Modélisation et simulation d'attaque laser sur des circuits sécuritaires

Stephan de Castro

Collège Doctoral du Languedoc-Roussillon

THÈSE

Pour obtenir le grade de

Docteur

Délivré par **Université de Montpellier**

Préparée au sein de l'école doctorale

Et de l'unité de recherche **Systèmes Automatiques et Microélectroniques**

Spécialité **: Microélectronique**

Présentée par **De Castro Stéphan**

Simulations et modélisation de fautes laser

Soutenue le 29 mars 2016 devant le jury composé de

Mme Lorena Anghel, TIMA	Rapporteur
Mr Guy Gogniat, Lab-STICC	Rapporteur
Mr Lionel Torres, LIRMM	Examinateur
Mr Bruno Rouzeyre, LIRMM	Directeur de thèse
Mr Jean-Max Dutertre, ENSMSE	Co-encadrant
Mr Giorgio Di Natale, LIRMM	Invité
Mme Marie-Lise Flottes, LIRMM	Invité

Université Montpellier

Remerciements

Avant de présenter les travaux effectués lors de cette thèse, je souhaite remercier les personnes qui ont participées à ces travaux et sans qui cela n'aura pas eu lieu.

Je souhaite tout d'abord remercier mon directeur de thèse, Mr Rouzeyre Bruno, qui m'a suivi durant ces trois ans. En faisant preuve de patience et de disponibilité à mon égard, afin que cette thèse se déroule dans les meilleures conditions.

Je voudrais ensuite remercier mes encadrants du LIRMM, Mme Flottes Marie-Lise et Mr Di Natale Giorgio, pour leurs suivis et leurs conseils avisés sur mes travaux. Je remercie également Mr Dutertre Jean-Max, qui m'a encadré lors de mon année passée sur le site de Gardanne et qui m'a fait profiter de son savoir-faire ainsi que de ces connaissances concernant l'injection laser.

Je remercie également mes rapporteurs, Mme Lorena Anghel et Mr Gogniat Guy, qui ont pris le temps d'étudier mes travaux à travers ce manuscrit et de me renvoyer des rapports avisés. Je souhaite aussi les remercier ainsi que Mr Torres Lionel d'avoir accepté de participer à mon jury de thèse.

Je souhaite remercier tous les partenaires du projet AnR LIESSE dans lequel s'inscrit cette thèse, pour le temps qu'ils m'ont accordés ainsi que le partage de leurs savoirs sur des sujets connexes à ceux présentés dans cette thèse.

Je voudrais ensuite remercier mes collègues de travail. Mr Sarno Thomas pour m'avoir hébergé lors de périodes expérimentales sur le site de Gardanne. Je souhaite aussi remercier Mr Lacruche Marc pour le temps et le savoir-faire qu'il m'a accordé concernant l'utilisation du banc laser. Je voudrais aussi remercier plus généralement, Mme Exurville Ingrid, Mr Zussa Loic, Mr Moro Nicolas, Mr Lashermes Ronan, Mme Lebouder Helene, Mr Cambon David et Mr Allais Jérémy pour la bonne ambiance qu'ils ont apportés durant ces trois années de thèse.

Je souhaiterais remercier Mme Lavernhe Laurie et Mr Serrurier Nicolas pour leur temps, leur accueil souriant et leur aide dans les démarches administratives.

Je voudrais dire un grand merci à mon frère, Nadine et Eloi, ainsi que ma belle-famille pour tout le soutien moral et la bonne humeur qu'ils m'ont apportés durant ces trois ans.

Finalement je voudrais remercier Estelle, qui partage ma vie et qui m’a soutenu et motivé tous les jours durant ces trois ans et sans qui cette thèse aurait été beaucoup plus difficile.

Table des matières

Table des figures

Liste des tables

Introduction

Dans un contexte de mondialisation grandissante où les échanges numériques sont de plus en plus présents, impliquant des données personnelles et/ou financières, il est important de pouvoir garantir la sécurité de ces échanges. Afin d'assurer cette sécurité, divers algorithmes de chiffrement/déchiffrement prouvés mathématiquement sûrs ont été développés. Ils reposent sur l'utilisation d'une donnée secrète (clé).

L'algorithme fournit un message chiffré qui est incompréhensible pour quiconque ne possède pas la clé. Afin de pouvoir accéder au message initial, il faut déchiffrer le message chiffré à l'aide de la clé. Sans cette clef, tout observateur extérieur de l'échange entre les deux interlocuteurs n'a pas accès au message clair (non chiffré).

Les circuits électroniques implantés sur des supports de type carte à puce ont permis d'accroître la portabilité et la rapidité des échanges puisqu'ils permettent l'implantation matérielle des algorithmes cryptographiques, donc plus rapides que leur pendants logiciels. Toutefois, cette implantation matérielle sur un support crée des vulnérabilités. En effet, l'étude du fonctionnement du circuit permet d'obtenir de l'information sur la donnée secrète stockée.

Diverses méthodes d'attaques sur le circuit ont été développées afin d'obtenir la donnée secrète. Parmi toutes ces méthodes, il en existe notamment une qui vise à obtenir de l'information à partir d'un comportement anormal volontairement déclenché du circuit. Ce type d'attaque est appelé attaque en fautes.

Afin de pouvoir réaliser ces attaques, plusieurs moyens sont possibles (modification de la température, champ électromagnétique, modification de l'alimentation, etc.) pour perturber le fonctionnement normal du circuit. Chaque moyen a ses avantages et inconvénients en termes de coût, de précision et de temps d'utilisation. L'un de ces moyens est l'utilisation d'une source lumineuse de type laser. L'utilisation d'une source laser présente l'avantage par rapport aux autres moyens d'injections, pour un attaquant, de pouvoir cibler finement à la fois l'instant où la perturbation est déclenchée et sa position. En effet, il est possible pour les bancs les plus performants, mais aussi les plus coûteux, d'atteindre une précision spatiale d'un micron, i.e. de l'ordre de quelques transistors.

Il est donc devenu important pour les concepteurs de circuits sécuritaires de les protéger face à de telles attaques. La vulnérabilité d'un circuit dépend de multiples paramètres, notamment la technologie utilisée et l'implantation du circuit. Il est donc nécessaire de réévaluer la résistance du circuit sécuritaire lorsque des modifications lui sont apportées.

Cependant l'établissement du niveau de résistance d'un circuit face à des attaques par injection laser a un coût important en temps et en argent puisqu'il faut produire un circuit puis tester ses vulnérabilités. Si le circuit ne répond pas aux exigences sécuritaires, un nouveau design doit être créé. Pour éviter cette perte de ressources et pouvoir prédire le comportement à priori d'un circuit, les premiers simulateurs d'injection laser ont été développés.

Pour avoir le simulateur le plus fidèle possible, il faut comprendre et mesurer les phénomènes physiques mis en jeu lors de l'injection afin de produire le modèle le plus proche de la réalité physique. Des modèles physiques ont déjà été développés pour certains nœuds technologiques. La diminution de la taille des transistors et l'émergence de nouvelle technologie comme le Fully Depleted Silicon On Insulator (FDSOI) implique une mise-à-jour voire une redéfinition de ces modèles.

L'objectif de cette thèse est de modéliser électriquement le comportement sous illumination laser des transistors utilisant différents nœuds technologiques et de comparer la résistance des technologies 28nm CMOS bulk et FDSOI face à l'injection laser. Les modèles électriques développés seront ensuite utilisé dans un simulateur afin de prédire les effets d'une injection laser sur un circuit. La comparaison de ces deux technologies (28nm CMOS bulk et FDSOI), face à l'injection laser, a pour but de déterminer si les attaques sont toujours possibles et quelle technologie est plus résistante. Cette thèse s'inscrit dans le cadre du projet ANR LIESSE. Ce projet a pour but d'étudier les effets laser et les fautes sur les circuits intégrés dédiés à la sécurité.

Le premier chapitre de ce manuscrit présente un état de l'art sur l'injection de fautes à l'aide d'un laser et des attaques en fautes. Les phénomènes physiques de l'interaction laser/silicium ainsi que leurs modélisations électriques y sont présentés.

Le second chapitre décrit les méthodes et les caractéristiques de l'injection laser dans la pratique. Le mode opératoire de préparation d'un circuit en vue d'une injection laser est ensuite présenté. Enfin, une comparaison expérimentale est faite entre l'injection laser en face avant et en face arrière. Afin de déterminer la méthode d'injection optimale suivant le matériel et la cible à disposition de l'attaquant.

Le troisième chapitre est dédié à la création du modèle électrique pour les technologies CMOS 28nm bulk et FDSOI. Cette partie décrira le cheminement de l'expérimentation jusqu'à la création du modèle, ainsi que de la modification du modèle pour la prise en compte des spécificités amenées par la technologie FDSOI.

Dans le chapitre quatre, des injections seront effectuées sur des circuits plus complexes (bascules D flip-flop) afin de confirmer les résultats d'injection sur transistor, ainsi qu'une discussion sur la faisabilité d'une attaque par injection laser sur des circuits 28nm bulk et FDSOI.

Chapitre I.

Attaque en faute par injection laser

Préambule

L'objectif de ce chapitre est de présenter succinctement l'état de l'art sur les attaques en fautes par injection laser. Tout d'abord, une présentation du fonctionnement des algorithmes cryptographiques ainsi qu'une classification des attaques sur ces algorithmes est donnée. Ensuite, les phénomènes physiques intervenant lors de l'interaction entre le laser et le silicium ainsi que leurs modélisations électriques sont décrits. Finalement, le simulateur tLIFTING et une description du modèle électrique pour la technologie 90nm CMOS bulk seront présentés.

I.1. La sécurité de l'information

I.1.1. Les algorithmes cryptographiques

Un algorithme cryptographique est un calcul mathématique de chiffrement et déchiffrement, qui permet d'assurer un échange entre un émetteur et un récepteur de manière sécurisée. On définit quatre propriétés qui peuvent être assurées par l'algorithme (certains algorithmes ne remplissent pas ces quatre conditions simultanément) :

- Seuls l'émetteur et le récepteur sont capables de lire le message (confidentialité)
- Le message provient bien de l'émetteur (authenticité)
- Le message n'a pas été modifiée (intégrité)
- Aucune partie ne peut remettre en cause l'échange (non-répudiation)

Afin d'assurer ces fonctions, l'algorithme s'appuie sur un secret ou une clé secrète. On différencie deux types d'algorithmes de chiffrement: les algorithmes symétriques et asymétriques.

Les algorithmes symétriques ont pour particularité d'utiliser une seule et même clé pour le chiffrement et le déchiffrement. Les deux interlocuteurs doivent partager la même clé, ils ont donc dû se rencontrer afin de convenir d'une clé secrète pour leur communication. Ce genre d'algorithme, par exemple l'AES [1], est très souvent utilisé pour les transactions sécurisées utilisant un support matériel. En effet, les algorithmes symétriques nécessitent moins de ressources de calcul que les algorithmes asymétriques et sont donc plus rapides.

C'est pour répondre à la problématique de l'échange de clés entre les deux interlocuteurs que les algorithmes asymétriques ont été développés. Ils ont la particularité d'utiliser deux clés, une pour le chiffrement et une pour le déchiffrement d'un message, respectivement la clé publique et privée. Le récepteur possède une clé secrète qui lui est propre et qu'il ne partagera avec personne (clé privée). A partir de cette clé privée, une clé publique est générée. Il peut donner cette clé à ses correspondants sans aucune restriction. La clé publique sert à tous les correspondants pour lui faire parvenir un message chiffré. L'émetteur chiffre le message avec la clé publique et envoie le message chiffré au récepteur. Celui-ci utilise alors sa clé privée afin de déchiffrer le message et d'obtenir le contenu en clair. Cependant le récepteur ne peut envoyer de message à l'émetteur avec sa clé publique. L'émetteur doit donner au récepteur sa propre clé publique. En effet, la clé publique du récepteur ne sert qu'à chiffrer des messages qui lui sont destinés.

Les algorithmes asymétriques, comme le RSA [2], sont généralement utilisés pour les transactions pour lesquelles les deux interlocuteurs ne sont pas en contact (échange distant de

donnée sur un support non physique). Le RSA est notamment utilisé pour la sécurisation de transaction sur internet. Les recommandations en termes de taille de clé afin d'assurer une sécurité suffisante est souvent de l'ordre de 2048bits et plus [3]. Cette taille de clé est difficilement compatible avec les contraintes liés à la taille du circuit pour des supports de type carte à puces.

Ces algorithmes de cryptographie sont conçus de telle manière qu'il est impossible (avec les moyens de calculs actuels et en un temps raisonnable) de trouver la clé ou le contenu du message par simple observation des messages chiffrés.

L'implantation de ces algorithmes peut se retrouver sur des plateformes diverses et variées (implantation logicielle ou bien matérielle). On s'intéresse ici à l'implantation matérielle sur support tels que des smartcard (cartes de paiement, d'accès, etc.). La différence du support d'implantation va influencer la méthode d'intégration de l'algorithme (contraintes de temps, ressources de calculs, etc.).

De tels algorithmes permettent de communiquer des données « sensibles » (code d'accès, authentification, message secret, etc.). C'est la sensibilité de ces données et les utilisations possibles de celles-ci qui ont amené des personnes mal intentionnées à développer des méthodes afin d'obtenir la clé secrète. Ces méthodes sont appelées attaques.

I.1.2. Les attaques cryptographiques matérielles

L'objectif d'une personne malveillante est d'obtenir la clé afin par exemple de déchiffrer les messages, se faire passer pour l'émetteur ou même altérer une partie du message. Deux types d'attaques peuvent être distingués, les attaques mathématiques ou logicielles qui s'attaquent aux vulnérabilités de l'algorithme et les attaques matérielles qui se concentrent sur les vulnérabilités dues à l'implantation de cet algorithme. On s'intéresse dans ce manuscrit plus particulièrement aux attaques matérielles qui nécessitent d'avoir accès au support physique réalisant le chiffrement. On distingue trois grands types d'attaques matérielles sur des circuits microélectroniques implantant des algorithmes cryptographiques :

- Les attaques non-invasives
- Les attaques invasives
- Les attaques semi-invasives

S. Skorobogatov dans [4], présente cette classification ainsi qu'une description de chacune d'elles. Ces types d'attaques peuvent également être différenciés en deux classes, celle des attaques

par observation ou attaques dites passives (attaque par canaux auxiliaires) ou par perturbation du circuit ou attaques actives (injection de fautes). Dans la première catégorie, l'attaquant obtient l'information en observant le circuit lors de son fonctionnement, en mesurant la consommation de celui-ci par exemple. La seconde catégorie (i.e. les attaques actives) nécessite une intervention active de l'attaquant sur le circuit durant le calcul afin de le perturber, par illumination laser par exemple.

La catégorie des attaques non-invasives regroupe les attaques ne nécessitant pas de préparation particulière du circuit. L'attaquant pourra par exemple observer la consommation du circuit [5] ou perturber son fonctionnement en faisant varier la tension d'alimentation de celui-ci brutalement [6].

Les attaques invasives au contraire nécessitent une préparation du circuit. Une fois le circuit ouvert (retrait du capot), l'attaquant peut à l'aide de sondes, par exemple posées sur le bus de données, lire le flux de données transitant dans le circuit (probing) [7] . Le circuit peut aussi être altéré notamment par l'utilisation d'un laser de découpe ou un Focus Ion Beam (FIB). Celui-ci permettant de sectionner des capteurs ou des chemins de donnés du circuit.

Les attaques semi-invasives quant à elles sont des attaques qui requièrent une préparation ne modifiant pas l'intégrité et les fonctionnalités du circuit, généralement il suffit d'ouvrir le circuit en retirant le boitier qui l'encapsule ou en amincissant le substrat. Ce type d'attaque regroupe par exemple l'observation de l'émission de photon [8] ou l'injection laser de fautes [9].

La table 1 présente quelques-unes de ces attaques regroupées suivant les catégories définies précédemment.

Table 1: Exemples de différents types d'attaques

	Par observation	**Par injection de fautes ou perturbation**
Attaques non invasives	Consommation d'énergie [5] Temps d'exécution [10] Mesures du champ EM [11]	Glitch de tension [6] Glitch électromagnétique [12] Glitch d'horloge [13]
Attaques semi-invasives	Emission de photons [8]	Injections de fautes laser [9]
Attaques invasives	Probing	Découpe de lignes et modification du circuit

Dans le cadre de cette thèse, nous nous sommes intéressés plus particulièrement à l'injection de fautes par laser. L'injection laser comme méthode d'obtention d'information présente un intérêt au niveau de sa précision. Avec des méthodes classiques de focalisation de faisceau laser, il est possible d'obtenir un faisceau ayant un diamètre de l'ordre du micromètre. La figure I-1 représente la taille d'un faisceau de diamètre 1µm en comparaison d'une cellule SRAM pour différents nœuds technologiques. Pour ces technologies, avec un faisceau de 1µm de diamètre il est possible de cibler précisément une seule SRAM ou même un seul transistor. Cela permet d'avoir une très grande précision et donc de cibler plus facilement la zone recherchée pour un attaquant. Avec la réduction des nœuds technologiques, cette précision n'est plus aussi grande, par exemple pour le nœud technologique 28nm, le faisceau illumine entièrement 2 cellules SRAM proches. Ainsi, on peut se demander si l'injection laser est toujours un outil d'attaque aussi puissant pour ces technologies. Des éléments de réponses sont apportés dans le Chapitre IV.

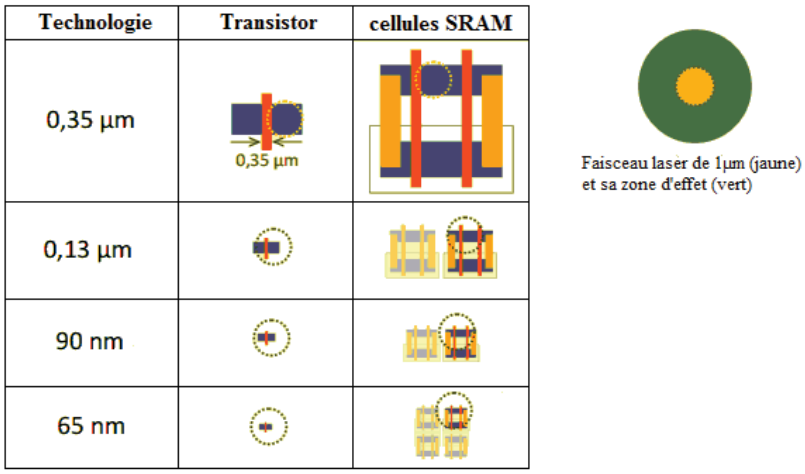


Figure I-1: Taille du faisceau laser en comparaison de transistors et cellules SRAM pour différents nœuds technologiques [14] [15]

Le laser possède aussi une grande précision temporelle avec des durées d'illumination pouvant aller de l'illumination continue à une illumination pulsée de quelques dizaines de picosecondes. Cette durée d'illumination correspond à un cycle d'horloge complet pour un circuit qui fonctionnerait à une fréquence de quelques dizaines de gigahertz. La gigue peut atteindre quelques dizaines de nanosecondes au niveau de la précision du temps d'injection. Cependant la précision temporelle d'injection ainsi que la gigue dépend de l'électronique de commande et de synchronisation du tir laser avec le circuit. Un laser ayant de telles capacités d'injections est très coûteux (plusieurs dizaines de milliers d'euros pour les sources laser).

Toutes ces caractéristiques font du laser un outil pouvant être d'une très grande efficacité (en fonction du banc laser) pour la réalisation d'attaques en fautes.

I.1.3. Les attaques en fautes

Parmi toutes les méthodes d'attaques décrites dans la sous-section I.1.2, on s'intéresse ici plus particulièrement à l'injection de fautes et au moyen d'obtenir de l'information avec ces dernières.

Tout d'abord, on distinguera les attaques en faute visant à faire du déni de service. En effet, ici l'intérêt n'est pas d'obtenir la clé secrète mais d'empêcher la communication entre les deux interlocuteurs. Pour cela, on peut injecter des fautes lors du processus d'authentification ou modifier le message chiffré afin qu'il perde son sens.

Les autres attaques en faute ont pour but d'obtenir de l'information sur le secret. Ce principe d'attaque a été présenté dans [4] sur des cellules SRAM. Pour obtenir de l'information sur le secret, l'attaquant peut cibler la donnée lors de son traitement afin d'injecter une faute et d'observer l'erreur résultante. L'autre cible de l'attaquant est la machine d'états finis gérant l'ordonnancement des opérations de l'algorithme. Ce type de commande est utilisé pour certains algorithmes qui réutilisent les mêmes opérations ou qui fonctionnent à l'aide de ronde (succession d'opérations répétées plusieurs fois) afin de réduire l'encombrement du circuit. La faute injectée dans cette partie du circuit vise à réduire le nombre de rondes de l'algorithme ou de ne pas effectuer certaines opérations pour réduire le niveau de protection du chiffrement. Ci-après deux exemples de types d'attaques.

- **Differential Fault Analysis (DFA):**

Cette attaque consiste à injecter une faute dans le message lors du traitement de celui-ci par l'algorithme. L'information sur le secret provient de la comparaison entre le message chiffré erroné obtenu avec le message chiffré correct (même message clair et même clé). Plus l'attaquant a d'information sur la faute qu'il a injecté plus l'attaque est efficace. Il est aussi préférable d'injecter une faute modifiant peu de bit (1 bit ou 1 octet) afin de se placer dans le cas d'un traitement mathématique des résultats plus simple.

- **Round counter :**

Dans cette attaque, la cible n'est plus la donnée à chiffrer mais la machine d'état gérant l'exécution de l'algorithme. L'attaquant souhaite créer une vulnérabilité en altérant l'exécution du

calcul. Ce type d'attaque est souvent utilisé pour les algorithmes qui s'exécutent sur plusieurs rondes. A cause des contraintes d'implantations dû au support de type carte à puce, on implante généralement qu'une seule ronde de l'algorithme que l'on réutilise. Dans ce cas, un compteur peut être utilisé pour gérer le nombre d'itérations de celle-ci. L'objectif est d'injecter une faute dans ce compteur afin de réduire le nombre de rondes et donc de diminuer la sécurité de l'algorithme. En effet, le nombre d'inconnus étant plus faible, il est plus facile de filtrer les hypothèses de clé. Il existe des attaques utilisant le même principe afin de ne pas exécuter une partie du calcul de l'algorithme.

Pour comprendre comment l'illumination laser permet d'injecter une faute dans le circuit, dans la suite nous rappelons les principes physiques mis en jeu lors de l'interaction entre le faisceau laser et le silicium.

I.2. L'injection de faute par illumination laser

I.2.1. Le laser et ses caractéristiques

Dans cette section, une description du fonctionnement du laser et de son mode d'émission de photon est réalisée. Lorsqu'un matériau semi-conducteur est illuminé, si l'énergie du photon reçu est suffisante, celui-ci est absorbé par le matériau (figure I-2.a). L'énergie absorbée par le matériau permet à un électron d'un des atomes composant le matériau de passer de la bande de valence à la bande conduction. Un électron de la bande de conduction est toujours lié à son atome mais participe à la conduction électrique contrairement aux électrons de la bande de valence. Un électron de la bande de conduction est dans un état instable, afin de retrouver l'état stable de la bande de valence, celui-ci se désexcite. Le passage de la bande de conduction à la bande de valence produit une libération d'énergie sous forme de photon, ce phénomène est appelé émission. On distingue deux types d'émission d'un photon par un matériau : l'émission spontanée et l'émission stimulée. Dans le premier cas (figure I-2.b), lorsque l'électron d'un atome passe d'un niveau d'énergie excité à un niveau de plus basse énergie, l'énergie est restituée sous la forme d'un photon. Pour l'émission stimulée, le changement de niveau d'énergie sera enclenché par un photon incident qui n'est pas absorbé lors du mécanisme (figure I-2.c). Ce transfert de niveau d'énergie s'accompagne également par l'émission d'un photon. Il faut noter que le photon généré a les mêmes grandeurs caractéristiques que le photon incident (phase, direction, longueur d'onde, polarisation). Ainsi pour l'émission stimulée, on obtient deux photons ayant les mêmes caractéristiques.

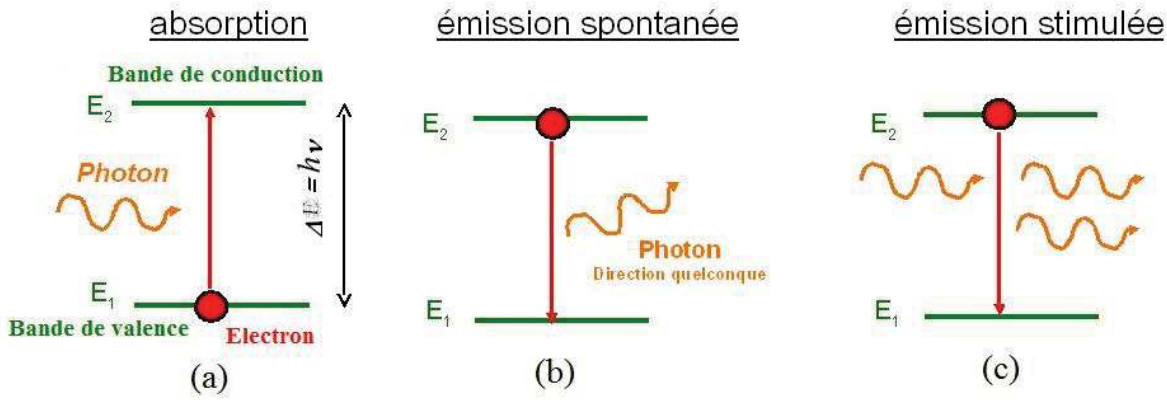


Figure I-2: Mécanismes d'absorption (a) et d'émission spontanée (b) et stimulée(c) d'un photon par un électron [16]

Le laser est un système d'émission stimulée de photons. Le but d'une source laser est d'émettre des photons ayant des caractéristiques ondulatoires identiques. Pour cela, toutes les sources laser sont composées de trois éléments de bases :

- **Un milieu amplificateur**, il peut être constitué d'un cristal, d'un gaz, d'un colorant ou d'un semi-conducteur. C'est le matériau qui par désexcitation d'un électron (passage de la bande de conduction à la bande de valence) va générer les photons suivant le mécanisme d'émission stimulée.
- **Une source externe d'énergie,** cette source peut être optique, électrique ou chimique. Elle permet de placer les électrons des atomes du milieu amplificateur dans un état excité (don d'énergie pour le passage d'un électron de la bande de valence à la bande de conduction), on appelle cette opération le pompage.
- **Une cavité optique résonante** a pour but d'assurer la cohérence spatiale et temporelle des photons. Une fois le photon émis il se déplace dans la cavité optique. Afin de conserver la cohérence entre les photons, les caractéristiques de cette cavité doivent satisfaire certaines conditions.

Dans cette thèse nous ne nous intéresserons pas à l'aspect cohérence spatiale et temporelle des photons.

Dans le cadre de notre étude, nous nous intéressons aux caractéristiques suivantes d'un faisceau laser:

- **La longueur d'onde**, cette grandeur correspond à la distance parcourue en une période par le photon. Pour un matériau donné, la distance parcourue avant d'être absorbée varie

suivant la longueur d'onde (coefficient d'absorption du matériau dépendante de la longueur d'onde).

- **Le diamètre du faisceau laser** (spot), qui détermine la zone spatiale de dépôt de l'énergie dans le matériel, ici le silicium.
- **La durée d'illumination du matériel**, elle correspond au temps pendant lequel des photons sont envoyés sur le matériel et donc le temps de dépôt d'énergie dans le silicium. Si le temps de dépôt est trop long on peut assister à un échauffement du silicium pouvant entraîner une détérioration.
- **L'énergie du faisceau laser**, cette énergie donne une indication quant à l'énergie déposée dans le silicium. Si cette dernière est trop haute, alors le tir laser peut avoir un effet néfaste sur le circuit (dommage ou casse).

La distribution énergétique du faisceau laser n'est pas uniforme. Cette distribution à un profil gaussien comme illustré par la figure I-3. L'équation 1 présente la fonction du profil énergétique du faisceau laser pour une énergie normalisée et un faisceau centré en l'origine.

$$E(x,y) = e^{-x^2-y^2} \qquad (1)$$

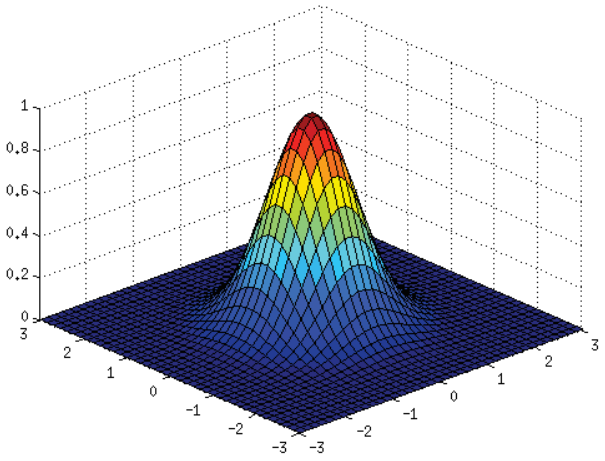


Figure I-3: Distribution énergétique du faisceau laser (gaussien)

Le faisceau laser est un faisceau gaussien, i.e. que le profil de la zone d'illumination est proportionnelle à une fonction gaussienne. Ainsi la largeur du faisceau $\omega(z)$ diminue jusqu'à atteindre sa valeur minimale ω_0 au point focal comme montré sur la figure I-4, puis augmente lorsque l'on s'éloigne de ce point. L'angle Θ correspond à l'ouverture du faisceau.

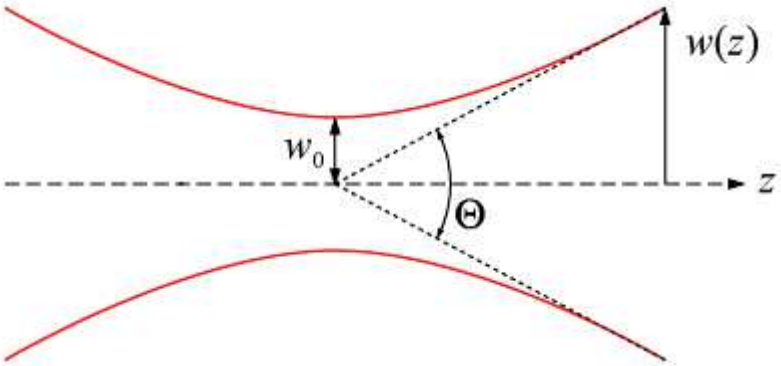


Figure I-4: Largeur d'un faisceau divergent [17]

L'évolution de cette grandeur est donnée par l'équation (2).

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z}{z_0}\right)^2} \qquad (2)$$

où Z_0 correspond à la profondeur de champ (ou portée de Rayleigh). Pour cette distance on a $(z_0) = \omega_0\sqrt{2}$.

Dans la suite de ce manuscrit la taille de spot citée correspond à ω_0. En effet le laser est focalisé de telle manière que la taille de spot au niveau de la surface du transistor correspond au minimum de cette fonction. En pratique, on peut aussi se placer hors du plan focal pour avoir une zone illuminée plus large au niveau du transistor mais l'énergie surfacique déposée sera plus faible.

I.2.2. L'absorption de l'énergie par le silicium

a) Pour un semi-conducteur intrinsèque

Un matériau semi-conducteur a une conductivité électrique intermédiaire entre celle des conducteurs et celle des isolants. Cette caractéristique vient du fait que la probabilité qu'un électron participe à la conduction électrique est faible mais non nulle. On appelle semi-conducteur intrinsèque un matériau semi-conducteur dont le réseau cristallin est pur (i.e. non dopé). Comme présenté dans I.2.1, lorsqu'un matériau est illuminé, par une source émettant des photons d'énergie suffisante, on observe alors le phénomène d'absorption. On s'intéresse dans cette section à l'absorption pour un matériau semi-conducteur intrinsèque et plus particulièrement du silicium.

- ***Absorption interbande***

L'absorption interbande est le mécanisme par lequel l'énergie est absorbée, faisant passer un électron de la bande de valence à la bande de conduction. Dans notre cas, la source d'énergie est le photon généré par le laser.

On appelle bandgap, l'énergie minimale nécessaire pour effectuer la transition d'un électron de la bande de valence à la bande de conduction. La valeur de ce bandgap est dépendante de la nature du matériau composant le semi-conducteur, plus particulièrement des interactions entre le noyau et les électrons. Le bandgap représente une bande interdite, l'électron n'a que deux états possibles, sur la bande de valence ou sur la bande conduction. Tout état intermédiaire est interdit, ce qui conduit au fait que si l'énergie du photon incident est inférieure au bandgap alors le photon n'est pas absorbé. Ceci s'applique à un semi-conducteur de type bande interdite directe, il existe un second type dit de bande interdite indirecte (figure I-5). Ce type de matériau fait intervenir un mécanisme plus complexe lors de l'absorption. Pour les matériaux à bande interdite indirecte, il est possible de réaliser un passage de la bande de valence à celle de conduction avec moins d'énergie que celui requis mais cela demande l'intervention d'une autre particule, le phonon. Le photon va venir frapper l'électron de la bande de valence ce qui va le mettre dans un état interdit et le phonon va fournir l'impulsion nécessaire à l'électron pour rejoindre la bande de conduction.

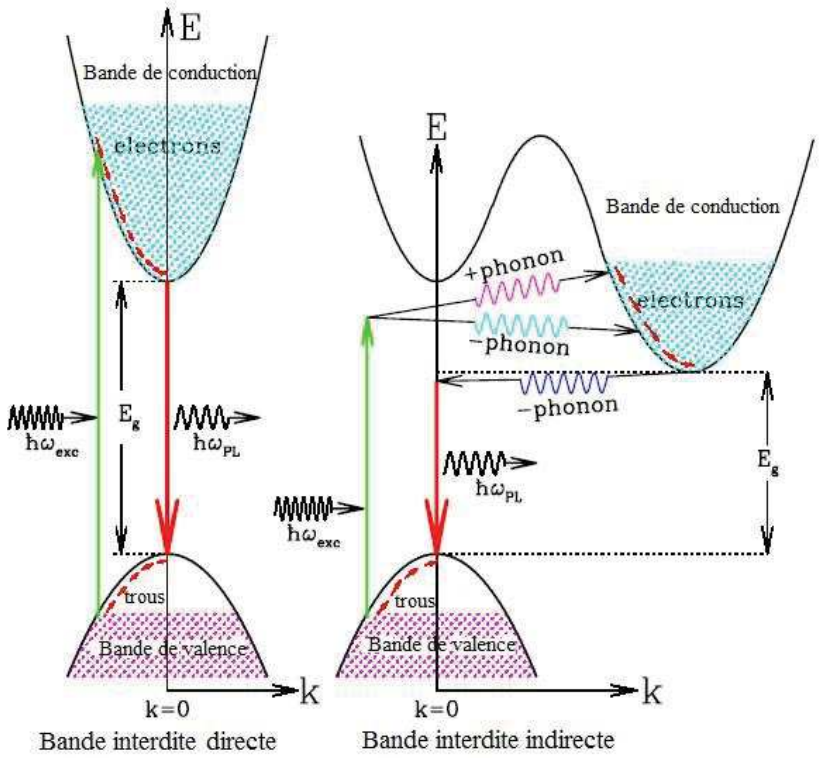


Figure I-5: Mécanismes d'absorption directe et indirecte [16]

L'absorption indirecte peut aussi se produire pour les semi-conducteurs à bande interdite directe mais elle est secondaire par rapport à l'absorption directe. Le silicium est un semi-conducteur de type bande interdite indirecte. Le type d'absorption privilégié pour ce type de matériau est celui faisant intervenir le phonon.

- ***Absorption « deux photons »***

L'absorption « deux photons » consiste à l'absorption de deux photons afin de faire passer un électron de la bande de valence à la bande de conduction. Pour que ce phénomène soit réalisable, certaines conditions doivent être satisfaites. D'une part il faut que l'énergie du photon soit inférieure au bandgap du matériau (ici le silicium) pour que celui-ci ne soit pas absorbé et d'autre part que l'énergie du photon soit supérieure à la moitié du band gap. L'intérêt est la possibilité d'utiliser des longueurs d'ondes plus grandes pour l'injection. Dans notre cas, la longueur d'onde verte peut être utilisée pour réaliser une injection par la face arrière du circuit en considérant ce mode d'absorption. Ceci n'est pas possible autrement qu'en absorption deux photons car l'épaisseur du substrat empêche les photons d'être absorbé dans la zone d'implantation des transistors et donc de générer des porteurs de charges dans cette zone. Le problème de cette méthode est que la probabilité que la double absorption se produise est très faible.

La génération de charges ainsi que la profondeur de pénétration d'un photon dans le silicium sont décrits ci-après.

- ***Génération de porteurs de charges et profondeur d'absorption du silicium***

L'absorption des photons dans un matériau sous illumination dépend du matériau illuminé ainsi que de la longueur d'onde du faisceau utilisé. La figure I-6 présente les mesures expérimentales du coefficient d'absorption et de la profondeur d'absorption du silicium intrinsèque pour plusieurs longueurs d'onde d'illumination. La profondeur d'absorption est l'inverse du coefficient d'absorption. Cette profondeur correspond à la distance au bout de laquelle l'énergie du faisceau a diminué de 36% (1/e). On remarque que pour le silicium pur, plus la longueur d'onde est grande, plus la profondeur d'absorption est grande. Le silicium est quasiment transparent pour des longueurs d'ondes infrarouges et supérieures.

Les profondeurs d'absorption dans le silicium pour chaque longueur d'onde sont les suivantes :

- Infrarouge : 1mm
- Vert : 1µm
- Ultraviolet : 10nm

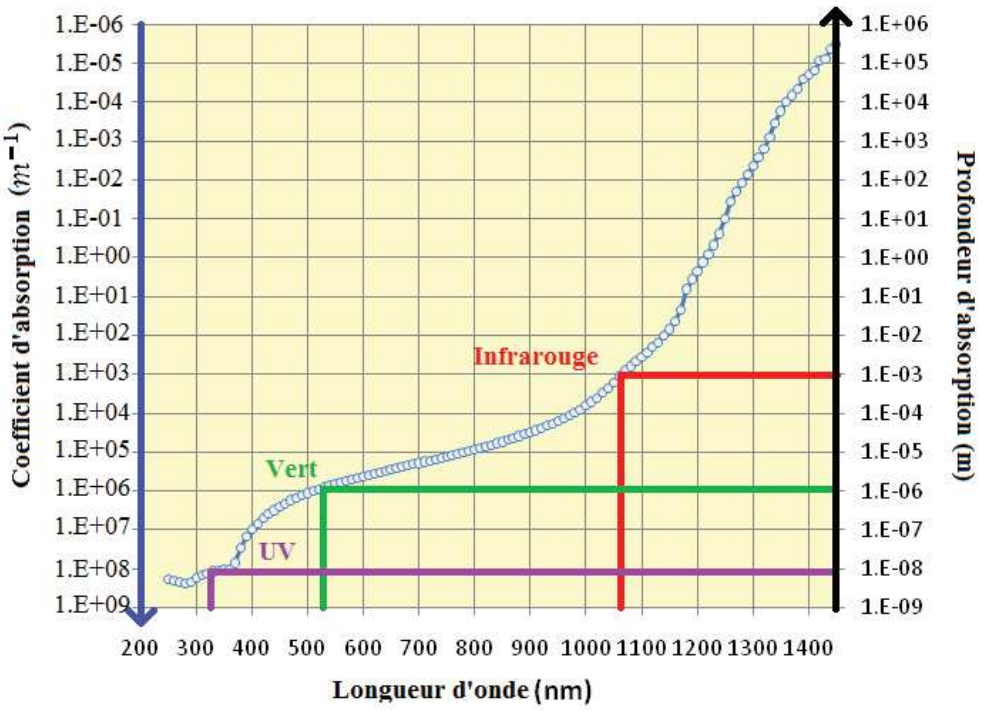


Figure I-6: Coefficient d'absorption et profondeur d'absorption du silicium intrinsèque pour plusieurs longueurs d'ondes [18]

Si l'on considère que l'énergie absorbée par le silicium ne sert qu'à générer des porteurs de charges (électrons/trous) et qu'il n'y a aucune réflexion du faisceau laser on peut alors déterminer le nombre de porteurs de charges généré dans le silicium suivant la distance de silicium parcourue par le faisceau. Le nombre de porteurs de charges est donné par l'équation (3) suivante :

$$G = \alpha N_0 * e^{-\alpha x} \quad (3)$$

Avec α le coefficient d'absorption en m^{-1}, N_0 le flux de photons à la surface du silicium en $m^{-2}s^{-1}$ et x la distance parcouru par le faisceau en mètre. la figure I-7 présente la génération normalisée de porteurs de charges en fonction de la distance parcourue dans le silicium pour plusieurs longueurs d'ondes. La génération de porteurs de charges est normalisée afin de s'affranchir de l'énergie du faisceau laser. De plus, on limite l'épaisseur de silicium à 100µm (abscisse). Cette longueur correspond approximativement à l'épaisseur d'un wafer aminci. Pour les longueurs d'ondes ultraviolettes et vertes, la totalité des porteurs de charges est générée en surface du silicium (resp. 1µm et 8µm). Au contraire, pour une longueur d'onde infrarouge les porteurs sont générés sur toute l'épaisseur du silicium.

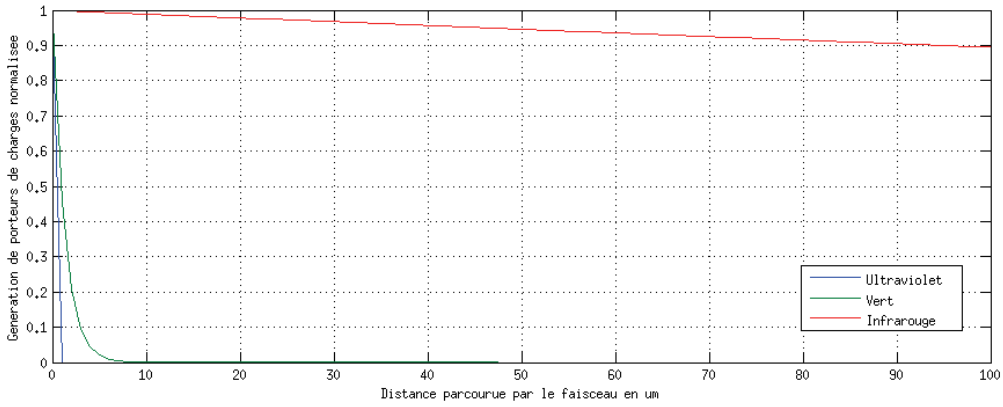


Figure I-7: Génération de porteurs de charges normalisée en fonction la distance parcourue par le faisceau dans le silicium

L'illumination laser d'un matériau semi-conducteur tel que le silicium conduit à la génération de porteurs de charges, électrons et trous. Cependant, les transistors utilisés dans les circuits sont composés de silicium dopé (P ou N). Dans la suite, on étudie l'impact du dopage sur la génération des porteurs de charges.

b) Pour un semi-conducteur dopé

On appelle semi-conducteur dopé un réseau cristallin de semi-conducteur dans lequel on a placé (par insertion dans les interstices ou par substitution atomique) des atomes d'un autre élément. On considère trois types d'atomes qui peuvent être insérés dans un semi-conducteur:

- L'espèce donneuse d'électrons, qui a une bande de conduction relativement plus basse que celle du silicium, permettant de faciliter la conduction des électrons. Lorsqu'on insère ce type d'atome, on a un dopage de type N. Généralement on utilise les atomes de phosphore, d'arsenic ou d'antimoine (resp. P, As et Sb).
- L'espèce accepteuse d'électrons, qui a une bande de valence relativement plus haute que celle du silicium, permettant de faciliter la conduction des trous. Avec ce type d'atome on a un dopage de type P. On utilise couramment les atomes de bore (B).
- les impuretés qui ajoutent des états discrets dans la bande interdite.

L'atome de silicium possède 4 électrons sur sa couche de valence (couche électronique la plus externe). Ces 4 électrons sont utilisés afin de réaliser 4 liaisons covalentes (mise en commun d'électrons pour réaliser la liaison) avec 4 autres atomes de silicium. La figure I-8 présente un schéma de la maille d'un cristal de silicium pur (type diamant). Chaque sphère représente un atome de silicium qui est connecté par liaison covalente à 4 autres atomes de silicium.

