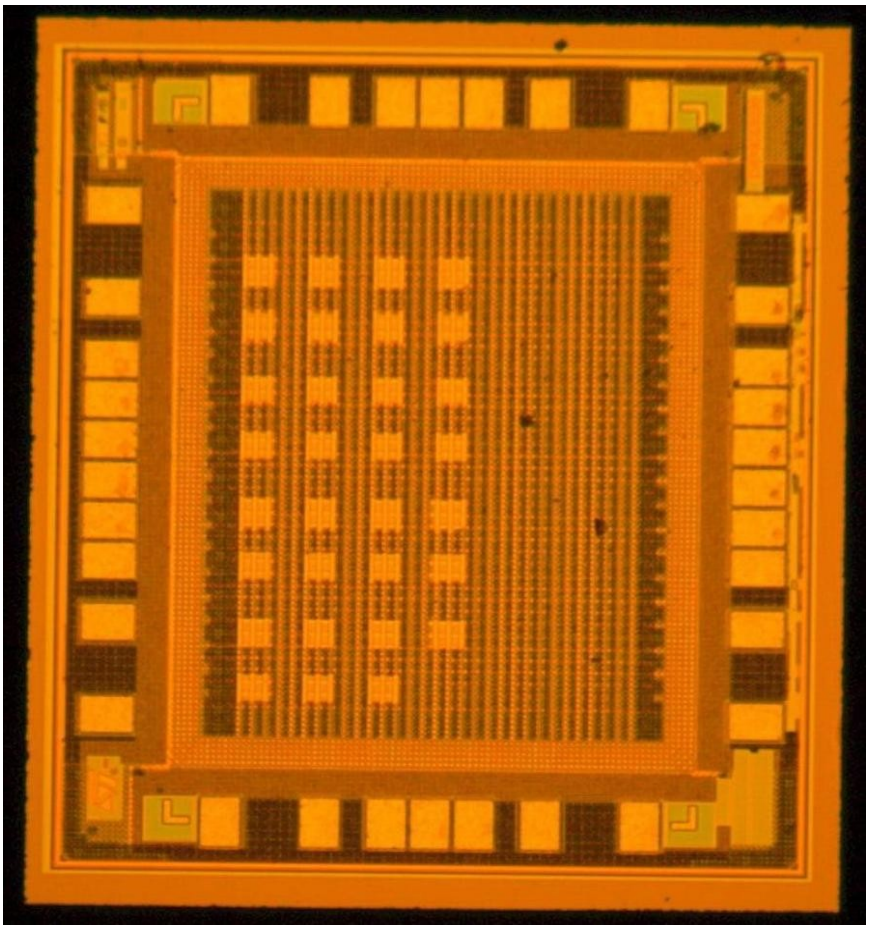


Figure 60: Photographie du circuit PROBES.

Un test de puissance réalisé sur un rail d'alimentation a d'ailleurs prouvé que les rails d'alimentation étaient totalement opaques au rayonnement laser utilisé et que les portes situées en dessous ne généraient aucune impulsion jusqu'à destruction du rail d'alimentation.

Quand nous essayons de traverser les couches parasites du circuit PROBES, nous augmentons graduellement la puissance du laser jusqu'à obtenir des impulsions provenant des portes situées sous la couche parasite. La puissance utilisée pour obtenir ces impulsions provoque cependant la destruction du circuit pour les couches non protégées. La puissance utilisée pour traverser les couches protectrices du circuit PROBES est environ 3 fois plus élevée que celle utilisée pour provoquer des impulsions dans les cellules découvertes.

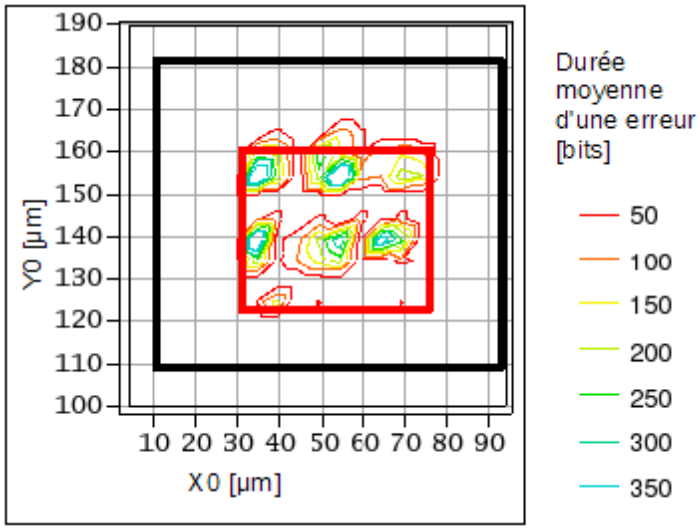


Figure 61: Carte de sensibilité d'une zone de tir.

4.5 Attaques laser et techniques de protection

4.5.1 Faiblesses des techniques de protection habituelles

Les techniques de protection contre les erreurs transitoires classiques se basent sur les propriétés d'apparition de ces erreurs. En effet, il est admis qu'une perturbation apparaissant dans un circuit intégré perdra son caractère transitoire (i.e. sera stockée dans un point de mémorisation ou bien se sera évanouie) avant qu'une autre perturbation n'apparaisse. Les protections utilisent cette propriété pour détecter l'erreur et tenter de la corriger. Nous allons montrer que la source laser peut mettre en défaut ces techniques de protection.

