Injection de fautes par impulsion laser dans des circuits sécurisés

Alexandre Sarafianos

NNT : *2013 EMSE 0703*

THÈSE

présentée par

Alexandre SARAFIANOS

pour obtenir le grade de
Docteur de l'École Nationale Supérieure des Mines de Saint-Étienne

Spécialité : La Spécialité

INJECTION DE FAUTES PAR IMPULSION LASER DANS LES CIRCUITS SÉCURISÉS

soutenue à Gardanne, le 17 septembre 2013

Membres du jury

Président :	Bruno ROUZEYRE	Professeur, LIRMM Montpellier
Rapporteurs :	Régis LEVEUGLE	Professeur, TIMA, Grenoble
	Jean-Michel PORTAL	Professeur, IM2MP, Marseille
Examinateur(s) :	Jean-Max DUTERTRE	Co-encadrant, EMSE, Gardanne
	Pascal FOUILLAT	Professeur, IMS, Bordeaux
	Mathieu LISART	Co-encadrant, STMicroelectronics, Rousset
	Vincent POUGET	Chargé de recherches, IES, Montpellier
	Bruno ROUZEYRE	Professeur, LIRMM Montpellier
Directeur(s) de thèse :	Assia TRIA	Directeur, CEA, Gardanne
Invité(s) éventuel(s):	Guillaume HUBERT	Chercheur, ONERA, Toulouse

Spécialités doctorales :	Responsables :
SCIENCES ET GENIE DES MATERIAUX	K. Wolski Directeur de recherche
MECANIQUE ET INGENIERIE	S. Drapier, professeur
GENIE DES PROCEDES	F. Gruy, Maître de recherche
SCIENCES DE LA TERRE	B. Guy, Directeur de recherche
SCIENCES ET GENIE DE L'ENVIRONNEMENT	D. Graillot, Directeur de recherche
MATHEMATIQUES APPLIQUEES	O. Roustant, Maître-assistant
INFORMATIQUE	O. Boissier, Professeur
IMAGE, VISION, SIGNAL	JC. Pinoli, Professeur
GENIE INDUSTRIEL	A. Dolgui, Professeur
MICROELECTRONIQUE	

EMSE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

AVRIL	Stéphane	PR2	Mécanique et ingénierie	CIS
BATTON-HUBERT	Mireille	PR2	Sciences et génie de l'environnement	FAYOL
BENABEN	Patrick	PR1	Sciences et génie des matériaux	CMP
BERNACHE-ASSOLLANT	Didier	PR0	Génie des Procédés	CIS
BIGOT	Jean Pierre	MR(DR2)	Génie des Procédés	SPIN
BILAL	Essaid	DR	Sciences de la Terre	SPIN
BOISSIER	Olivier	PR1	Informatique	FAYOL
BORBELY	Andras	MR(DR2)	Sciences et génie de l'environnement	SMS
BOUCHER	Xavier	PR2	Génie Industriel	FAYOL
BRODHAG	Christian	DR	Sciences et génie de l'environnement	FAYOL
BURLAT	Patrick	PR2	Génie Industriel	FAYOL
COURNIL	Michel	PR0	Génie des Procédés	DIR
DARRIEULAT	Michel	IGM	Sciences et génie des matériaux	SMS
DAUZERE-PERES	Stéphane	PR1	Génie Industriel	CMP
DEBAYLE	Johan	CR	Image Vision Signal	CIS
DELAFOSSE	David	PR1	Sciences et génie des matériaux	SMS
DESRAYAUD	Christophe	PR2	Mécanique et ingénierie	SMS
DOLGUI	Alexandre	PR0	Génie Industriel	FAYOL
DRAPIER	Sylvain	PR1	Mécanique et ingénierie	SMS
FEILLET	Dominique	PR2	Génie Industriel	CMP
FOREST	Bernard	PR1	Sciences et génie des matériaux	CIS
FORMISYN	Pascal	PR0	Sciences et génie de l'environnement	DIR
FRACZKIEWICZ	Anna	DR	Sciences et génie des matériaux	SMS
GARCIA	Daniel	MR(DR2)	Génie des Procédés	SPIN
GERINGER	Jean	MA(MDC)	Sciences et génie des matériaux	CIS
GIRARDOT	Jean-jacques	MR(DR2)	Informatique	FAYOL
GOEURIOT	Dominique	DR	Sciences et génie des matériaux	SMS
GRAILLOT	Didier	DR	Sciences et génie de l'environnement	SPIN
GROSSEAU	Philippe	DR	Génie des Procédés	SPIN
GRUY	Frédéric	PR1	Génie des Procédés	SPIN
GUY	Bernard	DR	Sciences de la Terre	SPIN
GUYONNET	René	DR	Génie des Procédés	SPIN
HAN	Woo-Suck	CR	Mécanique et ingénierie	SMS
HERRI	Jean Michel	PR1	Génie des Procédés	SPIN
INAL	Karim	PR2	Microélectronique	CMP
KERMOUCHE	Guillaume	PR2	Mécanique et Ingénierie	SMS
KLOCKER	Helmut	DR	Sciences et génie des matériaux	SMS
LAFOREST	Valérie	MR(DR2)	Sciences et génie de l'environnement	FAYOL
LERICHE	Rodolphe	CR	Mécanique et ingénierie	FAYOL
LI	Jean Michel		Microélectronique	CMP
MALLIARAS	Georges	PR1	Microélectronique	CMP
MOLIMARD	Jérôme	PR2	Mécanique et ingénierie	CIS
MONTHEILLET	Franck	DR	Sciences et génie des matériaux	SMS
PERIER-CAMBY	Laurent	PR2	Génie des Procédés	DFG
PIJOLAT	Christophe	PR0	Génie des Procédés	SPIN
PIJOLAT	Michèle	PR1	Génie des Procédés	SPIN
PINOLI	Jean Charles	PR0	Image Vision Signal	CIS
POURCHEZ	Jérémy	CR	Génie des Procédés	CIS
ROUSTANT	Olivier	MA(MDC)		FAYOL
STOLARZ	Jacques	CR	Sciences et génie des matériaux	SMS
SZAFNICKI	Konrad	MR(DR2)	Sciences et génie de l'environnement	CMP
TRIA	Assia		Microélectronique	CMP
VALDIVIESO	François	MA(MDC)	Sciences et génie des matériaux	SMS
VIRICELLE	Jean Paul	MR(DR2)	Génie des Procédés	SPIN
WOLSKI	Krzysztof	DR	Sciences et génie des matériaux	SMS
XIE	Xiaolan	PR1	Informatique	CIS

ENISE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

BERGHEAU	Jean-Michel	PU	Mécanique et Ingénierie	ENISE
BERTRAND	Philippe	MCF	Génie des procédés	ENISE
DUBUJET	Philippe	PU	Mécanique et Ingénierie	ENISE
FORTUNIER	Roland	PR	Sciences et Génie des matériaux	ENISE
GUSSAROV	Andrey	Enseignant contractuel	Génie des procédés	ENISE
HAMDI	Hedi	MCF	Mécanique et Ingénierie	ENISE
LYONNET	Patrick	PU	Mécanique et Ingénierie	ENISE
RECH	Joël	MCF	Mécanique et Ingénierie	ENISE
SMUROV	Igor	PU	Mécanique et Ingénierie	ENISE
TOSCANO	Rosario	MCF	Mécanique et Ingénierie	ENISE
ZAHOUANI	Hassan	PU	Mécanique et Ingénierie	ENISE

Mise à jour : 07/04/2013

PR 0	Professeur classe exceptionnelle
PR 1	Professeur 1ère classe
PR 2	Professeur 2ème classe
PU	Professeur des Universités
MA (MDC)	Maître assistant
DR	Directeur de recherche

Ing.	Ingénieur
MCF	Maître de conférences
MR (DR2)	Maître de recherche
CR	Chargé de recherche
EC	Enseignant-chercheur
IGM	Ingénieur général des mines

SMS	Sciences des Matériaux et des Structures
SPIN	Sciences des Processus Industriels et Naturels
FAYOL	Institut Henri Fayol
CMP	Centre de Microélectronique de Provence
CIS	Centre Ingénierie et Santé

REMERCIEMENTS

Une thèse de doctorat, qui plus est une thèse CIFRE, ne peut se réaliser sans un travail collaboratif fort que ce soit aussi bien du côté académique que du côté industriel. Dans cette optique, je tiens à remercier de nombreuses personnes.

Je souhaiterais en premier lieu remercier ma directrice de thèse, Madame Assia TRIA, du CEA LETI, qui m'a encadré durant les trois années de ma thèse. Je lui suis également extrêmement reconnaissant de l'intérêt qu'elle a porté afin que ma thèse se déroule dans les meilleures conditions.

Je remercie également Monsieur Jean-Max DUTERTRE, mon co-encadrant académique, au centre de Microélectronique de Provence - Georges Charpak, pour tout le travail d'encadrement scientifique et pour les différentes corrections de rédaction qu'il a pu effectuer tout au long de ma thèse. Je lui suis également extrêmement reconnaissant pour toutes les qualités humaines dont il a fait preuve avec moi durant ces trois années de thèse.

Du côté industriel où s'est déroulée ma thèse de nombreuses personnes sont également à remercier.

Je remercie en premier lieu mon co-encadrant industriel Monsieur Mathieu LISART, ingénieur sécurité « hardware » à STMicroelectronics Rousset, pour les orientations et l'encadrement qu'il a su donner à ma thèse.

Je remercie également Madame Sylvie WUIDART de m'avoir accueilli dans son équipe. Le travail aux côtés des membres de son équipe a été extrêmement enrichissant pour moi tant sur le plan professionnel qu'humain.

Je remercie également très chaleureusement Christophe LAURENCIN, de m'avoir intégré dans sa nouvelle équipe, et d'avoir supervisé la fin de ma thèse.

Entre autres, je souhaiterais remercier chaleureusement tous mes collègues du département Secure Microcontroller Development de STMicroelectronics Rousset avec qui

j’ai pu travailler. Un remerciement tout particulier à Fabrice MARINET, Pierre-Yvan LIARDET, Marc BENVENISTE, Laurent DI RUSSO pour tous les judicieux conseils qu’ils m’ont donnés tout au long de ma thèse. Une mention spéciale de mes remerciements revient à Bruno NICOLAS, pour toute l’aide qu’il a pu m’apporter dans le pilotage des différents équipements laser.

Un sincère remerciement à Julien, Fabrice, Thomas, Karim, Nicolas, du département Secure Microcontroller pour la bonne ambiance qu’ils out su créer sur le lieu de travail.

J’adresse de chaleureux remerciements à Valérie SERRADEIL d’avoir accepté qu’un des membres de son équipe de simulation TCAD m’épaule tout au long de ma thèse. C’est dans ce cadre, que je souhaite adresser un grand remerciement à Olivier GAGLIANO pour tout l’excellent travail de simulation TCAD qu’il a su effectuer.

Ma reconnaissance s’adresse également à Monsieur Jean-Luc OGIER directeur du laboratoire de caractérisation électrique du RCCAL (Rousset Central Characterization and Analyze Laboratory) pour m’avoir donné la possibilité d’utiliser ses équipements. Mes remerciements dans cette équipe s’adressent également à Lionel, Olivier, Guillaume, Laurin.

Je souhaiterais également remercier Roxane LLIDO, pour tout le travail que l’on a pu effectuer ensemble et qui a donné lieu à différentes publications scientifiques.

De plus, je souhaiterais remercier ma famille, sans qui je n’aurais jamais pu mener à bien cette thèse. Un grand merci s’adresse donc tout d’abord à mes parents qui ont su m’épauler et m’encadrer tout au long mes études, un grand merci à ma mère pour tout ce qu’elle m’apporte encore au quotidien. Dans ce cadre, je souhaite également remercier mes grands-parents pour toute l’attention bienveillante qu’ils ont su me porter depuis tout petit. Je souhaiterai ainsi, remercier tout particulièrement mon grand-père pour la relation, et l’échange scientifique que l’on a pu avoir depuis mon enfance.

Je remercie enfin, Justine, avec qui je partage ma vie depuis déjà de nombreuses années, pour m’avoir soutenu tout au long de mes études, sans qui la réalisation de cette thèse aurait était beaucoup plus difficile.

A la mémoire de mon père

Table des matières

Liste des figures

Chapitre I. État de l'art de l'injection de fautes par impulsions lasers dans des circuits sécurisés.

Chapitre II. Modélisation électrique de l'injection de fautes par impulsions lasers dans des circuits sécurisés.

Chapitre III. Contre-mesures aux injections de fautes par impulsion laser.

Liste des Tableaux

Chapitre I. Etat de l'art de l'injection de fautes par impulsions lasers dans des circuits sécurisés.

Chapitre II. Modélisation électrique de l'injection de fautes par impulsions lasers dans des circuits sécurisés.

Chapitre III. Contre-mesures aux injections de fautes par impulsion laser.

Introduction générale

Les premières traces connues d'échanges de communications chiffrées se voulant secrètes, datent du XVI^{ème} siècle avant J.C. Elles ont été retrouvées en Irak au XIX^{ème} siècle. Il s'agit d'une tablette d'argile gravée par un potier qui désirait cacher son procédé de fabrication en modifiant de façon astucieuse l'orthographe de sa recette.

Plus tard, les Grecs, entre le X^{ème} et le VII^{ème} siècle avant J.C. semblent avoir développé une technique de chiffrement en enroulant une bandelette de cuir sur un bâton de diamètre bien précis, celui-ci portait le nom de scytale ou bâton de Plutarque. La bandelette enroulée en hélice autour de la scytale recevait un message écrit suivant la génératrice du bâton. Une fois déroulé, le message était ainsi envoyé à son destinataire, il n'avait plus aucun sens pour un lecteur non averti. La bandelette-message une fois repositionnée en hélice sur un bâton de même diamètre que celui de l'expéditeur, restituait le message d'origine.

Il faut attendre deux siècles avant J.C. pour voir apparaître de « vrais » systèmes de codages plus performants basés sur un chiffrement par substitution de lettres. Le plus connu parmi les systèmes antiques porte le nom de code César (I^{er} siècle avant J.C.). Cette méthode, utilisée par l'armée romaine, consistait à décaler les lettres de l'alphabet d'un nombre de lettres *n* pour rédiger le message codé. Sa robustesse restait néanmoins faible.

Bien plus tard, lors de la Première Guerre mondiale, le déchiffrement des messages des unités belligérantes a pris un essor considérable, au point de devenir stratégiquement vital sur le sort des batailles. Les services français possédaient une grande maîtrise en ce domaine, ce qui leur permit de déchiffrer dès le début des hostilités les messages ennemis, leur procurant ainsi un certain avantage.

Bien évidemment, par la suite, les moyens de communication se développant, la cryptologie fut encore plus sollicitée pour jouer un rôle très important durant la Seconde Guerre mondiale. Les exploits des alliés en la matière auraient permis selon les spécialistes

d'écourter le conflit mondial de plusieurs mois, poussant même le premier ministre britannique W. Churchill à citer ce domaine comme l'un des facteurs clefs de la victoire.

Du côté allemand, une invention remarquable, la machine *Enigma* leur conféra une avance aux lourdes conséquences pour les alliés. L'histoire de cette machine débute dans les années qui suivirent la première Guerre mondiale. Un ingénieur allemand, du nom d'Arthur Scherbius, avait mis au point une machine à crypter très sophistiquée qu'il baptisa *Enigma*. Elle prétendait sécuriser les échanges bancaires, mais n'eut pas de succès. Par contre les états-majors allemands s'intéressèrent à elle, l'adoptèrent secrètement en la perfectionnant pour leurs propres besoins. Si nous nous arrêtons sur cette machine, c'est qu'elle préfigure l'arrivée des systèmes hautement technologiques que nous connaissons de nos jours.

Sur cette machine électromécanique, le chiffrement se fait sur des suites intriquées de lettres de façon très complexes. Son fonctionnement met en œuvre trois rotors qui combinaient les lettres de l'alphabet suivant un processus préalablement déterminé où des systèmes mécaniques se croisaient avec des circuits électriques pour encoder les messages.

Concurremment à cette période, le service de renseignements polonais fut, semble-t-il, le premier à réellement « casser » le chiffre allemand dans les années 1930. Ils travaillèrent ensuite en collaboration avec le service cryptographique du 2^{e} bureau français, dirigé par le colonel Gustave Bertrand, aidé dans cette tâche par les informations fournies par la « taupe » française Hans Thilo Schmidt (« Asche » pour les services français). Par la suite, une collaboration s'instaure avec les services britanniques, qui rassemblèrent leurs meilleurs spécialistes en cryptologie dont le mathématicien Alan Turing prit la tête. Ce corps des services secrets britanniques avait son cantonnement à Bletchley Park. Par ces travaux en ce domaine, Allan Turing fut de ce fait l'un des pères fondateurs de ce qui deviendra l'informatique.

La Kriegsmarine utilisait une *Enigma* adaptée à ses besoins, elle était réputée inviolable. Les sous-marins *U-boot* détenaient un de ces modèles. La capture d'un de ces bâtiments, le 9 mai 1941, permit aux alliés, d'étudier dans le plus grand secret l'architecture de cette machine et ainsi déchiffrer les messages de l'état-major allemand. L'équipe de Bletchley Park baptisa tout son système de décryptage « la Bombe », en clin d'œil à la destruction des messages de l'ennemi. A partir des messages radio reçus par les Britanniques, leurs spécialistes réglaient en conséquence « la Bombe » et les rendaient exploitables après seulement une demi-heure environ, ce qui rendait la réactivité des contre-

attaques Alliers rapidement opérationnel. Trois à quatre mille messages étaient ainsi déchiffrés chaque jour par les neuf mille personnes travaillant à Bletchley Park.

De nos jours, la sécurité de l'information est devenue une contrainte stratégique décisive dans presque tous les domaines. La sécurité de l'information, dans l'ère actuelle du tout numérique, est réalisée grâce au développement de nouvelles générations de systèmes microélectroniques destinés à traiter, stocker ou transférer des informations sensibles chiffrées ou non (concernant les données bancaires, l'identité, la santé, la biométrie, les communications, etc.). Elles siègent au niveau des circuits intégrés, aussi doit-elle être introduite lors de la conception pour assurer une sécurité maximale. Elle doit être contrôlée dès sa fabrication pour confirmer son efficacité. Sachant toutefois, que le ratio coût/sécurité doit respecter des contraintes économiques fortes.

Aujourd'hui, l'une des techniques d'attaques consiste en l'injection de fautes, à l'aide d'un faisceau laser. Ce qui conduit, par utilisations de méthodes semblables, à évaluer la sensibilité d'un circuit à une erreur induite par un tel faisceau en agissant sur les différents matériaux du composant. Cette attaque, bien maîtrisée, permet d'évaluer le niveau de sécurité de différents circuits à base de semi-conducteurs. Dans ce contexte, il est donc vital de bien comprendre les phénomènes physiques mis en jeu lorsqu'une puce de silicium est soumise à un tel faisceau. Cette compréhension fine des effets physiques doit permettre de modéliser et de simuler l'injection de fautes par faisceau laser. Ces simulations peuvent servir à tester la robustesse de différents blocs constituant un circuit intégré sécurisé. Elles peuvent également permettre aux développeurs de circuits, de concevoir certaines contre-mesures afin d'augmenter la robustesse de leurs produits. Ainsi de nouvelles parades aux attaques par faisceau laser pourront être mises en place pour accroître la sécurité des informations sensibles.

Dans ce manuscrit, le premier chapitre abordera, l'état de l'art de l'injection de fautes par impulsion laser dans les circuits sécurisés, pour appréhender les différentes techniques connues à ce jour. Dans ce chapitre, une présentation générale d'une carte à puce et tout d'abord faite. Un état de l'art des différentes attaques matérielles est également présentés dont font parties les attaques par injection de fautes par faisceau laser. Une explication des phénomènes physiques mis en jeu lorsque le silicium est éclairé par une onde lumineuse

laser est également développée. Ensuite, un état de l'art des modélisations de l'illumination laser sur le silicium et des différentes contre-mesures est présenté.

Le deuxième chapitre de ce travail, concernera les mesures et à la modélisation électrique de l'interaction laser-silicium en partant de l'élément semi-conducteur le plus simple, la jonction PN, pour aller jusqu'à des éléments CMOS plus complexes comme par exemple une cellule SRAM. Les modèles développés dans ce chapitre permettent de tester la sensibilité des portes CMOS aux attaques laser.

Enfin dans le dernier chapitre seront présentées différentes contre-mesures possibles aux attaques par impulsion laser en les classant en deux grandes catégories qui sont l'amélioration de la robustesse des portes CMOS vis-à-vis des attaques laser et les détecteurs laser embarqués sur les microcontrôleurs sécurisés.

Chapitre I. ÉTAT DE l'ART DE l'INJECTION DE FAUTES PAR IMPULSION LASER

Introduction

Le premier chapitre de ce manuscrit est consacré à l'état de l'art de l'injection de fautes par impulsion laser dans les circuits sécurisés. La carte à puce servira de présentation générale pour examiner ce qu'est un circuit sécurisé. En détaillant notamment de manière succincte son fonctionnement. Dans la deuxième partie, un rapide état de l'art des différentes attaques matérielles connues à ce jour, sera présenté, en insistant tout particulièrement sur la technique d'attaque par injection de fautes. La troisième partie de ce premier chapitre est consacrée à la connaissance actuelle de l'onde lumineuse laser et de son effet lors de son interaction avec le silicium. L'état de l'art des phénomènes physiques connus à ce jour sera présenté dans cette partie, en particulier l'effet photoélectrique qui est à l'origine des fautes injectées par laser. De plus, un état de l'art de la modélisation et des contre-mesures aux attaques sera mis en évidence en fin de chapitre.

I.1 Présentation générale d'une carte à puce

Une carte à puce est une carte en matière plastique, de quelques centimètres de côté et moins d'un millimètre d'épaisseur, portant au moins un circuit intégré capable de contenir des informations plus ou moins sensibles. Le circuit intégré communément appelé « *puce* » contient généralement un microprocesseur capable de traiter ces informations. Les cartes à puce sont principalement utilisées comme moyens d'identification personnelle (carte d'identité, badge d'accès aux bâtiments, carte d'assurance maladie, carte SIM, etc.), de paiement (carte bancaire, porte-monnaie électronique, etc.) ou de preuve d'abonnement à des services prépayés (carte de téléphone, titre de transport, carte d'accès à la télévision payante, etc.). La lecture ou l'écriture des données sont réalisées par des équipements spécialisés. Certaines puces nécessitent un contact électrique, d'autres peuvent fonctionner à distance grâce à un mode de communication par ondes radio.

De manière générale, le circuit intégré d'une carte à puce est constitué d'un microprocesseur, d'une mémoire morte (ROM : Read Only Memory), d'une mémoire vive (RAM : Random Access Memory), et d'une mémoire non volatile de type EEPROM ou Flash.

Les composants pour cartes à puce suivent l'évolution générale de l'électronique décrite par la loi empirique de Moore, en termes de puissance des microprocesseurs et de capacité mémoire. Ceci se traduit par une miniaturisation rapide et une décroissance des coûts de fabrication.

I.1.1 Mécanisme d'encartage

La communication avec le circuit intégré de la carte à puce peut être réalisée de diverses manières. La première, qui paraît la plus simple et la plus « naturelle » se fait contact électrique. L'interface entre les contacts de la puce et ceux du lecteur est réalisée par un circuit imprimé doré très mince appelé micromodule mettant en contact les broches de la carte avec le lecteur. Il est divisé en 8 parties, chacune ayant un rôle précis permettant

l'échange des données entre la puce et le lecteur (cf. norme ISO7816). La puce est quant à elle située sous ces contacts (***Figure I. 1***).

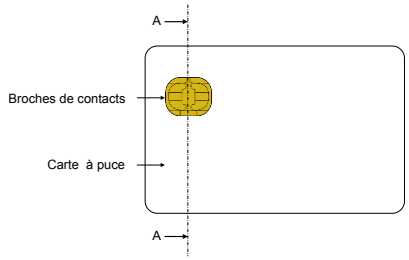


Figure I. 1. Vue de dessus d'une carte à puce avec plan de coupe A-A.

La ***Figure I. 2*** présente le plan de coupe défini à la figure précédente ***Figure I. 1***. Cette coupe permet de visualiser la position du circuit intégré sous le micromodule.

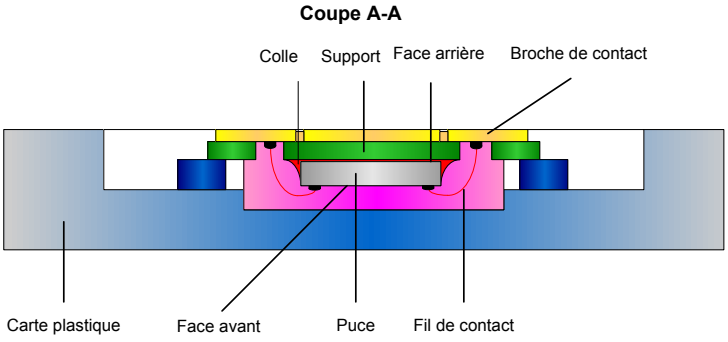


Figure I. 2. Vue en coupe d'une carte à puce.

La seconde manière de communiquer avec la puce peut se faire sans contact, par radiofréquence à courte ou moyenne portée, via une antenne interne dont les spires sont moulées dans l'épaisseur de la carte en plastique (voir ***Figure I. 3***).

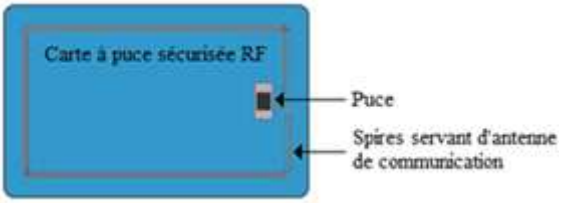


Figure I. 3. Schéma d'une carte à puce radio fréquence.

Le dernier mode de communication se fait par une combinaison des deux précédentes: on parle alors de cartes « combi » ou plus communément en anglais « dual interface » (cf. norme ISO14443).

I.1.2 Principe de fonctionnement

Actuellement, les cartes à puce comportent le plus souvent un microcontrôleur permettant des fonctions élaborées. Comme vu dans le paragraphe précédent, elles comportent principalement des zones mémoires (RAM, ROM, EEPROM, etc.), ainsi que plusieurs dispositifs de calcul destinés entre autres à la cryptographie. Ainsi, une carte à puce est constituée de manière générale par un microprocesseur, différentes mémoires plus d'éventuels coprocesseurs cryptographiques (ou autrement dit accélérateurs crypto-matériels). Une fois insérée dans un lecteur, elle se comporte en fait de la même manière qu'un micro-ordinateur, capable de traiter des informations.

Le microcontrôleur comporte au total 5 voies d'interface (cf. norme ISO7816) : 2 voies d'entrées qui sont les suivantes (CLK et RST), 2 voies d'alimentation et une voie d'entrée/sortie (I/O, Input/Output en anglais) afin de permettre l'échange de données). Le ***Tableau I. 1*** présente ces différentes voies.

Nom	**Fonction**	**Type de voie**
CLK	Signal d'horloge cadençant le circuit	Entrée
RST	Signal de remise à zéro du circuit	Entrée
VCC	Signal de potentiel positif alimentant le microcontrôleur	Alimentation
GND	Masse du circuit.	Alimentation
I/O	Signal d'entrée et sortie de communication avec la puce	Entrée/Sortie

Tableau I. 1. Signaux d'entrées/sorties d'un circuit de carte à puce.

I.1.3 Différentes composantes d'une carte à puce «intelligente»

La ***Figure I. 4*** présente les différents organes constitutifs d'une carte à puce dual interface.

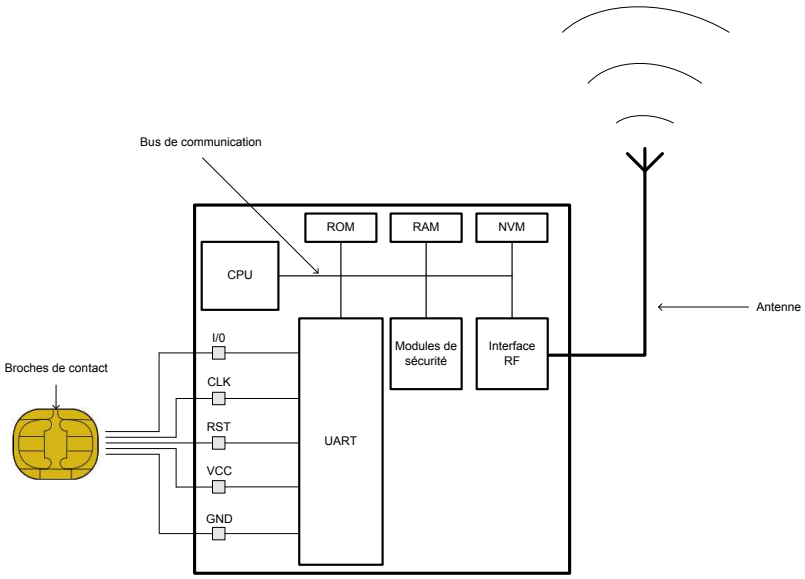


Figure I. 4. Schéma de principe du fonctionnement d'une carte à puce dual.

La carte à puce dite « intelligente » est constituée principalement d'un CPU, de mémoires et de modules de sécurité. L'UART (Universal Asynchronous Receiver-Transmitter), communique avec le monde extérieur de la carte à puce au travers des broches de contacts. De plus, dans le cas d'une carte à puce dual interface, un module d'interfaçage radiofréquence, communique sans contact avec l'extérieur par l'intermédiaire d'une antenne.

Avant d'être remise à la personne qui l'utilisera, une carte à puce est normalement « personnalisée » électriquement (par l'organisme émetteur) via un encodeur de cartes et un programme informatique (outil de personnalisation), afin d'inscrire dans la puce les informations nécessaires à son utilisation. Par exemple, dans une carte bancaire les références de l'utilisateur y sont inscrites, ou dans une carte d'un contrôle d'accès, les autorisations accordées au porteur de la carte y sont également stockées. La personnalisation physique de la carte consiste quant à elle à imprimer des données supplémentaires

apparentes (nom de la personne, photographie, etc.) sur le support plastique constituant la carte, par exemple à l'aide d'une imprimante à sublimation.

Les microcontrôleurs dits sécurisés contiennent donc des données sensibles. C'est pour cela que de nombreuses personnes tentent de les « attaquer » afin de récupérer leurs données confidentielles. Il peut s'agir également, d'industriels voulant caractériser la robustesse de leurs produits ou celles de leurs concurrents, mais aussi de « hackers » désirant s'approprier les données cachées ou privées. Par exemple, le clonage d'une carte bancaire peut permettre à une personne mal intentionnée d'acheter des biens sur le compte d'autrui, ou encore, le piratage d'une carte d'abonnement à une télévision payante pour utiliser gratuitement un chaîne de TV codée. La finalité des organismes mettant à disposition ces services (banques, télévision payante, transport en commun, etc.) est d'être sûr que la personne ayant souscrit ait accès au service correspondant. Ces organismes demandent des exigences de sécurité afin d'éviter le clonage ou la modification des droits sur la carte.

Le travail réalisé dans le cadre de cette thèse CIFRE a été effectué dans le département « Secure Microcontroller Developpement » de la société STMicroelectronics situé sur le site de Rousset (France). Ce département, conçoit et vend des puces dites sécurisées. Pour être vendus, ces produits doivent passer tout un processus de certification afin de valider que le niveau de sécurité des données qui vont être manipulées par le circuit est suffisant. Au cours de ces certifications, l'évaluateur teste la vulnérabilité du produit par le biais de diverses techniques d'attaques. L'une des attaques possibles utilisées par ces experts est celle pratiquée par faisceau laser. Une bonne compréhension des phénomènes physiques mis en jeu lorsqu'un laser attaque un microcontrôleur sécurisé est nécessaire pour mettre en œuvre des contre-mesures efficaces. Ces contre-mesures sont donc majeures en vue de la certification du produit. En effet, tout retard dans la certification d'un produit entraîne des pertes financières importantes puisqu'il ne pourra sortir sur le marché au moment opportun. C'est donc dans ce contexte, que cette thèse a été menée.

La partie suivante fait donc un état des lieux des différentes attaques matérielles connues à ce jour. Bien évidemment la liste n'est pas exhaustive, et de nombreuses attaques restent encore secrètes.

I.2 État de l'art sur les attaques matérielles

De nos jours, tous les réseaux hertziens ou téléphoniques de communication se croisent sur la planète, mettant à la disposition de tout un chacun de gigantesques quantités d'informations et des possibilités exceptionnelles de mise en relation. Seulement, si cette circulation profite à tous, il y a une dangereuse contrepartie payée par le fait que des données sensibles peuvent être piratées pour être utilisées frauduleusement. Aussi, toutes les données confidentielles doivent être sécurisées au maximum, sachant que tous les réseaux publics ou privés sont concernés.

Les transactions utilisant ces outils, sont multiples. Parmi ces derniers les cartes à puce sont souvent utilisées pour les échanges monétaires courants, contenant des données confidentielles qu'il est important de protéger au maximum.

Dans leur forme originelle, les cartes stockaient des renseignements anodins. De nos jours, elles incluent nombres de données concernant la personne ou l'organisme utilisateur. Les crypto-processeurs utilisent des algorithmes de chiffrement/déchiffrement pour atteindre un haut niveau de de sécurisation. Il est possible de citer les DES (Data Encryption Standard), triples DES, ou bien AES (Advanced Encryption Standard) pour la famille des algorithmes à clef secrète. Economiquement et stratégiquement les enjeux sont à l'évidence névralgiques. Aussi, ces cartes, vecteurs de communication et de reconnaissance personnalisée doivent être le plus inviolables possibles. Pour ce faire elles exploitent des algorithmes cryptologiques extrêmement sophistiqués, et cherchent à consolider structurellement le support par une construction très élaborée de ses composants, pour faire barrage le plus efficacement possible à toute intrusion éventuelle.

Une grande famille de techniques d'attaque concerne les attaques matérielles fondées sur des procédés d'analyse de cryptographie. Ces attaques décortiquent les phases successives du déroulement de l'algorithme lors de la mise en service de la puce, pour détecter par tous les moyens les informations clés inscrites dans ce support. Ainsi, par ce type d'approche, les spécificités inhérentes au circuit intégré sont observées.

Il est difficile d'être exhaustif pour décrire toutes les menaces actuellement déployées. Trois grandes classes peuvent toutefois être observées : la première concerne les méthodes invasives, la seconde les semi-invasives, et la dernière les non-invasives. Ces techniques sont toutes dangereuses, seulement la dernière utilisant des moyens de mise en œuvre relativement simples présente quant à elle une menace beaucoup plus forte compte tenu du coût financier relativement faible pour sa réalisation, facilitant ainsi, l'intervention d'un plus grand nombre de pirates. Les deux premiers procédés qui entraînent de plus grand frais d'investissement sont exploités majoritairement par des organismes dotés d'équipements sophistiqués quasi industriels.

Aussi, pour s'opposer à ces menaces, des contremesures doivent intervenir dès la conception et se poursuivre jusqu'à la fabrication finale du produit pour échafauder de solides contre-mesures à toute attaque éventuelle.

Les systèmes d'attaques qui perturbent les circuits intégrés se font en général par injections de fautes laser. Les moyens à mettre en œuvre pour contrecarrer ces attaques font l'objet du travail développé dans cette thèse.

I.2.1 Familles d'attaques matérielles

Les différentes attaques susceptibles d'intervenir sur des structures matérielles dans un système sécurisé sont abordées graduellement suivant le type d'intrusion. L'une d'elle concerne l'attaque invasive, qui peut être relativement complexe, risque de détruire définitivement les circuits.

I.2.1.1 Attaques invasives

En règle générale, une attaque invasive se déroule principalement en deux phases : la préparation des échantillons et l'attaque en elle-même. Ce sont des attaques menées en général par des experts, car elles requièrent un matériel spécifique de haute technologie.

I.2.1.1.1 Préparation des échantillons

Pour atteindre la puce, il faut la décapsuler en lui ôtant son emballage. Trois procédés sont en présence, soit par décomposition de l'entourage par action chimique, soit par abrasion mécanique ou soit par découpe laser. Ces actions sont menées pour extraire la puce de son support en plastique et parvenir à sa couche de passivation [Lee93] [Bec98].

Après les érosions faites par voies mécaniques, il convient de dégager la couche de passivation (d'oxyde de silicium SiO_2) en la décomposant à l'aide d'acides (nitrique et/ou fluoridrique suivant les cas). Il existe également des procédés par érosions manuelles utilisant des abrasifs courants pour aboutir au même résultat.

Des pratiques complémentaires, largement disponibles dans le domaine public, peuvent être mises en pratique. Il est possible de citer les attaques chimiques par gravure (type extraction électrochimique) ou l'érosion mécanique, voire les attaques par méthodes au plasma. Dans cette dernière méthode, des radicaux libres mis en présence avec la carte dans une chambre spéciale, produisent un gaz de type plasma qui réagit avec les couches de la puce à détruire (ce type d'intervention nécessite des moyens importants). Il est à noter que les procédés les plus élaborés permettent d'éliminer strates après strates les couches protectrices. Les résultats, dans ce cas de figure, n'en sont que meilleurs

Pour faciliter la mise en œuvre des attaques et plus particulièrement celles des attaques par sondage, l'échantillon ainsi préparé est collé et relié électriquement par des fils de « bonding » aux broches du support.

I.2.1.1.2 Attaques par reconstruction de layout

Une attaque est toujours possible sur le layout pour récupération de sa structure électrique. Cette opération est nommée rétro-ingénierie, (communément appelé reverse engineering en anglais). Elle va s'intéresser à étudier un ou des composants électroniques pour découvrir sa conception interne et ainsi s'approprier par simulation/émulation son fonctionnement. Dans le domaine plus particulier des cartes à puce, la reconstruction de layout permet d'une part d'analyser l'architecture de la puce afin d'en comprendre les mécanismes de sécurité et de pouvoir ainsi les contourner, et d'autre part de lire le contenu

d'une mémoire de type ROM pour récupérer les informations secrètes, si toutefois celles-ci ne sont pas cryptées.

Par les moyens vus précédemment, les couches sont retirées successivement, ensuite, plan après plan, des cartographies sont établies grâce à un examen par microscope électronique à balayage (SEM, ***Figure I. 5a***). Une reconstitution partielle ou totale du layout est ainsi possible. Il est alors également possible de reconstituer des netlists de simulation de type SPICE par exemple pour comprendre le fonctionnement du circuit.

Sur la même figure, en (***b***) est présentée la photographie obtenue par un tel microscope.

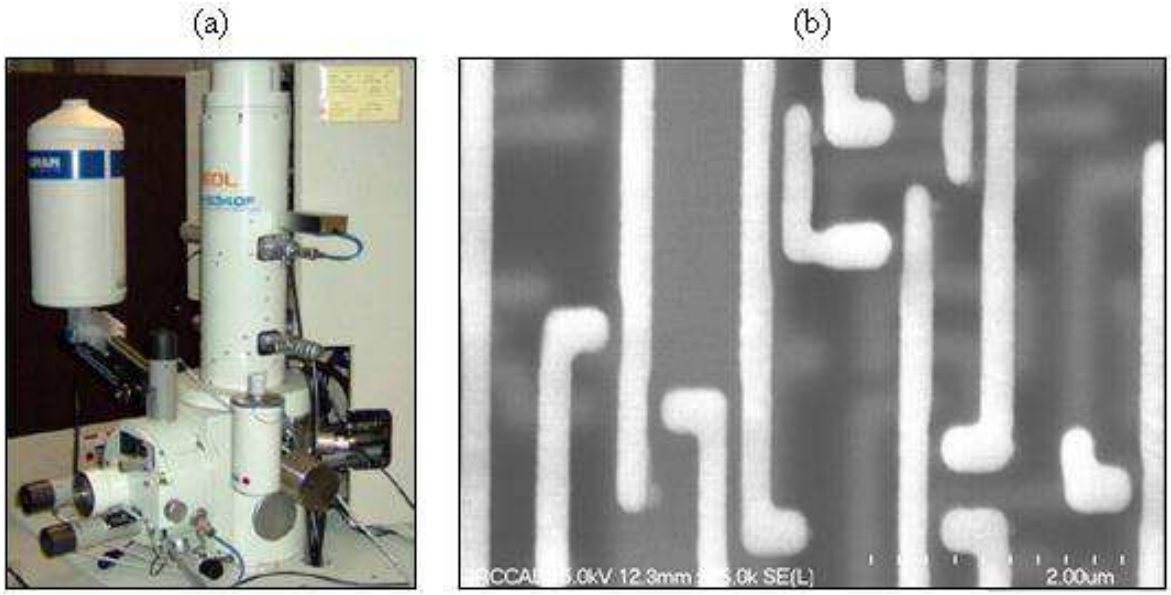


Figure I. 5. a) Microscope électronique à balayage JEOL JSM-6340F,
b) Une porte CMOS photographiée par un tel microscope.

I.2.1.2 Attaques par sondage sur un circuit actif

Une attaque par sondage ou « probing » en anglais, consiste à suivre l'activité électrique d'un circuit intégré fonctionnel tel qu'un crypto-processeur, lorsqu'il est alimenté, en implantant des sondes en contact avec les signaux internes du circuit cible.

Ce procédé réclame une plate-forme très performante. Sur la photographie de la ***Figure I. 6*** où le circuit étudié (1) est placé sur un support déplaçable par une table de translation XY (2). Les micromanipulateurs avec pointes (3) permettent à l'utilisateur de polariser ou de mesurer les signaux qu'ils souhaitent sur le circuit cible pour extraire des informations recherchées. Un système de grossissement optique (4) permet à l'utilisateur de placer correctement les pointes sur le circuit avec une précision micrométrique.

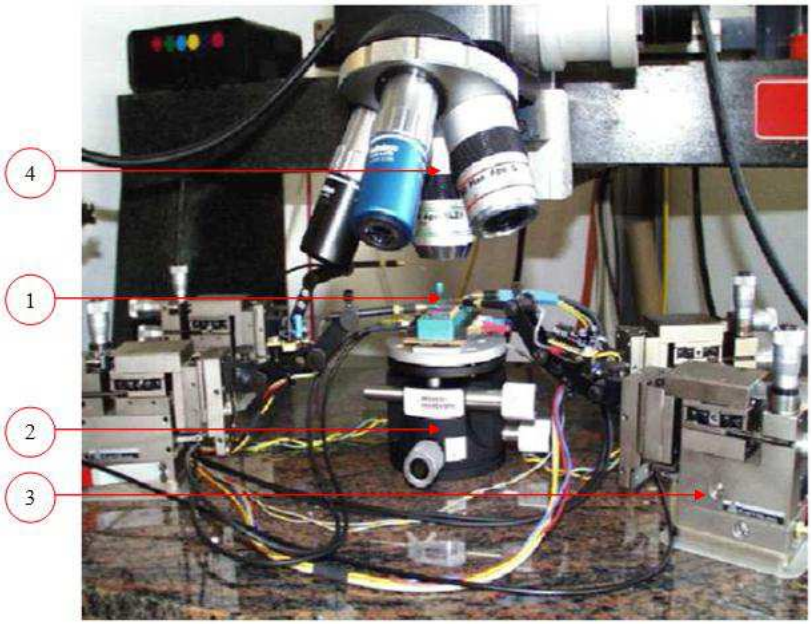


Figure I. 6. Plateforme d'attaque par sondage.

Ce matériel permet, non seulement de récupérer les informations transitant sur un bus de données, mais aussi d'imposer des valeurs logiques sur certains nœuds stratégiques du circuit. Avec un tel contrôle de l'environnement, l'attaquant peut être en mesure de déduire un grand nombre d'informations secrètes contenues dans un circuit sécurisé. Dans la pratique ce type d'attaque reste assez difficile à mettre en œuvre pour un intervenant puisqu'elle nécessite l'accès à du matériel de mesure sophistiqué et par conséquent onéreux.

Une des autres attaques possibles, consiste à utiliser un FIB (Focus Ion Beam), pour pouvoir faciliter l'attaque par sondage en déposant par exemple un plot conducteur qui permettra de recueillir ou de forcer un signal sur un point précis du circuit. Une autre utilisation du FIB peut consister à couper certaines pistes afin de désactiver des alarmes, ou

de recréer des interconnexions (par exemple : rétablir la connexion d'un fusible de sécurité qui aurait sauté lors d'une précédente attaque).

I.2.1.3 Attaques par canaux auxiliaires

Les attaques invasives nécessitent des accès directs à la puce, alors que les attaques utilisant des canaux auxiliaires n'ont pas de contacts directs avec celle-ci. Dans ce cas de figure, ce sont les syndromes physiques générés durant les calculs qui fournissent des renseignements sur les implémentations matérielles des algorithmes de chiffrement. Ces canaux auxiliaires peuvent concerner le temps de calcul, la consommation électrique du composant [Koc99], ses différents rayonnements (électromagnétique [Gan01], calorifique, sonore, etc.), mais également les résultats de calculs comportant des erreurs obtenus par injection de fautes pendant la mise en œuvre du procédé cryptographique, dans le cas d'attaques combinées qui associent une faute avec l'étude des canaux auxiliaires.

La ***Figure I. 7*** reprend les différents paramètres exploitables les canaux auxiliaires d'un circuit sécurisé.

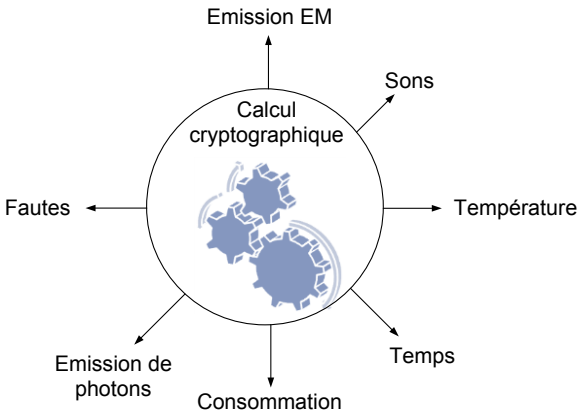


Figure I. 7. Exploitation des canaux auxiliaires d'un circuit sécurisé.

I.2.1.3.1 Attaques par analyse du temps de calcul

Ce type d'attaque exploite la corrélation entre les données manipulées et les temps de calcul, comptabilisé en mesurant le nombre de cycles d'horloge. Ceci afin d'extraire, lors

des opérations cryptographiques, les contenus confidentiels stockés dans la puce. Il est alors question d'attaque dite temporelle.

Sachant que les implémentations d'algorithmes cryptographiques peuvent avoir des temps de calcul très dépendants des données injectées en entrée, des mesures et des analyses très avancées effectuées lors de ces actions, permettent de retrouver les éléments constitutifs de la clé secrète dévoilant ainsi son contenu.

Il est possible de distinguer deux types d'analyses, la SPA (Simple Power Analysis) faisant une analyse simple et la DPA (Differential Power Analysis) utilisant des outils statistiques.

Déjà, en 1996, P. Kocher [Koc96], proposait d'utiliser ce principe de fonctionnement d'un canal temporel pour effectuer des lectures. Puis en 1998, J.F. Dhem démontra à partir d'une version améliorée qu'il était possible de faire la cryptanalyse matérielle d'une implémentation naïve de l'algorithme à clef publique RSA [Fip186].

Cet algorithme est maintenant connu pour n'être pas sécurisé, possédant des implémentations particulièrement vulnérables aux attaques temporelles.

De nos jours la majorité des circuits résistent à ces attaques temporelles, grâce aux contre-mesures déployées. Néanmoins, combinées avec d'autres types d'attaques, elles restent potentiellement dangereuses [Bon06].

I.2.1.3.2 Attaques par analyse de consommation

La consommation des produits sécurisés est corrélée aux données manipulées. Ceci permet donc de mener des attaques par analyse de consommation. Ces analyses associées à un traitement mathématique permettent d'extraire des informations secrètes comme par exemple des clés de chiffrement [Koc99].

La majorité des circuits sont construits en technologie CMOS. Une de leurs caractéristiques est la différence de signature de consommation lorsqu'un transistor commute de 0 vers 1 ou de 1 vers 0.

Par une analyse pointue sur le traitement du signal, les résultats relevés concernant la consommation permettent de retrouver l'intégralité ou une partie des données manipulées, lors des calculs de lecture de la clé de chiffrement.

Deux types d'attaques sont concernés par l'analyse de consommation. Le premier concerne l'analyse simple de la consommation SPA et l'autre l'analyse différentielle de la consommation DPA.

L'attaque par analyse simple de la consommation [Bih99] consiste à effectuer une analyse directe des profils en courant durant le déroulement des opérations cryptographiques et permet de récupérer des informations sur le type d'instruction en cours d'exécution sur une partie de la clé secrète dans le cas d'un algorithme de chiffrement asymétrique. La réussite de la SPA demande une connaissance du modèle de l'algorithme cryptographique utilisé et en particulier la manière dont il est implémenté.

L'analyse différentielle de la consommation (DPA) [Koc99] est une technique plus puissante que la SPA. Aussi l'attaque DPA ne nécessite pas une connaissance particulaire de l'implémentation de l'algorithme de chiffrement. Par contre, elle utilise des outils statistiques pour établir une correspondance entre les données et la consommation. Les plus petites variations de la consommation peuvent être ensuite exploitées pour extraire les données de la clé secrète. Actuellement, ces attaques sont prises très au sérieux et sont prises en considération par les concepteurs de circuits sécurisés. Leur simplicité est un véritable danger.

I.2.1.3.3 Analyse par rayonnement électromagnétique

Les attaques par le canal auxiliaire électromagnétique se subdivisent en l'analyse des émanations électromagnétiques indirectes (attaque non-invasive) et l'analyse des émanations électromagnétiques directes (attaque semi-invasive) [Arc03]. Les émissions électromagnétiques indirectes sont générées par différents couplages qu'ils soient électriques ou électromagnétiques dus à la proximité des composants. Des phénomènes de modulation d'amplitude, de phase et de fréquence des signaux porteurs apparaissent dans ce type d'émanation [Ord10]. La mesure de ces émanations électromagnétiques est facilement

réalisable boîtier ouvert, comme le montre la ***Figure I. 8***, par le biais d'une sonde électromagnétique.

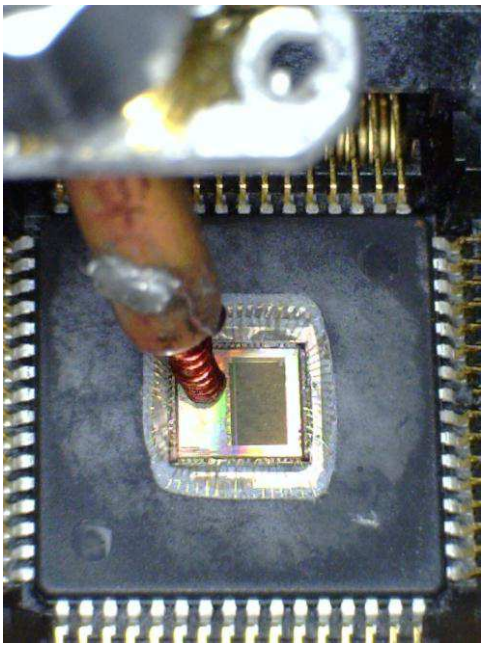


Figure I. 8. Capture des émissions électromagnétiques directes.

En fonction de la méthode d'analyse du rayonnement EM, il est possible de distinguer deux sous-catégories d'attaques: les attaques par analyse simple du rayonnement EM (SEMA) équivalente à la SPA et celles par analyse différentielle du rayonnement (DEMA) similaire à la DPA.

L'attaque par analyse simple du rayonnement EM consiste à recueillir directement les émissions électromagnétiques pendant que le circuit est en fonctionnement. De Mulder [Mul05], montre que cette attaque permet de récupérer des informations sur le type d'instruction en cours. Néanmoins, la réussite de la SEMA exige une connaissance de l'algorithme et de son implémentation. L'attaque par analyse différentielle du rayonnement EM est une version plus puissante de la SEMA. La réussite de l'attaque DEMA n'exige pas une connaissance détaillée de l'implémentation. Elle utilise des analyses statistiques intelligentes et établi la corrélation entre données traitées et rayonnement EM. Les méthodes statistiques identifient les plus petites variations du rayonnement. Ces faibles variations

peuvent être exploitées, toujours dans le but de retrouver les informations cachées [Qui01], [Gan01], [Ott04].

I.2.1.4 Attaques semi-invasives

En 2002, S. Skorobogatov et R. Anderson, [Sko02] ont publié un travail sur un type d'attaque semi-invasif. Ils montrent qu'une décapsulation (ou depackaging en anglais) du circuit est nécessaire pour atteindre les faces avant ou arrière sans nuire au bon fonctionnement de la puce. Les attaques semi-invasives ne nécessitent pas de contact physique avec la puce. Elles se situent entre les attaques invasives et les non-invasives.

Les circuits intégrés devenant de plus en plus complexes, les attaques invasives deviennent de plus en plus onéreuses. En conséquence, les attaques semi-invasives deviennent plus fréquentes puisqu'elles reviennent moins chères (à part certains équipements lasers). D'autre part, elles permettent d'obtenir des résultats de manière relativement rapide.

Les attaques par injections de fautes, par analyse, par émission électromagnétique, etc., font partie des attaques semi-invasives. Il est cependant possible de noter que sans décapsulation (et sans extraction de la couche de passivation de la puce), les attaques par analyse des champs électromagnétiques sont classées parmi les attaques non-invasives.

I.2.1.5 Attaques par injection de fautes

En 1997, Boneh, Demillo et Lipton dans [Bon97], ont montré qu'il était intentionnellement possible de générer des fautes dans un circuit en cours de fonctionnement par des attaques consistant à perturber les conditions nominales de fonctionnement du circuit cible. Ils montrèrent ainsi qu'il était possible d'exploiter des comportements anormaux d'un circuit. Par ce procédé, les données manipulées peuvent altérer ou corrompre les opérations cryptographiques, permettant ainsi de receuillir des informations secrètes [Bih97]. Dans l'ensemble, les fautes sont générées par des modifications anormales des paramètres externes du circuit. Il est possible de les retrouver

dans des variations intempestives des signaux d'horloge et d'alimentation, dans des variations de température, ou encore, dans une exposition du circuit à des faisceaux de lumière cohérente.