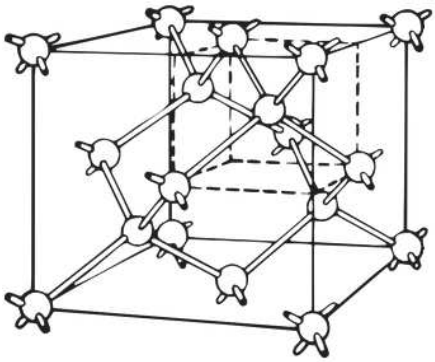


Figure I-8: Schéma d'une maille de cristal de silicium intrinsèque [19]

Lors d'un dopage de type N, des atomes ayant plus de 4 électrons sur leurs couches de valence sont ajoutés par insertion ou substitution. Les électrons supplémentaires n'interviennent pas dans les liaisons covalentes avec le silicium, ceux-ci ont plus de facilité à passer de la bande de valence à la bande de conduction et facilite donc la conduction électrique. Par exemple le phosphore a 5 électrons sur sa couche de valence, 4 sont utilisés afin d'assurer les liaisons covalentes avec les atomes de silicium voisins. Comme le 5eme électron ne participe pas à une liaison, l'énergie nécessaire pour faire passer cet électron de la bande de valence à la bande de conduction est plus faible que ceux participant aux liaisons. Cet électron facilite alors la conduction électrique.

De même pour un dopage P, des espèces ayant moins de 4 électrons sur leurs couches de valence sont ajoutées au réseau cristallin de silicium. Pour le silicium, on utilise par exemple du bore qui possède 3 électrons sur sa couche de valence. Cette espèce ajoute un trou (porteur de charge positif) au réseau cristallin. Ce trou qui n'intervient pas dans les liaisons atomiques facilite la conduction électrique.

Pour le silicium dopé, l'énergie nécessaire pour faire passer les porteurs de charges majoritaires (qui n'interviennent pas dans les liaisons) de la bande de valence à la bande de conduction est plus faible que celle du silicium intrinsèque. Les dopants ajoutent des niveaux quantiques qui réduisent le bandgap entre la bande de valence et celle de conduction.

L'illumination laser du silicium dopé a aussi pour effet de générer des porteurs de charges. Mais le dopage facilite la transition des électrons (resp trous) de la bande de valence à la bande de conduction, pour un dopage N (resp dopage P), en ajoutant des états quantiques plus rapprochés que le silicium intrinsèque (énergie nécessaire à la transition plus faible). Outre la génération de charges, l'énergie du faisceau laser est aussi convertie en énergie thermique, au sein du silicium. On

étudie dans la suite, l'effet de la température du matériau sur la génération de charges, et plus particulièrement sur le phénomène d'absorption.

c) *Effet de la température sur l'absorption du silicium*

En parallèle du phénomène d'absorption, le faisceau laser a d'autres effets lorsqu'il rentre en interaction avec le silicium. Une partie de l'énergie lumineuse absorbée par le silicium est convertie en énergie thermique. Dans [20], une étude a été menée sur la dépendance du coefficient d'absorption du silicium à la température. Pour cela, plusieurs mesures du coefficient d'absorption ont été réalisés en envoyant des photons (d'énergie supérieure au bandgap du silicium) sur du silicium microporeux. Pour les gammes de températures et d'énergies utilisées dans cette étude, le silicium microporeux se comporte comme du silicium cristallin utilisé pour la fabrication de circuit. La figure I-9 présente le résultat de cette expérimentation. Le coefficient d'absorption augmente de manière quasi exponentielle avec l'élévation de la température du silicium. Donc plus la température augmente et plus le photon est absorbé rapidement à la traversée du silicium. Pour l'injection par la face avant, cela signifie que lorsque le silicium est chaud, le canal de conduction créé par l'illumination laser se situe en surface du circuit. Pour l'injection par la face arrière, si le silicium est à une température plus élevée, alors le photon est absorbé avant d'atteindre la zone d'implantation des transistors.

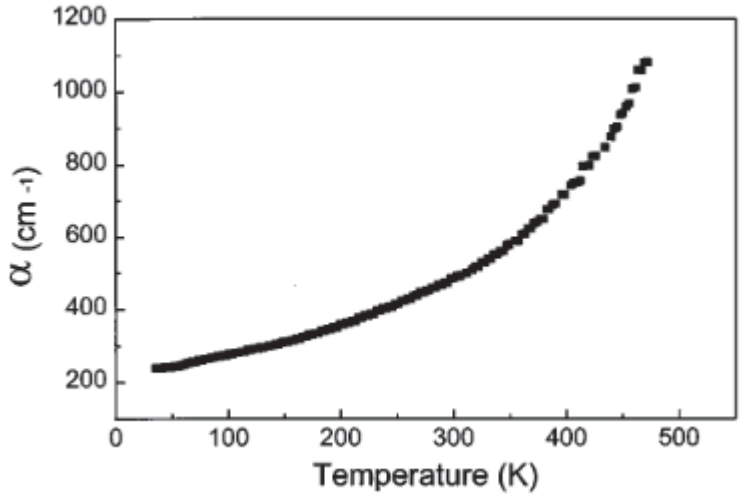


Figure I-9: Coefficient d'absorption en fonction de la température pour du silicium microporeux [20]

L'injection laser sur du silicium (dopé ou intrinsèque) conduit à la création de paires électrons trous dans le silicium, par absorption des photons. On s'intéresse maintenant à l'impact de cette

génération de charges sur le fonctionnement d'un circuit bulk. Pour cela, dans un premier temps, on étudie l'effet de ces charges sur du silicium, puis une jonction PN et finalement sur un inverseur.

I.2.3. De l'effet photoélectrique à la faute induite

On s'intéresse ici, à l'impact des charges générées par effet photoélectrique sur un circuit microélectronique. On étudie alors l'effet de ces charges dans un barreau de silicium intrinsèque (non polarisé). Le faisceau laser va générer des charges dans le silicium sur son trajet. Ainsi localement dans le silicium, une zone ayant une plus forte concentration de porteurs de charges va se créer dans la zone de silicium illuminée. Ce gradient dans la concentration de porteur de charges va entraîner un phénomène de diffusion. En effet, afin de rétablir une concentration en porteurs de charges constante dans tout le silicium, les charges générées vont se déplacer dans des zones de plus faible concentration en porteurs de charges, i.e. vers le silicium non illuminé. La figure I-10 présente une vue de principe du phénomène de diffusion. Les directions de déplacement (flèche sur la figure) de chaque charge est aléatoire, cependant le sens du déplacement va toujours vers les zones de concentrations plus faibles.

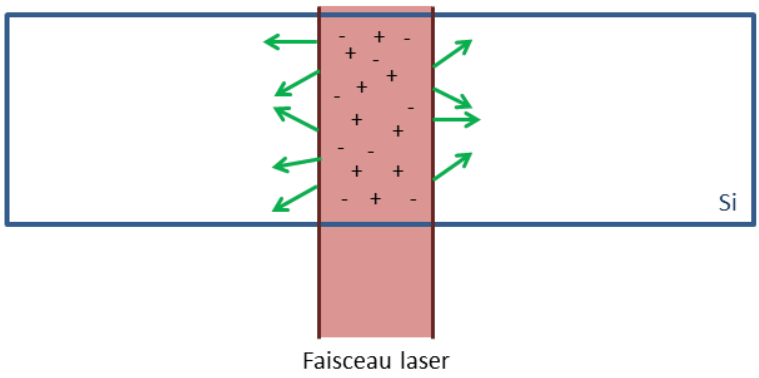


Figure I-10: Schéma de principe du phénomène de diffusion des charges dans un barreau de silicium non polarisé

L'expression de ce phénomène de diffusion est donnée par (4) (première loi de Fick).

$$\overrightarrow{J_A} = -D_A \overrightarrow{grad}\ c_A \qquad (4)$$

Où $\overrightarrow{J_A}$ représente le vecteur densité de courant de particules (en mol/m².s), pour les particules A (ici soit les électrons ou les trous), D_A le coefficient de diffusion de A dans le silicium (m²/s), $\overrightarrow{grad}$ correspond à l'opérateur de gradient et c_A la concentration de A pour une position et un instant donné (mol/m^3).

Ce déplacement de porteurs dans le silicium génère un courant. Le courant résultant du phénomène de diffusion est souvent très faible et très localisé. En effet, la vitesse de déplacement des charges est faible et la recombinaison rapide.

On s'intéresse maintenant à l'effet de l'illumination laser sur une jonction PN polarisée en inverse. En effet, dans cette configuration, la jonction PN présente une zone de charge espace plus large que lorsque celle-ci est polarisée dans le sens direct. Lors de l'illumination laser des charges sont générés le long du passage du laser dans le silicium (figure I-11.a). Sous l'effet du champ électrique présent dans la zone de charge espace, les charges vont se déplacer dans des sens opposés. Ce mouvement de charge va déformer la zone de charge espace le long de la trajectoire du laser (figure I-11.b) et ainsi balayer les charges en quelques pico secondes (funneling). Ce mouvement de charge va créer un pic de courant. Lorsque le silicium n'est plus illuminé (figure I-11.c), les charges restantes diffusent et se recombinent dans le silicium sans entraîner de modification significative sur le fonctionnement du circuit. La figure I-11.d représente le profil du courant lors de l'illumination de la jonction PN polarisée en inverse. On retrouve ainsi, la collection rapide due à l'effet du champ électrique présent dans la zone de charge espace et la collection lente due au phénomène de diffusion qui dure plus longtemps.

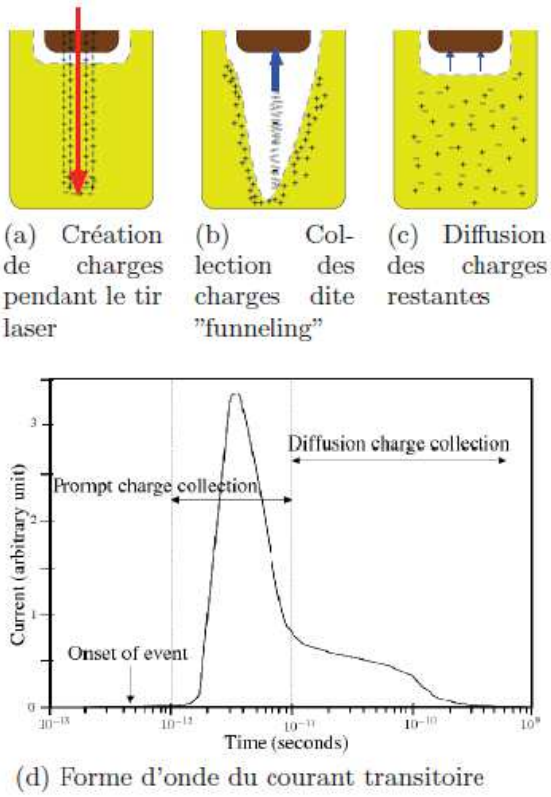


Figure I-11 : Vue de principe des phénomènes physiques mis en jeux lors de l'illumination d'un jonction PN polarisée en inverse [21]

On peut donc considérer que dans un transistor CMOS, les principales zones de génération du photocourant sont les jonctions PN présentes dans sa structure, et plus précisément celles polarisées en inverse (zone de génération d'un courant d'intensité importante). Dans [22], une étude est réalisée sur l'injection laser sur des portes logiques ainsi que sur leurs zones sensibles. On appelle zones sensibles, les jonctions PN du transistor qui permettent de modifier, par illumination laser, l'état logique de sortie d'une porte. Il ressort de cette étude deux résultats sur l'injection laser sur des portes logiques :

- Les zones sensibles d'une porte logique dépendent de la donnée d'entrée de celle-ci. Par exemple pour un inverseur suivant si l'entrée est '0' ou '1', la zone sensible n'est pas la même.
- Les zones sensibles correspondent aux drains (jonction PN composé du drain et du substrat ou Nwell) des transistors non passant (mode off) composant la fonction logique.

On s'intéresse maintenant à l'effet d'un tir laser sur un inverseur logique CMOS. La figure I-12 présente l'effet de l'injection sur un inverseur CMOS dont l'entrée est au niveau logique bas. Si le drain du transistor NMOS (zone sensible de l'inverseur dans cette configuration) est illuminé, les charges générées induisent un courant au niveau de la jonction PN polarisée en inverse composée du drain et du substrat P du transistor NMOS. Le chemin de conduction ainsi créé résulte en un court-circuit entre le rail d'alimentation et celui de la masse. Ceci a pour effet de décharger la capacité de sortie de l'inverseur pendant la durée d'illumination. On peut observer un changement de valeur logique si l'illumination dure assez longtemps. Ce temps nécessaire d'illumination dépend des caractéristiques technologiques, telles que le courant et la capacité de charge en sortie de l'inverseur.

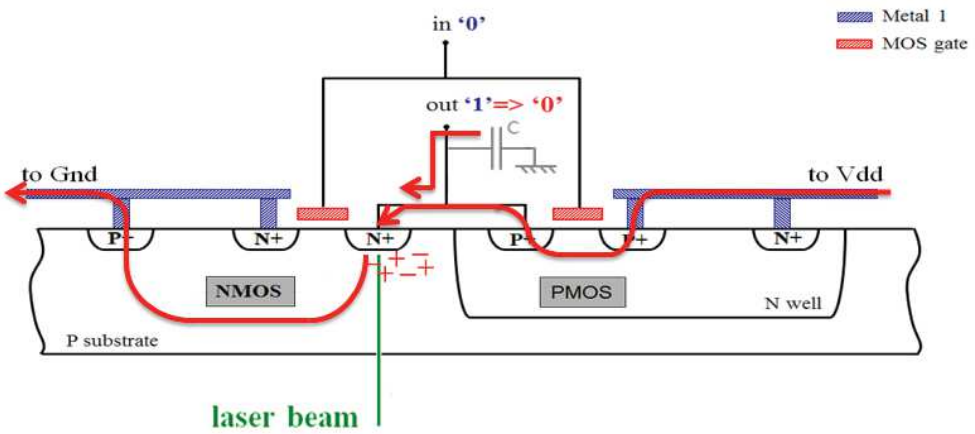


Figure I-12: Mécanisme de changement de la valeur logique en sortie par illumination laser sur un inverseur CMOS bulk

Cette perturbation est transitoire, i.e. lorsque le transistor PMOS n'est plus illuminé, les charges générées sont toutes évacuées (ici par le transistor PMOS qui est passant) et la sortie de l'inverseur repasse au niveau haut. Ce mécanisme peut, sous certaines conditions, conduire à une faute dans le circuit, faute qui peut engendrer une erreur. Le concept de faute et d'erreur est présenté dans la section suivante.

I.2.4. La faute et l'erreur

La faute et l'erreur sont deux choses distinctes. Dans le cadre de cette thèse, on utilise la convention suivante afin de différencier la faute de l'erreur.

Une faute correspond au changement de la valeur logique à un instant donné engendré par l'injection (figure I-13). Par exemple, si la donnée traitée à un instant précis est '0' et qu'après une perturbation, la valeur du bit devient '1', on a injecté une faute.

L'erreur correspond à la modification de la donnée en fin de calcul due à l'injection de la faute (figure I-13). La valeur de l'erreur dépend de la faute injectée.

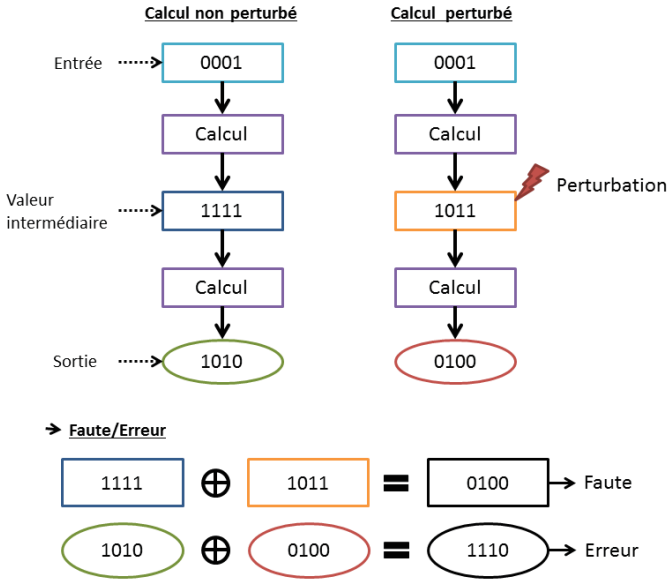


Figure I-13: Différenciation entre une faute et une erreur sur un calcul perturbé

I.2.5. Les évènements singuliers

Les évènements singuliers sont des perturbations du régime normal du circuit à un instant donné. Ces perturbations peuvent être permanentes, on parle de Hard Error, ou temporaires on parle alors de Soft Error. Ces évènements ont tout d'abord été associés au passage d'une particule

énergétique à travers le silicium. Par la suite, cette dénomination a été aussi appliquée à la perturbation engendrée par une illumination laser. Bien que le mécanisme de génération de charges dans le silicium soit différent pour le passage d'une particule énergétique et d'une illumination laser, l'effet macroscopique reste le même (i.e. la génération d'un courant électrique dans le silicium) [23].

Certains de ces évènements singuliers sont propres à la perturbation due au passage d'une particule énergétique, comme les dommages physiques entraînés par l'impact de la particule sur la grille d'un transistor par exemple. Dans la suite, on décrit seulement les évènements singuliers pouvant être causés par l'illumination laser du circuit.

a) Hard Error

Il existe trois types d'évènements singuliers permanents liés à la technologie CMOS. Le « Latch-Up », la « Gate Rupture » et le « Snapback ». Ces évènements singuliers mènent à la destruction partielle d'un ou plusieurs transistors, cette dégradation conduit à une faute permanente lorsque ces transistors sont sollicités. Le Gate Rupture n'est pas décrit ici, car il implique un ion lourd comme particule énergétique incidente.

- Latch-Up :

Le phénomène de Latch-up se produit lorsque la structure thyristor parasite d'un inverseur logique CMOS se déclenche. Dans [24], les causes et les conséquences sont décrites. La figure I-14 montre les différents transistors parasites présents dans la structure d'un circuit CMOS ainsi que la structure thyristor qui cause le Latch-up. Lorsque le thyristor s'enclenche, un courant fort venant de la source d'alimentation traverse la structure en un instant très bref. La dissipation de cette forte puissance peut endommager voire casser la structure.

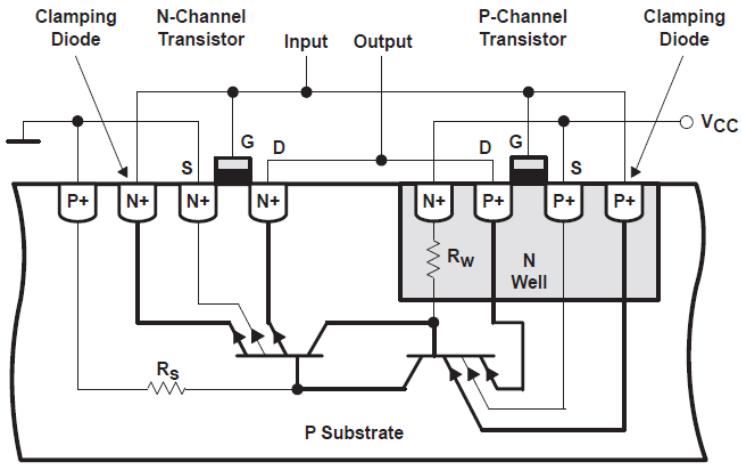


Figure I-14: Détails des transistors parasites d'un inverseur CMOS [24]

- Snapback :

Finalement le phénomène de « Snapback » est dû au transistor bipolaire parasite NPN dans un transistor NMOS (resp. PNP pour le PMOS) comme le montre la figure I-15. Dans [25] , l'effet de Snapback a été modélisé par le circuit équivalent donné en figure I-16. Lorsqu'une tension importante est appliquée entre le collecteur et base du transistor parasite, un courant est alors généré au niveau de la base de celui-ci. Ce courant fait passer le transistor bipolaire de l'état off à l'état on. Une diminution de la tension au niveau du collecteur est alors observée. Le collecteur du transistor bipolaire correspond au drain du transistor NMOS. Ainsi ce phénomène va perturber le fonctionnement du transistor en faisant diminuer la tension du drain.

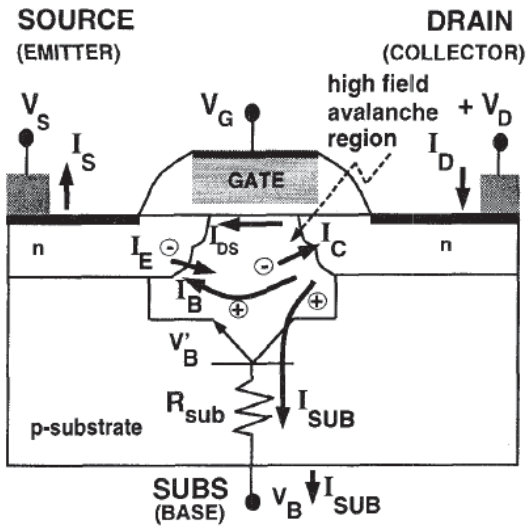


Figure I-15: Vue en coupe d'un transistor NMOS avec le transistor bipolaire parasite NPN [26]

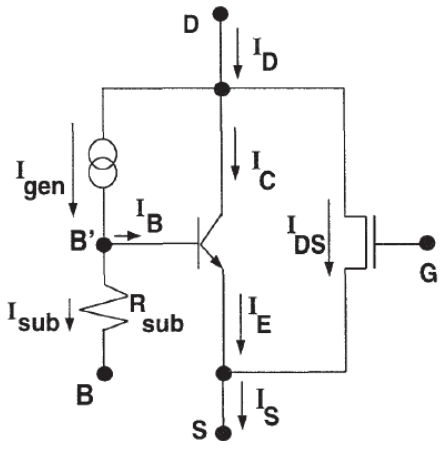


Figure I-16: Circuit équivalent d'un transistor NMOS incluant le transistor parasite de Snapback [26]

b) Soft Error

On distingue deux grands types d'évènements singuliers transitoires, l'un où la faute est produite directement sur la mémoire (Single Event Upset) et l'autre où elle se manifeste sur la partie combinatoire du circuit (Single Event Transient).

Lorsqu'une porte logique est illuminée, l'état logique de sortie de celle-ci peut être modifié transitoirement durant le temps de l'illumination comme présenté dans la section I.2.3. On observe alors un "Single Event Transient" (SET), ou transitoire de tension, sur la sortie de la porte. Afin que cette faute transitoire puisse se propager dans le circuit et générer une erreur, elle doit être mémorisée par une bascule avant d'être relâché au front d'horloge suivant. Les figure I-17 et figure I-18 présente un chronogramme de l'effet de l'illumination d'un inverseur (au niveau logique), qui est suivi d'un élément de mémorisation (bascule DFF). Le signal d'entrée de l'inverseur In est maintenu à l'état logique bas, lors de son fonctionnement normal, le signal de sortie de l'inverseur (signal D) reste à la valeur logique 1. Le signal Clk représente le signal d'horloge de la bascule et le signal Out, la sortie de celle-ci. On suppose, qu'on se place dans des conditions d'injections certaines de fautes (position et puissance d'illumination nécessaire), ainsi à chaque injection sur l'inverseur, le signal D passe de la valeur logique 1 à 0 comme décrit dans la section I.2.3. Ainsi si l'illumination n'a pas lieu lors d'un front montant du signal d'horloge comme présenté sur la figure I-17, alors il n'y a aucun effet en sortie de la bascule (valeur logique de sortie: '1'). La seconde injection présentée sur la figure I-18 est effectuée lors d'un front montant de l'horloge, la sortie de la bascule passe à la valeur logique 0 durant un cycle d'horloge. Afin que la faute transitoire soit stockée dans un élément de mémorisation, il faut donc que ce transitoire se propage jusqu'à l'entrée de l'élément de mémorisation durant la phase d'écriture de celui-ci (c'est-à-dire lors d'un front montant du signal d'horloge). La faute est alors maintenue en sortie de la bascule durant un cycle d'horloge [27] [28] . Le cas présenté ici, ne tient pas compte du masquage logique pouvant se produire dans un circuit logique plus complexe. En effet, par exemple si l'illumination laser provoque un changement d'état logique sur un signal d'entrée d'une porte de type NAND2, si l'entrée non fautée est à l'état bas (valeur prioritaire), alors quel que soit le changement d'état logique provoqué par l'injection, la sortie de la porte logique NAND reste 1 et le transitoire ne se propage plus (masquage logique).

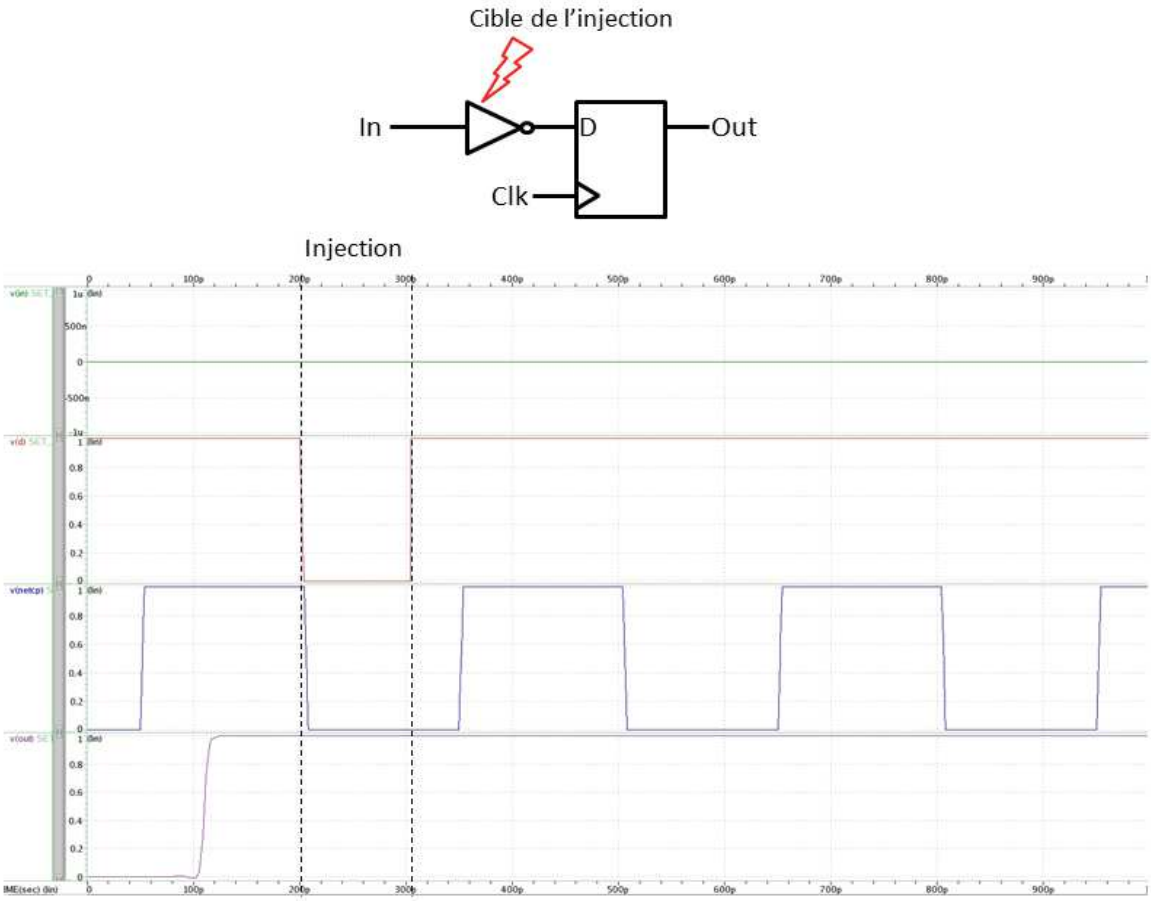


Figure I-17: Mécanisme d'injection d'une faute de type single Event Transient (injection hors front montant)

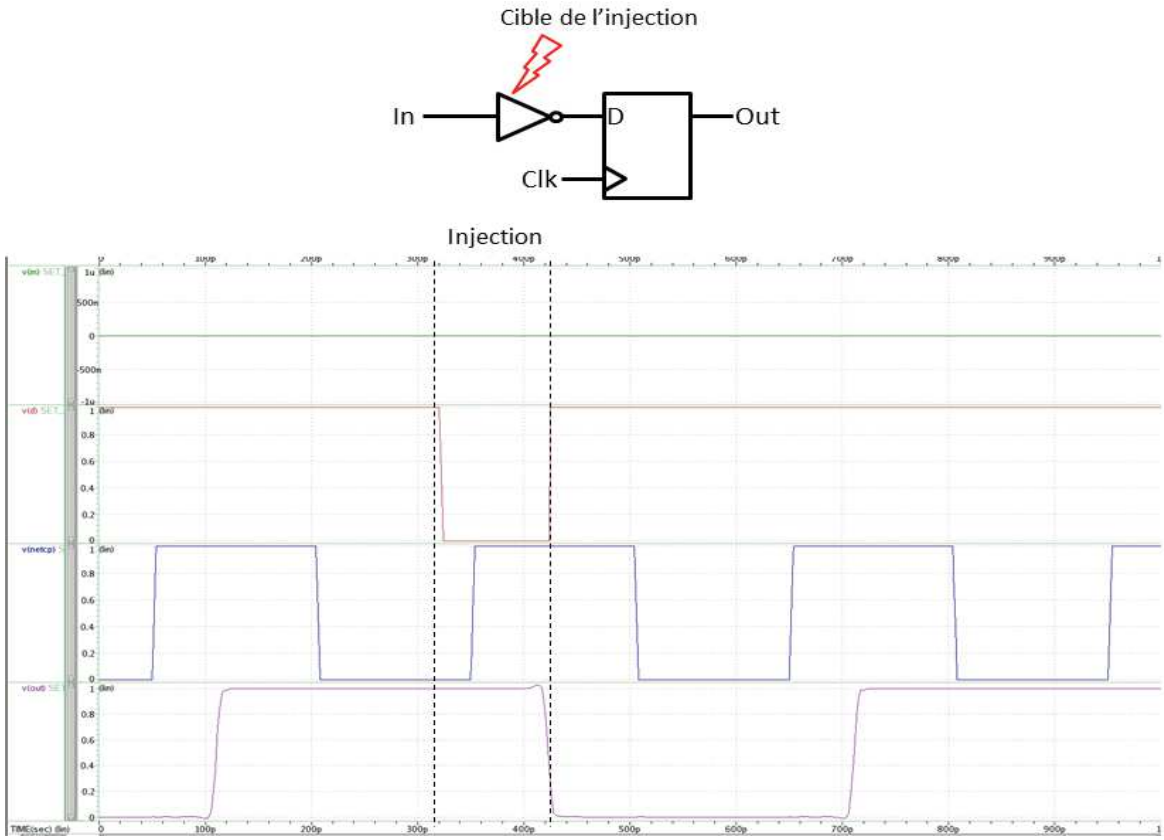


Figure I-18 : Mécanisme d'injection d'une faute de type single Event Transient (lors d'un front montant d'horloge)

Si un élément de mémorisation est directement illuminé, les contraintes temporelles pour injecter une faute dans le circuit sont plus faibles que pour un SET. En effet, ce type d'injection modifie directement la valeur logique stockée. Cette modification de la valeur logique s'appelle un Single Event Upset (SEU). La figure I-19 présente un schéma de principe de l'injection ainsi qu'un chronogramme de la propagation de la faute. Le signal d'entrée In de la bascule est maintenu à la valeur logique 1, cela a pour effet lors d'un fonctionnement normal de la bascule de maintenir la sortie (signal Out) de celle-ci à la valeur logique 1. Le signal Clk représente le signal d'horloge gérant la bascule. Le signal Injection représente le moment et la durée d'illumination de la bascule (la valeur de tension pour ce signal n'a aucune signification). On observe que lorsque la faute est injectée directement dans la bascule, quel que soit le moment d'injection (vis-à-vis du signal d'horloge), la faute est maintenue en sortie de la bascule jusqu'à la fin du cycle d'horloge durant lequel s'est produit l'illumination.

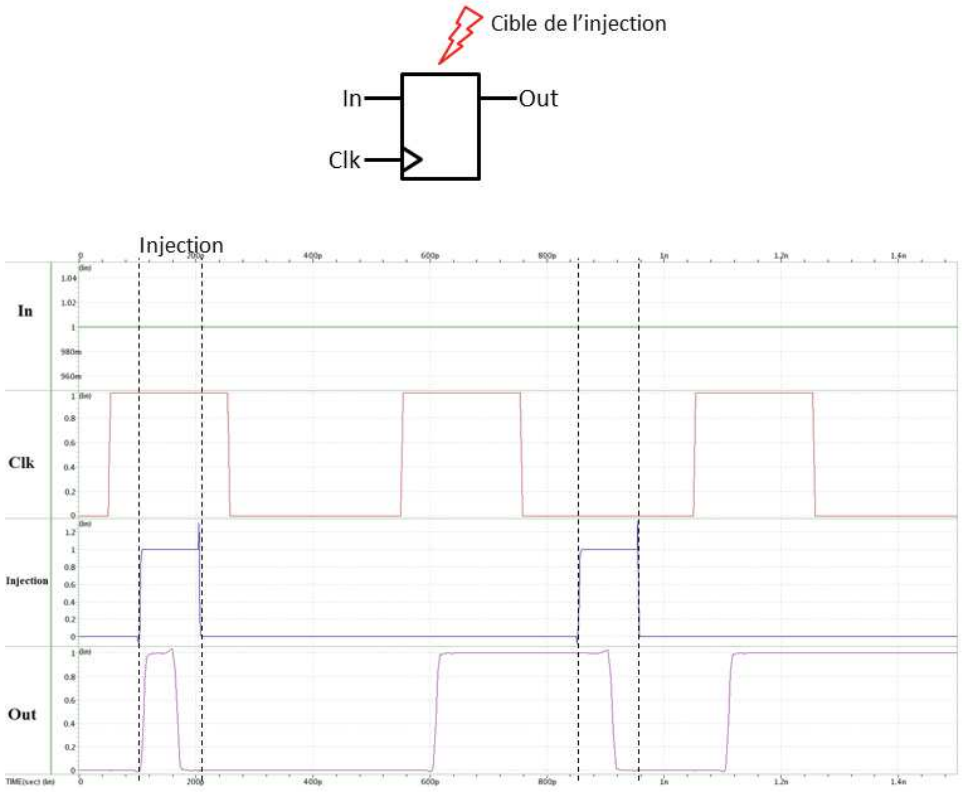


Figure I-19: Chronogramme d'injection d'un Single Event Upset

Ces évènements singuliers, qu'ils soient temporaires ou permanents, ont pour effet de créer des fautes dans le circuit. Une classification des différents types de fautes engendrés par ces évènements singuliers a été réalisée. Cette classification a pour but de pouvoir définir plus facilement le type de faute nécessaire à la réalisation d'une attaque en faute.

I.2.6. Les modèles de faute

Afin de pouvoir étudier les fautes sur le circuit, il est nécessaire de créer des modèles permettant de répertorier les différents comportements anormaux qu'il est possible de générer. Ainsi en connaissant ces effets, il est possible de mettre en place des attaques théoriques sur les algorithmes existant en réalisant des hypothèses impliquant ces modèles. Dans [28], les différents modèles de fautes sont présentés.

- Les fautes de type collage :

Les bits concernés par une faute de type collage ne changent plus, ils gardent la même valeur et écrasent toutes les valeurs arrivant sur ceux-ci.

Soit $B = \{b_0, b_1, \dots, b_n\}$ un set de bit choisi arbitrairement stocké dans la mémoire, on a alors :

$$b_i \rightarrow b_i{}' = b_i \quad \forall 0 \leq i \leq n$$

L'effet est permanent mais pas nécessairement destructif, c'est-à-dire qu'une remise à zéro (reset) complet du circuit peut permettre de récupérer un comportement normal du circuit. La valeur des bits collés n'est pas connue de l'attaquant. On considère généralement que les fautes de collage sont irréversibles car ce genre de faute provient souvent d'un court-circuit.

- Le bit flip :

Un bit flip consiste en un changement de la valeur logique en sa valeur complémentaire indépendamment de l'état initial. On a alors :

$$b_i \rightarrow b_i{}' = 1 - b_i \quad \forall 0 \leq i \leq n$$

Une telle faute peut provenir d'un effet transitoire, permanent ou destructif. La valeur du bit $b_i{}'$ est inconnue de l'attaquant à moins que celui-ci n'ait déjà connaissance de la valeur de b_i. L'un des intérêts de ce type de faute est que l'attaquant est sûr de créer une erreur quel que soit la donnée traitée.

- Le bit set et bit reset :

La faute de type bit set ou reset consiste au changement de la valeur d'un bit par une valeur fixe. On a alors :

$$b_i \rightarrow b_i{}' = c_i \begin{cases} c_i = 0 \rightarrow bit\ reset \\ c_i = 1 \rightarrow bit\ set \end{cases} \quad \forall 0 \leq i \leq n$$

Pour ce type de faute, l'attaquant modifie la valeur logique de manière fixe, la valeur logique est remplacée par 0 pour un bit reset ou par 1 pour un bit set, sans que l'attaquant ne connaisse à priori la valeur du bit avant la faute. On remarque aussi que le bit set (respectivement bit reset) ne modifie pas un bit qui était déjà à la valeur logique 1 (resp. à 0). Dans ce cas, le chiffré n'est pas erroné (ce phénomène est exploité lors des Safe Error Attack [29]).

- La faute aléatoire :

On peut aussi considérer comme modèle de faute plus général, la faute aléatoire. C'est une faute qui modifie la valeur de plusieurs bits du texte de manière aléatoire. On a :

$$b_i \rightarrow b_i{}' \in \{0,1\} \quad \forall 0 \leq i \leq n$$

La faute aléatoire est le modèle de faute le plus réaliste. Afin de pouvoir tirer des informations d'une telle faute, on considère généralement que la distribution a autant de chance de changer la valeur d'un bit en 0 ou en 1.

I.3. Modélisation et simulation

Quatre types de simulateurs permettent de modéliser les effets d'une injection laser sur un circuit : les simulateurs physiques, les simulateurs électriques, les simulateurs logiques et les simulateurs mixtes. Chacun de ces simulateurs utilise un niveau d'abstraction différent (silicium, transistor, porte logique).

Les simulateurs physiques (TCAD par exemple) modélisent les phénomènes physiques mis en jeu dans les matériaux se produisant au cœur du silicium lors de l'injection laser. Ce type de simulateur est très précis et donne un résultat proche de la réalité. Cependant il nécessite beaucoup de ressources de calcul pour simuler quelques transistors. De plus, il est nécessaire d'avoir une connaissance précise de la technologie simulée (dimensions des transistors, dopages etc). Un tel simulateur ne permet donc pas de simuler un circuit complexe.

Les simulateurs électriques (de type SPICE) reposent sur des modèles électriques modélisant l'injection laser. La précision d'un tel simulateur repose sur le modèle utilisé. Ceux-ci sont moins précis que les simulateurs physiques mais permettent d'accélérer grandement le temps de simulation, pour un résultat proche de la réalité.

Les simulateurs logiques travaillent au niveau d'abstraction des portes logiques. Ils permettent de connaître la propagation d'un ou plusieurs bits fautés à travers le circuit. Ce type de simulateur est très rapide mais permet seulement d'obtenir de l'information sur la propagation des fautes et de l'erreur obtenue.

Finalement les simulateurs mixtes mêlent les qualités des types de simulateurs précédents (précision et rapidité). Le niveau d'abstraction de la simulation est adapté à chaque partie du circuit. La simulation physique est réalisée sur la zone d'impact du laser. Un simulateur électrique est utilisé pour modéliser la propagation du courant au niveau des transistors environnant la zone de tir. Finalement, le simulateur logique sert à observer la propagation de la faute jusqu'en sortie du circuit.

I.3.1. Simulateur tLIFTING

Le simulateur tLIFTING a été développé par F.Lu dans le cadre du projet LIESSE (qui inclut les travaux présentés dans cette thèse) et présenté dans [30]. tLIFTING est un simulateur multi-niveaux (mixte) de propagation de fautes dans un circuit microélectronique.

La figure I-20 présente le mode de fonctionnement de ce simulateur. On quantifie d'abord la zone du layout illuminée ainsi que les caractéristiques du laser. On observe quelles jonctions PN sont

illuminées. Puis on détermine pour chaque jonction PN le photocourant induit à l'aide de modèles préétablis par expérimentation et/ou par modélisation physique. On réalise ensuite une simulation électrique (ici avec HSPICE) sur les portes logiques avales afin de déterminer la propagation de la perturbation (prise en compte des délais). Finalement, on utilise une simulation logique afin d'observer le cheminement de cette faute jusqu'à la sortie du circuit.

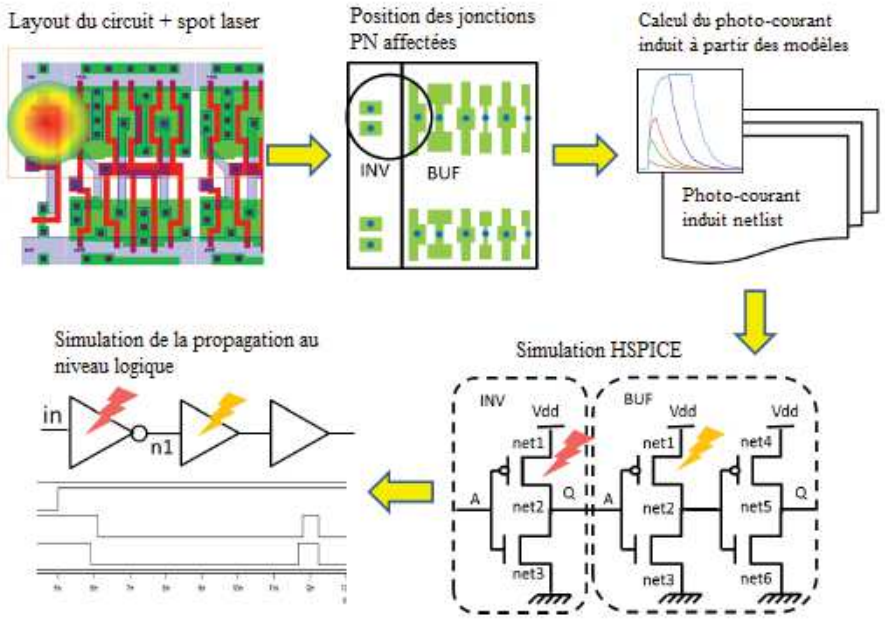


Figure I-20: Mode de fonctionnement schématique du simulateur tLIFTING [30]

L'intérêt de ce simulateur est donc la rapidité qu'il offre en ne simulant électriquement qu'une partie réduite du circuit. La zone illuminée ainsi que les transistors avals sont simulés de manière précise, on obtient donc un résultat de simulation proche d'une simulation électrique complète du circuit. La table 2 présente les temps de simulation de l'effet d'une illumination laser sur un circuit pour les simulateurs tLIFTING et HSPICE (simulateur purement électrique).

Le circuit cible ici, un circuit purement combinatoire, est un multiplieur 16x16bits (circuit de référence C6288 ISCAS-85). Ce multiplieur a une taille de 1286 (en équivalent porte). La simulation d'injection a été effectuée pour 63 vecteurs d'entrée différents. La valeur rapportée dans la table 2, correspond à la somme des temps de simulation du circuit pour les 63 vecteurs.

Pour le simulateur tLIFTING, les niveaux correspondent aux nombres de niveaux de portes logiques avals à la zone d'injection simulés de manière précise (prise en compte des délais de propagation du courant). Chaque porte logique directement connectée à la porte logique illuminée

représente le niveau 1 de simulation, les portes connectées à une porte du niveau 1 forment le niveau 2, etc. L'erreur donnée dans la table présente l'imprécision du simulateur tLIFTING sur le délai de propagation du signal fauté par rapport au délai obtenu en simulation HSPICE (erreur sommée pour les 63 vecteurs).

On remarque, d'une part que le temps de simulation de tLIFTING est beaucoup plus court que celui obtenu par HSPICE quel que soit le niveau de simulation de tLIFTING. On a un facteur de 30,5 entre le temps de simulation du circuit par tLIFTING (avec un niveau 27) et celle obtenue avec HSPICE. D'autre part, l'erreur dans les délais disparaît rapidement lorsque le niveau de simulation augmente. tLIFTING est donc un simulateur plus rapide et tout aussi performant qu'une simulation complète du circuit avec un simulateur électrique.

Table 2: Temps de simulation et erreur relative d'une injection laser sur un multiplieur 16x16bits [30]

Circuit	Taille	Vecteurs	tLIFTING					HSPICE
C6288	1286	63	Niveau 2	Niveau 7	Niveau 15	Niveau 23	Niveau 27	
Temps de simulation [s]			9,58	18,47	33,93	39,46	40,85	1248,75
Erreur [ns]			3,16	1,02	0	0	0	/

Nous nous intéressons dans la section suivante à l'établissement des modèles électriques utilisés dans ce simulateur.