- Redondance d'information

Le rayon laser est une source pouvant irradier une surface conséquente d'un circuit avec une grande efficacité. On peut donc générer des perturbations simultanées en plusieurs endroits du circuit qui mettent à mal les algorithmes de détection et de protection du circuit. De manière générale tout code correcteur appliqué à un circuit pourra être saturé par le grand nombre d'erreurs créé par un seul tir laser. Cependant, les erreurs apparaissant un peu au hasard dans la fenêtre de tir, le code correcteur pourra souvent détecter une perturbation, même sans pouvoir la corriger.

L'implantation d'un code détecteur puissant en association avec un module de redémarrage du système très protégé peut donc être une bonne source de protection pour un circuit à vocation sécuritaire.

- Redondance temporelle

Comme on l'a vu, les techniques de protection basées sur la redondance temporelle ont une capacité de protection qui ne dépasse pas l'écart séparant deux calculs successifs. Dans le cas classique où les deux calculs sont séparées par une fraction de la fréquence d'horloge, des erreurs de quelques nanosecondes, comme nous en avons généré dans le circuit PROBES, seront largement capables de saturer la protection. De plus, la stabilité des erreurs sur toute la durée du tir laser pourront tromper le comparateur et faire croire à un calcul juste.

Cette technique est donc à proscrire de manière générale, sauf dans le cas de calculs très longs où le logiciel commandant le circuit demande une vérification du calcul au moins plusieurs microsecondes après le résultat du premier.

- Redondance spatiale

Dans le cas d'un système de redondance spatiale implanté sur un unique circuit (deux coeurs identiques unis par un mécanisme de vote), un tir laser couvrant les deux coeurs peut saturer le mécanisme de correction d'erreur. Par contre, le comparateur pourra détecter une anomalie sans pouvoir la corriger vu que les erreurs produites seront souvent différentes d'un coeur à l'autre.

- Utilité de ces techniques de protection

Comme on vient de le voir, ces techniques ne sont en aucun cas infaillibles devant une attaque laser. Cependant, ces techniques augmentent la difficulté d'une attaque en détectant certaines perturbations, et donc en diminuant le taux nombre d'erreurs exploitables sur nombre d'attaques. Elles rendent donc l'exploitation des résultats plus hasardeuse, ce qui augmente encore le coût de l'attaque.

Placer des protections de ce genre à plusieurs endroits clefs de l'architecture peut gêner considérablement un attaquant en augmentant considérablement le temps et le nombre de tirs nécessaires à l'obtention des informations confidentielles.

4.5.2 Stratégie de protection adaptée aux attaques laser

4.5.2.1 Vers une stratégie de déni de fonctionnement

Pour certaines applications sécuritaires il est primordial que l'intégrité de fonctionnement du système soit préservée, même aux dépends éventuels de l'utilisateur. Par exemple, une clé de code bancaire pourra être réinitialisée si elle détecte une perturbation de son mode de fonctionnement normal. Le temps de remise en marche n'excédant pas une dizaine de secondes, le désagrément pour l'utilisateur en cas de perturbation temporaire et fortuite du système (par exemple par un impact de particule) n'est pas excessif.

Par contre, pour l'attaquant cette stratégie de protection est extrêmement contraignante car elle vise à lui refuser tout moyen d'exploiter ses résultats. Cela lui place une contrainte supplémentaire obligatoire sur ses tirs, celle de ne pas être détecté.

Bien sûr, l'attaquant peut essayer de saturer les détecteurs (come le fait de créer des erreurs de multiplicité paire dans un code de parité) mais cette stratégie nous épargne le besoin d'implanter des structures de correction d'erreurs qui sont à la fois lourdes à mettre en place et facile à déjouer.

4.5.2.2 Stratégie de détection distribuée

Pour éviter que le pirate puisse détourner facilement une structure de protection basée sur la redondance (par exemple en attaquant le comparateur final), on peut concevoir des systèmes de détection distribués dans lesquels le concepteur implante en plusieurs endroits du circuit de petites structures très simples de détection d'éventuelles perturbations.

Si ces structures sont bien dispersées à coté des zones les plus sensibles du circuit, il sera très difficile à l'attaquant de les éviter tout en créant une perturbation qui serait exploitable en sortie. Si ces détecteurs ont tous le pouvoir de stopper le calcul et de réinitialiser le système, on se

rapproche d'une stratégie de protection efficace. Il reste donc à protéger très lourdement un bloc centralisant les signaux de tous ces détecteurs, et commandant par exemple un signal de coupure de l'alimentation interne au circuit.

Dans l'ensemble cette stratégie permet de déplacer le problème de la protection par redondance à partir de la partie fonctionnelle du système vers une série de modules dédiés. Le taux de couverture de fautes serait donc directement proportionnel à la densité de ces modules détecteurs (une dizaine de portes logiques par détecteur tout au plus) dans le plan de masse du circuit. Le concepteur n'a donc pas à changer en profondeur l'architecture du circuit et peut implanter une protection aussi efficace que possible en prenant en compte les coûts de surface.

Cette stratégie à l'avantage d'être économe en énergie (les structures de détection ne s'activent qu'en cas d'attaque), de ne pas pénaliser les performances du système (à part sur d'éventuelles fausse alertes) et enfin de ne pas modifier l'architecture du circuit. On peut implanter ces modules au niveau de la phase de placement-routage comme des blocs de propriété intellectuelle et placer le reste du circuit autour, ce qui s'insère très facilement dans un flot de conception classique. Le module final devra par contre utiliser des spécifications de protection matérielles et fonctionnelles très strictes, mais comme c'est un module très simple cette protection ne sera pas vraiment pénalisante pour le circuit.

4.5.3 Techniques de conception pour un circuit résistant aux attaques laser

D'après notre expérience dans la mise en place d'attaques laser dans le cadre du projet Duracell, nous pouvons proposer quelques astuces de conception qui augmenteront à moindre coût les facultés d'un circuit à résister aux attaques laser.