Ces fautes sont de différentes natures. Tout d'abord les fautes dites transitoires sont limitées dans le temps. Le circuit fonctionne à nouveau normalement après que la faute transitoire a disparu. Les fautes permanentes, comme leur nom l'indique, persistent jusqu'au redémarrage du circuit. Il ne retrouve sa fonctionnalité qu'au redémarrage suivant. L'un des exemples pour ce type de fautes est la mémoire SRAM, utilisée pour stocker une clef. Enfin, les fautes destructives ne permettront plus au circuit de fonctionner correctement, et cela de manière irrémédiable. Un transistor ou une interconnexion peuvent être détruits [Ott04]. Générer une faute permanente peut par exemple consister à figer le contenu d'une cellule mémoire à une valeur constante [Sko02]. A l'inverse, une faute transitoire induit le circuit en erreur durant une fraction temporelle bien délimitée correspondant à une séquence opérationnelle propre au circuit que l'on cherche à corrompre. Injecter une variation intempestive des signaux d'horloge et/ou d'alimentation constitue un moyen efficace pour générer des erreurs logiques transitoires.

L'injection de fautes à des fins de cryptanalyse matérielle nécessite la définition de modèles de fautes. En effet, ces modèles sont utilisés pour retrouver des informations secrètes et plus particulièrement des portions de la clef de chiffrement [Ott04].

Le principe d'une attaque par injection de fautes exploitant un modèle spécifique a été présenté pour la première fois en 1997 par Boneh, Demillo et Lipton [Bon97]. Les cibles principales de ces attaques concernées des circuits à clef publique et notamment ceux implémentant un RSA_CRT [FIP186] basé sur le théorème des restes chinois [Sti96]. D'autres travaux de recherche similaires ont également été publiés dans [Yen02], [Yen03]. Des travaux plus spécifiques ont porté sur les algorithmes à clef secrète comme mentionné dans les travaux de Biham et Shamir [Bih97]. Ces travaux, proposaient une attaque par injection de fautes dite DFA (Differential Fault Analysis). Ce type d'attaque consiste à analyser les différences entre deux ensembles de résultats de chiffrement dont le premier est correct et le deuxième incorrect et ce en utilisant le même message d'entrée et la même clef. Ils ont ainsi montré qu'il était possible de retrouver la clef secrète complète d'un algorithme

DES en analysant seulement entre 50 et 200 couples de textes chiffrés corrects et fautés. Une autre attaque consiste à s'infiltrer dans un algorithme de chiffrement AES, l'une d'elle [Pir03], est représentative de cette attaque dite DFA.

Les attaques par injection de fautes sont d'une efficacité remarquable. Elles représentent une énorme menace pour la sécurité des circuits sécurisés. Néanmoins, pour que ces attaques réussissent, elles réclament des compétences en microélectronique ainsi qu'une connaissance approfondie de la structure interne du circuit.

Pour conclure sur les attaques matérielles, dans l'état actuel de nos connaissances, il est important de savoir que l'état de l'art sur les différentes attaques présentées précédemment n'est pas exhaustif. Il existe bien d'autres méthodes, moins connues, pouvant être exploités comme l'analyse des émissions de lumière, des émissions acoustiques ou encore les injections électromagnétiques [Deb12].

Une fois l'état de l'art des attaques matérielles présenté avec notamment le principe de l'injection de faute par faisceau laser, il est possible de faire un état de l'art de l'onde lumineuse laser et de ses effets physiques mis en jeu lorsqu'un faisceau laser illumine un semi-conducteur. Dans un premier temps, des précisions sur ce qu'est précisément une onde lumineuse laser sont présentées. Et, dans un second temps, son effet sur le silicium est mis en évidence. Différents effets physiques seront alors introduits, comme la notion de génération de paires électron-trou dans le silicium liée à l'effet photoélectrique, ou le phénomène d'absorption.

I.3 État de l'art de l'interaction d'une onde laser sur le silicium

Le terme laser provient de l'anglais « Light Amplification by Stimulated Emission of Radiation ». Cette dénomination est traduite en français par « amplification de la lumière par émission stimulée de rayonnement ». Le laser est un dispositif générant une lumière spatialement et temporellement cohérente. L'intensité lumineuse à la sortie de l'équipement

laser est de forme gaussienne. La partie suivante décrit de manière physique la forme spécifique du faisceau laser.

I.3.1 Description d'un faisceau laser de type gaussien

Dans toute cette partie, le faisceau laser est considéré comme étant de forme gaussienne. En effet, l'intensité lumineuse n'est pas constante d'un point de vue spatial. La majorité de cette intensité est concentrée dans ce qui est appelé communément le spot laser. En s'éloignant du centre, l'intensité lumineuse décroît suivant un profil gaussien. Dans un premier temps, la formulation mathématique d'un tel faisceau est présentée.

Le faisceau émis, opère dans un mode transverse fondamental communément appelé "TEM_{00} mode". En optique, tout faisceau de lumière visible ou invisible est un rayonnement électromagnétique.

La formulation mathématique de l'intensité lumineuse dans un repère aux coordonnées cylindriques est de la forme suivante (voir ***Eq. I. 1***) [Pou00(c)]. Cette expression met en évidence le profil transverse gaussien en tout point *z* de l'onde considéré.

$$I(r,z) = I_0(z)e^{\frac{-2r^2}{w^2(z)}} \qquad \textbf{Eq. I. 1}$$

Avec I_0 étant définit de la manière suivante (***Eq. I. 2***):

$$I_0(z) = \left(\frac{w_0}{w(z)}\right)^2 \qquad \textbf{Eq. I. 2}$$

La ***Figure I. 9*** montre le graphique de l'intensité lumineuse en fonction de la distance *r* pour une coordonnée *z* donnée et avec $I_0(z=0) = 1$.

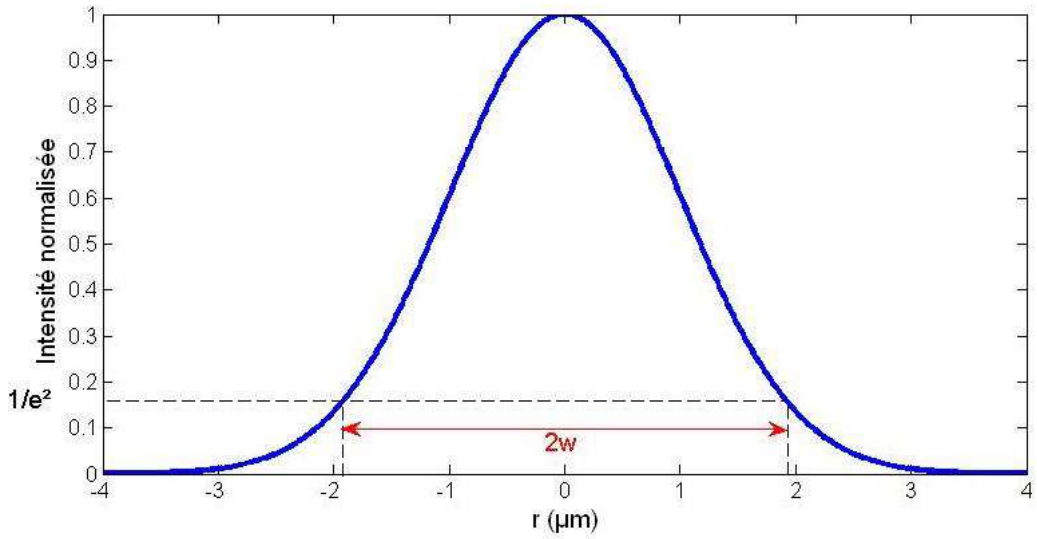


Figure I. 9. Profil d'intensité gaussien.

Le paramètre *w* est la distance à partir de laquelle l'intensité lumineuse normalisée est égale à *1/e²*.

La loi d'évolution de *w* en fonction de *z*, est également présentée (***Eq.*** I. 3) comme définit par [Yar97] et [Kog66] :

$$w(z) = w_0\sqrt{1+\left(\frac{\lambda z}{\pi w_0^2}\right)^2} \qquad \textbf{Eq. I. 3}$$

Le paramètre *w* est minimal à l'origine *z=0*. A cette coordonnée le rayon de courbure *R(z)* est infini. La valeur du col du faisceau (ou « waist » en anglais), est alors notée w_0.

La longueur de Rayleigh qui décrit la divergence du faisceau est également présentée ci-dessous (***Eq. I. 4***) :

$$Z_R = \frac{\pi w_0^2}{\lambda} \qquad \textbf{Eq. I. 4}$$

La taille du faisceau à l'origine, est minimale (disque de rayon w_0). Lorsque *z* augmente le faisceau diverge (voir ***Figure I. 10***). Au col, le front d'onde est localement plan avec un rayon de courbure infini.

L'équation du rayon de courbure *R(z)* est présentée ci-dessous (***Eq. I. 5)*** :

$$R(z) = z\left[1 + \left(\frac{\pi w_0^2}{\lambda z}\right)^2\right] \qquad \textbf{Eq. I. 5}$$

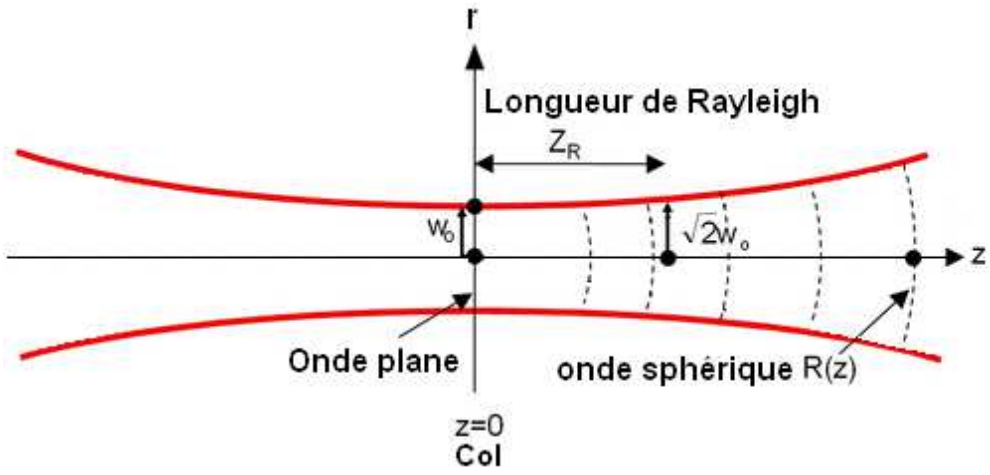


Figure I. 10. Propagation d'un faisceau gaussien.

L'intensité lumineuse du faisceau « s'étale » transversalement (suivant l'axe *r*) au cours de la propagation suivant l'axe *z*, tandis que son amplitude diminue. Ce phénomène est propre à la conservation de l'énergie. Le profil, quant à lui, reste toujours de type gaussien. La ***Figure I. 11*** montre ce phénomène. En effet, la fonction présentée à l'***Eq. I. 1*** est tracée à partir des paramètres présentés dans le ***Tableau I. 2*** pour une longueur d'onde du faisceau laser de 1064 nm comme celle produite par les équipements laser utilisés en injection de fautes par la face arrière.

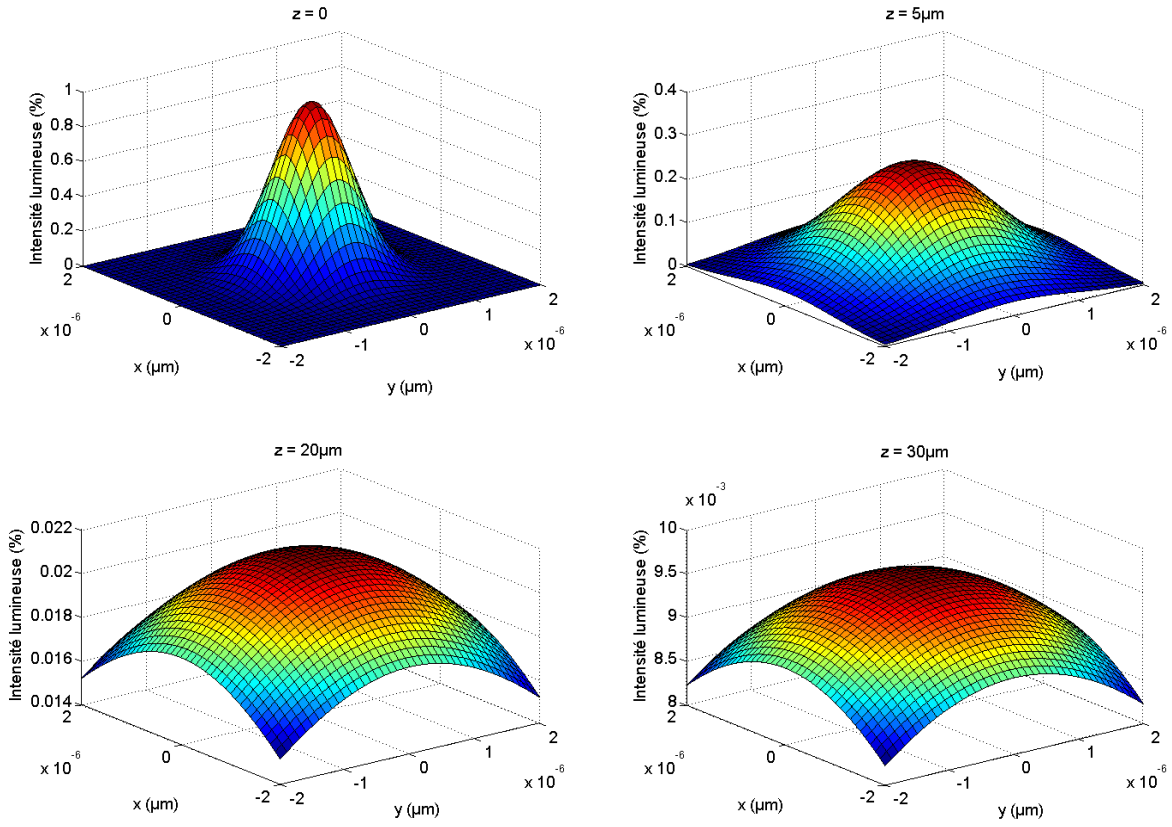


Figure I. 11. Evolution de l'intensité lumineuse en fonction de la distance *z*.

Paramètre	**Valeur**
w_0	1 µm
λ	1064 nm
I_0	1

Tableau I. 2. Valeurs de différents paramètres de l'équation Eq. I. 1.

Il existe également d'autres relations utiles, qu'il est possible de déduire des équations précédentes. Celles-ci permettent de retrouver par exemple, la taille du col (***Eq. I. 6***) ou sa position sur l'axe *z* (***Eq. I. 7***):

$$w_0^2 = \frac{w^2}{1+\left(\frac{\pi w^2}{\lambda R}\right)^2} \qquad \textit{Eq. I. 6}$$

Et :

$$z = \frac{R}{1+\left(\frac{\lambda R}{\pi w^2}\right)^2} \qquad \textbf{Eq. I. 7}$$

Où R est le rayon de courbure.

I.3.2 Interaction entre un faisceau laser et le silicium

Le paragraphe précédent (***I.3.1***) a décrit la propagation d'un faisceau laser gaussien à l'air libre. La suite décrit l'interaction de ce faisceau avec un milieu absorbant. Dans cette configuration, le milieu absorbant choisi est le silicium. La première étape consiste donc à appréhender le phénomène d'absorption dans le silicium.

I.3.2.1 Faisceau gaussien dans le silicium

Dans la partie précédente, la description a été faite considérant que le faisceau se propageait dans l'air. Lorsque le faisceau laser rencontre un milieu absorbant comme le silicium, d'indice de réfraction n, de nombreux paramètres sont modifiés. Dans cette étude, le col du faisceau est localisé sur la face arrière d'une tranche de silicium à l'aide d'un système de focalisation (voir ***Figure I. 12***).

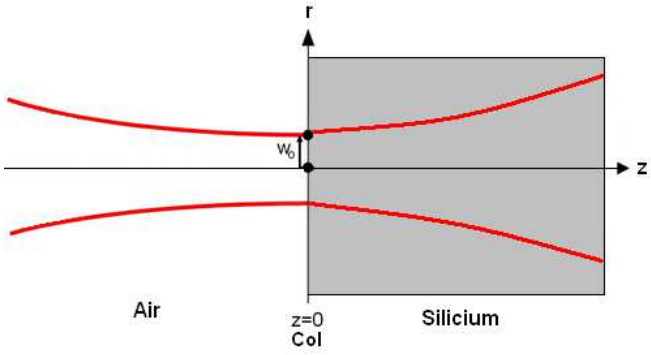


Figure I. 12. Faisceau gaussien pénétrant dans un milieu absorbant.

L'expression de l'intensité lumineuse I_{SI} dans le silicium a été présentée par Fouillat [Fou90] ***Eq. I. 8*** :

$$I_{SI}(r,z) = I_0 \frac{W_0^2}{W_{SI}^2(z)} e^{-\frac{2r^2}{W_{SI}(z)}} e^{-\alpha z} \qquad \textbf{Eq. I. 8}$$

Avec :

$$W_{SI}(z) = W_0 \sqrt{1 + \frac{\lambda_0 z}{\pi w_0^2 n_{SI}}} \qquad \textbf{Eq. I. 9}$$

Et :

$$R_{SI}(z) = z\left(1 + \left(\frac{\pi w_0^2 n_{SI}}{\lambda_0 z}\right)^2\right) \qquad \textbf{Eq. I. 10}$$

L'intensité lumineuse en fonction de la coordonnée *z* est présentée ***Figure I. 13***.

Le ***Tableau I. 3*** présente des valeurs des différents coefficients utilisés pour réaliser la ***Figure I. 13***.

Paramètre	**Valeur**
W_0	1 µm
λ	1064 nm
I_0	1
n	4
α	200 cm^{-1}

Tableau I. 3. Coefficients de l'équation Eq. I. 8.

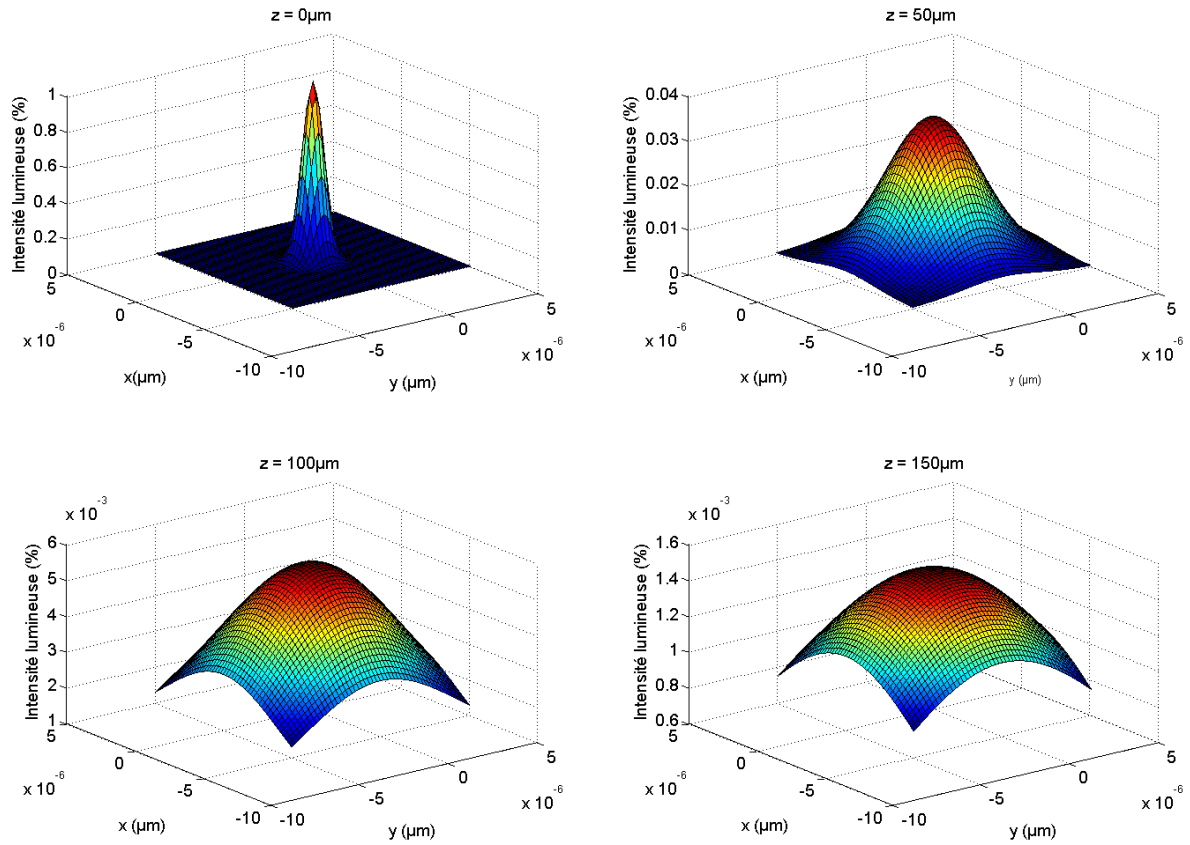


Figure I. 13. Intensité lumineuse du laser en fonction de la position *z* dans le silicium.

Il est possible de constater que similairement à un faisceau gaussien se propageant dans l'air libre, l'intensité lumineuse du faisceau pénétrant un milieu absorbant comme le silicium « s'étale » transversalement tout en diminuant son intensité suivant l'axe *z*. Son profil reste néanmoins toujours de type gaussien.

I.3.2.2 Absorption dans le silicium et effet du dopage

I.3.2.2.1 Description

Pour du silicium de type P peu dopé (< 10^{17} cm^{-3}), le coefficient d'absorption à température ambiante est donné, pour des longueurs d'onde comprises entre 0,7 µm et 1,07 µm, par la formule empirique suivante donnée par [Ger93] et reprise dans [Pou00(c)] :

$$\alpha(\lambda) = (85.7\,\lambda^{-1} - 77.4)^2 \qquad \textbf{Eq. I. 11}$$

Avec la longueur d'onde λ exprimée en μm et le coefficient d'absorption $\alpha(\lambda)$ en cm^{-1}.

La ***Figure I. 14*** montre le tracé de la fonction présentée ***Eq. I. 11*** ainsi que son inverse. Sa fonction inverse est appelée profondeur de pénétration.

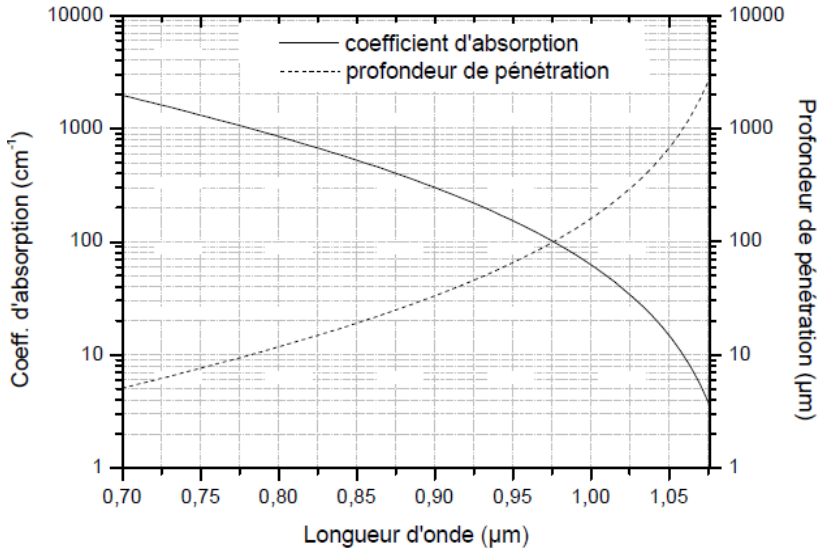


Figure I. 14. Coefficient d'absorption et profondeur de pénétration en fonction de la longueur d'onde [Pou00(c)].

Une énergie du photon supérieure à celle du band gap du silicium impose que la longueur d'onde soit inférieure à 1,1 µm. De plus, la ***Figure I. 14*** montre que l'absorption est minimale à cette longueur d'onde alors pour l'effet photoélectrique persiste encore. C'est pour cette raison que, la plupart des équipements laser utilisés pour l'injection de fautes par faisceau lumineux en face arrière de composant ont une longueur d'onde de 1064 nm. En face avant, les faisceaux laser verts ou ultraviolets peuvent être aussi utilisés.

Il est ensuite proposé d'étudier l'influence du coefficient d'absorption α sur l'intensité lumineuse (présenté à l'équation ***Eq. I. 8*** dans le ***paragraphe I.3.2.1***) à une coordonnée $z = 150\ \mu m$ (voir ***Figure I. 15***). Les mêmes valeurs que celles présentés au ***Tableau I. 3*** ont été utilisées.

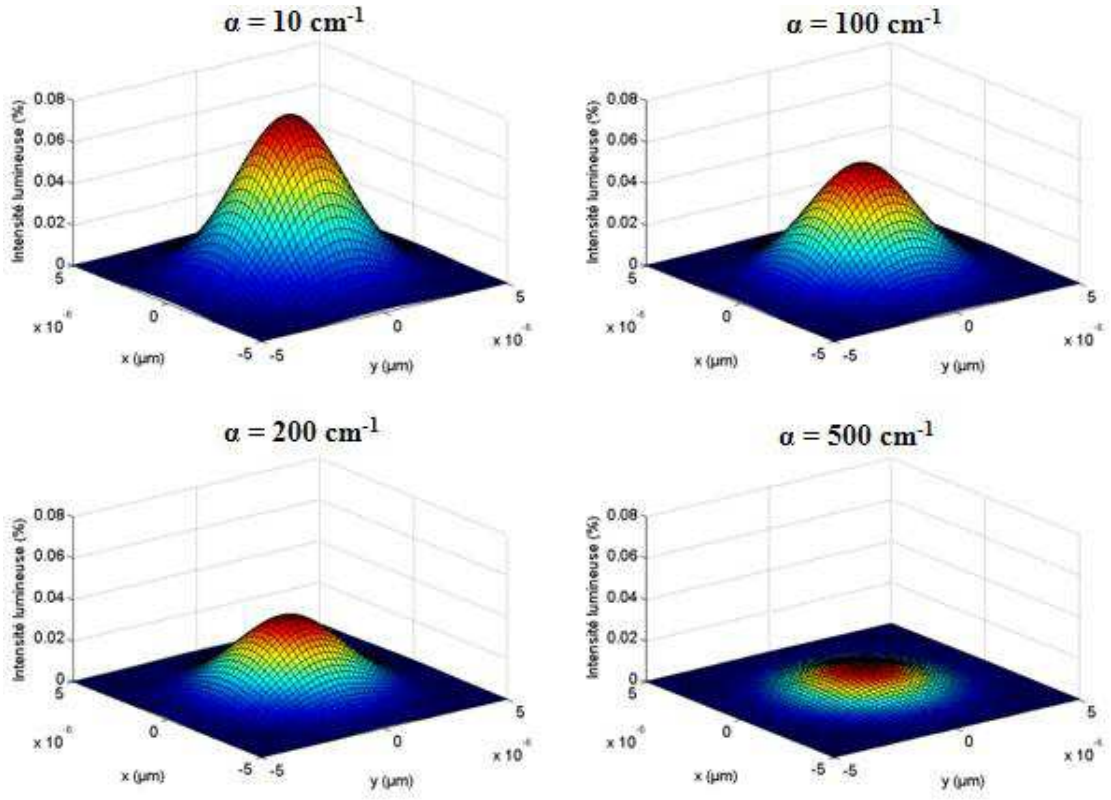


Figure I. 15. Intensité lumineuse du laser pour différentes valeurs du coefficient α à la position *z=150 µm* dans le silicium.

Par convention z = 0 correspond à la face arrière du silicium. Il est possible de remarquer que plus le coefficient d'absorption du silicium est important et plus l'intensité lumineuse du faisceau qui a pénétré 150 µm de silicium s'affaiblit.

I.3.2.2.2 Effet du dopage

Le dopage du substrat a une influence directe sur le coefficient d'absorption du silicium. Pour illustrer cet effet, des circuits de test réalisés en deux technologies différentes (technologie A: substrat fortement dopé: ***Figure I. 16***) et (technologie B : substrat faiblement dopé: ***Figure I. 17***) ont été utilisés. Des amincissements différents du silicium ont été pratiqués sur des circuits de test. Les photographies suivantes ont été réalisées dans les technologies A et B à partir une caméra infrarouge de type InGaAs observant la face arrière du circuit de test.

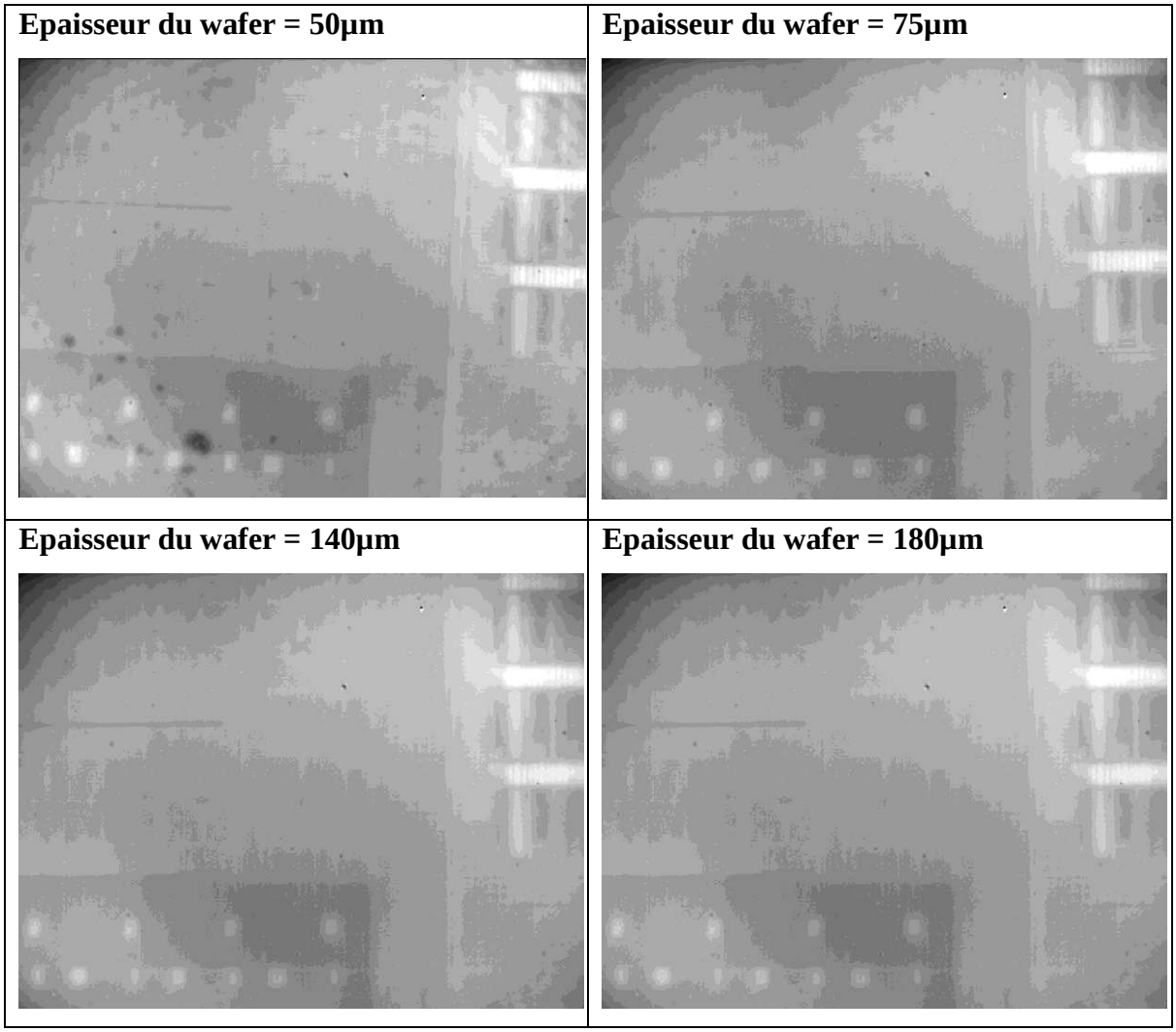


Figure I. 16. Photographies du circuit de test à différentes épaisseurs du silicium issues de la technologie A.

En technologie de type A, avec un substrat faiblement dopé, le coefficient d'absorption est faible. L'amincissement a un effet négligeable sur la netteté de la photographie. Cette technologie peut donc être considérée quasiment comme « transparente » à l'onde lumineuse laser d'une longueur d'onde de l'ordre du micromètre (proche de la longueur d'onde de la caméra infrarouge).

En technologie B, le substrat est fortement dopé. Le coefficient d'absorption est donc plus fort que dans la technologie A. Par les mêmes procédés, les photographies présentées ***Figure I. 17*** montrent que la netteté est meilleure pour une faible épaisseur de la puce.

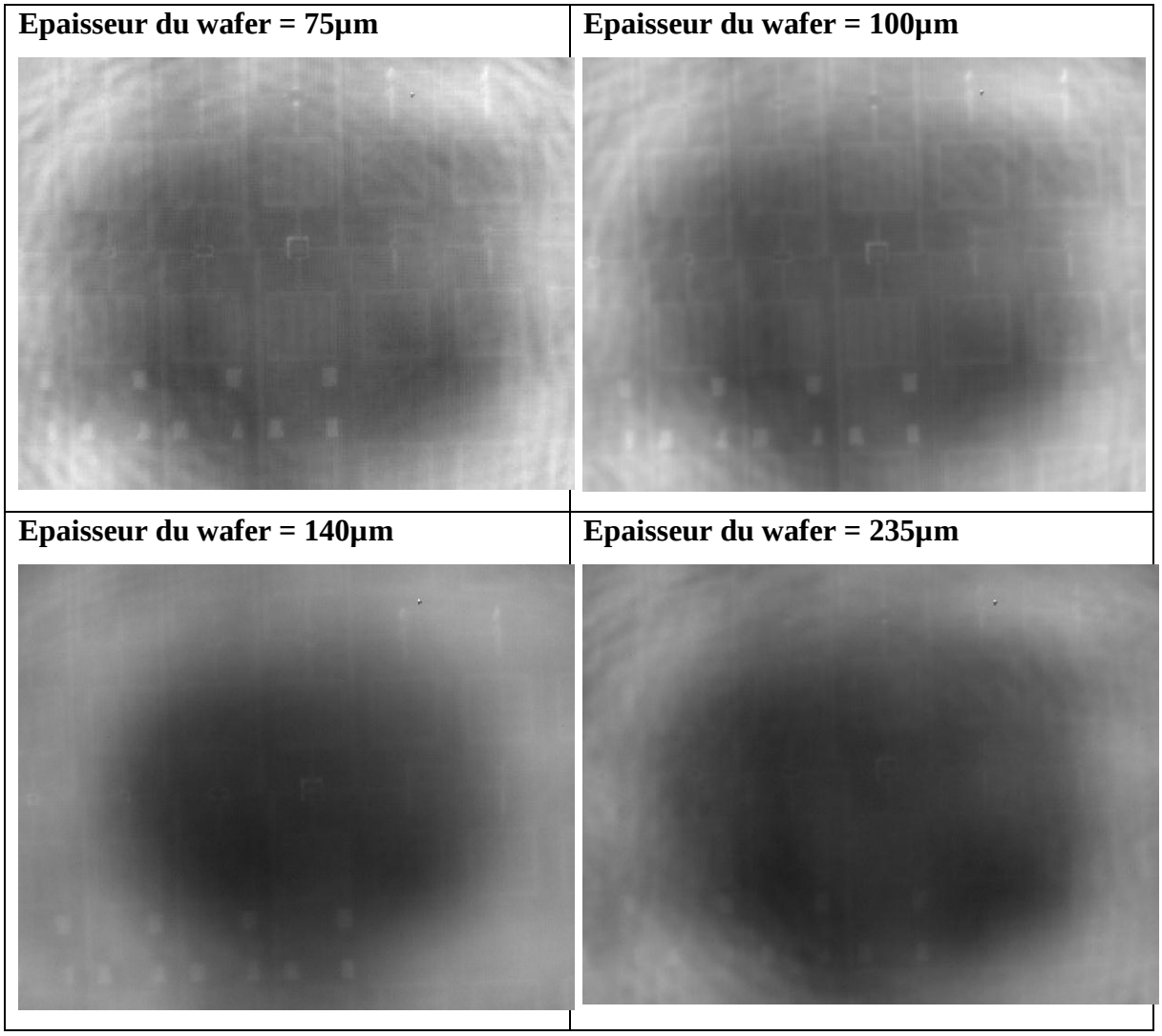


Figure I. 17. Photographies du circuit de test à différentes épaisseurs du silicium issues de la technologie B.

Ainsi, afin de générer le même photocourant entre une technologie de type A et une de type B, il est donc nécessaire d' amincir plus la puce en technologie B que dans la technologie A.

I.3.2.3 Effet photoélectrique

Dans un semi-conducteur, un photon provenant d'un faisceau de type laser dont l'énergie E_{ph} est supérieure à la largeur énergétique de la bande interdite (communément appelée le gap) peut être absorbé. Cette absorption permet à un électron de quitter la bande

de valence pour aller dans la bande de conduction. Ce phénomène physique est appelé effet photoélectrique par absorption inter-bandes.

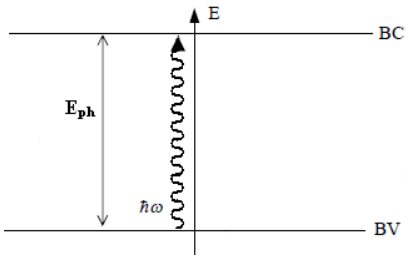


Figure I. 18. Diagramme d'état d'un semi-conducteur mettant en évidence le phénomène d'absorption direct.

Le phénomène physique qui peut permettre l'injection de faute dans un circuit sécurisé est le photocourant produit par l'effet photoélectrique qui intervient à certains nœuds sensibles d'un circuit en créant des transitoires de tensions. Le paragraphe qui va suivre détaille brièvement cet effet.

Lorsqu'un faisceau laser illumine le silicium, des paires électrons-trous sont créées sur toute la trajectoire du tir laser. Ces paires électrons-trous, si elles sont éloignées des jonctions PN, se recombinent sans effet notable. Par contre, si elles sont situées à proximité de jonctions PN polarisées en inverse, dans lesquelles il y a présence d'un champ électrique assez intense, entraîne la création d'un photocourant.

L'effet photoélectrique consiste en l'émission d'électrons par un matériau soumis à la lumière. Des porteurs de charges se séparent sous l'effet d'un champ électrique dans la zone de charge d'espace d'une jonction PN. Dans ce chapitre, l'effet photoélectrique est présenté en prenant l'exemple d'une jonction PN (voir ***Figure I. 19***).

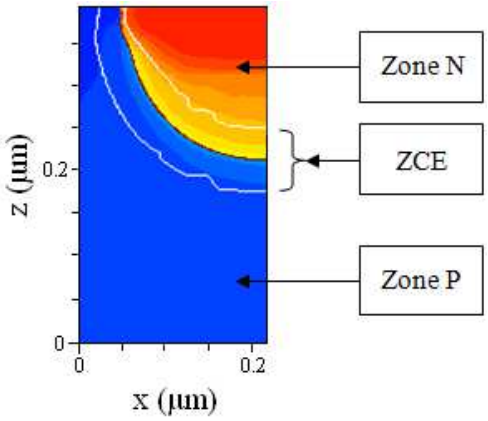


Figure I. 19. Coupe d'une jonction PN utilisée pour des simulations physiques de type TCAD.

La jonction PN est composée d'une zone de charge d'espace (ZCE) appelée couramment zone de déplétion, d'une région neutre de type N et une autre de type P.

Le tracé de la caractéristique courant–tension de la jonction PN présentée ***Figure I. 19*** obtenue par simulation physique (TCAD) pour différentes puissance laser illustre le courant traversant cette jonction PN en fonction de la puissance du laser. La composante du photocourant est présentée sur le graphique ***Figure I. 20***.

I_{PH} présent sur la figure ci-dessous est le photocourant généré par la jonction PN lorsque la jonction est polarisée en inverse.

L'expression du courant traversant la jonction est le suivant :

$$I = I_S\left(e^{\frac{eV}{kT}} - 1\right) - I_{PH} \qquad \textbf{Eq. I. 12}$$

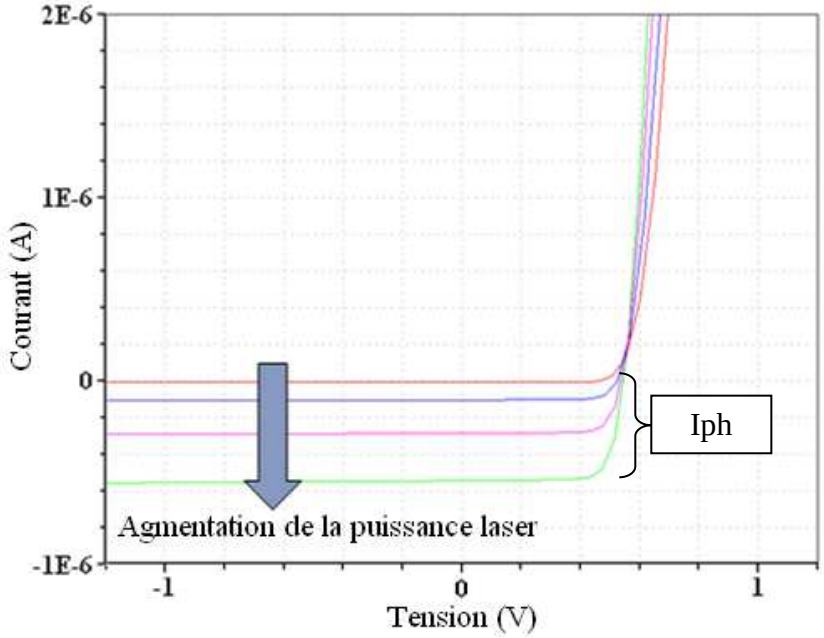


Figure I. 20. Simulation TCAD de la caractéristique courant-tension I(V) pour différentes puissances lasers mettant en évidence l'amplitude du photocourant.

I.3.2.1 Taux de génération de paires électrons-trous

Lors de l'interaction entre le laser et le silicium, des paires électrons-trous peuvent être générées dans le semi-conducteur par effet photoélectrique lorsqu'il est stimulé par un faisceau laser (comme décrit dans le ***paragraphe I.3.1***).

Si chaque photon absorbé génère une paire d'électrons-trous, le taux de génération de ceux-ci exprimé en $cm^{-3}.s^{-1}$ est donné par la relation suivante :

$$G_{p,light} = G_{n,light} = \alpha \frac{P_{opt}(z)}{E_{ph} A} \qquad \textbf{Eq. I. 13}$$

α (exprimé en m^{-1}) est le coefficient d'absorption du semi-conducteur. E_{ph} est l'énergie du photon (en eV). A est l'aire du silicium illuminée par le laser (en m^2). L'absorption de l'onde lumineuse a pour effet de diminuer la puissance optique P_{opt} en relation avec la distance suivant l'axe z. Cet effet est décrit par la relation mathématique suivante :

$$\frac{dP_{opt}(z)}{E_{ph}A} = -\alpha P_{opt}(z) \qquad \textbf{Eq. I. 14}$$

Dans le cas d'un laser pulsé de type gaussien, le taux de génération de paires électrons-trous pour un laser pulsé est défini par la relation suivante [Pou00(c)]:

$$g(r,z,t) = \frac{\alpha T_{trans} E_{ph}}{\pi^2 \omega_0^2 E_\gamma} e^{\frac{-2r^2}{\omega^2(z)}} \frac{\omega_0^2 e^{-\alpha z}}{\omega^2(z)} \frac{2e^{-\frac{t^2}{\tau_{las}^2}}}{\tau_{las}\sqrt{\pi}} \qquad \textbf{Eq. I. 15}$$

Où E_{laser} est l'énergie de l'impulsion laser, pour une émission limitée dans le temps, E_{ph} est l'énergie du photon, ω_0 est le « col » localisé sur la face arrière du semi-conducteur, τ_{las} est la durée de l'impulsion et z_{sc} est la distance confocale (profondeur d'observation de pénétration).

La formule ***Eq. I. 15*** est réduite à une impulsion laser de type gaussienne TEM_{00}.

La ***Figure I. 21*** présente le taux de génération de paire électrons-trous pour quatre temps différents avec une durée d'impulsion laser de 1 µs.

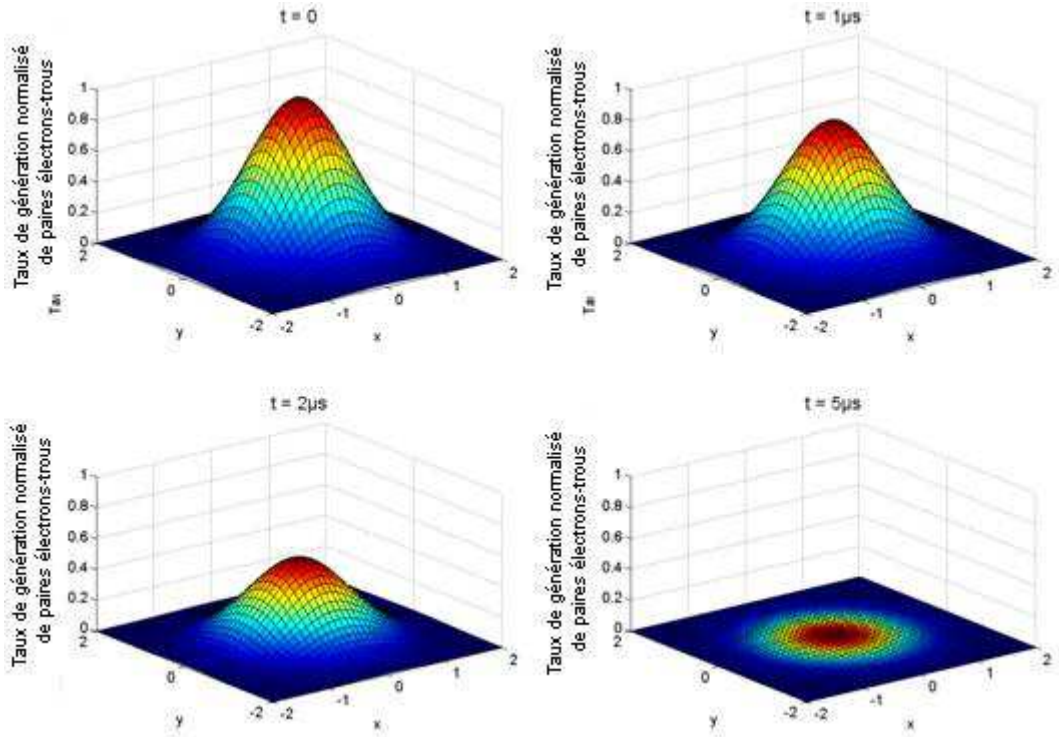


Figure I. 21. Evolution du taux de génération de paires électron-trous en fonction du temps pour une durée d'impulsion laser égale à 1 µs.

Une simulation TCAD 2D afin d'illustrer l'effet de l'absorption du silicium sur le taux de génération de paire électrons-trous a été faite. Une coupe d'une structure avec une épaisseur de $140\ \mu m$ a été créée à partir des étapes successives du process respectant la technologie (voir ***Figure I. 22***).

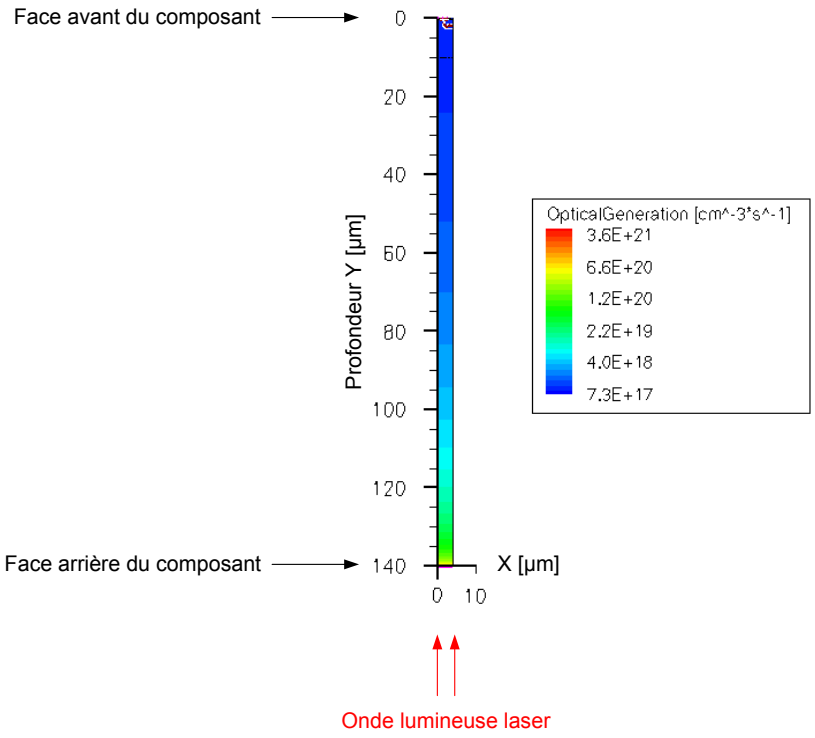


Figure I. 22. Composant CMOS avec une épaisseur de silicium de 140 µm.

Le taux de génération optique en fonction de l'épaisseur de la profondeur dans le silicium a été simulé. La cartographie du taux de génération pour une illumination en face arrière du composant est présentée ***Figure I. 22***.

Le taux de génération optique en fonction de la profondeur dans le composant est présenté ***Figure I. 23***. Il est possible de retrouver la forme en *exp(-αz)* (voir ***Eq. I. 15***) de l'expression du taux de génération, avec α étant le coefficient d'absorption. Il est donc possible de noter que le taux de génération de paires électrons-trous est maximal sur la face où le faisceau laser arrive sur le silicium ($z = 0$), et que plus on pénètre dans le composant et plus le taux de génération de paires électrons-trous diminue, cela étant dû à l'absorption dans le composant. Chaque technologie a un coefficient d'absorption différent en fonction du dopage du substrat.

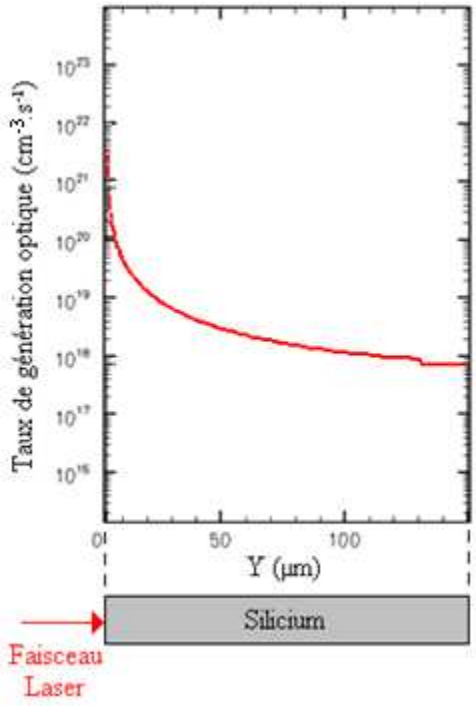


Figure I. 23. Taux de génération optique en fonction de la profondeur dans le silicium.

Le taux de génération optique, comme le montre l'***Eq. I. 15*** a un rapport direct avec le coefficient d'absorption α. Le plan constitué par la face arrière sur laquelle arrive le faisceau laser est l'endroit où un maximum de paires électrons-trous est généré. En pénétrant dans le matériau, cette génération de paires électrons-trous décroît à cause de l'absorption du milieu.

I.3.3 Différents types de Stimulation laser

En termes de Stimulation Laser, il existe de nombreuses techniques différentes.

I.3.3.1 Stimulation laser thermique

La stimulation laser thermique, utilisant des longueurs de l'ordre de 1300 nm est largement utilisée dans le domaine de l'analyse de défaillance. Le principe de base réside dans le fait que le faisceau laser provoque un échauffement localisé du silicium pouvant provoquer une modification de la résistance des connexions métalliques. La consommation

du circuit est ainsi modifiée. Une corrélation entre la position du laser et les mesures des variations anormales du courant ou de la tension permet une localisation du défaut. Il existe différentes techniques utilisant un laser thermique. Les plus connues sont l'OBIRCH qui analyse les modifications de courant et le TIVA qui est basé sur une modification de la tension.

I.3.3.2 Stimulation Photoélectrique Laser statique

La Stimulation Photoélectrique laser, à une longueur d'onde proche de 1000 nm, induit un photocourant dans les jonctions PN du circuit cible. Comme le laser thermique, la Stimulation Photoélectrique Laser statique est principalement utilisé dans le monde de l'analyse de défaillance. Elle regroupe différentes techniques comme l'OBIC ou le LIVA.

I.3.3.3 Stimulation Photoélectrique Laser dynamique

La Stimulation Photoélectrique Laser dynamique, ou en anglais « Dynamic Laser Stimulation » est une techniques spécifique à l'analyse de défaillance qui consiste à perturber le fonctionnement d'un circuit intégré défaillant (par effet photoélectrique ou photothermique), en fonctionnement dynamique, à l'aide d'un faisceau laser continu balayant la surface du circuit. Cette technique peut être avantageuse pour localiser des défauts non accessibles par des techniques purement statiques comme l'OBIRCH ou l'OBIC par exemple. L'analyse de la réponse des paramètres électriques à la perturbation laser conduit à une identification de l'origine de la défaillance. L'optimisation des techniques DLS permet d'améliorer l'efficacité des analyses de défaillance.

Il a été vu dans ce paragraphe qu'en terme d'interaction laser-silicium diverses techniques existent. Elles peuvent utiliser différent type de laser (photoélectrique, thermique…). La polarisation du circuit et le laser peuvent être statiques ou dynamique. De manière générale, dans ce manuscrit, les différents circuits étudiés ont été polarisé de

manière statique. Le faisceau laser illuminant le composant étudié était, lui, soit statique, soit à impulsion.