I.3.2. Modélisation électrique d'un transistor 90nm sous illumination laser

Une modélisation électrique des transistors bulk en technologie 90nm sous illumination laser est présentée dans [31]. Cette section revient sur cette modélisation et son établissement. Cette modélisation servira de base pour l'établissement du modèle correspondant pour la technologie 28nm bulk et FDSOI.

a) Source de courant modélisant le photocourant induit

Le photocourant généré par l'illumination laser d'une jonction PN est modélisé par une source de courant connecté au nœud de collection de la jonction. On distingue pour cette source de courant deux grandes caractéristiques, l'amplitude maximale et l'enveloppe de la fonction de la source. L'amplitude maximale dépends des conditions expérimentales et notamment des paramètres du laser. La forme de l'enveloppe de courant dépend de la technologie et de la durée d'illumination.

i. Enveloppe du photocourant induit par illumination laser

L'enveloppe du photocourant induit dans une jonction PN est indépendante des conditions expérimentales, à part le temps d'illumination. En effet, cette enveloppe est une représentation mathématique du phénomène de collection des charges par la jonction. La figure I-21 présente l'enveloppe du photocourant induit. Elle est composée de deux exponentielles. La première exponentielle, croissante débute au moment de l'illumination de la jonction. Elle représente le moment où les porteurs de charges sont générés et commence à être collecté. Si le temps d'illumination est assez long (temps dépendant de la technologie utilisée pour la conception de la jonction PN) alors on atteint un régime stationnaire pour lequel la collection de charges ne peut plus augmenter. La seconde exponentielle de l'enveloppe quant à elle débute à la fin de l'illumination. Elle représente la collection des derniers porteurs de charges présents dans le silicium.

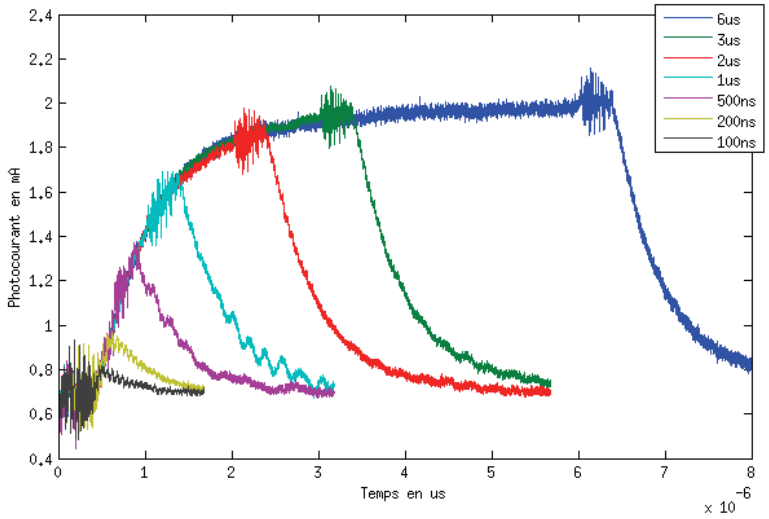


Figure I-21: Chronogramme du photocourant généré dans une jonction PN pour plusieurs durées d'illumination

Les équations (5) et (6) donne l'expression mathématique du modèle de l'enveloppe utilisé.

$$t_1 \rightarrow t_2 \qquad 1 - \exp\left(-\frac{t - t_1}{\tau_1}\right) \qquad (5)$$

$$t_2 \rightarrow +\infty \qquad exp\left(-\frac{t - t_2}{\tau_2}\right) * \left[1 - \exp\left(-\frac{t_2 - t_1}{\tau_1}\right)\right] \quad (6)$$

Où t_1 représente le début de l'illumination, t_2 la fin de l'illumination et τ_1 et τ_2 respectivement les constantes de temps de montée et de descente.

La constante de temps de descente τ_2 est liée à la vitesse de collection des porteurs par la jonction. Elle varie en fonction du nœud technologique utilisé. La constante de temps de montée est

indépendante du nœud technologique utilisé mais dépend des dopages du silicium. Elle est liée à la vitesse de génération des porteurs dans le silicium.

La forme de l'enveloppe étant relativement indépendante de la technologie utilisée, dans la suite du manuscrit, on ne modélise que les nouveaux paramètres modifiant l'amplitude maximale du photocourant induit pour les nouvelles technologies.

ii. Modélisation de l'amplitude maximale du photocourant induit

L'effet de l'injection laser est modélisé par une source de courant dont l'amplitude maximale dépend des caractéristiques suivantes :

- La puissance de tir du laser en W
- La polarisation en inverse des jonctions PN touchées en V: V_{PN}
- La dépendance spatiale (distance horizontale de la source à la jonction PN) : α_{gauss}
- La durée d'illumination : $Pulse_{width}$
- L'épaisseur du wafer (épaisseur de silicium traversée) : W_{coeff}
- La distance entre le plan focal et la zone sensible (appelé ici focalisation) : I_{ph_z}
- La surface de la jonction PN illuminée en µm²: S

Afin d'avoir un modèle simple facilitant les calculs pour une analyse au 1er ordre, on considère que chacun des paramètres cités plus haut sont indépendants les uns des autres.

La formule (7) donne l'expression de l'amplitude maximale de la source de courant (en ampère) modélisant le photocourant induit :

$$I_{ph} = (a * V_{PN} + b) * \alpha_{gauss} * Pulse_{width} * W_{coeff} * I_{ph_z} * S \qquad (7)$$

Les paramètres a et b sont des fonctions de la puissance du tir laser.

b) Détail de l'effet des paramètres sur une jonction PN

L'effet de chaque paramètre présenté dans la section I.3.a a été mesuré expérimentale par A. Sarafianos dans [31] sur une jonction PN. Dans la suite l'effet de chaque paramètre est décrit ainsi que la modélisation correspondante.

- <u>Dépendance de la polarisation et de la puissance de tir</u>

L'influence de la puissance du laser ainsi que de la tension de polarisation en inverse de la jonction PN est étudiée ici. Plusieurs expérimentations ont été réalisées pour modéliser l'effet de l'illumination par laser d'une jonction PN. Les jonctions PN étudiées sont les suivantes : N+/Pwell (drain/canal, source/canal pour un NMOS), P+/Nwell (drain/canal, source/canal pour un PMOS) et Nwell/Psub (jonction PN entre le puit dopé N contenant les PMOS et le substrat P du circuit). La figure I-22 présente un graphique de la valeur du courant traversant une jonction PN de type N+/Pwell suivant la polarisation et la puissance d'injection. En polarisation inverse, plus la puissance de tir est importante plus le photocourant traversant la jonction (en valeur absolu) est grand. La modélisation de la jonction Nwell/Psub est donnée en annexe. Pour chaque jonction, la forme du modèle est la même seule l'amplitude maximale change.

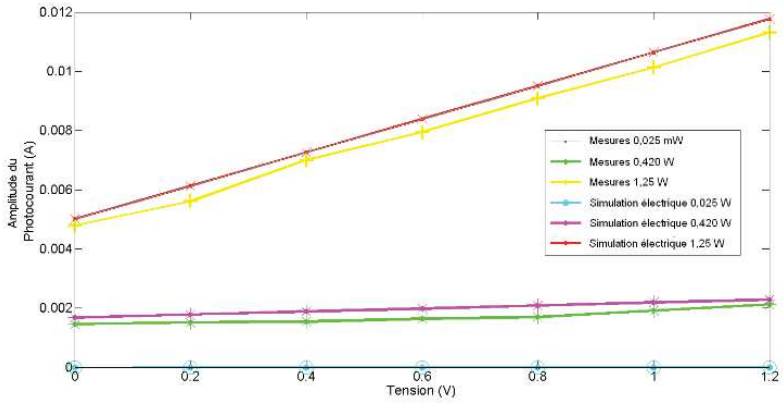


Figure I-22: Amplitude du photocourant induit en fonction de la tension de polarisation inverse de la jonction N+/Psub et de la puissance de tir [31]

La formule (8) permet de modéliser l'effet de la tension de polarisation et de la puissance de tir sur le photocourant :

$$I_{ph} = a * V_{PN} + b \qquad (8)$$

Avec I_{ph} le photo-courant induit, V_{PN} la tension de polarisation en inverse de la jonction. Les formules (9.1) et (9.2) donnent l'évolution des paramètres a et b qui sont fonctions de la puissance du tir (P_{laser}) :

$$a = 4 * 10^{-9} * {P_{laser}}^2 - 5 * 10^{-7} * P_{laser} + 9 * 10^{-6} \qquad (9.1)$$

$$b = 4 * 10^{-6} * P_{laser} \qquad (9.2)$$

- Dépendance spatiale

Afin de mesurer l'effet de la distance du laser à la jonction PN de type N+/Pwell, un balayage spatial suivant les deux dimensions du plan horizontal (x,y) a été réalisé. Compte tenu de l'aspect symétrique de la jonction PN utilisée pour les expérimentations, les mesures ont été restreintes à la partie positive d'un axe. On obtient alors la figure I-23, qui représente la valeur normalisée de l'amplitude du photocourant induit suivant la distance du faisceau à la jonction (l'aplomb de la jonction correspondant à d=0µm) pour plusieurs tailles de faisceau. On remarque que plus le faisceau est large (i.e. le grossissement est grand) plus la zone d'effet du faisceau sur la jonction est grande. La décroissance de l'amplitude du courant induit est gaussienne.

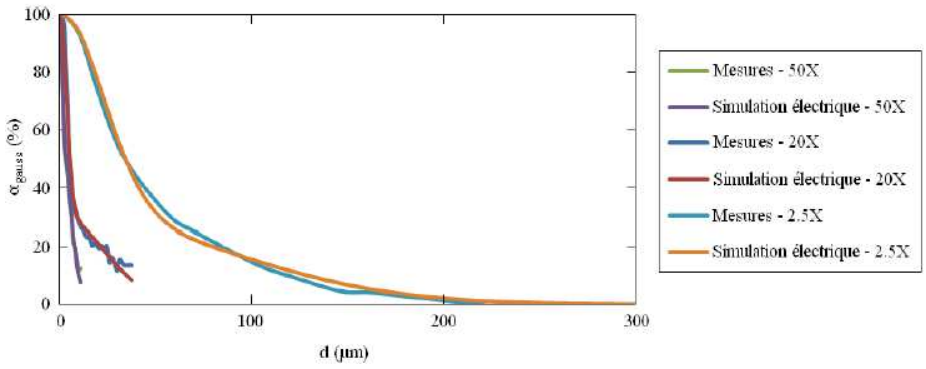


Figure I-23: Amplitude normalisée du photocourant induit en fonction de la distance du faisceau laser à la jonction PN [31]

La formule (10) modélise l'effet de la distance (horizontale) entre le faisceau et la jonction PN sur l'amplitude du photocourant induit:

$$\alpha_{gauss}(d) = \beta * exp\left(-\frac{d^2}{c_1}\right) + \gamma * exp\left(-\frac{d^2}{c_2}\right) \qquad (10)$$

- Durée d'illumination laser

L'effet de la durée d'illumination sur l'amplitude du photocourant induit dans la jonction PN est étudié ici. Pour mesurer cet effet, la jonction PN est illuminée avec plusieurs durées d'illumination. La figure I-24, présente l'amplitude du photocourant normalisée en fonction de la durée d'impulsion laser mesurée expérimentalement. On remarque que pour des temps longs (ici à partir de 500ns) on atteint le maximum de l'amplitude du photocourant généré. On a une amplitude plus faible pour des temps d'illumination plus courts. En plus de cet effet sur l'amplitude maximale du courant induit, la durée d'illumination a un effet sur le profil de l'impulsion de courant générée (cf I.3.2.a.i)

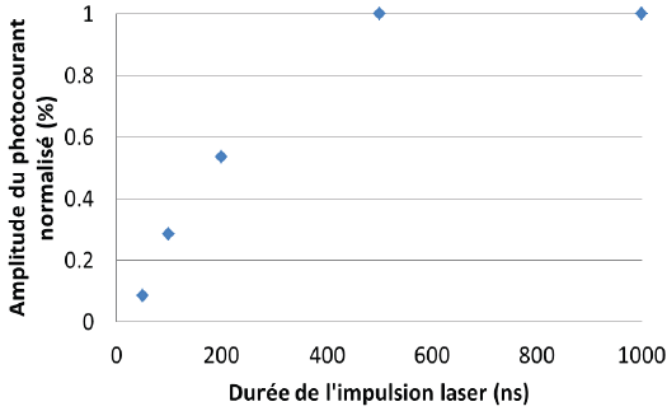


Figure I-24: Amplitude normalisée du photocourant induit en fonction du temps d'illumination de la jonction PN [31]

L'effet de la durée d'illumination est donné par la formule (11):

$$Pulse_{width} = 1 - exp\left(\frac{\omega}{250 * 10^{-9}}\right) \qquad (11)$$

Où ω qui représente le temps d'illumination est exprimé en s.

La figure I-25 présente le chronogramme de l'évolution de l'amplitude du photocourant induit en fonction du temps pour différents temps d'illumination. Pour des durées supérieures à 500ns (pour cette jonction), l'amplitude atteint une valeur maximale qui va se maintenir le temps de l'injection.

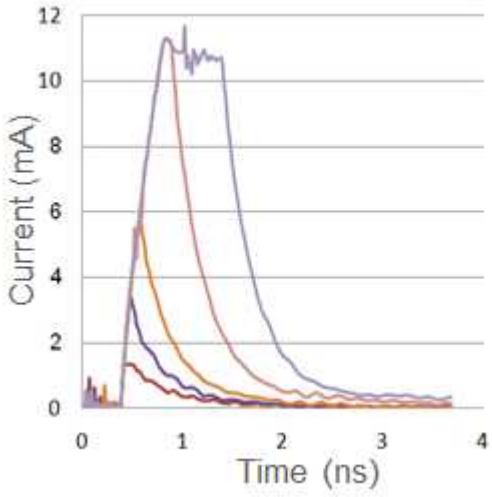


Figure I-25: Chronogramme du courant induit par l'illumination laser [31]

- Epaisseur du wafer

Ici l'effet de l'épaisseur du wafer sur le photocourant induit a été mesuré. Les résultats de ces expérimentations ont été rapportés dans la figure I-26. L'épaisseur du wafer a pour effet de modifier la distance parcourue par le faisceau à travers le substrat. Plus le wafer est mince, moins il y a de pertes d'énergies jusqu'à la zone sensible et donc plus la densité de charges générées au niveau de la zone sensible est importante. On observe donc bien sur la figure I-26 ce phénomène. Plus le wafer est épais, plus l'amplitude du photocourant induit est faible. On peut noter que le gain sur l'amplitude du courant est très faible pour des épaisseurs d'amincissement du wafer inférieures à 180µm.

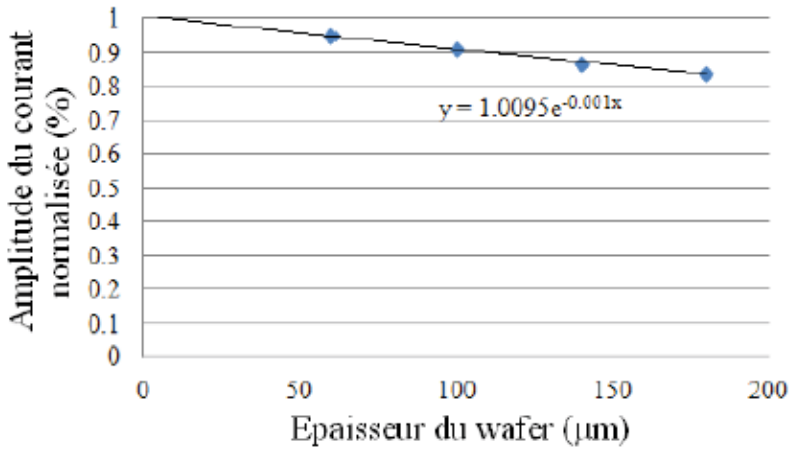


Figure I-26: Amplitude normalisée du photocourant induit en fonction de l'épaisseur du wafer [31]

L'effet de l'épaisseur du wafer sur le coefficient Wcoeff de l'équation 3 est modélisé par l'équation (12) suivante :

$$W_{coeff} = exp\left(-\frac{Wafer}{1000}\right) \quad (12)$$

où wafer représente l'épaisseur du wafer en µm.

- Focalisation du faisceau

La focalisation du faisceau à un rôle important lors d'un tir. C'est elle qui détermine la taille de la zone illuminée et donc l'énergie surfacique déposée. Si le faisceau est parfaitement focalisé sur la jonction PN alors l'énergie déposée par unité de surface au niveau de la jonction sera maximale. Au contraire si le faisceau est mal focalisé alors l'énergie surfacique de celui-ci sera répartie sur une plus grande surface, donc moins d'énergie par unité de surface déposée au niveau de la jonction PN. Les résultats des expérimentations concernant l'effet de la focalisation sont rapportés dans la figure I-27.

La position z=0µm correspond à une focalisation sur la jonction PN et donc au maximum d'amplitude de photocourant induit. Plus on s'éloigne du point de focalisation (dans un sens ou dans l'autre) et plus l'amplitude du photocourant induit est faible.

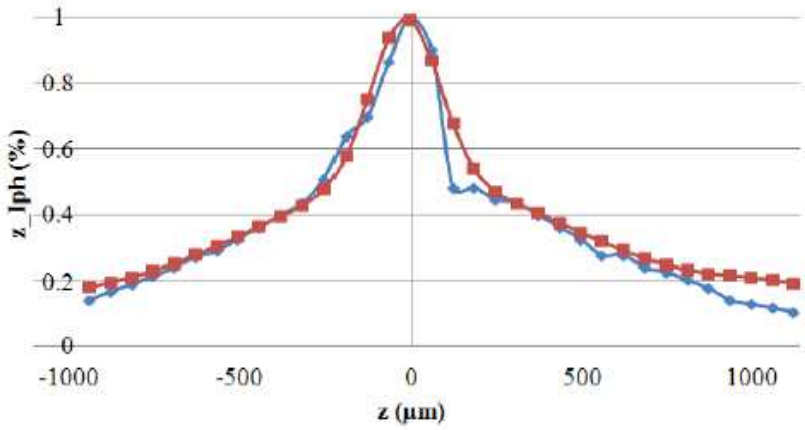


Figure I-27: Amplitude normalisée du photocourant induit en fonction de la focalisation du faisceau laser: courbe expérimentale (bleue) et modélisation (rouge) [31]

L'effet de la focalisation est modélisé par l'équation 13 suivante :

$$I_{phz} = (cz^6 + dz^5 + ez^4 + fz^3 + gz^2 + hz + i)(j * exp(-z/20000)) \quad (13)$$

Le modèle de la source de courant étudié précédemment, permet de modéliser le photocourant induit par un tir laser dans une jonction PN. Ce modèle peut être adapté afin de pouvoir modéliser l'effet de l'injection laser sur un transistor complet NMOS et PMOS en tenant compte des jonctions PN qui les constituent. La table 3 présente la valeur des coefficients de modélisation.

Table 3: Coefficients de modélisation de l'effet de la focalisation sur l'amplitude du photocourant induit

Coefficients	Valeurs	Unité
c	-3e-19	μm^{-6}
d	-9e-17	μm^{-5}
e	-8e-13	μm^{-4}
f	2e-10	μm^{-3}
g	-8e-7	μm^{-2}
h	-1e-4	μm^{-1}
i	0,49	ø
j	0,5	ø

c) *Modèle électrique d'un transistor bulk NMOS complet*

Afin de pouvoir modéliser l'effet d'un tir laser sur un transistor NMOS bulk complet, on décompose celui-ci en plusieurs jonctions PN de type N+/Pwell (drain/substrat P et source/substrat P). L'illumination laser de chaque jonction est modélisée par une source de courant. La figure I-28 donne une vue de principe d'un transistor NMOS bulk avec la mise en évidence des jonctions PN et du transistor bipolaire parasite le composant. Le transistor NMOS bulk est composé de deux jonctions PN de type N+/Pwell, drain/substrat P et source/substrat P (numéroté respectivement 1 et 2), ainsi que d'un transistor bipolaire (numéroté i). Chacune de ces entités va générer un courant lors de l'illumination laser.

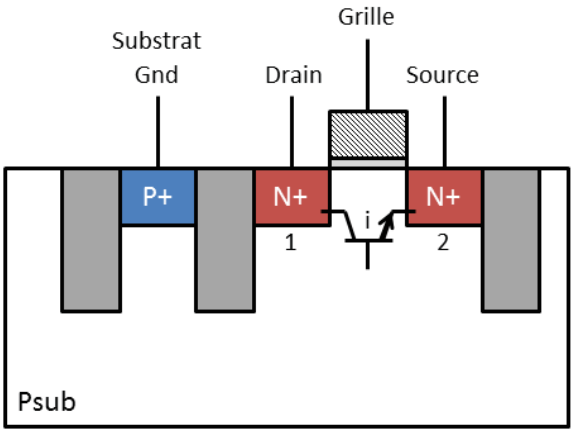


Figure I-28: Vue en coupe de principe d'un transistor NMOS bulk avec la mise en évidence des jonctions PN et du transistor bipolaire

Le modèle électrique présenté dans la figure I-29 est le résultat de cette décomposition. Pour le transistor NMOS on a deux types de sous-circuits modélisant le photocourant induit (cf. figure I-30) au niveau d'une jonction PN (Subckt Iph) et celui pour le transistor bipolaire NPN (Subckt SD). Les autres composants sont des résistances et des capacités permettant de modéliser les phénomènes physiques du matériau (temps de relaxation etc.).

Le premier sous-circuit, Subckt Iph, à gauche sur la figure I-30 modélise le courant injecté par une jonction PN illuminée. Ce sous-circuit est utilisé pour modéliser les deux jonctions PN, drain/substrat et source/substrat, du transistor NMOS. Il se compose d'une source de courant (modèle de source présenté dans la section I.3.ii.a) commandée par la tension de polarisation en inverse et par le signal LT ou laser trigger correspondant au temps l'illumination de la jonction par le laser. Sans illumination, la source de courant ne débite aucun courant dans le circuit. Lors de

l'illumination laser, la boucle se ferme et la source de courant débite un courant dépendant de la polarisation en inverse de la jonction PN dans le transistor.

Le second sous-circuit (Subckt SD) présenté à droite sur la figure I-30, modélise le courant induit par l'illumination du transistor bipolaire NPN. Ce transistor bipolaire étant composé du drain, du substrat et de la source du transistor NMOS. Ce sous-circuit est composé de deux sources de courant commandées par la tension du substrat. Lorsque le transistor NMOS n'est pas illuminé, la tension du substrat est nulle, aucunes sources de courant n'injectent de courant dans le transistor. Lors de l'illumination, la génération de charge dans le substrat due à l'effet photoélectrique va localement faire augmenter la tension de substrat. Si cette tension dépasse un certain seuil, le transistor NPN s'enclenche et les sources de courants débitent un courant au niveau du transistor NMOS.

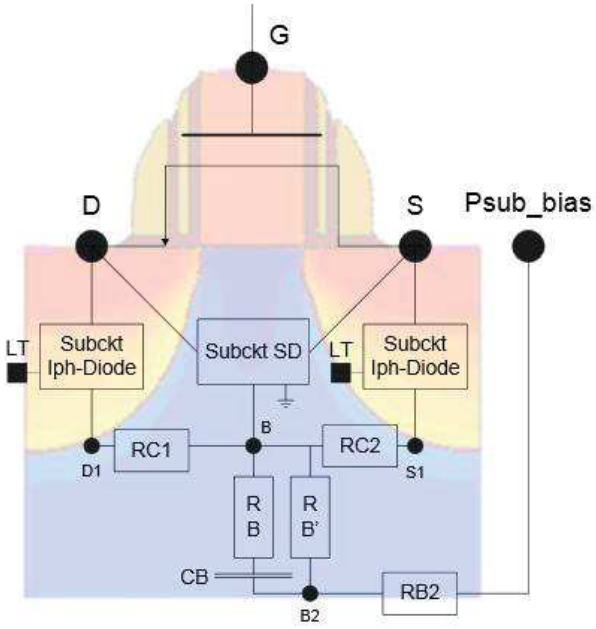


Figure I-29: Modèle électrique d'un transistor bulk NMOS sous illumination laser [31]

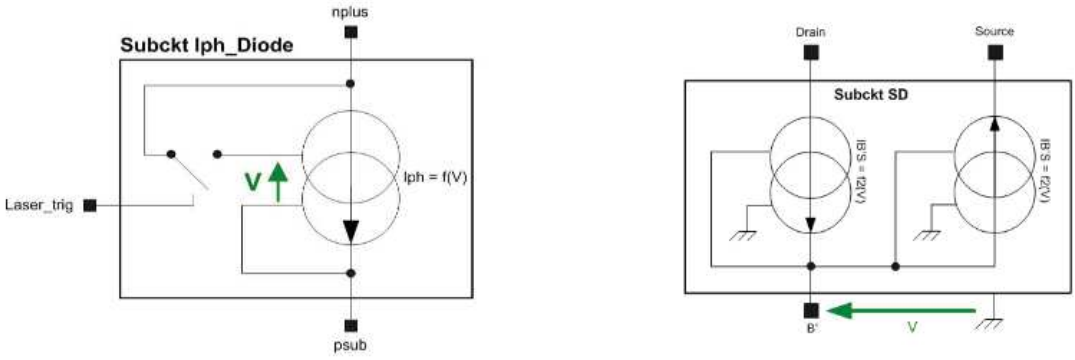


Figure I-30: Sous-circuit modélisant l'illumination d'une jonction PN (à gauche) et d'un transistor NPN (à droite) [31]

d) Modèle électrique d'un transistor bulk PMOS complet

Dans cette section, on s'intéresse au modèle électrique sous illumination d'un transistor bulk PMOS présenté dans [31]. La figure I-31 présente une vue en coupe de principe du transistor PMOS bulk avec la mise en évidence des jonctions PN et des transistors bipolaires présents dans cette structure.

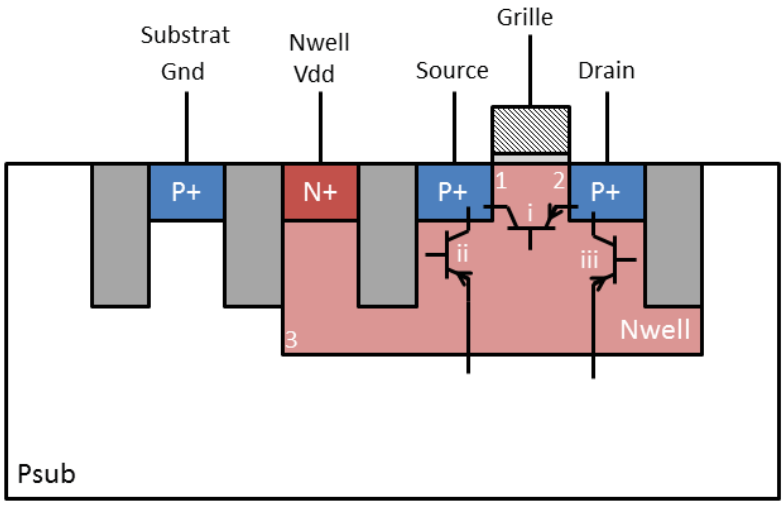


Figure I-31: Vue en coupe de principe de la structure d'un transistor PMOS bulk avec la mise en évidence des jonctions PN et transistors bipolaires présents

On a donc les jonctions PN et transistors bipolaires suivants :

- Source/Nwell (1) : jonction PN type P+/Nwell
- Drain/Nwell (2) : jonction PN type P+/Nwell
- Nwell/Psubtrat (3): jonction PN type Nwell/Psub
- Drain/Nwell/Source (i) : transistor bipolaire PNP
- Source/Nwell/Psubstrat (ii) : transistor bipolaire PNP

- Source/Nwell/Psubstrat (iii) : transistor bipolaire PNP

Ce modèle plus complexe, du fait de la présence du caisson N autour du transistor PMOS, est présenté dans la figure I-32. Comme pour le modèle du transistor NMOS, les résistances et capacités modélisent les caractéristiques physiques du matériau.

Les sous-circuits (Subckt Iph_diode et Subckt bip) utilisés pour le modèle électrique PMOS sont les mêmes que ceux présentés dans la section I.3.2.c. En effet, les sous-circuits dépendent du type d'entité (jonction PN ou transistor bipolaire). Le type de jonction (N+/Psub, P+/Nwell, etc.) ou de transistor bipolaire (NPN ou PNP) est pris en compte dans les caractéristiques intrinsèque de la source de courant utilisé dans le sous-circuit.

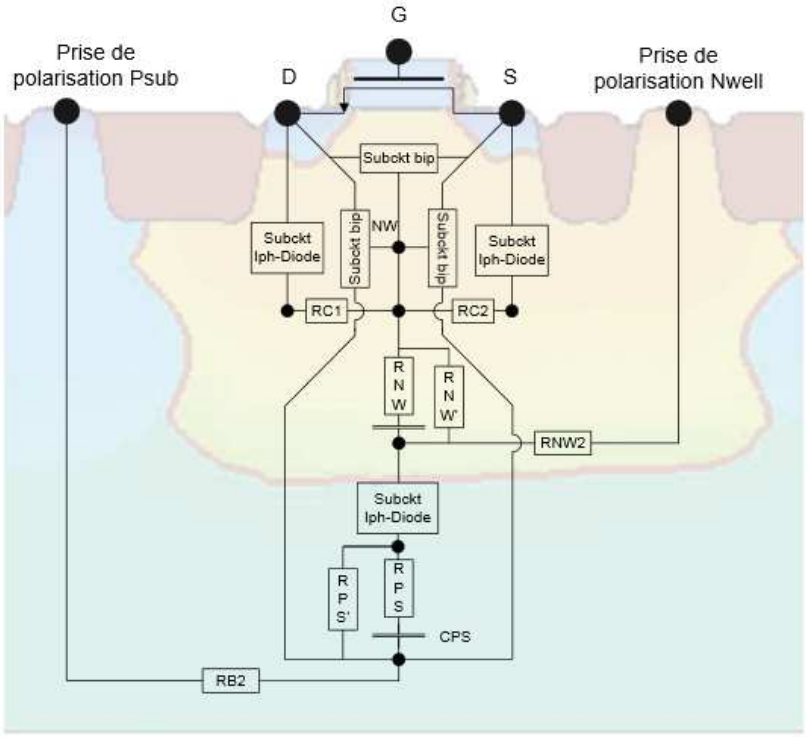


Figure I-32: Modèle électrique d'un transistor bulk PMOS complet sous illumination laser [31]

Les modèles présentés pour les transistors CMOS bulk précédemment ont été validés par l'expérience sur des transistors de technologie 90nm dans [31].

Conclusion

L'injection laser est une méthode de perturbation des circuits microélectroniques permettant de réaliser des attaques en fautes. L'illumination du silicium par le laser génère des porteurs de charges

dans le silicium par absorption de l'énergie apporté par les photons incidents (effet photoélectrique). La collection de ces charges au niveau de la zone sensible va créer un courant transitoire dans le circuit. Ce transitoire peut engendrer une faute, puis une erreur lors du calcul. C'est cette faute qui sera exploitée pour réaliser l'attaque en faute. Afin de pouvoir connaître les vulnérabilités d'un circuit, des simulateurs ont été développé. Des modèles électriques de transistors CMOS sous illumination laser ont été créés afin de simuler plus rapidement et plus précisément l'effet de l'injection sur le circuit. Le modèle élaboré par A. Sarafianos s'applique aux technologies CMOS bulk 90nm. Afin de compléter cette modélisation pour des technologies récentes, nous avons effectué des mesures sur des transistors en technologies 28nm bulk et FDSOI. Mais avant de nous intéresser à une modélisation précise de l'injection de fautes par laser, le chapitre suivant présente une étude pratique de l'injection de faute par laser dans un circuit cryptographique. Cette étude compare plus précisément les propriétés de l'injection par les faces arrière et avant d'un circuit cible.

Chapitre II.

Pratique de l'injection laser

Préambule

Ce chapitre présente la mise en place et la réalisation pratique d'attaques par injection de fautes par laser sur circuit intégré. Tout d'abord, deux méthodes d'injection, injection par la face avant et par la face arrière, sont décrites. Le protocole expérimental de préparation du circuit avant injection est décrit succinctement. Finalement, les méthodes d'injection par la face avant et par la face arrière sont comparées. Ces travaux ont fait l'objet d'une publication dans [32].

II.1. Description des méthodes d'injection laser sur un circuit microélectronique

La figure II-1 présente un schéma de chacune des méthodes d'injection. L'injection par la face avant (à gauche) correspond à un tir avec le faisceau allant des lignes de métallisations du circuit vers le substrat. Au contraire, l'injection par la face arrière traverse le circuit passant du substrat vers les lignes de métaux. Que ce soit l'injection par face avant ou par face arrière du circuit, chacune de ces méthodes possède ses avantages et inconvénients. Historiquement, pour l'injection de fautes à l'aide d'une source laser, la première méthode à avoir été utilisée est l'injection par la face avant. Cependant, cette méthode est beaucoup moins utilisée pour des circuits récents, car ceux-ci présentent de plus en plus de niveaux de métaux (de l'ordre de la dizaine pour les technologies récentes) et de protections visant à empêcher l'accès aux transistors (ajout de niveaux de métaux passifs ou actifs par exemple), au profit de l'injection par la face arrière qui permet de contourner ces protections.

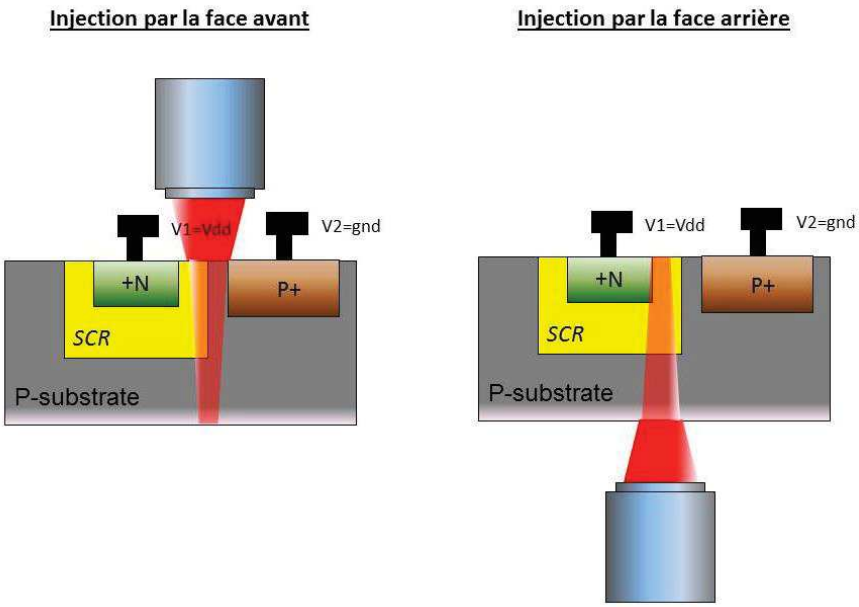


Figure II-1 : Les deux méthodes d'injection par laser, par la face avant (à gauche) et la face arrière (à droite)

Dans la section I.2.2.a, la génération de porteurs de charges dans le silicium a été décrite. Pour rappel, les distances de génération de porteurs suivantes sont données pour chaque longueur d'onde. Cette distance correspond à la profondeur de silicium à partir de laquelle il n'y a plus aucun

porteur de charges généré dans le silicium. La figure II-2 représente une vue à l'échelle de la profondeur de génération des charges dans un wafer de silicium de 100µm pour chaque longueur d'onde utilisée.

- Infrarouge : >>100µm
- Vert : 8µm
- Ultraviolet : 1µm

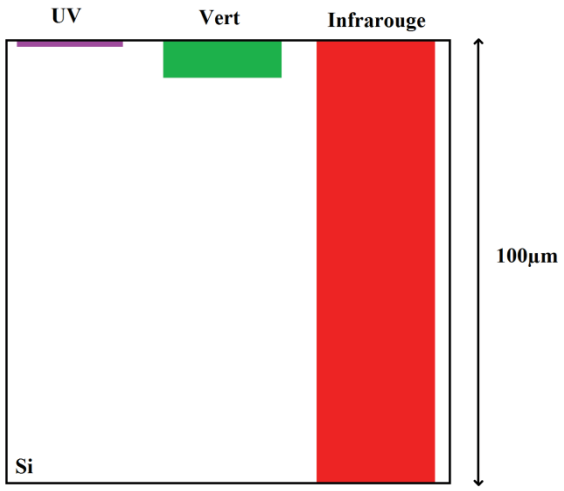


Figure II-2: Schéma à l'échelle de la profondeur de génération de porteurs de charges dans du silicium pour plusieurs longueurs d'ondes

Pour créer une faute dans le circuit, il faut que les porteurs de charges soient générés suffisamment proche des transistors pour être collectés. La méthode d'injection (par l'avant ou l'arrière) va impliquer l'utilisation d'une longueur d'onde spécifique afin de générer le plus de porteurs de charges au voisinage des transistors.

L'injection en face avant peut être effectuée en utilisant un faisceau laser de longueur d'onde verte, infrarouge ou ultraviolette. En effet, le faisceau laser n'a pas besoin de pénétrer profondément dans le silicium pour atteindre les transistors.

En injection par la face arrière, le faisceau doit traverser le substrat avant d'atteindre la zone des transistors. Il est donc nécessaire de réduire l'épaisseur de substrat. Un wafer non aminci a une épaisseur de l'ordre de 300µm et de l'ordre de 100µm après amincissement. Pour l'injection par la face arrière, seules certaines longueurs d'onde infrarouge sont possibles (de 700nm à 1100nm). L'utilisation d'une longueur d'onde infrarouge plus grande ne permet pas de générer un effet photoélectrique car l'énergie est inférieure au bandgap du silicium (on ne considère pas ici l'absorption deux photons). Une longueur d'onde plus faible ne permettrait pas d'atteindre ces zones en utilisant une énergie raisonnable.

II.2. Présentation de la préparation du circuit en vue d'une injection laser

Pour chaque méthode d'injection, le circuit doit être préparé afin de pouvoir être illuminé de manière optimale.

- Préparation pour l'injection en face avant :

Pour l'injection en face avant, le circuit doit être décapsulé. Cette opération consiste en le retrait du boitier du circuit tout en assurant l'intégrité du circuit et de ses fonctionnalités. Cette opération est généralement faite par traitement chimique manuel, semi-automatique ou automatique. La figure II-3 présente un banc de traitement chimique pour décapsuler le circuit. Cependant la décapsulation nécessite de manipuler des produits chimiques dangereux tels que de l'acide nitrique et de l'acide sulfurique fumants. Dans [33], une vidéo présente la décapsulation manuelle d'une carte SIM.

Figure II-3: Outil d'ouverture chimique de la face avant [14]

La décapsulation requiert un protocole de manipulation très précis pour obtenir un échantillon fonctionnel. Par exemple pour une carte à puce, on retire tout d'abord le circuit du support plastique en le découpant. Puis on place le circuit dans un bain d'acide afin de retirer le support collé à la puce. On place ensuite de l'acide nitrique fumant sur le circuit à l'aide d'une pipette afin de retirer la couche d'époxy du circuit. On laisse agir l'acide durant 10 à 30 secondes puis on place le circuit dans un bain d'acétone afin d'arrêter et d'enlever les produits de la réaction. Afin de retirer les derniers résidus d'acides de la surface de la puce, celle-ci est placée dans un bain à ultrason (solution

d'acétone soumise à des ultrasons). On obtient finalement une puce nettoyée et prête pour l'injection.

- Préparation pour l'injection face arrière :

Un wafer non aminci a une épaisseur de l'ordre de 300µm. La profondeur d'absorption de l'infrarouge dans le silicium est 1mm, c'est-à-dire que 36% de l'énergie maximale du faisceau est absorbée par le silicium au bout d'un millimètre. Afin de générer le maximum de porteurs de charges au niveau du transistor, le circuit doit être aminci. Cette opération est réalisée de manière mécanique afin d'obtenir une surface plane et polie pour éviter les pertes et avoir une énergie uniformément répartie (suivant le profil gaussien) dans la zone illuminée. On utilise un élément abrasif afin de venir retirer de manière progressive le substrat jusqu'à l'épaisseur voulue, comme sur le banc présenté sur la figure II-4. La difficulté de cette opération vient du fait que le circuit doit être aminci de manière uniforme sur toute la surface et assez aminci pour faciliter l'injection sans altérer les fonctionnalités du circuit. Pour une injection optimale sans destruction du circuit on réduit l'épaisseur du circuit à environ 100µm.

Figure II-4: Outil mécanique d'amincissement en face arrière [14]

II.3. Comparaison pratique de la méthode d'injection laser

II.3.1. Présentation de l'algorithme ciblé

La méthode à utiliser, face avant ou face arrière, afin d'injecter des fautes dans un circuit dépend du type de circuit et du banc d'injection. Nous avons mené une étude comparative de ces deux types d'injections vis-à-vis des fautes injectées sur un circuit ST CMOS 130nm bulk implantant un AES 128.

L'AES 128 est un algorithme de chiffrement symétrique, il est constitué d'une ronde initiale et de 10 rondes (9 rondes identiques et une ronde finale) manipulant des données organisées en blocs de 128 bits. La donnée et la clé se présentent sous la forme d'une matrice 4x4 respectivement M et K, chaque case de cette matrice contenant un octet (8bits). La figure II-5 représente une ronde de traitement de la donnée.

Chaque ronde comporte 4 transformations élémentaires :

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey.

- **SubBytes** est une opération de substitution d'octet. Cette bijection peut s'effectuer en utilisant une table préenregistrée ou en implantant la fonction logique correspondante. C'est la seule opération non-linéaire de l'AES.

- **ShiftRows** est un changement de position d'un octet dans la matrice de donnée, sans modification de la valeur logique de celui-ci. La permutation s'effectue entre octets d'une même ligne de la matrice de donnée.

- **MixColumns** est une multiplication (dans GF(2^8)) entre une matrice constante et la matrice de données. Cette opération utilise les 4 octets d'une même colonne de la matrice de donnée. Les opérations suivantes sont effectuées pour chaque colonne de donnée :

$$b_0 = 2a_0 + 3a_1 + 1a_2 + 1a_3$$
$$b_1 = 1a_0 + 2a_1 + 3a_2 + 1a_3$$
$$b_2 = 1a_0 + 1a_1 + 2a_2 + 3a_3$$
$$b_3 = 3a_0 + 1a_1 + 1a_2 + 2a_3$$

Où a_i représente le ième octet d'un vecteur de la matrice de donnée avant opération et b_i le ième octet de ce vecteur après l'opération du MixColumns.

- **AddRoundKey** est l'opération qui fait intervenir la clé de ronde. On ajoute à la matrice de donnée la clé de ronde par une opération de ou exclusif (xor) bit à bit.

Finalement après ces opérations sur la matrice M, on obtient une nouvelle matrice (ici C) qui est utilisé pour une nouvelle ronde de l'AES. 9 rondes sont ainsi exécutées. Le résultat de la 10eme ronde, identique aux 9 rondes précédentes à l'exclusion de l'opération MixColumns, est le message chiffré.

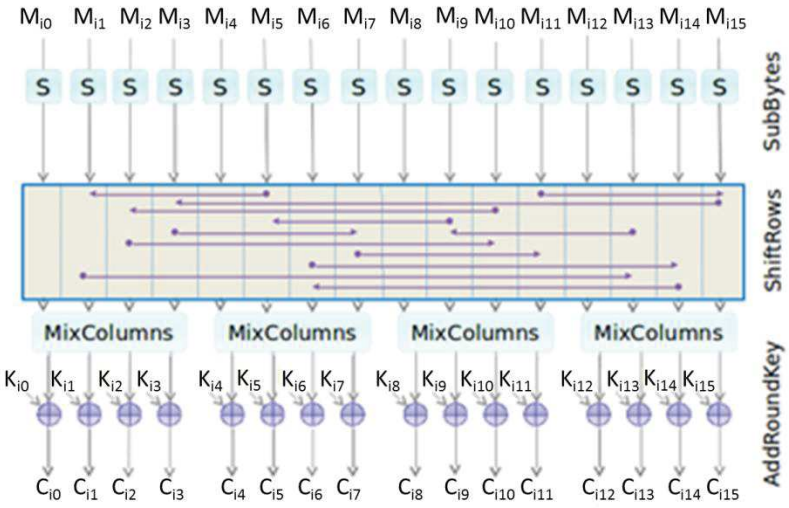


Figure II-5: ième ronde de l'AES (traitement de la donnée)

Le traitement de la donnée par l'AES est aussi accompagné d'un traitement de la clé secrète. Ce traitement a pour but de générer des sous-clés pour chaque ronde de l'algorithme à partir de la clé secrète. Chaque sous-clé est utilisée pour l'opération AddRoundKey. Si un attaquant connaît une clé de ronde (de n'importe quelle ronde), il peut alors retrouver la clé secrète complète.

La génération des sous-clés à partir de la clé secrète n'est pas détaillée ici.

On s'intéresse maintenant aux attaques sur cet algorithme. La table 4 décrit quelques-unes de ces attaques vis-à-vis de leurs cibles dans l'algorithme ainsi que le nombre de fautes à injecter nécessaires afin de retrouver la clé. Le nombre de fautes donné ici correspond au nombre d'injections nécessaires afin de réduire l'espace des clés et de pouvoir pratiquer une attaque par force brute (trouver la partie manquante de la clé en testant toutes les possibilités restantes).