4.5.3.1 Choix de la couverture du circuit par les cellules factices

Dans les technologies modernes, l'implantation des différentes couches de matière ne peut se faire de manière localisée à cause de problèmes de régularité et d'empilement des masques. Ce problème est résolu par l'utilisation de cellules factices (les dummy cells ou dummies) pour remplir la totalité de chaque couche et ainsi homogénéiser la répartition de matière dans l'axe

vertical. Les règles d'implantation des dummies sont données en terme de densité minimum de matière par unité de surface ce qui laisse tout de même une certaine liberté au concepteur.

L'avantage de ces dummies est qu'elles se comportent comme un blindage face aux attaques laser, blindage qui peut être contourné en utilisant une énergie plus élevée pour le laser. Le risque avec l'augmentation de l'énergie laser est que les circuits peuvent facilement être détruits en cas de surexposition, ce qui contrecarrerait les vues d'un éventuel attaquant. Dans cette optique le concepteur pourrait ménager des zones de forte sensibilité dans son circuit pour qu'elles se comportent comme des sortes de fusibles garantissant qu'une cartographie classique de la surface du circuit (méthode utilisée pour trouver des points faibles lors d'une première approche d'un circuit) aboutisse à sa destruction.

Bien sûr, les zones de forte sensibilité devront être cachées à la vue de l'observateur par la plus haute couche de cellules factices ou la passivation pour éviter qu'une simple analyse optique du circuit révèle les zones « fusibles ». Cependant un attaquant disposant d'un grand nombre de pièces pourra apprendre à éviter de détruire les zones de haute sensibilité en adaptant la puissance de son laser.

4.5.3.2 Optimisation de l'effet protecteur des rails d'alimentation

Dans les différentes cartographies laser du circuit PROBES, on voit clairement un quadrillage qui correspond (après observation au microscope) aux rails d'alimentation des cellules du circuit.

Après test, nous avons observé que ces rails sont totalement opaques au laser, à tel point qu'une augmentation conséquente de l'énergie du laser les détruira plutôt que de provoquer des erreurs dans les cellules placées sous ces rails. Le concepteur peut donc utiliser cette propriété pour optimiser la couverture des zones sensibles d'un circuit par un blindage infranchissable par face avant. Cela nécessite par contre une intervention lourde pendant l'étape physique (placement-routage, génération des masques) du flot de conception. En outre une attaque par face arrière à l'aide d'un laser infrarouge réduira à néant l'efficacité de cette technique.

4.6 Conclusion

Dans ce chapitre j'ai montré que le circuit PROBES Laser est fonctionnel et qu'il possède des caractéristiques qui en font un outil performant adapté à la mesure de la durée des perturbations générées par un tir laser. Les différences de comportement des portes combinatoires de la technologie ST HCMOS9GP 0.13 µm ont aussi été étudiées.

Le résultat de cette campagne de tests a été de proposer diverses méthodes aidant à protéger au niveau physique un circuit moderne face aux attaques laser, avec leurs avantages et leurs inconvénients.

J'ai aussi proposé de nouvelles architectures de surfaces sensibles servant à vérifier les diverses hypothèses qui peuvent lui être apportées pour augmenter encore son apport à la compréhension de ce phénomène. Ce circuit peut être utilisé pour aider les concepteurs à trouver quelles portes logiques sont les plus sensibles aux attaques et à connaître les profils des erreurs qui seront produites par un tir laser sur leur circuit.

Un nouveau circuit PROBES Laser est ainsi nécessaire pour valider les nouvelles hypothèses de génération des perturbations proposées et pour tester les astuces de conception et la stratégie sécuritaire proposée.

Conclusion et perspectives

La conception de circuits sécuritaires, spécifiquement les cartes à puces, est un domaine en évolution permanente. Les concepteurs tentent de contrecarrer les nouveaux types d'attaques utilisés par les hackers afin d'obtenir les informations confidentielles qui y sont stockées. C'est aussi un domaine où la pression concurrentielle est très forte et où les volumes en jeu sont tels que les contraintes de coûts sont draconiennes. Ceci étant posé, il est nécessaire d'une part de développer des techniques très avancées de contre mesure et d'autre part de standardiser ces dernières au maximum. Dans cette optique, proposer des protections efficaces qui s'intègrent dans les flots de conception classiques et conçues en cellules de bibliothèque standard est un besoin essentiel de l'industrie. À ce jour, les attaques documentées les plus pointues se basent sur l'injection de fautes transitoires dans un circuit sécuritaire, les plus efficaces utilisant des sources contrôlables finement comme le laser.

Ces attaques sont basées sur les études concernant les perturbations transitoires dans les circuits intégrés, un domaine intéressant les chercheurs depuis les années 80. Ce domaine s'est développé avec la recherche de sources de perturbations fiables pouvant se substituer aux accélérateurs de particules utilisés pour reproduire l'impact des particules cosmiques sur les circuits intégrés. La source laser a été reconnue comme une source contrôlable très précisément, à la fois aux niveaux spatial et temporel. Cette source est donc efficace pour perturber de manière très précise les circuits intégrés. Les pirates se sont donc inspirés de ce domaine de recherche pour établir des méthodologies d'attaques des circuits intégrés par injection de fautes.

Partant de ces faits, cette thèse a été mise en place pour étudier ces moyens de perturbation et leurs effets sur des technologies récentes. Elle est le fruit d'une collaboration entre le laboratoire LICM de l'université Paul Verlaine de Metz et la société iRoC Technologies. Le travail s'est appuyé sur le projet Duracell financé par le RNRT. Ce projet a regroupé le laboratoire TIMA et les sociétés Thales (conception de circuits sécuritaires), Gemplus (fournisseur de cartes à puces) et iRoC Technologies (conception d'architectures tolérantes aux fautes).