I.4 Notion de zones sensibles

Une zone sensible à la Stimulation Photoélectrique Laser (SPL) d'une porte CMOS est une jonction PN qui, lorsqu'elle est illuminée par un faisceau laser, induit des courants modifiant la tension de sortie de la porte. La localisation des zones sensibles varie en fonction des données manipulées. Pour mettre en évidence cette notion de zone sensible, un exemple a été pris sur la porte CMOS la plus simple qui existe, l'inverseur comme analysé en [Dut02]. Afin de trouver les zones sensibles d'un circuit CMOS en fonction de sa polarisation, l'étude se résume à une recherche des jonctions PN les plus fortement polarisées en inverse qui ont une influence sur la tension de sortie.

Dans le cas de l'inverseur, lorsque son entrée est polarisée à la valeur logique « 0 », la zone sensible se situe sur le drain du transistor NMOS *MN1* (voir ***Figure I. 24***). La jonction PN drain/bulk (N+/Psubstrat) est alors la plus fortement polarisée en inverse, générant ainsi le photocourant le plus fort. Dans ces conditions le photocourant allant du drain du transistor NMOS au substrat de type P a tendance à faire « écrouler » la tension de sortie de l'inverseur, si toutefois, la valeur du photocourant est supérieure au courant de saturation de du transistor PMOS *MP1 (IDSMP1)*.

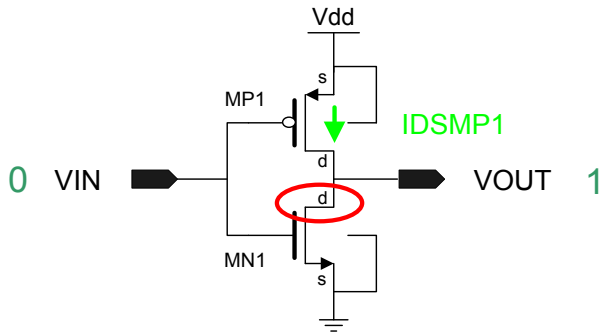


Figure I. 24. Zone sensible d'un inverseur lorsque l'entrée est polarisée à la valeur logique "0".

Si l'entrée de l'inverseur est maintenant à la valeur logique « 1 », la zone sensible de l'inverseur est le drain du transistor PMOS *MP1* (voir ***Figure I. 25***). Dans cette configuration, si le photocourant généré par le drain du transistor PMOS est supérieur au courant de saturation du transistor NMOS *IDSMN1*, la tendance sera à l'augmentation de la tension de sortie *VOUT* de l'inverseur, puisque le photocourant généré par le drain du transistor PMOS, va du puits N, polarisé à *VDD* à la sortie *VOUT*.

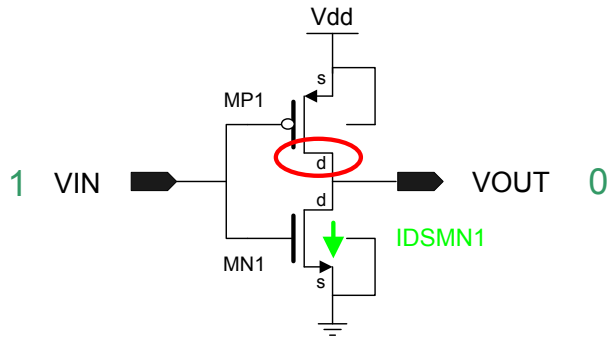


Figure I. 25. Zone sensible d'un inverseur lorsque l'entrée est polarisée à la valeur logique "1".

En résumé, sur un inverseur, la zone sensible est le drain du transistor bloqué (OFF). Bien évidemment, plus les portes CMOS sont complexes et plus le nombre de zones sensibles augmente.

I.5 État de l'art de la modélisation de l'injection de fautes par impulsion laser

Ce paragraphe, présente l'état de l'art de la modélisation de l'interaction entre le faisceau laser et le silicium. Afin de simuler les effets de l'onde lumineuse laser sur le composant, deux types de modélisations différentes sont envisagées. Le plus simple et le plus rapide en temps de calcul, mais également le moins précis, c'est la simulation électrique de type SPICE. De nombreux modèles de l'interaction entre le laser et le silicium ont déjà été développés [Roc92], [Cal96], [Mon99]. La seconde solution consiste à

modéliser les effets d'une SPL sur un composant microélectronique à l'aide du logiciel de simulation physique TCAD. Le temps de mise en œuvre et de simulation peut être un paramètre handicapant s'il est nécessaire de lancer un grand nombre de simulations en faisant varier les paramètres.

I.5.1 Modélisation de type SPICE

La modélisation la plus simple des effets du laser sur des transistors MOS est constituée d'une simple source de courant connectée sur chaque jonction PN. Afin de modéliser au mieux l'effet du laser sur le silicium, ses sources de courant, peuvent être de forme double exponentielle. La suite de ce paragraphe présente des modèles plus élaborés de transistor sous illumination laser.

I.5.1.1 Modèle d'un transistor NMOS pour une durée d'impulsion inférieure à 30 ps

Afin de modéliser les effets du laser sur des transistors MOS pour de faibles durées d'impulsion (<30 ps), des modèles électriques ont été établis entre autre par Pouget [Pou00(b)]. Le but est de simuler de manière assez fidèle les photocourants générés par le laser et mesurés sur les électrodes du transistor. De plus, ce modèle, peut également être utilisé pour le passage d'une particule radiative. La source de courant *Irad*, de type double exponentielle, modélise ce photocourant, dépendant de plusieurs paramètres. Différents éléments électriques sont rajoutés, simulant les mécanismes physiques induits par l'illumination laser du composant (voir ***Figure I. 26***).

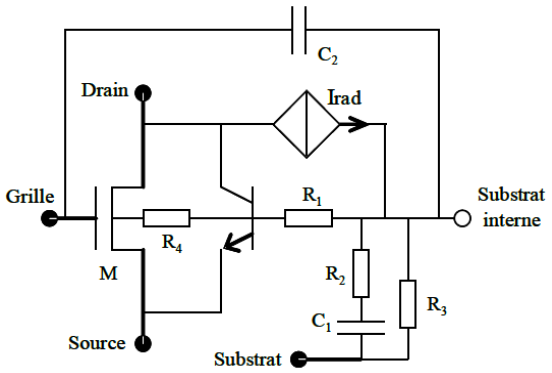


Figure I. 26. Modèle électrique complet d'un transistor NMOS sous illumination laser.

De plus, un nœud interne nommé *Substrat interne* permet de modéliser les lignes de potentiels dans le substrat liées au phénomène de funnelling. Ce nœud permet de déclencher un bipolaire parasite NPN formé par le drain (N+), le substrat de type P (Psub) et la source (N+). Un réseau passif de résistances et capacités, détermine la constante de temps qui décrit l'effet de relaxation diélectrique. Cette relaxation dite diélectrique est le temps nécessaire au rétablissement de la neutralité électrique dans la structure.

I.5.1.2 Modèle d'un transistor NMOS pour une durée d'impulsion supérieure à 8 ns

Un modèle électrique pour des durées d'impulsion plus longues (>8ns) a été également développé.

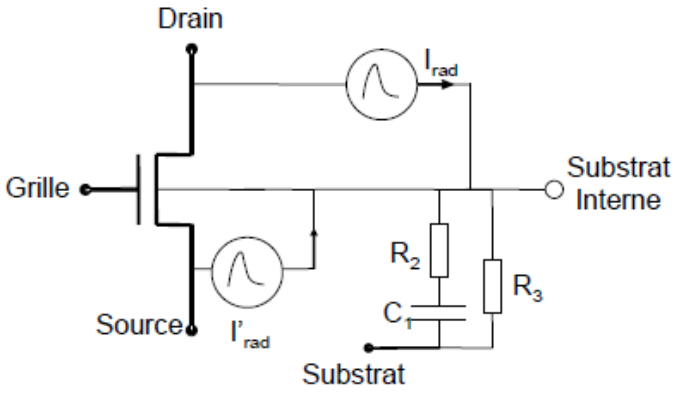


Figure I. 27. Modèle électrique simplifié d'un transistor NMOS sous illumination laser pour des durées d'impulsion longue.

Les impulsions de longue durée, n'ont pas les mêmes mécanismes de collection de charges. En effet, les lignes de potentiels ne se distribuent pas dans le substrat de manière significative. Le transistor bipolaire parasite NPN et la capacité *C2* présentent dans le modèle ***Figure I. 26*** n'est donc plus nécessaire dans le modèle. De plus, une deuxième source de courant *I'rad* a été connectée à l'électrode de source, vu que la jonction source/Psubstrat reste bloquée en polarisation inverse, mais génère tout de même un photocourant. Un facteur d'atténuation pour générer le courant de source, par rapport à celui du drain est utilisé comme il a été fait par Pouget en 2000, [Pou00(b)], puis reprit par Douin en 2005 [Dou05].

I.5.2 Modélisation TCAD

Une autre méthode afin de simuler les effets du laser sur des composants microélectroniques est de reconstruire le circuit à analyser en trois dimensions, grâce au logiciel TCAD [Sen], en respectant toutes les différentes étapes du process. Un module optique simulant l'effet du laser est ajouté, afin de recréer les phénomènes physiques qui se produisent lorsque le composant est illuminé. Ainsi, par exemple, une cellule SRAM complète a pu être créée en 3D sous TCAD comme présenté en [Dod05], [Gio07] (voir ***Figure I. 28***).

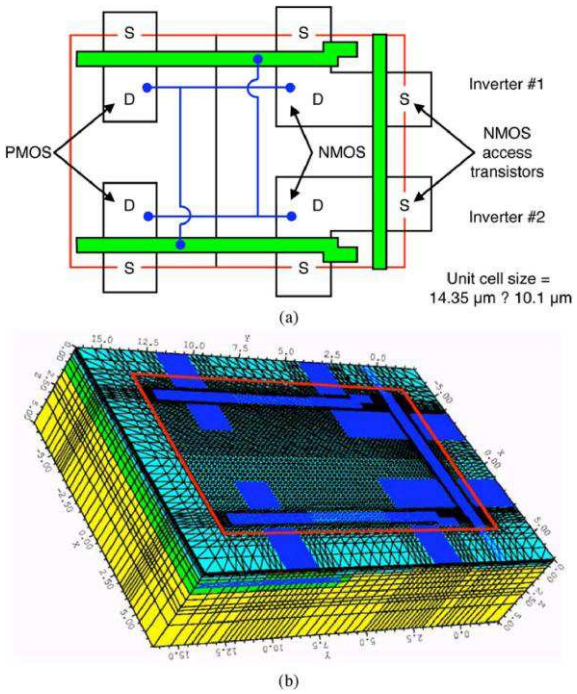


Figure I. 28. Simulation TCAD 3D d'une cellule SRAM (a) Layout. (b) Création de la structure 3D extraite de [Dod05].

Cette simulation peut par exemple faire apparaître les zones sensibles à une particule radiative (voir ***Figure I. 29***), de la cellule en fonction du LET (Linear Energy Transfert). Le LET est l'énergie de la particule radiative transférée au composant [Dod05]. Ce type de simulation a des similitudes importantes avec celle montrant les effets d'un laser sur ce type de cellule.

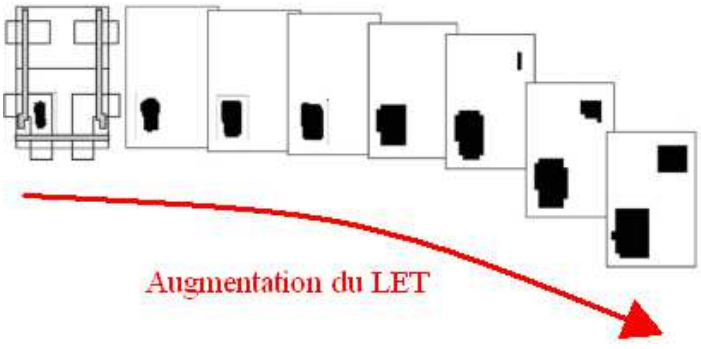


Figure I. 29. Apparition des zones sensibles en fonction de la puissance du laser extraite de [Dod05].

Cette solution a l'avantage de mettre en évidence des phénomènes physiques précis sur des solutions plus ou moins complexes à plusieurs transistors comme présenté en [Ols05]. En revanche le désavantage principal réside dans le temps et la complexité nécessaires pour créer le modèle 3D. De plus le temps de calcul peut être extrêmement long (de quelques heures à plusieurs jours en fonction de la puissance de calcul mis à disposition). Il est également possible de faire des simulations 2D (comme développées dans ce manuscrit), qui donnent des renseignements souvent suffisants avec des temps de simulation nettement moins élevés que pour des structures 3D.

I.5.3 Simulation mixte SPICE-TCAD

Une autre solution, mêlant les avantages de la simulation SPICE (rapidité de mise en œuvre et de calcul) et ceux de la simulation TCAD existe (précision de phénomènes physiques mis en jeu). Il s'agit de la simulation mixte abordé dans les publications suivantes [Woo93], [Dod95], [Dod96], [Dod96(b)]. Cette solution consiste à simuler en 2D ou 3D le ou les transistors MOS impactés par le faisceau laser (voir ***Figure I. 30*** et ***Figure I. 31***) et de l'insérer ensuite dans une netlist SPICE plus complexe.

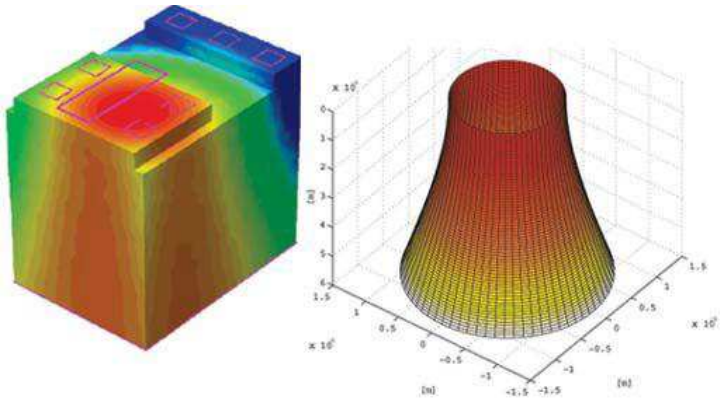


Figure I. 30. Modélisation TCAD du transistor impacté par le faisceau laser [Dod95].

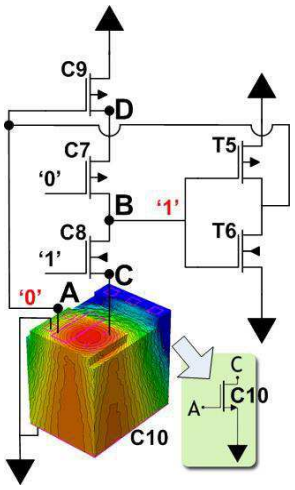


Figure I. 31. Exemple du principe de simulation mixte SPICE-TCAD [Dod95].

Cette solution peut ainsi permettre de simuler des portes CMOS bien plus importantes que dans un cas de simulation purement de type TCAD, tout en gardant les avantages de l'analyse des phénomènes physiques créés par le laser sur le composant.

I.6 Défis de l'injection de fautes

Dans cette partie sont présentées les difficultés à réaliser une attaque par injection de fautes, en se consacrant à l'injection de faute par faisceau laser.

I.6.1 Problématique mécanique

Afin de réaliser une attaque par injection de fautes sur un composant, il est nécessaire de prendre en compte la problématique non négligeable d'adaptation mécanique de la puce sur l'équipement laser. Bien souvent il faut créer une carte de test spécifique capable de s'adapter aux contraintes mécaniques du banc laser, pouvant également communiquer avec le circuit à attaquer (voir ***Figure I. 32***).

Figure I. 32. Photographie de la carte de test du circuit cible et de son adaptation sur l'équipement laser.

Une injection de fautes par impulsion laser peut se faire aussi bien en face avant qu'en face arrière. Toutefois, un faisceau laser n'arrive pas à traverser les niveaux de métallisation en face avant. Cette tendance est de plus en plus importante dans des technologies actuelles qui vont dans le sens de l'augmentation du niveau de métallisation. De plus, les microcontrôleurs sécurisés actuels possèdent un shield métallique en face avant qui agit notamment comme un « bouclier » limitant ainsi les attaques laser par cette face. En face arrière le faisceau laser arrive directement sur le silicium. L'injection par ce côté de la puce est donc plus facile, mais plus restrictif au niveau de la longueur d'onde. En effet, un laser vert ne peut pas être utilisé en face arrière du fait d'un coefficient d'absorption élevé à cette longueur d'onde.

La ***Figure I. 33*** montre qu'il est nécessaire de réaliser également une ouverture mécanique du boîtier dans lequel se trouve la puce.

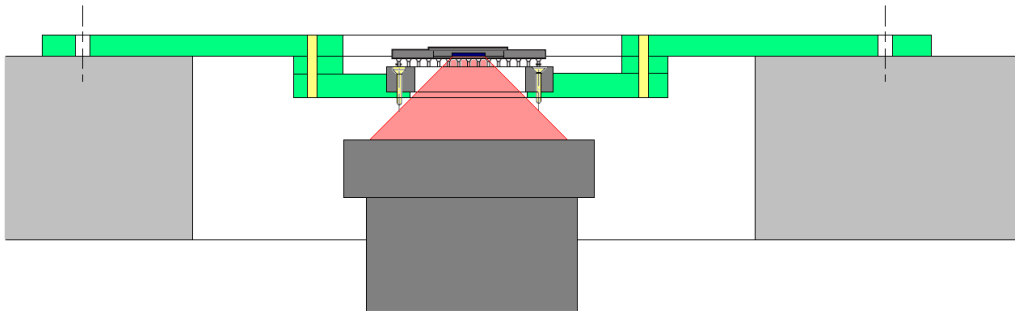


Figure I. 33. Coupe de la carte de test s'adaptant sur l'équipement laser.

L'une des grandes difficultés de l'injection de faute, réside dans l'accès à la face arrière du boîtier. En effet, il faut que le perçage du trou et le collage de la puce sur le boitier coïncide avec la zone à illuminer avec le faisceau laser. L'une des solutions proposée a été de réaliser un usinage du boîtier au laser. L'exemple de la ***Figure I. 34*** montre l'usinage d'un DIL24 en matière plastique.

(a) (b)

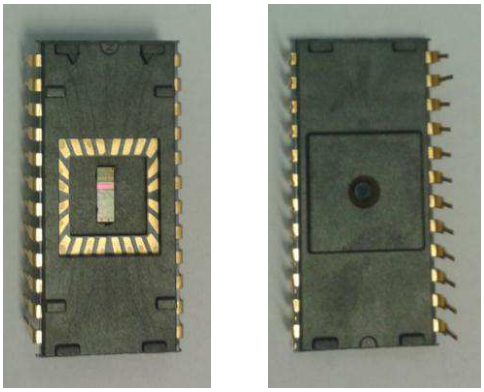


Figure I. 34. Photographie de l'usinage d'une puce de test montée sur DIL plastique usiné afin de pouvoir faire une injection laser. (a) Face avant, (b) Face arrière du DIL.

Une cavité (voir ***Figure I. 35***) a été ainsi usinée par faisceau laser, pour pouvoir positionner la puce correctement par rapport au trou. Ensuite la puce est collée sur le DIL puis des fils de bonding relient les Pads de la puce aux différentes Pins du support plastique.

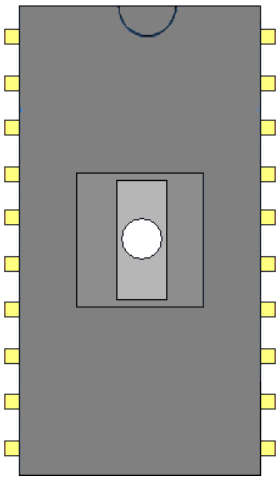


Figure I. 35. Schéma de l'usinage d'un DIL plastique afin de pouvoir faire une injection laser en face arrière de la puce.

Ces étapes d'ouverture de boîtier peuvent également se faire en chimie classique, car l'usinage par découpe laser à un coût non négligeable et nécessite un équipement dédié à la découpe fine.

I.6.2 Comparatif entre le diamètre du spot laser et la diminution de la taille des transistors

Une autre problématique liée à l'injection de fautes est la diminution constante de la taille des transistors comme explicité par [Amu08]. En effet il devient de plus en plus difficile de perturber uniquement un seul transistor avec un faisceau laser. La ***Figure I. 36*** présente la diminution de layout d'un nœud technologique comparée à un spot laser d'un diamètre de 1 µm qui correspond à une certaine limite physique.

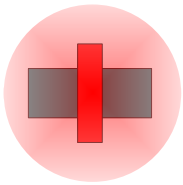
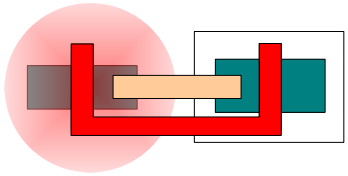
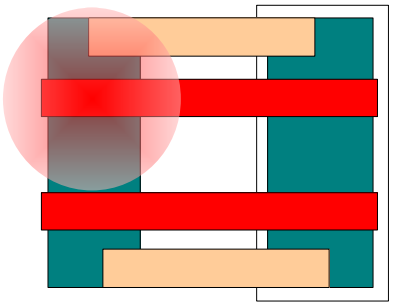
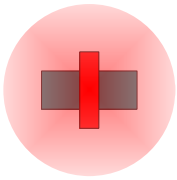
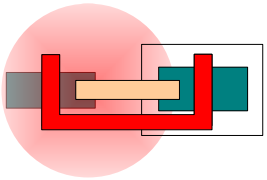
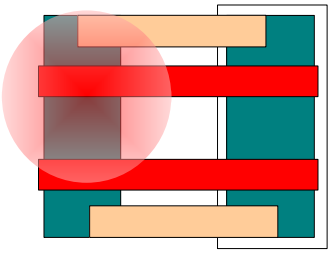
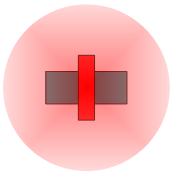
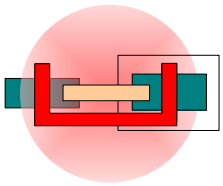
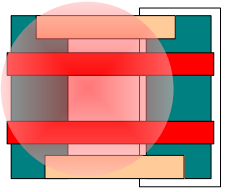
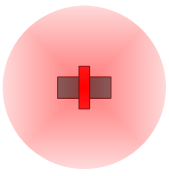
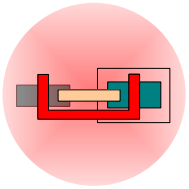
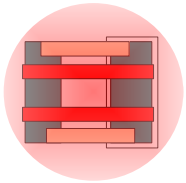
	Transistor	**Inverseur**	**Cellule SRAM**
130 nm 2002			
90 nm 2004			
65 nm 2006			
32 nm 2010			

Figure I. 36. Evolution de la technologie des semi-conducteurs par rapport à un faisceau laser de diamètre 1 µm [Pou00(c)].

En technologie 130 nm, un faisceau d'un diamètre de 1 µm pouvait impacter quasiment un transistor unitaire. Avec les nouvelles technologies de 65 nm ou inférieur, un spot de 1 µm recouvre l'intégralité d'un point mémoire de type SRAM. Une injection fine

devient donc de plus en plus difficile avec l'évolution de la technologie du semi-conducteur. De plus, il faut considérer que l'intensité du faisceau laser est de forme gaussienne, illuminant une surface plus importante que la taille de spot nominale.

I.7 Etat de l'art des contre-mesures aux injections de fautes par impulsion laser

Depuis que les attaques par faisceau laser sont connues pour être capables de générer des erreurs exploitables afin d'extraire de manière frauduleuse des données confidentielles, les concepteurs de circuits intégrés ont tenté de développer diverses contre-mesures de protection pour faire obstacle à ses attaques. Ces différentes contre-mesures (technologiques, contre-mesures architecturales, contre-mesures logiciels et détection d'intrusion laser) sont présentées dans la suite de ce paragraphe.

I.7.1 Contre-mesures technologiques

Cette partie présente un état de l'art des différentes contre-mesures technologiques aux attaques par impulsion laser.

I.7.1.1 Protection par la face avant grâce au Shield

Une contre-mesure actuelle pour protéger la face avant des microcontrôleurs sécurisés, est d'utiliser des couches métalliques. La plupart du temps, ces couches sont constituées de lignes métalliques enchevêtrées. Ces couches de métal initialement prévues pour faire face au probing de signaux en face avant font également barrage naturellement à un faisceau de longueur d'onde de type laser, empêchant ainsi l'injection de fautes par cette face. En effet les lignes de métallisation réfléchissent la quasi-totalité du faisceau.

I.7.1.2 Protection de la face arrière grâce à la technologie SOI

Les technologies de type CMOS – SOI (SOI pour Silicon On Insulator), créées principalement pour réduire la consommation des circuits, font barrage aux attaques laser par la face arrière du composant. En CMOS – SOI, il existe une isolation diélectrique totale entre les transistors qui sont réalisés sur une couche de matière isolante (SiO_2). Ceci a pour effet de réduire le volume de silicium dans lequel le faisceau laser peut générer des paires électrons-trous. La ***Figure I. 37*** donne le schéma de principe de la réalisation de ces transistors en technologie SOI.

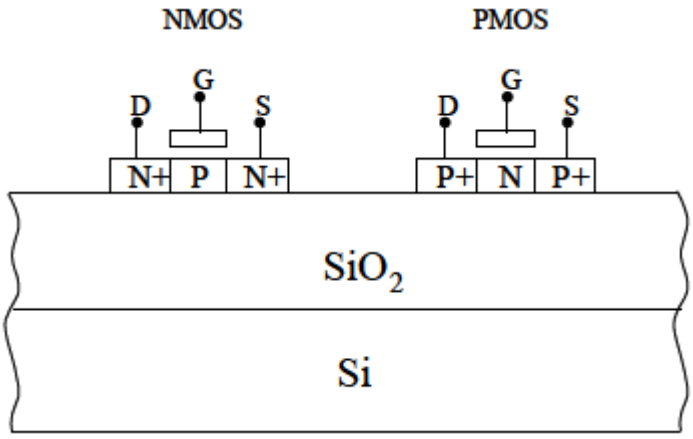


Figure I. 37. Coupe de transistors MOS en technologie CMOS SOI.

La réduction du volume de génération des tels porteurs est clairement significative pour ce type de technologie. Ainsi, la technologie CMOS – SOI semblerait être un obstacle aux attaques par faisceau laser des circuits intégrés, sans cependant les rendre totalement impossible.

I.7.2 Durcissement par conception

Une autre technique afin de contrer les attaques par impulsion laser consiste dans le durcissement lors de la conception des circuits intégrés. Cette technique regroupe aussi bien des approches s'appliquant à l'échelle des transistors aussi bien qu'à l'échelle du système dans sa globalité. En conséquence, une partie de ces techniques nécessite de la part

d'intervenant mal intentionné, l'augmentation de la puissance du laser ou la mise en œuvre simultanée d'un second faisceau lui permettant de créer des fautes exploitables. Cette technique d'opposition aux attaques est rendue principalement possible par un jeu sur le dimensionnement des transistors ou sur une augmentation des différentes capacités du circuit.

I.7.3 Contre-mesures architecturales

Le concept architectural comprend plusieurs notions différentes. Tout d'abord, l'algorithme utilisé dans le circuit est mis en œuvre lors de sa conception. Ainsi il est possible de voir que le choix du module de calcul détermine son implantation physique, de même le choix de l'architecture du circuit a une grande importance dans la stratégie de contre-mesure. Enfin, la définition des protocoles d'échanges de données inhérents au circuit est également un point crucial à gérer. En vue d'augmenter la sécurité, des solutions différentes devront être proposées selon que les blocs fonctionnels traitent des données sensibles ou qu'ils assurent simplement le routage des données via des interfaces de communication.

Le microprocesseur devra gérer les dialogues avec l'environnement extérieur afin et maîtriser les flux de données ainsi que les instructions et mettre en œuvre les algorithmes de chiffrement, toutefois aucun accès ne devra atteindre les clefs secrètes, ainsi que tout résultats de calcul intermédiaires. En vue de protéger le produit, toute perturbation du fonctionnement du processeur ne doit pas laisser fuir des données protégées.

Il est possible de retenir de ce qui précède qu'une architecture sécuritaire, doit être constituée par différents blocs dont le microcontrôleur supervise les données sensibles. Des spécifications strictes et hiérarchisées sont à respecter selon les informations que le bloc fonctionnel manipule. Une architecture peut être considérée comme sécurisée s'il existe une barrière physique entre la zone ou les clefs sont stockées et manipulées et les zones d'accès avec le monde extérieur.

Malheureusement, le circuit reste sensible aux attaques par canaux auxiliaires qui exploitent la corrélation entre les clefs utilisées et les données disponibles en sortie du

circuit pour récupérer ces clefs. Ils utilisent pour ce faire toute la gamme des émissions physique du circuit (comme vu au ***paragraphe I.2.1.3***).

I.7.4 Techniques de contre-mesures par redondance

En matière de redondance, il existe principalement deux concepts, la redondance temporelle et la spatiale.

I.7.4.1 Redondance temporelle

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

Cette méthode a un coût quasiment nul sur la surface de silicium, mais elle ralentit considérablement les calculs (d'un facteur proche de 2). Elle est préconisée dans les applications ou la surface de silicium est moins importante que la vitesse de calcul ou que la consommation.

I.7.4.2 Redondance spatiale

La technique de redondance spatiale consiste à faire exécuter le même calcul en parallèle par des blocs redondants, puis à comparer ces résultats en sortie. Il est préconisé d'appliquer cette technique dans les systèmes incluant des modules spécifiques effectuant un traitement complexe des données en un temps extrêmement court.

Cette technique est donc gourmande en surface de silicium et en consommation car les modules de calculs sont dupliqués et fonctionnent en parallèle. Par contre, la vitesse de traitement des informations est peu affectée dans ce type d'architecture.

I.7.4.3 Redondance d'information et code correcteur d’erreurs

La redondance d'information consiste à augmenter la cohérence des données grâce à un codage judicieux. C'est une technique largement utilisée car elle englobe les codes détecteurs et correcteurs d’erreurs tels que par exemple les codes de parité ou le code de Hamming. Cependant, dans la majorité des cas, ces codes sont développés pour une architecture qui leur est propre.

Les codes détecteurs et correcteurs d’erreurs sont fréquemment utilisés dans les mémoires. Il est possible de citer entre autre, le contrôle de la parité, le code Berger, le code de Hamming, le code Reed-Solomon, etc. Ils permettent de détecter et de corriger une ou plusieurs erreurs dans des groupes de bits en fonction de leur complexité.

I.7.5 Contre-mesures logicielles

La couche logicielle d'un circuit sécuritaire fait évidemment aussi l'objet d'une réflexion pour le rendre plus sûr. Les principales vulnérabilités de cette couche proviennent, en grande majorité, d'un accès possible aux données non encryptées par le biais d'un mode de test du logiciel ou bien grâce à des failles dans le protocole de transmission des données comme abordé en [Bon01].

Comme les techniques actuelles d'injection de fautes par impulsion laser permettent d'affecter un registre précis d'un circuit, il est donc nécessaire de protéger les parties critiques de l’algorithme du logiciel qui contrôle le registre. Cela peut être réalisé en utilisant par exemple la redondance de code, ou des codes correcteurs d’erreur afin de s’assurer que les données manipulées ne sont pas erronées.

I.7.6 Les détecteurs

Il est possible de détecter les attaques dans un circuit sécurisé de diverses manières.

I.7.6.1 Par variation de tension

L'une des techniques de détection d'une attaque en faute est de concevoir des circuits capables de détecter d'éventuelles variations de tension induite par exemple par un faisceau laser. En effet les forts photocourants générés principalement par les jonctions PN formées par les caissons de type N sur le substrat P peuvent créer des chutes de tensions sur les rails d'alimentation. Ces chutes (appelées glitch en anglais) peuvent alors être détectées par un simple comparateur en tension.

I.7.6.2 Par variation de la fréquence d'horloge

Une autre méthode possible réside dans la détection d'une variation de la fréquence de l'horloge. En effet une injection de fautes peut modifier le cadencement du signal de l'horloge interne. Il est alors possible d'imaginer un détecteur capable de signaler une modification de cette fréquence d'horloge.

I.7.6.3 Par lumière laser

L'approche la plus simple est d'implémenter dans le circuit des organes de détection spécifiques capables de détecter une attaque laser. Il peut s'agir tout simplement d'une photodiode polarisé en inverse, qui lorsqu'elle est illuminée génère un photocourant plus important. Cette augmentation de courant peut ensuite être détectée par un simple circuit logique.

Une autre solution consiste à utiliser un circuit appelé BBICS (Bulk Build In Current Sensor), comme présenté entre autre par Bastos en 2011 [Bas11], [Wir07], capable de détecter des impulsions laser très courtes (de l'ordre de quelques centaines de ps) comme celle utilisées pour simuler les effets des radiations sur les circuits. Un tel détecteur est basé sur la génération d'un photocourant venant faire basculer de manière non volatile un verrou mémoire de type latch. Cette solution pourrait être utilisée pour détecter un tir laser sur une puce, cette information serait reconnue par le circuit, déclenchant ainsi certains mécanismes de protection pouvant par exemple activer le reset de ce circuit.

En outre, ses diverses solutions sont extrêmement dépendantes de la technologie utilisée, et doivent être repensées et conçues à chaque nouveau changement technologique.

Malgré toutes ces protections, un pirate bien informé, peut, dans un premier temps mettre tous ces détecteurs hors d'usage avant de s'attaquer au circuit.

Les techniques de contre-mesures telles que par exemple les process CMOS SOI ont un coût financier important. En outre, les solutions de redondances spatiales imposent des surfaces additionnelles qui peuvent être importantes entrainant également des couts élevés. Ces différentes techniques peuvent également entraîner une dégradation des performances temporelles et une augmentation de la puissance consommée.

De plus, malgré toutes ces contraintes, elles ne garantissent pas une immunité totale. A ce jour, il n’existe pas de solutions optimales à ces problèmes. Un concepteur de contre-mesures devra toujours penser à trouver un compromis entre la sécurité, la surface de silicium, la rapidité et la consommation pour que son produit obtienne le meilleur ratio.

Conclusion

Dans ce premier chapitre, une présentation générale d'un circuit intégré sécurisé a été faite au travers de la description de la carte à puce. Dans un second temps les différents types d'attaques matérielles sont présentés, en insistant tout particulièrement sur le principe d'injection de fautes par faisceau laser. Il convenait donc naturellement de présenter les caractéristiques physiques d'un laser. L'interaction entre le laser est le silicium, principe de base de l'injection de faute, a ensuite été détaillée. De plus, l'état de l'art des modélisations de l'injection laser et des contre-mesures a également été présenté dans cette partie. Ce premier chapitre est donc une base de référence pour la lecture de la suite de ce manuscrit.

Dans le chapitre qui va suivre, les campagnes de mesures réalisées afin de comprendre finement les effets d'un laser continu ou à impulsion sur les éléments de base d'un semi-conducteur, tel qu'une jonction PN ou des transistors CMOS y sont présentées. De plus des simulations TCAD permettent de confirmer certains phénomènes ou d'expliquer des points de mesures incompris. Des modèles électriques ont pu être réalisés à partir de ces mesures. Ces modèles permettent de simuler électriquement de manière extrêmement rapide le comportement de portes relativement simples soumises à une injection de fautes par faisceau laser.

Chapitre II. MODÉLISATION ÉLECTRIQUE DE L'INJECTION DE FAUTES DANS DES CIRCUITS SÉCURISÉS

Introduction

Un état de l'art non exhaustif de l'injection de fautes par stimulation photoélectrique laser a été présenté au chapitre précédent. Ce chapitre est dédié à la compréhension et à la modélisation des phénomènes physiques mis en jeu lors de l'interaction entre une onde lumineuse de type laser et le silicium. Toutes les mesures ainsi que les modèles électriques associés, présentés dans ce chapitre, ont été réalisés grâce à deux équipements laser aux caractéristiques bien différentes. Le premier est un laser délivrant une faible puissance continue qui est utilisée principalement dans le domaine de l'analyse de défaillance de circuits. Il s'agit d'un I-phemos de la société japonaise Hamamatsu [Ham11] dont la puissance laser maximale est de l'ordre de quelques milliwatts. A cette puissance, seuls des effets photoélectriques d'amplitude limitée peuvent être générés dans le silicium [Sar12], [Sar12(b)], ce qui est suffisant pour l'analyse de défaillance (OBIC ou OBIRCH). Avec ce type d'équipement, l'injection de fautes est donc très difficile à réaliser. C'est la raison pour laquelle un deuxième équipement laser, plus puissant, a été utilisé afin d'étudier d'autres phénomènes physiques [Sar13], [Sar13(b)]. Ce deuxième équipement est un laser impulsionnel de forte intensité dont la puissance maximale est de l'ordre du Watt en sortie d'objectif. Cet équipement peut être utilisé dans divers domaines tel que l'injection de fautes ou bien permettre de recréer l'effet d'une particule radioactive présente dans l'environnement sur un circuit, et ce grâce à un laser. Toute la série de tests pratiqués dans ce chapitre ont été réalisés avec une longueur d'onde de 1064 nm. La première étape a été de comprendre les phénomènes mis en jeu lorsqu'une jonction PN est illuminée par un faisceau laser afin de pouvoir bâtir un modèle électrique. En effet l'étude des jonctions PN sous stimulation photoélectrique laser est une étape fondamentale dans la compréhension des phénomènes mis en jeu lors de l'illumination en face arrière de transistors MOS, vu qu'il est constitué de plusieurs jonctions PN, et par association, des portes CMOS. Aussi, dans un second temps l'étude a été menée sur des transistors MOS. Le modèle électrique associé est donc constitué principalement d'un assemblage de jonction PN. Afin de complexifier encore un peu plus la problématique, l'étude a porté sur la modélisation

électrique de porte CMOS [Sar13(c)] faite de transistor NMOS et PMOS dont l'élément le plus simple est un inverseur. En dernier lieu, une cellule SRAM a été étudiée. De plus dans tout ce chapitre, des simulations TCAD ont été faites dans le but de répondre à certaines interrogations soulevées lors de mesures ou pour permettre d'illustrer des phénomènes physiques particuliers observés lors des mesures. La finalité de la modélisation serait de pouvoir prédire de manière extrêmement rapide la réponse d'un circuit à une illumination laser afin que les concepteurs de circuits puissent tester en simulation leurs solutions pour augmenter la robustesse des portes CMOS aux attaques laser avec un bon niveau de confiance.

II.1 Jonction PN sous stimulation photoélectrique laser

II.1.1 Étude de la jonction PN N+/Psubstrat

Afin de commencer le processus de modélisation des effets du laser sur les transistors MOS, l'étude se porte en premier lieu sur la jonction PN constituée d'une diffusion dopée N+ gravé sur un substrat de type P: jonction N+/Psub [Sar12], [Lli12(a)]. Cette jonction est l'une des briques de base de la technologie CMOS. En effet un transistor NMOS comporte deux jonctions N+/Psubstrat.

II.1.1.1 Mesure à faible puissance laser continu (I-phemos)

L'I-phemos utilisé pour mener ces travaux, principalement utilisé dans le domaine de l'analyse de défaillance, délivre une puissance laser maximale d'environ 40 mW, à une longueur d'onde de 1064 nm. L'illumination laser se fait en face arrière du composant et de manière continue.

II.1.1.1.1 Laser centré sur la diode

Dans cette première partie, le faisceau laser est centré en plein milieu de la jonction PN étudiée. Le circuit de test utilisé pour cette mesure est une diode formée par une diffusion N+ sur un substrat de type P, polarisé par un anneau de diffusion P+, d'une taille W=L=14 µm, embarquée sur une structure de test réalisé en technologie CMOS STMicroelectronics de 90 nm. La série de tests a été faite en utilisant un objectif d'un grossissement de 20 X, qui délivre une taille de spot de 3,25 µm. Le faisceau laser est centré en plein milieu de la diode, la focalisation étant faite sur la zone active (***Figure II. 1***). La puissance laser à la sortie de l'objectif est ajustable entre 0 et 40 mW. Les principales conditions de test sont explicitées à la ***Figure II. 1***. Le spot rouge représente la position du faisceau laser par rapport au layout de la structure.

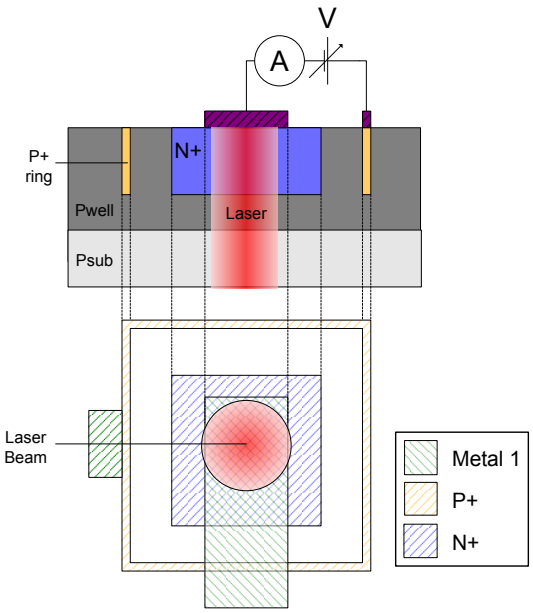


Figure II. 1. Localisation du faisceau laser par rapport au layout de la jonction N+ sur un substrat de type P.

Les caractéristiques courant-tension sont données ***Figure II. 2*** pour différentes puissances laser (allant de 0 à 35 mW). Un fort photocourant a été mesuré lorsque la jonction PN était polarisée en inverse. L'amplitude du photocourant augmente avec la puissance du laser : par exemple, environ 10 µA à 5 mW, 30 µA à 14 mW et 100 µA à 35 mW (pour une tension inverse de 1 V). Dans ces conditions, plus la jonction PN est polarisée en inverse et plus la ZCE est large générant ainsi un plus fort photocourant. De

plus aux faibles puissances laser produites par cet équipement, pour une puissance laser donnée, les variations de polarisation inverse de la diode influent de manière quasi négligeable sur le photocourant. Quoi qu'il en soit, lorsque la diode est polarisée en direct (au-dessus de sa tension seuil vers ~0,7 V) la largeur de la zone de charge d'espace se trouve amincie et le photocourant devient faible en comparaison avec le courant direct de la diode [Glo10].

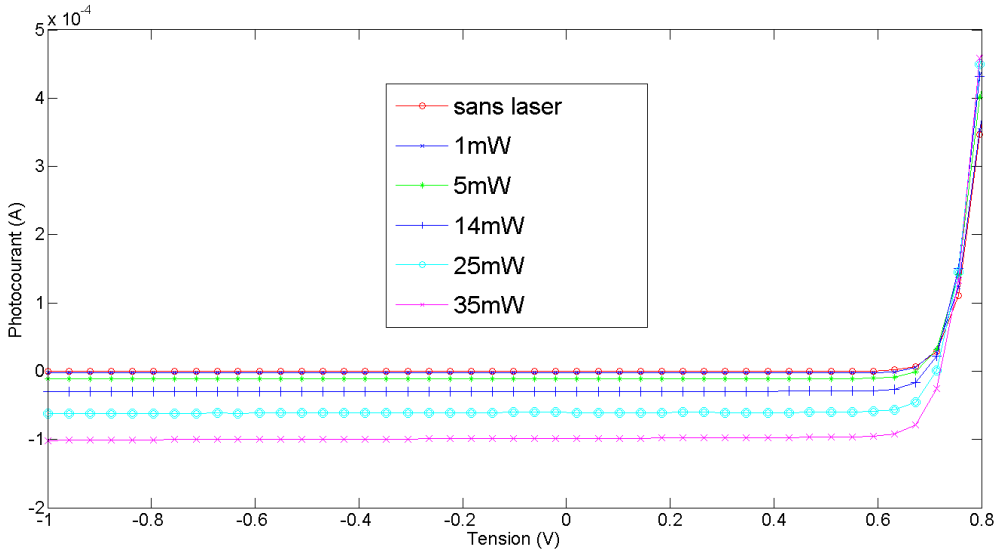


Figure II. 2. Caractéristique courant-tension I(V) mesurée d'une jonction PN sous Stimulation Photoélectrique Laser pour différentes puissances laser.

Les résultats précédents ont été corrélés avec les résultats obtenus en simulation TCAD. La ***Figure II. 3*** montre la structure TCAD [Min06] utilisée pour faire la corrélation avec les résultats obtenus en mesure (***Figure II. 2***). Cette jonction N+/Psub a été isolée à partir d'un transistor NMOS.

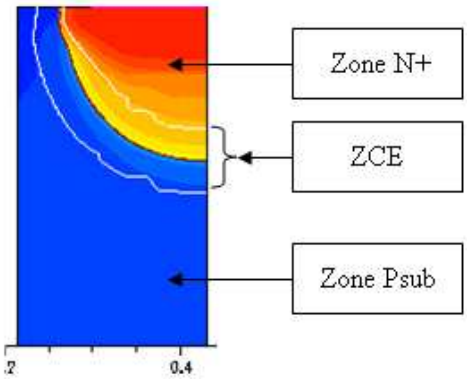


Figure II. 3. Coupe TCAD d'une jonction N+/Psub.

La caractéristique courant-tension à différentes puissances laser, a été effectuée en simulation (voir ***Figure II. 4***). Les résultats de simulation TCAD sont qualitatifs et non quantitatifs car la simulation n'est pas calibrée. Toutefois, une bonne cohérence a été obtenue avec la mesure pratique (voir ***Figure II. 2***).

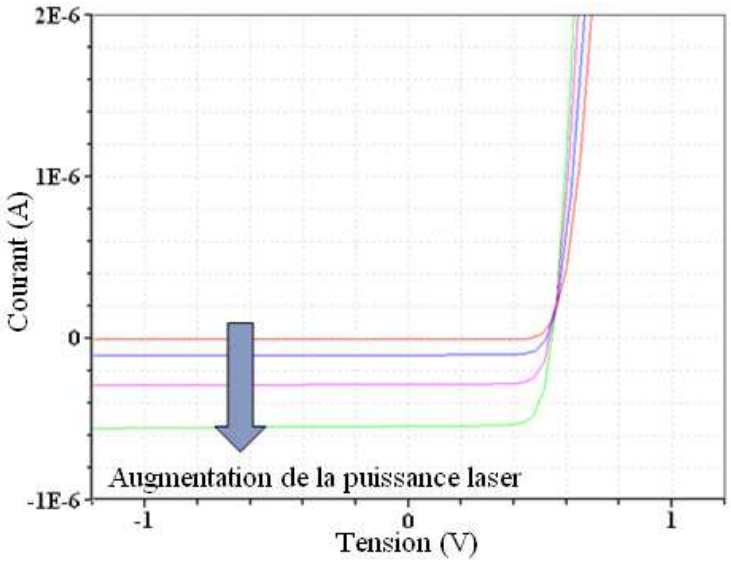


Figure II. 4. Caractéristique courant-tension I(V) extraite de simulation TCAD d'une jonction PN sous Stimulation Photoélectrique Laser pour différentes puissances laser.

Les mesures expérimentales réalisées permettent de modéliser l'effet de la Stimulation Photoélectrique Laser (SPL) continue d'une jonction PN polarisée en inverse par une source de courant dont la valeur nominale de courant est définie par :

$$I_{ph} = S \times I_{laser} \qquad \textbf{Eq. II. 1}$$

$$I_{LASER} = 0.0323 \times P_{LASER}{}^{2} + 0.03335 \times P_{LASER} - 0.1624 \qquad \textbf{Eq. II. 2}$$

I_{LASER} est le photocourant généré en simulation par unité de surface et exprimé en ($A/\mu m^2$).

S est la surface de la jonction PN en (μm^2).

Et P_{laser} la puissance du laser exprimée en W.

Il est à préciser que la calibration de l'***Eq. II. 2*** a été faite à partir des mesures et non à partir des simulations TCAD.

Il faut s'intéresser principalement à une polarisation en inverse d'une jonction PN, puisque dans le fonctionnement d'une porte CMOS, toutes les jonctions sont dans cette configuration.

II.1.1.1.2 Dépendance spatial

La distance entre le spot laser et la jonction PN a un fort impact sur la valeur du photocourant généré.

En effet, lorsque le faisceau laser est centré sur la jonction PN (drain/Psub d'un transistor NMOS), le photocourant est maximum, et plus le faisceau laser s'éloigne dans le plan de la jonction PN, plus le photocourant diminue (***Figure II. 5***).

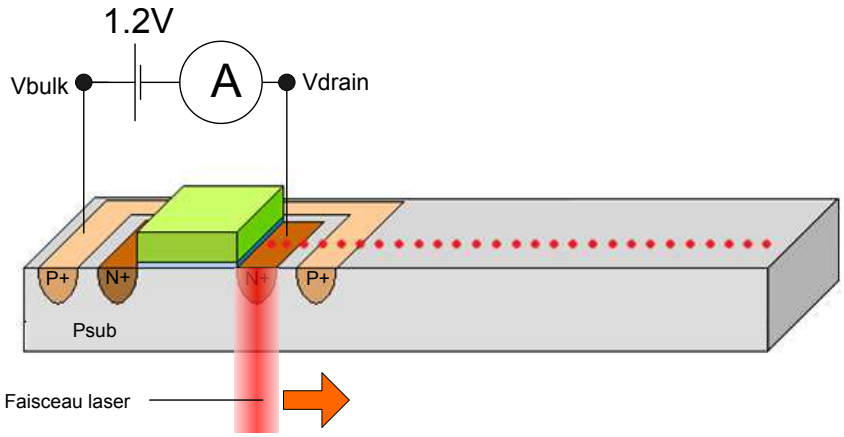


Figure II. 5. Présentation schématique de l'expérience réalisée dans le but d'évaluer l'effet spatial du laser sur une jonction PN.

Dans le but de modéliser la dépendance spatiale du laser sur le silicium, une diode drain/Psub (N+/Psub), d'un transistor NMOS canal long (W=L=10 µm) a été utilisée. La structure de test est embarquée sur un wafer d'une technologie STMicroelectronics de 90 nm sans aucunes autres structures polarisés. Les mesures ont été faites avec le drain polarisé à 1,2 V, le substrat de type P connecté à la masse, et les deux autres électrodes du transistor MOS (Grille et source) laissées flottantes.

Le spot laser a été déplacé suivant une ligne allant du centre de la jonction PN jusqu'à 300 µm de distance avec un pas de 1,5 µm (voir ***Figure II. 5***). Pour chaque déplacement le photocourant a été mesuré. Cette expérience a été faite avec les trois objectifs différents de l'I-phemos (2,5 X, 20 X, et 50 X) donnant respectivement des tailles de spot de 1,7 µm, 3,25 µm et 13 µm. Le photocourant mesuré en fonction de la distance est présenté ***Figure II. 6*** après normalisation par rapport au photocourant maximum. Le photocourant maximum est obtenu lorsque le faisceau laser est centré en plein milieu de la jonction drain/bulk. Cette courbe à un profil gaussien.

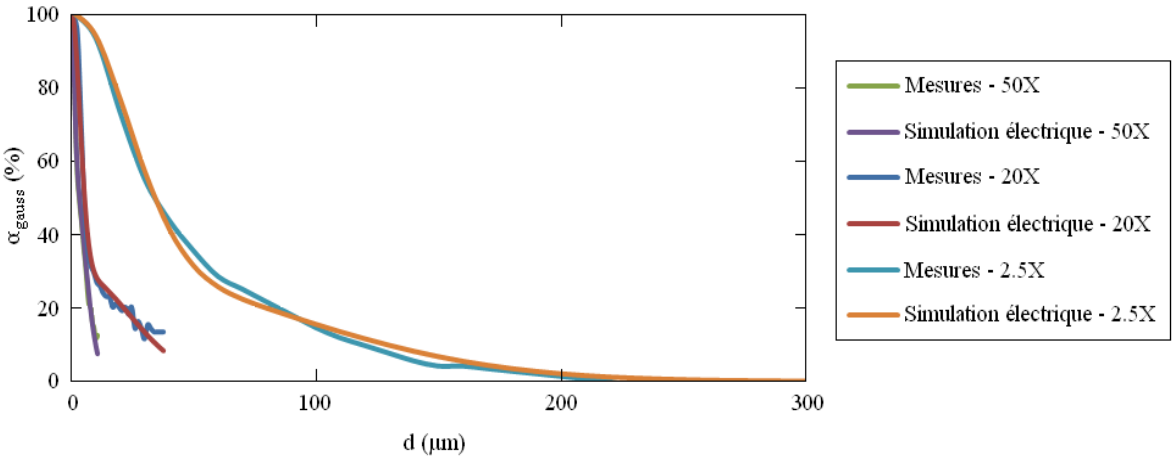


Figure II. 6. Courant photoélectrique généré par la diode drain/bulk polarisé à 1.2 V en inverse en fonction de la distance entre le spot laser et le centre de la jonction pour les différents objectifs de l'I-phemos.

A partir du graphique présenté ***Figure II.* 6** il est possible d'extraire un modèle mathématique basé sur la somme de deux fonctions gaussiennes dont le coefficient est appelé α_{gauss} (***Eq. II. 3***), où d est la distance entre le centre du spot laser et le centre de la jonction PN exprimée en micromètre.

$$\alpha_{gauss}(d) = \beta \times \exp\left(-\frac{d^2}{c_1}\right) + \gamma \times \exp\left(-\frac{d^2}{c_2}\right) \qquad \textbf{Eq. II. 3}$$

Pour chaque objectif de l'I-Phemos, les coefficients β, γ, c_1 et c_2 sont différents (voir ***Tableau II. 1***).

	2.5X	**20X**	**50X**
β	0.4	0.6	0.7
γ	0.6	0.4	0.3
c_1	2.5	23.8	1000
c_2	55	654	15000

Tableau II. 1. Coefficients de la fonction Gaussienne (Eq. II. 3) pour les différents objectifs de l'I-phemos étudié sur la jonction PN drain/Psubstrat.

L'équation ***Eq. II. 4*** donnant la valeur du courant photoélectrique créé au niveau de la jonction PN lorsque le spot laser est distant de *d* est obtenue après la multiplication de l'équation ***Eq. II. 1*** et du coefficient α_{gauss} :

$$Iph\_val = S \times I_{laser} \times \alpha_{gauss} \qquad \textbf{Eq. II. 4}$$

Comme le montre la figure ***Figure II. 6***, grâce à l'équation ***Eq. II. 3*** une bonne corrélation est obtenue entre la mesure et la modélisation.