On remarque dans ce tableau que pour des attaques visant les différentes parties de l'algorithme (donnée, clé ou compteur de ronde), les cibles (focalisation de l'attaque) sont, pour la plupart, des bits ou des octets. Par exemple pour l'attaque présentée dans [34], l'attaquant doit injecter une faute sur un bit du message durant la 9eme ronde. Il faut 16 injections de ce type afin de réduire

suffisamment l'espace des clés pour déterminer la clé complète par force brute (test de toutes les possibilités de clés restantes) en un temps raisonnable. Si l'injection ne donne pas une faute de ce type, alors la faute injectée est considérée comme inexploitable pour cette attaque.

Table 4: Quelques attaques en faute sur l'AES 128 [14]

Références	Nom usuel	Cible	Focalisation	#fautes
[35]	Biham et Shamir	Donnée (M_0)	Bit	128
[36]	Chien-Ning et Sung-Ming	7*donnée(M_8)+4*clé(K_9)	Octet	11
[34]	Giraud	16*donnée(M_9)	Bit	16
[37]	Piret et Quisquater	4*clé(K_9)+4*clé(K_{10})+4*donnée(M_8)	Octet	12
[37]	Piret et Quisquater	4*donnée(M_9) ou 1*donnée(M_8)	Octet	4 ou 1
[38]	Choukri et Tunstall	Compteur de ronde	Octet	1
[39]	Park, Moon et Cho	Compteur de ronde	Octet	1
[40]	Dusart, Letourneux et Vivido	4*donnée(M_9)	Octet	4
[41]	Robisson et Manet (DBA)	Donnée avant le premier SubByte	Bit ou Octet	16
[42]	Kim et Quisquater	Clé(K_7)	Octet	1
[43]	Ali, Mudhopadhyay et Michael	Donnée avant la 8eme ronde	Octet	1
[44]	Ali et Mudhophyay	Première colonne de la clé (K_8)	Octet	1

II.3.2. Obtention de l'information pour l'attaque de Piret et Quisquater (DFA)

On s'intéresse dans cette section à une attaque de type DFA sur l'AES, plus particulièrement l'attaque de Piret et Quisquater sur la donnée et à l'obtention d'information sur la clé par l'attaquant par cette attaque.

L'objectif de cette attaque est de modifier la valeur d'un octet de donnée entre l'opération de MixColumn de la ronde 8 et 9. La figure II-6 présente la propagation de la faute injectée jusqu'en sortie de l'algorithme.

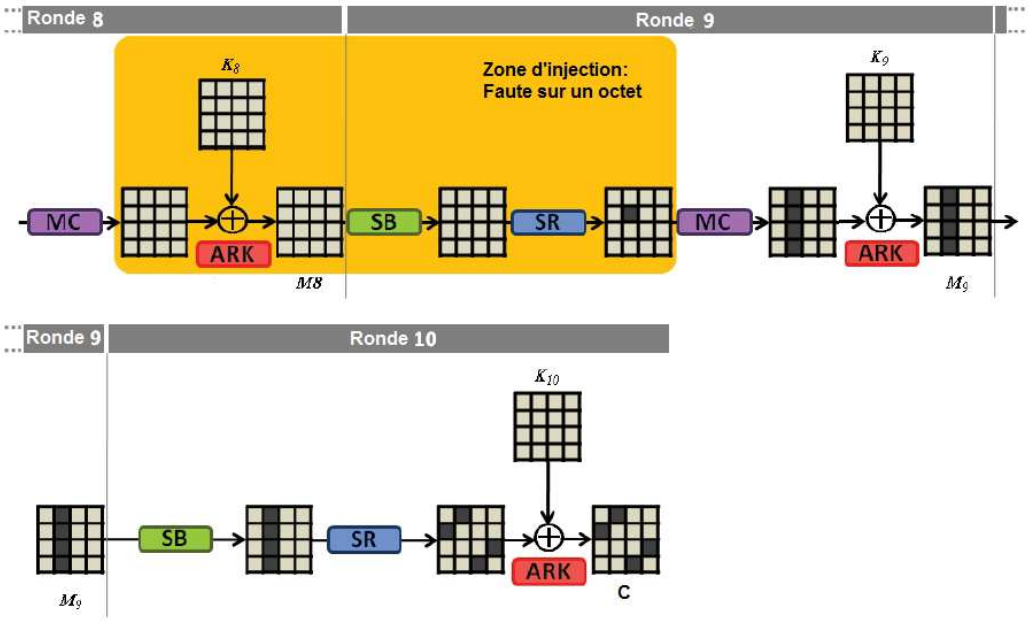


Figure II-6: Schéma d'injection de l'attaque de Piret et Quisquater [14]

On considère qu'une faute e est injectée sur un octet du State dans la zone d'injection (xor de e avec le State). On appelle M'_9 et C' respectivement la version erronée de M_9 et C (chiffré après la ronde 9 et chiffré de fin d'algorithme).

On a alors les équations suivantes :

$$M'_9 = MC\big(SR\big(SB(M_8)\big) \oplus e\big) \oplus K_9 \qquad (15)$$

$$C' = SR\big(SB(M'_9)\big) \oplus K_{10} \qquad (16)$$

$$C = SR(SB(M_9)) \oplus K_{10} \qquad (17)$$

On considère pour cette attaque, que l'attaquant peut choisir le texte clair et qu'il a accès au texte chiffré mais qu'il ne connaît pas la faute injectée. L'attaquant peut alors comparer les équations (16) et (17), il obtient :

$$ISR(C \oplus C') = SB(M_9) \oplus SB(M'_9) \qquad (18)$$

où ISR représente l'opération inverse du ShiftRow. A l'aide de l'équation (15), l'attaquant obtient :

$$ISR(C \oplus C') = SB(M_9) \oplus SB\big(MC\big(SR\big(SB(M_8)\big) \oplus e\big) \oplus K_9\big) \qquad (19)$$

L'opération de MixColumn est linéaire, on a alors l'équation (20) suivante :

$$ISR(C \oplus C^{'}) = SB(M_9) \oplus SB\left(MC(SR(SB(M_8))) \oplus K_9 \oplus MC(e)\right) \qquad (20)$$

De cette équation on en déduit l'équation (21) :

$$ISR(C \oplus C') = SB(M_9) \oplus SB(M_9 \oplus MC(e)) \qquad (21)$$

Ainsi pour cette équation, l'attaquant connaît le membre de gauche mais ne connaît pas le texte M_9 (qu'il cherche à obtenir), ni la faute injectée. L'attaquant peut alors faire des ensembles de distance suivant la valeur de la faute injectée pour une hypothèse de texte M_9 (octet par octet). En effet, l'attaquant connaît l'écart entre les deux SubBytes représenté par la valeur $C \oplus C'$, il peut alors créer des ensembles pour lesquels à un octet de texte donné M_9, on a une faute injectée correspondante. En effectuant cette étude pour plusieurs fautes différentes injectées, l'attaquant réduit ces ensembles jusqu'à retrouver la valeur du message chiffré M_9 et finalement retrouver la valeur de la clé. En effet, l'attaquant connaît alors l'entrée de la dernière ronde ainsi que la sortie, la seule inconnue est la clé K_{10}, il suffit après l'obtention de cette clé d'effectuer un traitement de clé inverse afin d'obtenir K_0 à partir de K_{10}.

II.3.3. Description de la cible d'injection

L'injection laser, de par sa précision temporelle et spatiale, permet d'atteindre de telles cibles avec plus ou moins de facilité suivant le matériel d'injection. Ici, la précision temporelle d'injection, temps d'injection dans l'algorithme, est grandement augmentée grâce à l'accès à un signal de trigger de début de l'algorithme. Nous comparons l'injection par face avant et par face arrière afin de déterminer si l'injection par la face avant est devenue impossible à réaliser (à cause des lignes de métaux) et si celle-ci est réalisable, quelle méthode est la plus efficace pour injecter des fautes mono-bit ou mono-octet.

Pour ce faire, nous utilisons un circuit implantant l'algorithme AES. Ce circuit a été développé par l'école des Mines de Saint-Etienne et fabriqué en technologie AMS CMOS 130nm. Le circuit fonctionne à une fréquence de 25MHz. Chaque opération de l'AES est implantée en bloc logique gérant les 128 bits de données en parallèle. Le circuit comprend aussi deux registres de 128 bits (registre de ronde et registre de clé) ainsi qu'une machine à états finis gérant l'ordonnancement des différentes opérations. Une ronde de l'AES s'effectue en un cycle d'horloge soit 40ns. Les bascules composant le registre de donnée sont dispersées dans le circuit. La figure II-7 présente une vue du circuit et des zones dans lesquelles sont placées les différentes partie du registre mémorisant un octet de donné. Chaque zone est un carré de 100µm*100µm. Par exemple la zone bleue notée #15 stocke la valeur du 16eme octet de la donnée (valeur des zones allant de 0 à 15).

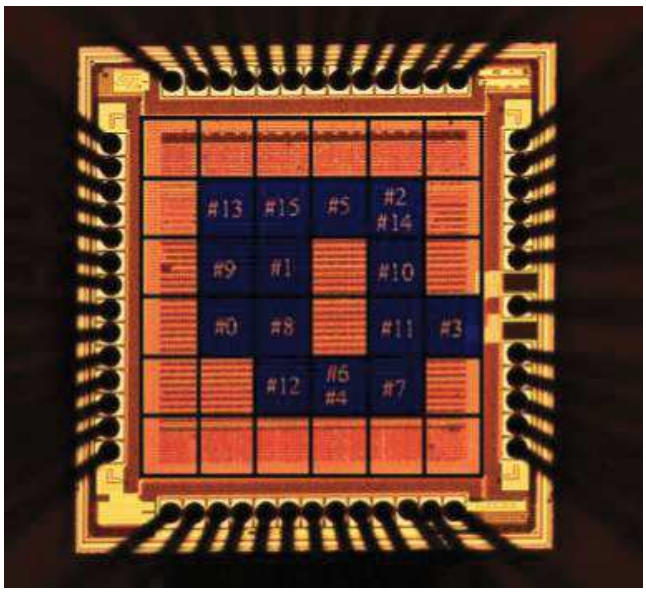


Figure II-7: Placement des registres dispersés à travers le circuit (zones bleues) [21]

Pour l'expérimentation, ce circuit est placé sur une carte fille, elle-même reliée à un FPGA. La figure II-8 présente une image de ce montage. Le FPGA synchronise les commandes de tirs avec la source laser et les commandes de communications avec le circuit (chargement des registres, lancement du chiffrement).

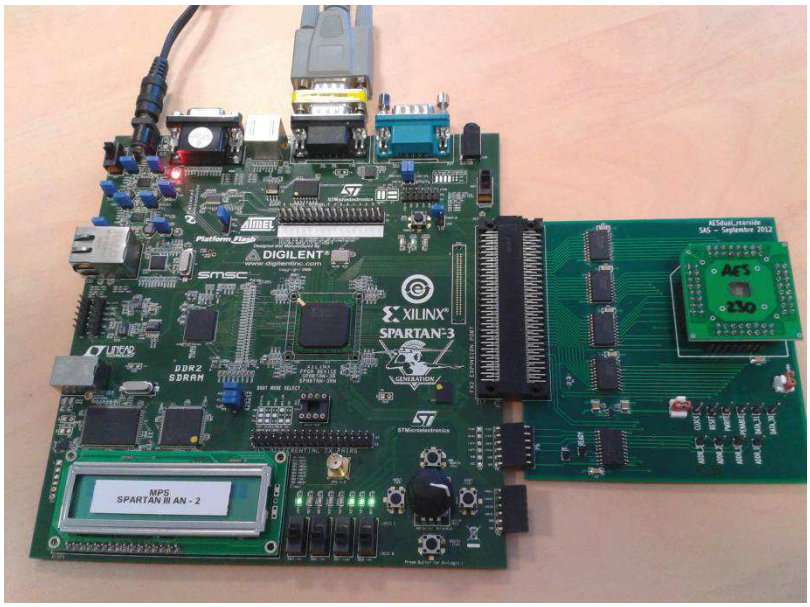


Figure II-8: Montage expérimental (FPGA, carte fille et circuit)

Lorsque l'utilisateur envoie une requête de chiffrement via le port série du FPGA, celui-ci génère un signal composé de deux triggers. Le premier trigger lance la préparation de la source laser. La

source laser utilisée a un temps de préchauffage de 200µs avant chaque tir. L'autre trigger correspond à la commande de chiffrement de l'AES. Le délai entre ces deux triggers est paramétrable par pas de 40ns. Ceci permet d'illuminer le circuit durant une ronde spécifique de l'AES. Une gigue de 10ns peut être observée entre l'ordre de tir (préchauffage fini) et le tir effectif.

Le circuit est placé sur une table XY permettant de déplacer le circuit sous la source laser avec une précision de 0,1µm.

II.3.4. Comparaison des deux méthodes d'injections en termes de fautes exploitables

Afin de comparer les deux méthodes d'injection (face avant et arrière), on s'intéresse à la facilité de réussite de chacune de ces méthodes à créer des fautes exploitables pour l'attaque de Piret et Quisquater. Pour réaliser cette attaque, les fautes doivent être injectées dans la donnée sur un seul octet avant l'opération de MixColumn de la 9eme ronde de l'AES.

Ici, l'objectif n'est pas de réaliser une attaque pratique sur l'AES mais de déterminer les caractéristiques des fautes injectées suivant les deux méthodes. Pour cela, l'expérience est facilitée par l'accès à un signal de début de chiffrement, ainsi que par le choix du texte et la connaissance de la clé de chiffrement. On peut donc avec ces informations supplémentaires, connaître la faute injectée ainsi que le moment d'injection au niveau du chiffrement.

La table 5 résume les paramètres expérimentaux utilisés pour l'injection laser pour chaque méthode. L'énergie du faisceau laser utilisée est sensiblement la même pour les deux méthodes. La taille du faisceau est différente pour les deux méthodes. On utilise ici les plus grandes tailles de spot laser possibles (sur le banc laser) à notre disposition pour chaque méthode. Ce choix de taille des faisceaux permet d'émuler les résultats qui pourraient être obtenus avec un banc laser de moins bonne qualité, i.e. un banc ne disposant que d'optiques peu performantes.

Table 5: Paramètres laser expérimentaux

	Injection par face avant	Injection par face arrière
Durée d'illumination	5ns	5ns
Longueur d'onde utilisée	Vert (532nm)	Infrarouge (1064nm)
Energie du faisceau*	525nJ	675nJ
Taille de faisceau	125µm*125µm	50µm*50µm

L'énergie du faisceau est donnée à titre indicatif, elle représente la valeur donnée en commande à la source laser. Cette énergie ne correspond pas à l'énergie déposée sur le circuit, celle-ci est plus faible (atténuation des chemins optiques, etc.)

Pour comparer les deux méthodes d'injection en termes d'efficacité, c'est-à-dire en termes d'injection utile, nous définissons les métriques suivantes.

Le taux d'injection donné par l'équation 22 représente la facilité d'injection de n'importe quel type de faute comparée au nombre de tir effectué. C'est-à-dire le quotient du nombre de fautes injectées par le nombre de tirs effectués.

$$Taux\ d'injection = \frac{\#fautes}{\#tir} \qquad (22)$$

Le taux de fautes mono-octet et le taux de succès mono-octet sont définis par les équations 23 et 24. Ils représentent respectivement le nombre de fautes mono-octet injectées en rapport au nombre de fautes injectées (n'importe quel type) et au nombre de tir effectué.

$$Taux\ de\ fautes\ mono-octet = \frac{\#fautes\ mono-octet}{\#fautes} \qquad (23)$$

$$Taux\ de\ succès\ mono-octet = \frac{\#fautes\ mono-octet}{\#tirs} \qquad (24)$$

De la même manière, nous définissons le taux de fautes mono-bit et le taux de succès mono-bit. Les équations 25 et 26 donnent l'expression de ces taux.

$$Taux\ de\ fautes\ mono-bit = \frac{\#fautes\ mono-bit}{\#fautes} \qquad (25)$$

$$Taux\ de\ tirs\ réussis\ mono-bit = \frac{\#fautes\ mono-bit}{\#tirs} \qquad (26)$$

La campagne d'injection a été réalisée en utilisant une clé et un texte fixe pour toute la durée de l'expérimentation. Chaque zone du circuit définie figure II-7 a été illuminée 1000 fois, et pour chaque tir la faute injectée a été enregistrée.

La table 6 résume les valeurs obtenues pour le taux d'injection, le taux de fautes mono-octet et le taux de fautes mono-bit.

Le taux d'injection pour l'injection par face arrière est de 100%, alors qu'il n'est que de 55% en face avant bien que la taille du spot laser soit plus grande (50µmcontre 125µm de diamètre). Nous détaillerons plus loin les raisons de ce résultat.

Inversement, le taux de fautes mono-octet est de 78% pour l'injection par face avant et de 32% pour l'injection par face arrière. Il est plus facile d'injecter, au moins sur le circuit utilisé, des fautes mono-octet avec une injection par la face avant, même avec un faisceau plus large.

On observe la même tendance pour les fautes mono-bit puisque le taux pour l'injection face avant est de 4% alors qu'il n'est que de 0,4% en face arrière.

Table 6: Taux d'injection et taux de fautes

	Taux d'injection	Taux de fautes mono-octet	Taux de fautes mono-bit	Taux de fautes multi-octets
Face avant	55,4%	78%	4%	12%
Face arrière	100%	32%	0,4%	68%

Par la face avant, avec un faisceau laser de 125µm de diamètre, avec cette technologie, quelques dizaines d'éléments de mémorisation sont illuminés simultanément contre 2 ou 3 pour l'injection par la face arrière avec un faisceau de 50µm de diamètre. Pourtant le taux de fautes multi-octets est bien plus grand lors d'une illumination en face arrière qu'en face avant. Ces résultats expérimentaux peuvent être expliqués par la présence des lignes de métaux sur la face avant du circuit. En effet ces lignes de métaux agissent comme un miroir et reflètent une partie des rayons laser incidents. Ainsi même avec un faisceau plus large, il est plus difficile d'injecter une faute (tous types confondus) dans le circuit en utilisant l'injection par la face avant que par la face arrière. De plus, du fait qu'une partie du faisceau laser incident est réfléchie par les lignes de métaux, la zone de silicium illuminée est alors plus petite. Ceci explique le fait qu'il est possible d'injecter plus facilement des fautes mono-octet et mono-bit par la face avant. Ainsi pour ce circuit, il est plus simple de réaliser une attaque en injectant par la face avant.

La table 7 donne les résultats des taux de tir mono-octet et mono-bit pour chaque octet de la donnée. On remarque qu'il est impossible de réaliser une injection de faute de type mono-bit et quasiment impossible pour des fautes de type mono-octet, par la face arrière avec un faisceau aussi large. Tous les taux de tir mesurés pour chaque octet de la donnée sont plus élevés pour l'injection en face avant. Ceci s'explique encore par un effet de filtrage du faisceau laser par les lignes

métalliques présentes au-dessus du circuit. Il faut cependant remarquer que pour les taux de tir mesurés pour l'injection en face avant, on observe une disparité dans les valeurs des taux. Par exemple on a un taux de tir mono-octet de 45% pour l'octet 7 alors qu'il est de 1% pour l'octet 12. Cette disparité s'explique par le fait que les lignes de métaux ne permettent pas d'illuminer toutes les zones du circuit puisqu'elles créent des zones d'ombres. Ainsi si un des registres 8 bits est placé sous une ligne de métal il sera plus difficile de l'atteindre (d'où le taux de tir plus bas).

Table 7: Taux de tir mono-octet et mono-bit pour l'injection en face avant et arrière selon l'octet visé

	Taux de tir réussis mono-octet		Taux de tir réussis mono-bit	
Octet	**Face avant (%)**	**Face arrière (%)**	**Face avant (%)**	**Face arrière (%)**
#0	28	0,5	3,3	0
#1	1,8	0,4	1	0
#2	15	0,3	0,9	0,2
#3	32	0,4	6,2	0
#4	29	0	5	0
#5	5	0	0	0
#6	18	0.1	5	0
#7	45	0.1	1,6	0
#8	17	0,1	2,5	0
#9	2,5	0,1	1	0
#10	6	0	3,3	0
#11	34	0,1	2,2	0
#12	1	1	0	0
#13	15	0	1,4	0
#14	24	0	1,6	0
#15	6,9	0,1	2,9	0

II.3.5. Mesures de la taille du faisceau illuminant le silicium par injection en face avant

Nous avons souhaité estimer expérimentalement l'effet de la réduction de la taille du faisceau laser. Pour ce faire, nous avons réalisé une campagne d'injection par la face arrière du circuit en réduisant progressivement la taille du faisceau jusqu'à obtenir un taux de fautes mono-octet équivalent à celui obtenu par la campagne d'injection par face avant précédente (faisceau 125µm de

diamètre). Ici on fait l'hypothèse que le résultat obtenu en injectant par la face arrière est équivalent à une injection par la face avant, sans ligne de métallisation. La figure II-9 représente le taux de faute mono-octet en fonction de la taille du faisceau. Comme attendu, plus la taille du faisceau est grande et plus le taux de fautes mono-octet est faible. Le taux de 78% de fautes mono-octet, obtenu en face avant, est atteint avec une taille de 5µm de diamètre en face arrière. Paradoxalement, pour ce circuit, cette mesure montre que l'injection avec un faisceau laser large par la face avant est aussi efficace que l'injection par la face arrière avec un faisceau de 5µm de diamètre.

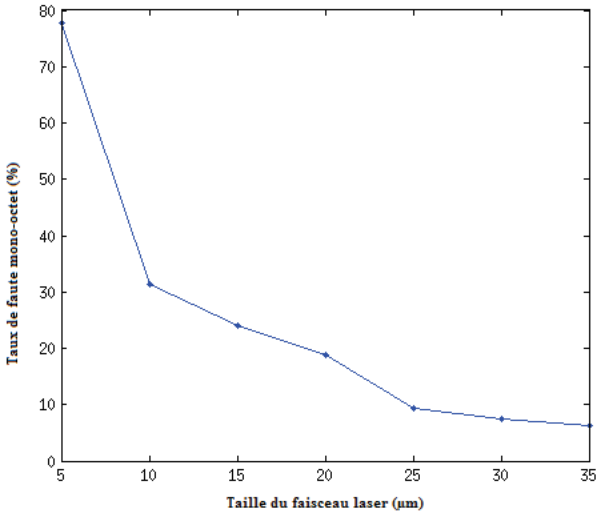


Figure II-9: Taux de faute mono-octet en fonction de la taille du faisceau pour l'injection en face arrière

Ce résultat expérimental correspond aux règles appliquées lors de la conception de ce circuit. En effet, six niveaux de lignes de métallisation sont utilisés. Les deux premiers niveaux de métal forment une grille régulière dont les « carreaux » ont une largeur de 12µm et sont espacés de 8µm.

Ces « trous » de 8µm*8µm correspondent à la taille de 5µm*5µm mesuré en injectant en face arrière.

Les 4 niveaux inférieurs sont quant à eux composés de lignes de métaux large seulement de 0,8µm et espacées de 0,8µm au moins. Ils n'agissent donc que très peu en tant qu'écran. De plus la taille des bascules utilisées pour mémoriser les bits de données est de 4,8µm*5,6µm. Ainsi, la disparité observée dans les taux de tir mono-octet et mono-bit observés précédemment s'explique par le fait que lors d'une injection par la face avant, certains éléments de mémorisation sont occultés par les lignes de métaux.

On peut conclure des expériences précédentes, qu'avec un équipement de bas coût, i.e. des optiques ne permettant pas une focalisation fine, les attaques par la face arrière du circuit semblent difficiles à mener. En effet, il est difficile pour cette méthode d'injection d'obtenir des fautes de type mono-bit ou mono-octet, qui sont les plus courantes pour des attaques en fautes. De plus, paradoxalement, l'injection par la face avant avec un faisceau large permet d'obtenir ce type de faute et donc de pouvoir réaliser des attaques en fautes.

Cependant, cet avantage tend à disparaître au profit de l'injection par la face arrière. En effet, sur les technologies plus récentes que celle utilisée pour l'expérimentation (130nm) le nombre de niveaux de ligne de métallisation a augmenté de manière considérable. La figure II-10 présente l'évolution du nombre de niveau de métallisation en fonction du nœud technologique. Ainsi pour les technologies 65nm, 10 niveaux de métallisations sont utilisés pour assurer le fonctionnement d'un circuit. Avec un tel nombre de niveaux, les zones d'ombres sont beaucoup plus étendues, il faut alors s'interroger sur la possible obtention de fautes exploitables en utilisant l'injection par la face avant.

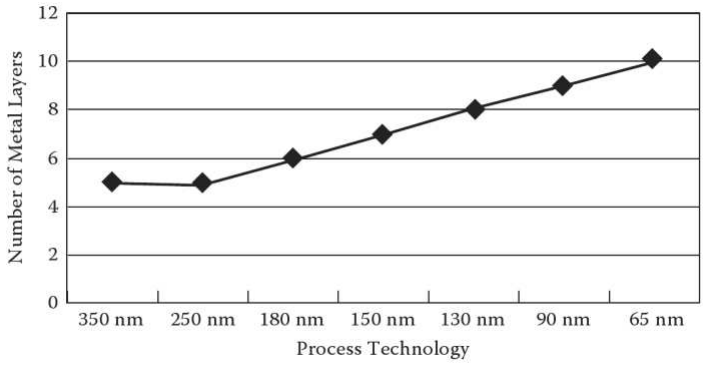


Figure II-10: Nombre de niveaux de métallisation en fonction du nœud technologique [45]

De plus, afin d'assurer la planéité du wafer lors de la fabrication en fonderie, l'espace entre les lignes des métallisations sont remplis par un matériau diélectrique. Cette planéité est nécessaire afin de réaliser les opérations de polissage chimique et mécanique de la fabrication du circuit. Pour des technologies inférieures à 65nm, des contraintes supplémentaires sont nécessaires lors de la réalisation du circuit. En plus de l'ajout du matériau diélectrique, des « tuiles » (lignes de métallisation ne transportant aucun signal) sont ajoutées afin de combler les espaces dans chaque niveau de métallisation.

Cette comparaison a fait l'objet de la publication [32].

Conclusion

L'injection laser peut être effectuée par la face avant ou arrière d'un circuit. L'injection par la face avant ne nécessite qu'une ouverture du boitier. Par contre, le circuit pour l'injection en face arrière doit être aminci afin de réduire l'épaisseur de silicium traversée par le faisceau et ainsi réduire les pertes d'énergies. Suivant le banc laser à disposition et la cible de l'injection, l'une de ces deux méthodes présente plus d'avantages en termes de fautes exploitables pour une attaque. L'injection face avant peut permettre d'obtenir plus facilement des fautes exploitables même avec un banc laser de qualité moyenne en termes de focalisation spatiale du faisceau, et ce pour des technologies « anciennes » que par une injection par la face arrière avec la même focalisation spatiale. Les lignes de métal présentes à la surface du circuit agissent comme un miroir pour le faisceau, réduisant ainsi la zone de silicium illuminée. Cependant les zones pouvant être illuminées sont dépendantes du layout du circuit et des lignes de métallisations. Ces résultats ne sont plus vérifiés pour des technologies plus récentes où des lignes métalliques supplémentaires sont ajoutées afin de répondre aux contraintes de conception du circuit. Pour ces technologies, l'injection par la face arrière est préférable. Cependant afin d'obtenir des fautes exploitables la focalisation du faisceau doit être plus importante, ce qui entraîne un coût plus élevé sur l'achat du banc laser. Dans le chapitre suivant, une mise à jour du modèle électrique des transistors 28nm Bulk est réalisée. Ensuite un nouveau modèle électrique est établi pour la technologie 28nm FDSOI.

Chapitre III.
Modélisation électrique de transistors CMOS 28nm sous illumination laser

Préambule

Dans ce chapitre, des injections par face arrière sont réalisées sur des motifs élémentaires (jonctions PN, transistors) afin de mesurer les courants induits par l'illumination. La caractérisation de ces courants permet d'établir les modèles électriques correspondants pour des transistors de technologie 28nm bulk et FDSOI. Une description de la technologie CMOS bulk et FDSOI est donnée dans la première partie. Puis, la mise à jour du modèle électrique du transistor 28nm bulk sous illumination laser est présentée. Finalement, l'établissement du modèle pour le transistor 28nm FDSOI est décrit.

III.1. Description des technologies CMOS bulk et FDSOI 28nm

III.1.1. Structures des transistors bulk et FDSOI

Avec la réduction des nœuds technologiques, la consommation statique est devenue presque aussi importante que la consommation dynamique des circuits [46]. Il est donc devenu important d'adapter la structure des transistors afin de réduire la consommation statique. La figure III-1 présente l'évolution structurelle (vue de principe) d'un transistor MOS. La première structure (figure III-1.a) présente un transistor NMOS et un transistor PMOS en technologie CMOS bulk. Ce type de structure est utilisé pour des nœuds technologiques anciens. Le transistor NMOS est composé d'un substrat P, de deux implants N (source et drain) et une grille séparée par un isolant.

La réduction des nœuds technologiques a conduit à une augmentation de l'intégration dans le silicium. Afin d'éviter toute interaction entre des transistors voisins, des plots isolants (STI) ont été ajoutés au transistor (figure III-1.b). Cette structure permet de supprimer les transistors et/ou jonctions parasites entre les transistors voisins.

Dans le but de réduire l'effet des transistors et des jonctions présentes entre les implants et le substrat, la technologie SOI a été créée (figure III-1.c). En plus des plots isolants, une couche isolante est placée entre le substrat et le canal de conduction du transistor (box) d'environ 145nm. Cette box permet donc de réduire la consommation statique du transistor en supprimant les jonctions et transistors parasites composés du substrat et du canal de conduction. Cette technologie est essentiellement utilisée pour des circuits spécifiques.

Finalement, la technologie Fully Depleted Silicon On Insulator (FDSOI) a été développée afin d'augmenter les performances du transistor (figure III-1.d) et de pouvoir diminuer la taille du nœud technologique. Cette technologie est une variante du SOI où le canal de conduction du transistor entre les deux implants est composé de silicium intrinsèque (non dopé). Le box est plus fin (25nm) ainsi que le canal (6-8nm). Cette réduction des dimensions permet d'avoir un contrôle sur la conduction du canal en agissant sur la tension de polarisation du body et ainsi de pouvoir modifier les caractéristiques dynamiques du transistor.

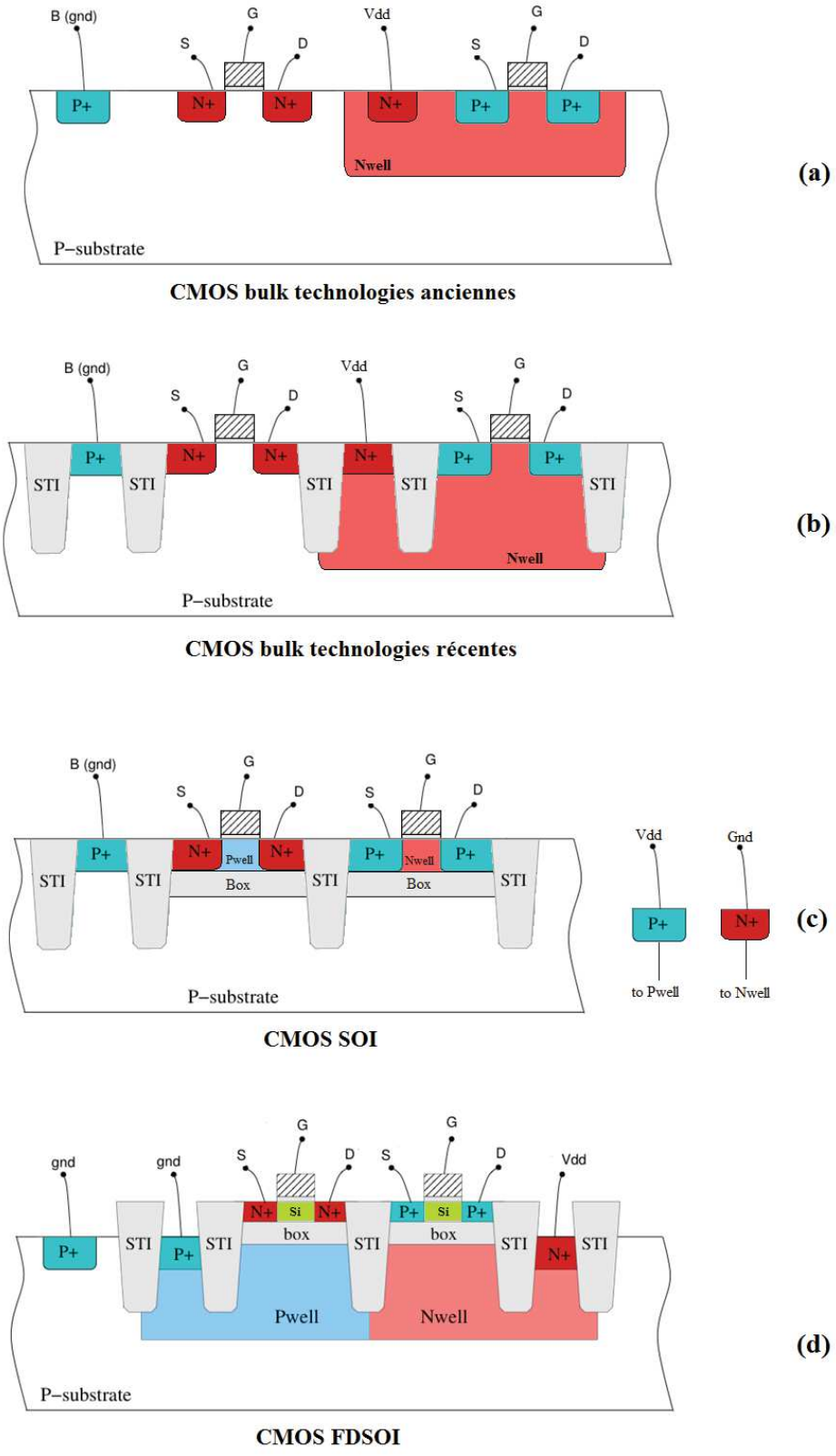


Figure III-1: Vue en coupe des structures des transistors CMOS bulk, SOI et FDSOI (échelle non respectée)

En parallèle de la technologie FDSOI, Intel a développé la technologie FinFET. La figure III-2 présente une vue schématique de cette technologie sur un transistor NMOS ainsi qu'une vue en

coupe du transistor suivant la ligne pointillée. Le canal de conduction dopé P (pour le NMOS) est plus fin que pour la technologie bulk. Cette caractéristique permet de réduire la taille des jonctions PN parasites. La grille des transistors FinFET entoure le canal de conduction afin d'avoir un meilleur contrôle sur la conduction dans le canal. Il existe deux variations de la technologie FinFET, bulk et SOI. Pour la première le canal de conduction fait une partie du substrat (pour le NMOS) alors que pour le FinFET FDSOI, une couche isolante sépare le canal de conduction du substrat. Pour le FinFET bulk, une méthode existe pour limiter les échanges électriques entre le canal et le substrat. Cette méthode consiste à adapter le dopage du substrat afin de rendre plus difficile le passage des porteurs de charges.

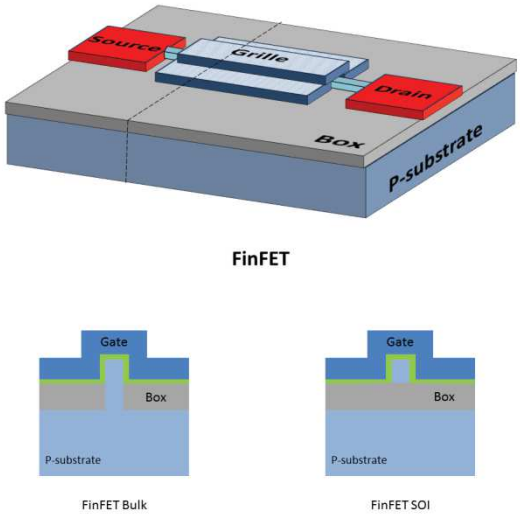


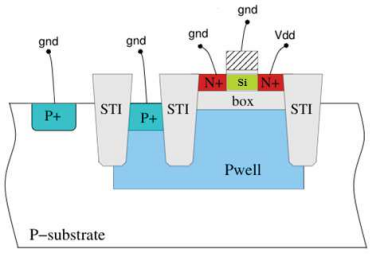
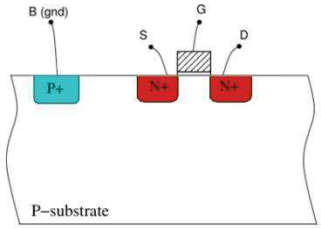
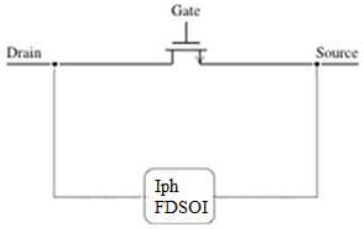
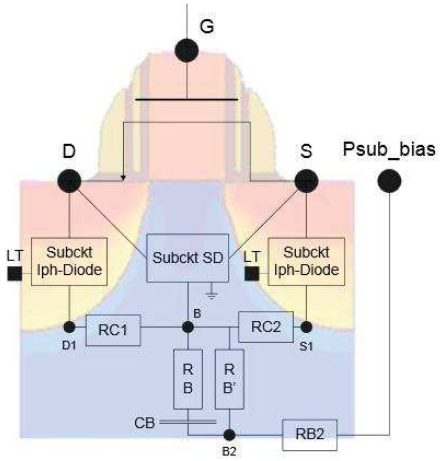
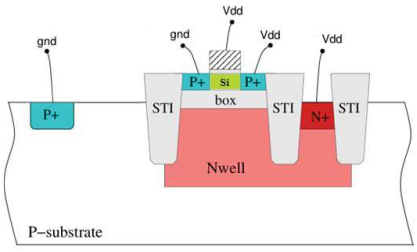
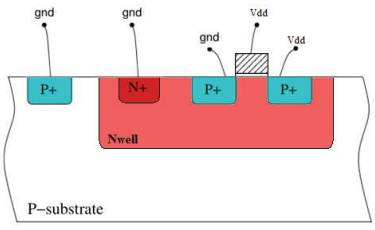
Figure III-2: Vue schématique de la technologie Intel FinFET bulk et FDSOI (échelle non respectée)

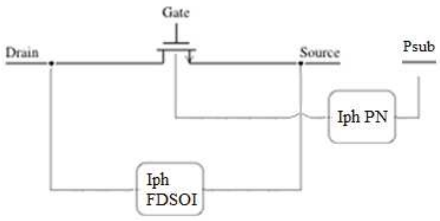
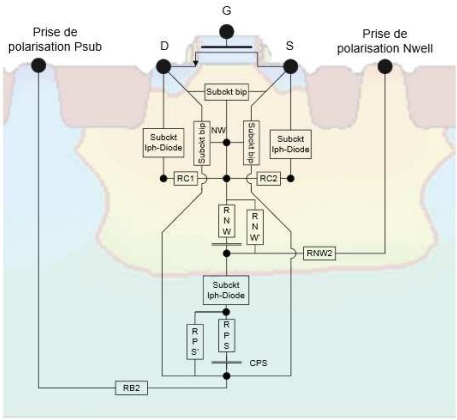
III.1.2. Effets de l'illumination laser des transistors en technologies CMOS bulk et FDSOI

Le photocourant induit par l'illumination laser au niveau des jonctions PN est modélisé par une source de courant comme décrit dans la section I.3.2. Celle-ci débite un courant qui dépend des paramètres expérimentaux d'injections, comme la durée d'illumination par exemple. La génération du courant par illumination laser est plus intense au niveau des jonctions PN polarisées en inverse du transistor. En effet, la zone de charge espace de telles jonctions est grande car élargie par la tension appliquée à la jonction PN. Cette zone de charge espace a pour effet d'accélérer le déplacement des charges et donc augmente l'intensité du courant. Afin de modéliser un transistor NMOS complet sous illumination laser, on utilise le modèle électrique du transistor auquel on ajoute des sources de courant au niveau de ses jonctions PN et transistors bipolaires susceptibles de s'amorcer afin de

modéliser l'effet de l'illumination. La table 8 présente la modélisation électrique des transistors NMOS et PMOS bulk et FDSOI sous illumination laser. Pour les transistors FDSOI, il n'y a aucune jonction PN, ni aucun transistor bipolaire impactant l'intensité du courant induit par l'illumination laser dans le canal du transistor. Cependant, une jonction PN est présente entre le Nwell et le substrat qui compose le transistor PMOS FDSOI. Pour la technologie FDSOI, d'autres jonctions PN sont présentes pour les transistors low Vt. En effet, pour de tels transistors, le caisson est du même type que celui du canal (caisson Nwell pour le NMOS et Pwell pour le PMOS). Ces types de transistors (low Vt) ne seront pas étudiés dans cette thèse.

Table 8: Modèle électrique des transistors CMOS bulk et FDSOI sous illumination laser

		FDSOI	Bulk
NMOS	Structure		
	Modèle		
PMOS	Structure		

	Modèle		

L'isolant qui entoure le canal de conduction des transistors FDSOI permet de réduire le volume de silicium dans lequel sont générés des porteurs par illumination laser. Pour ce type de structure, on peut penser que le courant induit dans les transistors FDSOI est plus faible que celui induit dans des transistors bulk. En effet, pour le transistor CMOS bulk, le substrat (ou le caisson pour le PMOS) représente un réservoir de porteurs de charges important. Il y a alors plus de charges pouvant être collectées dans le canal donc un courant plus élevé (figure III-3). Au contraire, pour le FDSOI le volume de charge et la surface de collection sont plus faibles.

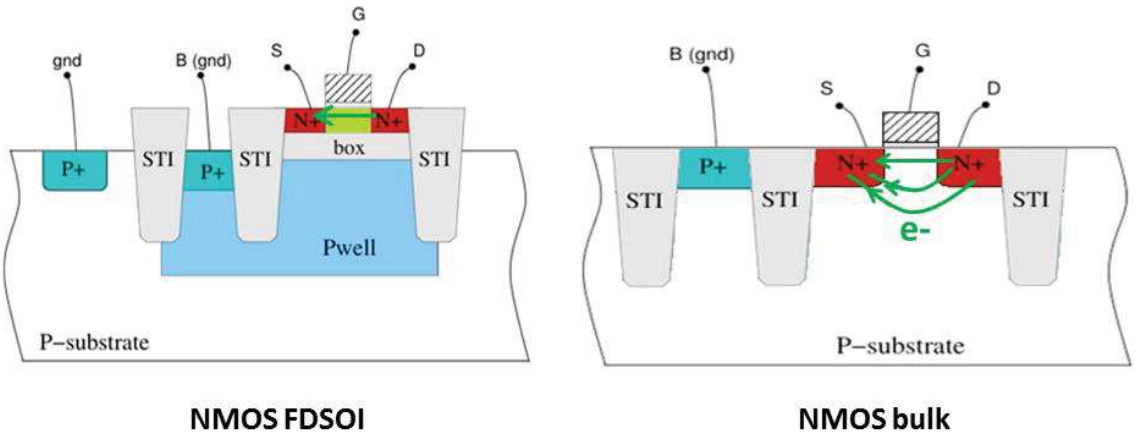


Figure III-3: Schéma de principe des chemins possibles de déplacement des électrons (en vert) dans le canal du transistor

Ainsi à priori, il semble que la technologie FDSOI soit plus résistante que la technologie bulk en termes d'injection de fautes. En effet, la réduction du volume de canal par le box et les STI, réduit le nombre de charges collectées par le transistor lors d'une illumination, diminuant alors le courant induit.

III.2. Mise à jour du modèle pour le transistor 28nm bulk

Dans cette section, on effectue une mise à jour du modèle électrique des transistors CMOS bulk sous illumination, afin de tenir compte de la modification apportée par le changement de nœud technologique (passage de 90nm à 28nm).

II.2.1. Présentation du circuit expérimental

La détermination des caractéristiques de la source de courant permettant de modéliser l'injection laser a été réalisée sur un circuit dédié où plusieurs motifs élémentaires (jonctions PN, transistors, etc.) ont été implantés. La figure III-4 présente une vue large plane des plots entre lesquels sont placés les motifs. Les plots permettent l'accès aux entrées du motif (drain, source, grille, etc.). Chacun de ces motifs élémentaires est implanté de manière à être séparé des autres motifs. Cette dissociation des motifs permet d'éviter l'illumination de plusieurs motifs simultanément.