Dans le premier chapitre, les divers environnements radiatifs auxquels peuvent être soumis les circuits ainsi que les sources de radiations qui peuvent y être attachées ont été introduits. Il a été vu que chaque type de radiation interagit de manière spécifique avec les matériaux entrant

dans la conception des circuits électroniques et que le risque de faute lié à cette interaction dépend à la fois des caractéristiques propres à la particule et au matériau. Les perturbations provoquées par ces sources provoquent une accumulation de courant dans le ou les noeuds frappés ce qui provoque des perturbations dans les portes combinatoires et séquentielles du circuit. Les erreurs logiques peuvent générer plusieurs types d'effets permanents ou passagers, réversibles ou irréversibles qui ont été passés en revue. J'ai mis en avant les spécificités de la source laser et de son interaction avec le silicium, et j'ai élaboré une représentation des perturbations générées par le laser ne prenant en compte que la durée de l'impulsion.

Dans le chapitre 2, j'ai présenté une analyse des conséquences de l'évolution technologique sur les principaux paramètres des circuits intégrés dans laquelle j'ai montré que l'immunité au bruit des structures CMOS diminuait constamment avec la réduction d'échelle. Les différents modes d'attaques des circuits sécuritaires ont été exposés, comme l'analyse différentielle de consommation (ou DPA) et l'analyse différentielle de fautes (ou DFA), ainsi que les différents points d'injection de fautes dans un circuit.

La stratégie sécuritaire a aussi été au coeur de mes recherches. Pour cela, j'ai exploré la problématique consistant à protéger les circuits du mieux possible au plus faible coût. J'ai ensuite décrit les 3 niveaux de protection d'un circuit (la redondance temporelle, la redondance d'information et la redondance spatiale) avant de présenter différents types de protection contre les erreurs transitoires. Je conclus sur l'impossibilité de garantir à 100% la résistance aux attaques d'un circuit moyennement complexe vu les modes d'action à la disposition des attaquants. Par conséquent, des méthodes de protection faciles à implanter et proposant une action large spectre ont été proposées dans le but de maximiser le ratio coût de l'attaque sur coût de l'implantation.

Le chapitre 3 a traité de la conception de circuits de type PROBES dédiés d'une part à la mesure de la durée des impulsions générées par un tir laser sur des structures CMOS et d'autre part, à la mesure de sensibilité d'une technologie CMOS aux perturbations provoquées par des sources laser et plus généralement radiatives. J'ai développé une méthodologie de conception de circuits permettant à la fois de réduire les coûts de fabrication et de maîtriser l'implantation physique du circuit. Cette méthodologie m'a permis de concevoir un échantillonneur ayant une résolution inférieure à 30 ps dans la technologie cible. De plus, j'ai proposé des structures provenant de

cellules de la librairie standard aptes à capturer des impulsions très courtes et ai évalué leur sensibilité.

Dans le chapitre 4, cette méthodologie a été validée par le biais d'une plate-forme de mesure que j'ai mis en place pour réaliser des tirs laser sur les surfaces sensibles du circuit. Ces expériences ont montré que le circuit de test était totalement fonctionnel et avait une résolution de 23.78 ps. J'ai aussi mesuré les altérations que font subir les différentes structures combinatoires aux impulsions les traversant. Les tirs laser effectués sur les surfaces sensibles du circuit ont aussi montré que les impulsions générées dans les portes inverseuses ont une durée d'environ 6.5 ns, soit un peu plus que la durée de l'impulsion laser. Les mêmes tirs laser produisent des impulsions plus courtes (environ 2 ns) dans les portes non-inverseuses à cause d'effets antagonistes entre l'étage logique et l'inverseur de sortie. Il a aussi été constaté que le faisceau laser touchait plusieurs portes en même temps, entraînant du bruit sur les données récoltées. Cependant, j'ai pu dégager quelques astuces de conception diminuant la sensibilité des circuits aux attaques laser tout en étant peu onéreuses et faciles à implanter. J'ai finalement proposé une stratégie de protection des circuits face aux attaques laser qui s'appuie sur l'implantation de modules simples (une dizaine de portes logiques) sur l'ensemble du circuit permettant de détecter des perturbations. Ces modules produisent un signal qui permet de réinitialiser le système, ceci empêchant l'attaquant de récupérer des informations confidentielles.

En conclusion, dans cette thèse j'ai réuni le domaine de la conception de circuits sécuritaires et celui de la conception de circuits robustes aux erreurs transitoires. Cette approche m'a permis de comparer les types d'erreurs potentiels dans les deux types de circuits et de proposer des méthodologie de conception très efficaces pour des circuits de mesure imposant très peu de tolérance sur les interconnexions. Cette méthodologie est par ailleurs très adaptée aux circuits fortement redondants. En me basant sur cette méthodologie, j'ai réalisé deux circuits PROBES, le premier destiné à l'analyse des effets du laser sur des portes logiques de la technologie STM HCMOS9GP 0.13 µm et le second mesurant la sensibilité de cette technologie aux impacts de particules. Le premier circuit a subi tout une campagne de tirs laser qui m'a permis de mettre en évidence la différence de comportement entre les chaînes de cellules inverseuses et non inverseuses. Il apparaît qu'une chaîne de cellules de type inverseuses a tendance à stabiliser la longueur d'une impulsion se propageant à travers elle, alors que la même chaîne de portes non-

inverseuses produira des impulsions plus courtes. En parallèle j'ai exploité les propriétés de blocage du rayonnement laser des cellules factices et des rails d'alimentation pour proposer quelques astuces de conception qui rendent un circuit plus résistant aux attaques.