II.1.1.2 Mesures à forte puissance laser pulsé

II.1.1.2.1 Modélisation électrique

L'étude de la diode N+/Psubstrat lorsque la puissance du laser est plus forte qu'aux paragraphes précédents est une étape nécessaire dans la compréhension des phénomènes mis en œuvre lors de l'illumination de la face arrière d'un transistor NMOS par des illuminations à caractère impulsionnel d'une durée supérieure à 50 ns.

Le circuit pour ce test est le même qu'au paragraphe précédent (jonction drain/Psubstrat d'un transistor NMOS de taille W=L=10 µm en technologie 90 nm. A partir de ces mesures il est possible de modéliser le photocourant I_{ph} induit par une impulsion laser passant sur une jonction PN polarisée en inverse par une fonction polynomiale d'ordre 2 (***Eq. II. 5***).

Dans la partie précédente, I_{ph} représentait la valeur nominale du photocourant qui était généré de manière continue. Dans cette partie, I_{ph} représente la valeur de l'amplitude maximale du photocourant durant l'impulsion laser.

$$I_{ph} = (a \times V + b) \times \alpha_{gauss} \times S \qquad \textbf{Eq. II. 5}$$

S est la surface de la jonction PN illuminée par le laser exprimé en µm².

α_{gauss} est le paramètre de dépendance spatial défini au paragraphe précédent, et *a* et *b* sont des fonctions dépendant de la puissance du laser P_{laser}:

$$a = 4.10^{-9} \times P_{laser}^2 - 5.10^{-7} \times P_{laser} + 9.10^{-6} \qquad \textbf{Eq. II. 6}$$

$$b = 4.10^{-6} \times P_{laser} \qquad \textbf{Eq. II. 7}$$

Un sous-circuit présenté ***Figure II. 7*** construit avec une source de courant contrôlée en tension est utilisé pour modéliser le photocourant.

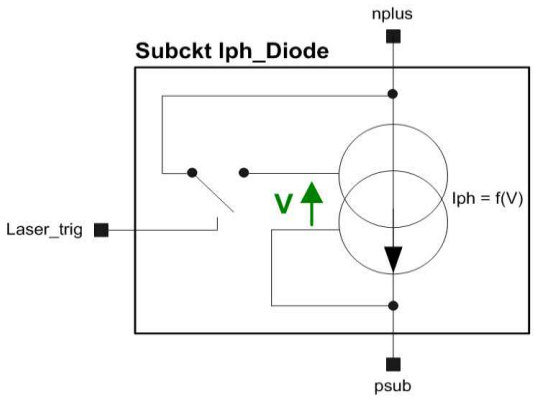


Figure II. 7. Représentation symbolique du modèle électrique d'une jonction PN sous stimulation photoélectrique laser impulsionnelle.

Ainsi le photocourant simulé par la présence de la source de courant contrôlée en tension dépend de la polarisation appliquée aux bornes de la diode. De plus le signal d'entrée *laser_trig*, de forme double exponentielle, présent sur le schéma ***Figure II. 7*** permet à l'utilisateur de décider à quel moment temporel il souhaite exécuter son tir laser dans sa simulation électrique. La forme de ce signal (double exponentiel [Bar07]) est utilisée pour modéliser au mieux la forme du courant impulsionnel généré par une jonction PN.

La ***Figure II. 8***, représente la comparaison entre mesures et simulations de l'amplitude du photocourant de la jonction N+/Psubstrat en fonction de la polarisation en inverse (à différentes puissances laser). Une très bonne corrélation entre simulations électriques et mesures est obtenue.

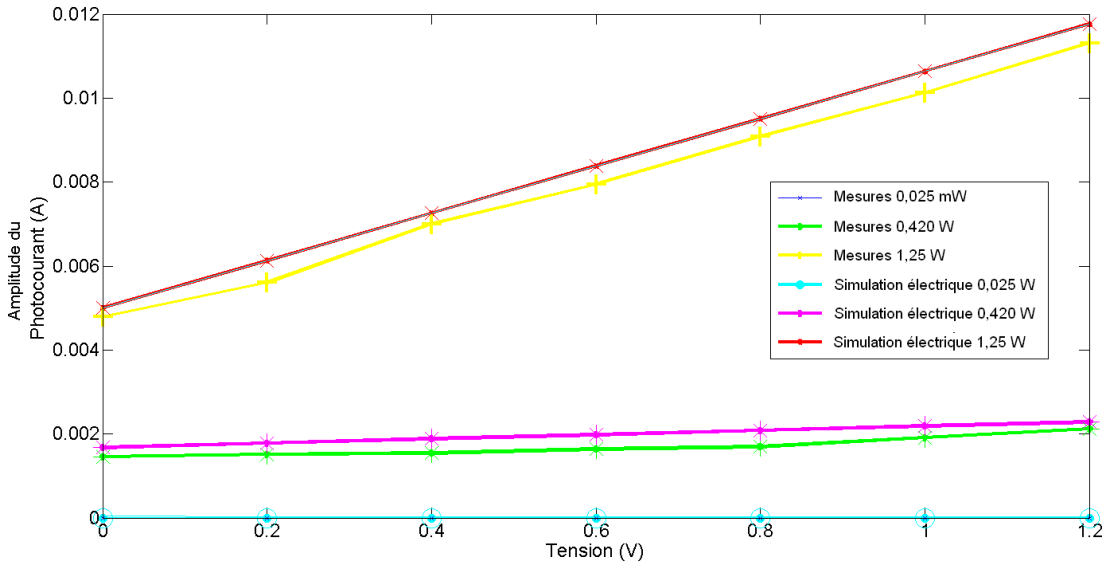


Figure II. 8. Comparaison entre caractéristiques courant-tension I(V) mesurée et simulée pour différentes puissances laser de la jonction PN N+/Psubstrat.

Dans la suite il est proposé d'étudier l'influence de paramètres comme la focalisation du faisceau laser ou bien l'épaisseur de silicium sur le photocourant généré par une jonction PN N+/Psubstrat (drain/bulk) d'un transistor NMOS W=L=10 µm. Pour toutes les mesures qui vont suivre, les conditions expérimentales suivantes sont appliquées: le drain est porté au potentiel de 1,2 V, le substrat de type P est connecté à la masse, et les autres électrodes sont laissées flottantes. Le spot laser est de 5 µm, et la puissance de 1,25 W. Ces études permettront d'inclure les dépendances concernant l'épaisseur de silicium, la modification du cône du faisceau laser par déplacement de l'axe *z*, ainsi que la durée de l'illumination laser, sur la modélisation du photocourant d'une jonction PN. De plus, comme pour la modélisation faite du laser continu, la distance entre le spot laser et la jonction PN est prise en compte grâce au coefficient α_{gauss} présenté à l'***Eq. II. 3***.

II.1.1.2.2 Effet de la durée de l'impulsion laser

La durée de l'impulsion laser à des puissances variant de 0 à 1,25 W, a une influence sur le photocourant généré par une jonction PN, surtout pour des durées d'impulsions inférieure à la centaine de ns. La ***Figure II. 9*** présente les photocourants générés par la jonction N+/Psubstrat, pour différentes durées d'impulsions. Lorsque la durée d'impulsion

est inférieure à 500 ns, le photocourant n'atteint pas un régime stationnaire. Les charges générées par le laser n'ont pas le temps d'être collectées par les prises N+ et P+.

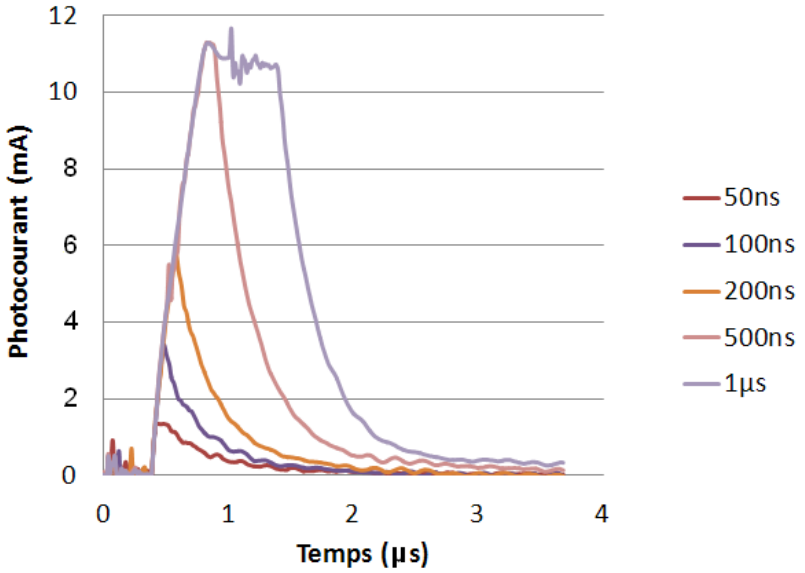


Figure II. 9. Photocourant de la jonction N+/Psub en fonction du temps pour différentes durées d'impulsion.

Le graphique ci-dessous présente le photocourant normalisé en fonction de la durée d'impulsion du tir laser extrait de la ***Figure II. 9***.

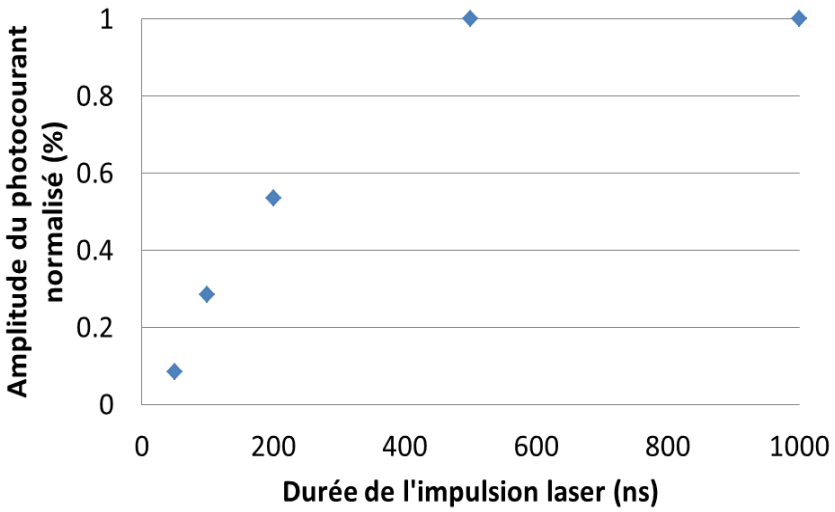


Figure II. 10. Amplitude du photocourant de la jonction N+/Psub normalisé en fonction de la durée d'impulsion.

Les mesures présentées ci-dessus peuvent être approximées par la fonction suivante :

$$Pulse_{width} = 1 - \exp\left(-\frac{w}{250E^{-9}}\right) \qquad \textit{Eq. II. 8}$$

w est la durée de l'impulsion laser exprimé en seconde.

Ainsi, l'équation, qui incorpore la dépendance de la durée de l'impulsion laser, est obtenue en multipliant les équations ***Eq. II. 5*** et ***Eq. II. 11*** pour aboutir à l'équation ***Eq. II. 9.***

$$I_{ph} = (a \times V + b) \times S \times \alpha_{gauss} \times Pulse_{width} \qquad \textit{Eq. II. 10}$$

II.1.1.2.3 Effet de l'épaisseur du Wafer

L'épaisseur du substrat, pour une injection laser en face arrière, à un effet non négligeable sur la génération du photocourant d'une jonction PN sous SPL [Pou00(a)]. L'intensité lumineuse décroît de manière exponentielle au travers du matériau. Il en est aussi de même pour le photocourant généré. Ainsi, plus l'épaisseur du wafer est grande et plus le photocourant généré par la jonction sous SPL sera faible.

Dans le but d'illustrer cet effet, les photocourants d'une jonction PN (drain/Psubstrat d'un transistor NMOS) ont été mesurés sur des échantillons lors d'une exposition à une SPL. Cette mesure est reportée ***Figure II. 11***. Pendant ces expériences, le faisceau laser était centré sur la jonction de drain, avec une durée d'impulsion fixée à 20 µs.

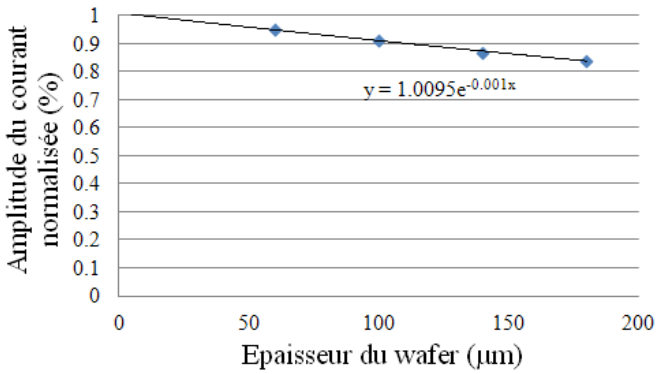


Figure II. 11. Photocourant normalisé dans une jonction PN en fonction de l'épaisseur du wafer.

Il est ainsi possible de modéliser l'effet de l'épaisseur du wafer sur le photocourant grâce à l'équation ***Eq. II. 11***:

$$W_{coef} = e^{-\frac{Wafer_{thickness}}{1000}} \qquad \textit{Eq. II. 11}$$

Où $Wafer_{thickness}$ représente l'épaisseur du wafer exprimée en µm.

Ainsi, l'équation, qui incorpore la dépendance de l'épaisseur du wafer, est obtenue en multipliant les équations ***Eq. II. 5*** et ***Eq. II. 11*** pour aboutir à l'équation ***Eq. II.*** 12.

$$I_{ph} = (a \times V + b) \times S \times \alpha_{gauss} \times Pulse_{width} \times W_{coef} \qquad \textit{Eq. II. 12}$$

L'expression complète du photocourant est donc donnée par l'équation ***Eq. II.*** 12.

De plus, les résultats théoriques présentés au chapitre I sont bien corrélés puisque l'équation ***Eq. II.*** 12 est de type *exp(-αz)* (voir ***chapitre I.3.2.2.1***).

II.1.1.2.4 Effet de la focalisation du faisceau laser

Le déplacement de l'objectif du laser selon l'axe vertical *z*, modifiant la focalisation du faisceau, a une influence sur le photocourant généré par une jonction PN. Par convention,

lorsque l'axe *z* est en position 0, le plan focal était confondu avec la zone active de la jonction PN. La ***Figure II. 12*** représente le photocourant normalisé induit dans la jonction PN en fonction du déplacement selon l'axe *z*.

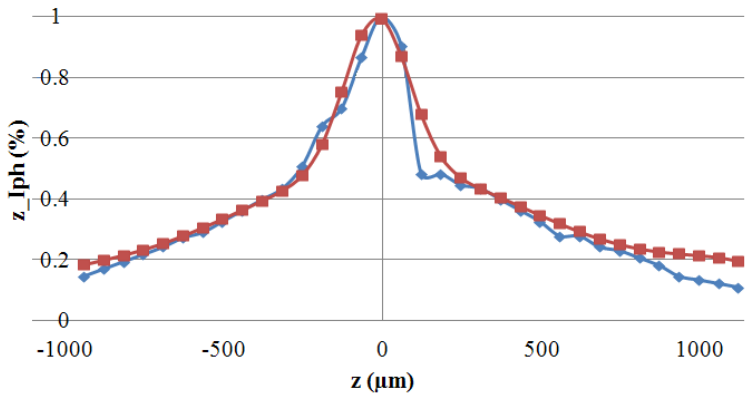


Figure II. 12. Photocourant normalisé généré par une jonction PN en fonction du déplacement de l'objectif du laser selon l'axe *z* qui modifie la focalisation du faisceau.

Une approximation de la courbe présentée ***Figure II. 12*** est faite grâce à l'équation ***Eq. II. 13***:

$$Iph\_z = \left(c \times z^6 + d \times z^5 + e \times z^4 + f \times z^3 + g \times z^2 + h \times z + i\right) \times \left(j \times e^{-\frac{z^2}{20000}}\right) \qquad \textit{Eq. II. 13}$$

Où les coefficients *c*, *d*, *e*, *f*, *g*, *h*, *i*, et *j* sont donnés dans le ***Tableau II.*** 2. L'équation ***Eq. II. 13*** qui est notamment constituée d'un polynôme d'ordre 6, a été utilisée pour modéliser au mieux l'effet de la focalisation. Dans la pratique d'autres fonctions mathématiques auraient pu être utilisées.

Coefficients	Valeurs
c	-3E-19
d	-9E-17
e	-8E-13
f	2E-10
g	-8E-7
h	-1E-4
i	0,49
j	0,5

Tableau II. 2. Coefficients de l'équation Eq. II. 13 qui régissent la modélisation de l'effet du focus.

Le coefficient *Iph_z*, qui tient compte de la focalisation du faisceau laser réalisé par le déplacement de l'axe *z* de l'objectif du laser, est utilisé pour modifier l'équation ***Eq. II.*** 12 en la multipliant par le coefficient *Iph_z* ***(Eq. II. 14)***:

$$I_{ph} = (a \times V + b) \times \alpha_{gauss} \times Pulse_{width} \times W_{coef} \times Iph\_z \qquad \textbf{Eq. II. 14}$$

Ainsi notre modèle de jonction PN (N+/Psubstrat) sous SPL pulsé tient compte de la position du faisceau laser par rapport à la topologie de la jonction, de l'épaisseur du wafer et de la focalisation du faisceau laser. Ces étapes de modélisation vont être utiles pour modéliser une jonction P+/Nwell, puisque le même principe va être appliqué pour cette jonction constitutive d'un transistor PMOS.

II.1.2 Etude de la jonction P+/Nwell

Toutes les étapes de mesures et de modélisations présentées pour la jonction N+/Psubstrat ont été également réalisées pour la jonction P+/Nwell, ce qui permettra de modéliser les effets du laser sur un transistor PMOS, puisqu'il comporte deux jonctions P+/Nwell. Afin d'étudier uniquement l'influence de la jonction PN P+/Nwell, la polarisation suivante a été réalisée : le caisson de type N était porté à la polarisation de 1,2 V, la tension de l'implant P+ variée de 0 à 1,2 V, et le substrat de type P était laissé flottant. Ces conditions de polarisation permettent de s'affranchir de l'effet de la jonction Nwell/Psub. Une vue en coupe d'une jonction P+/Nwell sur un substrat de type P est présentée ***Figure II. 13***. De manière générale les mesures ont été réalisées de la même manière que pour la jonction N+/Psub.

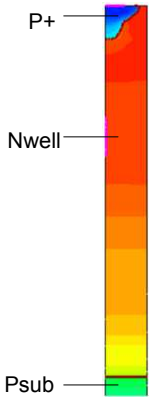


Figure II. 13. Structure TCAD de la jonction P+/Nwell d'un transistor PMOS.

Les caractéristiques courant-tension sous stimulation photoélectrique laser impulsionnel mesurées et celles obtenues par simulation sont présentées ***Figure II. 14***. Ce graphique montre, au niveau de l'amplitude maximale du photocourant généré, une bonne corrélation entre mesure et simulation.

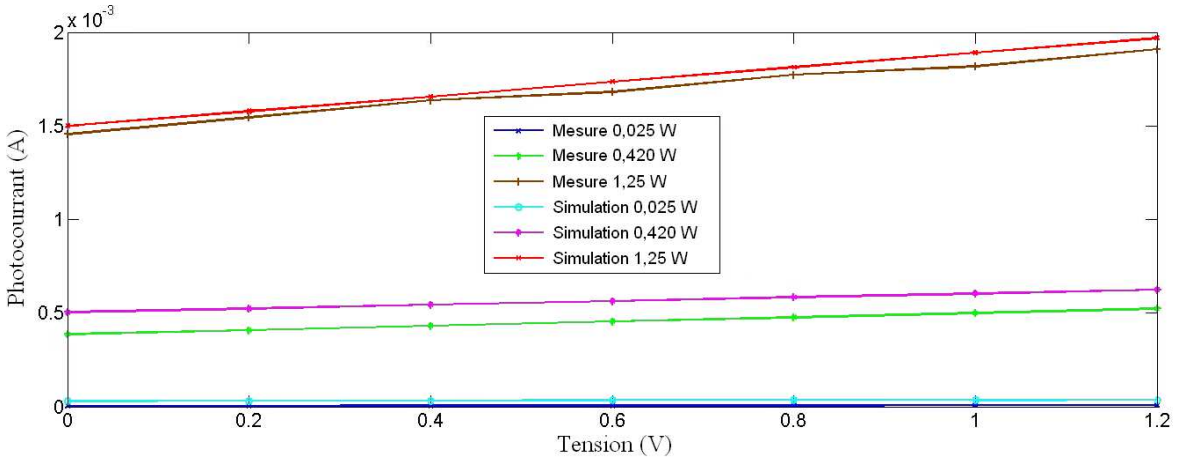


Figure II. 14. Comparaison entre les caractéristiques courant-tension I(V) mesurées et simulées de la jonction PN P+/Nwell pour différentes puissances laser.

De plus, il est possible de noter que la caractéristique courant-tension de la jonction P+/Nwell pour différentes puissances laser (***Figure II. 14***) à la même allure que celle de la jonction N+/Pwell (***Figure II. 8***). Toutefois, il est possible de remarquer que la jonction N+/Psub d'un transistor NMOS génère un photocourant de 12 mA pour une puissance de 1,25 W. Ce photocourant est, dans ces conditions, beaucoup plus important que la jonction

P+/Nwell (environ 2 mA). Ceci peut s'expliquer par les différences de dopage entre les caissons de type N et ceux de type P, ainsi que par l'interface optique supplémentaire créée par la jonction Nwell/Psubstrat. Dans le cas où le substrat P est connecté à la masse, le mécanisme de collection de charge est différent. Ainsi, le photocourant généré par les jonctions P+/Nwell est réduit. Ce phénomène sera étudié lorsque l'étude du transistor PMOS sera faite (voir ***paragraphe II.2.2.2.2***).

II.1.3 Etude de la jonction Nwell/Psubstrat

L'étude de la jonction Nwell/Psubstrat est une étape capitale pour modéliser un transistor PMOS sous Stimulation Photoélectrique Laser. En effet, c'est bien évidemment la jonction PN ayant la surface la plus importante. La mesure a été réalisée avec le laser impulsionnel forte puissance. La ***Figure II. 15*** présente le layout d'un transistor PMOS W=L=10 µm. La prise de polarisation du Pwell et par conséquent du Psub est localisée à 80 µm de distance de la jonction Nwell/Psub. C'est la prise Psub, la plus proche du transistor PMOS étudié, utilisée pour polariser le substrat de type P à la masse. Comme le montre le spot laser sur la ***Figure II. 15***, le faisceau était centré en plein milieu du transistor, afin de faire réaliser une caractéristique courant-tension à différentes puissances laser (voir ***Figure II. 16***).

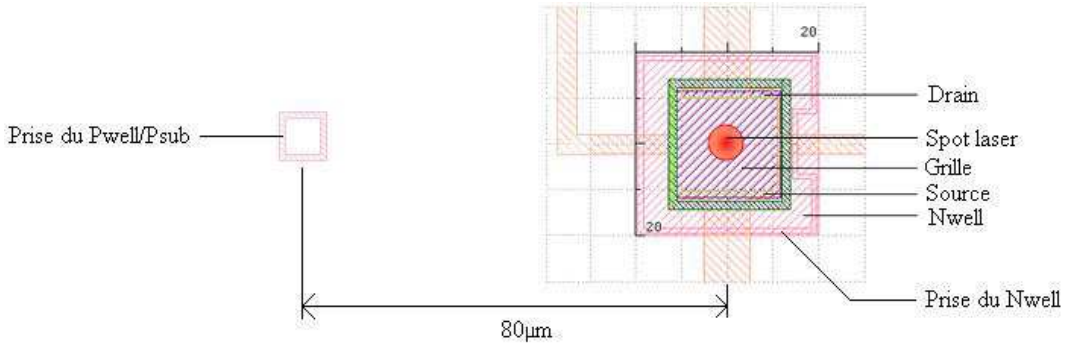


Figure II. 15. Layout du transistor PMOS de taille W=L= 10µm.

Les conditions de polarisation suivantes ont été appliquées sur le transistor PMOS: le Nwell était polarisé à une tension variable évoluant de 0 à 1,2 V et le substrat de type P était connecté à la masse. Les autres électrodes du transistor PMOS sont laissées flottantes. La

durée d'impulsion du laser était de 20 µs, et la taille de spot de 5 µm de diamètre. La ***Figure II. 16*** présente l'amplitude maximale du photocourant généré par la jonction Nwell/Psub en fonction de la tension en inverse de la jonction à différentes puissances laser.

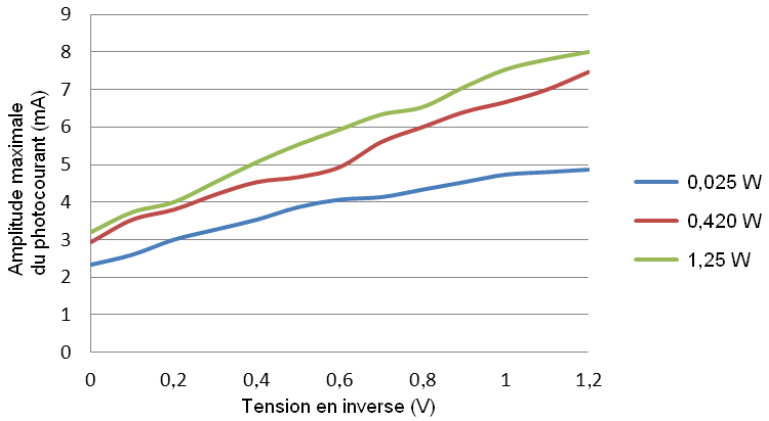


Figure II. 16. Caractéristique courant-tension I(V) de la jonction PN Psubstrat/Nwell pour différentes puissances laser.

Il est possible de remarquer que la puissance laser n'a pas d'effet très important sur la génération du photocourant en fonction de la polarisation en inverse de la jonction Nwell/Psub puisqu'une différence de la puissance laser d'environ 1,25 W génère une différence de photocourant d'environ 3 mA.

II.1.4 Effet de l'implant deep Nwell sur la jonction N+/Psubstrat

Dans cette partie, l'effet de l'implant deep Nwell sur les jonctions PN N+/Pwell et Nwell/Psub est étudié, dans l'optique de pouvoir voir l'effet de cet implant sur des portes CMOS.

Comme le montre la coupe TCAD présentée ***Figure II. 17*** , l'implant deep Nwell isole le caisson de type P (Pwell) du substrat P (b).

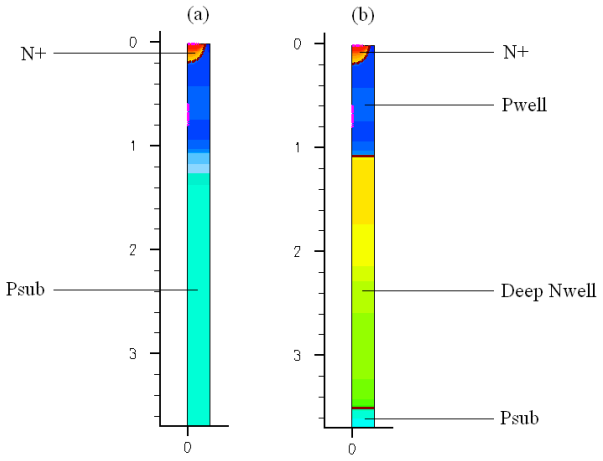


Figure II. 17. Coupe TCAD d'une jonction N+/Psub avec (a) et sans implant deep Nwell (b).

La présence ou l'absence de l'implant deep Nwell modifie la génération du photocourant de la jonction N+/Pwell. Dans un premier temps, le photocourant généré par la jonction N+/Pwell d'un transistor NMOS W=L= 10 µm sur implant Deep Nwell a été mesuré. La polarisation suivante a été réalisée : le N+ est polarisé à une tension variable de 0 à 1,2 V et le Pwell qui est également relié au substrat de type P est connecté à la masse. Le deep Nwell est, laissé flottant. La caractéristique courant-tension I(V) pour différentes puissances laser est présentée ***Figure II. 18***.

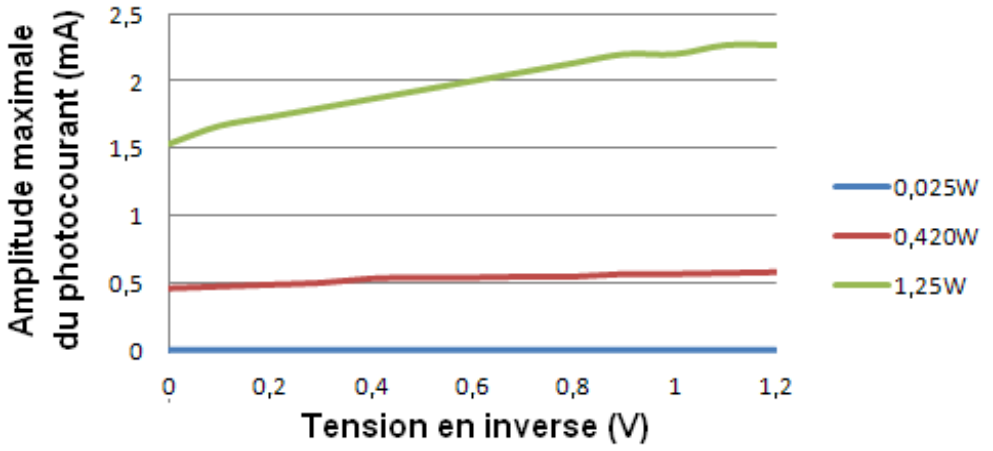


Figure II. 18. Caractéristique courant-tension de la jonction N+/Pwell d'un transistor NMOS avec implant deep Nwell laissé flottant.

La caractéristique courant-tension pour différentes puissances laser de la jonction N+/Pwell d'un transistor NMOS avec implant deep Nwell laissé flottant est très proche de celle d'un transistor NMOS sans implant entouré de type N. Sans cet implant, il a été vu à la ***Figure II. 4*** que la jonction N+/Psub lorsque la polarisation en inverse est de 1,2 V, pour une puissance laser de 1,25 W et une taille de spot de 5 µm, génère un photocourant de 12 mA. La diminution du photocourant généré lorsqu'un implant deep Nwell est ajouté sous un transistor NMOS est inférieure à -5 %. Cela signifie que l'implant deep Nwell, créant une interface optique supplémentaire à l'onde lumineuse laser arrivant en face arrière du composant, a une influence très faible sur la diminution du photocourant généré par une jonction N+/Pwell.

Dans un second temps, l'implant deep Nwell est polarisé à 1,2 V. La ***Figure II. 19*** présente la caractéristique courant-tension de la jonction N+/Pwell dans cette configuration.

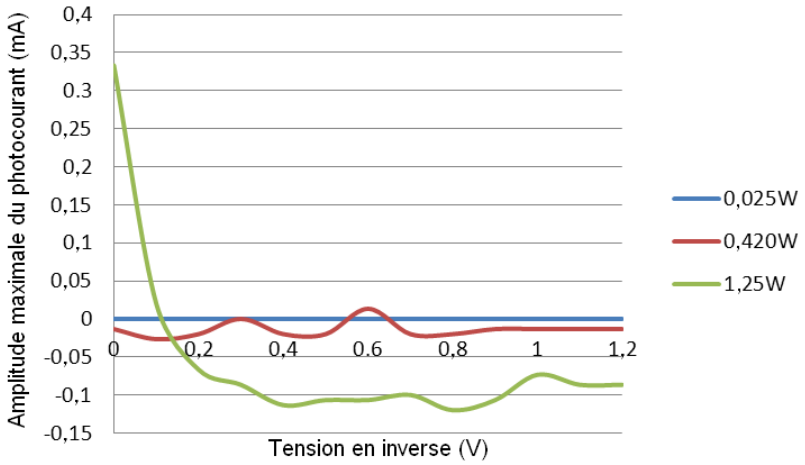


Figure II. 19. Caractéristique courant-tension de la jonction N+/Pwell d'un transistor NMOS avec implant deep Nwell polarisé à 1,2 V.

Lorsque le deep Nwell est polarisé à 1,2 V, c'est-à-dire dans les conditions normales de fonctionnement, le photocourant généré par la jonction N+/Pwell est fortement diminué (d'un facteur environ égal à 25). Ceci s'explique par un mécanisme de collection de charge différent lorsque l'implant deep Nwell est polarisé ou non. En effet dans ce cas de figure la majorité des paires électrons-trous sont générés par la jonction deep Nwell/Psub. Il y'a donc une compétition entre les deux.

II.2 Transistor MOS sous illumination laser

II.2.1 Transistor NMOS

II.2.1.1 Mesure et modèle électriques à faible puissance laser continu (I-phemos)

II.2.1.1.1 Présentation du modèle électrique

Après l'étape de calibration des sous circuits modélisant une jonction PN sous PLS, il est possible de modéliser un transistor NMOS en technologie 90 nm sous illumination laser en tenant compte de sa topologie [Lli12(a)], [Sar12(b)]. Sur les quatre électrodes du transistor NMOS deux sous-circuits modélisant les jonctions N+/Psubstrat sous illumination laser sont connectés respectivement aux nœuds de drain et de source (voir ***Figure II. 20***).

Lorsque l'utilisateur simule, en créant une netlist, il appelle ces deux sous-circuits dans la netlist principale, pour chaque jonction (drain/Psubstrat et source/Psubstrat) il doit définir deux paramètres: la valeur de *S* (aire de la jonction), et celle de *d* la plus courte distance entre le centre du spot laser et le centre de la jonction PN. C'est cette valeur de distance qui sert aux simulations pour tenir compte de l'aspect du transistor par rapport au déplacement du faisceau laser.

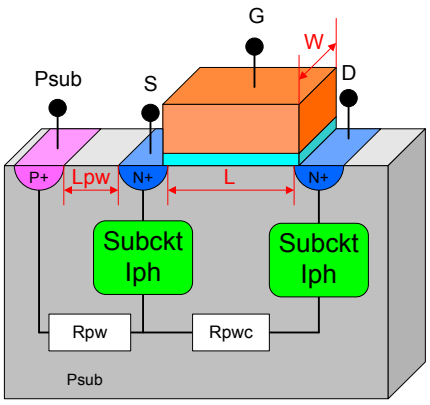


Figure II. 20. Principe de la modélisation électrique Spice d'un transistor NMOS sous stimulation photoélectrique laser continue à faible puissance.

Les valeurs des deux résistances présentes dans le modèle ***Figure II. 20*** sont définies de la manière suivante avec les paramètres géométriques L, L_{pw} et W en micromètres :

$$R_{pwc} = R_{pw}^{\square} \times \frac{L}{W} \qquad \textit{Eq. II. 15}$$

$$R_{pw} = R_{pw}^{\square} \times \frac{L_{pw}}{W} \qquad \textit{Eq. II. 16}$$

Où $R_{pw}^{\square}$ est la valeur de la résistance du substrat de type P par carré.

Ces résistances modélisent le chemin résistif que le photocourant doit parcourir pour atteindre les prises de polarisation du substrat de type P.

Ainsi le modèle prend en compte les dimensions géométriques du transistor NMOS, la position du faisceau laser par rapport à son layout, ainsi que sa polarisation.

II.2.1.1.2 Comparaison entre le modèle électrique et les mesures

Ce modèle permet donc de simuler électriquement l'effet du laser sur un transistor NMOS en technologie 90 nm, et de faire de nombreuses variations sur les paramètres inhérents au laser, comme sa puissance ou la position du faisceau par rapport au transistor, ou sur le diamètre du spot laser (via l'objectif de l'I-phemos choisi). Il est également possible de modifier la polarisation du transistor ainsi que les paramètres géométriques, tels que la dimension du transistor (W et L), et la distance entre les prises P+ et N+, vu ***Figure II. 20***. Ce paragraphe compare les simulations électriques avec les mesures effectuées faite sur le transistor NMOS.

II.2.1.1.2.1 Variation de puissance du laser

Dans le but de montrer l'influence de la puissance laser sur le photocourant, un transistor NMOS W=10 µm/L=0.1 µm est utilisé en mesures ainsi qu'en simulations. Ce transistor NMOS est polarisé de telle manière à ce qu'il soit bloqué (OFF). Le drain est au potentiel de +1,2 V, la source, la grille et le bulk (substrat de type P) sont connectés à la masse.

Les photocourants sur les quatre électrodes du MOS sont mesurés en fonction de la puissance du laser en simulation ainsi qu'en mesures. L'objectif choisi a un grossissement de 20X (ce qui correspond à une taille de spot de 3,25 µm). Il agit au milieu du transistor [Glo10].

Le graphique ***Figure II. 21*** montre la très bonne corrélation entre la simulation électrique et les mesures. Afin de réaliser cette mesure, la puissance du laser variait de 0 à 35 mW.

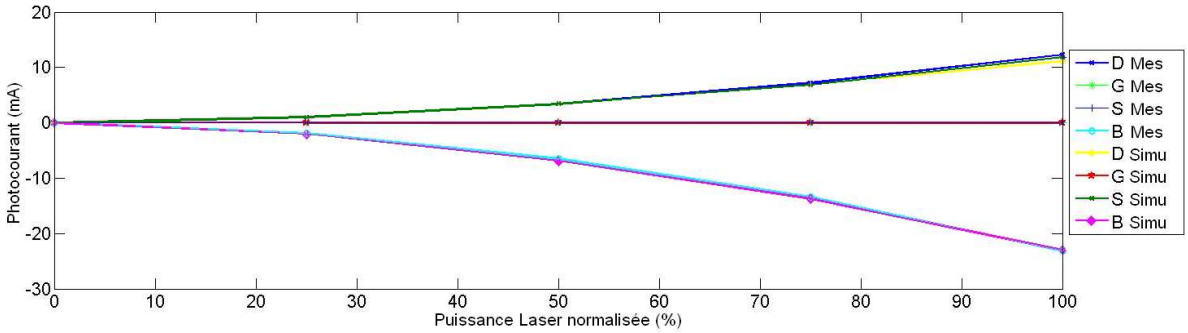


Figure II. 21. Evolution du photocourant mesuré en comparaison des simulations électriques d'un transistor NMOS W=10 µm/L=0,1 µm polarisé de manière à ce qu'il soit bloqué (OFF) en fonction de la puissance du laser.

Les photocourants générés par la source et le drain sont égaux (superposés sur la ***Figure II. 21***). Ceci montre que le spot laser est positionné à équidistance entre les jonctions de drain et de source. De plus, l'équation de conservation des courants ***(Eq. II. 17)*** est respectée quelle que soit la puissance du laser ce qui valide une mesure du courant correcte et montre que le composant n'est pas endommagé [Lli12(a)].

$$|I_{substrate}| = I_{drain} + I_{source} \qquad \textit{Eq. II. 17}$$

Les mesures de photocourant pour différentes longueurs de grille avec les mêmes surfaces de jonction N+/Psubstrat ont été testées dans les mêmes conditions de polarisation. Le transistor NMOS est polarisé de telle manière qu'il soit OFF comme précédemment. La

puissance du laser est choisie à la puissance maximale de l'équipement (40 mW), et le faisceau laser positionné au centre de chaque transistor.

Du fait de la zone de charge d'espace (ZCE) localisée sous la grille, l'aire entre la source et le drain à un impact sur le photocourant généré par les jonctions. Ainsi, le photocourant mesuré est plus fort dans le cas d'un transistor avec une longueur de grille importante que sur les transistors à grille plus courte comme le montre le graphique ***Figure II. 22***.

Il est possible de formuler l'hypothèse qu'une partie de la valeur totale du photocourant collectée par les électrodes de source et de drain provient de la zone de déplétion située sous la grille du transistor NMOS [Lli12(a)].

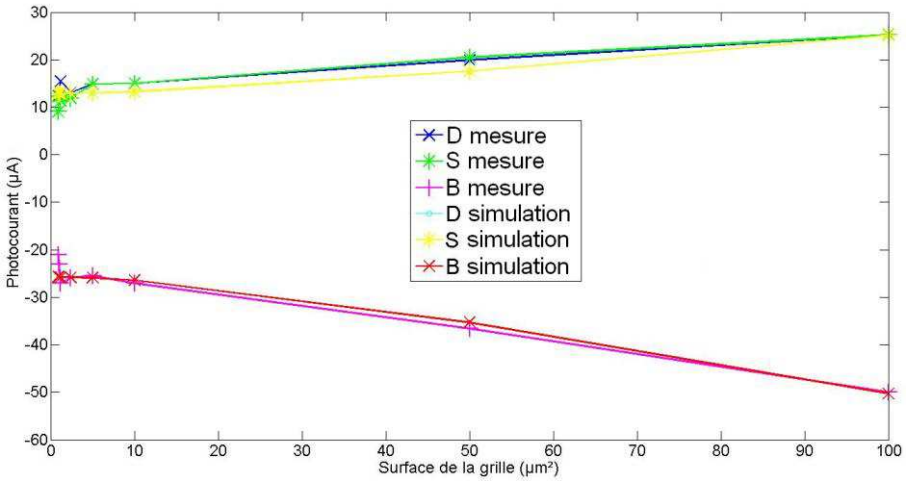


Figure II. 22. Evolution du photocourant en fonction de la taille de la grille.

Il est possible d'extraire une approximation linéaire des courbes présentes sur le graphique de la ***Figure II. 22*** qui est donnée par l'équation ***Eq. II. 18***.

$$Iph\_gate\_approx = 0.1203 \times x + 13.449 \qquad \textbf{Eq. II. 18}$$

Donc un terme additif exprimé par l'équation ***Eq. II. 18*** est ajouté à ***Eq. II. 14*** dans le but de former l'équation ***Eq. II. 19***:

$$Iph\_val = (S \times I_{laser} + Iph\_gate) \times \alpha_{gauss} \qquad \textbf{Eq. II. 19}$$

Iph_gate est une fonction linéaire normalisée proportionnelle à l'aire sous la grille. L'équation ***Eq. II. 20*** est obtenue à partir de l'équation ***Eq. II. 18***.

$$Iph\_gate = \frac{0.1203 \times W \times L}{6} \qquad \textbf{Eq. II. 20}$$

La ***Figure II. 22*** montre que l'effet de la surface de grille est bien pris en compte par le modèle au vu de la très bonne corrélation obtenue entre les mesures électriques et la simulation.

II.2.1.1.2.2 Cartographies en courant d'un transistor NMOS

Le but de dessiner des cartographies montrant le courant est de prédire la réponse correcte d'un circuit et cela indépendamment de la localisation du faisceau laser. Cela peut servir comme référence de base pour détecter certains défauts par comparaison entre la simulation électrique et la mesure, ceci notamment dans le cadre de l'analyse de défaillance.

II.2.1.1.2.3 Principe de la création de cartographies électriques

Le principe de simulation électrique afin de créer des cartographies, réside dans la création d'un maillage fictif sur le layout du transistor. Le pas du maillage est un paramètre d'entrée de la simulation appelé *stepXY* défini dans la netlist ELDO (langage SPICE). Il est nécessaire de calculer en chaque point du maillage deux valeurs de distance. La première est la distance entre le centre du spot laser et le centre de la jonction de drain, et la seconde entre les centres du spot laser et de la source.

Pour illustrer le principe de cartographie, il est possible de prendre un exemple simple sur un transistor NMOS W=L=10 µm. Dans cette étude, trois cas sont envisagés. Le premier lorsque le spot du laser est centré sur la jonction de drain. Le second lorsque le laser est positionné sur la jonction de source, et le troisième cas, lorsque le faisceau est en plein milieu du transistor NMOS (donc à égal distance des jonctions de source et de drain). Pour chacun des cas, les courants de drain, de source et de substrat de type P sont extrait de la simulation électrique (voir ***Figure II. 23***) [Lli12(b)].

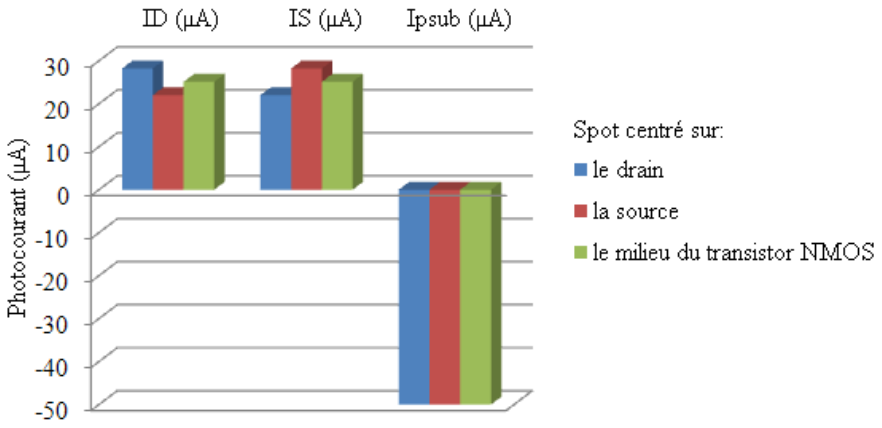


Figure II. 23. Simulation électrique pour différentes localisations du spot laser.

Dans un cas simple comme celui-ci où le maillage est constitué uniquement de trois points alignés, il est possible de définir les paramètres d_d (distance du centre du faisceau laser au centre de la jonction de drain) et d_s (distance du centre du faisceau laser au centre de la jonction de source).

$$d_d = m \times stepXY \qquad \textbf{Eq. II. 21}$$

$$d_s = L - m \times stepXY \qquad \textbf{Eq. II. 22}$$

Dans ce cas d'étude, le paramètre de densité du maillage défini par le *stepXY* est égal à 5 µm, où *m* est un paramètre évoluant entre 0 et 2 par pas de 1. *L* est la longueur de grille du transistor NMOS exprimée en micromètre.

Lorsque le faisceau laser est centré au milieu du drain, le photocourant généré par celui-ci, est plus important que celui de la source. Si le faisceau laser est centré cette fois ci sur la source, c'est maintenant le photocourant généré par celle-ci qui sera plus important que celui généré par le drain. Dans le dernier cas, lorsque le faisceau laser est centré en plein milieu du transistor NMOS, les photocourants générés par la source et le drain sont identiques (***Eq. II. 23***).

$$I_{PSUB} = 2 \times I_S = 2 \times I_D \qquad \textbf{Eq. II. 23}$$

Sur le même principe, il est possible de créer des cartographies plus complexes en densifiant le maillage passant ainsi en deux dimensions. La même méthode est toujours utilisée. En chaque point du maillage, deux valeurs de distances sont associées. La première valeur est la distance entre le centre du spot laser et le centre de la jonction de drain. Et la seconde valeur est la distance entre le centre du spot laser et le centre de la jonction de source. Cette méthodologie a permis de construire les cartographies de transistors.

II.2.1.1.2.4 Cartographies en courant d'un transistor NMOS polarisé en mode bloqué (OFF)

Dans cette partie, il est proposé de dessiner, à partir des relevés du simulateur, des cartographies montrant les courants générés par les deux jonctions PN d'un transistor NMOS [Lli12(b)].

Le graphique présenté ***Figure II. 24*** montre la cartographie en courant de l'électrode de drain extraite de la simulation électrique, au-dessus d'un layout fictif du transistor NMOS.

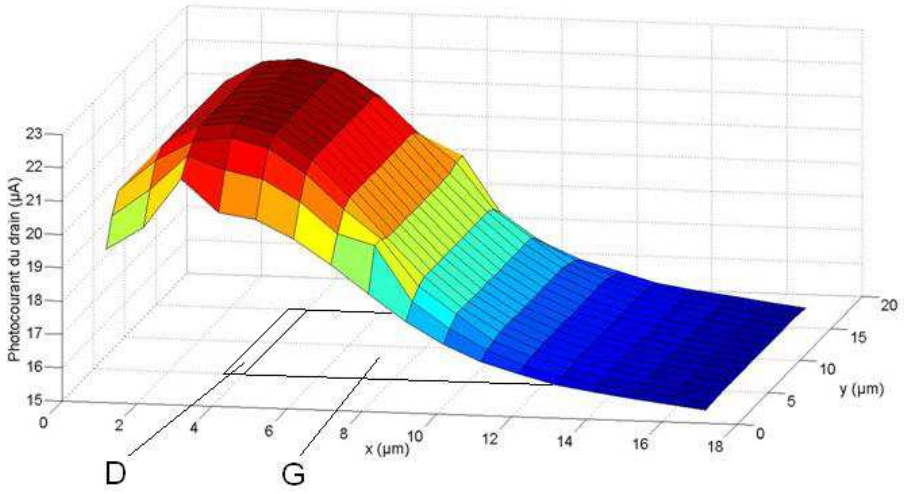


Figure II. 24. Cartographie de la contribution photoélectrique du drain sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

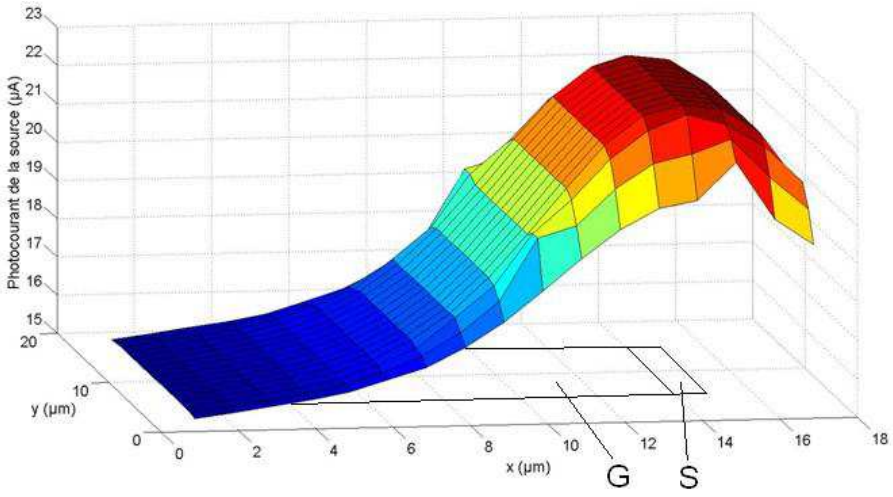


Figure II. 25. Cartographie de la contribution photoélectrique de la source sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

La figure ci-dessus, présente la cartographie extraite de la simulation pour l'électrode de source.

Les cartographies des photocourants générés par les deux jonctions N+/Psubstrat montrent l'effet gaussien de l'amplitude laser par rapport à la localisation du spot laser (voir ***Figure II. 24*** et ***Figure II. 25***).

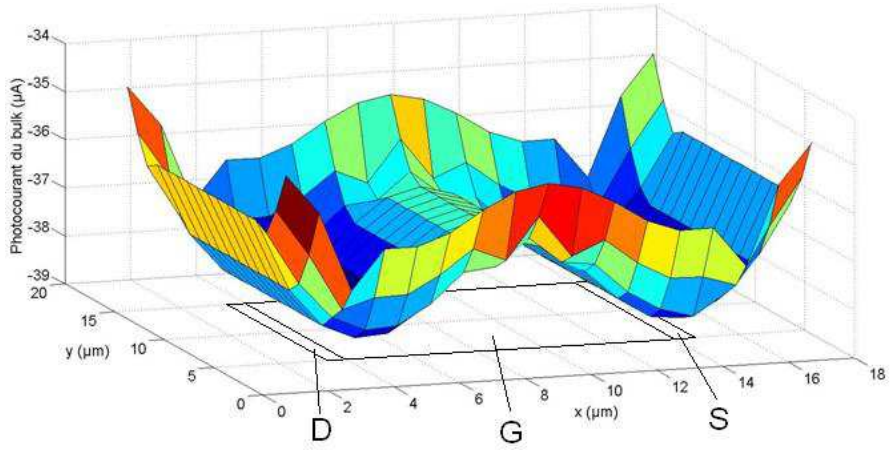


Figure II. 26. Cartographie du photocourant du bulk sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

Les cartographies montrées ci-dessus, obtenues par simulation n'ont pas pu être comparées à des mesures. En effet, l'équipement laser utilisé (I-phemos), ne permet pas de

gérer un déplacement du laser par rapport au composant étudié d'une manière fine (déplacement micrométrique).

Dans la partie précédente, seuls des effets purement photoélectriques ont été mesurés et simulés. Pour les paragraphes qui vont suivre, un banc laser de forte puissance a été utilisé (puissance maximale de 1,25 W). Les effets sur les circuits ne sont pas de mêmes natures que ceux réalisés à l'I-phemos. D'autres effets plus complexes que des effets purement photoélectriques peuvent apparaître, ce qui complique naturellement la compréhension des phénomènes ainsi que leur modélisation.

II.2.1.2 Mesures et modèle électrique à forte puissance laser pulsé

II.2.1.2.1 Présentation du modèle électrique

Les mesures dans ce paragraphe ont été réalisées sur un transistor NMOS W=L= 10 µm (le même que celui utilisé pour l'étude précédente sur l'I-phemos). Ce transistor est polarisé de manière à ce qu'il soit bloqué (le drain à un potentiel de 1,2 V est les autres électrodes sont à la masse) et exposé à une stimulation photoélectrique laser pulsé. En plus du photocourant observé sur les électrodes de source et de drain, il est possible d'observer le déclenchement du transistor bipolaire parasite NPN (drain/substrat de type P/source). La ***Figure II. 27*** présente le modèle électrique qui a été construit pour modéliser cet effet.

Dans cette partie, un modèle de transistor NMOS sous stimulation photoélectrique laser pulsée est proposé à partir notamment des travaux de Pouget [Pou00(b)], comme vu dans l'état de l'art de la modélisation électrique faite au ***paragraphe I.5.1.1***). Le modèle utilise les deux sous circuits qui modélisent les photocourants dans les jonctions PN N+/P-substrat. A forte puissance laser, le bipolaire parasite NPN (drain/Psubstrat/source) se déclenche lorsque le potentiel local du substrat de type P (nœud B) dépasse 0,6 V. En effet, le photocourant généré par les jonctions source/Psub et drain/Psub, ont tendance par effet résistif (dû aux différentes résistances présentent dans le modèle) à faire croître le potentiel du substrat local (potentiel B).