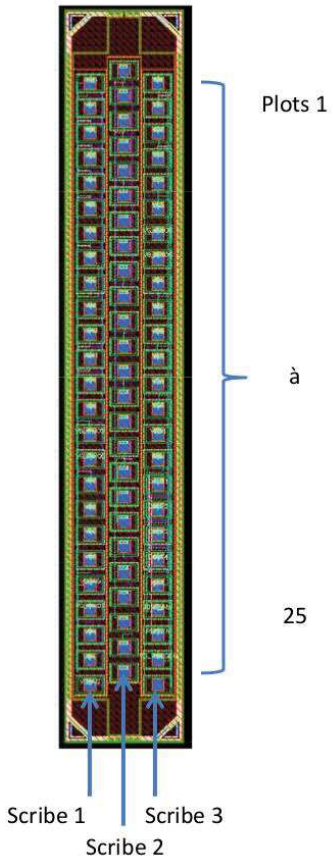


Figure III-4: Positionnement des motifs élémentaires

Ces motifs sont implantés dans un circuit ouvert par la face arrière. Cette ouverture permet d'effectuer des injections par la face arrière. Les signaux de contrôle des motifs (polarisation, etc..)

sont accessibles par des billes de contacts situées sur la face supérieure du circuit. On utilise des pointes posées sur des micromanipulateurs afin de polariser le motif, par contact, sur les billes correspondantes. La figure III-5 présente une vue de la face avant et arrière du circuit expérimental. Chacune des billes permet à l'aide d'une source de tensions externe de polariser le motif à tester. Afin de protéger les transistors des décharges électrostatiques (ESD) qui pourraient provoquer une casse de celui-ci (lors de la pose des pointes de mesures), des diodes de protections ont été ajoutées lors dans le layout du circuit. La zone plus claire sur l'image de la face arrière, correspond à la partie amincie du circuit, par laquelle seront effectuées les injections laser.

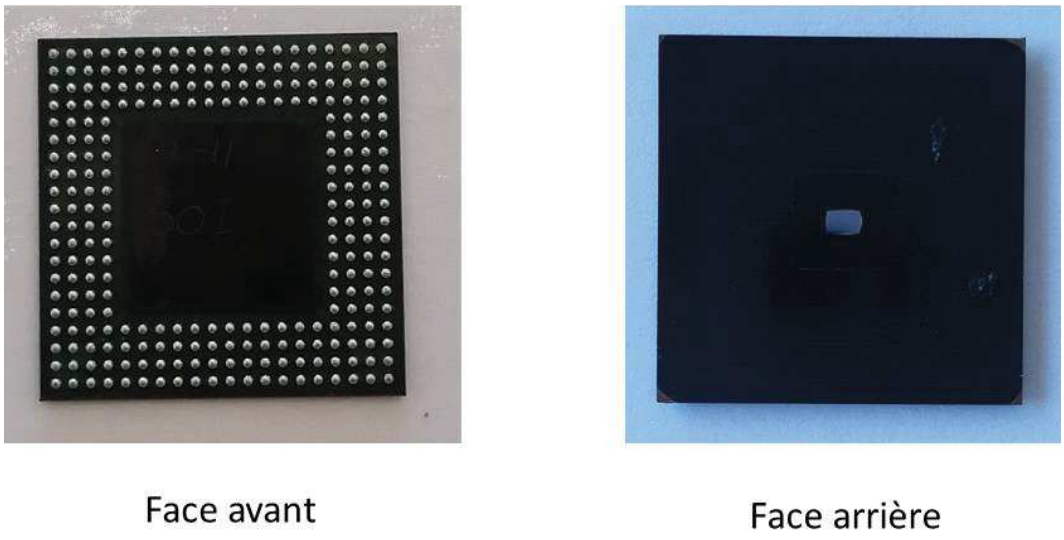


Figure III-5: Image du circuit expérimental : face avant (à gauche) et face arrière (à droite)

L'injection laser est effectuée avec une source laser de type infra-rouge (λ=1064nm) avec un faisceau de largeur 1µm au point de focalisation. Une caméra infrarouge additionnelle est utilisée afin de placer le faisceau laser sur le motif à tester. La figure III-6 présente une image obtenue par la caméra infra-rouge (à gauche) ainsi qu'un agrandissement de celle-ci (à droite). La bordure du circuit (en vert) représente la délimitation du circuit présenté sur la figure III-4 Les plots de connections (en bleu) et les lignes de métaux sont visibles et permettent de déterminer la zone d'implantation du motif (en rouge).

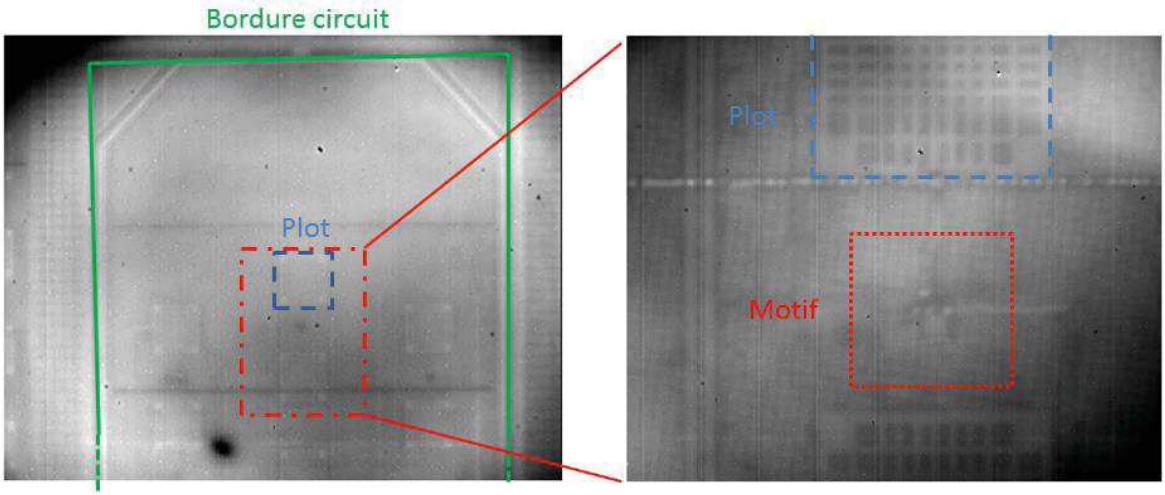


Figure III-6: Image infra-rouge d'une partie du circuit expérimental (grossissement x20 à gauche et x100 à droite)

II.2.2. Mise à jour du modèle

Le modèle électrique utilisé ici, pour la technologie 28nm, est le même que celui utilisé dans [31], pour la technologie 90nm. On modélise l'effet de l'illumination laser sur une jonction PN (type N+/Psub) puis on intègre ce modèle dans le transistor complet pour modéliser le courant induit dans celui-ci. La modélisation de la jonction PN (Nwell/Psub) est détaillée en Annexe. Pour des raisons de confidentialité, certaines valeurs de courant sont données en unité arbitraire.

a) Dispositif de mesure expérimentale

On détermine l'intensité du courant induit dans une jonction PN de type N+/Psub en mesurant la tension aux bornes d'une résistance connectée à celle-ci. La figure III-7 présente un schéma de principe du montage de mesure.

Les injections laser sont réalisées sur une jonction PN N+/Psub de 1,45µm*1,45µm. La figure III-7 présente le layout de cette photodiode ainsi qu'une vue de principe.

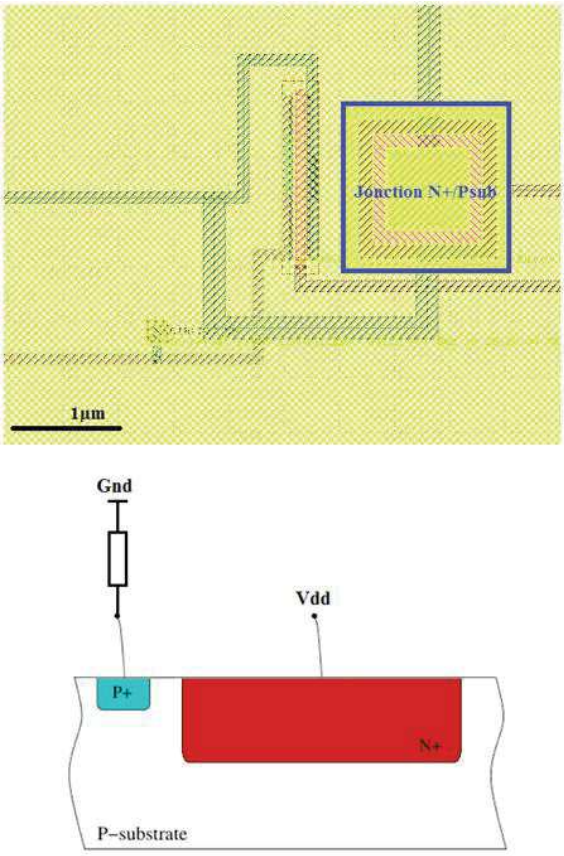


Figure III-III-7: Layout et schéma de principe de la photodiode N+/Psub

L'illumination est réalisée avec une source de diamètre 1µm, pour une durée d'illumination de 50µs et une tension de polarisation en inverse de la photodiode de 1V (sauf indication contraire).

Dans la suite, on fait varier les différents paramètres d'injections afin de mesurer leurs impacts sur l'intensité du photocourant.

Le modèle de l'amplitude maximale de la source de courant est donné par l'équation 27 :

$$I_{ph} = (a * V_{PN}) * \alpha_{gauss} * Pulse_{width} * W_{coeff} * I_{ph_z} * S \qquad (27)$$

On considère que l'effet de chacun des paramètres testés est indépendant de celui des autres paramètres.

Tous les paramètres suivants impactent l'amplitude du courant induit :

- La puissance de tir du laser (a,b)
- La polarisation en inverse des jonctions PN touchées : V_{PN}
- La dépendance spatiale (x,y) : α_{gauss}
- La durée d'illumination : $Pulse_{width}$

- L'épaisseur du wafer : W_{coeff}
- La focalisation (z) : I_{ph_z}
- La surface de la jonction en µm²: S

L'effet de l'épaisseur du wafer (Wcoeff) n'a pas été mesuré ici. On réutilise le modèle établi pour la technologie 90nm pour ce paramètre. Le circuit utilisé dans la suite est aminci, l'épaisseur du substrat et de 100µm. La figure III-8 présente un schéma de la variation de tous les paramètres mesurés.

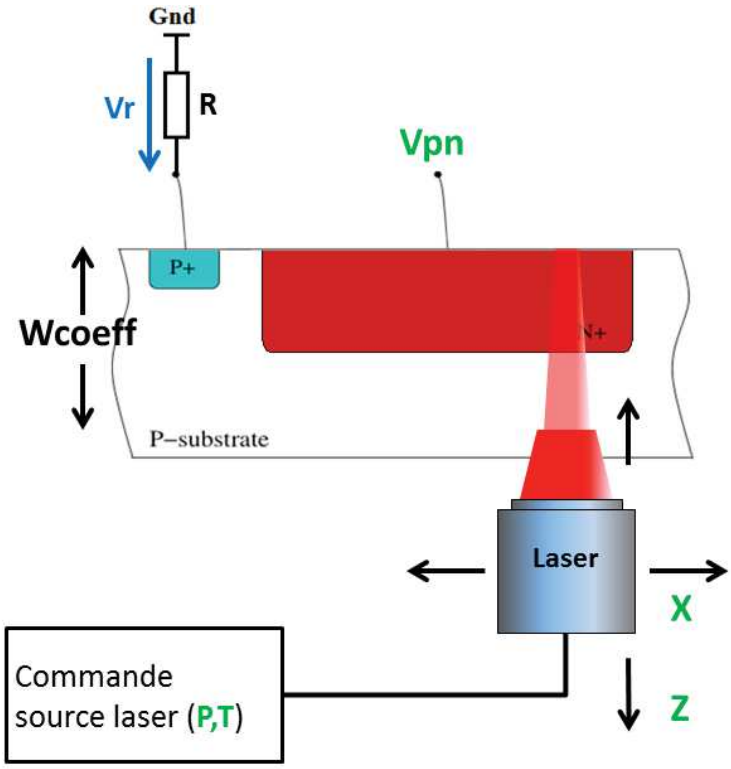


Figure III-8: Schéma des différents paramètres mesurés (en vert)

Le coefficient de détermination (R^2) est utilisé dans la suite, afin de quantifier la qualité du modèle comparée aux valeurs expérimentales. L'équation 28 donne l'expression de ce coefficient.

$$R^2 = \frac{\sum_{i=1}^{n}(\hat{y}_i - \bar{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y}_i)^2} \qquad (28)$$

Avec $\hat{y}_i$ représentant la valeur prédite, $\bar{y}_i$ la moyenne et y_i la valeur mesurée. Ce coefficient varie de 0 à 1. Lorsqu'il se rapproche de 1 alors le modèle prédit de manière efficace, au contraire lorsque ce coefficient tend vers 0 alors le modèle n'est pas adapté.

b) Dépendance de la puissance d'injection et de polarisation de la jonction en inverse

Des expérimentations sur une jonction PN (type N+/Psub) ont été effectuées afin de mesurer l'impact de la puissance du tir ainsi que la polarisation en inverse de la jonction sur l'amplitude du photocourant induit. La figure III-9 présente le résultat de cette expérience. Pour une puissance fixée, l'effet de la tension de polarisation en inverse de la jonction, a un effet linéaire sur le photocourant induit dans celle-ci. A tension fixe, la variation de l'amplitude du photocourant présente un terme quadratique en fonction de la puissance.

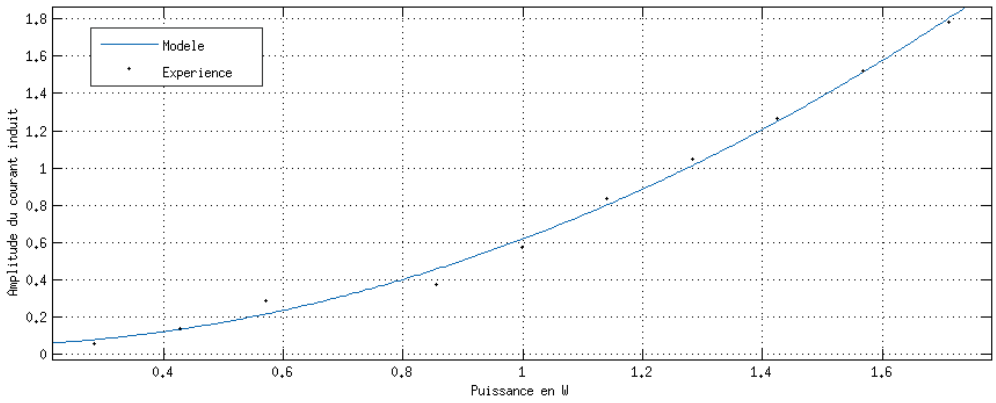


Figure III-9: Photocourant induit (unité arbitraire) dans une jonction PN (1,45µm*1,45µm) en fonction de la tension de polarisation en inverse pour plusieurs puissances d'injections : mesuré (points) et modèle (courbes)

L'équation 29 donne un modèle du résultat obtenu par expérimentation.

$$I(P,V) = [(a_0 * P^2 + a_1 * P + a_2) * V + b_0 * P + b_1] * S \qquad (29)$$

La table 9 donne la valeur des coefficients pour la jonction PN (1,45µm*1,45µm) :

Table 9: Coefficients du modèle pour la prise en compte l'effet de la puissance et de la tension de polarisation en inverse de la jonction PN

$\boldsymbol{a_0}$	7,543	$W^{-2}V^{-1}\mu m^{-2}$
$\boldsymbol{a_1}$	83,81	$W^{-1}V^{-1}\mu m^{-2}$
$\boldsymbol{a_2}$	-10,91	$V^{-1}\mu m^{-2}$
$\boldsymbol{b_0}$	20,23	$W^{-1}\mu m^{-2}$
$\boldsymbol{b_1}$	-4,608	μm^{-2}

Avec un tel modèle on a un coefficient de détermination R^2=99%.

c) Effet de la distance du faisceau laser à la jonction PN(N+/Psub)

Afin de mesurer l'effet de la distance du faisceau laser à la jonction PN, on réalise une campagne d'injection laser. Dans cette campagne, on mesure l'amplitude du photocourant pour plusieurs positions du faisceau laser. La figure III-10 montre les mesures effectuées (points) ainsi que le modèle établi à partir de ces résultats (courbe). La valeur de l'amplitude du photocourant mesurée est normalisée afin de connaître l'effet de ce paramètre sur l'amplitude maximale du courant induit. On remarque que plus on s'éloigne de la jonction, plus le photocourant induit dans la jonction diminue. Cette variation d'amplitude est gaussienne et centrée en x=0 c'est-à-dire le centre de la jonction. Cette variation s'explique par le fait que plus le faisceau s'éloigne de la jonction, plus les porteurs de charges sont générés loin de la jonction. Il devient donc plus difficile pour celle-ci de capter ces porteurs avant leur recombinaison dans le silicium. Le profil gaussien de ce phénomène est un effet direct de la distribution de l'énergie dans le faisceau laser qui elle aussi a un profil gaussien.

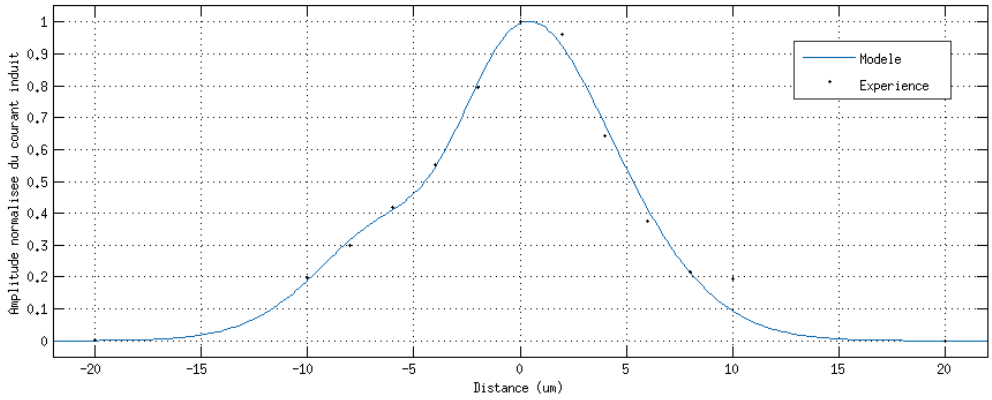


Figure III-III-10: Effet de la distance sur l'amplitude du photocourant collecté par la jonction N+/Psub

A partir des mesures effectuées, on obtient la modélisation (30) suivante :

$$\alpha_{gauss} = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{x - b_i}{c_i}\right)^2\right) \qquad (30)$$

Les valeurs des coefficients de ce modèle sont données dans la table 10 :

Table 10: Coefficients modélisant l'effet de la distance à la jonction sur le courant induit dans la jonction PN

a_0	-0,3847	a_1	1,129
b_0	-3,766 µm	b_1	-0,928 µm
c_0	3,402 µm	c_1	6,93 µm

Pour ce modèle, on a un coefficient de détermination de R^2=98,9%.

d) *Effet de la durée d'illumination sur l'amplitude maximale du photocourant induit*

On souhaite maintenant modéliser l'effet de la durée d'illumination sur le photocourant induit par l'illumination. Une campagne laser est réalisée, celle-ci consiste en des tirs lasers de durées différentes visant le centre de la jonction PN. La figure III-11 présente les résultats de cette campagne ainsi que la modélisation de ce phénomène. On observe, d'une part, que plus le temps de d'illumination de la jonction PN est long, plus l'amplitude du photocourant induit est grande. D'autre part, pour des durées d'illuminations longues, un maximum d'amplitude est atteint. Ce phénomène s'explique par le fait qu'à partir d'un certain temps, le mécanisme de génération de charge est aussi rapide que le mécanisme de collection des charges par la jonction. On atteint alors un régime stationnaire. Pour ce type de motif, on atteint le seuil maximum d'amplitude à partir d'une illumination de 2 µs environ.

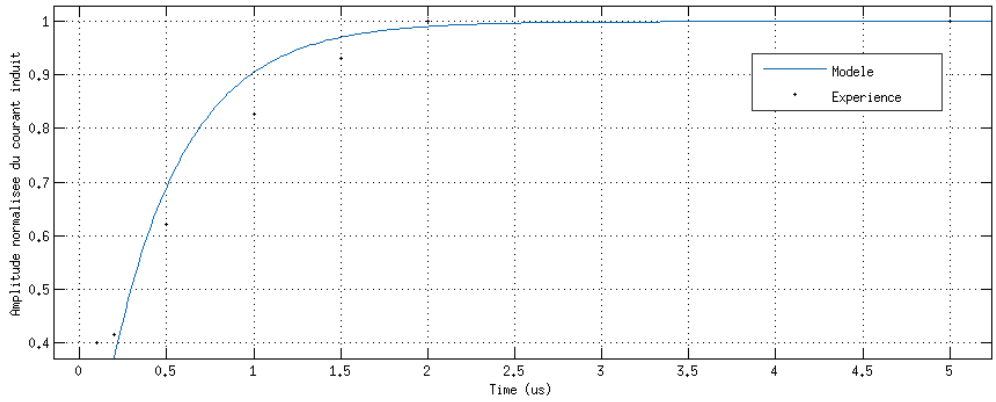


Figure III-III-11: Effet de la durée d'illumination sur l'amplitude maximale du courant collecté

De l'expérimentation, on obtient l'équation (31) permettant de modéliser l'effet de la durée d'illumination sur le photocourant induit.

$$Pulse_{width} = 1 - exp\left(\frac{-D}{a}\right) \qquad (31)$$

où D est le temps d'illumination en µs et a=0,4252 µs. Pour ce modèle on a un coefficient de détermination R^2=87,8%.

e) *Effet de la focalisation du faisceau sur le photocourant induit*

On s'intéresse ici à l'effet de la focalisation du faisceau laser et de son influence sur l'amplitude du photocourant induit. Une campagne d'illumination est donc réalisée. Pour cette campagne plusieurs illuminations sont effectuées visant le centre de la jonction PN (N+/Psub), avec une durée d'illumination fixe, mais en modifiant la distance de la source à la jonction. La figure III-12 donne les résultats de cette campagne ainsi que la modélisation de ce phénomène. On observe que la variation de l'amplitude du courant induit est symétrique par rapport au point focal (z=0). Ceci s'explique par le fait que si on modifie la distance de la source à partir du plan focal dans un sens ou dans l'autre (ici vers le haut ou vers le bas), la taille du faisceau s'étend de la même manière. La surface éclairée augmente avec le déplacement de la source, à partir du plan focal, mais l'énergie du faisceau reste la même. Ainsi lorsque le faisceau est défocalisé, on éclaire une plus grande zone mais avec une énergie surfacique plus faible. Lorsque le faisceau est plus large que la jonction, moins d'énergie est donc injectée au niveau de la jonction, on a alors une baisse de l'amplitude du courant induit par l'illumination.

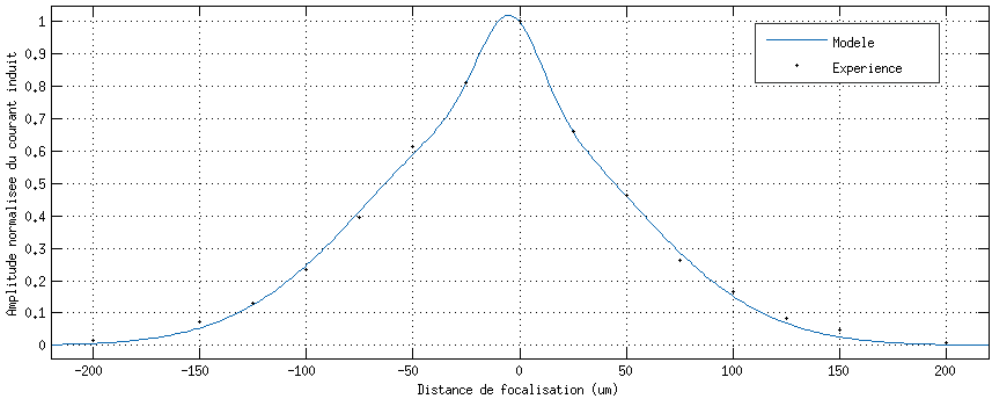


Figure III-12: Effet de la distance focale du laser sur l'amplitude maximale du courant collecté par la jonction PN de type N+/Psub

L'expression du modèle obtenu est donnée par l'équation 32 suivante :

$$I_{phz} = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{z - b_i}{c_i}\right)^2\right) \qquad (32)$$

Où z est la distance de la source par rapport au plan focal et la table 11 donne les coefficients du modèle.

Table 11: Coefficients du modèle de l'effet de la focalisation sur l'amplitude du courant induit

a_0	0,7259	a_1	1,129
b_0	-3,766 µm	b_1	-0,928 µm
c_0	3,402 µm	c_1	6,93 µm

Avec ces coefficients, on obtient un coefficient de détermination R^2=97,5%.

Ainsi la mise à jour du modèle électrique de la jonction PN (type N+/Psub) sous illumination laser présenté dans cette section 0, le modèle électrique pour la jonction PN (type Nwell/Psub) et celui du transistor bipolaire de type NPN développé en annexe, permettent de réutiliser la structure en bloc créer pour la technologie 90nm présenté dans la section I. Cette structure permet avec les nouveaux paramètres établis de modéliser électriquement l'effet d'une injection laser sur des transistors de la technologie CMOS 28nm bulk.

III.3. Modèle électrique d'injection pour la technologie FDSOI

Dans cette section, on s'intéresse à l'établissement d'un nouveau modèle électrique afin de modéliser l'effet de l'illumination laser sur des transistors implantés en technologie 28nm FDSOI.

III.3.1. Etablissement du modèle électrique pour le transistor NMOS FDSOI

On s'intéresse ici à la modélisation du transistor FDSOI. La structure du modèle utilisé pour la technologie CMOS bulk n'est pas applicable dans le cas de la technologie CMOS FDSOI. En effet, la présence du box empêchant le transfert de charges entre le substrat (ou Nwell dans le cas d'un PMOS) et le canal, alors la structure du modèle électrique est différente. De plus, comme le canal est composé de silicium intrinsèque entre deux implants N+ (respectivement P+ pour le PMOS) modifie l'intensité du courant induit dans le canal (figure III-13). Ainsi afin de modéliser électriquement cette technologie, on mesure directement le courant induit dans le canal de la structure complète.

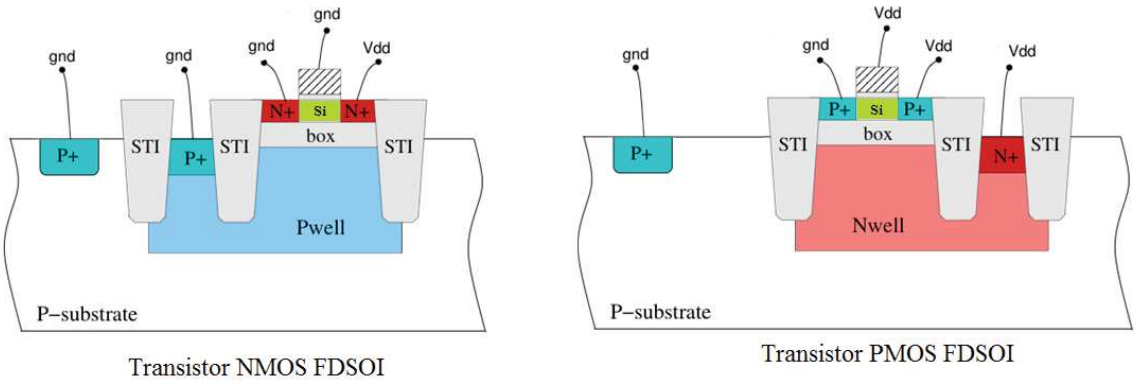


Figure III-13: Structure d'un transistor NMOS et PMOS FDSOI

Il faut donc, pour modéliser le courant induit dans le canal, mesurer directement le courant induit sur le transistor sous illumination. Nous mesurons l'effet des paramètres suivants sur le photocourant induit dans le canal :

- La puissance de tir du laser
- La dépendance spatiale (x,y)
- La durée d'illumination
- La focalisation (z)
- La surface du canal de conduction

Le transistor NMOS utilisé pour ces expérimentations est un transistor NMOS FDSOI (W,L) 1µm*500nm. La figure III-14 présente le layout du transistor NMOS. Pour ce transistor, des diodes de protection (jonctions PN contre l'ESD) sont placées au voisinage des transistors. Ces diodes sont reliées à la ligne de métal qui alimente chaque entrée du transistor (source, drain, grille). La présence de ces diodes altère la mesure du photocourant induit dans le transistor. Dans la section I.2, nous avons vu que l'illumination d'une jonction PN crée un photocourant. Or le photocourant généré dans ces diodes va modifier l'amplitude du photocourant généré dans le transistor. Ce phénomène est d'autant plus problématique que les diodes sont situées au voisinage du transistor. On considère que lorsque le faisceau laser cible le transistor, le courant mesuré dans le canal provient essentiellement des charges générées dans le canal. Lorsqu'on éloigne le faisceau du transistor, l'amplitude du courant généré par les diodes devient prédominant devant le courant généré par les porteurs de charges générés dans le canal du transistor.

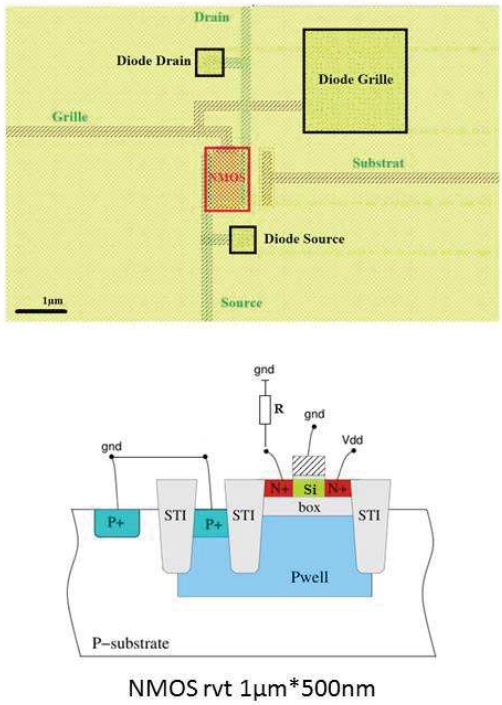


Figure III-14: Layout et schéma de principe du transistor NMOS 28nm FDSOI

Pour les mesures suivantes, on place la résistance de mesure sur la source du transistor. Pour cette entrée du transistor, la diode de protection est se situe entre deux potentiels Gnd. De cette manière, on réduit l'impact de la diode sur la mesure du courant collecté.

a) Effet de la puissance de tir sur le photocourant induit dans le canal du transistor

On s'intéresse ici à l'effet de la puissance du faisceau laser sur le photocourant induit dans le canal de conduction du transistor. Afin de mesurer cet effet, on place la source laser à l'aplomb du transistor NMOS (ici 1µm*3µm), au-dessus de la grille de celui-ci, puis on réalise plusieurs injections en modifiant la puissance de tir. La figure III-15 donne les résultats expérimentaux ainsi que le modèle choisi pour modéliser cet effet. On observe que, comme pour le modèle bulk, le modèle comporte un terme quadratique.

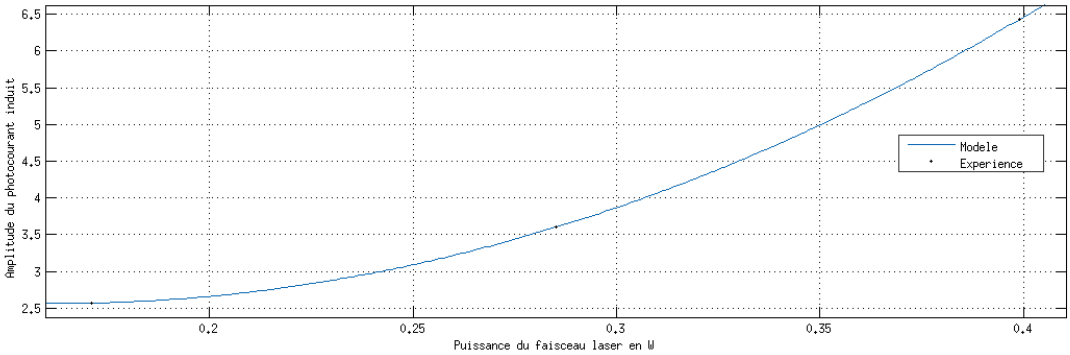


Figure III-15: Mesures et modélisation de l'effet de la puissance sur l'amplitude du photocourant induit dans le canal de conduction d'un transistor NMOS

Le modèle donné par l'équation (33) permet de modéliser l'effet de la puissance d'injection.

$$I_{ph} = (a * P^2 + b * P + c) * S \qquad (33)$$

Les coefficients de modélisation pour le transistor NMOS sont donnés par la table 12. Les paramètres P et S représentent respectivement la puissance en Watt du faisceau et la surface du transistor en µm².

Table 12: Coefficients de modélisation de l'effet de la puissance sur l'amplitude du photocourant induit dans le canal de conduction d'un transistor NMOS

Coefficient	Valeur	Unité
a	$82{,}3 * 10^{-9}$	$A.W^{-2}.\mu m^{-2}$
b	$-15{,}67 * 10^{-9}$	$A.W^{-1}.\mu m^{-2}$
c	$2{,}95 * 10^{-9}$	$A.\mu m^{-2}$

Pour ce modèle, on a un coefficient de détermination R^2=99,9%.

b) Influence de la distance du faisceau au transistor sur le courant induit

On réalise une campagne d'injection laser sur un transistor NMOS afin de modéliser l'influence de la distance sur le courant induit dans le canal par le tir laser. On déplace donc horizontalement la source laser entre chaque injection afin de balayer le transistor et son environnement. La figure III-16 représente le résultat de l'expérimentation ainsi que la courbe modélisant le phénomène pour une largeur de transistor de 500nm. On remarque que, comme pour l'injection sur la jonction PN, La représentation de ce phénomène a un profil gaussien. Ce profil est l'effet de la distribution énergétique du faisceau laser qui, elle aussi, a un profil gaussien. Plus la zone d'injection est éloignée du centre du transistor (x=0µm), plus le courant induit dans le canal est faible. La largeur à mi-hauteur pour cette expérimentation est de l'ordre de 3µm. C'est-à-dire que lorsque le spot laser

(diamètre 1µm) est placé à 3µm du centre du transistor alors l'amplitude du photocourant induit dans le canal a diminué de moitié. Pour rappel, pour la jonction PN de type N+/Psub modélisée précédemment, la largeur à mi-hauteur est de 10 µm. Cette différence s'explique par l'effet d'isolation du canal par la box.

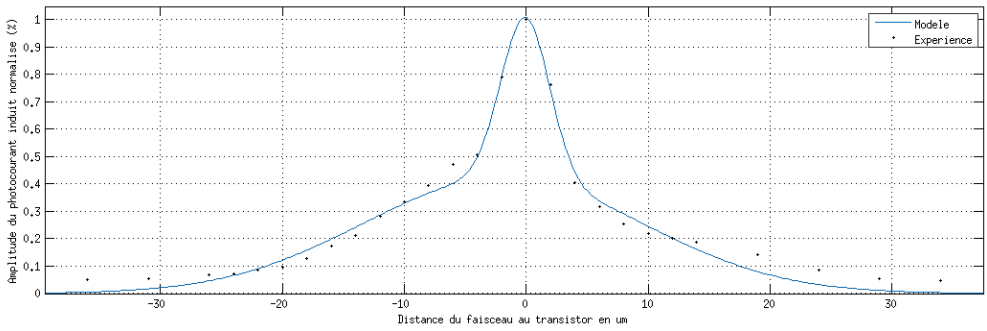


Figure III-16: Mesures (points) et modélisation (courbe) de l'effet de la distance du faisceau au transistor sur le courant induit dans le canal (largeur transistor 500nm)

De cette expérience nous avons pu établir la modélisation donnée par l'équation (34):

$$I_x = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{x-b_i}{c_i}\right)^2\right) \qquad (34)$$

Où x est la distance du faisceau au transistor avec x=0µm la position du centre du transistor et a, b et c les constantes données par la table 13 suivantes :

Table 13: Coefficients de modélisation de l'effet de la distance horizontale sur l'amplitude maximale normalisée du photocourant induit dans un transistor FDSOI

a_0	0,5916	a_1	0,4216
b_0	-0,0743 µm	b_1	-1,917 µm
c_0	2,822 µm	c_1	16,2 µm

Avec ce modèle on a un coefficient de détermination égal à R^2=98,3%.

c) Effet de la durée d'illumination sur le courant induit dans le transistor

On souhaite maintenant modéliser l'effet de la durée d'illumination du transistor sur le photocourant induit dans le canal du transistor. On illumine avec des durées différentes le transistor en son centre. On modélise ensuite cette influence à partir des données mesurées (figure III-17). On remarque que plus le temps d'illumination est long plus l'amplitude du photocourant induit augmente jusqu'à atteindre un seuil. Ce seuil maximum d'amplitude est atteint pour une durée

d'illumination d'environ 20µs. A partir de cette durée, le mécanisme de génération de porteurs de charges et celui de collection du transistor ont la même vitesse, on a atteint un régime stationnaire.

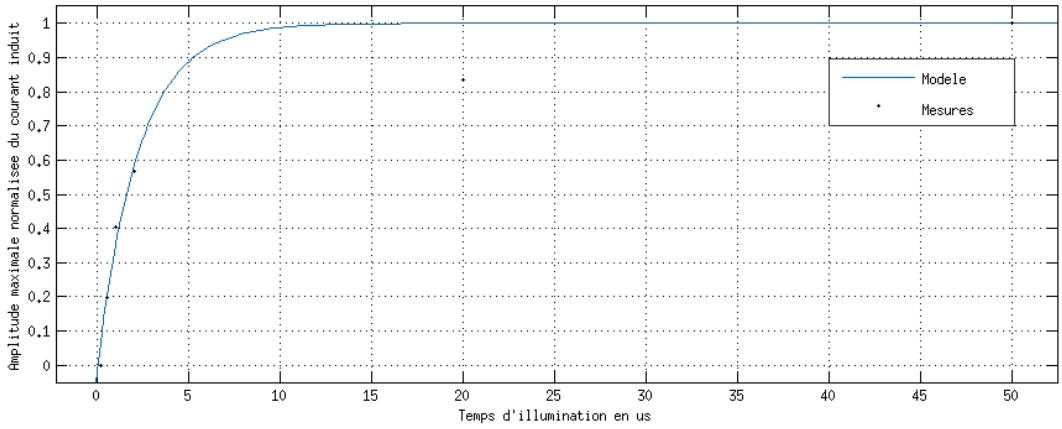


Figure III-17: Influence de la durée d'illumination sur le courant induit dans le canal du transistor

Pour ce phénomène, le modèle présenté dans l'équation (35) a été établi à partir de l'expérimentation.

$$I_D = 1 - exp\left(\frac{-D}{a}\right) \qquad (35)$$

Où D est la durée d'illumination du transistor en µs et a=2,272µs. Pour ce modèle on a un coefficient de détermination R^2=94,8%.

d) Effet de la focalisation du faisceau laser sur l'amplitude maximale du photocourant induit

On place le faisceau laser à l'aplomb du centre du transistor, puis on tir en modifiant la distance verticale de la source par rapport à la distance focale. Cette campagne de tir a pour but de modéliser l'effet de la focalisation du faisceau sur l'amplitude maximale du courant induit dans le canal du transistor NMOS. La figure III-18 présente les résultats de cette campagne ainsi que la modélisation établie pour ce paramètre. La forme de la courbe décrivant l'influence de la focalisation est une gaussienne centrée en z=0µm (plan focal). Si le faisceau s'éloigne de cette position (z=0µm) alors l'amplitude maximale du photocourant diminue. Cette diminution est symétrique si on augmente ou diminue la valeur de z par rapport à la position focale. Ce caractère symétrique provient de la forme du faisceau laser (divergent). En effet la taille de la zone éclairée par le laser évolue de la même manière lorsque l'on défocalise le faisceau.

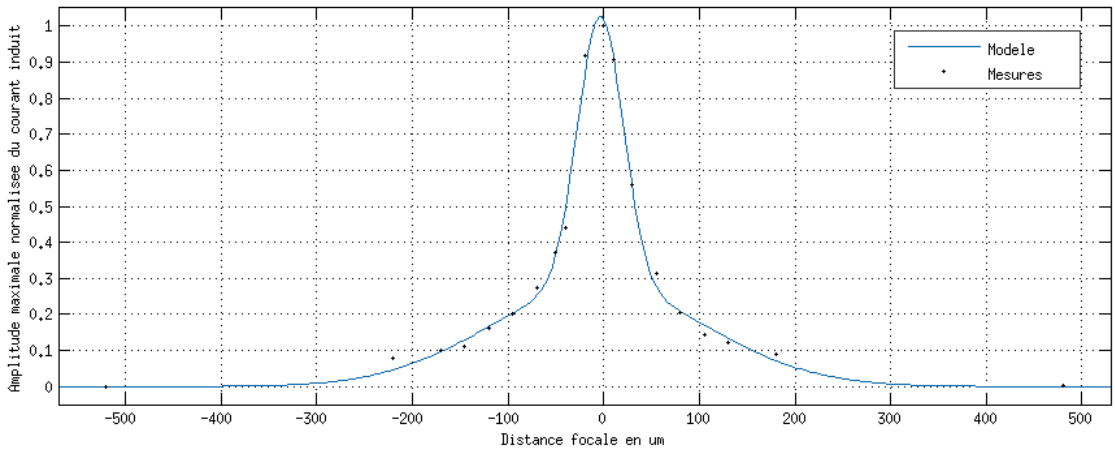


Figure III-18: Effet de la focalisation sur l'amplitude maximale du photocourant induit dans le canal du transistor

L'équation (36) présente la modélisation de l'influence de ce paramètre.

$$I_z = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{z-b_i}{c_i}\right)^2\right) \qquad (36)$$

Où Z est la distance de la source par rapport au plan focal et avec a, b et c les constantes données par la table 14 :

Table 14: Coefficients de modélisation de l'effet de la distance verticale au transistor sur l'amplitude maximale normalisée du photocourant induit dans le canal

a_0	0,7526	a_1	0,2765
b_0	-3,313 µm	b_1	-5,955 µm
c_0	33,83 µm	c_1	160 µm

Pour cette modélisation, on a un coefficient de détermination R^2=99,4%.

III.3.2. Modélisation du transistor PMOS 28nm FDSOI

Dans cette section, on modélise les effets des paramètres expérimentaux sur le courant induit dans le canal d'un transistor PMOS. La figure III-19 présente une vue schématique du transistor PMOS ainsi que le layout de celui-ci. Le transistor sous illumination à une surface de 3µm*1µm (W>>L). Comme pour le transistor NMOS, le transistor utilisé pour l'expérimentation possède des diodes de protection à son voisinage.

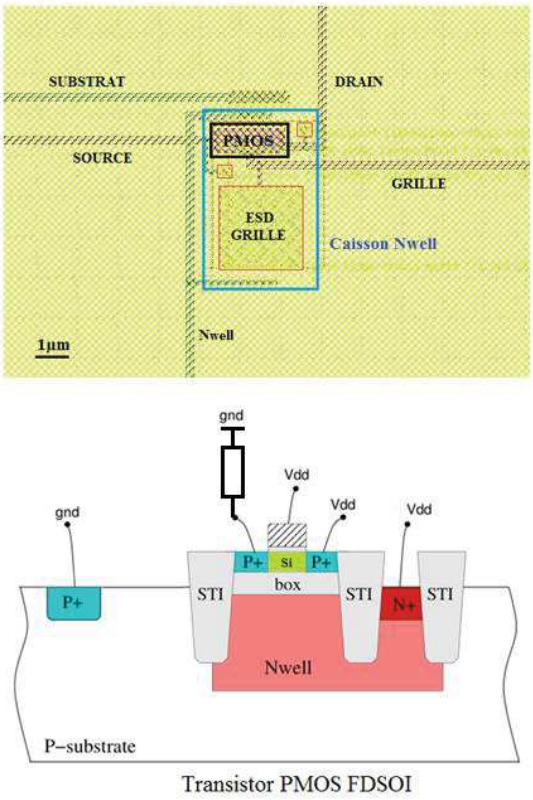


Figure III-19: Vue schématique et layout du transistor PMOS FDSOI

Pour les mêmes raisons que pour le transistor NMOS FDSOI, la résistance de mesure est placée sur le drain du transistor PMOS. En effet, de cette manière on limite l'impact de la diode de protection sur la mesure du courant.

a) Effet de la puissance de tir sur l'amplitude maximale du photocourant induit

On s'intéresse ici, à l'effet de la puissance d'injection sur l'amplitude maximale du photocourant induit. Pour cela, on réalise une injection, avec une source laser à l'aplomb du transistor PMOS, pour différentes puissances d'injection. La figure III-20 présente les résultats expérimentaux ainsi que le modèle utilisé pour modéliser cet effet.