Dans la suite proche, nous aimerions revoir la conception des surfaces sensibles du circuit PROBES Laser pour créer des surfaces de tir comportant une unique cellule pour mieux mesurer la longueur des impulsions créées, ou encore pour pouvoir contrôler la polarité des portes non-inverseuses. De plus il faudrait augmenter la base de données de résultats pour obtenir de meilleurs statistiques et éliminer certains artefacts de mesure. Les architectures de circuit proposées sont simples à transposer sur de nouvelles technologies et il serait intéressant de comparer les résultats obtenus sur cette technologie 0.13 µm avec ceux d'une technologie 90 nm voire 65 nm par exemple.

Ce travail ouvre la voie à de nouvelles recherches, comme par exemple l'étude en profondeur du comportement de structures de portes logiques pour les classer et les corréler avec les résultats du laser. En effet la structure des portes logiques influe sur la collection des charges créées par le laser dans le silicium et l'exploration de ces possibilités peut conduire à de grandes avancées dans le domaine de la conception de bibliothèques logiques. Un autre domaine est aussi ouvert avec l'amélioration des structures de test PROBES qui pourraient bénéficier d'une automatisation de la conception plus importante et d'améliorations au niveau de l'architecture générale. Un nouveau circuit PROBES pourrait aussi utiliser les pistes données pour la conception de nouvelles surfaces sensibles capables de corroborer les hypothèses émises dans le dernier chapitre. Il serait profitable d'étudier sérieusement les possibilités d'utilisation du routage des signaux d'alimentation comme boucliers contre les attaques par rayonnement. Il serait intéressant d'étudier les spécifications des technologies actuelles pour proposer des règles précises de conception et proposer une aide automatisée au routage s'intégrant dans les flots de simulation standards. Enfin, il est important de valider la stratégie de protection qui a été proposée en concevant les modules de détection appropriés et en développant une méthodologie efficace de durcissement du module final.

Références

[ALE02] D. Alexandrescu, L. Anghel, M. Nicolaidis, « Simulating single event transients in VDSM ICs for ground level radiation », Journal of Electronic Testing: Theory and Applications, Vol. 20, 2004, pp. 413-421.

[ALL94] M. Allenspach, J.R. Brews, I. Mouret, R.D. Schrimpf, K.F. Galloway, « Evaluation of SEGR threshold in power mosfets », IEEE Trans. Nucl. Sci., Vol. NS-41, 1994, pp. 2160-2166.

[ALL96] M. Allenspach, C. Dachs, G.H. Johnson, R.D. Schrimpf, E. Lorfèvre, J.M. Palau, J.R. Brews, K.F. Galloway, J.L. Titus, and C.F. Wheatley, « SEB and SEGR in N-channel power mosfets », IEEE Trans. Nucl. Sci., Vol. NS-43, No. 6, 1996, pp. 2927-2931.

[AND97] R. Anderson, M. Kuhn, « Low cost attacks on tamper resistant devices », in Proc. 5th Int. Workshop on Security Protocols, 1997, pp. 125-136.

[AND01] R. Anderson, « Security engineering : a guide to building dependable distributed systems », Ed. Wiley, 2001.

[ANE00] G.M. Anelli, « Conception et caractérisation de circuits intégrés résistants aux radiations pour les détecteurs de particules du LHC en technologies CMOS sub-microniques profondes », Thèse de doctorat, INP Grenoble, 2000.

[ANG00] L. Anghel, « Les limites technologiques du silicium et tolérances aux fautes », Thèse de doctorat, INP Grenoble, 2000.

[BAR95] C. Barillot, « Anomalies observées en vol », Cours RADECS, Arcachon, 1995.

[BAR04] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, C. Whelan, « The sorcerer's apprentice guide to fault attacks », Workshop on Fault Diagnosis and Tolerence in Cryptography, in association with DSN 2004, Florence, Italy, June 2004, Disp. @ http://eprint.iacr.org/2004/100.

[BAU00] R.C. Baumann, E.B. Smith, « Neutron-induced boron fission as a major source of soft errors in deep submicron SRAM devices », in Proc. of IEEE Int. Reliability Physics Symp., San Jose, USA, 2000, pp. 152-157.

[BAU01] R. Baumann, « Silicon amnesia - terrestrial effects », Short courses in 6th European Conf. RADECS, Grenoble, France, 2001, p. I.

[BAZ97] M.P. Baze, S.P. Buchner, « Attenuation of single event induced pulses in CMOS combinational logic », IEEE Trans. Nucl. Sci., Vol. NS-44, 1997, pp. 2217-2223.

[BID01] C. Bidan, P. Girard, « La sécurité des cartes à microprocesseur », Revue de l'électricité et de l'électronique (REE), No. 5, Mai 2001, pp. 60-65.

[BIH96A] E. Biham, A. Shamir, « A new cryptanalytic attack on DES », October 18, 1996 (DRAFT).

[BIH96B] E Biham, A Shamir, « DFA: Identifying the structure of unknown ciphers sealed in tamper-proof devices », preprint, 10/11/1996.

[BIH97] E. Biham, A. Shamir, « Differential Fault Analysis of Secret Key Cryptosystems », in Proc. Advances in Cryptography Conf. - CRYPTO '97, Lecture Notes in Computer Science, Vol. 1294, 1997, pp. 513-525.

[BON01] D. Boneh, R. Anderson, « API-Level Attacks on Embedded Systems », Computer, Vol. 34, No. 10, 2001, pp. 67-75.