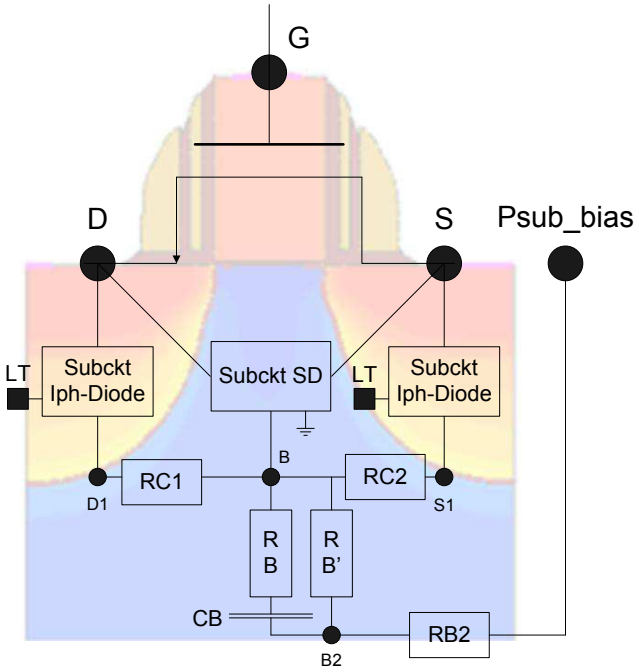


Figure II. 27. Modèle électrique d'un transistor NMOS sous Stimulation Photoélectrique Laser Pulsé.

Les résistances *RC1* et *RC2* représentent le chemin résistif sous le canal du transistor NMOS. La résistance *RB2*, représente le chemin résistif entre la prise de polarisation du substrat de type P et le potentiel local du substrat (*B2*).

Le réseau électrique constitué des résistances *RB* et *RB'* et de la capacité *CB* modélise l'effet de relaxation diélectrique qui se produit dans le substrat lors d'une illumination laser [Dou08]. Ce réseau permet de modéliser la dynamique de la mise en conduction du transistor bipolaire parasite drain/Psub/source.

De plus, le sous circuit *SD* modélise l'effet du bipolaire parasite qui se déclenche lorsque le potentiel de substrat local (B) augmente sous l'action du faisceau laser [Mus91]. Ce sous circuit a été calibré grâce à des mesures électriques, faites sans illumination laser.

Dans le but de savoir comment la structure du bipolaire parasite réagit [Dod96(b)], [Det97], [Roc98] à une modification de tension du substrat de type P des mesures électriques ont été réalisées sur un transistor NMOS sans illumination laser. Les conditions de polarisation de ce transistor sont identiques à celles présentées dans les parties en amont.

Les courants de source, de drain et de substrat de type P ont été mesurés en fonction de la tension de substrat de type P qui évolue de 0 à 1,2 V (voir ***Figure II. 28***).

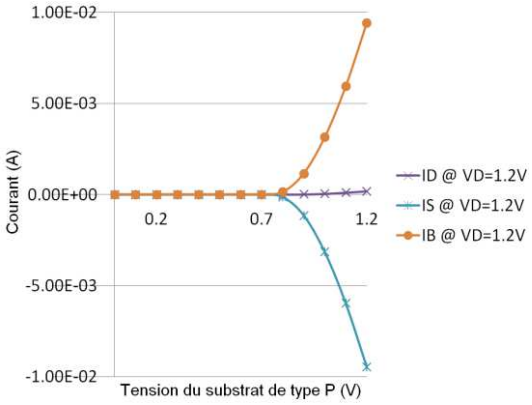


Figure II. 28. Courant sans illumination laser du transistor bipolaire parasite NPN (drain/substrat de type P/source) en fonction de la tension du substrat de type P.

Lorsque la tension du substrat de type P est supérieure au seuil de déclenchement d'une diode (0,6 V), la diode substrat de type P/source devient passante. Cette diode substrat de type P/drain quant à elle reste en polarisation inverse. Ainsi, une augmentation de la tension de substrat local déclenche le transistor bipolaire parasite drain/substrat de type P/source. Le gain de ce transistor bipolaire parasite est très faible (~10^{-3}). C'est l'activation de ce transistor bipolaire parasite qui fait que le courant peut aller du drain à la source du transistor NMOS en passant par le substrat de type P.

Le modèle utilisé pour émuler l'effet du transistor bipolaire parasite NPN est présenté ***Figure II. 29***. Afin de simplifier au maximum la modélisation de ce transistor bipolaire parasite, le modèle est constitué de deux sources de courant contrôlées en tension par le nœud *B'*. La calibration de ces deux sources de courant est néanmoins nécessaire pour chaque changement de taille de transistor. Dans ce cas de figure, les valeurs de ces sources de courant ont été calibrées grâce au mesures réalisées sans illumination laser du courant des différentes électrodes du transistor bipolaire en fonction de la tension du substrat de type P présentées ***Figure II. 28***.

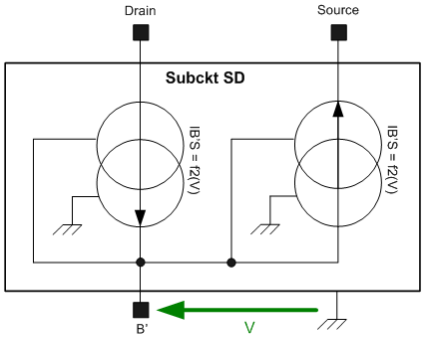


Figure II. 29. Modélisation électrique du transistor bipolaire parasite NPN drain/Psub/source.

II.2.1.2.2 Comparaison entre la simulation électrique et les mesures

Dans cette partie, il est proposé de comparer les résultats de simulation avec ceux obtenus en mesure, afin de valider le modèle électrique présenté précédemment. En mesure comme en simulation, le transistor NMOS (W=L=10 µm) est polarisé de la manière suivante pour le bloquer: le drain est porté à une potentiel de 1,2 V. La grille, la source et le substrat de type P sont connectés à la masse. Dans un premier cas, le laser est centré en plein milieu du transistor. La puissance est fixée à 1,25 W avec une durée d'impulsion égale à 20 µs.

II.2.1.2.2.1 Comparaison des pulses obtenus

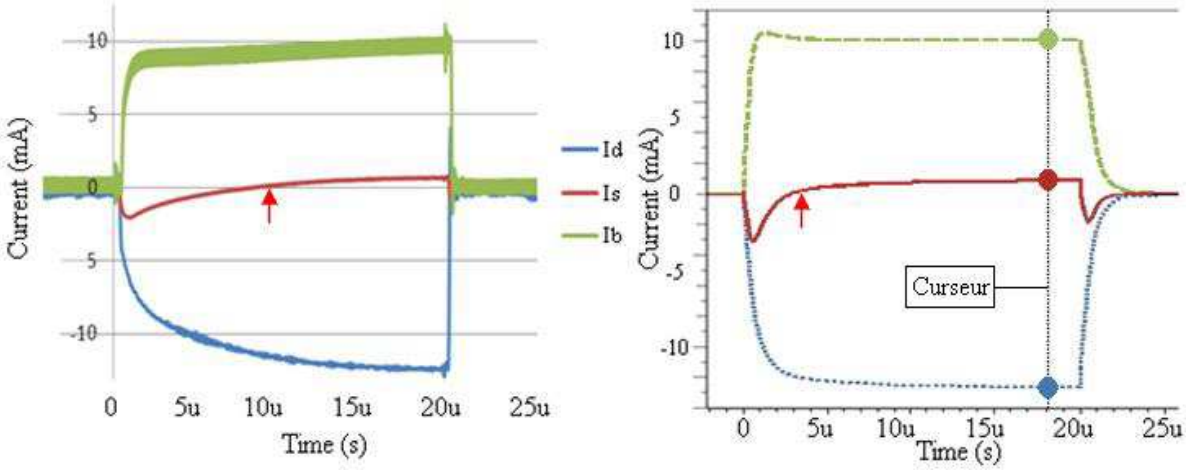


Figure II. 30. Courant d'un transistor NMOS exposé à une impulsion photoélectrique laser impulsionnelle. (a) Mesures (b) Simulations électriques.

Les mesures (a) et la simulation (b) présentées ***Figure II. 30*** montrent la très bonne corrélation obtenue par la modélisation. L'inversion du courant de source (en rouge) due au déclenchement du transistor bipolaire parasite NPN (lorsque le potentiel local du substrat est supérieur à 0,6 V) est mise en évidence par les flèches rouges. Cette inversion est due au fait que le courant allant du drain à la source devient progressivement, durant l'impulsion laser, supérieur au photocourant généré par la source. Ce phénomène a pu être modélisé grâce au sous circuit *subckt SD* présenté ***Figure II. 29*** et calibré grâce aux mesures faites au paragraphe précédent (voir ***Figure II. 28***).

II.2.1.2.2.2 Comparaison des cartographies en courant

Comme pour l'I-phemos, le modèle est capable de générer des cartographies correspondant à l'amplitude maximale du photocourant durant l'impulsion laser. L'amplitude pour réaliser les cartographies a été mesurée à un temps égal à 18 µs comme le montre le curseur placé sur les résultats de la simulation électrique présentés ***Figure II. 30***.

Les ***Figure II. 31.a*** et ***Figure II. 31.b*** présentent les résultats de cartographie simulée et mesurée, durant l'impulsion laser sur l'électrode de drain.

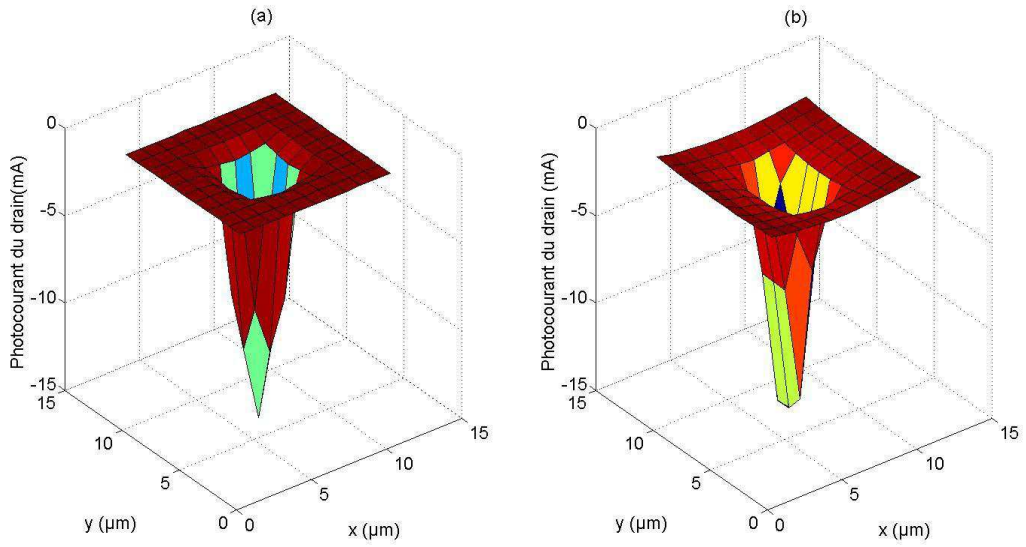


Figure II. 31. Cartographies de la contribution photoélectrique du drain sous stimulation photoélectrique laser impulsionnelle extraite à partir de simulation électrique (a) et de mesures (b).

La même méthodologie a été utilisée sur l'électrode de source (***Figure II. 32.a*** et ***Figure II. 32.b***).

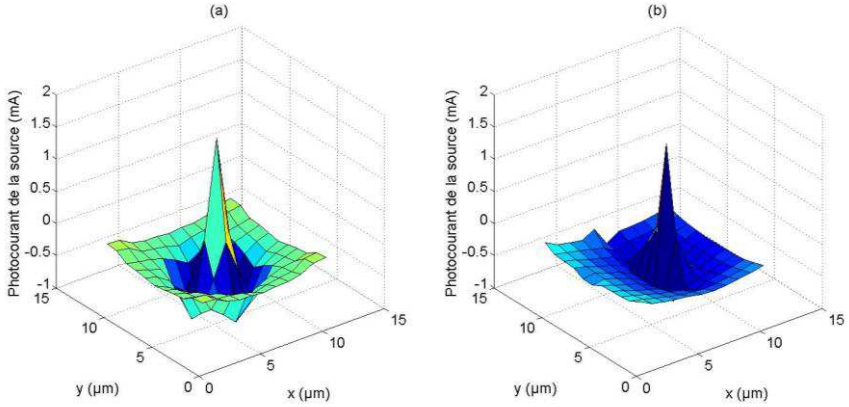


Figure II. 32. Cartographies de la contribution photoélectrique de la source sous stimulation photoélectrique laser impulsionnelle extraite à partir de simulation électrique (a) et de mesures (b).

Les ***Figure II. 33.a*** et ***Figure II. 33.b*** présentent la cartographie en courant de l'électrode du substrat de type P du transistor NMOS.

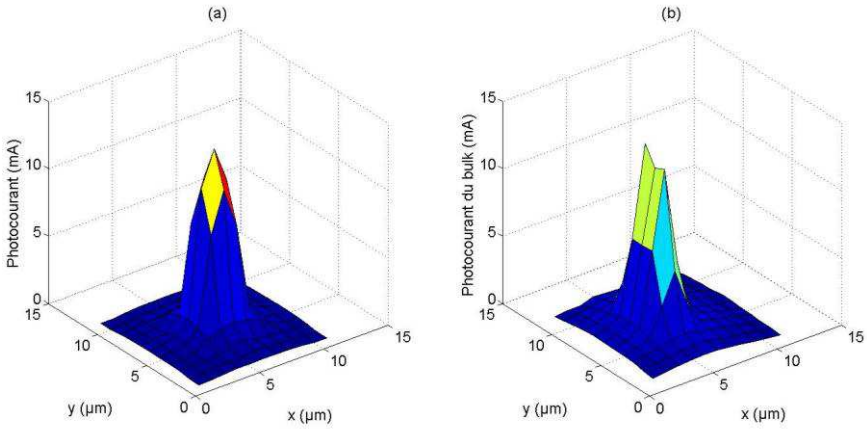


Figure II. 33. Cartographies de la contribution photoélectrique du substrat de type P sous stimulation photoélectrique laser impulsionnelle extraite à partir de simulation électrique (a) et de mesures (b).

Il est possible de remarquer (cf. ***Figure II. 32***) le changement de régime du courant de source en fonction de la puissance du laser. Ceci est dû à la mise en conduction du transistor

bipolaire parasite drain/Substrat de type P/source, il est nécessaire de centrer le faisceau laser au plus proche du transistor NMOS. En effet le fait de centrer le faisceau sur les jonctions de source et de drain génère un plus fort photocourant sur ces jonctions. Produisant un photocourant plus important, par effet résistif. Le potentiel de substrat local pourra alors plus facilement atteindre 0,6 V et donc déclencher le bipolaire parasite source/Psubstrat/drain rendant ainsi le courant mesuré positif conformément à la convention: sortant s'il est positif et rentrant s'il est négatif.

II.2.2 Transistor PMOS

II.2.2.1 Mesures et modèle électrique à faible puissance laser (I-phemos)

La même méthodologie que pour le transistor NMOS a été utilisé pour créer le modèle du transistor PMOS sous stimulation photoélectrique laser. La seule caractérisation supplémentaire concerne la jonction Nwell/Psubstrat présente dans un transistor PMOS.

II.2.2.1.1 Présentation du modèle électrique

Il est possible de noter que le modèle électrique simulant l'effet du laser à faible puissance ne provoque pas de déclenchement de bipolaires parasites. C'est la raison pour laquelle, sur les cinq électrodes d'un transistor PMOS, uniquement deux sous circuit modélisant les jonctions P+/Nwell sous SPL (sous circuit *Iph*) sont appelés par la netlist principale. Les valeurs de ces sources de courant sont définies suivant les équations ***Eq. II. 2***, ***Eq. II. 3*** et ***Eq. II. 4*** et les coefficients définis au ***Tableau II. 1***. De la même manière le sous-circuit *Iphnw_Psub* modélisant la jonction Nwell/Psubstrat sous SPL est appelé (voir ***Figure II. 34***).

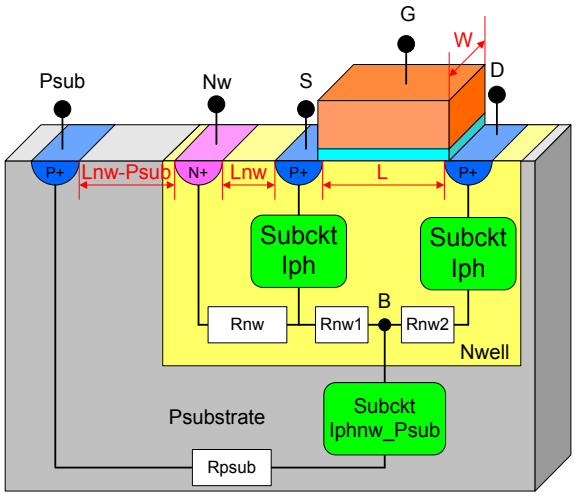


Figure II. 34. Modèle électrique SPICE d'un transistor PMOS sous Stimulation Photoélectrique Laser continue.

Les résistances *Rnw1*, *Rnw2*, *Rnw* et *Rpsub* représentent les différents chemins résistifs que peuvent rencontrer les différents photocourants générés dans le transistor. Les valeurs des résistances sont définies de la manière suivante (avec les paramètres géométriques définis en micromètre sur la ***Figure II. 34***):

$$R_{nw1} = R_{nw2} = R_{nw}^{\square} \times \frac{L}{2W} \qquad \textit{Eq. II. 24}$$

$$R_{nw} = R_{nw}^{\square} \times \frac{L_{nw}}{W} \qquad \textit{Eq. II. 25}$$

$$R_{psub} = R_{Psub}^{\square} \times \frac{\left(L_{nw} + L_{nw-Psub} + \frac{L}{2}\right)}{W} \qquad \textit{Eq. II. 26}$$

Où $R_{nw}^{\square}$ et $R_{psub}^{\square}$ sont les valeurs des résistances de chaque différent type de silicium par carré. Afin d'être plus précis sur les valeurs de ces résistances, un simulateur de substrat pourra être utilisé.

II.2.2.1.2 Comparaison entre simulation et mesures

II.2.2.1.2.1 Laser continu centré sur le transistor PMOS

Comme pour le modèle du transistor NMOS sous PLS continue, il est possible de comparer les résultats de simulation par rapport aux mesures. Le graphique présenté ***Figure***

II. 35 montre la très bonne corrélation entre la simulation électrique et les mesures sur un transistor PMOS W=L=10 µm.

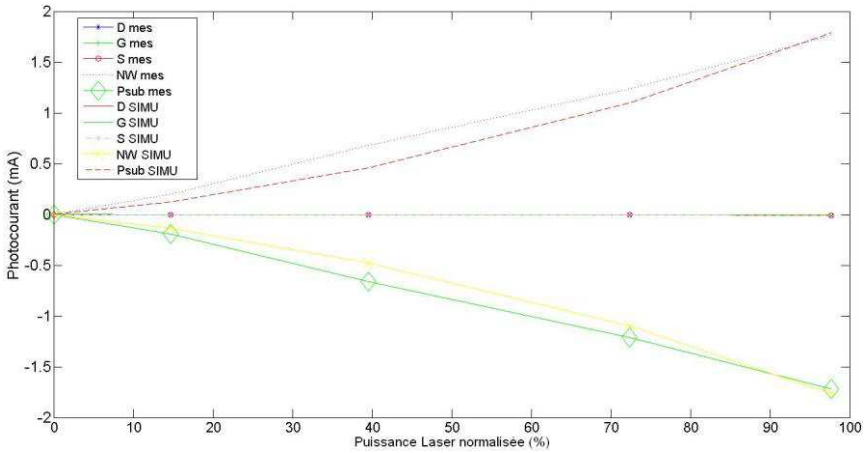


Figure II. 35. Comparaison entre simulation électrique SPICE et mesures du courant dans un transistor NMOS W=L=10 µm sous stimulation photoélectrique laser faible puissance continue à différentes puissance laser, avec une taille de spot de 3,25 µm.

Il est possible de noter que dans ce cas de figure, l'effet prépondérant est le photocourant généré par la jonction Nwell/substrat de type P par rapport au photocourant généré par les jonctions drain/substrat de type P et source/substrat de type P. Ce résultat s'explique de plusieurs façons. Tout d'abord, la surface de la jonction Nwell/Psubstrat est environ 70 fois supérieure aux jonctions P+/Nwell. Ensuite, les dopages des deux jonctions ne sont pas identiques, ce qui peut expliquer cette importante différence. De plus, il y a également le fait que les charges générées dans le Nwell sont plus souvent capturées par le Psub que par le P+.

II.2.2.1.2.2 Cartographies en courant

De même que pour le transistor NMOS, il est proposé dans ce paragraphe de dessiner des cartographies en courant d'un transistor PMOS extraites du simulateur ELDO. Un transistor PMOS W=L=10 µm est simulé dans le cas d'étude suivant.

Les figures suivantes présentent les cartographies de source de drain et de substrat de type P pour une puissance laser fixée à 40 mW et une taille de spot de 3,25 µm.

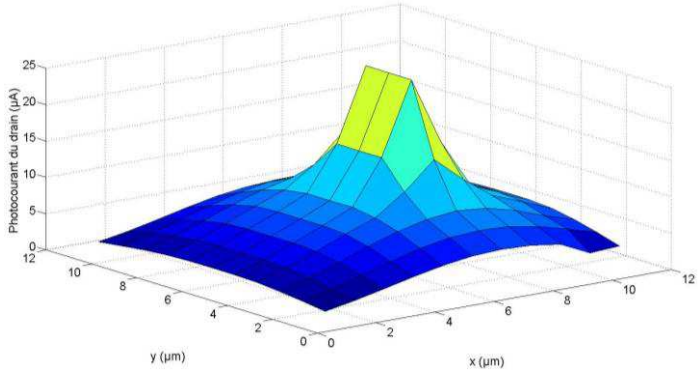


Figure II. 36. Cartographie de la contribution photoélectrique du drain d'un transistor PMOS sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

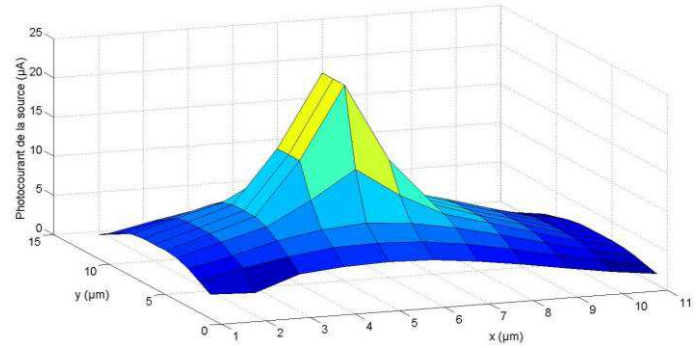


Figure II. 37. Cartographie de la contribution photoélectrique de la source d'un transistor PMOS sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

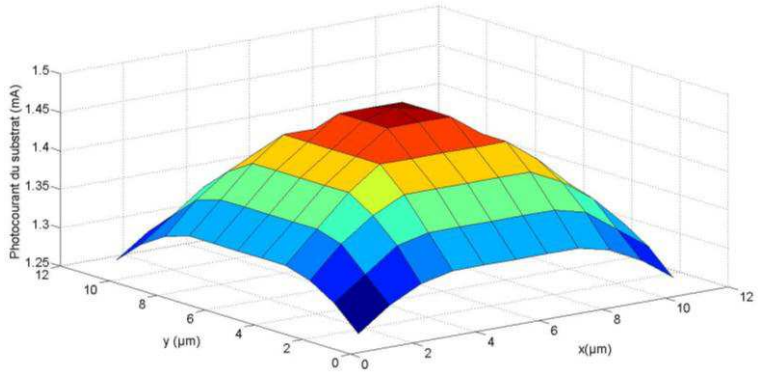


Figure II. 38. Cartographie de la contribution photoélectrique du substrat de type P d'un transistor PMOS sous Stimulation Photoélectrique Laser extraite du simulateur électrique.

Les cartographies du transistor PMOS montrent comme celles du transistor NMOS, la dépendance spatiale du laser sur le silicium. De plus, il est possible une nouvelle fois de remarquer la contribution très forte de la jonction Nwell/substrat de type P par rapport aux autres jonctions PN présentes dans le transistor PMOS. En effet la jonction Nwell/Psubstrat génère un photocourant environ 70 fois supérieur aux jonctions P+/Nwell. Cette différence peut s'expliquer par deux facteurs que sont les différences de surface et de dopages entre les deux types de jonction. De plus, la présence de la jonction Nwell/Psub modifie le mécanisme de capture de charges générées dans le transistor PMOS. En effet la jonction Nwell/Psub entre en « compétition » avec les jonctions P+/Nwell en ce qui concerne le phénomène de capture des porteurs de charges générées dans le Nwell.

II.2.2.2 Mesures et modèle à forte puissance laser

Afin de modéliser un transistor PMOS sous stimulation photoélectrique laser, la même méthodologie que celle du NMOS a été utilisée. Des mesures sur l'équipement laser impulsionnel forte puissance ont permis de confirmer et de valider la modélisation.

II.2.2.2.1 Mesures avec substrat de type P laissé flottant

Dans ce sous paragraphe, le transistor PMOS avec le Psubstrat laissé flottant est utilisé afin de comprendre les mécanismes physiques mis en jeu lorsque ce transistor est sous illumination laser, la jonction PN Nwell/Psubstrat n'intervenant pas. Cette méthode permet d'étudier le déclenchement potentiel du transistor bipolaire parasite PNP drain/Nwell/source. La mesure du photocourant est présentée ***Figure II. 39***.

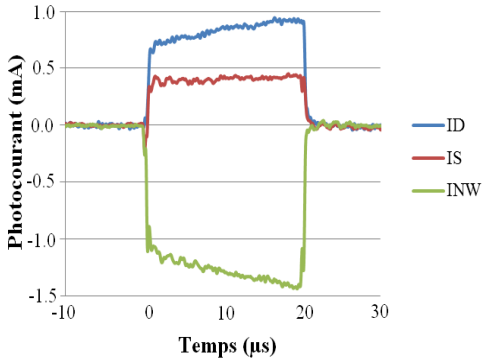


Figure II. 39. Mesure du photocourant d'un transistor PMOS transistor sous SPL impulsionnelle, à une puissance laser de 1,25 W, avec le substrat de type P laissé flottant.

Il est possible de remarquer, ce faisant, qu'à cette puissance laser il n'y a pas de déclenchement du transistor bipolaire parasite PNP drain/Nwell/source parce qu'il n'y a pas d'inversion du courant de source mesuré comme observé pour le déclenchement du transistor bipolaire parasite NPN dans un transistor NMOS (voir ***paragraphe II.2.1.2***).

II.2.2.2.2 Transistor PMOS avec substrat de type P connecté à la masse

Dans cette sous-section, le substrat de type P est connecté à la masse. L'étude se fait ainsi sur le transistor PMOS complet en prenant également en compte la jonction Nwell/Psubstrat.

Dans ces conditions, le photocourant de chaque électrode du transistor PMOS est présenté ***Figure II. 40***.

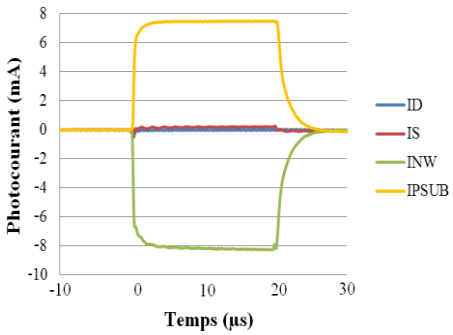


Figure II. 40. Mesures du courant d'un transistor PMOS sous SPL impulsionnelle, à une puissance laser de 1,25 W avec le substrat de type P connecté à la masse.

Le fait de connecter le substrat de type P à la masse réduit le photocourant généré par la source et le drain en passant d'environ quelques mA à quelques centaines de µA. Le photocourant est généré de manière majoritaire par la jonction Nwell/Psubstrat du à son importante surface illuminée par le spot laser.

Afin de valider la constatation précédente observée en mesures, des simulations TCAD ont été faites. Le but était de bien caractériser la différence de photocourant générée entre la jonction P+/Nwell et la Nwell/Psubstrat d'un transistor PMOS polarisé de manière bloquée. La structure utilisée en simulation TCAD est polarisée de la manière suivante: la source, la grille et le Nwell sont fixés au potentiel de 1,2 V. Le drain et le substrat de type P sont connectés à la masse. Le graphique présenté ***Figure II. 41*** montre le photocourant simulé aux différentes électrodes d'un transistor PMOS en fonction de la puissance du laser.

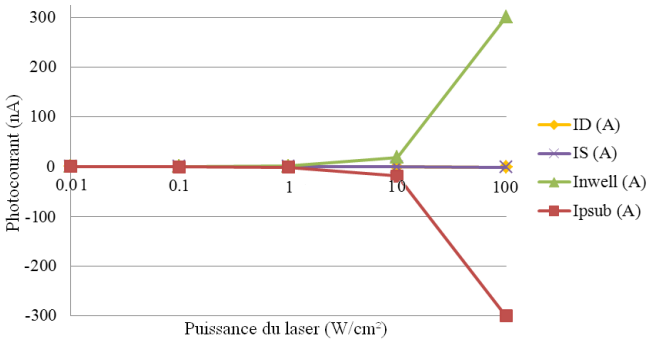


Figure II. 41. Photocourant extrait de la simulation TCAD d'un transistor PMOS bloqué sous SPL avec un substrat de type P connecté à la masse en fonction de la puissance laser.

Comme le confirme la simulation TCAD le photocourant majoritaire dans un transistor PMOS est créé par la jonction Nwell/Psubstrat.

II.2.2.2.2.1 Modèle électrique

Un modèle électrique particulier des effets de la SPL impulsionnelle sur un transistor PMOS a été créé. Trois sous-circuits *Subckt_Iph_Diode* pour la jonction P+/Nwell (l'un pour la jonction source/Nwell et l'autre celle drain/Nwell) et un pour la jonction Nwell/Psubstrat ont été utilisés dans cette modélisation. De plus un paramètre d'atténuation

a été ajouté à l'équation qui régit le photocourant des jonctions P+/Nwell lorsque la puissance du laser devient importante (~1 W) créant principalement un photocourant allant du Nwell au substrat de type P. La modélisation prend en compte la chute du potentiel local du Nwell pouvant ainsi déclencher les deux transistors bipolaires parasites verticaux P+/Nwell/Psub: *subckt_bip* dans la ***Figure II. 42***. Les résistances *RNW, RNW'* et la capacité *CNW* sont utilisées pour fixer la constante de temps de ce phénomène. Cette constante de temps décrit l'effet de relaxation diélectrique [Dou08]. Pour un fort photocourant généré par la jonction Nwell/Psubstrat (modélisé par le sous-circuit *Iph-diode*), le potentiel local du caisson de type N chute par effet résistif dû principalement à la résistance *RNW2* (potentiel *NW* ***Figure II. 42***). Si la chute est supérieure à 0.6 V, les transistors bipolaires parasites verticaux P+/Nwell/Psub peuvent s'enclencher. Il est possible de remarquer que le transistor bipolaire parasite drain/Nwell/source est présent dans le modèle ***Figure II. 42***. Bien que la mesure du transistor PMOS sous SPL impulsionnelle avec substrat de type P laissé flottant (voir ***Figure II. 39***) n'est pas mis en évidence, la mise en conduction de ce transistor pourrait apparaître toutefois dans d'autres technologies. Dans la suite des simulations électriques de type SPICE, ce transistor bipolaire parasite n'est pas pris en compte.

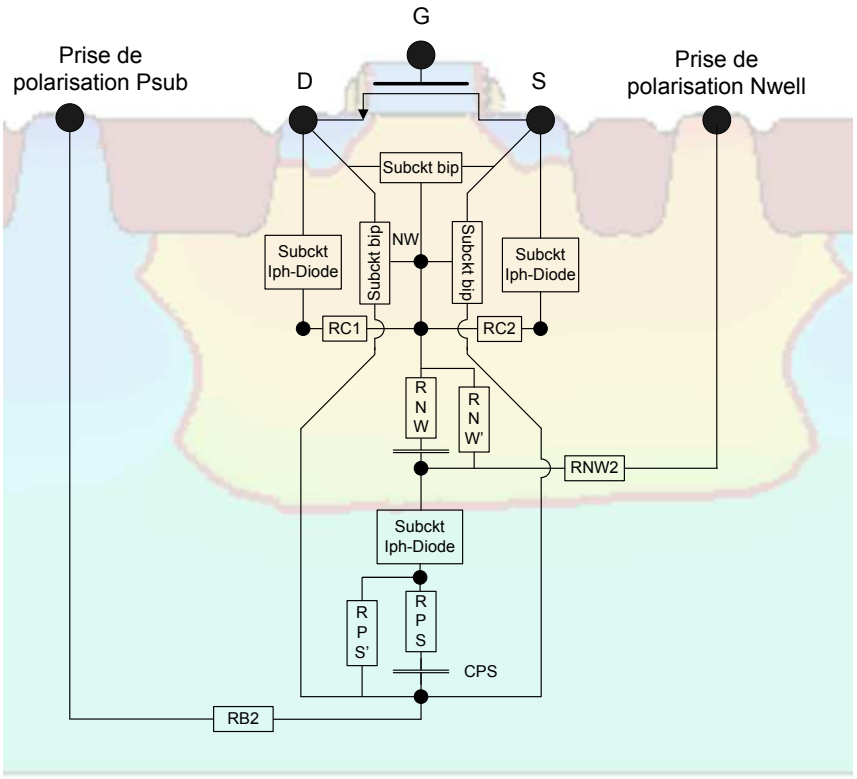


Figure II. 42. Modèle électrique d'un transistor PMOS sous SPL impulsionnelle.

La ***Figure II. 43*** montre le résultat de simulation sur le transistor PMOS bloqué (drain et substrat de type P connectés à la masse et Grille, Source ainsi que Nwell porté au potentiel de 1,2 V) pour une puissance laser de 1,25 W, et une durée d'impulsion de 20 µs.

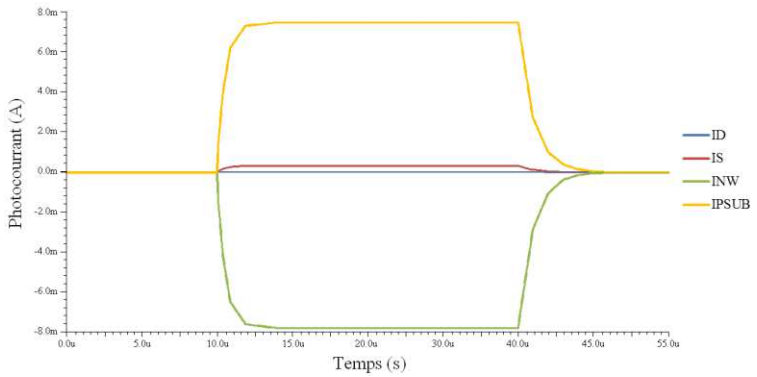


Figure II. 43. Courants simulés du transistor PMOS sous SPL impulsionnelle.

Il est possible de remarquer la bonne corrélation obtenue entre les mesures (***Figure II. 40***) et la simulation (***Figure II. 43***).

II.2.2.2.2.2 Cartographies en courant: comparaison entre mesure et simulation

Dans cette partie, il est proposé de dessiner un exemple de cartographies en courant [Glo10(b)] (extrait du simulateur ELDO) du photocourant du Nwell généré par un transistor PMOS W=L=10 µm. Pour une puissance laser maximale (1,25 W) les valeurs extraites de la simulation sont comparées aux mesures et montre la bonne corrélation obtenue entre simulation et mesures pratiques (***Figure II. 44.a*** et ***Figure II. 44.b)***.

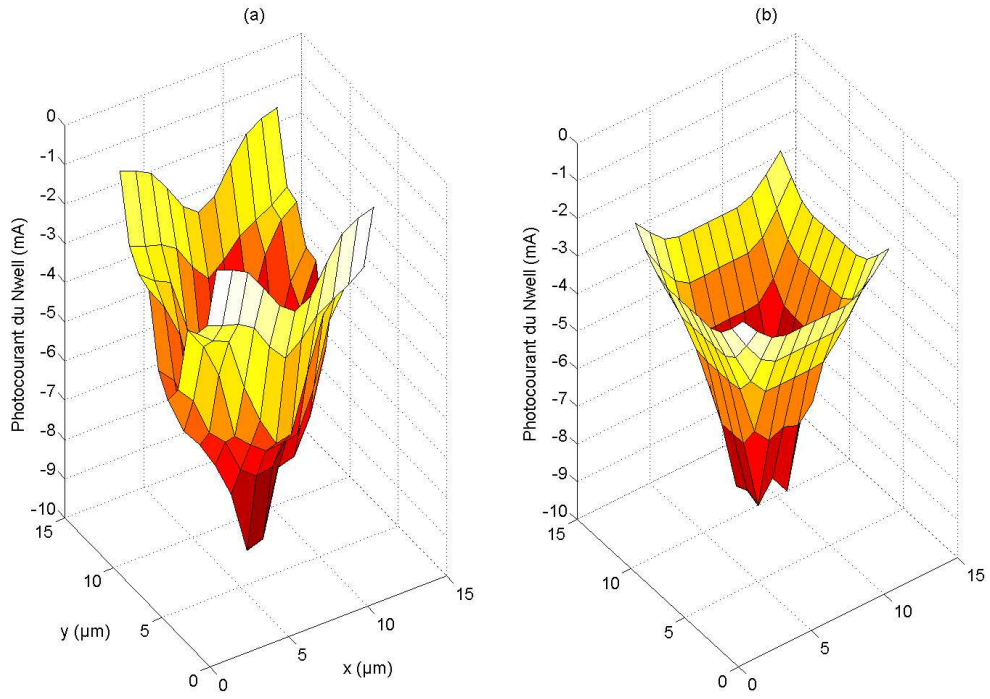


Figure II. 44. Cartographies en courant de l'électrode du Nwell d'un transistor PMOS. Mesure (a) et simulation électriques (b).

II.3 Effet de l'implant enterré de type N sur des transistors MOS

L'effet de l'implant enterré de type N (deep Nwell) après avoir été présenté sur la jonction N+/Psubstrat (voir ***paragraphe II.1.4***) est maintenant étudié sur les transistors de type MOS.

II.3.1 Effets sur des transistors NMOS

L'implant deep Nwell est utilisé pour placer un ou plusieurs transistors NMOS dans des puits de type P (Pwell) isolés du substrat P. La présence de cet implant, par rapport à un transistor NMOS standard modifie le mécanisme de collection de charges. Le photocourant généré par les différentes jonctions PN n'est donc pas identique.

Afin d'illustrer les effets de cet implant deep Nwell sur un transistor NMOS, la ***Figure II. 45*** donne la vue en coupe d'un NMOS et de son puits P isolé (Pwell) à partir d'une structure TCAD 2D. Les conditions de polarisation « normales » sont les suivantes. Le drain et la prise du Nwell qui contacte de deep Nwell est polarisé à 1,2 V. La source, la grille, le Pwell et le substrat de type P sont connectés à la masse. Dans cette structure de test, les prises de polarisation du Pwell et du Psub sont connectées à un seul et même Pad.

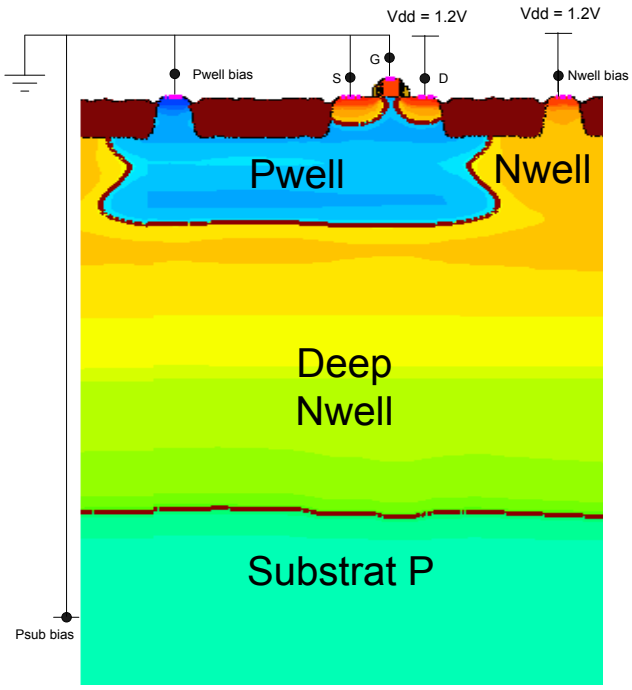


Figure II. 45. Vue en coupe TCAD d'un transistor NMOS avec l'implant deep Nwell.

Le faisceau laser était centré en plein milieu du transistor avec une taille de spot de 5 µm de diamètre, une puissance de 1,25 W. La durée d'impulsion était fixée à 20 µs. Dans un premier cas, la prise de polarisation de l'implant Nwell/deep Nwell est laissée flottante.

Cette configuration permet d'étudier uniquement la perte de puissance de l'onde lumineuse laser due à la l'interface deep Nwell/Psub. La ***Figure II. 46*** présente les courants mesurés de drain de la source et du Pwell/Psub dans ces conditions de polarisation.

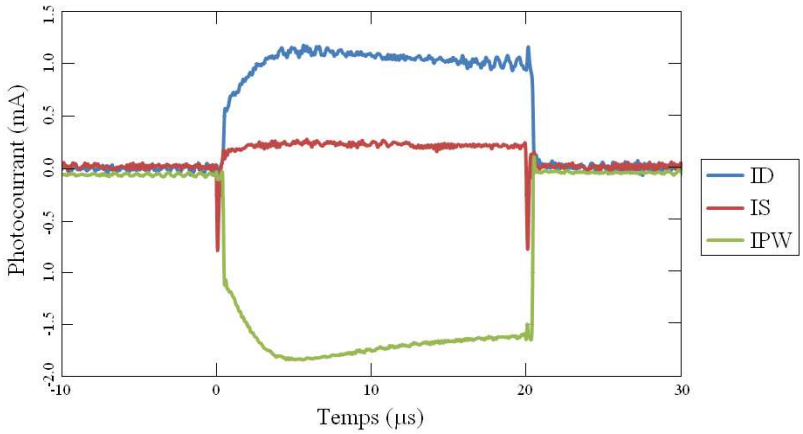


Figure II. 46. Photocourant du transistor NMOS (W=L=10 µm) avec implant de type deep Nwell, avec l'électrode de polarisation du deep Nwell laissée flottante.

En connectant la prise de polarisation de l'implant deep Nwell à 1,2 V l'effet est différent (voir ***Figure II. 47***).

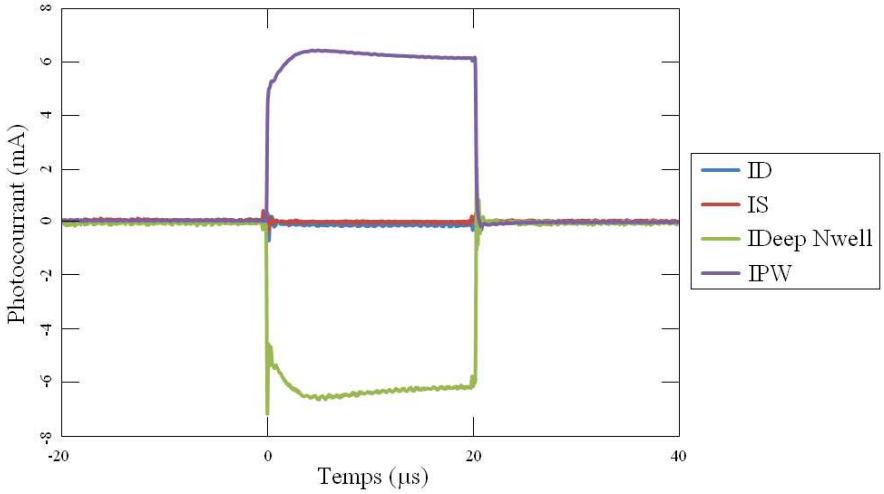


Figure II. 47. Photocourant du transistor NMOS (W=L=10 µm) avec implant de type deep Nwell - électrode de polarisation du deep Nwell polarisée à 1,2 V.

Le changement de signe du courant mesuré sur l'électrode du Pwell (IPW) constaté entre la ***Figure II. 46*** et la ***Figure II. 47*** est dû au fait que la jonction deep Nwell/Psub

génère un important photocourant photocourant lorsque le deep Nwell est polarisé (de l'ordre 6mA).

Les photocourants générés par la source et le drain lorsque la prise du Nwell/deep Nwell est polarisée, sont de l'ordre de 200 µA (soit 10 fois moins que pour un transistor NMOS de même technologie dans les mêmes conditions de test). De plus, la différence entre un transistor NMOS standard (sans implant deep Nwell) et un avec implant deep Nwell, est très faible. En effet, l'interface optique créée par la jonction deep Nwell/Psub n'a engendré qu'une perte de 5 % du photocourant de la source et du drain. Ainsi le comportement d'un transistor NMOS avec deep Nwell non polarisé est quasiment équivalent à celui d'un transistor NMOS standard. Par contre lorsque le deep Nwell est polarisé, les mécanismes de collection de charge sont différents. Ceci étant dû aux différents champs électriques présents dans la structure.

II.3.2 Effet sur des transistors PMOS

Dans cette partie il est proposé d'étudier l'influence d'un implant de type deep Nwell (encore appelé NISO) sur le photocourant généré par les jonctions PN d'un transistor PMOS. La ***Figure II. 48*** présente les vues en coupe de transistors PMOS sans (a) et avec (b) implant deep Nwell.

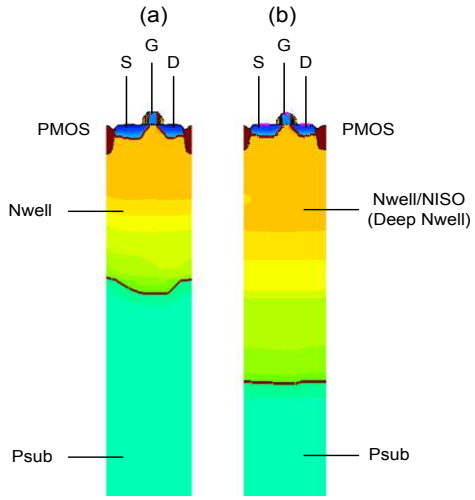


Figure II. 48. Coupe TCAD d'un transistor PMOS : (a) Standard et (b) NISO.

La présence ou l'absence d'un implant deep Nwell sous un transistor PMOS, ne modifie pas a priori fondamentalement le mécanisme de génération du photocourant dans le transistor. En effet dans le cas d'un transistor PMOS avec implant deep Nwell, le caisson de type N est plus profond, cela étant dû à l'épaisseur de l'ordre du µm de l'implant deep Nwell. L'absence de structure de test n'a pas permis de quantifier les effets du triple well sur un transistor PMOS.

II.4 Inverseur

A ce stade du manuscrit, il est donc possible de créer des modèles de portes plus complexes constituées de transistors NMOS [Sar12] et PMOS [Sar12(b)] sous Stimulation Photoélectrique Laser.

Après avoir modélisé les effets physiques de l'interaction laser silicium sur des transistors MOS, il est naturel de se pencher sur le cas de l'inverseur. En effet c'est la porte CMOS la plus simple constituée uniquement d'un transistor NMOS et d'un PMOS.

II.4.1 Présentation de la structure de test

Afin d'étudier la réponse d'un inverseur à une stimulation photoélectrique laser, une structure de test a été créée. Elle est constituée de 18 inverseurs avec des variations géométriques de layout. Neuf inverseurs sont situés au-dessus d'un implant deep Nwell (autrement appelé NISO). Le schéma de la ***Figure II. 49*** présente le schéma électrique de cette structure.

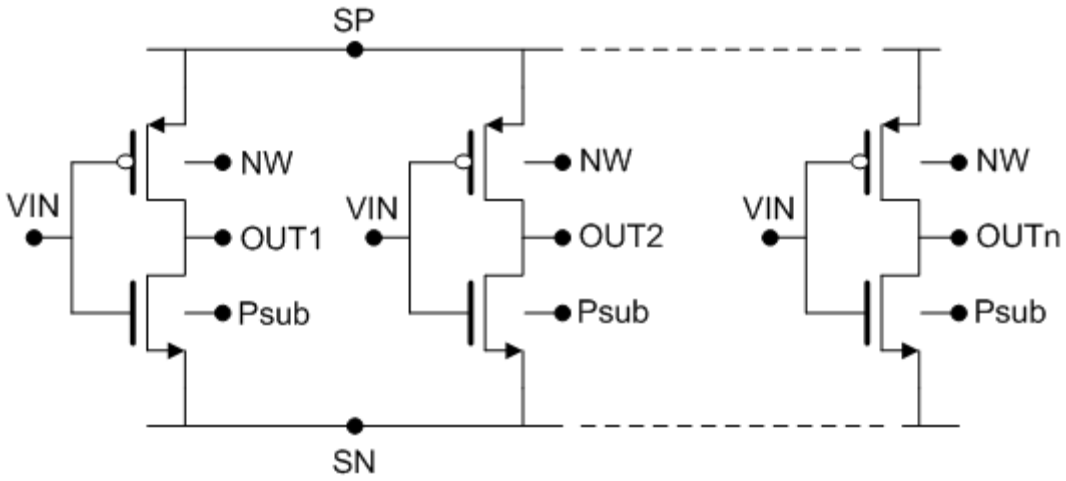


Figure II. 49. Schéma de la structure de test constituée d'inverseurs connectés en parallèles.

Le fait d'avoir uniquement à disposition 22 Pads pour faire toutes les connexions électriques de la structure de test, (elle comporte 18 inverseurs), a rendu nécessaire de connecter plusieurs éléments en parallèle. Ainsi, toutes les sources des transistors PMOS sont communes et reliées à un seul et même Pad. Il en est de même pour les sources des transistors NMOS. De la même manière toutes les entrées des différents inverseurs sont connectées à un PAD unique. Les sorties sont, elles, connectées à des Pads différents.

Le layout de la structure complète est présenté ***Figure II. 50*** :

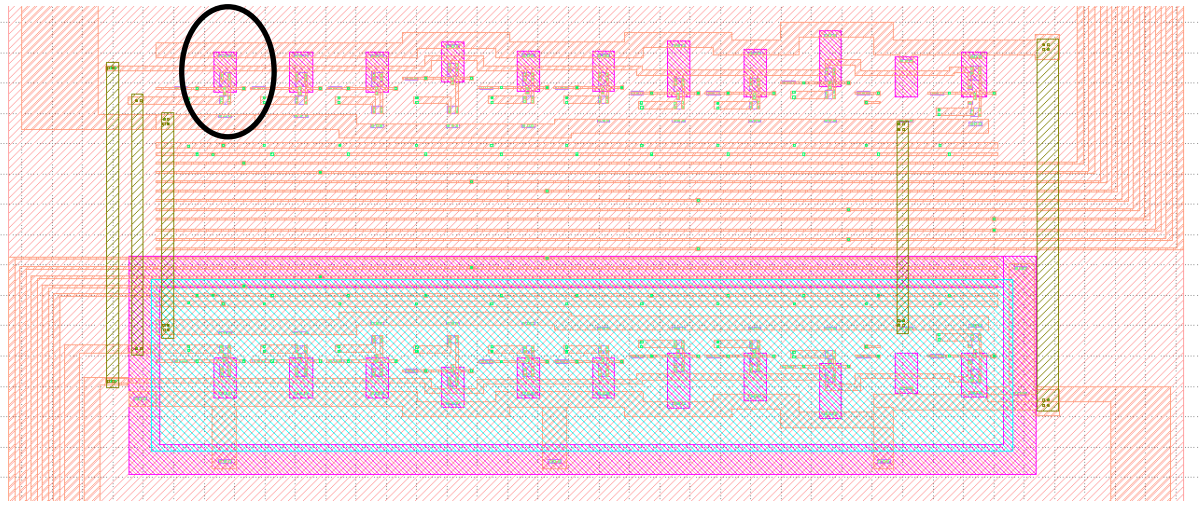


Figure II. 50. Layout de la structure de test constituée d'inverseurs.

Le layout de l'inverseur illuminé par le laser, entouré en noir sur la ***Figure II. 50***, est classique (voir l'agrandissement ***Figure II. 51***).

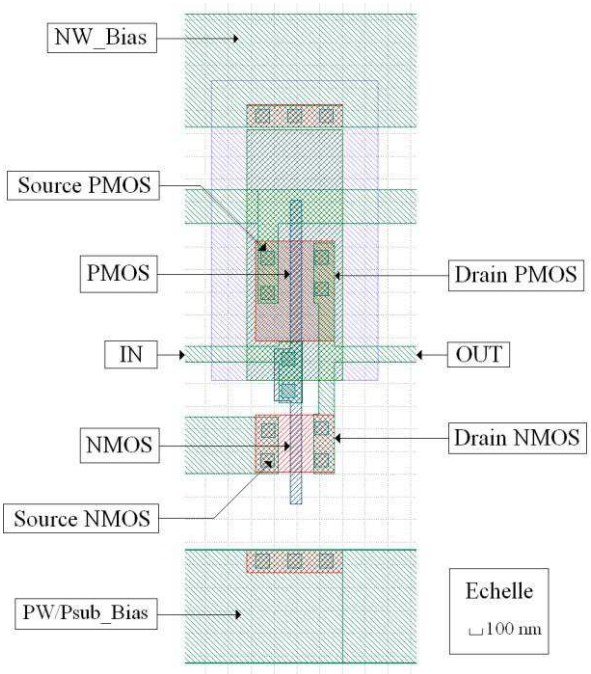


Figure II. 51. Layout de l'inverseur étudié.

La structure de test est réalisée en technologie CMOS 90 nm. Le ***Tableau II. 3*** présente les dimensions des transistors NMOS et PMOS de la ***Figure II. 51***.

	W (µm)	**L (µm)**
NMOS	0,44	0,1
PMOS	0,88	0,1

Tableau II. 3. Taille des transistors de l'inverseur.