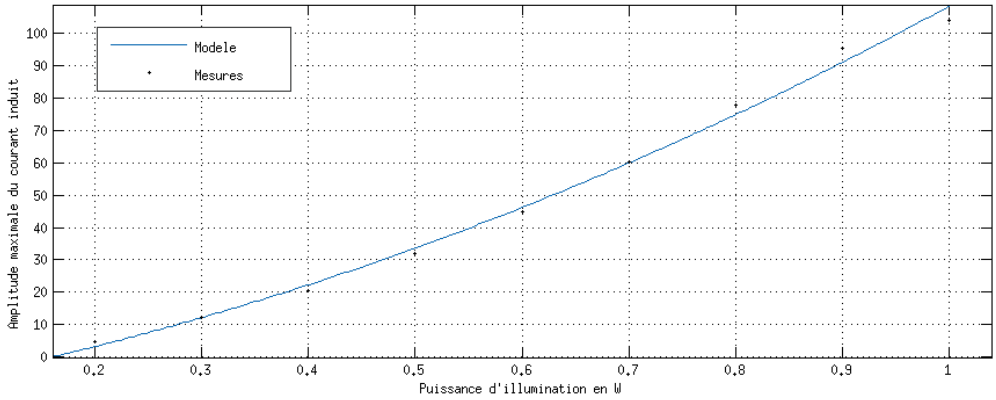


Figure III-20: Effet de la puissance sur l'amplitude maximale du courant induit dans le canal de conduction d'un transistor PMOS FDSOI (3µm*1µm)

L'équation (37) présente l'expression mathématique de la modélisation de l'effet de la puissance sur l'amplitude du courant induit dans le canal.

$$I_{ph} = (a * P^2 + b * P + c) * S \qquad (37)$$

Les coefficients de modélisation sont donnés par la table 15 :

Table 15: Coefficients de modélisation de l'effet de la puissance sur l'amplitude du courant induit dans le canal d'un transistor PMOS FDSOI

Coefficient	Valeur	Unité
a	12,6	$W^{-2}\mu m^{-2}$
b	1,246	$W^{-1}\mu m^{-2}$
c	−2,32	μm^{-2}

Pour ce modèle, on a un coefficient de détermination de R^2=99 ,4%

b) Effet de la distance du faisceau au transistor PMOS sur l'amplitude du courant induit dans le canal de conduction

On modélise ici l'effet de la distance du faisceau laser au transistor PMOS. La figure III-21 représente les résultats de l'expérimentation et la modélisation de cet effet, pour un transistor de largeur 3µm. Le modèle est symétrique par rapport à l'aplomb du transistor (x=0µm). La fonction utilisée pour le modèle est une double gaussienne. On remarque que, comme pour le transistor NMOS, lorsque le faisceau laser est écarté de 3µm du centre du transistor, alors l'amplitude maximale du courant induit dans le canal diminue de 50% de sa valeur maximale.

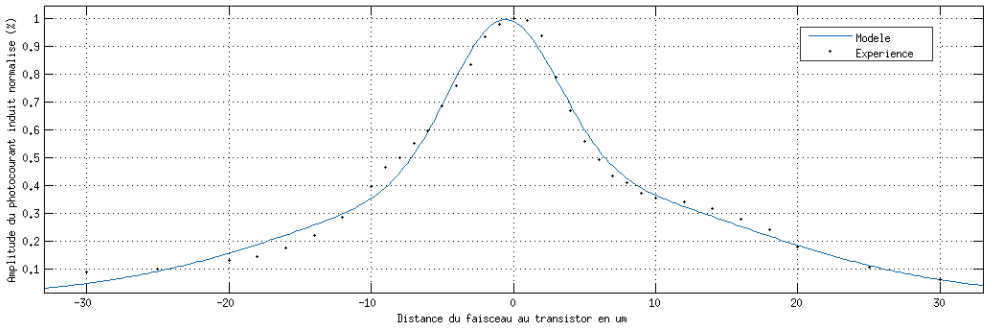


Figure III-21: Effet de la distance sur l'amplitude maximale normalisée du courant induit dans le transistor PMOS FDSOI (largeur transistor 3µm)

L'équation (38) donne l'expression du modèle utilisé.

$$I_x = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{x - b_i}{c_i}\right)^2\right) \qquad (38)$$

La table 16 donne les valeurs des coefficients de modélisation.

Table 16: Coefficients de modélisation de l'effet de la distance horizontale sur le photocourant induit dans le canal du transistor PMOS FDSOI

a_0	0,5711	a_1	0,4273
b_0	-0,6389 µm	b_1	0,8916 µm
c_0	5,393 µm	c_1	20,77 µm

Pour cette modélisation, on a un coefficient de détermination de R^2=98,7%.

c) Effet de la durée d'illumination sur l'amplitude maximale du courant induit dans le canal de conduction du transistor PMOS FDSOI

On modélise ici, l'effet de la durée d'illumination sur l'amplitude du photocourant induit dans le canal du transistor PMOS FDSOI. La figure III-22 représente les résultats de l'expérimentation ainsi que la modélisation de ce phénomène. Pour le transistor PMOS, l'amplitude maximale du courant induit est atteinte pour une durée d'illumination supérieure à 15µs. Pour le transistor NMOS, cette durée est atteinte pour une durée d'illumination de 10µs environ.

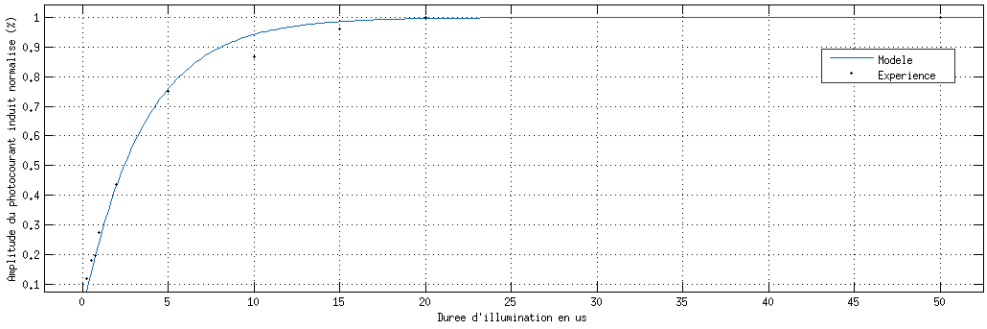


Figure III-22: Effet de la durée d'illumination sur l'amplitude maximale du courant induit.

L'équation (39) donne l'expression de la modélisation de l'effet de la durée d'illumination sur l'amplitude maximale du photocourant induit.

$$I_D = 1 - exp\left(\frac{-D}{a}\right) \qquad (39)$$

Ou a=3,507 et le coefficient de détermination R^2=99%.

d) Effet de la focalisation sur l'amplitude maximale du photocourant induit

On s'intéresse dans ce paragraphe à l'effet de la focalisation sur l'amplitude du photocourant induit dans le canal de conduction. La figure III-23 présente les résultats expérimentaux ainsi que la modélisation de ce phénomène. Le modèle utilisé est une double gaussienne centré en z=0µm, position correspondant au point de focalisation maximal du faisceau sur le transistor. La largeur à mi-hauteur est atteinte pour une défocalisation de 50µm. On retrouve le même résultat que pour le transistor NMOS (largeur à mi-hauteur 40µm).

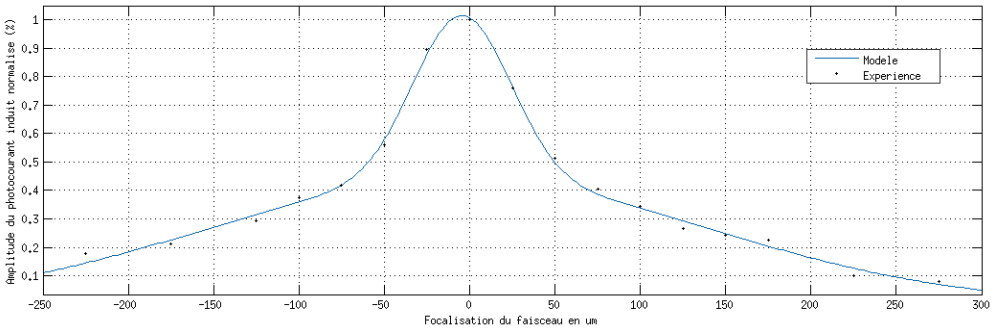


Figure III-23: Effet de la focalisation sur l'amplitude maximal du courant induit dans le transistor PMOS FDSOI

L'équation (40) présente l'expression du modèle utilisé.

$$I_z = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{z-b_i}{c_i}\right)^2\right) \qquad (40)$$

La table 17 donne la valeur des coefficients constants du modèle pour le transistor PMOS FDSOI.

Table 17: Coefficients de modélisation de l'effet de la focalisation sur l'amplitude maximale du courant induit dans le canal de conduction du transistor PMOS FDSOI

a_0	0,7259	a_1	0,2965
b_0	16,77 µm	b_1	13,16 µm
c_0	35,25 µm	c_1	220,3 µm

Avec ces coefficients de modélisation, on a un coefficient de détermination R^2=99,5%.

e) Effet de la polarisation du puit sur le photocourant induit

Afin d'avoir un contrôle électrostatique sur la conduction du canal du transistor, les concepteurs de la technologie FDSOI utilisée ici ont souhaité réduire l'épaisseur du box isolant.

En effet due à la faible épaisseur du box isolant, la tension du Nwell a le même rôle (avec un effet moindre) que la tension de grille du transistor. En effet, lorsque la tension du puit N est à Vdd, alors par effet de champ les trous du canal vont se rapprocher du box. Une zone plus peuplée en trous va alors se créer dans le canal à proximité du box, cette zone va ralentir le passage des trous du drain vers la source du transistor. De même, lorsque le potentiel du puit N diminue alors par effet de champ, on va observer une zone moins peuplée en trous à proximité du box dans le canal, ce dépeuplement va faciliter la traversée des trous. Ainsi la tension de polarisation du puit a un effet sur l'intensité du courant ainsi que sur le temps de commutation du transistor.

Il faut noter cependant que l'état du transistor PMOS (passant ou non passant) est indépendant de la tension du Nwell, celle-ci ne permet que de modifier les caractéristiques dynamiques du transistor (de manière faible).

Le puit Nwell, du transistor PMOS FDSOI, constitue une jonction PN avec le substrat P (figure III-24). Bien que cette jonction ne soit pas directement connectée au canal, lors d'une illumination, celle-ci va modifier les caractéristiques du transistor illuminé. L'illumination de cette jonction va entraîner une modification locale du potentiel du puit N. Cette modification impacte alors l'amplitude du photocourant induit dans le canal mais aussi modifier le temps de commutation du transistor.

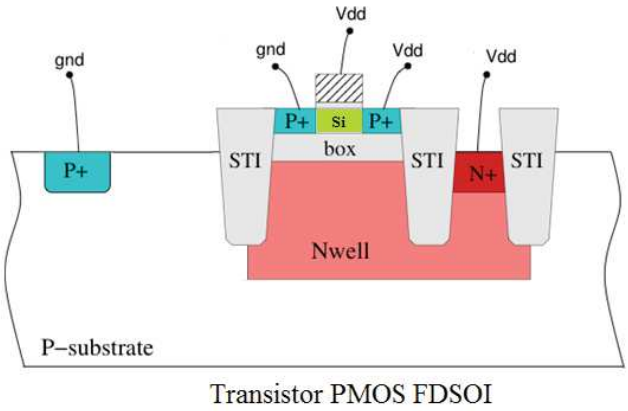


Figure III-24: Vue de principe de la structure du transistor PMOS FDSOI

f) Modification du courant induit dans le canal

On s'intéresse ici à l'effet de la tension de polarisation de la jonction PN Nwell/Psub sur l'amplitude maximale du courant induit dans le canal. Dans des conditions normales de polarisation, on a $V_{psub} = 0V$ et $V_{nwell} = 1V$. En effet, lors de l'illumination de cette jonction, une chute de tension au niveau du Nwell est observée. Cette chute de tension a un impact sur la conduction du canal modifiant l'amplitude du photocourant induit dans celui-ci. Afin de pouvoir modéliser l'influence de la tension de polarisation du Nwell sur l'amplitude du photocourant induit, on réalise plusieurs injections sur un transistor PMOS en modifiant la tension de polarisation du puits N (Nwell). La figure III-25 représente les mesures expérimentales ainsi que la modélisation de ce phénomène. On observe que lorsque la tension de polarisation du Nwell diminue alors le courant induit dans le canal est plus faible. Cette variation n'est pas linéaire avec la tension de polarisation.

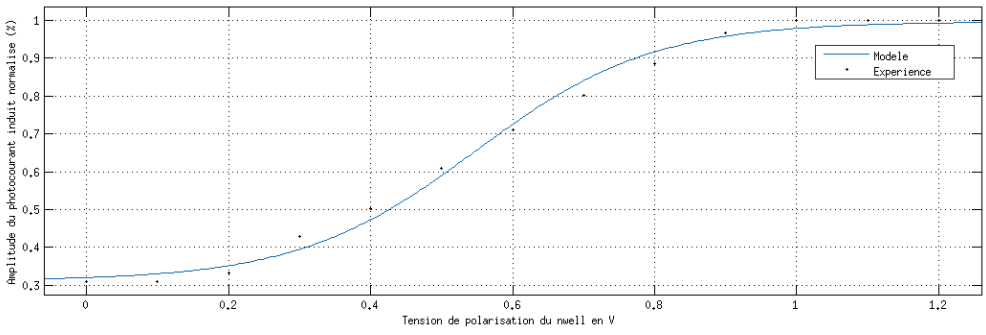


Figure III-25: Mesures (point) et modèle (courbe) de l'effet de la polarisation du Nwell sur l'amplitude maximale du photocourant induit

De cette expérimentation, on détermine le modèle donné par l'équation (41) :

$$I_{nw} = a * th(b * V_{nwell} + c) + d \qquad (41)$$

Où th est la fonction tangente hyperbolique, V_{nwell} représente la tension de polarisation du puits N en Volt et a, b et c les constantes de modélisations. Ces constantes de modélisations sont données par la table 18.

Table 18: Coefficients de modélisation de l'effet de la tension de polarisation du Nwell sur l'amplitude maximale normalisée du photocourant induit dans un transistor PMOS FDSOI

a	0,3427
b	$4\ V^{-1}$
c	-2,19
d	0,6542

Avec ce modèle, on a un coefficient de détermination R^2=99,3%.

III.3.3. Nouveau modèle d'injection de faute

Les caractéristiques structurelles du canal de conduction du transistor NMOS FDSOI conduit à l'établissement d'un modèle électrique différent de celui utilisé pour les transistors NMOS bulk. On modélise le photocourant induit par une source de courant ayant les caractéristiques décrites précédemment dans la section III.3.1. La figure III-26 présente le montage permettant de modéliser l'effet de l'illumination laser sur un transistor NMOS et PMOS FDSOI. Pour le NMOS, la source de courant relie le drain et la source du transistor. En effet, le courant induit ne circule que dans le canal de conduction du transistor (i.e. entre le drain et la source). Pour le transistor PMOS, il faut tenir également compte de la jonction PN composée par le Nwell et le substrat. Dans la section III.2, l'impact de la tension de polarisation du Nwell sur l'amplitude maximale du photocourant induit dans le canal de conduction a été étudié. On modélise donc l'effet de l'illumination de cette jonction PN en utilisant le modèle utilisé pour le bulk.

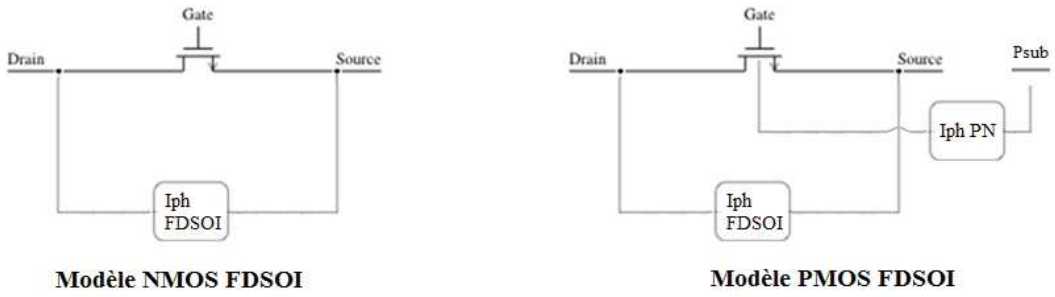


Figure III-26: Modèle électrique des transistors NMOS et PMOS FDSOI sous illumination laser

L'équation (42) donne l'expression du courant débité par la source de courant Iph FDSOI.

$$I_{ph\_fdsoi} = I_p * S * I_x * I_D * I_z * I_{nw} \quad (42)$$

Pour le transistor NMOS FDSOI, il n'y a pas de caisson Nwell. On considère que dans ce cas $I_{nw} = 1$. En effet, le transistor NMOS a un caisson Pwell polarisé à Gnd. Or le substrat est lui aussi polarisé à Gnd, il n'y a donc pas d'effet de champ pour accélérer les porteurs générés dans cette zone. Les porteurs se recombinent rapidement et n'influencent pas l'amplitude induite sur le canal.

III.4. Résultats expérimentaux de l'illumination laser de transistors CMOS bulk et FDSOI

Dans cette section, des campagnes d'injection laser ont été réalisées sur des transistors NMOS Bulk et FDSOI et PMOS bulk et FDSOI. L'objectif de ces campagnes est de comparer la résistance de la technologie bulk et FDSOI face à l'injection laser en termes de courant collecté. Ces campagnes ont fait l'objet d'une publication [47].

III.4.1. Comparaison entre les transistors NMOS bulk et FDSOI

L'injection est réalisée par la face arrière à l'aide d'un faisceau infrarouge (1064nm). Le faisceau laser a un diamètre de 5µm. Le motif expérimental est un transistor NMOS avec (W,L) égal 1µm*3µm. A une puissance fixe, la distance horizontale entre le faisceau et le centre du transistor est modifiée par pas de 1µm. On mesure l'amplitude du photocourant induit collecté au niveau de la source du transistor à l'aide d'une résistance connectée en série avec le drain du transistor pour le transistor NMOS bulk et avec la source pour le transistor NMOS FDSOI. La figure III-27 présente un schéma de principe des courants collectés au niveau de la source du transistor. Pour le transistor NMOS bulk, la mesure s'effectue au niveau du drain du transistor afin de mesurer le courant induit maximal.

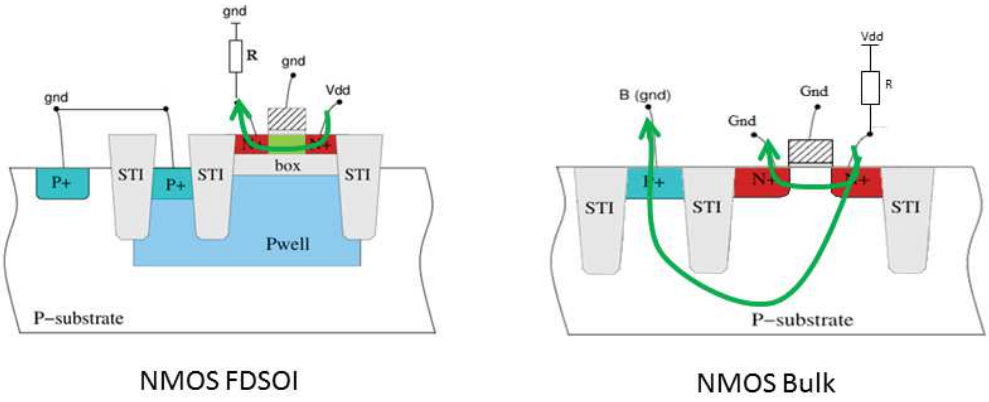


Figure III-27: Schéma de principe du courant collecté au niveau de la source du transistor NMOS pour la technologie FDSOI (à gauche) et bulk (à droite)

La figure III-28 présente les résultats expérimentaux obtenus après une illumination laser de 50µs sur les transistors NMOS bulk et FDSOI. Pour des raisons de confidentialité, les résultats obtenus sont exprimés dans une unité arbitraire. On remarque que l'amplitude du photocourant collecté au niveau du drain d'un transistor NMOS bulk est 5 fois plus élevée que le courant induit dans le canal du transistor NMOS FDSOI. Cette différence est due au substrat Psub du transistor NMOS bulk qui permet la génération d'un plus grand nombre de porteurs de charges qui sont, ensuite, collectées au niveau de la source et du drain du transistor.

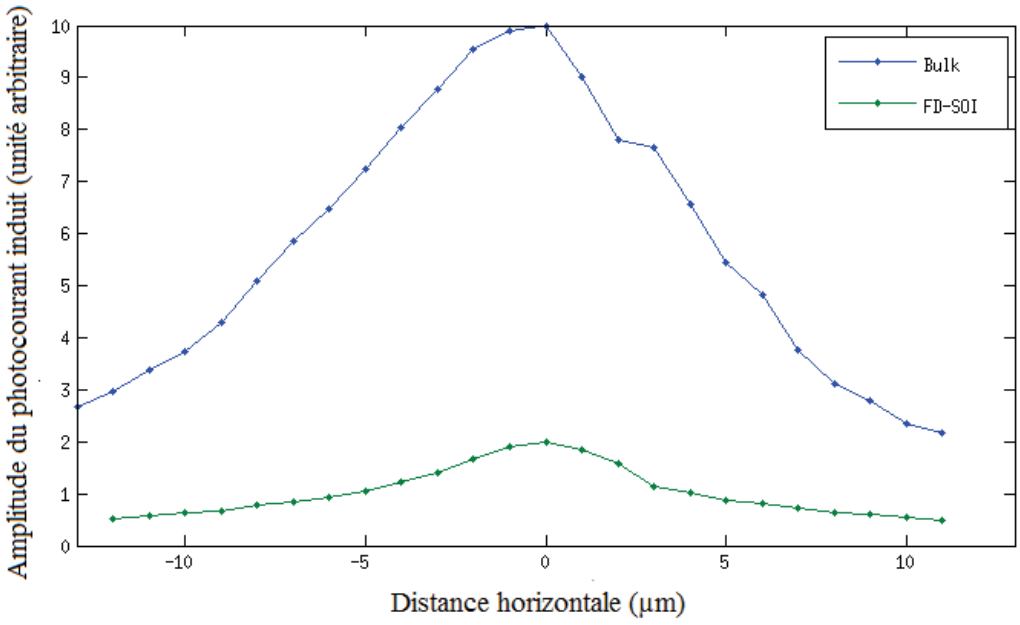


Figure III-28: Comparaison de l'amplitude du photocourant induit pour un transistor NMOS bulk et FDSOI

Afin de tester la résistance du transistor face à l'injection laser, on compare l'amplitude maximale du photocourant induit par rapport au courant nécessaire pour faire changer l'état logique

en sortie d'un inverseur. Les mesures précédentes représentent l'amplitude maximale du photocourant induit dans le pire cas. En effet, le temps d'illumination utilisé correspond au temps à partir duquel l'amplitude maximale de photocourant est atteinte. La table 19 donne la valeur des courants nécessaires pour modifier la valeur logique d'un inverseur. Le courant maximal induit est supérieur au courant nécessaire au changement de valeur logique d'un inverseur pour les deux types de technologies. Cependant la différence entre ces deux courants pour le transistor NMOS FDSOI est beaucoup plus faible que pour le transistor NMOS Bulk. Des fautes peuvent donc être injectées sur des circuits FDSOI à l'aide d'un laser.

Table 19: Tableau comparatif du courant maximal induit et du courant nécessaire au changement d'état logique d'un inverseur

	FDSOI	**Bulk**
Amplitude maximale du photocourant induit	2u	10u
Courant nécessaire au changement d'état logique	0,7u	0,8u

III.4.2. Comparaison entre les transistors PMOS bulk et FDSOI

On compare la résistance des transistors PMOS FDSOI et bulk face à l'injection laser. Pour cela, nous avons réalisé une campagne d'injection sur deux transistors, un transistor PMOS 3µm*1µm bulk et un autre en technologie CMOS FDSOI. La figure III-29 présente une vue de principe des deux transistors qui ont été mis à notre disposition ainsi que leurs layout. Pour ces motifs expérimentaux des diodes de protections (ESD) ont été placés afin d'éviter une casse. Le transistor PMOS bulk a une diode de protection au niveau de sa grille et le transistor FDSOI est protégé par 3 diodes (grille, drain et source). La proximité de ces diodes va avoir un impact sur le photocourant induit dans le canal de conduction du transistor. En effet ces diodes sont des jonctions PN reliées à la ligne de métal du drain, de la source et de la grille. Lors de l'illumination de ces diodes un photocourant va être généré, celui-ci est ajouté au courant induit dans le canal. Ainsi, lorsque le faisceau s'écarte de l'aplomb du transistor, l'effet de l'illumination de la diode devient prédominant devant celui de l'illumination du transistor.

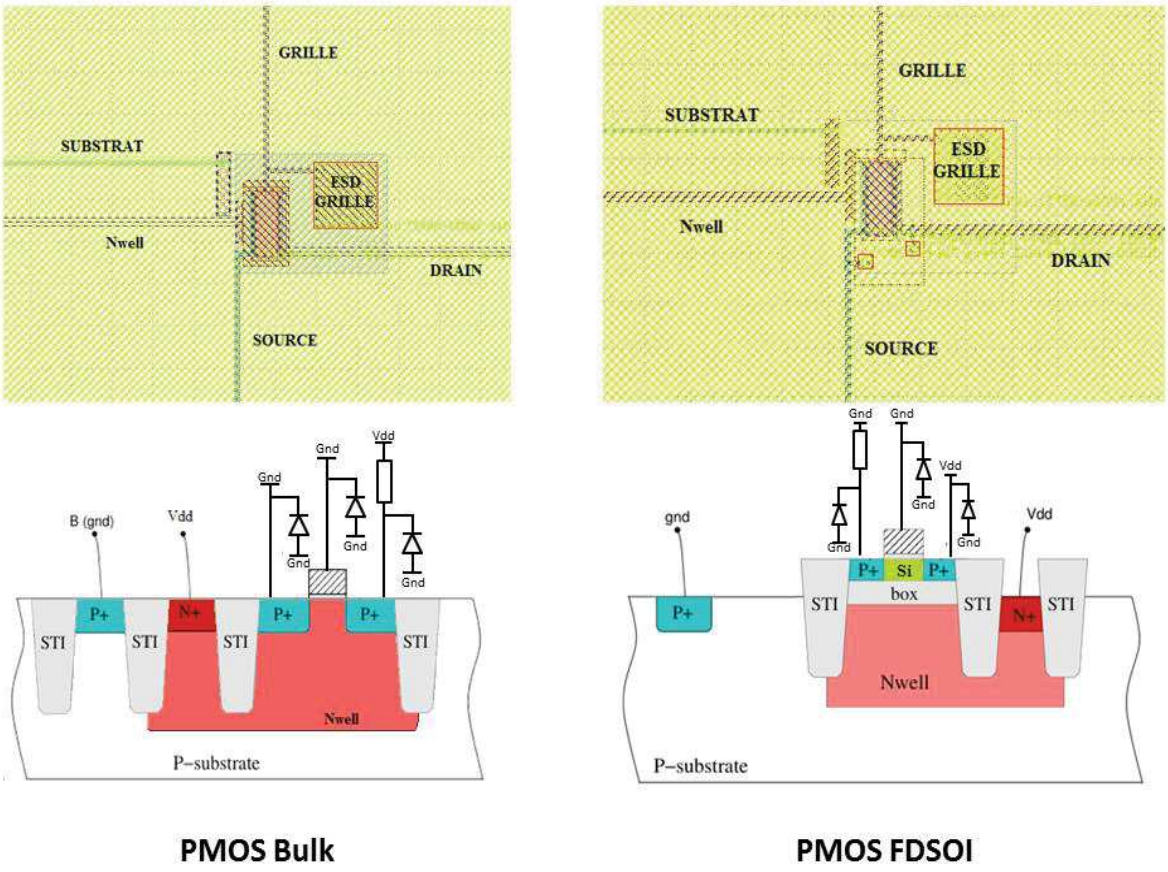


Figure III-29: Layout et vue de principe des transistors PMOS bulk et FDSOI expérimentaux

La figure III-30 présente des cartographies d'amplitude du courant induit collecté au niveau du drain (polarisé à 1V) du transistor. Afin de réaliser ces cartographies, le faisceau laser est déplacé de 1µm suivant les deux axes horizontaux (x et y). Pour chaque position du faisceau une illumination laser de 50µs est réalisée. La mesure de l'amplitude du courant induit est ensuite reportée sur la cartographie. Le code couleur utilisée sur la cartographie représente le pourcentage de l'amplitude maximale du courant induit du bleu vers le rouge (respectivement 0% à 100%). La zone d'effet du laser est plus grande pour le transistor bulk que le FDSOI, 8µm*11µm contre 6µm*7µm. De plus, la diminution d'amplitude du courant collecté, lorsque le faisceau laser s'écarte du transistor est plus forte pour le transistor PMOS FDSOI que bulk. Ceci s'explique par l'effet de l'isolation présente autour du canal du transistor FDSOI. En effet, lorsque le faisceau laser n'est plus à l'aplomb du transistor, moins de charges sont générées dans le canal. L'amplitude du courant collecté, diminue plus rapidement lorsque l'on s'écarte de l'aplomb du transistor.

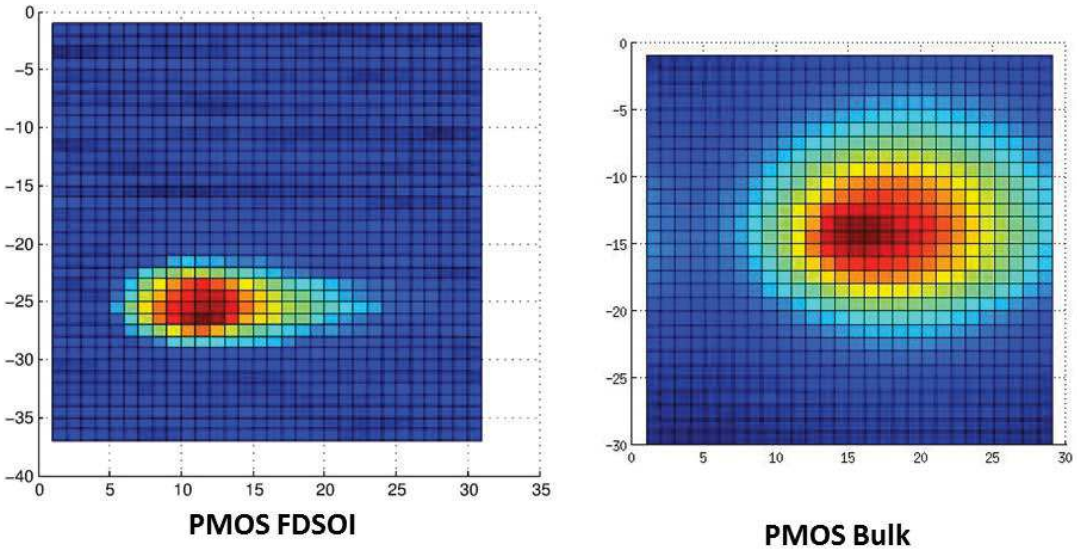


Figure III-30: Cartographie de l'amplitude du photocourant induit dans le canal de conduction (vue de dessus)

La cartographie de l'amplitude maximale du photocourant induit est donnée par la figure III-31. L'amplitude maximale du courant induit dans le canal du transistor est plus faible pour le transistor PMOS FDSOI que pour le transistor PMOS bulk, 4,5ua contre 300ua. Cette différence s'explique par le fait que le canal de conduction du transistor PMOS FDSOI représente un volume dans lequel les charges sont générées plus faibles. De plus, pour le transistor FDSOI, il n'y a pas d'échanges de porteurs de charges à distance à cause de la présence de l'isolant autour du canal du transistor, ce qui a pour effet de réduire la zone de sensibilité de ces transistors à l'illumination.

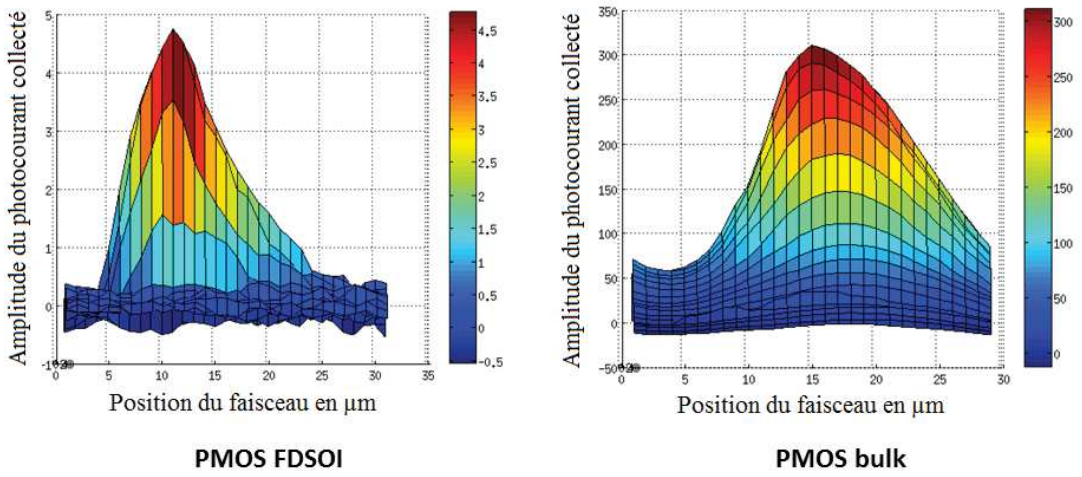


Figure III-31: Amplitude maximale du courant induit injecté pour un transistor PMOS FDSOI et PMOS Bulk (1µm*3µm)

Les courants présentés ici représentent les courants injectés dans le pire cas (temps d'illumination long et puissance élevée). De plus le profil non symétrique des cartographies

présentées dans cette section s'explique par la présence des diodes de protection autour du transistor.

Conclusion

Dans cette partie, nous avons mis à jour un modèle électrique du transistor CMOS bulk sous illumination laser pour la technologie 28nm basé sur le modèle proposé par A. Sarafianos [31]. Puis nous avons développé un nouveau modèle de l'effet d'une injection laser sur les transistors 28nm FDSOI. En effet, l'absence de jonction PN dans le canal de conduction du transistor ne permet pas d'utiliser le modèle pour les transistors bulk (généralisation de la jonction PN). Cependant les paramètres qui influencent le courant induit dans le canal par le laser sont les mêmes. Seul l'effet de la polarisation du Nwell pour le PMOS FDSOI doit être pris en compte en plus des paramètres. Bien qu'il n'y ait pas d'échanges de charges entre la jonction PN formée par le Nwell et le Psub et le canal de conduction, l'effet de l'illumination de cette jonction, impacte à distance l'amplitude du photocourant induit dans le canal mais aussi sur la vitesse de commutation du transistor PMOS FDSOI. La comparaison entre les transistors NMOS, en technologie bulk et FDSOI, confirment les effets théoriques attendus par la technologie FDSOI sous illumination laser. En effet, l'isolation du canal de conduction a pour effet de réduire le volume de charges collectées, donc de réduire le courant induit dans le canal, ainsi que de limiter spatialement l'effet du laser, le courant collecté diminue rapidement lorsque le faisceau s'écarte du canal du transistor.

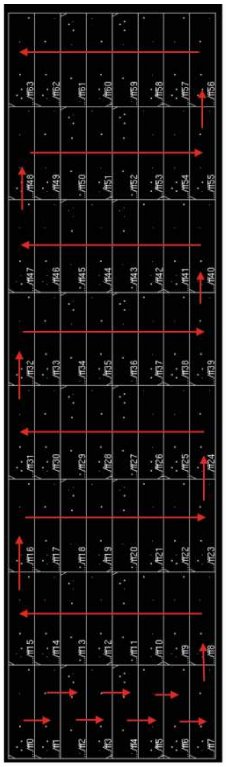
Chapitre IV.
Etude de l'injection de fautes par laser dans les registres des technologies CMOS 28nm bulk et FDSOI

Préambule

Afin de confirmer les observations faites sur les transistors 28nm bulk et FDSOI, des injections laser sont effectuées sur des éléments plus complexes. On étudie ici, l'injection laser sur une chaîne de bascules D Flip-flop implantées en technologies CMOS 28nm bulk et FDSOI. Chacun des motifs, bulk et FDSOI, est comparé en terme de type de fautes injectées ainsi qu'en terme de sensibilité à l'énergie d'injection. Ensuite, une comparaison de la résistance de ces deux technologies face à une attaque par injection laser est menée.

IV.1. Présentation de la cible : le circuit DFF matrix

On s'intéresse dans la suite au motif "Matrix" composé d'une chaîne de 64 bascules maitre-esclaves, ces bascules seront décrites plus en détail au paragraphe IV.3.1. La sortie de chacune des bascules est reliée à l'entrée de la suivante. Cette chaîne compose un registre à décalage, à chaque front montant du signal d'horloge, la valeur logique d'une bascule sera enregistrée dans la bascule suivante. Il faut donc 64 cycles d'horloge pour charger (resp. décharger) le registre. La figure IV-1 représente une vue de l'implantation des bascules pour ce motif. Les flèches rouges sur la figure indiquent le sens de connexion des bascules constituant le registre à décalage, la connexion de ces dernières forme un serpentin.



Matrix

Figure IV-1: Schéma de l'implantation des bascules pour le motif Matrix

La figure IV-2 présente le positionnement du motif Matrix sur le circuit en vue layout.

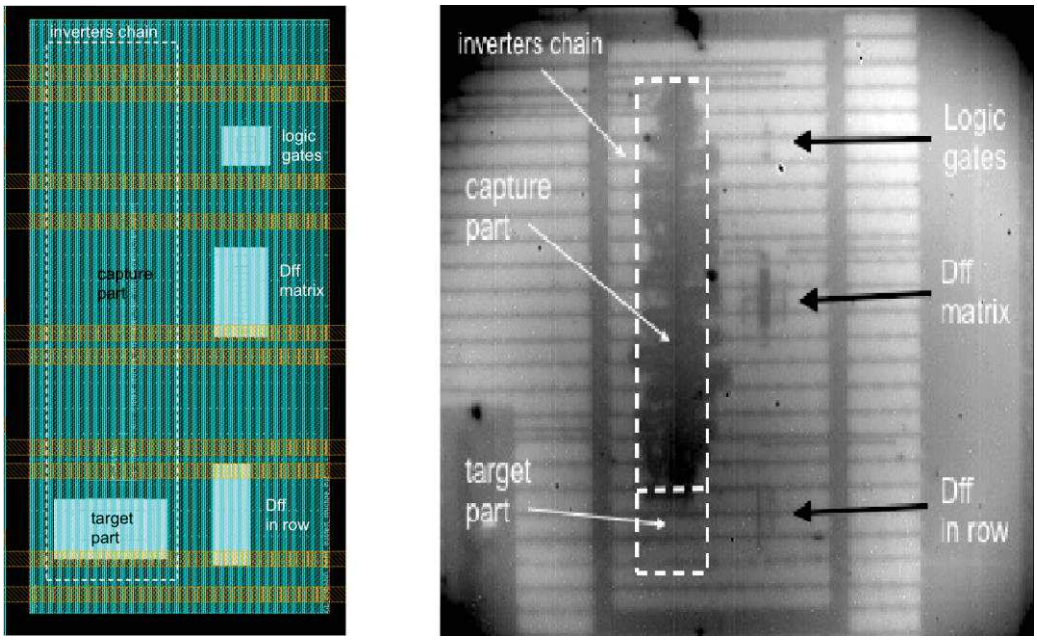


Figure IV-2: Abstract et image infrarouge du placement du motif Matrix sur le circuit testé

La figure IV-3 présente l'abstract de la vue layout du motif Matrix. On observe un espace séparant les 32 premières bascules des 32 dernières.

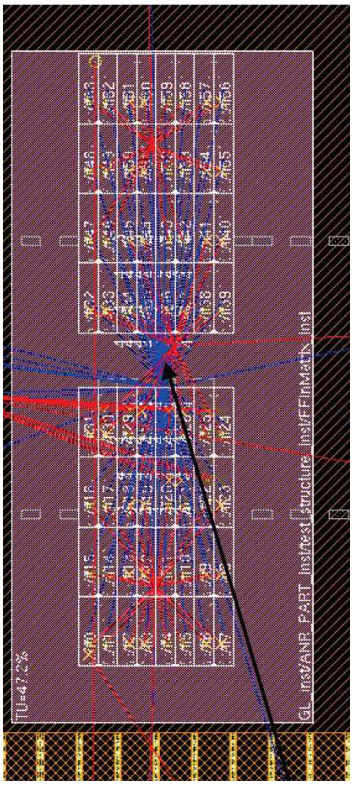


Figure IV-3: Positionnement spatial des cellules standards des bascules du motif DFF matrix

Afin de tester la résistance de chaque technologie face à l'injection laser, sur des circuits plus complexes que des transistors isolés, des campagnes d'injections sont effectuées sur le motif Matrix bulk et FDSOI.

IV.2. Injection de fautes sur le motif DFF Matrix

L'injection sur le motif Matrix est réalisée de manière statique, c'est-à-dire que l'état logique du signal d'horloge ne varie pas durant l'illumination du circuit. Ici durant l'illumination le signal d'horloge est maintenu à l'état bas. On charge au préalable les 64 registres à 0 et à 1 afin de déterminer les zones de bit set et bit reset (cf. I.2.6). L'illumination du circuit est faite par la face arrière à l'aide d'un faisceau infrarouge de diamètre 1 µm. Afin de réaliser les injections, on utilise une source laser dite « picosecondes » qui permet une illumination de 30 ps fixe. Le faisceau laser est déplacé par pas de 1 µm afin de balayer la zone d'implantation du motif. La figure IV-4 présente un exemple de résultat d'une cartographie 2D du motif DFF Matrix. On observe en abscisse et ordonnée, la position du faisceau laser lors de l'illumination. Les points bleus (resp. rouges) présentent les zones pour lesquelles une faute de type bit set (resp. bit reset) a été injecté dans le motif DFF matrix. Si pour une même position, on observe un bit set et un bit reset, alors on considère cette position comme une position d'injection de faute de type bit flip (point rose).

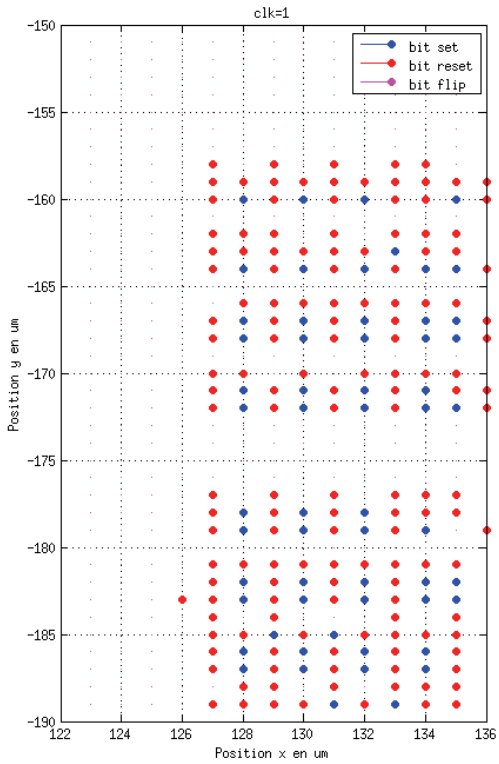


Figure IV-4 : Exemple de cartographie 2D d'injection sur le motif DFF matrix

La figure IV-5 représente la même cartographie que la précédente mais en trois dimensions. La hauteur (axe z) représente la position de la bascule fautée dans la chaîne (de 1 à 64).