[BON90] D. Boneh, R.A. Demillo, R.J. Lipton, « On the importance of checking cryptographic protocols for faults », in Proc. Advances in Cryptography Conf. - AUSCRYPT'90, Lecture Notes in Computer Science, Vol. 453, 1990, pp. 229-243.

[BRU96] G. Bruguier, J.M. Palau, « Single particle-induced latchup », IEEE Trans. Nucl. Sci., Vol. NS-43, 1996, pp. 522-532.

[BUC87] S. P. Buchner; D. Wilson, K. Kang, D. Gill, J. A. Mazer, W. D. Raburn, A. B. Campbell and A. R. Knudson, « Laser simulation of single event upsets », IEEE Trans. Nucl. Sci., Vol. NS-34, No. 6, 1987, pp. 1228-1332.

[BUC88] S. Buchner, A. Knudson, K. Kang and A. B. Campbell, « Charge collection from focused picosecond laser pulses », IEEE Trans. Nucl. Sci., Vol. NS-35, No. 6, 1988, pp. 1517-1522.

[CAS02] K. Castellani-Coulié, « Recherche des paramètres déterminants pour la prévision des aléas logiques induits par les protons et les neutrons sur les technologies CMOS avancées », Thèse de doctorat, Université de Montpellier2, 2002.

[CLA00] C. Clavier, J. S. Coron, N. Dabbous, « Differential power analysis in the presence of hardware countermeasures », in Proc. Cryptographic Hardware and Embedded Systems Conf. - CHES, Lecture Notes in Computer Science, Vol. 1965, 2000, pp. 252-263.

[CRE96] « Cosmic Ray Effects on Micro Electronics », Disp. @ https://creme96.nrl.navy.mil/.

[DAC95] C. Dachs, « Etude et modélisation du phénomène de burnout induit par ion lourd dans un MOSFET de puissance à canal N », Thèse de doctorat, Université de Montpellier 2, 1995.

[DES01] D. Desilets, M. Zreda, « On scaling cosmogenic nuclide production rates for altitude and latitude using cosmic-ray measurements », Earth and Planetary Science Letters, vol. 193, 2001, pp. 213-225.

[DET97] C. Detcheverry, C. Dachs, E. Lorfèvre, C. Sudre, G. Bruguier, J.M. Palau, J. Gasiot, R. Ecoffet, « SEU critical charge and sensitive area in a submicron CMOS technology », IEEE Trans. Nucl. Sci., Vol. NS-44, No. 6, 1997, pp. 2266-2273.

[DOD96] P.E. Dodd, F.W. Sexton, G.L. Hash, M.R. Shaneyfelt, B.L. Draper, A.J. Farino, and R.S. Flores, « Impact of technology trends on SEU in CMOS SRAMs », IEEE Trans. Nucl. Sci., Vol. NS-43, No. 6, 1996, pp. 2797-2804.

[DOD97] P.E. Dodd, M.R. Shaneyfelt, and F.W. Sexton, « Charge collection and SEU from angled ion strikes », IEEE Trans. Nucl. Sci., Vol. NS-44, No. 6, 1997, pp. 2256-2265.

[DOD98] P. E. Dodd, O. Musseau, M.R. Shaneyfelt, F.W. Sexton, C. D'hose, G.L. Hash, M. Martinez, R.A. Loemker, J.L. Leray, P.S. Winokur, « Impact of ion energy on single-event upset », IEEE Trans. Nucl. Sci., Vol. NS-45, No. 6, 1998, pp. 2483-2491.

[DUT01] Dutertre, J.M. Roche, F.M. Fouillat, P. Lewis, D. , « Improving the SEU Hard Design using a Pulsed Laser », in Proc. RADECS, 2001, p.243-247.

[FAC98] F. Faccio, C. Detcheverry, M. Huhtinen, « First evaluation of the single event upset (SEU) risk for electronics in the CMS experiment », CMS NOTE 1998/054, 1998, pp. 1-15.

[HOH87] J.H.Hohl and K.F.Galloway, « Analytical model for Single Event Burn Out of power Mosfet », IEEE Trans. Nucl. Sci., Vol. NS-34, No. 6, 1987, pp. 1275-1280.

[HUA02] Huang Ching-Yuan, « Etude des antiprotons d'origine atmosphérique au voisinage de la Terre », Thèse de doctorat, CNRS/IN2P3, Grenoble, 2002.

[ITR05] « International Technology Roadmap for Semiconductors », ITRS05, 2005. Disp. @ http://www.itrs.net/Links/2005ITRS/PIDS2005.pdf

[JAC01] M. Jacob, « Au coeur de la matière », Ed. Odile Jacob, 2001.

[JES96] JEDEC Standard, « Test procedure for the measurement of single-event effect in semiconductor devices from heavy ions irradiation », EIAD/JEDEC, 1996.

[JOH96] A.H. Johnston, « The influence of VLSI technology evolution on radiation-induced latchup in space systems », IEEE Trans. Nucl. Sci., Vol. NS-43, 1996, pp. 505-521.

[JOY97] M. Joye, F. Koeune, and J.-J. Quisquater, « Further results on Chinese remaindering », Tech. Report CG-1997/1, UCL Crypto Group, Louvain-la-Neuve, Mars 1997.

[KOC99] P. Kocher, J. Jaffe, and B. Jun, « Differential power analysis: leaking secrets », in Proc. Advances in Cryptology Conf. - CRYPTO'99, Lecture Notes in Computer Science, Vol. 1666, 1999, pp. 388-397.

[KOG89] R. Koga, W.A. Kolasinski, « Heavy-ion induced snapback in CMOS devices », IEEE Trans. Nucl. Sci., Vol. NS-36, 1989, pp. 2367-2374.