II.4.2 Mesures et modèle électrique à faible puissance laser

II.4.2.1 Mesures

Dans cette étude l'équipement faible puissance laser continu I-phemos, a été utilisé. Le spot laser a été centré en plein milieu du premier inverseur (inverseur entouré en noir

dans le schéma présenté ***Figure II. 50***). La taille du spot était de 3,25 µm recouvrant la totalité de l'inverseur. La puissance laser était, quant à elle, réglable entre 0 et 40 mW.

Dans ce cas d'étude, l'inverseur était polarisé de la manière suivante: la source du transistor PMOS ainsi que le caisson de type N étaient portés au potentiel de 1,2 V, alors que la source du NMOS, l'entrée V_{IN} et la prise du substrat de type P étaient connectées à la masse (voir ***Figure II. 52***). Dans cette configuration, le transistor NMOS est bloqué (OFF) alors que le PMOS est en régime saturé (ON).

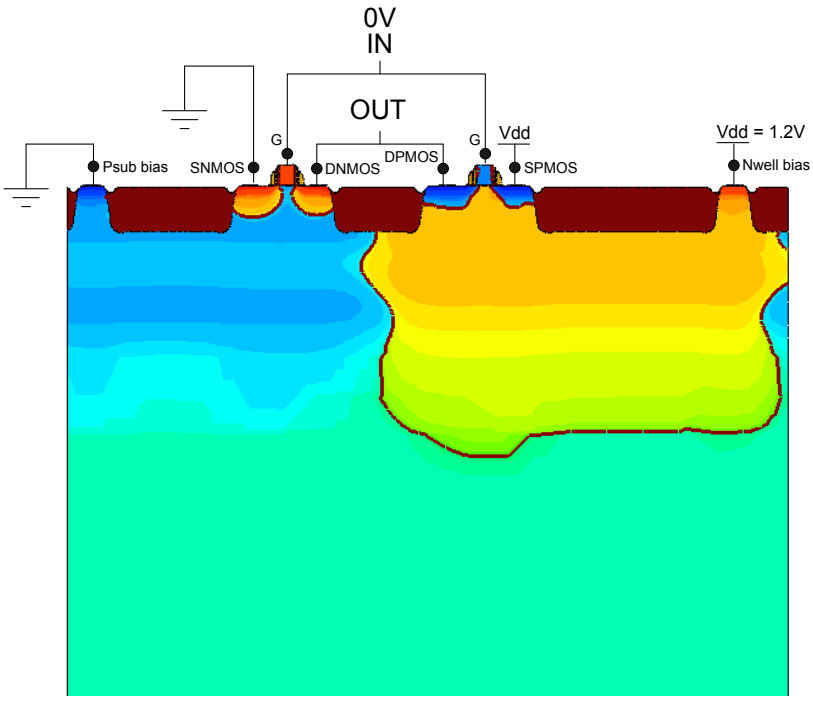


Figure II. 52. Schéma de polarisation électrique de l'inverseur présenté sur une coupe TCAD.

Les différents courants de l'inverseur ont été mesurés en fonction de la puissance du laser.

La ***Figure II. 53*** présente les différents courants mesurables au sein de l'inverseur. Ce sont les courants des sources des transistors, ainsi que des prises de caisson de type N et du substrat P.

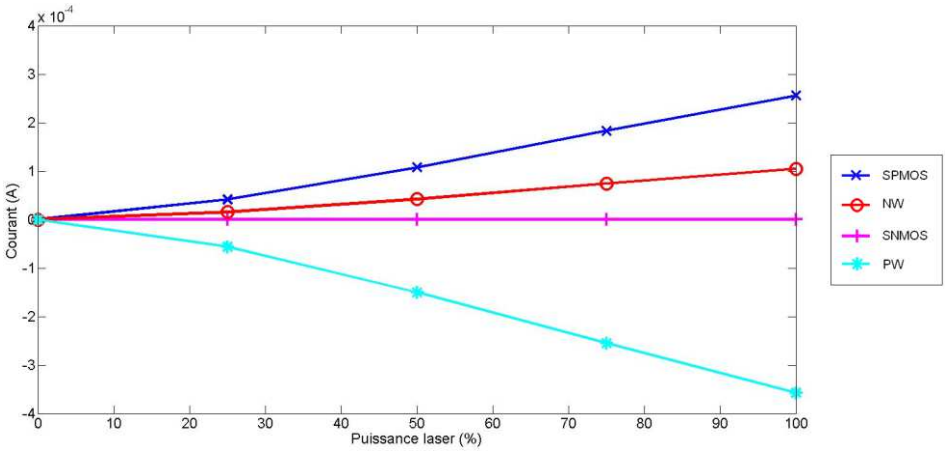


Figure II. 53. Courants mesurés dans la structure en fonction de la puissance laser.

Il est possible de faire un bilan des courants dans la structure afin de comprendre quels sont les phénomènes physique mis en jeu lors de la Stimulation Photoélectrique Laser.

En premier lieu, le courant mesuré sur la source du transistor NMOS, I_{SNMOS} n'est autre que le photocourant généré par la jonction PN source du NMOS/substrat de type P (I_{phSN}).

$$I_{SNMOS} = I_{phSN} \qquad \textit{Eq. II. 27}$$

En appliquant maintenant la loi des nœuds sur la prise du caisson de type N, il est possible d'effectuer le bilan en courant suivant, donnant le courant mesuré sur l'électrode du Nwell (I_{NW}) :

$$I_{NW} = I_{phSP} + I_{phDP} + I_{NW/Psub} \qquad \textit{Eq. II. 28}$$

Avec *IphSP* le photocourant généré par la source du transistor PMOS, *IphDP* le photocourant au niveau du drain du transistor PMOS et *IphNW/Psub* le photocourant généré par la jonction Nwell/Psubstrat.

Il est possible d'écrire le même type de relation en considérant la source du transistor PMOS :

$$I_{SPMOS} = I_{phDP} + I_{phDN} + I_{ON} \qquad \textbf{Eq. II. 29}$$

Avec I_{ON} le courant de saturation du transistor PMOS (à l'état passant).

En additionnant les courants précédents, il est possible d'obtenir le courant traversant le contact de polarisation du substrat P (polarisation à la masse) I_{PSUB}.

$$I_{PSUB} = I_{phSN} + I_{phDN} + I_{phSP} + I_{phDP} + I_{phNW\_Psub} + I_{ON} \qquad \textbf{Eq. II. 30}$$

Le schéma ***Figure II. 54*** présente les différents courants et photocourants qui interviennent dans cette étude.

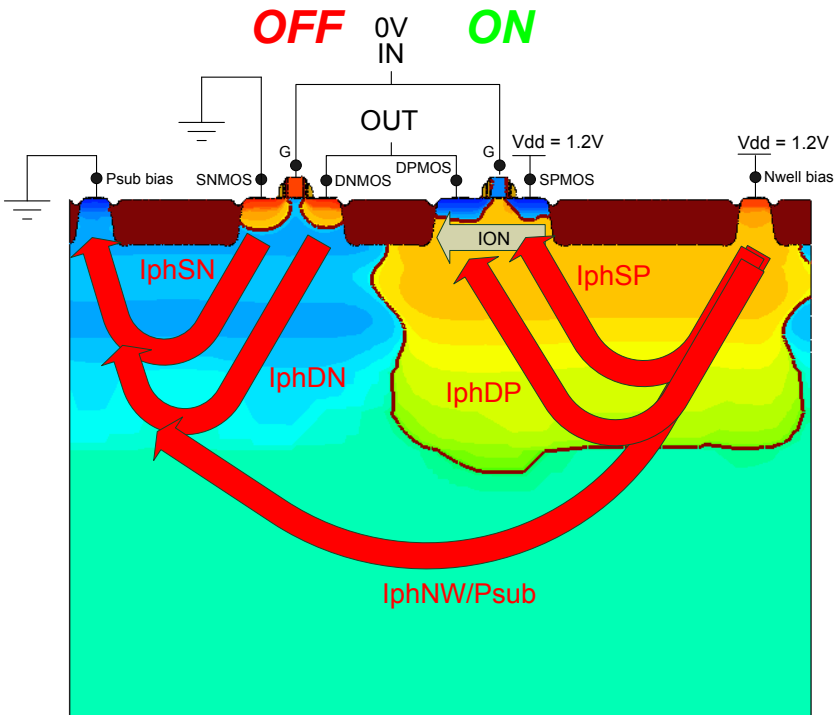


Figure II. 54. Schéma explicatif des différents courants et photocourants présents lors de la Stimulation Photoélectrique Laser d'un inverseur.

De plus, la tension de sortie de l'inverseur n'est que très faiblement modifiée par le tir laser (quelques dizaine de mV voir ***Figure II. 59***). En effet, le courant de saturation des transistors MOS est de l'ordre de la centaine de µA. Ce courant est beaucoup plus important

que le photocourant généré par le drain du transistor NMOS qui est de l'ordre de la dizaine de µA.

Lorsque l'entrée V_{IN} de l'inverseur est polarisée à 1,2 V, le transistor NMOS est cette fois-ci en régime saturé et le PMOS est bloqué. A pleine puissance laser (40 mW), la sortie V_{OUT} de l'inverseur augmente également de quelques dizaines de mV. En effet, le photocourant généré par le drain du transistor PMOS est trop faible (quelques dizaines de µA) par rapport au courant de saturation du transistor NMOS qui est de l'ordre d'une centaine de µA.

II.4.2.2 Simulation TCAD 2D

Afin de corréler les résultats de mesures, une structure TCAD 2D d'un inverseur a été créée en partant du layout de la structure utilisée en mesures. Ce layout a été légèrement modifié. En effet, les transistors MOS ont subi une rotation d'un angle de 90° par rapport au layout présenté ***Figure II. 50*** pour que toutes les jonctions PN de l'inverseur soient visibles dans le plan de coupe défini pour la simulation TCAD (voir ***Figure II. 55***). Dans cette simulation une onde plane illuminant la face arrière du composant est utilisée. La puissance du laser en simulation est à considérer de manière qualitative plutôt que quantitative, puisque les simulations ne sont pas calibrées par rapport aux mesures.

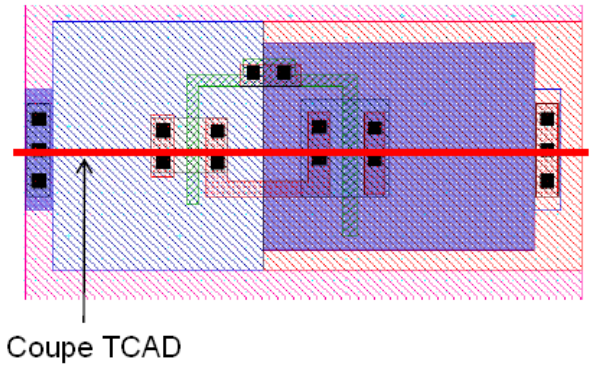


Figure II. 55. Layout de l'inverseur avec la ligne de coupe TCAD.

Le résultat de la coupe TCAD est présenté ***Figure II. 56***.

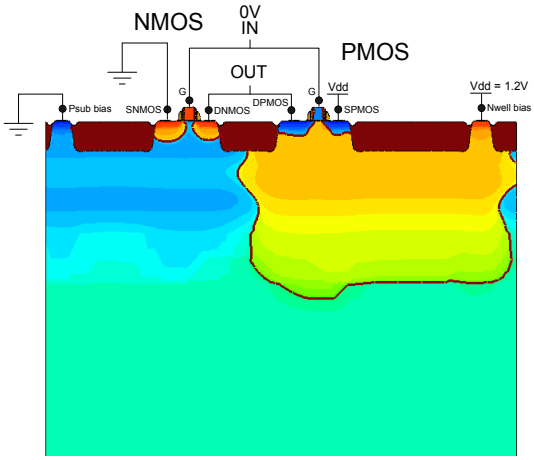
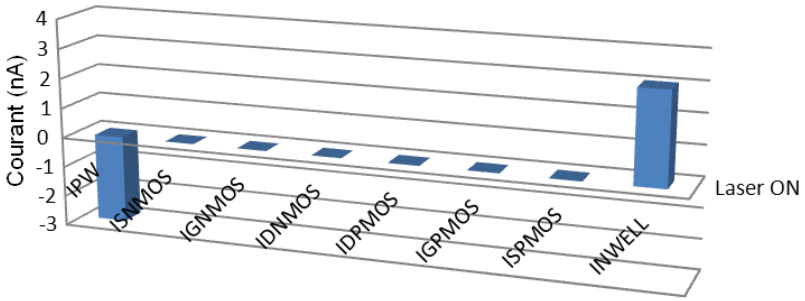


Figure II. 56. Coupe TCAD de l'inverseur.

Le graphique et le tableau présenté ***Figure II. 57*** donnent les courants obtenus par simulation TCAD 2D. Ils montrent de manière qualitative, que la majorité du photocourant est généré par la jonction Nwell/Substrat de type P. En effet, il existe pour ce photocourant, une différence d'environ 3 décades par rapport aux autres jonctions. Ceci est dû à la surface de la jonction Psub/Nwell qui est beaucoup plus importante que les autres présentes dans l'inverseur.



	IPW	ISNMOS	IGNMOS	IDNMOS	IDPMOS	IGPMOS	ISPMOS	INWELL
(A)	-2.90E-09	4.10E-13	0	1.00E-13	-9.60E-12	-2.17E-15	-9.58E-12	3.04E-09

Figure II. 57. Résultats de simulation TCAD 2D de l'inverseur sous Stimulation Photoélectrique Laser.

Une fois que la campagne de mesures et de simulation TCAD 2D a été réalisée, il est maintenant possible de modéliser l'inverseur sous SPL continue à partir des modèles développés pour des transistors MOS isolés.

II.4.2.3 Modélisation électrique

Une fois analysés les effets générés par Stimulation Photoélectrique Laser, il est possible de faire une modélisation assez fine de la structure de test d'inverseurs éclairés par une onde lumineuse laser. La ***Figure II. 58*** représente la méthode mise en œuvre pour assembler les modèles de transistors sous SPL continue déjà existant, pour modéliser la structure de test complète sous illumination laser. Seuls les neuf inverseurs sans deep Nwell ont été inclus dans notre modélisation.

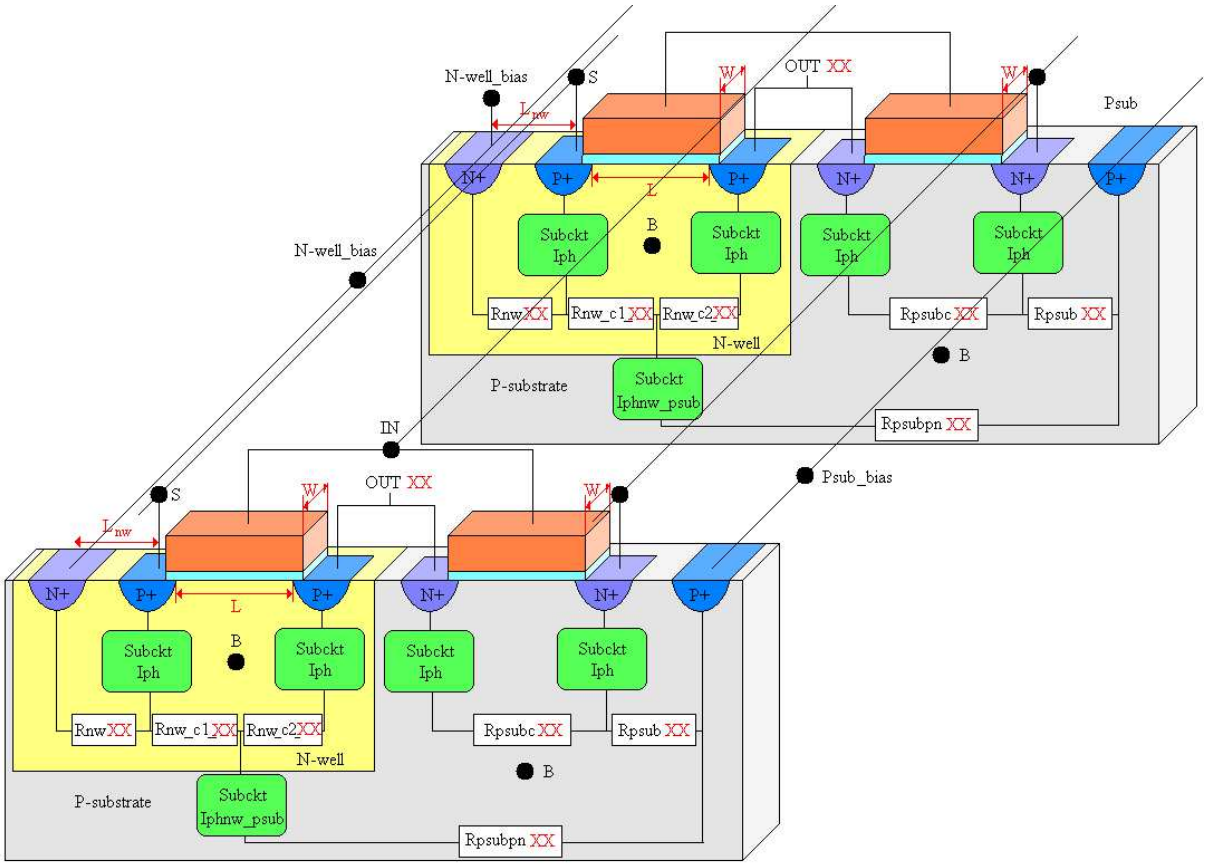


Figure II. 58. Principe de modélisation de la structure de test en réutilisant les modèles déjà développés de transistors sous stimulation photoélectrique laser.

Afin de calibrer le modèle, par simulation les paramètres du laser ont été fixés dans les mêmes conditions que lors de la campagne de mesure. La ***Figure II. 59*** montre la bonne corrélation entre la simulation électrique et les mesures, au niveau de la tension de sortie de

l'inverseur pour différentes puissances laser, validant ainsi toute les étapes précédentes de modélisations.

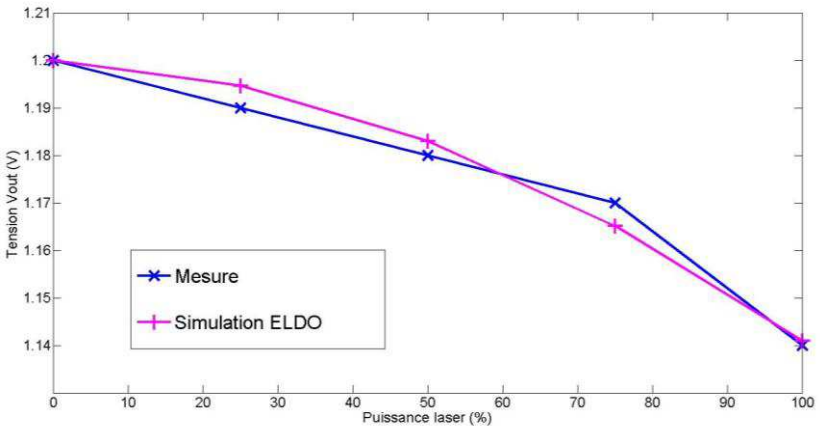


Figure II. 59. Comparaison entre mesures et simulation électrique de l'évolution de la tension de sortie en fonction de la puissance du laser.

Les effets du laser sur un inverseur constitué uniquement de deux transistors restent relativement simples dans le cas d'une SPL continu de faible puissance. Par contre dès que la puissance du laser augmente, comme c'est le cas avec le laser impulsionnel forte puissance, les effets deviennent beaucoup plus complexes. En effet, de nombreux transistors bipolaires parasites peuvent s'enclencher conséquemment à des modifications des tensions locales du substrat de type P ou du caisson de type N. La suite de ce chapitre présente les différentes mesures faites sur l'inverseur grâce au laser impulsionnel forte puissance. Le modèle proposé sera basé sur les modélisations déjà effectuées des transistors NMOS et PMOS. Ainsi des simulations électriques pourront être corrélées avec les mesures effectuées sur silicium afin de valider tout le flot de modélisation.

II.4.3 Mesures et modèle électrique à forte puissance laser

En termes d'injection de faute, l'un des aspects les plus importants consiste à analyser l'impact que peut avoir le laser sur la tension de sortie d'une porte. C'est la raison pour

laquelle la suite de cette étude va montrer l'effet d'une impulsion laser sur la tension de sortie de l'inverseur.

Dans cette partie, la même structure de test qu'au paragraphe précédent est utilisée. Cette fois-ci les mesures ont été réalisées avec le laser impulsionnel forte puissance. L'objectif utilisé a été celui produisant un grossissement de 20 X, délivrant une taille de spot de 5 µm. La durée d'impulsion du laser est fixée à 20 µs. L'injection laser était effectuée par la face arrière.

II.4.3.1 Mesures

Dans un premier temps, tous les courants mesurables de l'inverseur ont été relevés lorsque la tension d'entrée V_{IN} de l'inverseur était égale à 0 V. La ***Figure II. 60*** montre les mesures du courant de source du transistor PMOS pour une puissance laser variant entre 0,03 W et 0,67 W.

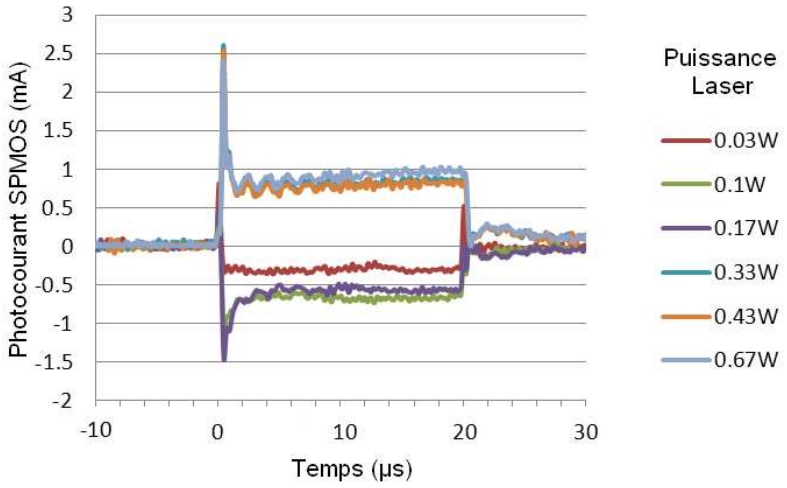


Figure II. 60. Courants mesurés de la source du transistor PMOS en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec une tension d'entrée V_{IN} à 0 V.

A des puissances inférieures à 0,17 W, le courant mesuré sur l'électrode de source du PMOS est constitué uniquement de son propre photocourant (généré par la jonction Source du PMOS/Nwell). A partir d'une puissance de 0,17 W le courant mesuré s'inverse (voir

Figure II. 60). L'une des hypothèses serait que le transistor bipolaire parasite SPMOS/Nwell/Psub se soit déclenché à forte puissance laser, comme vu lors de l'étude du transistor PMOS isolé (voir ***paragraphe II.2.2.2.2.1***).

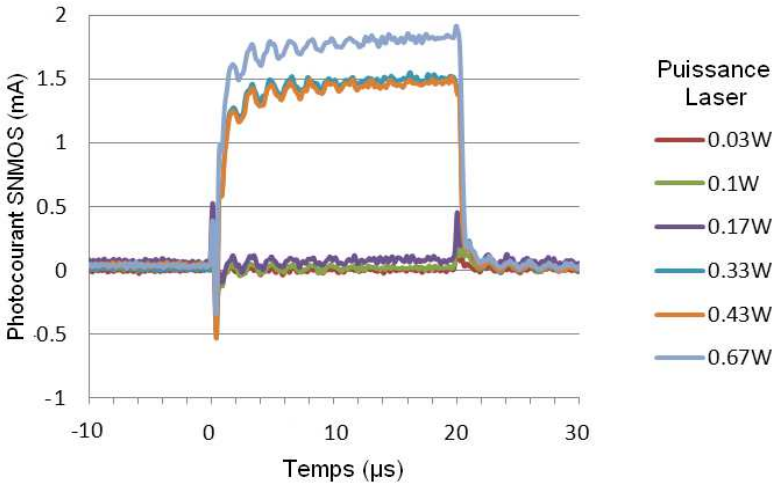


Figure II. 61. Courants mesurés de la source du transistor NMOS en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 0V.

Le graphique présenté ***Figure II. 61*** montre qu'à une puissance inférieure à 0,17 W le courant mesuré sur l'électrode de source du transistor NMOS est constitué de son propre photocourant (généré par la jonction source du NMOS/Psub). A partir de la puissance 0,17 W, le sens du courant mesuré s'inverse, et cela, de manière importante. L'hypothèse dans ce cas de figure semble être qu'à forte puissance laser, le transistor bipolaire parasite drain/Psub/source du transistor NMOS se soit déclenché, comme vu lors de l'étude du transistor NMOS isolé (voir ***paragraphe II.2.1.2***).

Les graphiques présentés ***Figure II. 62*** et ***Figure II. 63*** donnent respectivement les courants mesurés aux niveaux des contacts de polarisation du puits N et du substrat P. Ils mettent en évidence le photocourant généré par la jonction Nwell/Psub.

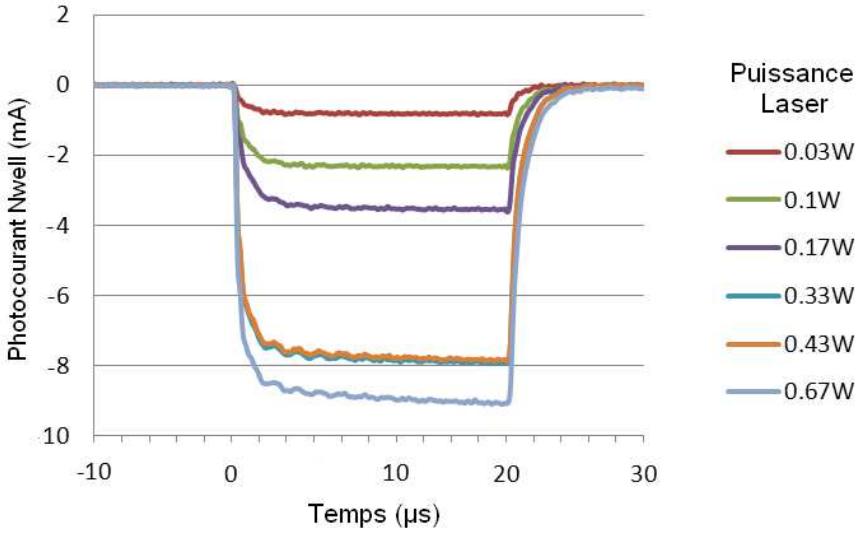


Figure II. 62. Courants mesurés sur le contact de polarisation du Nwell en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 0 V.

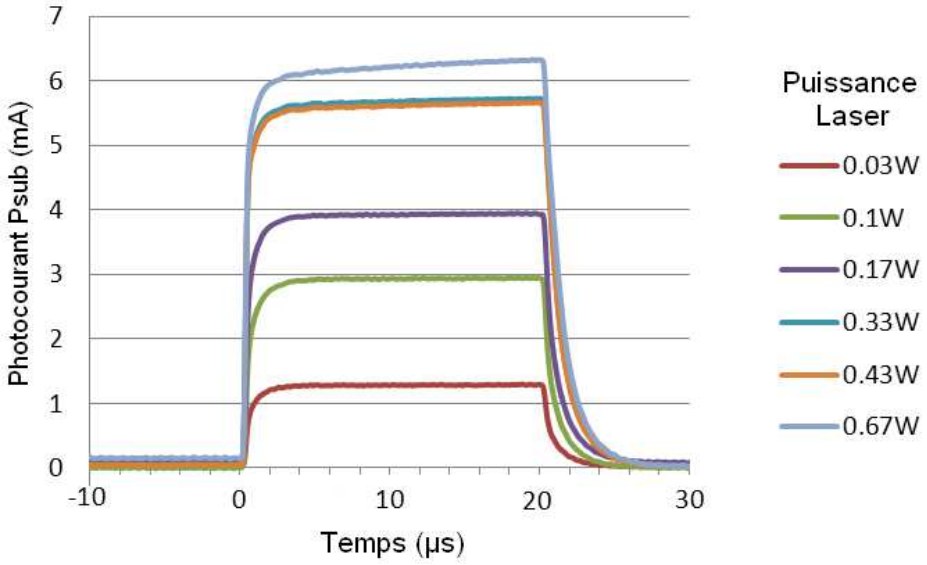


Figure II. 63. Courants mesurés sur le contact de polarisation du substrat de type P en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 0 V.

Il est possible de remarquer que le courant mesuré sur l'électrode de Nwell devient supérieur à celui du Psub. Ceci s'expliquerait par l'activation du transistor bipolaire parasite Nwell/Psub/implant N+ du transistor NMOS.

Le graphique présenté ***Figure II. 64*** met en évidence l'évolution de la tension de sortie de l'inverseur en fonction de la puissance du laser. Lorsque cette puissance est faible (jusqu'à 0,17 W), le photocourant généré par le drain du transistor NMOS permet de faire chuter la tension avec un impact limité à une centaine de mV. En augmentant la puissance du laser, le transistor bipolaire parasite drain du PMOS/Nwell/Psub, en s'enclenchant, va faire chuter plus fortement le potentiel de sortie de l'inverseur jusqu'à une saturation pour une puissance laser de 1 W (0,4 V sur la figure ci-dessous).

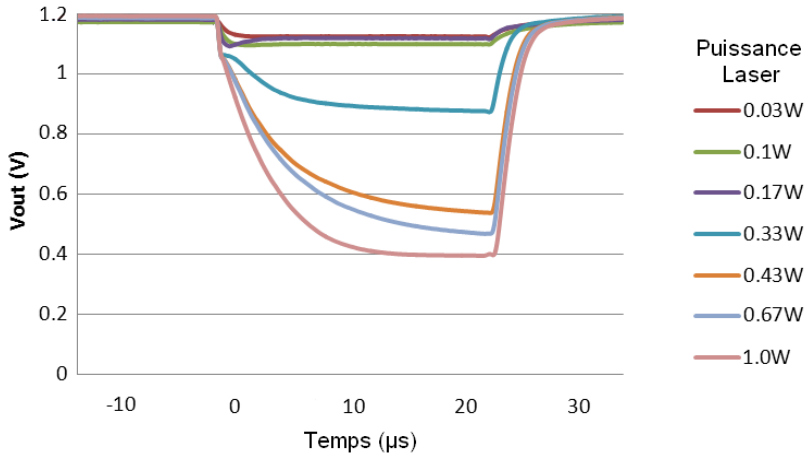


Figure II. 64. Evolution de la tension de sortie V_{OUT} en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 0V.

Il est possible d'observer qu'à partir de la puissance de 0,43 W la tension de sortie passe en dessous du seuil de l'inverseur (0,6 V).

Les mêmes mesures présentées précédemment ont été réalisées lorsque la tension d'entrée de l'inverseur était de 1,2 V. Le graphique présenté ***Figure II. 65*** montre l'évolution du courant de source du transistor PMOS en fonction du temps pour différentes puissances laser.

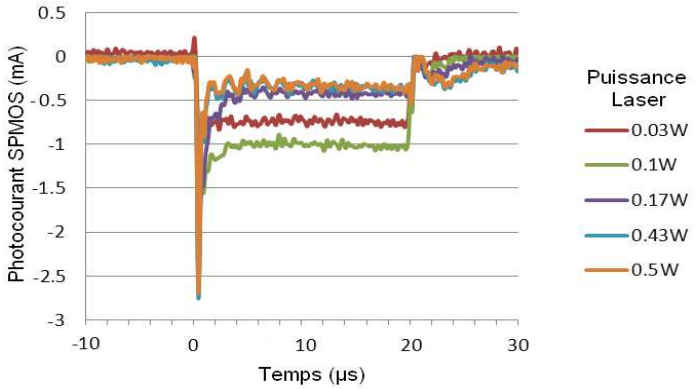


Figure II. 65. Courants mesurés de la source du transistor PMOS en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 1.2 V.

Le graphique présenté ***Figure II. 65*** montre qu'à une puissance inférieure à 0,17 W le courant mesuré sur l'électrode du transistor PMOS est constitué uniquement de son propre photocourant (généré par la jonction source du PMOS/Nwell). A partir d'une puissance laser de 0,17 W, le courant mesuré sur la source du transistor NMOS diminue sans changer de signe. L'hypothèse dans ce cas de figure semble être qu'à forte puissance laser, le transistor bipolaire parasite source du PMOS/Nwell/Psub du transistor NMOS soit déclenché, comme vu dans le cas où l'entrée de l'inverseur était polarisé à 0 V.

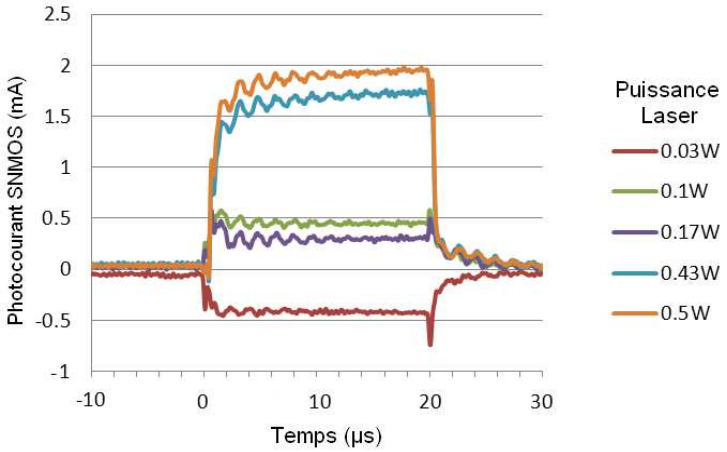


Figure II. 66. Courants mesurés de source du transistor NMOS en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 1,2 V.

L'inversion de sens du courant mesuré sur l'électrode de la source du transistor NMOS (due au transistor bipolaire parasite drain/Psub/source) est également visible dans cette configuration (voir ***Figure II. 66***).

Les graphiques présentés ***Figure II. 67*** et ***Figure II. 68*** donnent respectivement les courants mesurés aux niveaux des contacts de polarisation du puits N et du substrat P. Ils mettent en évidence le photocourant généré par la jonction Nwell/Psub.

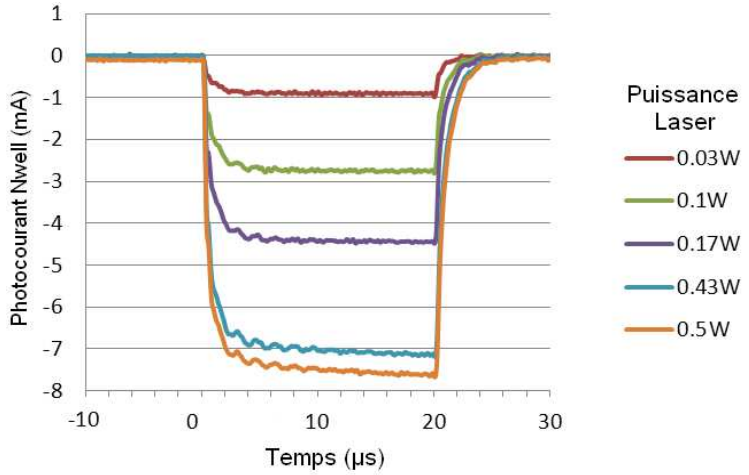


Figure II. 67. Courants mesurés sur le contact de polarisation du Nwell en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 1,2 V.

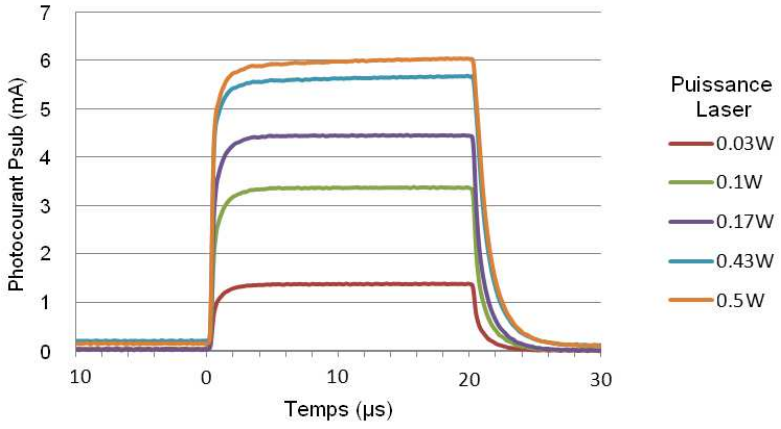


Figure II. 68. Courants mesurés sur le contact de polarisation du substrat P en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur étudié avec la tension d'entrée V_{IN} à 1,2 V.

A partir de la puissance laser 0,17 W, le courant mesuré sur l'électrode de Nwell, devient supérieur à celui du substrat de type P. Ceci semblerait être dû à l'activation du transistor bipolaire parasite Nwell/Psub/N+ comme dans le cas où la tension d'entrée était de 0 V. Ainsi du courant peut circuler du Nwell jusqu'au drain et source du transistor NMOS pouvant ainsi faire augmenter la tension de sortie de l'inverseur.

Le graphique de la ***Figure II. 69*** met en évidence l'évolution de la tension de sortie en fonction de la puissance sur laser.

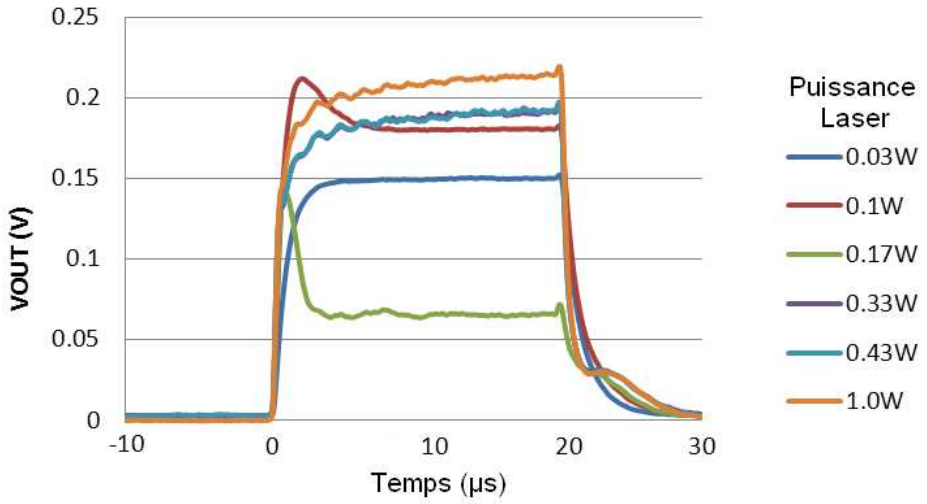


Figure II. 69. Evolution de la tension de sortie V_{OUT} en fonction de la puissance du laser lorsque le spot est centré en plein milieu de l'inverseur numéro 1 avec la tension d'entrée V_{IN} à 1,2 V.

A la puissance laser 0,03 W, la tension de sortie de l'inverseur V_{OUT} augmente jusqu'à 0,15 V, dû au photocourant généré par la jonction drain du PMOS/Nwell. Dès la puissance 0,1 W, la tension de sortie augmente jusqu'à 0,15 V au début de l'impulsion laser. Ensuite, un transistor bipolaire parasite a tendance à faire chuter la tension de sortie jusqu'à un état d'équilibre vers 0,7 V. Ceci est dû majoritairement à l'activation du transistor bipolaire parasite Drain du PMOS/Nwell/Psub. Par la suite, dès 0,33 W, l'activation du transistor bipolaire parasite Nwell/Psub/drain du NMOS a tendance à faire croître à nouveau la tension V_{OUT}.

II.4.3.2 Modélisation électrique de l'inverseur

II.4.3.2.1 Présentation du modèle

Grâce aux mesures présentées au paragraphe précèdent, il semblerait que les modèles développés pour les transistors séparés (NMOS et PMOS) peuvent être réutilisés. Une modélisation de l'inverseur sous SPL impulsionnel est proposée, ayant des similitudes avec celle de [Amu06] (voir ***Figure II. 70***).

Toutefois, il est nécessaire d'ajouter entre les modèles des transistors NMOS et PMOS, les transistors bipolaires parasites Nwell/Psub/N+.

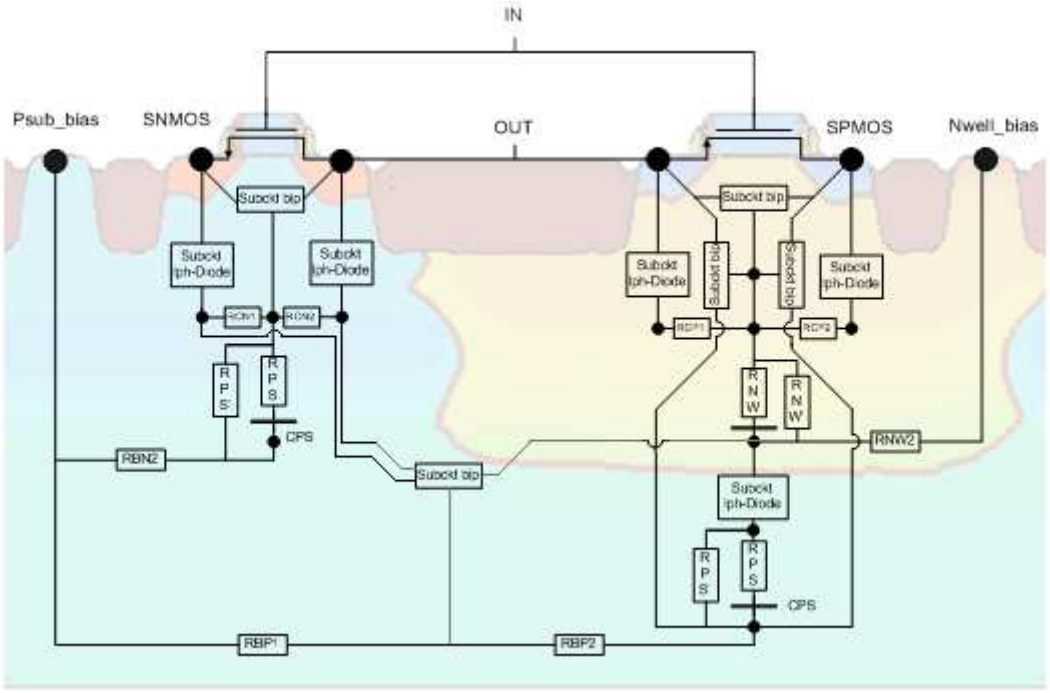


Figure II. 70. Modèle électrique complet de l'inverseur sous SPL impulsionnelle.

Une étape de calibration est nécessaire afin de retrouver les résultats obtenue en simulation. Cette calibration se fait notamment en changeant les valeurs des résistances présentes dans le modèle de la ***Figure II. 70***. Afin de rendre moins hasardeuse cette étape de calibration, le modèle a été simplifié, comme il est possible de le constater à la ***Figure II. 71***. Seules les résistances importantes du modèle ont été conservées. La résistance *RBN2* représente le chemin résistif que doit parcourir le photocourant allant du centre du transistor

NMOS à la prise de polarisation du substrat de type P. En outre c'est elle qui, lorsque le photocourant généré par les jonctions N+/Psub du transistor NMOS sera suffisamment important, va faire monter le potentiel local du substrat de type P (potentiel *N* sur la ***Figure II. 71***) ce qui pourra entraîner le déclenchement du transistor bipolaire parasite drain/Psub/source, comme vu en [Bua07]. La résistance *RNW2*, représente, elle, le chemin résistif allant du centre du transistor PMOS à la prise de polarisation du caisson de type N. Cette résistance est importante, car c'est elle qui, à forte puissance laser peut faire déclencher les transistors bipolaires parasites PNP verticaux (P+/Nwell/Psub), si le potentiel P chute en dessous de 0,6 V.

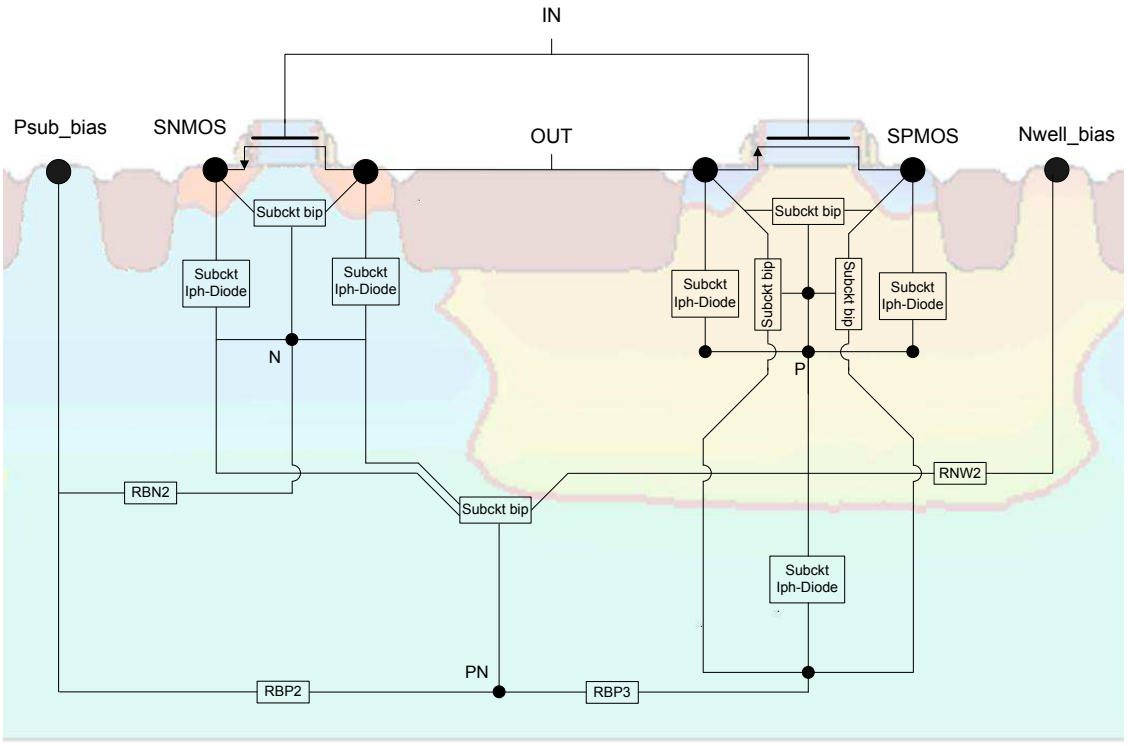


Figure II. 71. Modèle électrique simplifié de l'inverseur sous SPL impulsionnelle.

Afin de valider le modèle, des simulations électriques ont été réalisées et comparées aux mesures. Il est à noter que ces simulations sont plutôt qualitatives que quantitatives. Ceci est dû au fait que les sous-circuits utilisés pour simuler les effets des différents transistors bipolaires parasites pouvant s'amorcer dans le circuit, ne sont pas calibrés.

La ***Figure II. 72*** présente les courants mesurés sur les électrodes de sources du NMOS et du PMOS, ainsi que les courants sur les électrodes du Nwell et du Psub. La tension de

sortie de l'inverseur V_{OUT} est également représentée. Etant donné que la simulation n'est pas calibrée les valeurs de puissance laser ne peuvent pas être comparées aux mesures. La variation de puissance donne ainsi une indication sur les effets d'illumination de l'inverseur étudié.

La simulation électrique a été réalisée avec une tension d'entrée V_{IN} égale à 0 V.

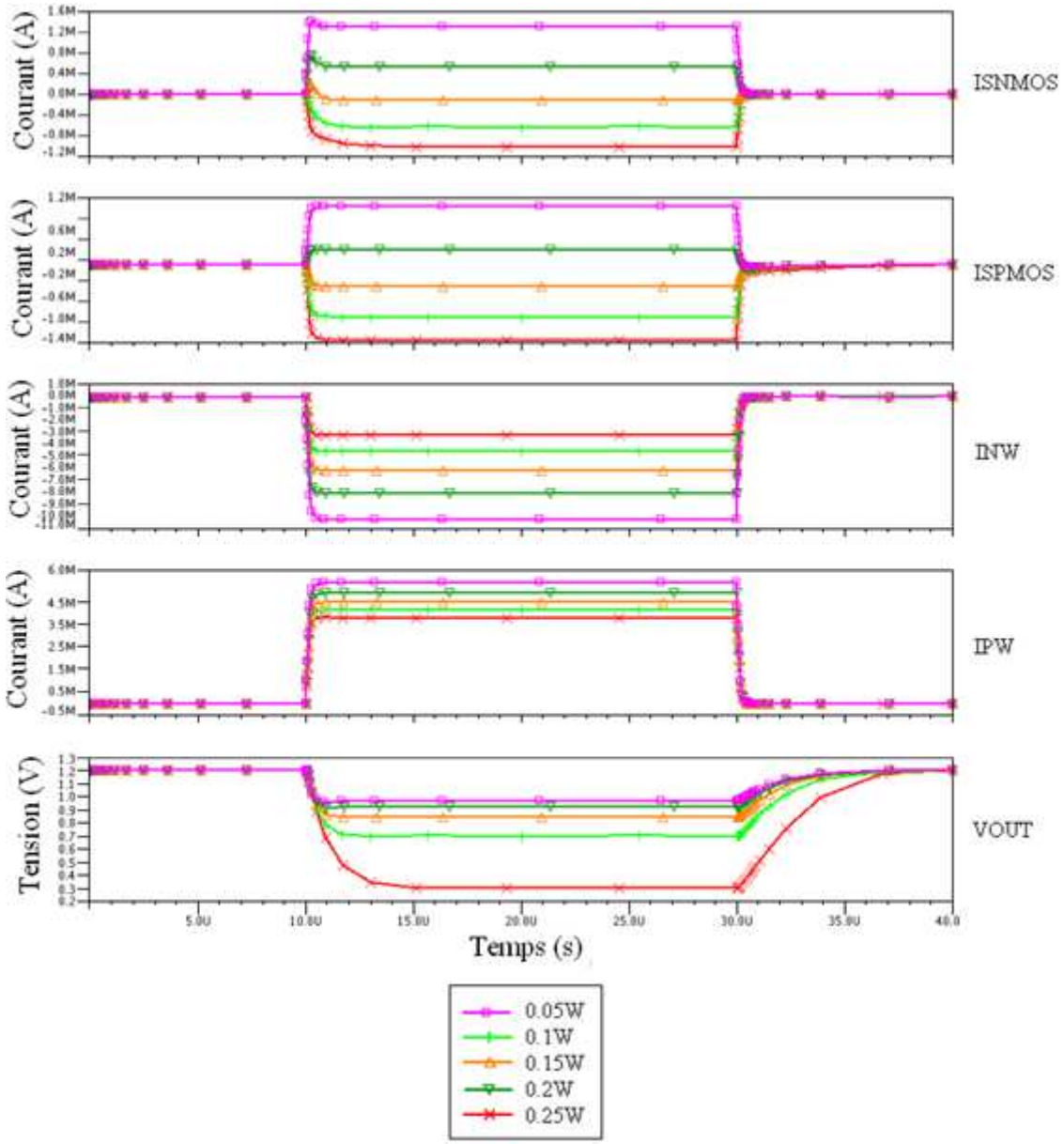


Figure II. 72. Simulations électriques de l'inverseur lorsque l'entrée V_{IN} est polarisé à 0V, pour différentes puissances laser.

La ***Figure II. 72*** montre l'inversion des courants des deux sources lorsque la puissance du laser augmente, comme vu en mesure. L'inversion du courant de source du transistor NMOS est due aux transistors bipolaires parasites drain du NMOS/Psub/source du NMOS et Nwell/Psub/source du PMOS. L'inversion de la source du PMOS est, elle, due au transistor bipolaire source du PMOS/Nwell/Psub. Il est également possible de noter que le courant mesuré sur le contact du Nwell est supérieur au courant mesuré sur le contact du Psub. Cet effet est dû aux transistors bipolaires parasites Nwell/Psub/source du NMOS et Nwell/Psub/drain du NMOS. Le courant passe donc de la prise de polarisation du caisson N aux implants N+ du transistor NMOS.

II.4.3.2.2 Cartographies de la structure de test d'inverseur

Alors que dans le ***paragraphe II.4.3.1***, le laser était positionné de façon centré en plein milieu de l'inverseur étudié, il est maintenant proposé d'établir des cartographies en courant et en tension de la structure de test d'inverseur.

Pour cette analyse, les paramètres suivants ont été fixés: la taille de spot était de 5 µm focalisé sur la zone active des transistors, la puissance du laser en sortie d'objectif était de 420 mW et la durée d'impulsion de 20 µs. Il est toutefois à noter que les résultats de cartographies sont une nouvelle fois qualitatifs plutôt que quantitatifs, étant donné que tous les éléments de la simulation ne sont pas calibrés.

La méthodologie pour créer les cartographies de simulation est la même que celle présentée au ***paragraphe II.2.1.1.2.3***. Le pas du maillage a été choisi égal à 15 µm. Les cartographies ont été réalisées, dans un premier temps, lorsque la tension d'entrée de la structure était polarisée à 0 V.

La ***Figure II. 73*** présente les cartographies de la tension de sortie V_{OUT} pour la mesure et la simulation.

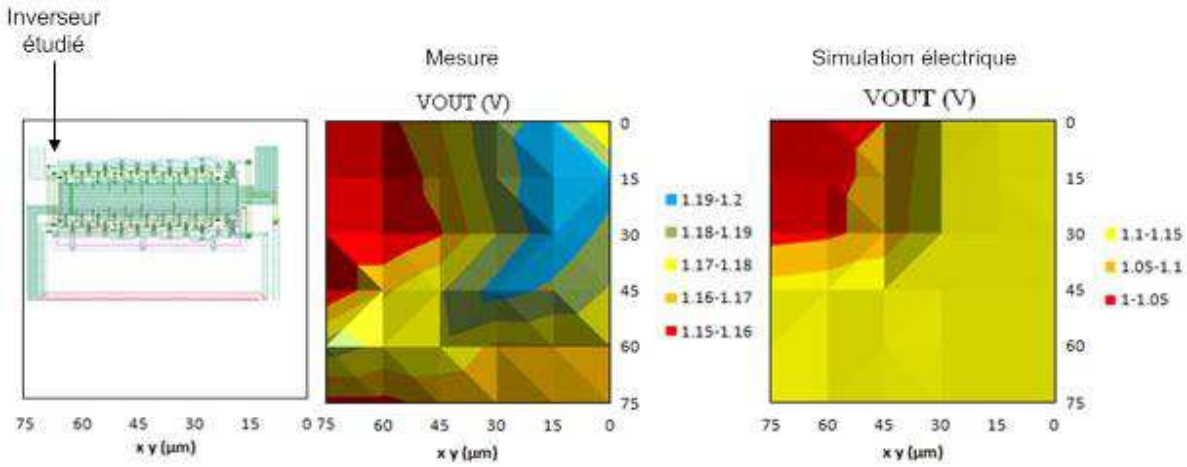


Figure II. 73. Cartographie de la tension de sortie de l'inverseur lorsque Vin est à 0V.