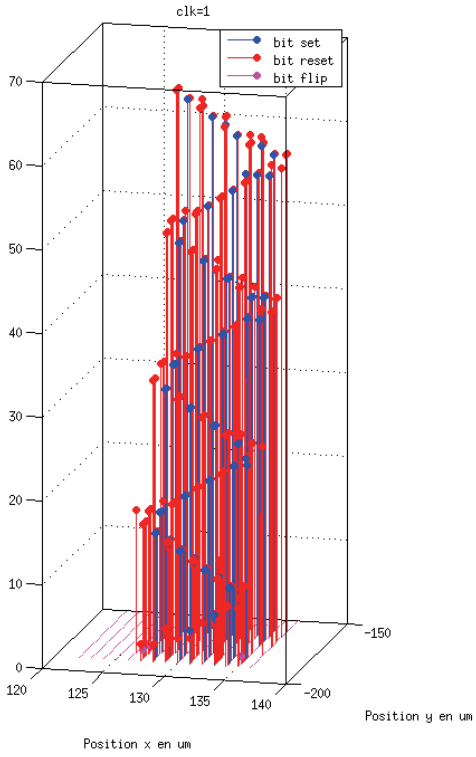


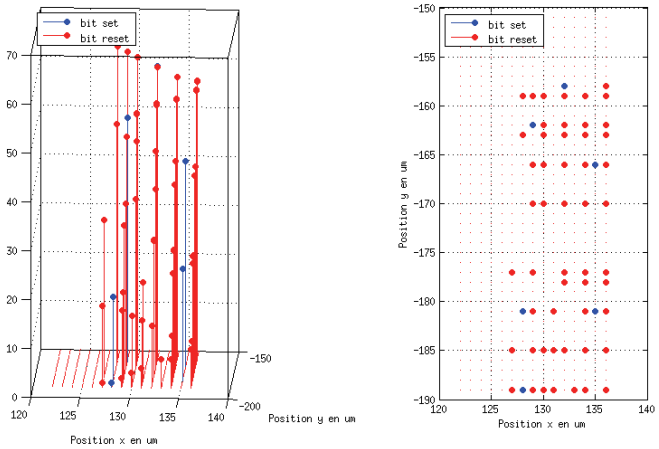
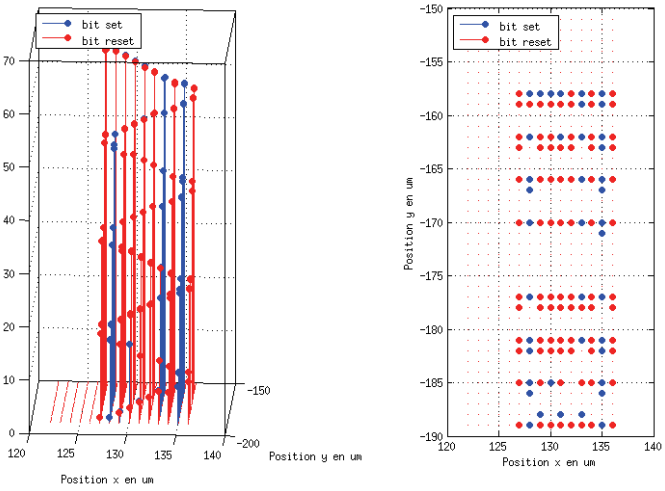
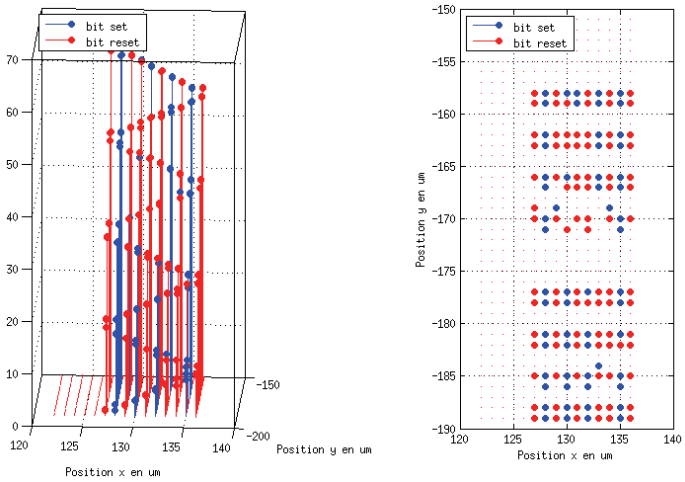
Figure IV-5 : Exemple de cartographie 3D d'injection sur le motif DFF Matrix

IV.2.1. Etude du type de fautes injectées

On compare le nombre de bascules DFF du motif Matrix fautées pour différentes énergies d'illumination. La table 20 présente les cartographies résultantes des campagnes d'injections sur le motif Matrix bulk. Les premières fautes apparaissent pour une énergie de 0,2 nJ. On remarque pour le motif bulk, qu'une faible augmentation de l'énergie au-dessus du seuil de faute entraîne la génération de fautes dans toutes les bascules de la matrice (taux de couverture de 100%). De plus, plus l'énergie d'injection augmente, plus le nombre de bit set augmente. On observe de plus l'espace présent entre les 32 premières bascules et les 32 dernières présentés sur la figure IV-3. Sur la cartographie en trois dimensions, on retrouve la connexion en serpentin entre toutes les bascules.

Table 20: Cartographies du motif DFF Matrix (bulk) pour différentes énergies d'injection

Energie	Bulk

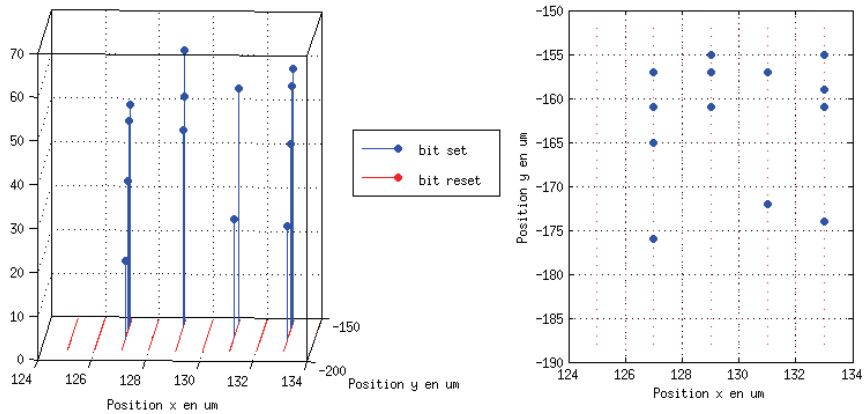
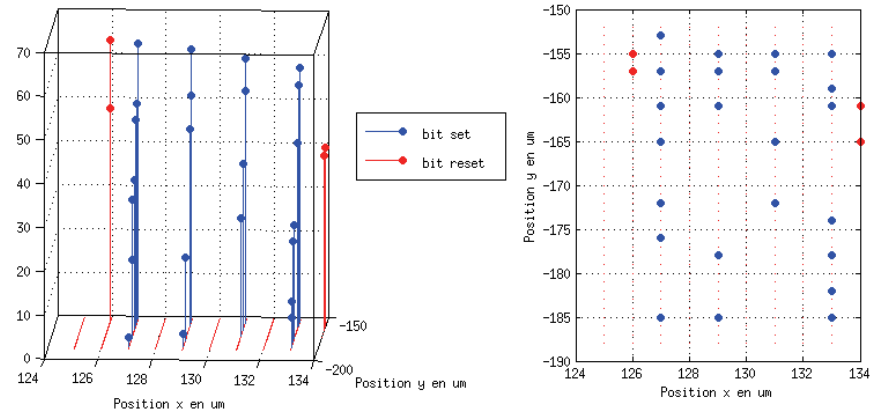
0,2nJ		
	Taux de couverture: 73,4%	
0,3nJ		
	Taux de couverture : 100%	
≥0,4nJ		
	Taux de couverture : 100%	

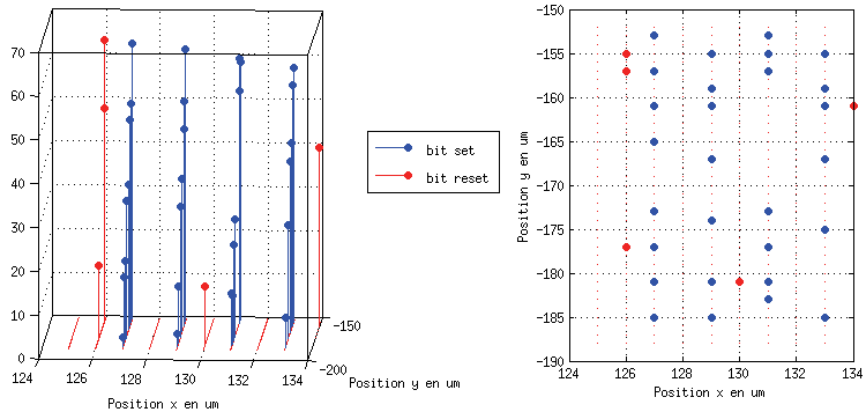
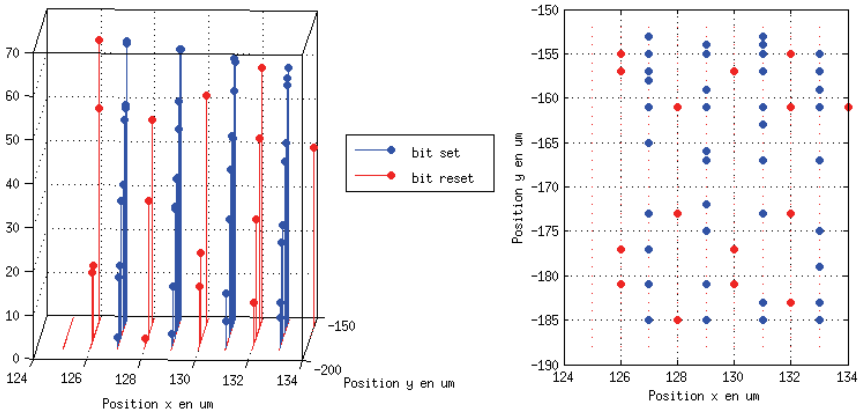
La table 21 présente les résultats d'injections laser réalisées sur le motif Matrix FDSOI. Pour une énergie inférieure ou égale à 0,2nJ, aucune faute n'est injectée dans le registre. Les premières fautes

apparaissent pour une énergie de 0,3nJ. On remarque aussi que pour ce circuit toutes les fautes injectées sont des fautes de type bit set.

Plus l'énergie d'injection augmente, plus le nombre de faute de type bit reset augmente. Cependant, ce nombre reste minoritaire devant le nombre de faute de type bit set injecté.

Table 21: Cartographies du motif DFF Matrix (FDSOI) pour différentes énergies d'injection

Energie	FDSOI
0,2nJ	Aucune faute injectée
	Taux de couverture: 0%
0,3nJ	
	Taux de couverture : 45,3%
0,4nJ	
	Taux de couverture : 65,6%

0,5nJ	
	Taux de couverture : 73,4%
0,6nJ	
	Taux de couverture : 89,1%

L'injection laser permet d'induire des fautes sur les bascules DFF 28nm bulk et FDSOI. Cette observation confirme les résultats obtenus sur l'injection sur les transistors de ces technologies.

Le taux de couverture est plus faible pour le motif Matrix FDSOI que pour le motif bulk. Le taux maximum (100%) est rapidement atteint pour le motif bulk, alors qu'il est nécessaire d'augmenter l'énergie d'injection, afin d'atteindre des taux du même ordre de grandeur pour le motif FDSOI (89,1% pour E=0,6nJ).

IV.2.2. Etude la zone de sensibilité de chacun des motifs

Afin de quantifier qualitativement l'effet de la box présent sur les transistors FDSOI, on mesure le nombre de bascules fautées en une seule injection. En effet, on a vu sur le transistor que la box limite les échanges de charges entre le substrat et le canal de conduction, ceci a pour effet de réduire la zone de sensibilité à l'injection des transistors FDSOI (cf. III.4.2). Donc a priori, le nombre de bascules fautées en une seule injection doit être plus faible pour le FDSOI que pour le bulk.

Les figure IV-6 et figure IV-7 présentent deux campagnes d'injections réalisées avec une durée d'illumination de 30ps, un faisceau de 1µm de diamètre et une énergie de 0,6nJ, respectivement sur le motif Matrix bulk et FDSOI. Chaque campagne présente deux cartographies, celle de gauche est obtenue lorsque la donnée stockée dans le registre est un 0 logique, et celle de droite lorsque la valeur logique est 1. Sur chacune des cartographies, les axes représentent la position du faisceau lors de l'injection. Les points bleus représentent les positions pour lesquelles, le tir laser a induit une faute sur une seule bascule. Les points bleus clairs représentent les positions pour lesquelles deux bascules ont été fautées simultanément.

L'illumination des deux motifs n'a pas induit de faute impactant trois bascules ou plus simultanément. Cela s'explique par le fait que le faisceau laser a un diamètre de 1µm et qu'une bascule a une surface de 1,2µm*4,352µm. Le faisceau ne peut donc pas illuminer les zones sensibles (cf. section IV.3.2) de plus de deux bascules simultanément.

La table 22 résume les proportions de fautes injectées sur une ou deux bascules simultanément pour le motif bulk et FDSOI et une donnée stockée 0 ou 1. Pour le motif bulk, le taux d'injection en un seul tir d'une faute sur une bascule est de l'ordre de 50% quel que soit la valeur stockée dans le registre. Cette proportion s'explique par le fait que lorsque le laser illumine une seule bascule, seule celle-ci est fautée. Cependant si le faisceau laser illumine simultanément deux bascules voisines, les charges générées dans le substrat (ou le Nwell), c'est-à-dire à distance du canal de collection des transistors sensibles, sont quand même collectées et induisent une faute dans les deux bascules.

Pour le motif FDSOI, lorsque la donnée stockée dans le registre est 0 alors on observe une majorité de fautes n'impactant qu'une seule bascule. De même, lorsque la donnée stockée est 1 alors les fautes injectées ne touchent qu'une seule bascule. Cela s'explique par le fait que l'isolation du canal de conduction du transistor FDSOI par le box réduit la zone de sensibilité du transistor. Ainsi pour fauter deux bascules, il faut que le faisceau illumine simultanément le canal des transistors sensibles des deux bascules.

Cette expérimentation sur un circuit plus complexe a permis de confirmer les résultats obtenus sur les zones de sensibilité des transistors bulk et FDSOI (cf. III.2). C'est-à-dire, que la zone de sensibilité de la technologie FDSOI est plus faible que celle de la technologie bulk grâce à l'effet du box isolant présent dans les transistors FDSOI.

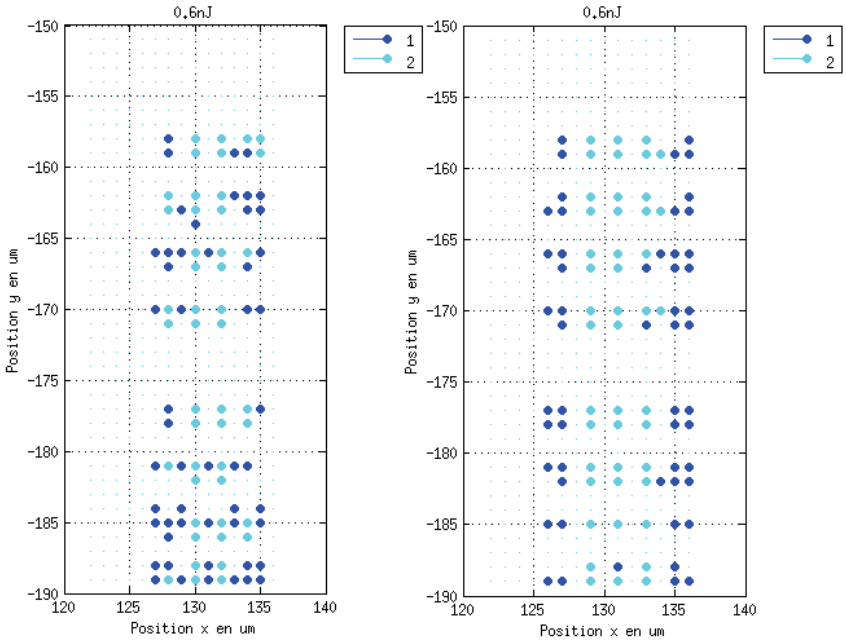


Figure IV-6: Multiplicité de la faute sur le motif DFF Matrix bulk avec E=0,6nJ

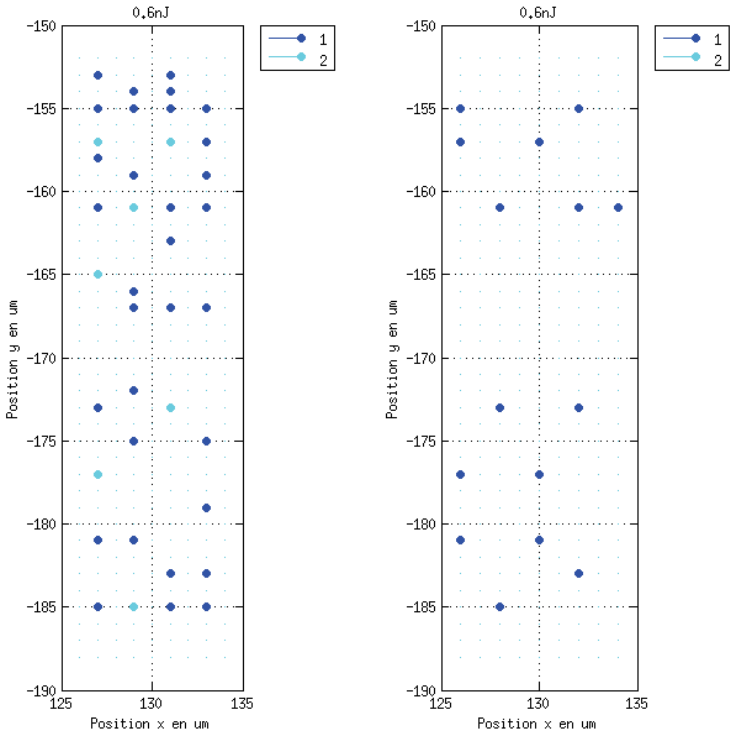


Figure IV-7: Multiplicité de la faute sur le motif DFF Matrix FDSOI avec E=0,6nJ

Table 22: Taux d'injection sur une bascule ou deux bascules simultanément en un seul tir pour le motif Matrix bulk et FDSOI

	Bulk		FDSOI	
Donnée stockée	0	1	0	1
1 bascule fautée	52,7%	54,5%	82%	100%
2 bascules fautées	47,3%	45,5%	18%	0%

Cette section a permis de confirmer que les observations obtenues sur les injections sur transistor. Ainsi, dans les mêmes conditions expérimentales, il est plus difficile d'injecter des fautes par illumination dans un circuit étant implanté en technologie FDSOI que bulk. Cependant, il est plus facile d'injecter une faute sur une seule bascule dans le registre en FDSOI qu'en bulk. Cet effet est du au box isolant présent dans la structure du transistor FDSOI.

D'après ces observations, la technologie FDSOI semble plus résistante à l'injection de faute par laser mais permet d'injecter plus facilement des fautes mono-bit, ce qui correspond au modèle de faute le plus exigeant. Dans la section suivante, on compare la résistance de ces deux technologies vis-à-vis de l'attaque en faute par illumination laser.

IV.3. Attaque en faute

L'objectif d'une attaque en faute est d'introduire un changement de valeur logique dans le circuit ciblé lors du calcul. On distingue deux cibles pour l'injection : les portes logiques et les éléments de mémorisations. Dans la section I.1.3, nous avons vu que pour des raisons de contraintes temporelles, il est plus facile pour l'attaquant d'injecter une faute en ciblant les éléments de mémorisations et donc de générer un Single Event Upset (SEU).

IV.3.1. Description de la bascule DFF

La figure IV-8 présente le symbole logique de la bascule utilisée pour les injections et la table 23 décrit sa table de vérité. Cette bascule possède une entrée de donnée D, une sortie non inversée Q, un signal de reset asynchrone actif à l'état bas, des signaux de scan TI et TE ainsi que CP le signal d'horloge. Lorsque le signal reset est à l'état bas, quel que soit l'état des signaux de la bascule la valeur logique retournée à la sortie Q est la valeur logique '0'. Lorsque le signal reset est à l'état haut ('1' logique), la bascule fonctionne normalement. Lors d'un front montant du signal d'horloge (CP), la valeur logique de l'entrée D est assignée à la sortie de la bascule (Q). Dans les autres cas où le signal d'horloge n'est pas un front montant, la valeur de la sortie est maintenue. SI lors d'un front montant

de l'horloge, le signal TE est à l'état haut alors la bascule stocke la valeur logique du signal TI et non celle de l'entrée D. Les signaux TE et TI sont des signaux de test et permettent de stocker des valeurs souhaitées (vecteur de test) dans chacune des bascules de la chaîne sans nécessiter 64 coups d'horloge (i.e. le chargement normal d'un registre à décalage composé de 64 bascules).

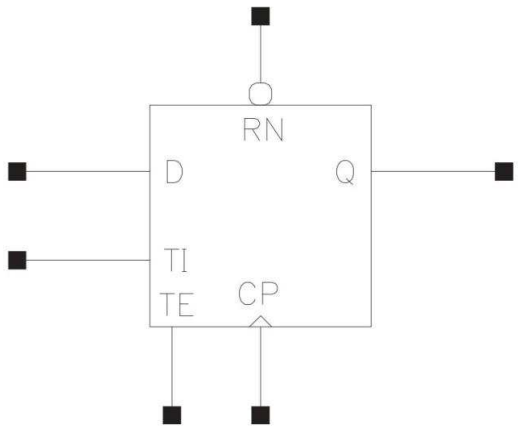


Figure IV-8: Symbole logique de la bascule D flip flop utilisée pour l'expérimentation

Table 23: table de vérité de la bascule utilisée pour l'expérimentation

D	CP	RN	TI	TE	Q	Q
-	-	0	-	-	-	0
D	↗	1	-	0	-	D
-	↘	1	TI	1	-	TI
-	-	1	-	-	Q	Q

La bascule utilisée pour notre expérimentation a une hauteur de 1,2µm et une largeur de 4,352µm, soit une surface de 5,2224µm².

La figure IV-9 présente le schéma au niveau transistor de la bascule DFF utilisée. Ce type de bascule est composé de deux latchs (i.e. verrous) de mémorisations, le maître et l'esclave. Chacun de ces verrous étant formée de deux inverseurs tête bêche. Lorsqu'une telle boucle est isolée (entrée non électriquement reliée), la valeur logique inscrite dans la boucle reste stockée.

L'état logique du signal de sortie Q de la bascule dépend de l'état logique du signal d'horloge CP. Le fonctionnement de la bascule pour un cycle complet d'horloge est décrit ci-après.

- **CP='0'** : Le maître qui, dans ce cas, est en mode transparent, i.e. le verrou est ouvert. L'esclave est en mode mémoire et propage sur la sortie de la bascule la valeur logique mémorisée précédente (cf. figure IV-10).
- **CP= front montant** : La valeur d'entrée, D ou Ti suivant la valeur de Te, est mémorisée dans le maître de la bascule. La sortie de la bascule correspond à la valeur d'entrée.

- **Cp='1'** : Le maître est en mode mémoire, il propage la valeur mémorisée sur la sortie de la bascule (cf. figure IV-11). L'esclave est en mode transparent, le verrou est ouvert.
- **CP= front descendant** : La valeur stockée dans la boucle maître est inscrite dans la boucle esclave de la bascule. Pour cet état on a l'état logique de sortie de bascule encore égal à la valeur logique stockée dans la boucle maître.
- **CP='0'** : On se retrouve dans l'état initial où la sortie de la bascule correspond à la valeur logique stockée dans la boucle esclave.

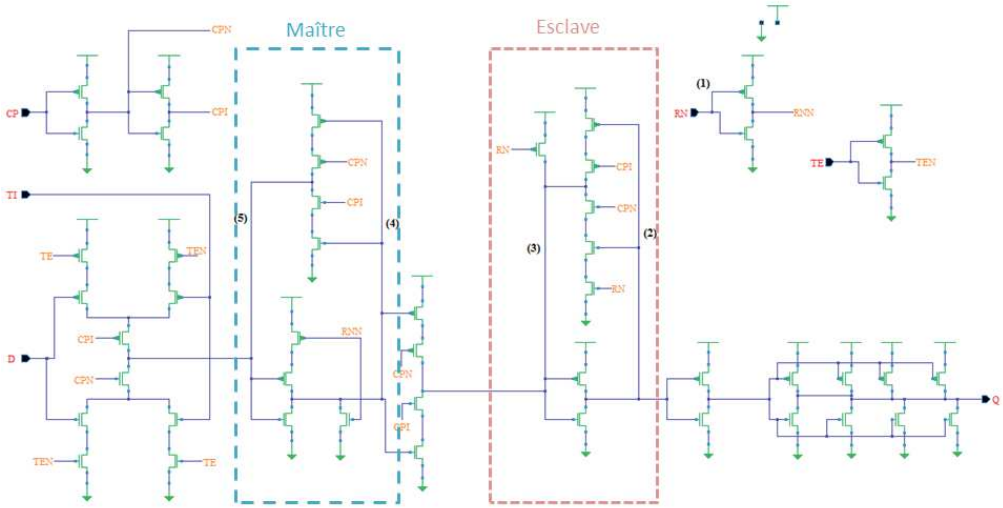


Figure IV-9: Schéma transistor de la bascule DFF

On s'intéresse donc au fonctionnement et à l'injection sur la bascule DFF 28nm FDSOI et bulk présentée précédemment. L'injection est réalisée de manière statique, c'est-à-dire qu'il n'y a pas de changement de niveau logique du signal d'horloge lors de l'illumination. L'étude des résultats d'injection dynamique reste plus complexe dans la mise en pratique, du fait des imprécisions inhérentes au matériel. On sépare quatre cas d'injection statique : lorsque durant l'illumination l'horloge est à l'état haut ou à l'état bas et lorsque la donnée stockée dans la bascule est '1' ou '0'.

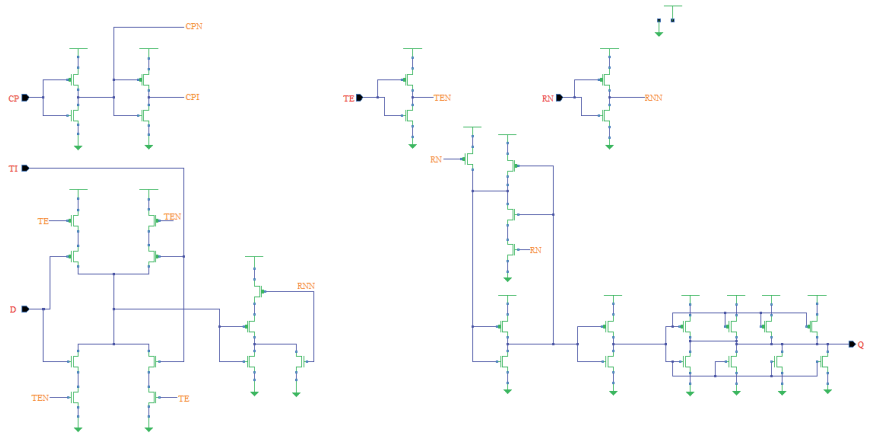


Figure IV-10: Vue schématique du circuit de la bascule lorsque le signal d'horloge est à l'état bas (CP='0')

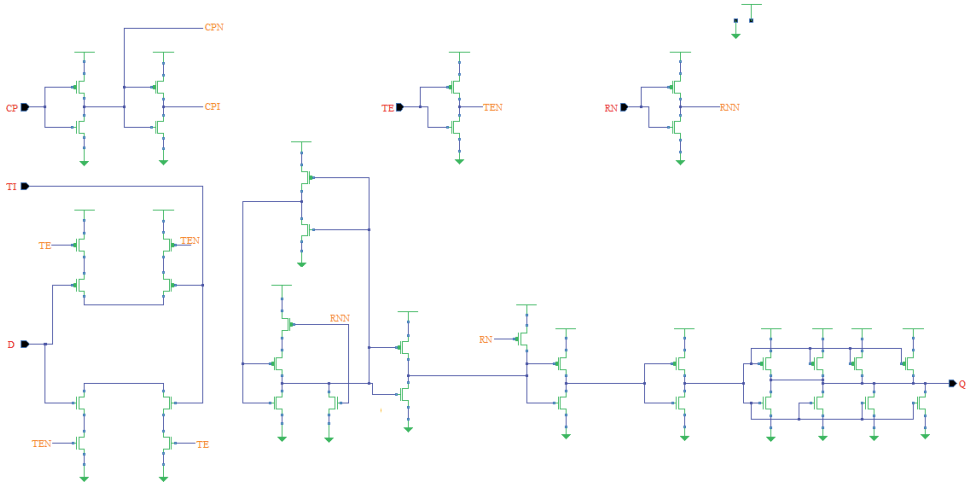


Figure IV-11: Vue schématique du circuit de la bascule lorsque le signal d'horloge est à l'état haut (CP='1')

IV.3.2. Zones sensibles de la bascule DFF

L'injection laser réalisée sur les bascules DFF est statique. C'est à dire que l'on charge la donnée 0 ou 1 logique dans la bascule puis on illumine la bascule en maintenant le signal d'horloge à l'état haut ou l'état bas.

La figure IV-12 présente les zones sensibles de la bascule lorsque le signal d'horloge est maintenu à 0 lors de l'illumination. L'injection est réalisée de manière statique, la faute doit être injecté dans la boucle esclave afin d'être relue lors du déchargement de la bascule au front montant suivant de l'horloge. Dans le cas où Clock=0, alors les zones sensibles correspondent aux transistors bloqués de la boucle esclave de la DFF. Les transistors encadrés en rouge sont les transistors bloqués lorsque la valeur stockée par la boucle esclave est la valeur 1. Lorsqu'un de ces transistors est illuminé, la valeur

stockée dans la bascule devient 0 (bit reset). De même les transistors encadrés en bleu sont les transistors non passant pour une valeur 0 mémorisée par la boucle esclave. L'illumination d'un de ces transistors entraîne un bit set (passage de 0 à 1).

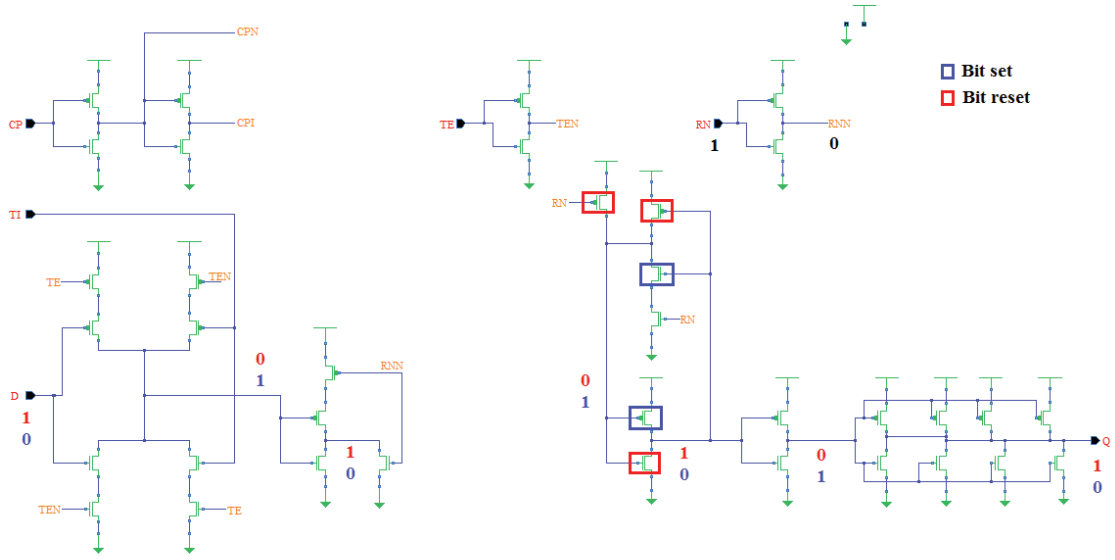


Figure IV-12: Zone de sensibilité de la bascule DFF à l'injection laser lorsque Clock=0

La figure IV-13 représente les zones sensibles de la bascule lorsque le signal d'horloge est maintenu à l'état haut lors de l'illumination laser. Dans ce cas, c'est la boucle maître qui stocke la valeur logique qui sera libérée au prochain front montant de l'horloge. L'illumination des transistors encadrés de bleu engendre un bit set. Les transistors encadrés en rouge permettent de réaliser un bit reset, s'ils sont la cible de l'illumination. En plus des transistors bloqués de la boucle maître, le transistor bloqué de l'inverseur générant le signal RNN (signal logique complémentaire au reset) permet d'induire un bit reset dans la boucle maître.

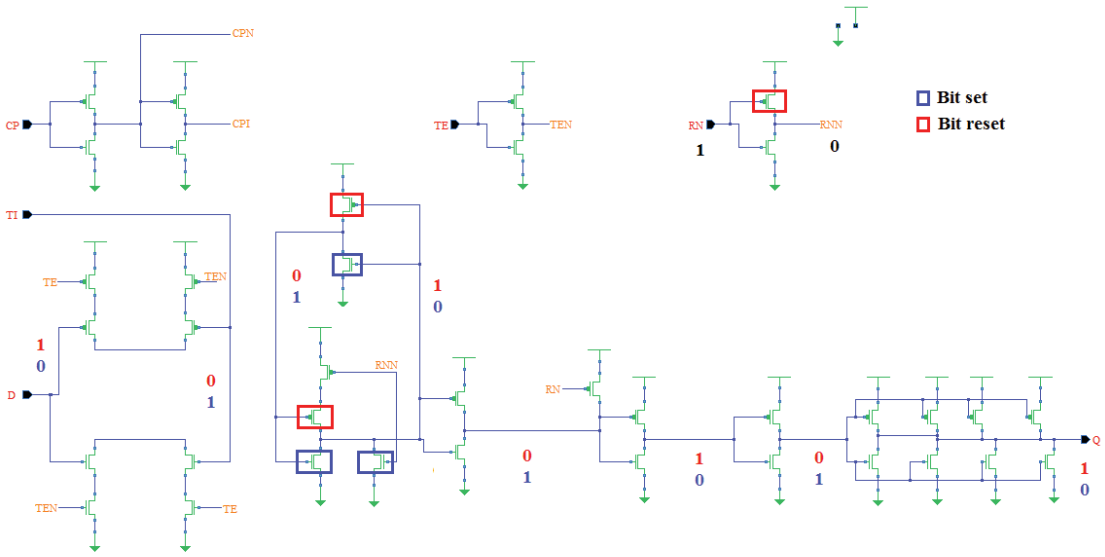


Figure IV-13: Zone de sensibilité à l'injection laser (Clock=1)

Ces différentes zones de sensibilités (boucle esclave, boucle maître et reset) sont représentées sur l'abstract de la bascule par la figure IV-14.

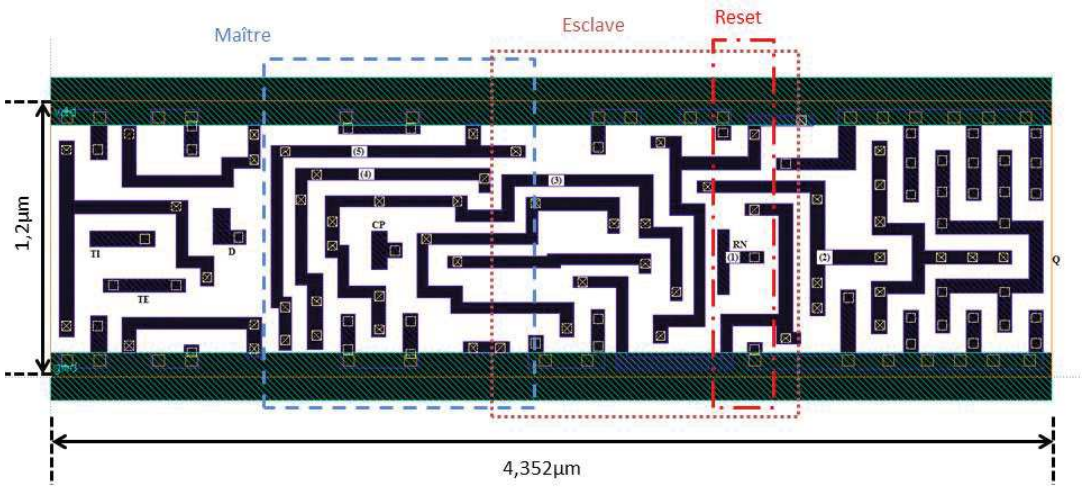


Figure IV-14: Abstract du layout de la bascule DFF

IV.3.3. Injection laser sur une bascule DFF

La bascule DFF est une cible importante pour l'injection laser. En effet, il est possible pour un attaquant, de modifier la valeur logique stockée directement dans l'élément de mémorisation, avec des contraintes temporelles plus faibles qu'en injectant sur la logique. Afin de quantifier la difficulté d'injection sur ces éléments, on réalise des injections laser en déplaçant un faisceau laser de 1µm de diamètre au-dessus d'une bascule par pas de 0,2µm. Ces campagnes ont pour objectifs de

déterminer le seuil de casse et de faute de la bascule ainsi que d'observer s'il est possible en pratique de distinguer les zones sensibles théoriques présentées précédemment. Pour ces injections, on utilise le motif DFF Row (cf. figure IV-15) qui est un registre à décalage de 10 bascules alignées. L'utilisation de ce motif permet les effets parasites des bascules latérales présentes dans le motif DFF Matrix.

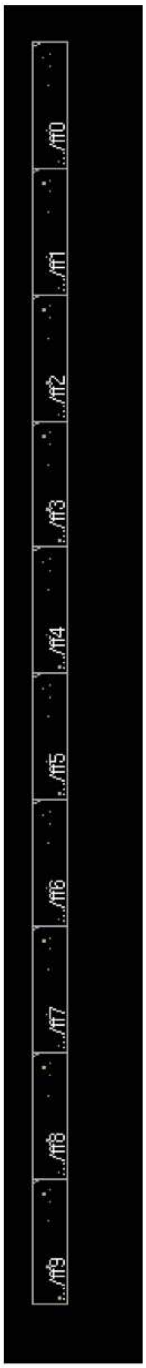


Figure IV-15 : Schéma d'implantation des bascules du motif DFF Row

La figure IV-16 présente la cartographie d'une bascule DFF bulk et FDSOI. La cartographie de la bascule FDSOI présentée ici n'est pas complète. En effet, à cause du phénomène de casse lors d'une répétition de tirs sur le FDSOI, il est difficile de réaliser une cartographie complète sans endommager la bascule de manière permanente.

Pour la bascule DFF bulk et FDSOI, on remarque que les zones de bit set et bit reset sont distinctes et que ces zones ne sont pas les mêmes lorsque le signal d'horloge est à l'état haut ou bas. Cela signifie qu'en pratique un attaquant peut choisir le type de faute à injecter (bit set ou bit reset) suivant la zone illuminée, même sur un circuit en 28nm.

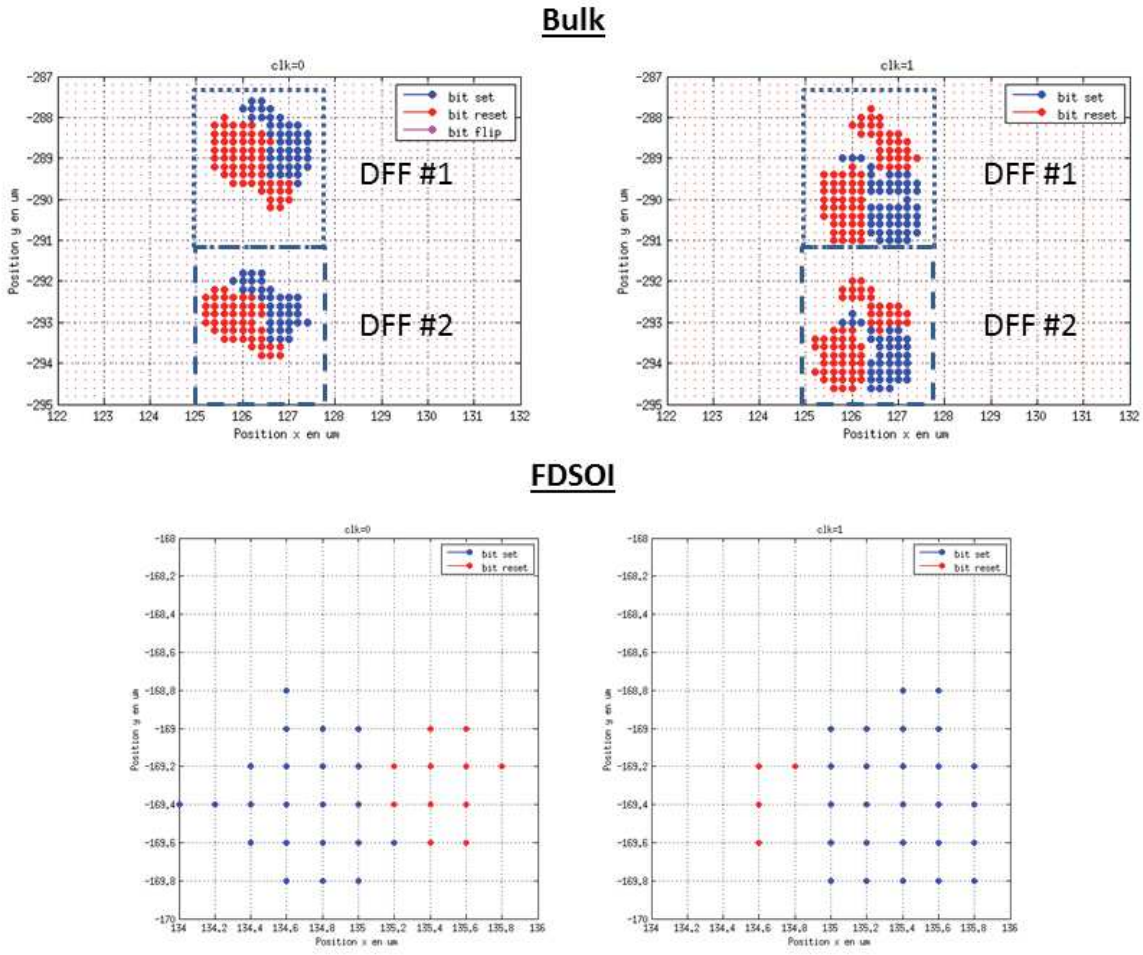


Figure IV-16: Cartographie d'une bascule DFF bulk et FDSOI

La correspondance entre la cartographie expérimentale de la bascule bulk et l'abstract de la DFF est donnée par la figure IV-17. Lorsque le signal d'horloge est à l'état bas, on a une zone d'injection de faute (zone 1) correspondant à la boucle esclave de la bascule sur l'abstract (cf. figure IV-14). Le découpage de cette zone en zone d'injection de bit set et de bit reset est dû à la séparation des plans PMOS et NMOS (Les PMOS sont placés à proximité du rail d'alimentation et les NMOS du rail de

masse). Lorsque Clock='1', on distingue deux zones d'injections distinctes, zone 2 et zone 3, celles-ci correspondent respectivement à l'inverseur du signal de reset (cf. figure IV-14) et à la boucle maître de la bascule.

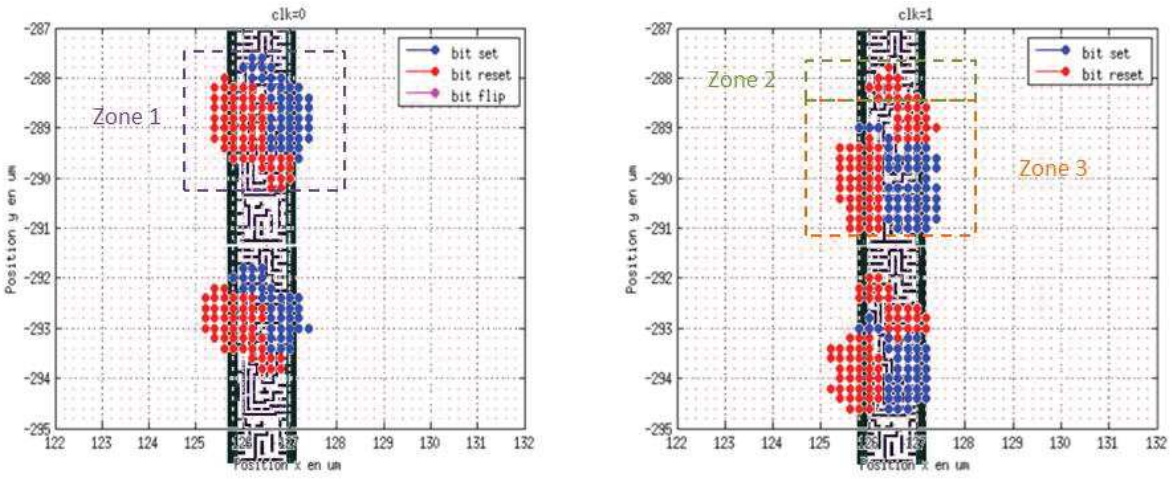


Figure IV-17: Correspondance cartographie/abstract pour une bascule DFF bulk

L'injection sur le motif bascule DFF bulk et FDSOI a permis de mettre en évidence la distinction des zones sensibles théoriques de manière expérimentale. Il est donc possible pour un attaquant connaissant le layout d'une bascule DFF 28nm bulk ou FDSOI de pouvoir injecter une faute de type bit set/reset en se positionnant avec un faisceau laser de 1µm sur la zone sensible correspondante.

IV.3.4. Résistance d'un circuit 28nm bulk et FDSOI face à l'injection laser

a) Seuils d'injection et de casse du circuit

Dans cette sous-section, on souhaite mesurer la résistance des technologies CMOS 28nm bulk et FDSOI en termes de faciliter pratique d'injection. Cette facilité se quantifie selon trois critères, le seuil d'injection de faute, le seuil de faute déterministe et le seuil de casse. Le seuil d'injection de faute correspond à l'énergie minimale permettant d'injecter une faute dans le circuit (ici une bascule). Le seuil de faute déterministe, correspond à l'énergie minimale permettant d'injecter la même faute, à la même position d'illumination, pour plusieurs campagnes d'injection espacées dans le temps. Finalement, l'énergie de casse correspond à l'énergie minimale permettant d'induire une faute permanente dans le circuit en une illumination. Les énergies données ici, sont à titre indicatif.

En effet, l'énergie donnée correspond à l'énergie fournie en commande de la source laser et ne correspond pas à l'énergie du faisceau qui traverse le silicium.