[KOG98] R. Koga, « Single event functional interrupt (SEFI) sensitivity in EEPROMs », in Proc. MAPLD, Greenbelt, Maryland, USA, 1998, pp. C2-C12.

[KOM99] O. Kömmerling and M. G. Kuhn, « Design principles for tamper-resistant smartcard processors », in Proc. USENIX Workshop on Smartcard Technology, Chicago, IL, USA, 10–11 May, 1999, pp. 9-20.

[LAL94] J. R. Lalanne, A. Ducasse, S. Kielich, « Interaction LASER molécule, physique du LASER et optique non linéaire moléculaire », Ed. Polytechnica, 1994.

[LAP96] H. Lapuyade, « Analyse physique et modélisation de l'interaction LASER-silicium. Application à la conception de cellules activées par faisceau LASER en vue du test interne des circuits intégrés », Thèse de doctorat, IXL, Université de Bordeaux 1, 1996.

[LER05] D. Leroy, S. J. Piestrak, F. Monteiro, A. Dandache, « Modeling of transients caused by a laser attack on smart cards », in Proc. 11th IEEE IOLTS, 2005, pp. 193-194.

[LER06] D. Leroy, S. J. Piestrak, F. Monteiro, A. Dandache, S. Rossignol, P. Moitrel, « Characterizing Laser-Induced Pulses in ICs: Methodology and Results », in Proc. 12th IEEE IOLTS, 2006, pp. 11-16.

[MAI03] J. Maiz, S. Hareland, K. Zhang and P. Armstrong, « Characterization of multi-bit soft error events in advanced SRAMs », in Digest of Int. Electron Devices Meeting, Washington D.C, 2003, pp. 21.4.1-21.4.4.

[MAR93] Y. Marfaing, « Physique des convertisseurs photovoltaïques », Energie solaire photovoltaïque, Ed. Ellipses, Vol. 1, Ch. 3, 1993.

[MIT05] S. Mitra, N. Seifert, M. Zhang, Q. Shi, K. S. Kim, « Robust system design with built-in soft error resilience », Computer, Vol. 38, No. 2, Feb. 2005, pp. 43-52.

[MOO65] G.E. Moore, « Cramming more components onto integrated circuits », Electronics, Vol. 38, No. 8, 1965, pp. 82-85, Disp. @ http://www.intel.com/research/silicon/moorespaper.pdf

[MUS96] O. Musseau, F. Gardic, P. Roche, T. Corbière, R.A. Reed, S. Buchner, P. McDonald, J. Melinger, L. Tran, A.B. Campbell, « Analysis of multiple bit upset (MBU) in a CMOS SRAM », IEEE Trans. Nucl. Sci., Vol. NS-43, 1996, pp. 2879-2888.

[NGU03] H. T. Nguyen, Y. Yagil, « A Systematic Approach to SER Estimation and Solution », in Proc. IEEE Int. Reliability Physics Symp., Dallas, Texas, 2003, pp. 60-70.

[NIC03] M. Nicolaidis, R. Perez, « Measuring the width of transient pulses induced by ionizing radiation », in Proc. IEEE Int. Reliability Physics Symp., Dallas, Texas, 2003, pp. 56-59.

[NIE01] P. Nieminen, « The in-orbit radiation environment and its effects on space-borne instrumentation », in Proc. Conf. « The Calibration Legacy of the ISO mission », Noordwijk, The Netherlands, Mar. 2002, pp. 74-87.

[NOR93] E. Normand, T. J. Baker, « Altitude and latitude variations in avionics seu and atmospheric neutron flux », IEEE Trans. Nucl. Sci., Vol. NS-40, 1993, pp. 1484-1490.

[OLS93] Olsen et al, « Neutron-induced single event upsets in static RAMS », IEEE Trans. Nucl. Sci., Vol. NS-40, 1993, pp. 74-77.

[ONE94] P.M. O'Neil , G.D. Badhwar, « Single event upset for space shuttle flights of new general purpose computer memory devices », IEEE Trans. Nucl. Sci., Vol. NS-41, 1994, pp. 1755-1764.

[PER04] R. Perez, « Contribution à la définition des spécifications d'un outil d'aide à la conception automatique de systèmes électroniques intégrés robustes », Thèse de doctorat, Université de Montpellier 2, 2004.

[PIC78] J. C. Pickel, J. T. Blandford, Jr. « Cosmic ray induced errors in MOS memory circuits », IEEE Trans. Nuc. Sci., Vol. NS-25, 1978, pp. 1166-1171.

[POU00] V. Pouget, « Simulation expérimentale par impulsion laser ultra-courtes des effets des radiations ionisantes sur les circuits intégrés », Thèse de doctorat, Université de Bordeaux 1, 2000.

[ROO53] W. van Roosbroeck, « The transport of added current carriers in a homogeneous semiconductor », Physical Review, Vol. 91, No. 2, 1953, pp. 282-289.

[SAI98] F. Saigne, « Une nouvelle approche de la sélection des composants de type MOS pour l'environnement radiatif spatial », Thèse de doctorat, Université de Montpellier 2, 1998.

[SAM02] D. Samyde,S. Skorobogatov, R. Anderson, J.-J.Quisquater, « On a new way to read data from memory », Univ. Catholique de Louvain, Louvain-la-Neuve, Belgium, in Proc. First Int. IEEE Workshop on Security in Storage, 2002, pp. 65-69.

[SEX97] F.W. Sexton, D.M. Fleetwood & al, « Single event gate rupture in thin gate oxides », IEEE Trans. Nucl. Sci., Vol. NS-44, 1997, pp. 2345-2352.