La chute la plus forte de la tension de sortie se trouve dans la localisation spatiale de l'inverseur étudié.

La ***Figure II. 74*** montre les cartographies du courant mesuré sur l'électrode du Nwell par la mesure expérimentale et par simulation. Cette électrode polarise parallèlement les différents caissons de type N des différents inverseurs. C'est cette raison qui explique le fait que le photocourant généré n'est pas uniquement localisé près de l'inverseur étudié.

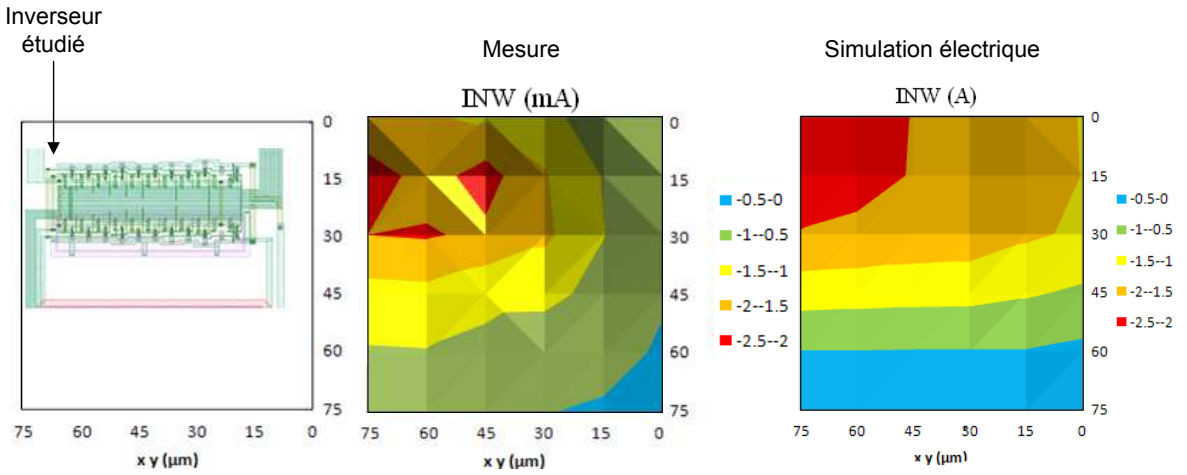


Figure II. 74. Cartographie du photocourant INWell de la structure d'inverseur lorsque V_{IN} est à 0V.

De la même manière, les cartographies en courant du Pwell sont présenté ***Figure II. 75***.

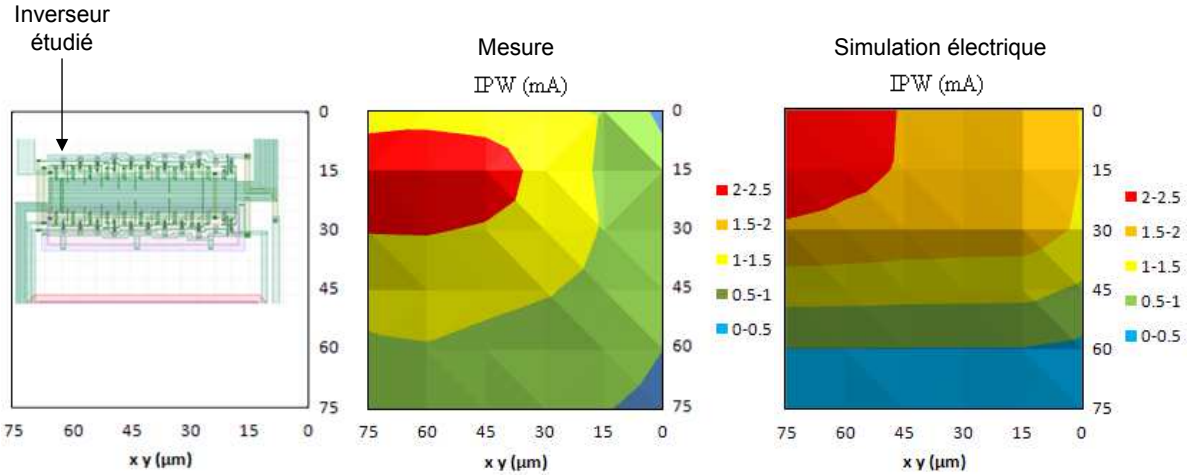


Figure II. 75. Cartographie du photocourant IPWell de la structure d'inverseurs lorsque V_{IN} est à 0V.

Il est ensuite proposé de comparer les cartographies de mesure et de simulation du courant de la source du transistor PMOS (voir ***Figure II. 76***).

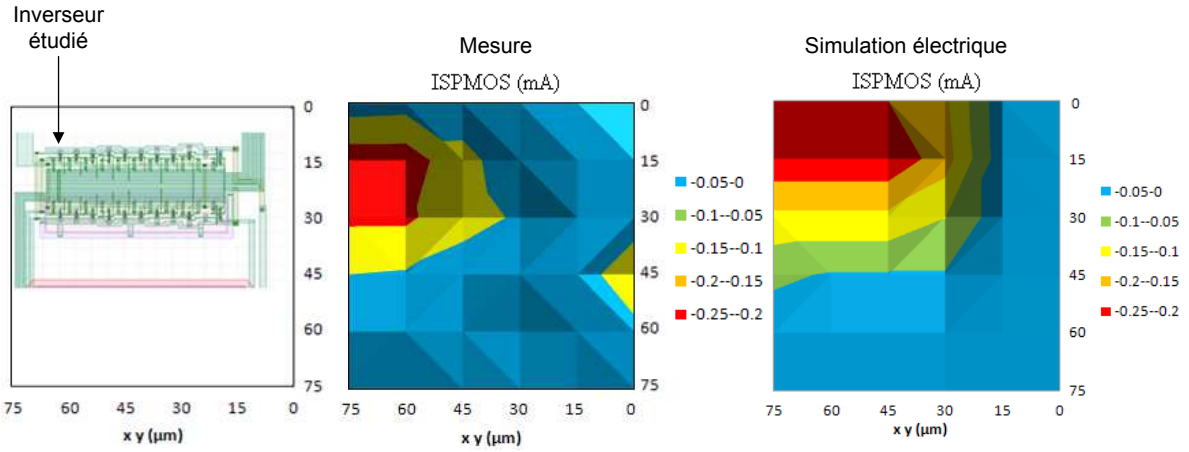


Figure II. 76. Cartographie du photocourant de la source du transistor PMOS de la structure d'inverseurs lorsque V_{IN} est à 0V.

Il est également possible d'observer les cartographies de mesure et de simulation de source du transistor NMOS (voir ***Figure II. 77***).

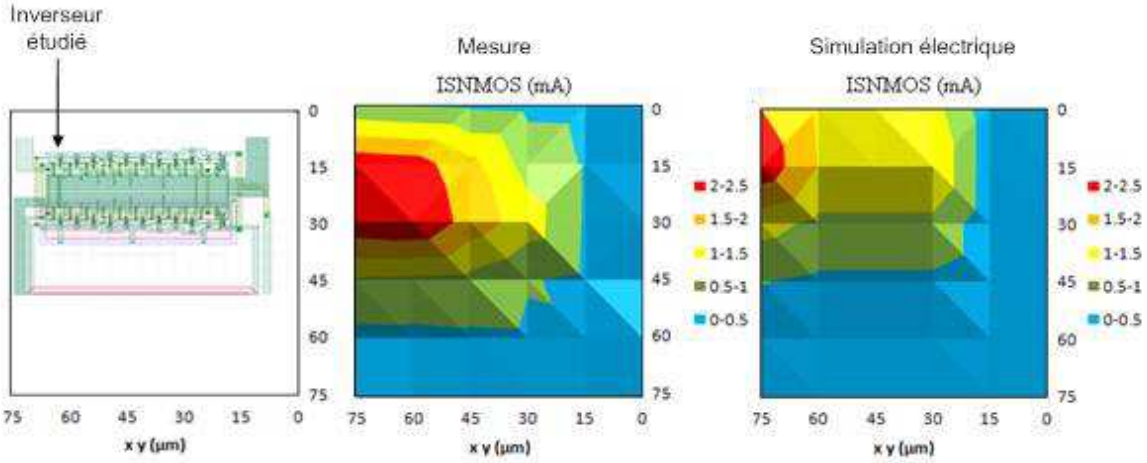


Figure II. 77. Cartographie du photocourant de la source du transistor NMOS de la structure d'inverseurs lorsque V_{IN} est à 0V.

Il est donc possible de remarquer certaines différences entre les cartographies de mesure et de simulation. Ceci est principalement dû au fait que le pas de maillage n'est pas assez fin et que les modèles développés ont été faits pour des structures plus grandes que la taille du spot laser alors que dans ce cas d'étude, c'est l'inverse.

II.4.4 Inverseur avec implant deep Nwell

L'effet de l'implant deep Nwell sur un inverseur, qui a déjà préalablement fait l'objet d'étude, comme présenté par exemple en [Vol05]. Dans cette partie, faute de mesure, des simulations TCAD ont été réalisées. La ***Figure II. 78*** présente une coupe TCAD 2D d'un inverseur avec (a) et sans deep Nwell (b).

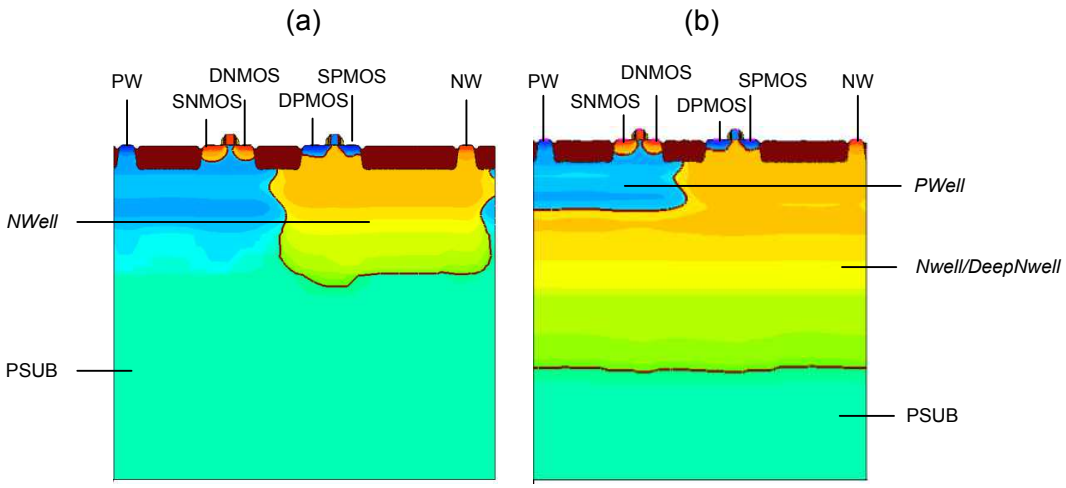


Figure II. 78. Coupe TCAD d'un inverseur: (a) standard (b) avec implant deep Nwell.

En simulation, la polarisation suivante a été appliquée sur les deux structures différentes présentées ci-dessus : les drains des transistors MOS ainsi que le Nwell (dans le cas de la structure standard) ou le Nwell connectant le deep Nwell dans le cas de la structure avec deep Nwell) était porté au potentiel de 1,2 V. Les autres électrodes étaient connectées à la masse.

Le ratio (courant simulé dans la structure standard divisé par celui de la structure avec deep Nwell) a été effectué à même puissance. Ces valeurs de ratio sont présentées dans le ***Tableau II. 4***.

Électrode	**Ratio**
IPW	0.77
ISNMOS	0.12
ISPMOS	0.88
IDNMOS	0.25
IDPMOS	0.55
INW	89
IPSUB	88

Tableau II. 4. Ratio entre le courant simulé dans la structure standard divisé par celui de la structure avec deep Nwell, pour les différentes électrodes.

L'ajout de l'implant deep Nwell semble donc augmenter drastiquement le courant dans le substrat tout en réduisant faiblement le photocourant sur les implants des transistors.

Ceci est dû à la différence de mécanisme de collection de charges, notamment au niveau du transistor NMOS, puisque le puits P (Pwell) où se trouve ce transistor est isolé du substrat de Psub. La tension V_{OUT} de l'inverseur serait donc moins perturbée grâce à l'implant Deep Nwell. Toutefois, ce propos est à nuancer car l'ajout de l'implant deep Nwell rajoute des transistors bipolaires parasites (Pwell/deep Nwell/Psub et N+/Pwell/deep Nwell) qui en s'enclenchant peuvent venir perturber tout autant la tension de sortie. Cependant, il est à préciser que les résultats concernant ce cas d'étude sont à l'heure actuelle incomplète. Des mesures et simulation afin de bien appréhender les phénomènes physiques mis en jeux reste encore à faire.

II.5 Cellule SRAM

Dans cette partie le modèle de transistors MOS sous stimulation photoélectrique a été appliqué à une cellule SRAM en technologie CMOS 0,25 µm. Le banc qui a été utilisé mettait en œuvre un laser impulsionnel forte puissance (allant de 0 à 1,6 W). Toutefois, les résultats de simulation qui suivent sont à considérer de manière qualitative plutôt que quantitative. En effet, les modèles de transistors MOS sous Stimulation Photoélectrique Laser ont été réalisés, en face arrière du composant, à partir d'une technologie CMOS 90 nm de STMicroelectronics alors que la cellule SRAM est fabriquée à partir d'une technologie CMOS STMicroelectronics de 0,25 µm. Il faut noter que l'injection laser sur cette cellule s'est faite par la face avant.

II.5.1 Analyse de la sensibilité de la SRAM aux SEU

II.5.1.1 Présentation de la cellule SRAM

La cellule SRAM étudiée dans ce paragraphe est une SRAM de configuration (CSRAM) constituée de 5 transistors (voir ***Figure II. 79***) similaire à celles utilisées pour stocker les bits de configuration des bitstreams dans les circuits programmables de type

FPGA. Dans ce paragraphe, le terme SRAM est utilisé, puisque l'hypothèse est prise que les résultats principaux, peuvent être généralisés à une SRAM classique à 6 transistors.

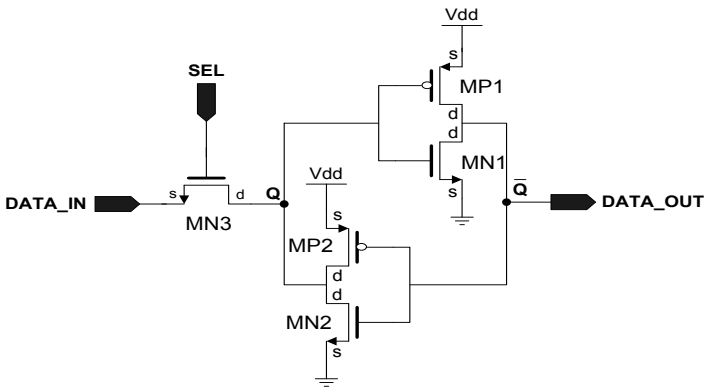


Figure II. 79. Schéma électrique de la cellule SRAM de configuration (CSRAM).

La cellule SRAM de configuration est constituée d'un couple d'inverseurs rebouclés (transistors *MP1*, *MN1*, *MP2*, *MN2*) pour la mémorisation de l'information et d'un transistor d'accès (*MN3*) qui, lorsqu'il est passant (ON) permet l'écriture et lorsqu'il est bloqué (OFF), permet de mémoriser la donnée écrite.

II.5.1.2 Etude de la sensibilité de la cellule SRAM

Dans ce paragraphe, la sensibilité de la cellule SRAM est étudiée à partir d'un point de vue théorique, en considérant son schéma électrique et son état défini de la façon suivante: l'état « 1 » (respectivement état "0") est défini, par convention, lorsque le nœud *DATA_OUT* est à l'état haut (respectivement état bas). Ainsi, à l'état « 0 », le nœud *Q* est à la valeur logique « 1 » alors que le nœud $\overline{Q}$ est à « 0 ». A l'état « 1 » les valeurs logiques des nœuds *Q* et $\overline{Q}$ sont inversées par rapport à celles de l'état « 0 ».

La sensibilité de la cellule, dans ce cas de figure statique (le transistor *MN3* étant bloqué), peut être étudiée en considérant quelles jonctions PN sont le plus fortement polarisées en inverse en fonction de l'état de la SRAM. Les cas « 1 » et « 0 » sont envisagés. Les flèches rouges présentent sur la ***Figure II. 80*** donnent les directions des photocourants induits entre le drain ou la source et le substrat des différents transistors. Les flèches les plus larges représentent de forts photocourants et les plus fines des photocourants plus faibles.

Les photocourants les plus importants sont générés par les jonctions PN les plus fortement polarisées en inverse. Les photocourants les plus faibles sont générés par les jonctions PN polarisées avec une différence de potentiel de 0 V.

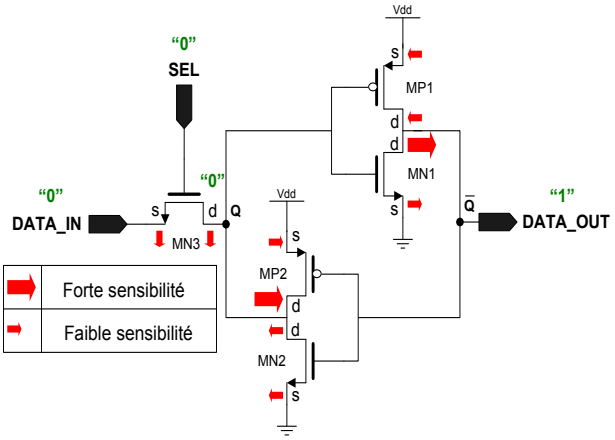


Figure II. 80. Détail des sensibilités de la SRAM à l'état "1".

Dans l'état "1", les deux zones les plus sensibles à une illumination laser sont les jonctions de drain des transistors *MN1* et *MP2* (drains des transistors bloqués comme vu au ***paragraphe I.4***). En effet dans ces conditions de polarisations, ce sont ces jonctions, qui sont le plus fortement polarisées en inverse.

Dans l'état "0", les deux zones les plus sensibles sont d'une part la jonction de drain du transistor *MP1* et d'autre part celle qui est commune aux drains des transistors *MN2* et *MN3* (voir ***Figure II. 81***).

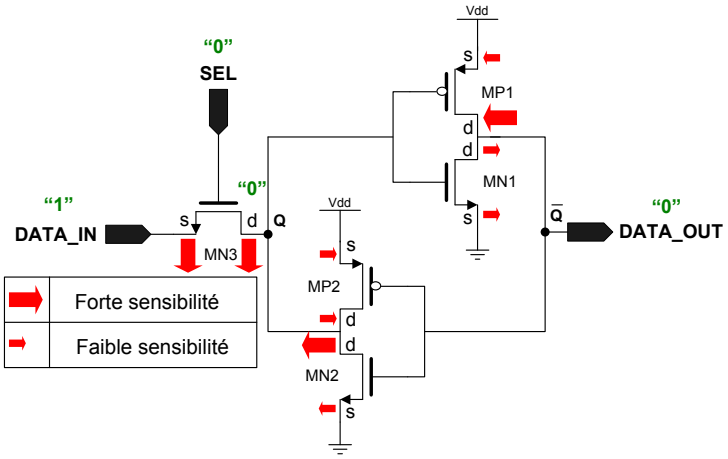
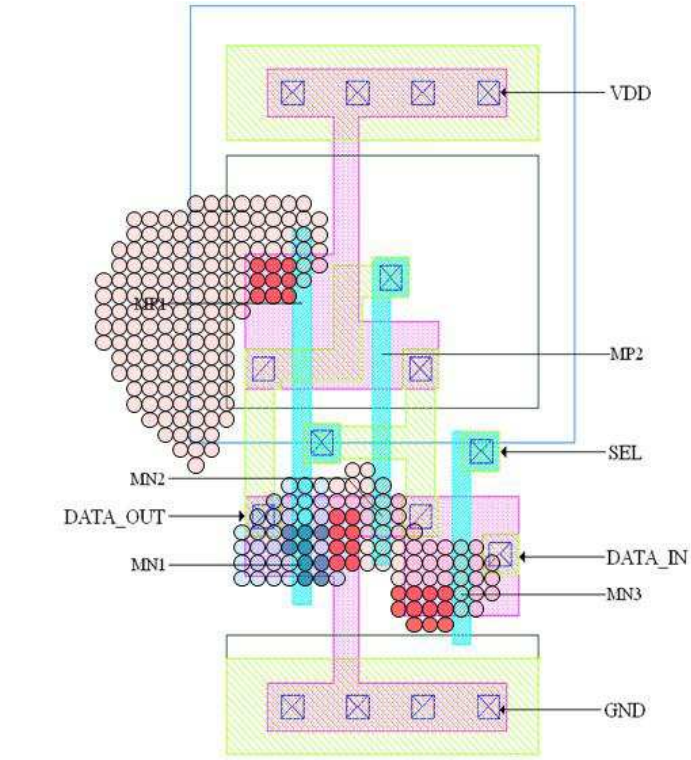


Figure II. 81. Détail des sensibilités de la SRAM à l'état "0".

L'étude précédente, basée sur la mesure de l'effet d'une SPL sur des transistors NMOS et PMOS isolés ***(paragraphes II.2.1 et II.2.2)***, permet d'identifier quatre zones particulièrement sensibles à une illumination laser. Ce sont les drains des transistors *MN1* et *MP2* à l'état « 1 », et les drains de *MN2/MN3* et *MP1* à l'état *« 0 »*. Il est effectivement possible de constater, sur le layout de la cellule SRAM (voir ***Figure II. 83***), que les drains de *MN2* et *MN3* sont mis en commun.

II.5.1.3 Mesures de la sensibilité de la cellule SRAM aux SEU

Il est possible de tester la sensibilité d'un circuit par la face avant dans le cas de faible densité de métallisation. Dans ce cas de figure le phénomène d'absorption du silicium par la face arrière, faisant perdre de la puissance à l'onde lumineuse laser arrivant sur les jonctions PN, n'entre pas en jeu. La densité de métallisation en face avant était donc réduite au minimum afin de ne pas gêner une injection laser par cette face. La série de test a été faite avec un laser à impulsion de forte puissance, attaquant le circuit par sa face avant. Le faisceau laser avait un spot d'un diamètre égal à 1 µm. La durée d'impulsion choisie pour ce test était de 50 ns. Afin de réaliser des cartographies de la cellule, le pas de déplacement de la table XY sur laquelle est fixé l'objectif du laser était réglé à 0,2 µm. La couleur rouge foncé a été utilisée pour représenter la localisation du spot laser lorsque la cellule a basculé de l'état "0" à l'état "1". La couleur bleu foncée pour représenter le basculement de l'état "1" à "0" pour une puissance laser égale à 0,3 W (voir ***Figure II. 82***). Les couleurs plus claires représentent l'extension des zones sensibles lorsque la puissance laser est passée à 0,42 W. A des puissances supérieures à 0,48 W la cellule SRAM était détruite. C'est la raison pour laquelle, les mesures n'ont pas était faites à des puissances supérieures.



○	Sensibilité à l'état "0" pour une puissance laser de 0,3 W
○	Sensibilité à l'état "1" pour une puissance laser de 0,3 W
●	Sensibilité à l'état "0" pour une puissance laser de 0,48 W
●	Sensibilité à l'état "1" pour une puissance laser de 0,48 W

Figure II. 82. Cartographie extraite de la mesure de la sensibilité de la cellule SRAM aux SEU aux puissances laser de 0,3 W et 0,48 W.

Il est possible de remarquer que la mesure a révélé seulement trois zones sensibles: les drains de *MN1*, *MN2/MN3* et *MP1*. Quatre zones étaient attendues en théorie, la zone sensible manquante est celle du drain de MP2.

II.5.2 Hypothèse de l'effet de masquage de zones sensibles.

La zone d'effet du laser s'étend au-delà du spot de diamètre de 1 µm (voir le profil gaussien du laser présenté au ***paragraphe II.1.1.1.2***). En outre, il recouvre simultanément plusieurs diffusions (voir la représentation du spot laser par rapport au layout de la cellule

SRAM présenté ***Figure II. 83***). En raison du profil d'intensité lumineuse de type gaussien du faisceau laser et de la réduction des nœuds technologiques des semi-conducteurs, il devient, en effet, de plus en plus difficile de n'illuminer qu'une seule jonction sans créer des effets photoélectriques sur les autres jonctions environnantes. En effet, d'après les mesures présentées au ***paragraphe II.1.1.1.2***, pour un objectif de 100 X (Ø 1 µm), 50 % du courant maximal est généré à environ 3 µm du centre de la zone sensible. La topologie de la cellule et l'emplacement du spot laser doivent donc être pris en compte, car plusieurs jonctions génèrent du photocourant en même temps.

Le layout de la cellule SRAM étudiée est présenté ***Figure II. 83***. Il est possible de remarquer que le drain commun des transistors *MN2* et *MN3* est proche du drain du transistor PMOS *MP2*. De plus la surface du drain *MN2/MN3* est d'environ 0,65 µm² alors que celle du drain de *MP2* est d'environ 0,28 µm².

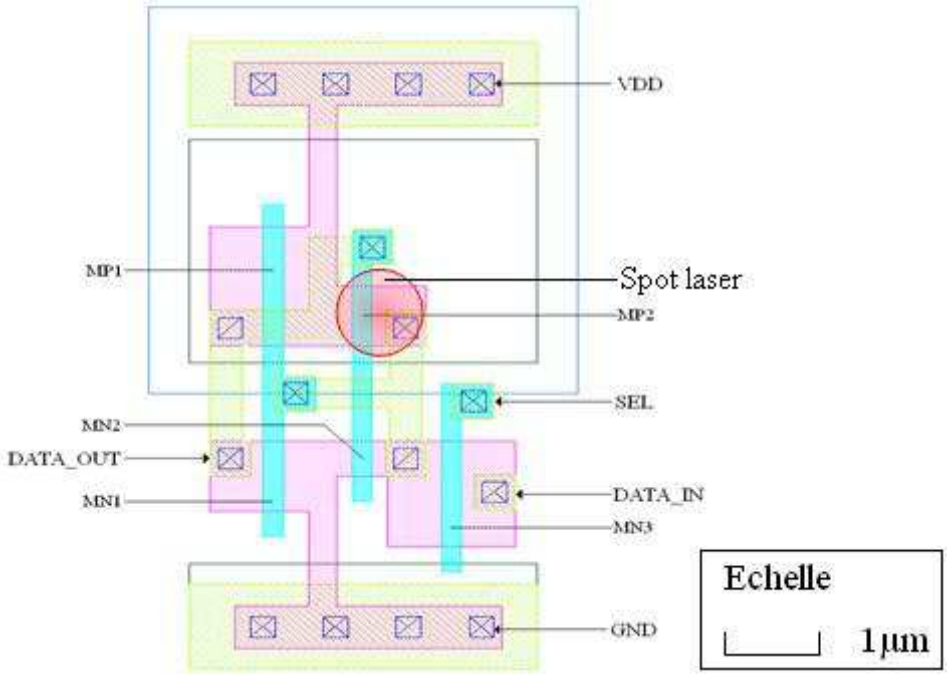


Figure II. 83. Layout de la cellule SRAM.

L'hypothèse que le layout a une influence sur l'effet de masquage de la zone sensible du drain du transistor PMOS *MP2* a été faite. La ***Figure II. 84*** illustre cette théorie d'effet de masquage dont l'origine est le photocourant généré par le drain partagé entre *MN2* et *MN3* (flèche bleue) qui contrebalance l'effet du photocourant induit par la jonction

drain/Nwell de *MP2* (flèche rouge barrée). Cet effet semblerait provenir du fait de la proximité entre les drains de *MP2* et *MN2/MN3*, ainsi que de leurs surfaces. En effet, la surface d'une jonction PN a une influence sur le photocourant généré. Plus la surface est importante et plus le photocourant généré sera également lui aussi important (voir ***Eq. II. 1.***).

Ainsi, en suivant les hypothèses selon lesquelles, le spot laser crée des photocourants simultanément sur plusieurs jonctions, il est possible de considérer qu'il n'y a qu'une zone sensible à l'état "1" qui est la jonction drain/Psubstrat de *MN1*. De plus, il n'y a pas d'effet similaire de masquage de zones sensibles à l'état "0", puisqu' aucun photocourant ne peut venir contrebalancer les photocourants générés par les drains de *MP1* et *MN2*.

En effet, si l'on considère uniquement le schéma électrique de la cellule, lorsque le photocourant généré par le drain du transistor *MP2* devient supérieure au courant de saturation du transistor *MN2* le nœud *Q* bascule de « 0 » à « 1 ». Alors que si l'on considère l'effet de proximité des zones sensibles, l'effet de masquage est présent. Dans ce cas de figure, le photocourant généré par le drain du transistor PMOS *MP2* reste inférieur à la somme du courant de saturation du transistor *MN2* et du photocourant généré par la jonction partagée des drains de *MN2/MN3*. Ainsi, le nœud *Q* reste à l'état logique « 0 ».

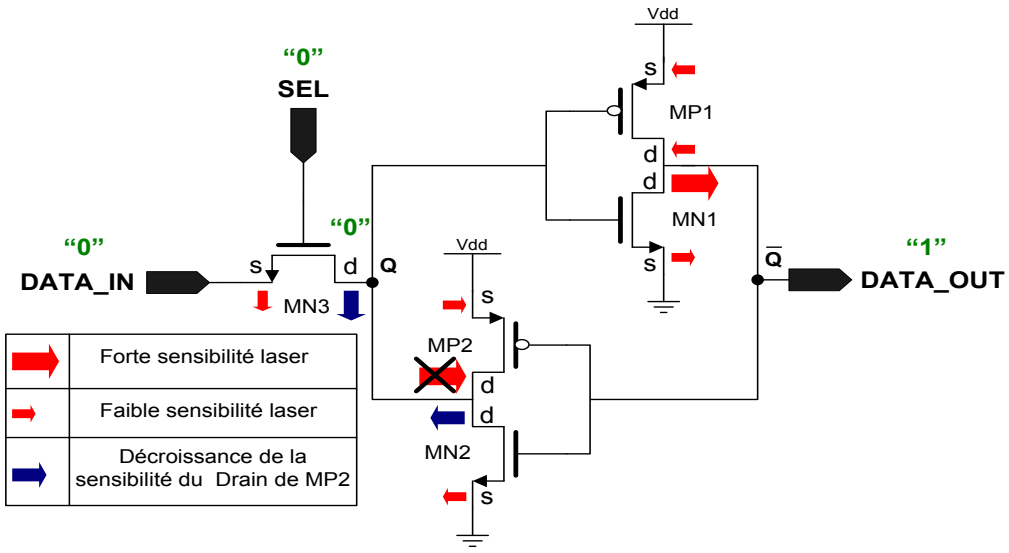


Figure II. 84. Illustration de l'effet de masquage à l'état "1".

Le paragraphe suivant permet de confirmer, grâce à la modélisation électrique, cet effet de topologie qui donne uniquement trois zones sensibles alors que quatre sont attendues en théorie.

II.5.3 Modèle électrique de la cellule SRAM sous SPL

Dans cette partie, un modèle électrique de la cellule SRAM sous Stimulation Photoélectrique Laser a été établi.

Le but de cette modélisation est de valider la méthodologie développée dans les parties précédentes, pour explorer par exemple certains résultats présentés en [Amu07, Amu07(b)] avec un temps de calcul extrêmement rapide (de l'ordre de la seconde). Ceci peut être une grande aide pour expliquer certains comportements électriques qui ont lieu lorsqu'une porte CMOS est exposée à une SPL impulsionnelle.

Pour chaque jonction PN de la cellule SRAM, un sous-circuit *Iph_Diode* contenant une source de courant contrôlée en tension (expliqué au ***paragraphe II.1***) modélisant son comportement sous SPL impulsionnel est ajouté à la netlist de simulation de la cellule SRAM (voir ***Figure II. 85***). La modélisation a été simplifiée à son maximum. En effet la modélisation faite des transistors NMOS et PMOS a été calibrée grâce aux mesures réalisées sur des transistors en technologie 90 nm alors que la cellule SRAM est en technologie 0,25 µm. C'est la raison pour laquelle les transistors bipolaires parasites présentés dans les modèles de MOS sous illumination laser n'ont pas été ajoutés dans cette simulation. Les résultats de simulation sont donc qualitatifs plutôt que quantitatifs. En outre la plupart des mesures faite pour calibrer les modèles de jonction PN sous illumination laser ont été réalisées sur des transistors ayant de grands dimensionels (surface de jonction de l'ordre de 6 µm²). Ainsi pour une étude qualitative plutôt que quantitative, l'utilisation de modèle de jonction PN sous illumination laser en technologie 90 nm sur une structure réalisée en technologie 0,25 µm n'a pas d'impact sur les résultats de la simulation.

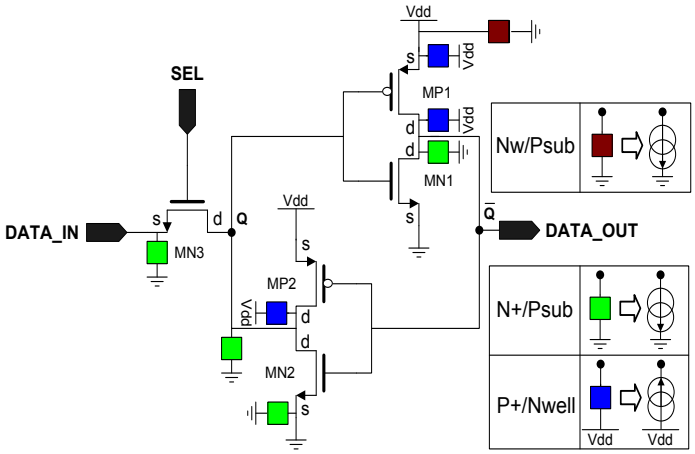


Figure II. 85. Modèle Electrique de la cellule SRAM sous PLS impulsionnelle.

Dans le layout de cette cellule SRAM, certaines jonctions sont partagées. C'est la raison pour laquelle, la cellule ne contient que huit sous-circuits *Iph_diode* puisque certaines jonctions PN sont communes (drains de *MN2/MN3*, sources de MP1/MP2 et sources de *MN1*/*MN2*). De plus un sous-circuit modélisant l'effet de la jonction Nwell/Psub est ajouté à la netlist. Le modèle basé sur les résultats de modélisation des ***paragraphes II.1.1*** et ***II.1.2*** permet de prendre en compte (entre autres) l'interaction entre la topologie de la cellule et le spot laser générant des photocourants sur plusieurs jonctions simultanément. Le pas du maillage nécessaire pour prendre en compte la topologie de la cellule a été fixé en simulation à 0,5 µm.

II.5.3.1 Cartographies électrique

Le résultat de la cartographie extrait du simulateur est présenté et comparé aux mesures.

Au départ, la puissance du laser est fixée à une faible valeur (0,2 W). Le simulateur ELDO (en langage SPICE) détermine l'état de la cellule SRAM. La couleur rouge foncé est utilisée pour représenter la localisation du faisceau laser lorsque l'état logique passe de "0" vers "1", et la couleur bleu foncé de "1" vers "0" (voir ***Figure II. 86***). Dans un second temps, la couleur claire représente l'extension des zones sensibles lorsque la puissance du laser est doublée (0,4 W). De plus, par simulation, la durée de l'impulsion laser était fixée à 50 ns avec une taille de spot de 1 µm. Il est également nécessaire d'ajouter que les

puissances utilisées pour la simulation n'ont pas de signification avec la réalité puisque les résultats sont qualitatifs plutôt que quantitatifs.

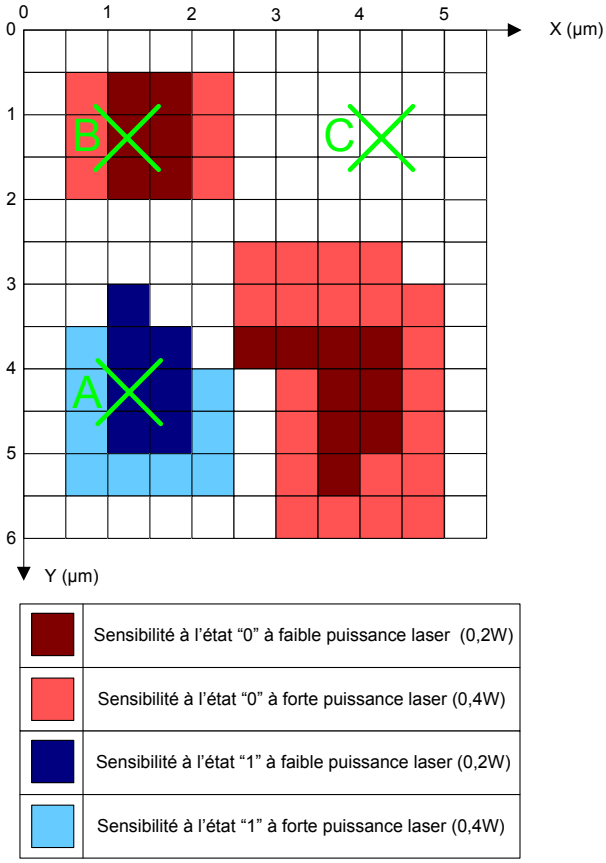


Figure II. 86. Cartographie de la sensibilité de la cellule SRAM aux SEU pour différentes puissances laser – Simulation électrique.

Toutefois, une très bonne corrélation qualitative est atteinte entre les cartographies extraites des mesures (voir ***Figure II. 82***) et celle issue des simulations électriques (***Figure II. 86***). En effet, il est possible de retrouver les zones sensibles notées lors des expériences d'injection réalisées sur l'équipement laser: les drains de *MN2* et *MP1* à l'état « 0 » et le drain de *MN1* à l'état « 1 ». En outre, les mesures réalisées afin de calibrer les sous-circuits *Iph_diode* utilisés pour modéliser la cellule SRAM sous illumination laser en face arrière l'ont été en technologie 90 nm. La cellule SRAM est, elle, réalisée en technologie 0,25 µm. Les mesures laser sur cette cellule ont été obtenues en illuminant la face avant de la cellule. Le fait qu'une bonne corrélation est obtenue entre les mesures et la simulation, prouve que les modèles peuvent être tout de même utilisés pour des portes logiques plus complexes.

II.5.3.2 Courants et tensions extraits de la simulation électrique

L'étude des courants photoélectriques et des tensions des nœuds mis en jeu dans l'effet de masquage permettent de confirmer et d'étudier plus précisément l'hypothèse présentée au paragraphe ***II.5.2***.

Pour cette étude, trois pointages du faisceau laser sont envisagés (points A, B, et C présentés sur la ***Figure II. 86***).

Dans le premier cas, le faisceau laser est centré par simulation sur le point A à l'état 1. Dans ces conditions, la modification de l'état de la cellule de "1" vers "0" est due à l'effet photoélectrique sur la jonction de drain du transistor NMOS *MN1* (IphDMN1). Le tir laser débute à t=150 ns. Avant le basculement de la cellule (pour un temps compris entre environ 150 ns et 170 ns sur la ***Figure II. 87***), il est possible d'observer une évolution progressive à la baisse du potentiel du nœud sensible $\overline{VQ}$ (c'est-à-dire *DATA_OUT*) jusqu'au seuil de basculement de la SRAM aux alentours de 0,6 V. Le photocourant au niveau du drain du transistor *MN1* (IphDMN1) est supérieur à la somme du photocourant généré par ailleurs au niveau du drain du transistor PMOS *MP1* (IphDMP1) et de son courant de saturation (IDSMP1). Ce dernier a un effet de compensation partiel vis-à-vis de IphDMN1. Ainsi, il est possible de noter qu'après le basculement (pour un temps supérieur à 170 ns), le photocourant du drain du transistor NMOS *MN1* est réduit puisque la différence de potentiel aux bornes de cette jonction drain/Nwell passe de 1,2 V à 0 V. Le courant IDSMP1 cesse après le basculement, car le transistor MP1 passe d'un état passant à un état bloqué. Les courants et tensions en fonction du temps extraits du simulateur au point A sont présentés ***Figure II. 87***.

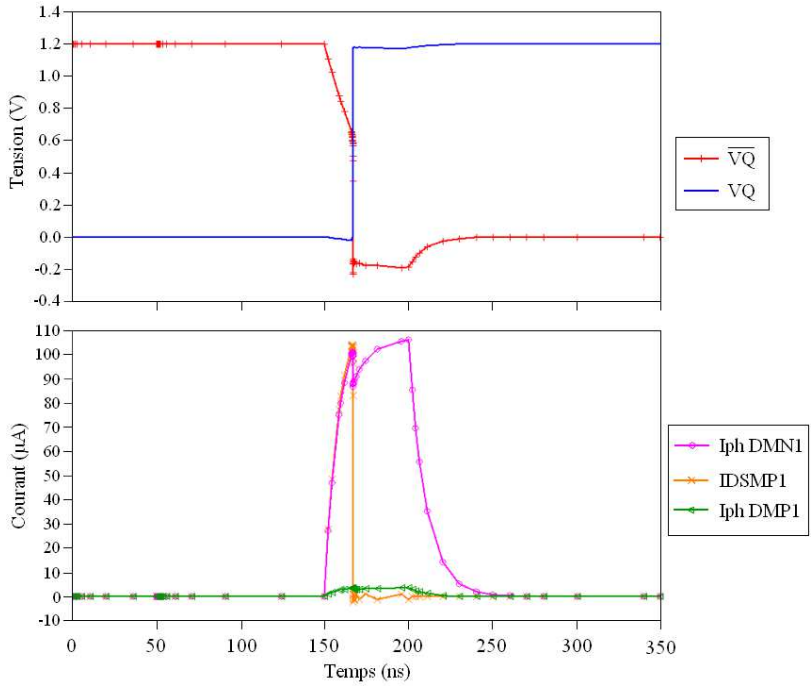


Figure II. 87. Courants et tensions en fonction du temps, extraits de la simulation électrique au point A.

La seconde localisation (point B à l'état initial 0 - drain du transistor bloqué PMOS *MP1*) se trouve sur une zone où il est possible de modifier l'état de la cellule de "0" à "1" grâce à l'effet photoélectrique de la jonction de drain du transistor PMOS *MP1* (IphDPN1). Le tir laser débute à t=150 ns. Avant le basculement de la cellule (pour un temps compris entre environ 150 ns et 170 ns sur la ***Figure II. 88***), il est possible d'observer une évolution progressive à la hausse du potentiel du nœud sensible jusqu'au seuil de basculement de la SRAM aux alentours de 0,6 V. Le photocourant au niveau du drain du transistor *MP1* (IphDMP1), environ égal à 105 µA, est supérieur à la somme du photocourant généré par ailleurs au niveau du drain du transistor NMOS *MN1* (IphDMN1) et de son courant de saturation (IDSMN1). Ce dernier a un effet de compensation partiel vis-à-vis de IphDPN1. Ainsi, il est possible de noter qu'après le basculement (pour un temps supérieur à 170 ns), le photocourant du drain du transistor PMOS *MP1* est réduit puisque la différence de potentiel aux bornes de cette jonction drain/Nwell passe de 1,2 V à 0 V. Le courant IDSMN1 cesse après le basculement, car le transistor MN1 passe d'un état passant à un état bloqué. Les courants et tensions en fonction du temps extraits du simulateur au point B sont présentés ***Figure II. 88***.

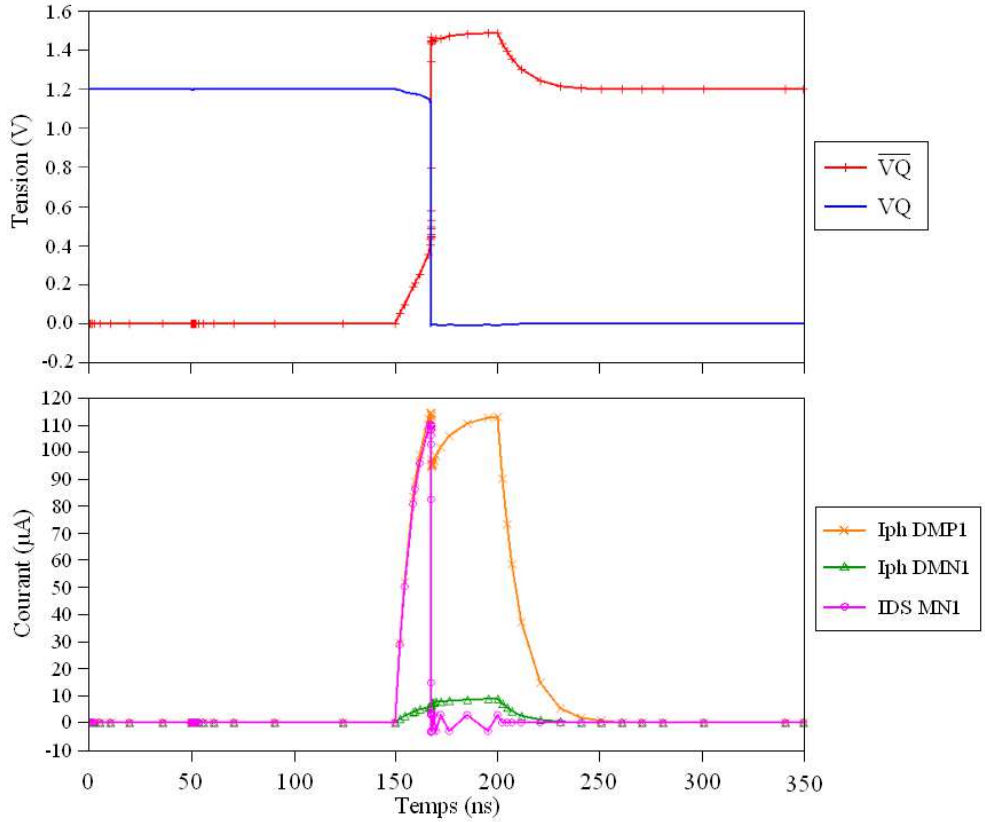


Figure II. 88. Courants et tensions en fonction du temps, extraits de la simulation électrique au point B.

Dans le dernier cas (point C à l'état 1), le photocourant généré par le drain des transistors PMOS *MP2 (Iph DMP2 ≈ 33 µA)* est inférieur à la somme du photocourant du drain partagé entre les transistors NMOS *MN2/MN3 (Iph MN2_MN3 ≈ 7 µA)* et le courant de saturation du transistor NMOS *MN1 (IDS MN1)*. Cet effet est dû à la faible surface de la jonction de drain du transistor *MP2* en comparaison avec celle plus importante du drain partagé entre les transistors *MN2* et *MN3* qui est localisé proche de lui (voir ***Figure II. 83***). Dans ces conditions, la cellule ne bascule pas. Les courants et tensions en fonction du temps extraits de la simulation électrique au point C qui illustrent ce phénomène sont présentés ***Figure II. 89***.

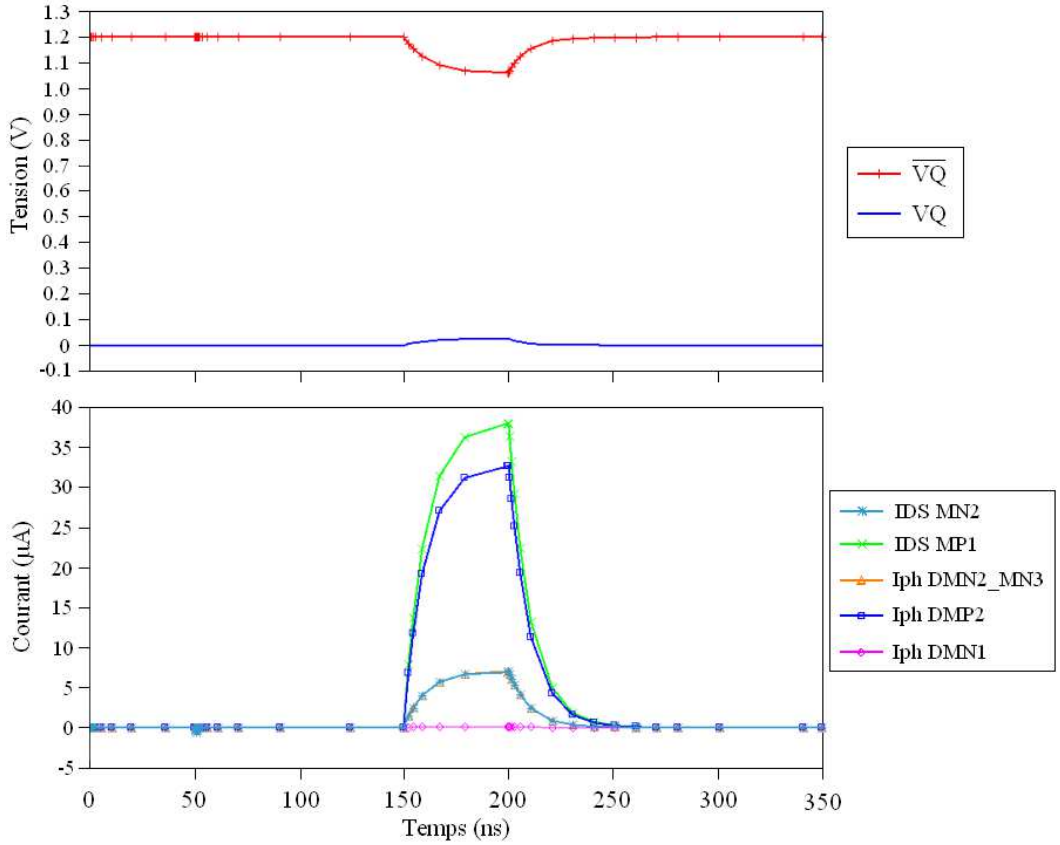


Figure II. 89. Courants et tensions en fonction du temps, extraits de la simulation électrique au point C.

Dans ce cas de figure, l'état de la SRAM n'a pas été modifié par le tir laser.

Donc, l'étude des courants et tensions de simulation mis en jeu lors de l'illumination laser de la cellule SRAM a permis de valider l'hypothèse de masquage d'une des zones sensibles à l'état 1 (drain du transistor PMOS *MP2*). En effet, il a été vu en simulation, que le masquage de cette zone sensible est créé par la proximité de la jonction de drain partagée entre les transistors NMOS *MN*2 et *MN3* avec celle du drain sensible *MP2*. Il en résulte une compensation du courant photoélectrique induit au niveau du drain de *MP2* par le courant photoélectrique généré au niveau du drain commun de *MN2/MN3* à l'origine du masquage de sensibilité (absence de basculement de la cellule SRAM).

Conclusion

Ce chapitre a présenté une modélisation électrique de l'injection de fautes par laser sur des porte CMOS. Les modèles résultants sont capables de simuler aussi bien des effets laser de faible puissance continu, que des effets pulsés de plus forte puissance. Les modèles peuvent être utilisés pour tracer par simulation des cartographies électriques permettant de révéler les zones sensibles des portes CMOS. De plus, l'utilisateur est susceptible de faire varier plusieurs paramètres, comme l'épaisseur de silicium, la focalisation du faisceau, la taille de spot, la puissance laser, etc. Les modèles développés tiennent compte de la topologie de la cellule. En effet, les distances entre le spot laser et les différentes zones sensibles sont prises en compte. En outre, à chaque développement d'une nouvelle technologie, les étapes de calibration du modèle sur des jonctions PN et des transistors sont à refaire.

Un tel modèle peut permettre aux concepteurs de circuit d'analyser les faiblesses de leurs portes CMOS dès la phase de conception. En termes de sécurité, ce modèle électrique peut également servir pour comprendre les effets de l'injection de fautes.

En termes de perspectives, la modélisation électrique présentée dans ce chapitre, a été faite pour des durées d'illumination allant de 50 ns à plusieurs secondes (laser continu). Il est possible de modéliser les effets du laser à des durées d'impulsion inférieures à 50 ns descendant jusqu'à la picoseconde. Pour cela, il sera nécessaire de reprendre toute la méthodologie présentée dans ce chapitre en mesurant tout d'abord des jonctions PN puis en complexifiant progressivement l'étude. En outre un travail d'optimisation des simulations reste encore à faire pour pouvoir extraire plus rapidement des simulations de cartographie laser.

Chapitre III. CONTRE-MESURES AUX INJECTIONS DE FAUTES PAR IMPULSION LASER DANS LES CIRCUITS SÉCURISÉS

Introduction

Les deux chapitres précédents ont permis d'avancer dans la compréhension des phénomènes physiques mis en jeu lors de l'interaction d'un faisceau laser sur le matériau physico-chimique qu'est le silicium. De cette meilleure compréhension, des modèles électriques de transistors et de portes CMOS sous illumination laser ont pu être établis. Dans ce troisième et dernier chapitre, différentes techniques de contre-mesures aux attaques laser sont présentées. La plupart des techniques suivantes ont fait l'objet d'un dépôt de brevet. Pour des raisons de confidentialité, seules les techniques dont le brevet est à l'heure actuelle dans le domaine public sont présentées dans ce manuscrit.

L'une des approches possibles dans le domaine de la contre-mesure aux injections de fautes par impulsion laser est de rendre plus robustes les circuits, de telle sorte que toute attaque conduise à augmenter la puissance du laser pour créer des fautes exploitables. Dès l'instant où il est demandé à ce laser une puissance plus grande, la probabilité croît pour que le tir soit plus facilement détecté par un éventuel capteur embarqué sur la puce.

Ainsi ce chapitre se subdivise en deux grandes parties distinctes. La première s'intéresse à l'augmentation de la robustesse des portes CMOS aux attaques laser. Les modélisations électriques présentées au chapitre précédent ont permis de valider certaines de ces contre-mesures. Et la seconde est consacrée aux différents détecteurs laser qui peuvent être embarqués dans un microcontrôleur sécurisé.