La figure IV-18 présente deux cartographies du motif DFF Matrix FDSOI pour une énergie d'injection de 0,4nJ. La distribution des bascules fautées est différente entre les deux cartographies. L'énergie injectée dans le motif n'est pas assez élevée pour garantir l'injection systématique d'une faute dans la bascule (seuil de faute déterministe).

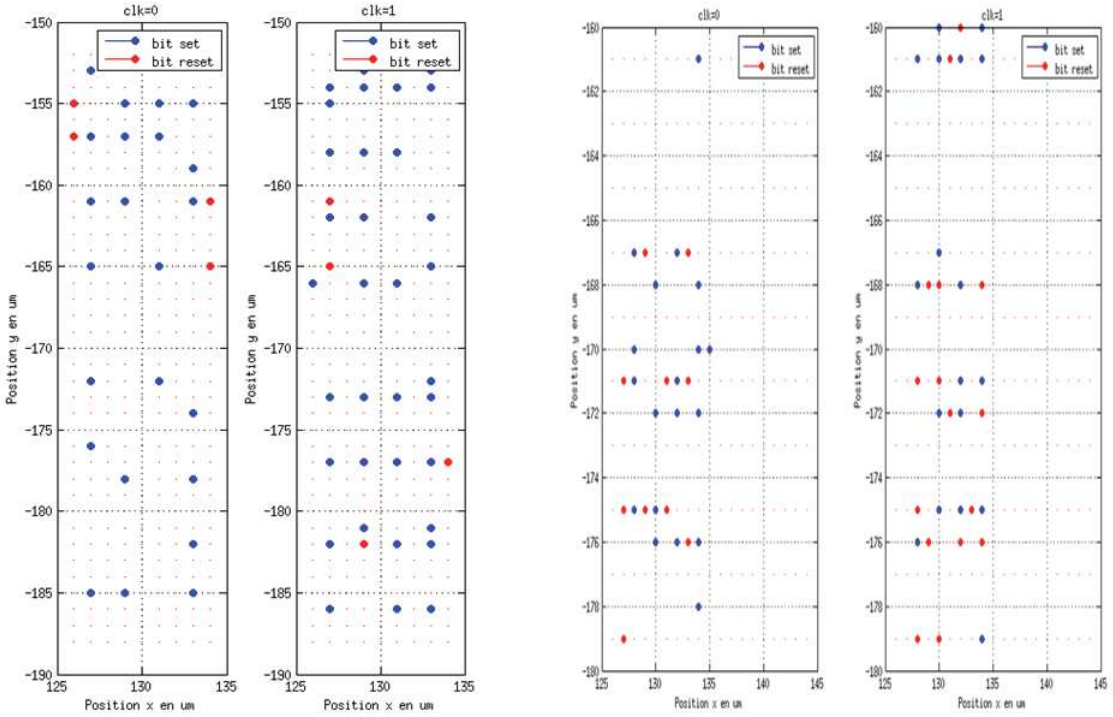


Figure IV-18: Cartographies du motif DFF Matrix FDSOI avec une énergie de 0,4nJ

Le seuil de casse pour le motif DFF Matrix bulk est de l'ordre de 1,2nJ, au-dessus de cette énergie lors de l'illumination, la bascule DFF a une grande probabilité de se casser de manière permanente. Pour le motif FDSOI, le seuil de casse de la bascule est 0,7nJ. Le seuil de casse du motif bulk est plus élevé que celui du motif FDSOI. La bascule FDSOI casse plus facilement que celle utilisant la technologie bulk.

La figure IV-19 résume schématiquement le positionnement des différents seuils pour le motif DFF Matrix bulk et FDSOI. Pour le FDSOI, la marge entre le seuil de faute et de casse est très proche contrairement au bulk. Cela signifie qu'il est plus difficile pour un attaquant d'injecter une faute sur un circuit FDSOI sans l'endommager de manière irréversible.

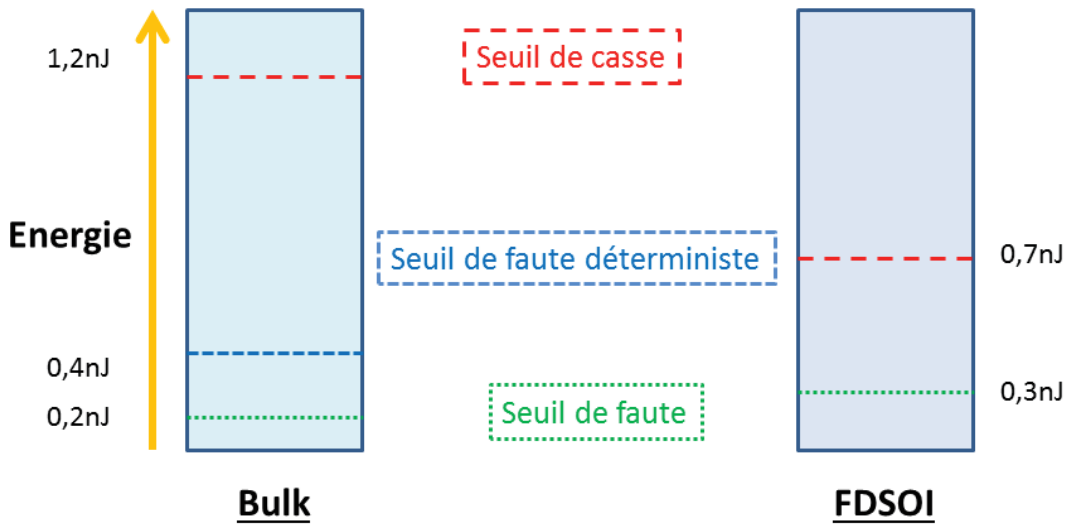


Figure IV-19: Vue schématique du positionnement relatif des seuils de fautes et de casse pour le motif bulk et FDSOI

Ces observations montrent que la technologie FDSOI semble plus résistante face à l'injection laser que la technologie bulk. D'une part car la différence entre le seuil de faute et de casse est plus faible que pour le bulk. Mais d'autre part, car les fautes injectées ne sont pas « déterministes ». Un autre avantage de la technologie FDSOI face à l'injection laser est le phénomène de « casse multi-tir », qui impose un temps entre chaque injection plus long, que pour un circuit bulk, afin de ne pas induire une « casse » dans le circuit FDSOI illuminé. Ce phénomène est décrit plus en détail dans la section suivante.

b) Casse multi-tir sur bascule DFF FDSOI

Observations

Un phénomène de « casse » a été observé lors des campagnes d'injections sur une bascule DFF. Cette casse de la bascule est survenue lors d'illuminations rapprochées sur la même position, quelques microsecondes de pause entre chaque tir, avec une énergie d'injection inférieure au seuil de casse (environ 3 ou 4 tirs successifs). La casse observée correspond à un collage, la valeur logique de la bascule est bloquée sur un état logique.

Cependant, le circuit récupère de cette casse après un temps long de repos, plusieurs dizaines d'heures, le phénomène de collage disparaît. De plus, la casse observée n'est pas à priori destructrice. En effet, après récupération le circuit ne présente plus aucune faute et retrouve une consommation normale. Cependant, cette récupération est limitée. En effet, après un certain nombre de récupération, le circuit ne récupère plus, entraînant alors une casse définitive du circuit.

Piste d'explication du phénomène de casse multi-tir

Une explication de ce phénomène peut être le piégeage de charges dans l'oxyde de box et/ou de la grille du transistor FDSOI. Les charges générées par illumination à l'interface entre le silicium et l'oxyde (SiO_2) vont se déplacer dans l'oxyde où elles vont être piégées. La figure IV-20 présente le mécanisme par lequel les charges du silicium sont capturées par l'oxyde [48]. Le bandgap du silicium est de l'ordre de 1.1eV et celui de l'oxyde de 9eV. Dans [48], des mesures ont permis de quantifier l'offset entre la bande de valence du silicium et de conduction de l'oxyde, dette différence est de 4,5eV. L'illumination expérimentale est réalisée avec une source infrarouge de 800nm. Pour une telle longueur d'onde, chaque photon transporte une énergie de 1,52eV. Cette énergie n'est pas suffisante pour faire passer un électron de la bande de valence du silicium à la bande de conduction de l'oxyde, afin que celui-ci soit piégé.

Ce passage de la bande de valence du silicium à la bande de conduction de l'oxyde fait intervenir le mécanisme d'absorption multi-photon. En effet, à forte intensité lumineuse, la probabilité qu'un électron absorbe plusieurs photons simultanément existe. Cette probabilité est proportionnelle à l'intensité lumineuse.

Il faut ici 3 photons afin de faire passer les électrons de la bande de valence à la bande de conduction de l'oxyde. Si l'intensité lumineuse est assez importante, on peut aussi observer le passage des trous de la bande de conduction du silicium vers la bande de valence de l'oxyde. Cette transition nécessite l'absorption de 4 photons.

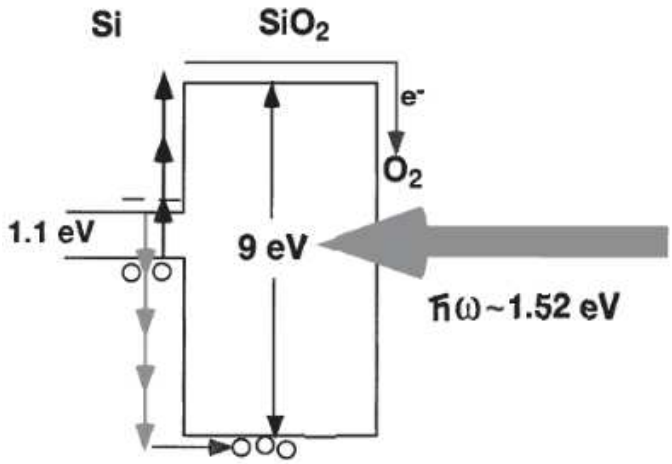


Figure IV-20: Mécanisme de passage des porteurs de charges du silicium vers l'oxyde [48]

Les charges piégées dans l'oxyde vont affecter la conduction du canal [49]. Les charges piégés dans l'oxyde vont créer une zone de charge espace au niveau de l'interface entre l'oxyde et le silicium. Cela a pour effet de modifier les caractéristiques de conduction du transistor. On observe un

déplacement de la tension de seuil Vt vers la gauche sur la caractéristique $I_D(V_G)$. Par exemple dans [49], cette mesure est effectuée pour plusieurs illuminations d'un transistor NMOS et PMOS par rayon X. Le résultat est donné par la figure IV-21. Pour cette mesure, durant l'illumination $V_G = 1V$ et $V_D = V_S = 0V$. L'épaisseur d'oxyde sous la grille est de 120nm. Pour la mesure de la caractéristique, le transistor est ensuite polarisé avec $V_D = 25mV$ et $V_S = 0V$. Par analogie, on peut considérer dans le cas du PMOS, que le box correspond à l'oxyde de grille et que le Nwell correspond à la grille du transistor.

Le déplacement de la caractéristique de conductance du transistor PMOS entraîne une conduction du transistor même lorsque la grille du transistor PMOS FDSOI est à l'état haut. Cela a pour effet d'induire une faute dans le circuit.

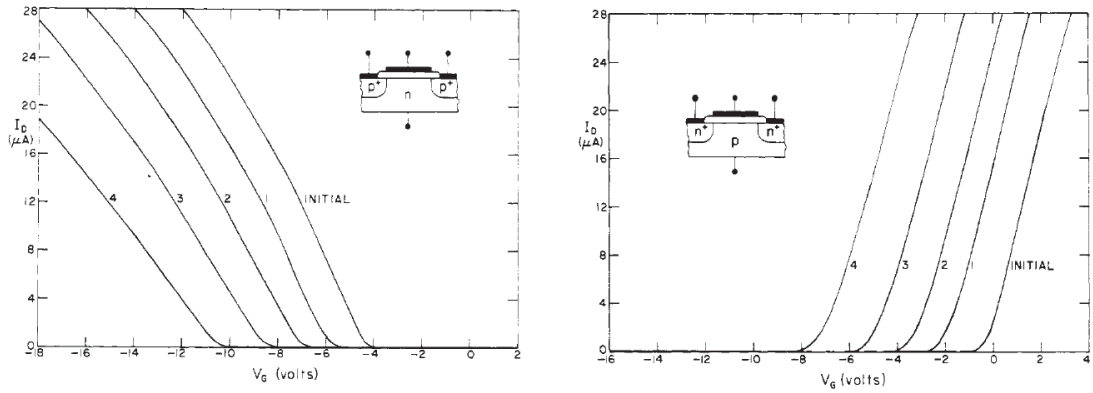


Figure IV-21: Caractéristiques de conductance des transistors MOS avant et après plusieurs expositions successives à des rayons X.

L'effet du piégeage de charges peut être annulé en effectuant un recuit.

Conclusion

L'injection sur un circuit complexe (chaîne de bascules D flip-flop) en technologie bulk et FDSOI a permis de corroborer les résultats obtenus sur les transistors dans le Chapitre III. Les campagnes laser montrent qu'il est possible d'injecter des fautes dans un chaîne de bascules DFF en bulk et FDSOI. Il est cependant plus difficile d'injecter des fautes sur le motif (chaîne de bascules DFF) FDSOI que sur le motif bulk avec les mêmes conditions expérimentales (taux de couverture plus faible). L'étude du nombre de bascules fautées par une seule injection, a confirmé l'effet de la box isolante présente dans les transistors de la technologie FDSOI sur la taille de la zone de sensibilité à l'injection laser. La zone de sensibilité de la technologie FDSOI est plus réduite que celle de la technologie bulk.

Des injections plus précises, ont ensuite été réalisées sur une bascule DFF pour la technologie 28nm bulk et FDSOI. L'expérience a montré que même pour des technologies fortement submicronique, il est possible d'induire une faute de type bit set ou bit reset dans la bascule avec un faisceau laser de 1µm de diamètre. Les zones de sensibilités expérimentales correspondent aux zones obtenues théoriquement. Les zones sensibles correspondantes à ces fautes étant distinctes, il est possible pour l'attaquant de choisir le type de faute qu'il induit dans la bascule.

Même si l'attaquant peut choisir le type de faute qu'il souhaite injecter dans la bascule, Il faut que celui-ci ait connaissance de la position des bascules dans le circuit. De plus, la marge entre le seuil d'injection de faute et de casse est faible. Cette marge est encore plus faible pour la technologie FDSOI. Cette difficulté à injecter des fautes dans les circuits FDSOI est encore augmentée grâce au phénomène de casse multi-tir. On peut donc en conclure que la technologie FDSOI semble être une alternative prometteuse au bulk pour implanter des circuits résistant à l'injection laser.

Conclusion générale

L'objectif de cette thèse était d'étudier l'effet de l'injection laser pour des nœuds technologiques avancés et des structures de type FDSOI ainsi que de réaliser la modélisation de cet effet. La modélisation du phénomène d'illumination laser sur des nouvelles technologies, a pour but de pouvoir simuler électriquement la résistance des circuits face à cette menace.

Dans un premier temps, un état de l'art de l'injection laser a été dressé. Cet état de l'art a permis de présenter les mécanismes mis en jeu lors de l'illumination laser, tel que l'effet photoélectrique, ainsi que le principe d'attaque en faute par injection laser et les travaux de modélisation électrique de l'injection sur des nœuds technologiques plus anciens (90nm).

Ensuite, une étude de la réalisation pratique d'une attaque par injection laser a été présentée. Cette étude présente la méthode et les caractéristiques de l'injection par la face avant et par la face arrière. La mise en pratique d'une attaque sur un ASIC AES de ces deux types d'injections, a permis de mettre en évidence le fait que l'attaquant doit choisir le type d'injection en fonction du circuit et du matériel qu'il possède. En effet, même avec un faisceau large, il est possible d'injecter des fautes de type mono bit et mono-octet, type de fautes intéressantes pour la réalisation d'une attaque, dans le circuit par la face avant. Cet effet est dû à la présence des lignes de métaux au-dessus du circuit qui agissent comme un filtre réduisant la dimension spatiale du faisceau illuminant le circuit. On peut cependant s'interroger sur l'effet de l'avancée des nœuds technologiques, pour lesquels les niveaux de lignes de métaux ont tendance à être plus nombreux, sur ce gain de précision spatiale.

Des injections laser ont été menées sur des transistors CMOS 28nm bulk et FDSOI, afin de mettre à jour ou d'établir un modèle électrique permettant de représenter de manière fidèle l'effet de l'illumination laser. Le modèle électrique pour la technologie bulk 28nm a été mis à jour à partir du modèle établi pour la technologie 90nm en mesurant l'effet des paramètres d'injections expérimentaux sur des jonctions PN. L'illumination de chaque jonction PN constituant le transistor est modélisée par une source de courant débitant un courant dépendant des paramètres expérimentaux d'injection (position du faisceau, durée d'illumination, etc.). Les transistors de la technologie 28nm FDSOI ayant une structure différente, due notamment à l'isolation du canal de conduction, un nouveau modèle a été établi. Pour cela, l'effet de l'illumination du transistor complet a été pris en compte. De plus, du fait de la structure du transistor PMOS FDSOI, un nouvel effet de la modélisation a dû être pris en compte. En effet, bien que les charges générées dans cette jonction ne

sont pas collectées par le transistor, l'illumination de la jonction Nwell/Psub du transistor PMOS FDSOI a pour effet de modifier l'amplitude du courant collecté dans le canal ainsi que de modifier les caractéristiques dynamiques du transistor. La comparaison de ces deux technologies (28nm bulk et 28nm FDSOI) face à l'injection laser sur des motifs de type transistors, montre que la technologie FDSOI est plus résistante que la technologie bulk (courant induit collecté plus faible, zone de sensibilité plus réduite) bien que l'injection de faute reste possible pour ces deux technologies.

Afin de corroborer les résultats obtenus sur la comparaison des technologies 28nm bulk et FDSOI face à l'injection (sur des transistors simples), des injections laser ont été réalisés sur un registre à décalage composé de 64 bascules D Flip-Flop. Ces campagnes d'injection ont montré qu'il est possible d'injecter des fautes dans le registre bulk et FDSOI, et que l'injection est moins contraignante pour le registre bulk que le registre FDSOI (taux de couverture plus élevé, zone de sensibilité plus large).

Finalement, afin de tester la résistance des technologies 28m bulk et FDSOI face à l'attaque en faute, des campagnes d'injection ont été menées sur une bascule D Flip-Flop. La bascule DFF représente une cible privilégiée pour l'attaque en faute, car elle permet de modifier directement la valeur du bit stockée, en ayant moins de contraintes temporelles qu'une injection sur la logique du circuit. L'expérience montre qu'il est possible pour les deux technologies d'injecter dans le registre des fautes de type bit set ou bit reset, qui représente le modèle de faute le plus exigeant lors d'une attaque. Chacune des zones sensibles permettant d'induire une faute de type bit set ou bit reset sont distinctes et correspondent aux zones sensibles théoriques. Cependant même si l'attaquant peut choisir le type de faute qu'il souhaite injecter, l'injection n'en demeure pas moins difficile du fait que la marge entre le seuil d'injection de faute et de casse est faible, d'autant plus dans le cas de la technologie FDSOI. De plus, Le seuil d'injection de faute de la technologie FDSOI est supérieur à celui de la technologie bulk. Ainsi cette différence facilite la détection d'une attaque par des capteurs, en effet l'attaquant pour injecter une faute doit utiliser une énergie plus grande. Cette technologie présente aussi un phénomène de casse lors d'injections répétés sur la même zone, ce qui a pour effet de rendre l'injection sur des circuits implantés en technologie 28nm FDSOI plus difficile sans endommager l'intégrité du circuit. Cette thèse n'a pas étudié le modèle de casse des transistors 28nm FDSOI. Il serait intéressant d'étudier l'effet destructif du faisceau laser sur les transistors FDSOI afin de comprendre quelle partie de cette structure est plus sensible et pourquoi. Cette étude peut servir à rendre le transistor FDSOI plus sensible à la casse dû à l'injection, et donc de renforcer son potentiel de résistance face à l'attaque en faute par injection laser pour l'implantation de circuits sécurisés.

Dans le futur, des injections dynamiques sur les bascules pourront être effectuées afin de se rapprocher des conditions expérimentales de la mise en pratique d'une attaque par injection laser et de comparer ces résultats avec ceux obtenus en injection statique. Une étude plus approfondie pourra être faite sur le phénomène de « casse » multi-tir afin de comprendre les mécanismes d'un tel phénomène.

Annexe A

Dans cette annexe A, nous présentons les résultats et modélisations effectuées sur une jonction PN de type Nwell/Psub. Comme pour la jonction N+/Psub, modélisée dans la section 0, nous modélisons l'effet des paramètres suivants sur l'amplitude maximale du courant induit :

- La puissance de tir du laser : I_p
- La dépendance spatiale (x,y) : I_x
- La durée d'illumination : I_t
- La focalisation (z) : I_z

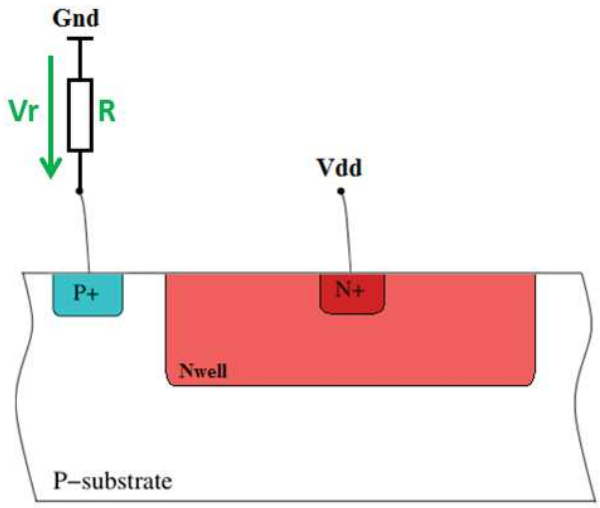


Figure A-0-1: Schéma de principe du montage de mesures expérimentales du courant induit dans la jonction PN (type Nwell/Psub)

La jonction utilisée pour les mesures expérimentales est une jonction PN Nwell/Psub de 4µm*4µm. Cette jonction se compose d'un caisson N dans un substrat P. La figure A-1 présente le layout de cette jonction.

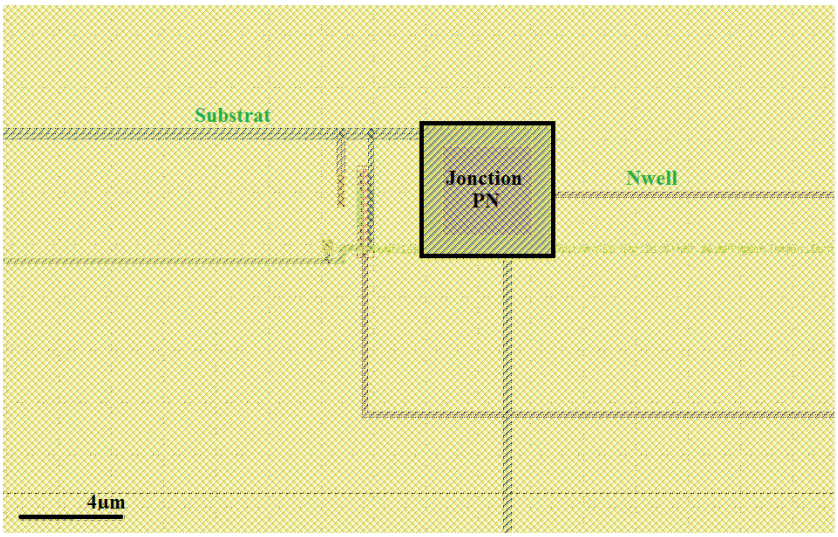


Figure A-0-2: Layout de la jonction PN Nwell/Psub utilisée pour les mesures expérimentales

A.1. Effet de la puissance de tir sur l'amplitude du courant induit dans la jonction PN Nwell/Psub

Dans cette section, on modélise l'effet de la puissance d'injection sur l'amplitude maximale du courant induit dans la jonction PN. La figure A-3 présente les résultats expérimentaux (points) ainsi que la modélisation de ce phénomène (courbe). On remarque que l'amplitude maximale du courant collecté augmente avec un terme quadratique.

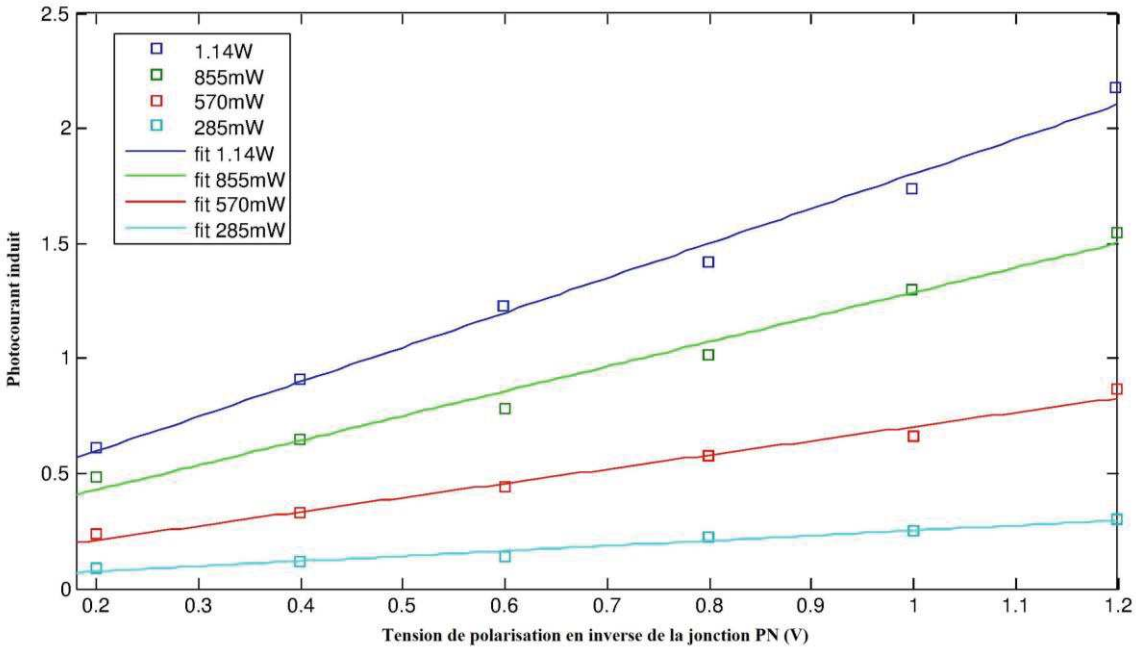


Figure A-0-3: Effet de la puissance d'illumination sur l'amplitude maximale du courant induit dans une jonction Nwell/Psub

L'équation (A.1) présente l'expression mathématique de la modélisation de l'effet de la puissance sur l'amplitude du courant induit dans le canal.

$$I_{ph} = [(a * P^2 + b * P + c) * V + d * P + e] * S \qquad (A.1)$$

Les coefficients de modélisation sont donnés par la table 24:

Table 24: Coefficients de modélisation de l'effet de la puissance sur l'amplitude du courant induit dans la jonction Nwell/Psub

Coefficient	Valeur	Unité
a	7,543	$W^{-2}\mu m^{-2}$
b	83,81	$W^{-1}\mu m^{-2}$
c	−10,91	μm^{-2}
d	20,23	$W^{-1}\mu m^{-2}$
e	-4,608	μm^{-2}

Pour ce modèle, on a un coefficient de détermination de R^2=99 ,3%.

A.2 Effet de la distance du faisceau à la jonction Nwell/Psub

On s'intéresse ici, à l'effet de la distance horizontale du faisceau par rapport à l'aplomb de la jonction PN Nwell/Psub. La figure A-4 présente la modélisation (courbe) et les résultats expérimentaux (points) de l'effet de ce paramètre expérimental (distance) sur l'amplitude du courant collecté par la jonction Nwell/Psub. La courbe de modélisation de ce phénomène a un profil gaussien

(double gaussienne) centré en x=0µm, centre de la jonction PN. La largeur à mi-hauteur est de 10µm. C'est-à-dire que lorsque le faisceau est éloigné de 10µm alors l'amplitude maximale du courant collecté est diminuée de moitié.

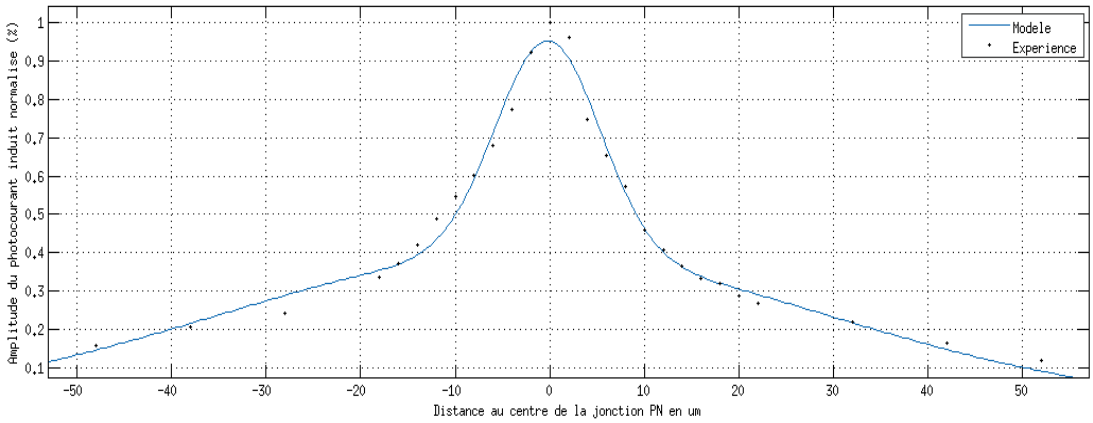


Figure A-0-4: Amplitude normalisée du photocourant induit en fonction de la distance du faisceau à la jonction PN

L'équation (A.2) donne l'expression du modèle utilisé.

$$I_x = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{x-b_i}{c_i}\right)^2\right) \qquad (A.2)$$

La table 25 donne les valeurs des coefficients de modélisation.

Table 25: Coefficients de modélisation de l'effet de la distance horizontale sur le photocourant collecté par la jonction PN

a_0	-0,3847	a_1	1,129
b_0	-3,766 µm	b_1	-0,928 µm
c_0	3,402 µm	c_1	6,93 µm

Pour cette modélisation, on a un coefficient de détermination de R^2=98,5%.

A.3 Effet de la durée d'illumination sur l'amplitude maximale du courant collecté par la jonction Nwell/Psub

L'effet de la durée d'illumination sur l'amplitude maximale du courant collecté est présenté par la figure A-5. Celle-ci donne les mesures expérimentales ainsi que la modélisation de cet effet choisie. Le profil de modélisation est une courbe croissante qui atteint sa valeur maximale au bout de 2µs.

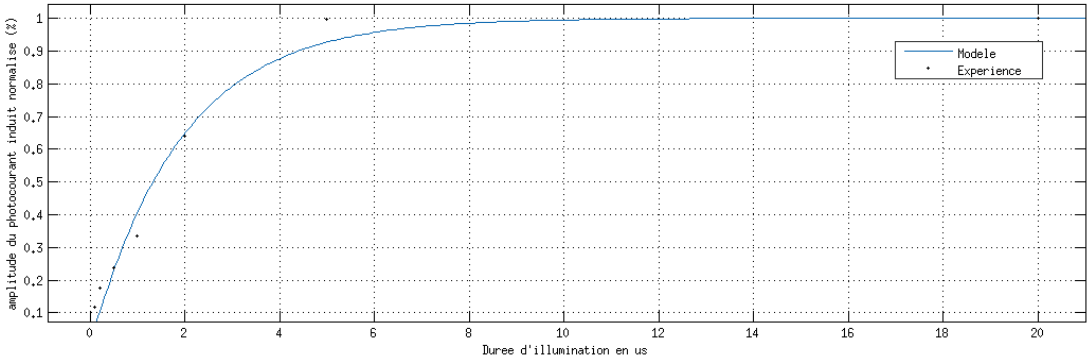


Figure A-0-5: Mesures (points) et modélisation (courbe) de l'effet de la durée d'illumination sur l'amplitude du photocourant induit

L'équation (A.3) donne l'expression de la modélisation de l'effet de la durée d'illumination sur l'amplitude maximale du photocourant induit.

$$I_D = 1 - exp\left(\frac{-D}{a}\right) \qquad (A.3)$$

Ou a=1,911 µs et le coefficient de détermination R^2=97,6%.

A.4 Effet de la focalisation sur l'amplitude du courant collecté par la jonction PN

Dans ce paragraphe, on mesure l'influence de la focalisation sur l'amplitude maximale du courant induit dans la jonction. Les mesures expérimentales ainsi que la modélisation de cette influence sont présentées dans la figure A-6. La distance à mi-hauteur pour cette expérimentation est de 200µm.

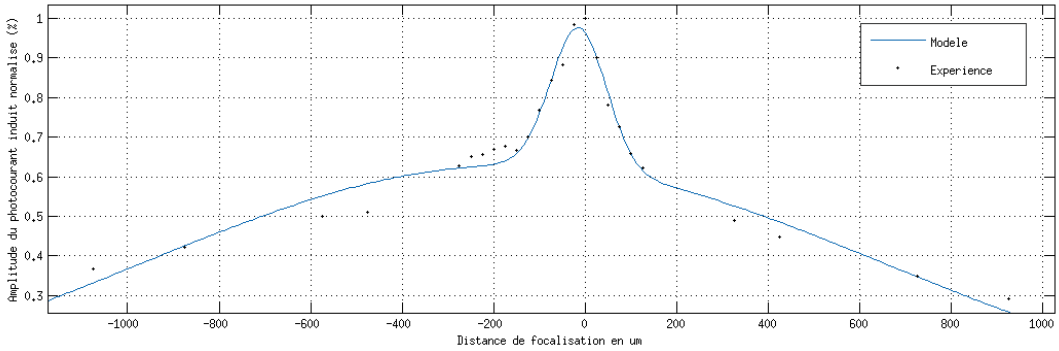


Figure A-0-6 Effet de la distance focale sur l'amplitude du courant induit: expérience (point) et modèle (courbe)

L'expression mathématique du modèle est donnée par l'équation (A.4).

$$I_z = \sum_{i=0}^{1} a_i * exp\left(-\left(\frac{z-b_i}{c_i}\right)^2\right) \qquad (A.4)$$

Avec les coefficients de modélisation donnés par la table 26 suivante :

Table 26: Coefficients de modélisation de l'effet de la focalisation sur l'amplitude maximale du courant induit dans la jonction Nwell/Psub

$\boldsymbol{a_0}$	0,7259	$\boldsymbol{a_1}$	0,2965
$\boldsymbol{b_0}$	16,77 µm	$\boldsymbol{b_1}$	13,16 µm
$\boldsymbol{c_0}$	35,25 µm	$\boldsymbol{c_1}$	220,3 µm

Bibliographie

[1] J. DAEMEN et V. RIJMEN, «Advanced encryption standard (AES)(FIPS197),» Katholijke Universiteit Leuven/ESAT, 2001.

[2] R. Rivest, A. Shamir et L. Adleman, «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,» *Communications of the ACM,* pp. 120-126, 1978.

[3] E. Barker et A. Roginsky, «Transistions: Recommendation for transitioning the Use of Cryptographic Algorithms and Key Lengths,» *NIST Special Pblication 800-131A,* 2015.

[4] S. Skorobogatov, *Semi-invasive attacks - A new approach to hardware security analysis,* University of Cambridge: Technical Report, 2005.

[5] P. Kocher, J. Jaffe et B. Jun, «Differential power analysis,» *Advances in Cryptology — CRYPTO' 99,* vol. 1666, p. 789–789, 1999.

[6] A. Barenghi, G. Bertoni, L. Breveglieri, M. Pellicioli et G. Pelosi, «Low voltage fault attacks to aes,» *HOST,* p. 7–12, 2010.

[7] H. HANDSCHUH, P. PAILLIER et J. STERN, «Probing attacks on tamper resistant devices,» *Cryptographic Hardware and Embedded Systems (CHES),* 1999.

[8] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic et J. Seifert, «Simple photonic emission analysis of aes,» *Cryptographic Hardware and Embedded Systems,* vol. 7428, p. 41–57, 2012.

[9] S. Skorobogatov et R. Anderson, «Optical fault induction attacks,» *Cryptographic Hardware and Embedded Systems,* vol. 2523, p. 31–48, 2002.

[10] F. Koeune et F.-X. Standaert, «A tutorial on physical security and side-channel attacks,» *Foundations of Security Analysis and Design III,* vol. 3655, p. 78–108, 2005.

[11] K. Gandolfi, C. Mourtel et F. Olivier, «Electromagnetic analysis : concrete result,» *Cryptographic Hardware and Embedded Systems,* vol. 2162, p. 251–261, 2001.

[12] A. Dehbaoui, J.-M. Dutertre, B. Robisson et A. Tria, «Electromagnetic transient faults injection on a hardware and software implementation of aes,» *Fault Diagnosis and Tolerance in Cryptography,* 2012.

[13] M. Agoyan, J.-M. Dutertre, D. Naccache, B. Robisson et A. Tria, «When clocks fail : On critical paths and clock faults,» *Smart Card Research and Advanced Application,* p. 182–193, 2010.

[14]A.-P. Mirbaha, Etude de la vulnérabilité des circuits cryptographiques: l'injection de fautes par laser, Ecole Nationale Supérieure des Mines de Saint-Etienne, 2011.

[15]V. Pouget, «Test et analyse par faisceau laser : plateforme et applications,» *Journée thématique GDR SOC-SIP,* 2007.

[16]Polytech'Lille, «Propriétés des matériaux III-IV,» [En ligne]. Available: http://www.polytech-lille.fr/cours-transistor-effet-champ/hemt/Hemtc1b1.htm. [Accès le décembre 2015].

[17]D. Kovalev, G. Polisski, M. Ben-Chorin, J. Diener et F. Koch, The temperature dependence of the absorption coefficient of porous silicon, American Institue of Physics, 1996.

[18]C. Roscian, J.-M. Dutertre et A. Tria, «Frontside laser injection on cryptosystems - Application to the AES' last round,» *HOST,* pp. 119-124, 2013.

[19]C. Roscian, A. Sarafianos, J.-M. Dutertre et A. Tria, «Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells,» *Fault Diagnosis and Tolerance in Cryptography (FDTC),* pp. 89-98, 2013.

[20]S. Buchner, F. Miller, V. Pouget et D. McMorrow, «Pulsed-Laser Testing for Single-Event Effects Investigations,» *Nuclear Science, IEEE,* vol. 60, n° %13, pp. 1852-1875, 2013.

[21]E. Haseloff, «Latch-up, ESD and other Phenomena,» Texas Instruments, 2000.

[22]A. Amerasekera, S. Ramaswamy, M.-C. Chang et C. Duvvury, «Modeling MOS snapback and parasitic bipolar action for circuit-level ESD and high current simulations,» *Reliability Physics Symposium,* pp. 318-326, 1996.

[23]H. Eilhard, «Latch-Up,ESD, and other phenomena,» Texas Instruments, 2000.

[24]H. Nguyen et Y. Yagil, «A systematic approach to SER estimation and solutions,» *Reliability Physics Symposium Proceedings,* pp. 60-70, 2003.

[25]M. Otto, «Fault attacks and countermeasures,» Diss. University of Paderborn, 2005.

[26]S.-M. Yen et M. Joye, «Checking Before Output May Not Be Enough Against Fault-Based Cryptanalysis,» *IEEE Transaction on Computers,* pp. 967-970, 2000.

[27]F. Lu, «Simulation de fautes par laser dans les circuits cryptographiques,» Université de Montpellier II , 2014.

[28]A. Sarafianos, «Injection de fautes par impulsion laser dans des circuits sécurisés,» Ecole Nationale Supérieure des Mines de Saint-Etienne, 2013.

[29]S. De Castro, J.-M. Dutertre, B. Rouzeyre, G. Di Natale et M.-L. Flottes, «Front-side vs backside laser injection: a comparative study,» 2015.

[30]C. Tarnovsky, «How to reverse-engineer TV smart card,» wired, juin 2008. [En ligne]. [Accès le 2015].

[31]C. Giraud, «DFA on AES,» *AES,* pp. 27-41, 2003.

[32]E. Biham et A. Shamir, «Differential fault analysis of secret key cryptosystems,» *CRYPTO,* vol.

1233, pp. 37-51, 1997.

[33]C. Chien-Ning et Y. Sung-Ming, «Differential fault Analysis on AES key schedule and some countermeasures,» *ACISP,* vol. 2727, 2003.

[34]G. Piret et J.-J. Quisquater, « A differential fault attack technique against spn structures, with application to the AES,» *CHES,* vol. LNCS 2779, pp. 77-88, 2003.

[35]H. Choukri et H. Tunstall, «Round reduction using faults,» *FDTC,* pp. 13-24, 2005.

[36]J. Park, S. Moon, D. Cho, Y. Kang et H. JaeCheol, «Differential Fault analysis for round-reduced AES by fault injection,» *ETRI,* 2011.

[37]P. Dusart, G. Letourneux et O. Vivolo, «Differential fault analysis on AES,» *ACNS,* pp. 293-306, 2003.

[38]B. Robisson et P. Manet, «Differential behavioral analysis,» *CHES,* pp. 413-426, 2007.

[39]C. H. Kim et J.-J. Quisquater, «New Differential Fault Analysis on AES key schedule: Two faults are enough,» *CARDIS,* vol. 5189, pp. 48-60, 2008.

[40]S. Ali, D. Mukhopadhyay et T. Michael, «Differential fault analysis of AES using a single multiple-byte fault».

[41]S. S. Ali et D. Mukhopadhyay, «a differential fault analysis on AES key schedule using single fault,» *FDTC,* pp. 35-42, 2011.

[42]D. Martinez, R. Bond et M. Vai, High performance embedded computing handbook: a systems perspective, CRC press, 2008.

[43]B. Jovanovic et M. Jevtic, «Static and dynamic power consumption of arithmetic circuits in modern technologies».

[44]S. De Castro, J.-M. Dutertre, G. Di Natale, M.-L. Flottes et B. Rouzeyre, «Sensitivity to fault laser injection: a comparison between 28nm bulk and FD-SOI technology,» *TRUDEVICE,* 2015.

[45]H. Park, *Second harmonic generation in Si/SiO2 systems,* Vanderbilt University: PhD thesis, 2010.

[46]E. Snow, A. Grove et D. Fitzgerald, «Effetcs of ionizing radiation on oxydized silicon surfaces and planar devices,» *proceedings of the IEEE,* vol. 55, n° %117, pp. 1168-1185, 2005.

[47]M. Baze et S. Buchner, «Attenuation of single event induced pulses in CMOS combinational logic,» *Nuclear Science, IEEE Transactions,* vol. 44, n° %16, pp. 2217,2223, Dec 1997.

[48]P. Schmid, «Optical absorption in heavily doped silicon,» *Phys. Rev. B,* vol. 23, n° %110, pp. 5531--5536, 1981.

[49]T. F. Wrobel, «On Heavy Ion Induced Hard-Errors in Dielectric Structures,» *Nuclear Science, IEEE Transactions on,* vol. 34, n° %16, pp. 1262-1268, 1987.

[50]J. Singh, Electronic and Optoelectronic Properties of semiconductor Structures, Cambridge University Press, 2003.

[51]M. Green et M. Keevers, «Optical properties of intrinsic silicon at 300 K,» *Progress in Photovoltaics: Research and Applications,* vol. 3, pp. 189-192, 1995.

[52]J. Lu, O. Dunkelman, N. Keller et e. al., «New impossible differential attacks on AES,» *INDOCRYPt,* pp. 279-293, 2008.

[53]A. Garnache, *Lasers: Conception, Propriétés Physiques et Applications,* Montpellier, 2012.

[54]S. Forget, «Optique des Lasers et faisceaux gaussiens,» Septembre 2007. [En ligne]. Available: http://www.optique-ingenieur.org/fr/cours/OPI_fr_M01_C03/co/Contenu_08.html. [Accès le octobre 2015].

[55]A. Li, «Interaction of Nanopaticles with Radiation - Excitation of photoluminescence,» juin 2014. [En ligne]. Available: https://ned.ipac.caltech.edu/level5/Sept03/Li/Li4.html. [Accès le octobre 2015].

[56]E. Petersen, «Single Event analysis and prediction,» *IEEE NSREC Short Course,* 1997.

[57]J.-M. Dutertre, S. De Castro, A. Sarafianos, N. Boher, B. Rouzeyre, M. Lisart, J. Damiens, P. Candelier, M.-L. Flottes et G. Di Natale, «Laser attacks on integrated circuits: from CMOS to FD-SOI,» *Design & Technology of Integrated Systems in Nanoscale Era (DTIS),* pp. 1-6, 2014.

[58]S. De Castro, J.-M. Dutertre, G. Di Natale, M.-L. Flottes et B. Rouzeyre, «figure of merits of 28nm Si technologies for implementing laser attack resistant security dedicated circuits,» *Computer Society Annual Symposium on VLSI (ISVLSI),* 2015.