[SKO03] S. Skorobogatov, R.J. Anderson, « Optical fault induction attacks », in Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2002, pp. 2-12, Disp. @ http://2003citeseer.ist.psu.edu/article/skorobogatov02optical.html

[TAB93] A. Taber, E. Normand, « Single event upset in avionics », IEEE Trans. Nucl. Sci., Vol. NS-40, 1993, pp. 120-126.

[VER89] J. T. Verdeyen, « LASER Electronics », 2nd edition, Ed. Prentice-Hall Int., 1989.

[WHE94] C.F. Wheatley, J.L. Titus, D.I. Burton, « Single event gate rupture invertical power mosfets, an original empirical expression », IEEE Trans. Nucl. Sci., Vol. NS-41, 1994, pp. 2 152-2 159.

[WRO02] F. Wrobel, « Elaboration d'une base de données des particules responsables des dysfonctionnements dans les composants électroniques exposés à des flux de protons ou de neutrons. Application au calcul des taux d'erreurs dans les mémoires sram en environnement radiatif », Thèse de doctorat, Université de Montpellier 2, 2001.

[ZIE96A] J.F. Ziegler et al, « IBM experiments in soft fails in computer electron », IBM Journal of Research and Development, Vol. 40, Jan. 1996, pp. 3-18.

[ZIE96B] J.F. Ziegler, « Terrestrial cosmic ray », IBM Journal of Research and Development, Vol. 40, Jan. 1996, pp. 19-40.

[ZIE98] J.F. Ziegler, « Terrestrial cosmic ray intensity », IBM Journal of Research and Development, Vol. 42, Janv 1998, pp. 117-139.

[ZOU89] J.A. Zoutendyk, L.D. Edmonds, L.S. Smith, « Characterization of multiple bit errors from single ion tracks in integrated circuits », IEEE Trans. Nucl. Sci., Vol. NS-36, 1989, pp. 2267-2274.

Liste des acronymes

BPSG : Borophosphosilicate glass

CAO : Conception assistée par ordinateur

CMOS : Complementary MOS

DES : Data Encryption Standard

DFA : Differential fault analysis

DNW : Deep N-well

DPA : Differential power analysis

DRC : Design Rule Checking

ECC : Elliptic Curve Cryptography

ITRS : International Technology Roadmap for Semiconductors

LET : Linear energy transfer

LVS : Layout versus Schematics

MBU : Multiple bit upset

MOS : métal oxide semiconductor

Nd:YAG : Neodymium-doped Yttrium Aluminium Garnet

PSG : Phosphosilicate glass

RSA : Rivest, Shamir and Adleman

SEB : Single event burnout

SEE : Single event effect

SEFI : Single event functional interrupt

SEGR : Single event gate rupture

SEL : Single event latchup

SER : Soft error rate

SES : Single event snapback

SET : Single event transient

SEU : Single event upset

SOI : Silicon on insulator

SPA : Simple power analysis

SRAM : Static random access memory

STM : ST microelectronics

TRIUMF : Laboratoire national canadien pour la recherche en physique nucléaire et en physique des particules

Résumé : Nous confions de plus en plus d'informations confidentielles à nos cartes à puces, comme les codes d'accès à notre banque, ou les clés de démarrage de la voiture. Ces circuits sécuritaires deviennent la cible de personnes malintentionnées qui cherchent à récupérer ces informations à leur profit. Ces attaquants utilisent des techniques de pointe comme la perturbation du fonctionnement des circuits, pour parvenir à leurs fins. Pour répondre aux besoins d'un marché très concurrentiel, les concepteurs doivent se protéger de ces perturbations tout en minimisant les coûts de conception. Ces contraintes imposent un compromis entre coût et efficacité, et justifient des techniques automatiques de conception adaptées.
La première partie de ce mémoire est consacrée à l'étude des différentes sources de perturbation d'un circuit intégré, où nous mettons en évidence les similitudes entre une attaque laser et l'impact de particules. Nous montrons ensuite les spécificités de la conception de circuits sécuritaires et les différents types d'attaque à la disposition des pirates. La troisième partie est dédiée à la caractérisation des perturbations. Une méthodologie de conception est proposée et utilisée sur deux circuits, l'un mesurant la durée des perturbations d'un tir laser sur des portes logiques 130nm MOS, l'autre mesurant la sensibilité de portes aux neutrons. Nous finissons par une présentation des résultats obtenus sur le premier circuit après une campagne de tests.

Mots clés : circuit sécuritaire, injection de fautes, méthodologie de conception, erreur transitoire, sensibilité aux radiations, circuit numérique, attaque par laser.

Abstract : More and more sensitive data are stored inside smart cards, like bank account or car access codes. Recently, these security circuits have become a target for hackers who try to get unauthorized access to these data. To achieve this goal, attackers use the state of the art technologies like fault injection. To comply with the smart card market requirements, designers have to build protections against these attacks while keeping design costs as low as possible. These constraints should lead to a cost-efficient design and benefit from dedicated automatic protection methodologies.
In this thesis, we first study radiation sources able to tamper with silicon circuit behavior, and then we reveal similarities between laser attacks and radiation effects on a digital circuit. Then we show the particularities of secure circuit design and the spectrum of attacks used by hackers. The third part of this thesis characterizes single event transients (SET). A design methodology is proposed, supported by experiments performed on two actually implemented circuits: one dedicated to measuring laser-induced SET duration in logic gates, the other dedicated to measuring gate sensitivity to neutrons. This work concludes the review of several results obtained after a laser shooting experiment campaign.

Keywords : circuit security, fault injection, design methodology, soft error, radiation sensitivity, logic circuit, laser attack.