III.1 Robustesse des portes CMOS aux attaques laser

Dans cette partie, une amélioration de la robustesse de portes CMOS aux attaques laser est présentée au travers de l'exemple d'une cellule SRAM. L'étude a été faite par simulation électrique grâce aux modèles de MOS sous SPL développés dans le précédent chapitre.

III.1.1 Description de la cellule SRAM étudiée

La cellule CSRAM (Configuration SRAM), étudiée dans un premiers temps, est la même que celle présentée au chapitre ***II.5.1.1***. La cellule est constituée de cinq transistors MOS (cf. ***Figure III. 1***).

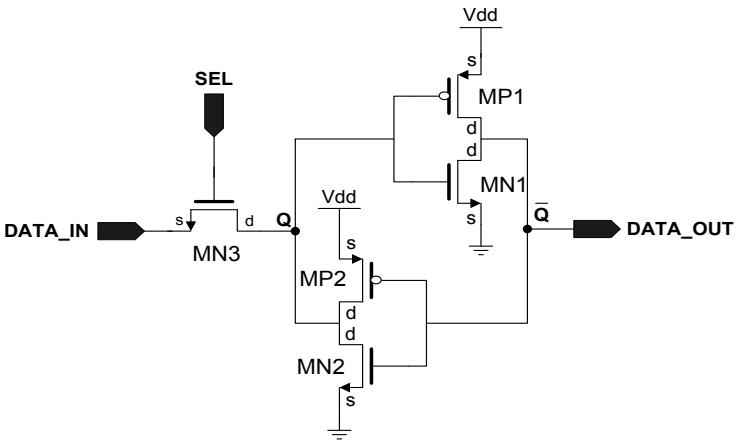


Figure III. 1. Schéma électrique de la cellule SRAM.

L'étude des nœuds sensibles de la cellule a été présentée au chapitre précédent (***paragraphe II.5.1***).

La ***Figure III. 2*** présente, comme vu au le chapitre II, la modélisation électrique utilisée pour simuler l'effet laser impulsionnel forte puissance avec une taille de spot de 1 µm sur une cellule SRAM.

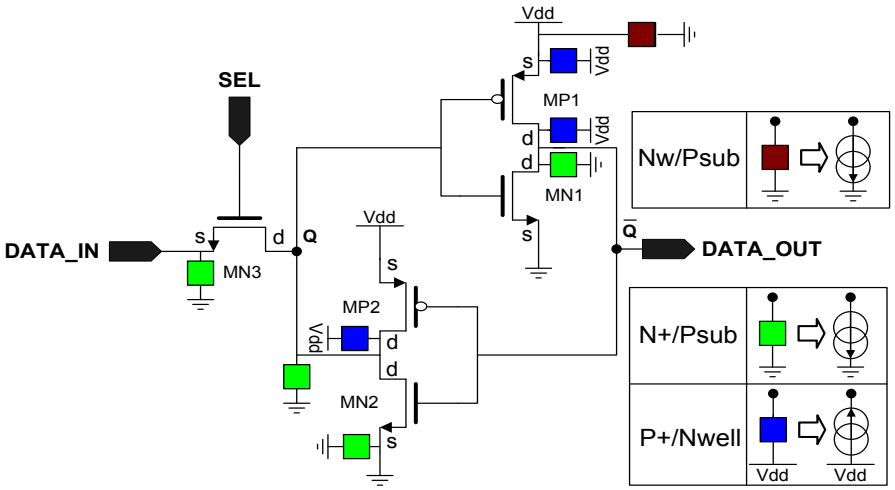


Figure III. 2. Modélisation électrique de la cellule SRAM sous SPL.

Le tableau ci-dessous reprend les équations mathématiques utilisées pour cette modélisation électrique présentée dans le chapitre précédent.

$I_{ph} = (a \times V + b) \times S \times \alpha_{gauss} \times V_{laser\_trig}$ ***Eq. III. 1***			
$a = p \times P_{laser}^{\ 2} + q \times P_{laser} + r$ ***Eq. III. 2***		$b = s \times P_{laser}$ ***Eq. III. 3***	
Coefficient	**N+/Psub**	**P+/Nwell**	**Nwell/Psub**
p	$4E^{-9}$	$9E^{-5}$	$6E^{-11}$
q	$-5E^{-7}$	$2E^{-4}$	$9E^{-9}$
r	$9E^{-6}$	$-5E^{-6}$	$1E^{-7}$
s	$4E^{-6}$	$1.2E^{-3}$	$6E^{-8}$
$\alpha_{gauss}(d) = \left[\beta \times \exp\left(-\frac{d^2}{c_1} \right) + \gamma \times \exp\left(-\frac{d^2}{c_2} \right) \right] \times w$ ***Eq. III. 4***			

Tableau III. 1. Equations mathématiques définissant la valeur des sources de courant contrôlée en tension.

III.1.2 Corrélation entre simulations électriques et mesures

Dans cette partie, la comparaison entre les cartographies extraites du simulateur développé dans cette thèse et celles basées sur des mesures (comme vu dans le chapitre précédent) est rappelée. De plus l'étude sur la cellule SRAM est faite sur une technologie CMOS 90 nm, tout comme pour la modélisation.

Le simulateur ELDO (langage SPICE), cartographie le niveau logique de sortie de la SRAM *(DATA_OUT)*. La couleur rouge sur le graphique ***Figure III. 3*** représente la localisation du spot laser lorsque la sortie bascule de la valeur logique "0" à la valeur "1", ainsi que la couleur bleue lorsqu'elle bascule de "1" à "0". Le nombre de zones sensibles se retrouvent en simulation, validant ainsi l'outil développé.

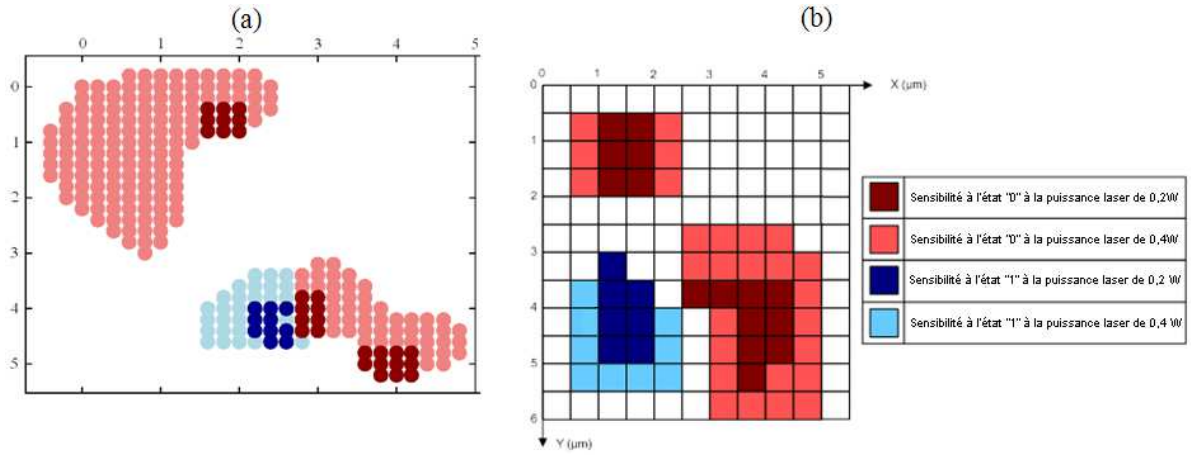


Figure III. 3. Cartographie de la sortie de la SRAM (*DATA_OUT*) pour différentes puissances laser. (a) Mesures (b) Simulations.

III.1.3 Amélioration de la robustesse de la cellule SRAM

Dans cette partie, le but est de diminuer le nombre de zones sensibles aux attaques laser pour une puissance donnée. Ceci permet aux concepteurs de circuit de concevoir un layout de manière astucieuse afin de diminuer ces zones sensibles, en prenant en compte l'effet de masquage vu au chapitre précédent. C'est cette méthodologie qui a été appliquée sur une cellule SRAM 6T classique.

III.1.3.1 Diminution du nombre de zones sensibles

La cellule SRAM, ici étudiée, est une cellule SRAM classique à 6 transistors (voir ***Figure III. 4***). Elle est constituée d'un couple d'inverseurs rebouclés pour mémoriser les informations (transistor *MP1*, *MN1*, *MP2* et *MN2*), et de deux transistors NMOS d'accès

(transistors *MN3* et *MN4*). La suite de l'étude a été réalisée en statique, c'est-à-dire que les transistors NMOS d'accès sont bloqués (OFF). L'idée de base afin de diminuer le nombre des zones sensibles de la cellule SRAM 6T est de s'inspirer du masquage d'une des jonctions de drain de la cellule CSRAM par le biais d'une des jonctions du transistor d'accès afin de réussir à masquer les deux zones sensibles qui sont les deux drains des transistors PMOS de la cellule SRAM 6T (voir ***paragraphe II.5.2***). Ceci se fait par l'intermédiaire des deux transistors d'accès (*MN3* et *MN4* sur la ***Figure III. 4***).

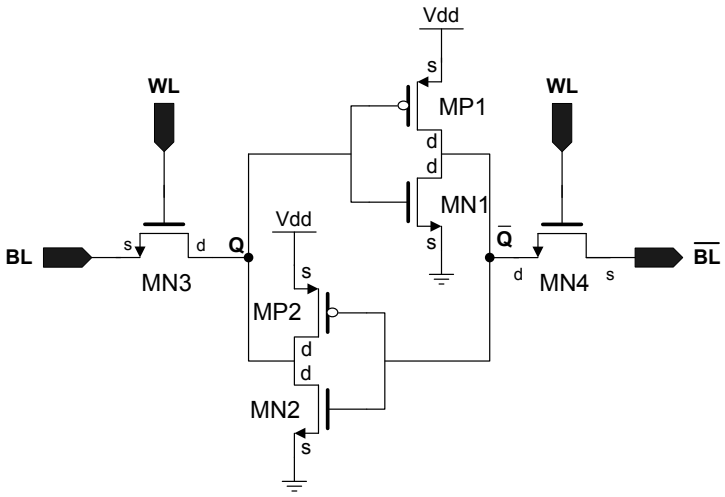


Figure III. 4. Schéma électrique de la cellule SRAM 6 transistors.

Les flèches rouges présentes sur les ***Figure III. 5*** et ***Figure III. 6*** donnent les directions des photocourants induits entre le drain ou la source et le substrat des différents transistors. Les flèches les plus larges représentent de forts photocourants et les plus fines des photocourants plus faibles.

Lorsque la cellule est à l'état "0" (défini lorsque le nœud Q est à un état logique bas), un effet de masquage de la zone sensible du drain du transistor PMOS *MP2* est ainsi possible (voir ***Figure III. 5***). Ceci peut être obtenu en plaçant les drains partagés des transistors NMOS *MN2* et *MN3* le plus près possible du drain du transistor PMOS *MP2*.

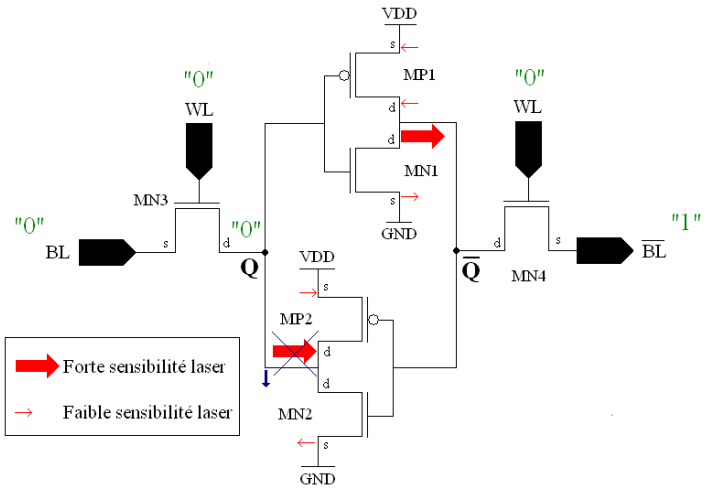


Figure III. 5. Schéma électrique de la sensibilité de la SRAM 6T soumise à une SPL à l'état "0".

De même, à l'état "1" (défini pour *Q* à l'état haut), la sensibilité du drain du transistor *MP1* peut être masquée pour une puissance donnée en plaçant les drains communs des transistors *MN1* et *MN4* proches de celui-ci (voir figure ci-dessous).

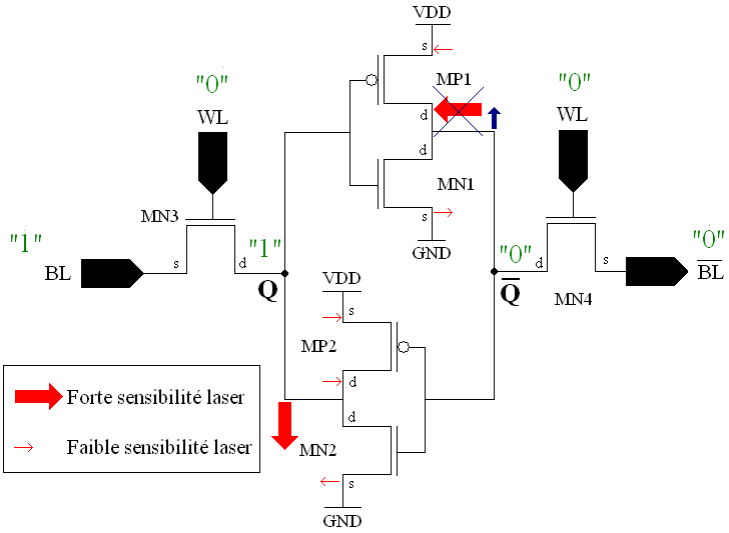


Figure III. 6. Schéma électrique de la sensibilité de la SRAM 6T soumise à une SPL à l'état "1".

Le layout de la cellule SRAM 6T est présenté ***Figure III. 7***. Les recommandations de dessin données par le document présenté en [Ish98] pour le layout de la cellule ont été suivies. De plus, il a été vu précédemment que le photocourant généré par les drains

partagés *MN2/MN3* peut annuler la zone sensible du drain de *MP2 (*d'une surface ≈ 0,19 µm²) (voir ***Figure III. 5***). En effet, lorsque le faisceau laser est centré sur le drain du transistor PMOS *MP2*, il génère également un photocourant sur la jonction de drain partagée de *MN2* et *MN3* annulant le photocourant du drain du transistor PMOS *MP2*, et faisant ainsi disparaître sa zone sensible. C'est la raison pour laquelle la surface des drains communs de *MN2/MN3* est maximisée. Elle a une surface approximée à 0,32 µm², positionnée très proche du drain de *MP2*. De la même manière le photocourant généré par le drain commun de *MN1/MN4* a la possibilité de masquer la zone sensible située sur le drain de *MP1*. La jonction des drains partagés *MN1/MN4* qui a la même surface que la jonction *MN2/MN*3 est placée le plus proche possible du drain de *MP1* (voir ***Figure III. 7***).

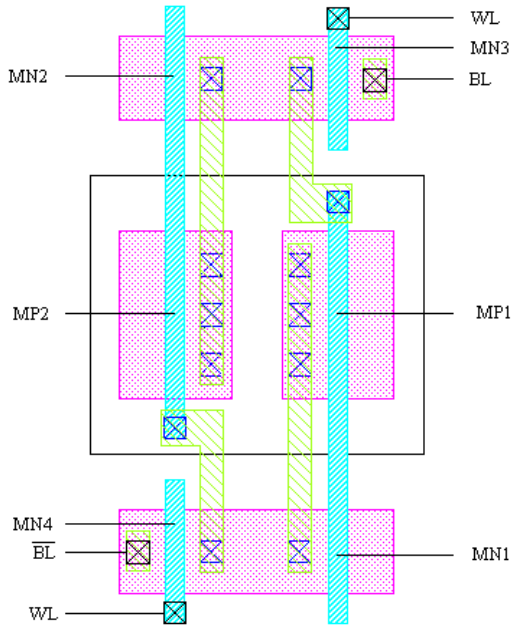


Figure III. 7. Layout de la cellule SRAM 6T respectant les considérations topologiques afin de masquer des zones sensibles à une SPL.

Les résultats de simulation de cartographie électrique aux sensibilités dues à une SPL pour une puissance de 0,2 W sont présentés ***Figure III. 8***. De plus, la puissance a été augmentée en simulation jusqu'à 1 W et a permis de vérifier que les zones sensibles des drains des transistors NMOS *MN1* et *MN2* n'apparaissent pas sur la cartographie.

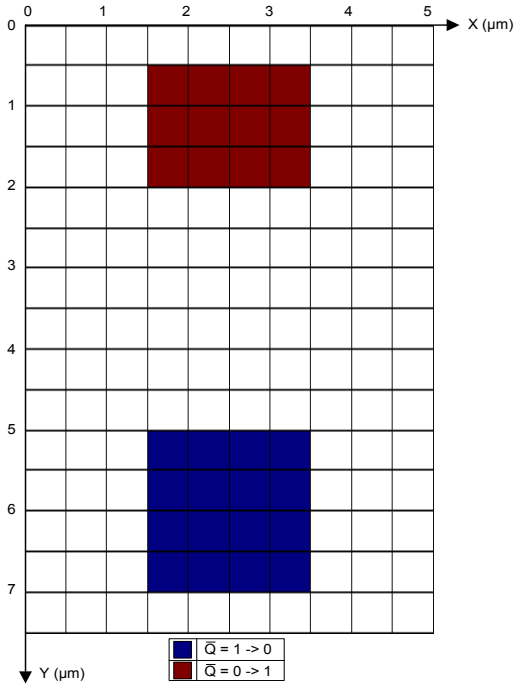


Figure III. 8. Cartographie de la sensibilité de la cellule SRAM 6T à une SPL.

Ce layout de la SRAM 6T présenté ***Figure III. 7*** a permis de masquer les deux zones sensibles des drains des transistors PMOS *MP1* et *MP2*. Ce qui permet d'avoir une zone sensible de moins que sur la cellule de la SRAM 5T, grâce au transistor d'accès additionnel *MN4*. Quoi qu'il en soit, il reste toujours deux zones sensibles qui sont les drains communs des transistors NMOS *MN1*/*MN4* et *MN2*/*MN3*. Dans la suite, il est proposé de diminuer le seuil de sensibilité de ces zones sensibles.

III.1.3.2 SRAM avec implant deep Nwell

III.1.3.2.1 Effet de cet implant sur un transistor NMOS

Une autre approche pour augmenter la robustesse de la cellule SRAM aux injections laser est de placer les transistors NMOS dans des caissons de type P (Pwell) isolés du substrat P par un implant de type N (communément appelé Deep Nwell en anglais). L'effet de cet implant sur un transistor NMOS, est principalement visible sur la réduction du photocourant généré par les jonctions N+/Pwell d'un facteur environ égal à 25 pour une puissance laser de 1,25 W et une durée d'impulsion de 20 µs (voir ***paragraphe II.1.4***). Le

détail de ces mesures confirmées par des simulations TCAD a été présenté au chapitre précédent (***paragraphe II.3.1***).

III.1.3.2.2 Nouvelle proposition de Layout de cellule SRAM 6T utilisant un implant deep Nwell

Un implant deep Nwell a été ajouté au layout de la cellule SRAM 6T présenté ***Figure III. 7*** afin de donner un nouveau layout (cf. ***Figure III. 9***). Ce design de la cellule SRAM, non optimal, n'a pas été étudié sous tous ces aspects (stabilité, rendement, etc.), mais a été conçu afin de mettre en évidence les phénomènes physiques mis en jeu pour augmenter sa robustesse.

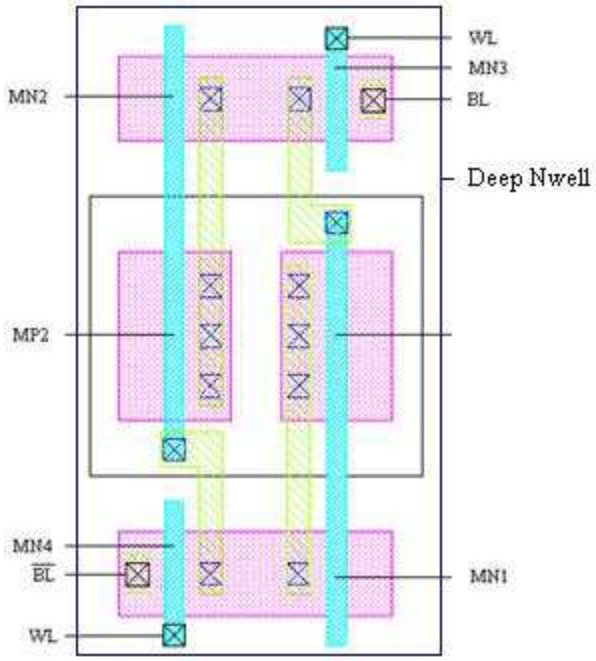


Figure III. 9. Layout de la cellule SRAM 6T avec implant deep Nwell.

Le même type de simulation électrique a été fait. Le modèle utilisé tient compte de l'effet du triple well sur la SPL (le modèle a été calibré grâce aux mesures faites sur un transistor NMOS avec deep Nwell) avec la même puissance laser (0,2 W) que celle qui a permis de dessiner la cartographie électrique présentée ***Figure III. 8***. Toutes les zones sensibles de la cellule ont ainsi disparu. Il a été nécessaire de multiplier la puissance du laser par un facteur 4 (0,8 W) pour voir réapparaître les zones sensibles sur une même surface.

Ainsi, la nouvelle solution rendant la SRAM plus robuste a nécessité de passer d'une puissance de 0,2 W à 0,8 W pour créer les mêmes fautes laser. Cette augmentation de la puissance est nécessaire pour fauter de nouveau la cellule SRAM. Cette contrainte permet d'accroître l'efficacité de détecteurs embarqués sur des circuits sécurisée (voir ***paragraphe III.2***).

Ceci semblerait confirmer que le simulateur puisse donner des indications aux concepteurs de circuit afin de les guider pour une conception plus sécurisée, et créer de nouvelles portes CMOS plus robustes aux attaques laser.

III.2 Détecteurs laser

Une simple augmentation de la robustesse de portes CMOS n'a de sens que si des détecteurs laser sont embarqués sur un microcontrôleur sécurisé. Si des portes plus robustes sont implémentées sur la puce, l'attaquant devra disposer d'une puissance laser beaucoup plus importante pour générer des fautes exploitables. Cette augmentation de puissance laser rend plus facile la détection du tir par des détecteurs embarqués sur la puce. C'est dans cet état d'esprit que des détecteurs laser ont été développés. La partie qui suit présente certaines solutions concernant les détecteurs laser embarqués sur les microcontrôleurs sécurisés.

III.2.1 Détecteur laser à base d'une jonction N+/Psubstrat fortement polarisée en inverse

Le chapitre précédent a mis en évidence le fait que le photocourant généré par une jonction PN augmente quasi-linéairement avec l'amplitude de la polarisation inverse qui lui est appliquée (voir ***Figure III. 10***). La mesure a été réalisée sur une technologie 90 nm, avec une taille de spot de 5 µm centrée en plein milieu d'une jonction N+/Psubstrat.

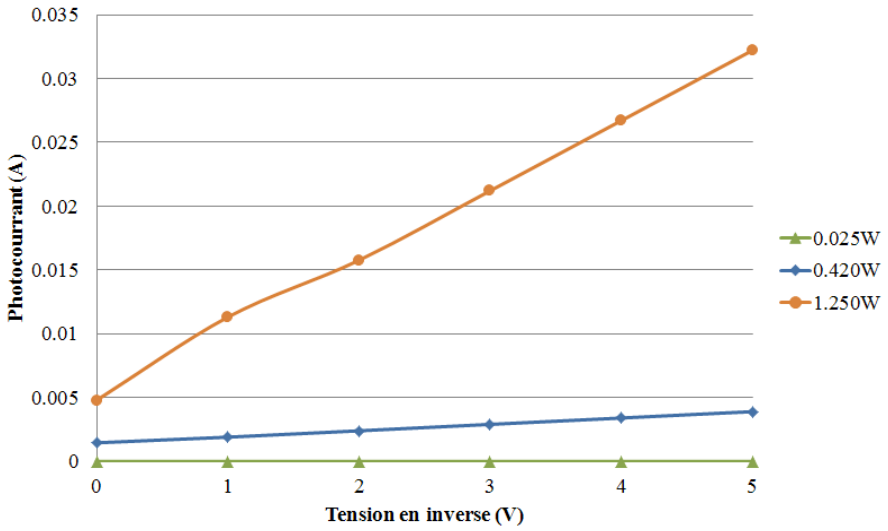


Figure III. 10. Caratéristique courant-tension d'une jonction PN, N+/Psubstrat, de dimension 10x0,6 µm pour différentes puissances laser.

Ainsi, en polarisant la jonction à une tension en inverse de 5 V, elle génére lorsque la puissance du laser est de 1,25 W, un photocourant de 32 mA. En comparaison, la puissance nécessaire pour créer des fautes est de l'ordre de quelques centaines de mW.

Dans ce cas de figure, l'intérêt est de mettre en œuvre un détecteur laser basé sur une jonction PN de type N+/Psubstrat et de la polariser en inverse à 5 V pour augmenter son efficacité. Une tension d'environ 5 V pour un détecteur embarqué dans un microcontroleur sécurisé peut être fournie par exemple grâce à la tension de lecture d'une mémoire de type FLASH.

De plus, l'effet du laser sur le silicium montre que pour générer un même photocourant, il faut écarter le spot laser plus loin du centre de la jonction dans le cas où la diode est polarisée en inverse à 5 V plutôt qu'à 1,2 V (voir ***Figure III. 11***). Afin de réaliser ces mesures, les conditions expérimentales suivantes ont été établies: le spot laser était de 5 µm, la puissance du laser de 1,25 W et la durée d'impulsion de 20 µs. Par exemple, dans le cas d'une polarisation en inverse de 1,2 V, pour générer un photocourant supérieur à 1 mA, il faut être à une distance inférieure à environ 40 µm. Alors que si la jonction est polarisée en inverse à 5 V, le spot laser doit être positionné à une distance inférieure à 200 µm du centre de la jonction PN.

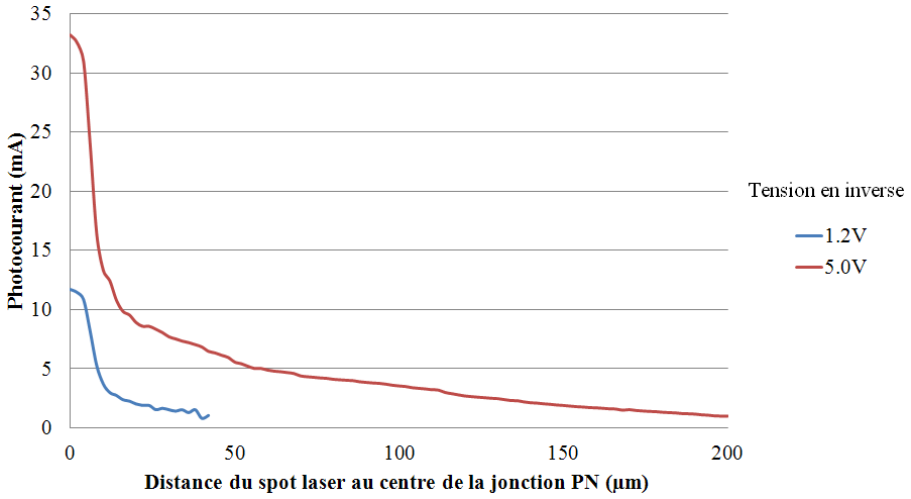


Figure III. 11. Comparaison du photocourant mesuré versus la distance entre le spot laser et le centre de la jonction entre une diode polarisée en inverse à 1,2 V et à 5 V, pour un spot laser de 5 µm, une durée d'impulsion de 20 µs et une puissance laser de 1,25 W.

Ces mesures permettent de concevoir un détecteur laser basé sur une jonction PN polarisé en inverse à 5 V, afin d'avoir un rayon de détection plus important qu'à 1,2 V.

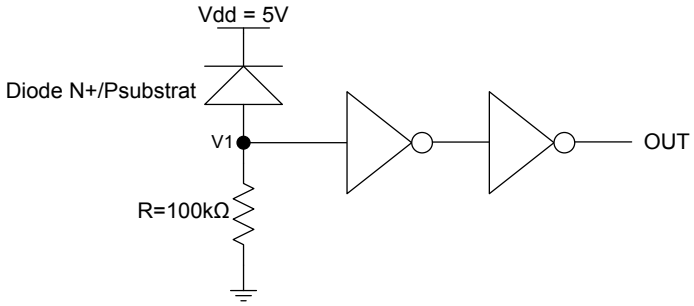


Figure III. 12. Schéma électrique du détecteur laser utilisant une jonction N+/Psubstrat polarisée en inverse à 5 V.

La ***Figure III. 12*** donne le schéma de principe du circuit électrique du détecteur. Il comprend la diode sensible à la génération du photocourant créé par le laser avec une résistance en série et deux inverseurs chaînés.

En l'absence de tir laser, le courant passant dans la diode n'est autre que son courant en inverse (de l'ordre du nA). Le potentiel V_1 (***Figure III. 12***) est alors à 0 V, ce qui implique que la tension de sortie du circuit V_{OUT} est aussi à 0 V.

Le fait d'avoir un tir laser à proximité du détecteur engendre un photocourant dans la jonction N+/Psubstrat qui fait augmenter le potentiel V_1. Dans ce cas, le seuil en courant nécessaire pour qu'il y ait une détection d'un tir laser est fixée à 25 µA. Si le photocourant est supérieur à cette valeur, le potentiel de V_1 passe à une tension supérieure à 2,5 V. La sortie *OUT* bascule alors de « 0 » à « 1 », signalant ainsi la présence d'une attaque laser sur la puce.

La ***Figure III. 13*** explicite le principe du détecteur laser basé sur une jonction N+/Psubstrat fortement polarisée en inverse. Le détecteur délimite, à l'endroit où il est implanté sur le silicium, un disque de détection. Le but est d'implémenter un détecteur occupant une surface minimale sur le silicium tout en générant ainsi un disque de détection maximal.

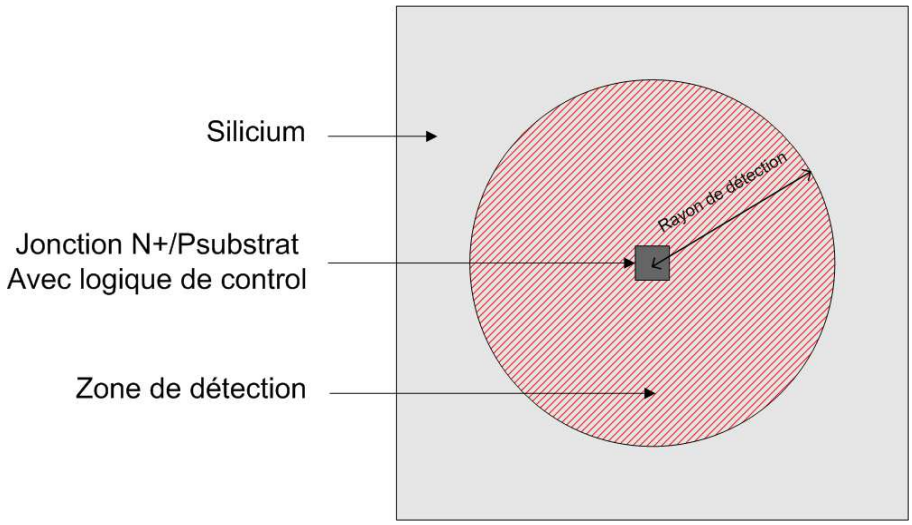


Figure III. 13. Schéma de principe du détecteur laser à base de jonction N+/Psubstrat polarisé en inverse à 5 V.

Grâce au simulateur mis en place et présenté au chapitre II, la zone de détection peut être simulée, en fonction des paramètres laser suivant: durée d'impulsion, puissance, taille de spot (voir ***Figure III. 14***).

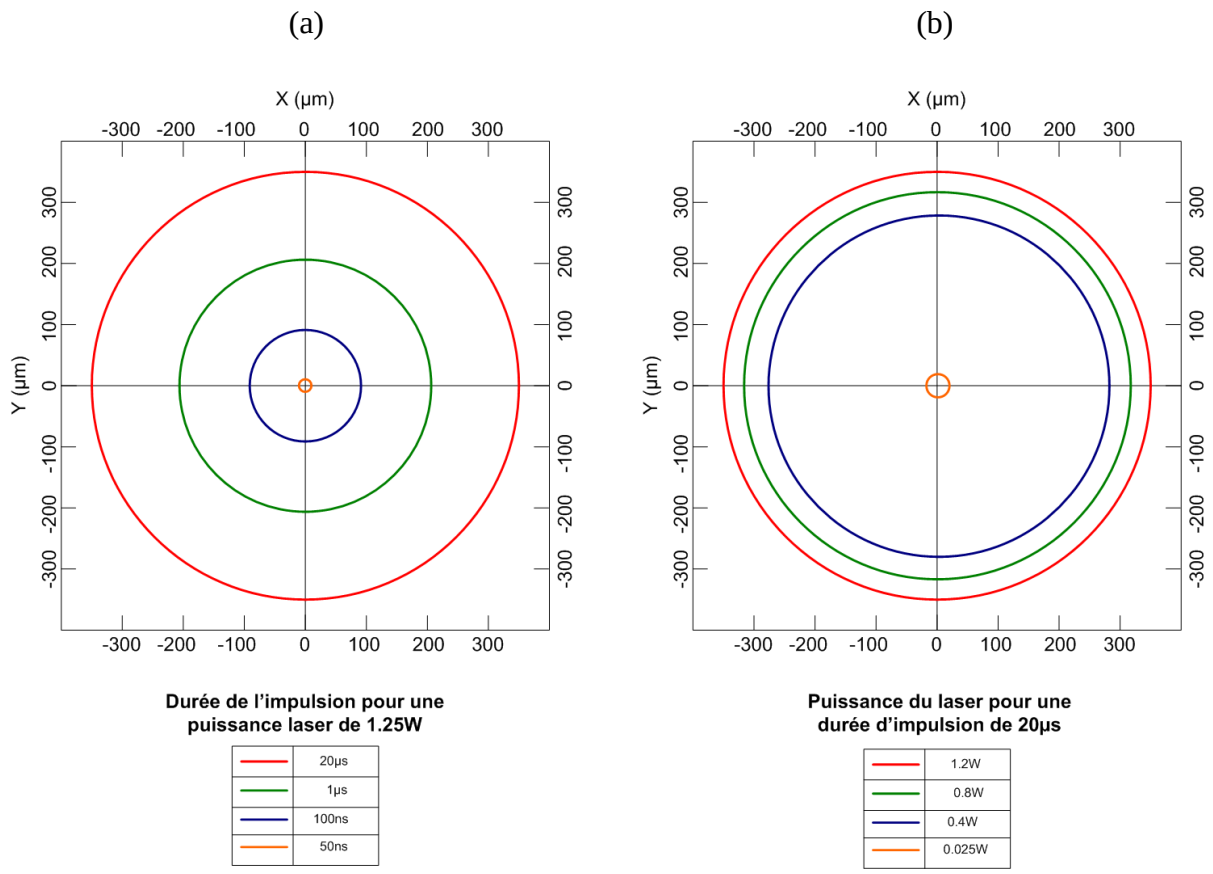


Figure III. 14. Diagrammes de la limite de détection du détecteur laser en fonction de: (a) la durée d'impulsion pour une puissance de 1,25 W et une taille de spot de 5 µm (b) la puissance du laser pour une durée d'impulsion de 20 µs et un spot de 5 µm.

Les résultats obtenus ***Figure III. 14*** montrent que la durée d'impulsion du laser à une forte influence sur le diamètre du disque de détection. En outre, une puissance laser évoluant de 0,4 W à 1,2 W n'a qu'une influence minime sur la détection du tir laser. De plus, le seuil pour faire des fautes est approximativement de quelques centaines de mW.

La solution qui consiste à mettre en œuvre un détecteur laser basé sur une jonction PN polarisé en inverse à 5 V a le mérite d'avoir une bonne couverture de protection par rapport à une moindre complexité de mise en œuvre et du peu de surface nécessaire à son implémentation sur un microcontrôleur sécurisé.

III.2.2 Détecteur laser à base de tranchée verticale de polysilicium (brevet d'invention [Lis11(a)], [Lis11(b)])

Le principe de fonctionnement de cet autre détecteur laser est basé sur le Deep Trench Isolation (DTI). Le deep trench isolation est une tranchée servant à isoler des transistors MOS les uns des autres. Elle est constituée de polysilicium conducteur en son centre et entourée d'oxyde isolant. La ***Figure III. 15*** présente une coupe extraite d'une simulation TCAD mettant en évidence le DTI (en violet).

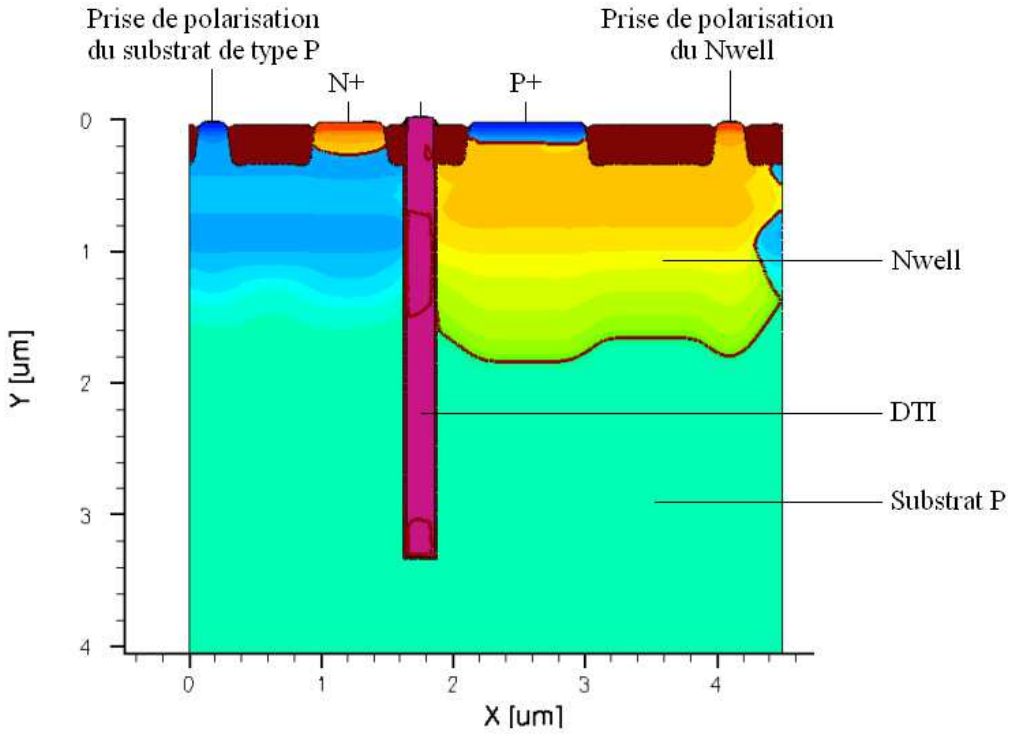


Figure III. 15. Coupe TCAD mettant en évidence le Deep Trench.

L'intérêt d'utiliser le Deep trench est multiple. Tout d'abord il n'augmente pas la surface globale de la puce, car il peut s'insérer entre les zones des transistors NMOS et celles des transistors PMOS, puisqu'il est implanté au milieu du STI (Swallow Trench Isolation) séparant ces deux zones. De plus, la capacité due à l'oxyde formé autour du DTI est « gratuite » en termes de surface puisque le DTI s'étire d'une manière orthogonale à la surface de la puce. Il est donc possible de prévoir un système de détection connecté au DTI dont le schéma de principe est donné ***Figure III. 16***.

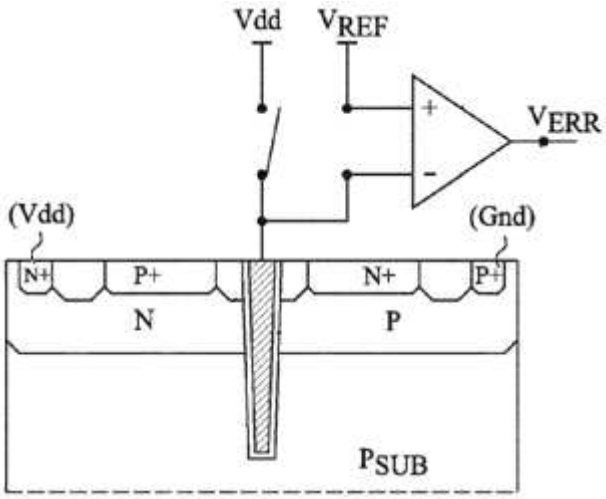


Figure III. 16. Présentation du principe du détecteur laser basé sur le DTI (extrait de [Lis11(b)]).

Pour détecter qu'une attaque est en cours, il suffit de constater des variations anormales du potentiel V_{TR} du DTI constitué de polysilicium.

La région conductrice du polysilicium du DTI constitue une électrode aux multiples capacités parasites, notamment entre le DTI et les caissons de type N, de type P, et du substrat.

L'illumination de la puce par un faisceau laser entraîne une modification rapide des potentiels de polarisation du substrat, et des caissons Pwell et Nwell. Les variations des potentiels de polarisation sont transmises par le réseau de capacités parasites mentionnées auparavant, se traduisant par une variation du potentiel du DTI.

Il est proposé ici de détecter, à l'aide du circuit présenté ***Figure III. 16***, les variations du potentiel du DTI, susceptibles d'être enregistrées lors d'une attaque frauduleuse. Une fois l'attaque détectée, diverses mesures de protections, ou de destructions des données confidentielles peuvent être mises en œuvre.

Dans cet exemple, le circuit comprend un comparateur comportant deux bornes d'entrée et une borne de sortie. La borne d'entrée est reliée électriquement au polysilicium du DTI. En fonctionnement, un potentiel de référence V_{REF} est appliqué sur l'autre borne

d'entrée et la borne de sortie fournit un signal V_{ERR} susceptible de commuter entre une valeur haute et une valeur basse selon que le potentiel V_{TR} du matériau conducteur est supérieur ou inférieur au potentiel V_{REF}. Le matériau conducteur remplissant la tranchée du DTI est en outre relié à une borne de potentiel haut (V_{DD}) par l'intermédiaire d'un interrupteur commandable. En fonctionnement, l'interrupteur, normalement ouvert, est fermé de façon périodique, par exemple à chaque front montant ou descendant d'un signal d'horloge de la puce, de façon à maintenir le DTI à un potentiel flottant sensiblement constant. En variante, un potentiel de polarisation peut être appliqué en permanence au matériau conducteur (polarisation non flottante).

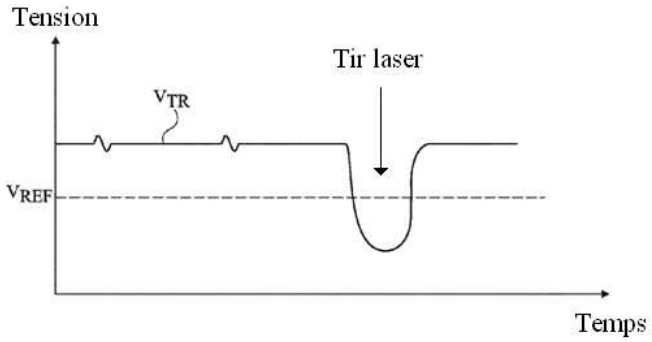


Figure III. 17. Chronogramme illustrant l'évolution du potentiel V_{TR} du DTI.

La figure ci-dessus est un chronogramme illustrant l'évolution du potentiel V_{TR} du DTI lors du fonctionnement de la puce. En fonctionnement normal, le potentiel V_{TR} est maintenu à un potentiel supérieur au potentiel V_{REF} appliqué sur la borne d'entrée du comparateur. A titre d'exemple, le potentiel V_{REF} est approximativement de 0,5 V, et le potentiel V_{TR} est maintenu à une valeur sensiblement constante de l'ordre de 0,7 V.

On observe des petits pics sur le signal V_{TR}, correspondant à des variations rapides et de faible amplitude du potentiel V_{TR}. Ces pics sont la conséquence de phénomènes transitoires normaux se produisant lors du fonctionnement de la puce. A titre d'exemple, l'amplitude de ces pics est inférieure à 0,1 V.

Sur le chronogramme de la ***Figure III. 17***, il est possible d'observer en outre un creux plus important que les petits pics présentés précédemment, correspondant à une chute brutale et de forte amplitude du potentiel V_{TR}. Une telle chute de potentiel se produit

typiquement en présence d'une attaque frauduleuse, par exemple lors d'une intrusion par faisceau laser. Plus généralement, lors d'une attaque frauduleuse, une variation rapide du potentiel V_{TR} se produit dans les régions du DTI de la zone attaquée. A titre d'exemple, des variations d'amplitude supérieure à 0,3 V sont typiquement observées en cas d'attaque laser sur des puces alimentées à 1,2 V. Le potentiel V_{TR} chute alors à une valeur inférieure au potentiel V_{REF}, conduisant à une détection de l'attaque comme présenté ***Figure III. 16***. En effet dans ces conditions-là, le potentiel V_{ERR} passe de 0 V à 1,2 V.

Bien évidemment, en pratique, plusieurs circuits de détection peuvent être prévus sur la même puce. Il est par exemple possible d'associer plusieurs circuits de détection à positionnés à différents endroits de la puce. Alternativement, il est également possible de prévoir des circuits de détection que dans les zones les plus sensibles de la puce. Il est également possible en outre de prévoir, sur une même puce, des circuits d'alerte présentant des seuils de détections distincts, par exemple en appliquant des potentiels de référence V_{REF} distincts sur les bornes d'entrées des différents comparateurs. Ce système de réglage de la sensibilité peut permettre d'augmenter le seuil de déclenchement des détecteurs, dans certaines zones sensibles aux bruits de substrat, pour éviter les risques de déclenchements intempestifs.

Conclusion

Dans ce dernier chapitre, différentes contre-mesures aux attaques laser concernant les circuits sécurisés ont été abordées. Deux approches intimement liées ont été développées. La première contre-mesure consiste à améliorer la robustesse des circuits, ou parties de circuits comme des portes CMOS, à toutes les intrusions laser. La technique utilisée, pour augmenter la robustesse de ces portes, est illustrée par le biais d'une étude sur une cellule SRAM, basée sur des simulations électriques réalisées grâce au modèle présenté au chapitre II. Ce simulateur électrique procure de bonnes orientations lors de la conception des circuits afin de les rendre plus robustes aux injections de fautes. Il peut se révéler extrêmement intéressant d'un point de vue sécuritaire, de prendre en compte très en amont tous les retours d'expériences pour accroitre leurs robustesses.

La seconde approche, vue précédemment au ***paragraphe III.1***, porte sur un travail conceptuel couplé à des détecteurs de tirs lasers embarqués sur des microcontrôleurs sécurisés, pour rendre le circuit plus sûr. Il est entendu que l'augmentation de robustesse d'un circuit, se traduit, pour tout attaquant, par la nécessité de mettre en œuvre des lasers de plus en plus puissants pour générer des fautes exploitables. De ce fait, si au sein de la puce des détecteurs lasers sont implémentés, la probabilité pour qu'ils détectent une attaque laser (générant une faute exploitable) croît correlativement en proportion. Dans cette optique, deux détecteurs lasers différents ont été présentés. Le premier est basé sur un organe de détection constitué simplement d'une jonction PN polarisée fortement en inverse pour accroître sa surface de détection. Le second porte sur l'ajout, entre les transistors de type N et ceux de type P, d'un DTI connecté à un système de détection d'une attaque.

Bien d'autres types de contre-mesures aux injections de fautes par impulsions laser peuvent être imaginés. Certaines solutions, développées et mises en œuvre lors de cette thèse, ont fait l'objet de dépôt de brevet en tant que co-auteur, mais n'ont malheureusement pas pu être présentées dans ce manuscrit, pour des raisons de confidentialité, notamment du fait que les solutions qui y sont développées ne sont pas encore dans le domaine public.

Conclusion générale

L'injection de fautes dans les circuits sécurisés par impulsion laser est, de nos jours, une réelle menace pour les fabricants de microcontrôleurs. Dans le cadre de ce travail, après une étude de l'état de l'art développé au cours du chapitre I, des mesures sur silicium ont été réalisées afin de mieux caractériser les effets induits par le laser. Issus de toutes ces études, des modèles électriques ont pu être réalisés, en les complexifiant graduellement (chapitre II), afin de simuler en un temps très court la réponse de portes CMOS soumises à des illuminations lasers. Des simulations TCAD peuvent donner des informations plus complètes sur les mécanismes physiques mis en jeu lors de l'illumination de ses portes. Le problème de simulation est plus complexe lorsqu'il est nécessaire de simuler des portes contenant plusieurs transistors. En effet, dans ce cas de figure, le temps de calcul devient très rapidement problématique. Aussi, la bonne corrélation obtenue entre mesures pratiques et simulations électriques sur une cellule SRAM, permettent de penser que le modèle développé dans le cadre de cette thèse pourra être appliqué assez facilement à d'autres portes CMOS plus complexes ou à des parties plus importantes de circuits sécurisés. Pour ce faire, il sera nécessaire de développer des outils d'extraction de données géométriques du layout, sachant que la topologie des cellules à une forte influence sur leurs réponses à la Stimulation Photoélectrique Laser.

D'ores et déjà, le modèle développé permet de tester des solutions de conception sur des portes contenant peu de transistors.

De plus l'une des solutions qui paraît être la plus pertinente pour éviter les fautes exploitables créées lors de ces intrusions et d'utiliser des détecteurs de lumière intégrés dans la puce.

Dans le futur, le développement de différentes solutions seront envisagées et testées par des simulateurs toujours plus sophistiqués.

La course initiée depuis longtemps, entre attaques et contre-mesures est une compétition perpétuelle. Ainsi, les attaquants de circuits poussent les concepteurs à élaborer continuellement des parades pour rendre leurs contre-mesures difficilement contournables. Néanmoins, la solution « *miracle* » créant des microcontrôleurs sécurisés totalement inviolables semble être une utopie. Les concepteurs de tels circuits doivent donc s'efforcer de conjuguer software et hardware pour répondre aux conditions de protections maximales. Toutefois, cette complexité a des répercussions à différents niveaux. Ce qui a pour corollaire l'augmentation des coûts financiers, et l'accroissement des temps de développement des produits pour le fabriquant.

L'avènement du numérique s'étendant de plus en plus dans nos sociétés modernes, la sécurisation de l'information restera l'un des défis majeurs du XXI^{ème} siècle. De nos jours, les circuits sécurisés renferment de nombreuses informations, mais également des secrets stratégiques qui circulent en permanence sur le net, (sont concernés l'internet mais aussi l'intranet). De nos jours, toutes les activités humaines sont impactées. Le piratage de circuits sécurisés est devenu une arme à part entière. Les Etats eux-mêmes doivent prendre des mesures draconiennes de protection. Récemment, la NSA (l'agence de sécurité américaine spécialisée dans l'écoute et le traitement des télécommunications), se serait introduite dans les programmes de gestion des centrifugeuses en enrichissement de l'uranium pour déstabiliser le processus iranien de fabrication de l'arme atomique. Cette intrusion aurait été le fait d'un simple virus nommé Stuxnet.

Cet exemple montre que la maîtrise du numérique devient une arme à part entière rejoignant en cela les prémisses des travaux d'Allan Turing et des « bombes » de Bletchley Park.

Table des acronymes

Acronyme	Description
AES	Advanced Encryption Standard
BBICS	Bulk Build In Current Sensor
BC	Bande de conduction
BI	Bande interdite
BV	Bande de valence
DES	Data Encryption Standard
DIL	Dual In Line
DPA	Differential Power Analysis
DTI	Deep Trench Isolation
ECC	Elliptic Curve Cryptosystem
EEPROM	Electrical Erasable Read Only Memory
LASER	Light Amplified by Stimulated Emission of Radiation
LIVA	Light Induced Voltage Alteration
MOS	Métal-Oxyde-Semiconducteur
NFC	Near Field Communication
NMOS	Transistor MOS de type N
NSA	National Security Agency
OBIC	Optical Beam Induced Current
OBIRCH	Optical Beam Induced Resistance Change
PMOS	Transistor MOS de type P
RAM	Read Only Memory
RF	Radiofréquence
RFID	Radio Frequency Identification
ROM	Random Access Memory
RSA	Algorithme pour la cryptographie à clef publique
SPA	Single Power Analysis
SIM	Subscriber Identity Module
SEM	Scanning Electron Microscopy
SPL	Stimulation Photoélectrique Laser
SRAM	Static Random Access Memory
TCAD	Technology CAD
TIVA	Thermally Induced Voltage Alteration
PIN	Personal Identification Number
ZCE	Zone de Charge d’Espace

Tables des symboles

Paramètre	**Unité**	**Description**
C_{OX}	$F.m^{-2}$	Capacité d'oxyde
D_{IT}	$eV^{-1}m^{-2}$	Densité moyenne des états d'interface
E	J	Energie
E	$Kg.m.A^{-1}.s^{-3}$	Champ électrique
E_C	J	Energie du niveau le plus bas de la bande de conduction
E_F	J	Energie du niveau de Fermi
E_{GAP}	J	Largeur de la bande interdite du semiconducteur
E_I	J	Niveau intrinsèque (loin de l'interface)
E_{PH}	J	Energie du photon
E_V	J	Energie du niveau le plus haut de la bande de valence
G	$cm^{-3}.s^{-1}$	Taux de génération de pair électrons-trous
H	eV.s	Constante de Planck : $h=6.626.10^{-34}$ J.s ou $4.14.10^{-15}$ eV.s
I	cd	Intensité lumineuse
I_{PH}	A	Photocourant
J	$A.m^{-2}$	Densité électrique
K	m^{-1}	Vecteur d'onde
K	$J.K^{-1}$	Constante de Boltzmann ($k=1.38.10^{23}$ $J.K^{-1}$)
L	m	Longueur de grille des transistors
N	cm^{-3}	Densité d'électrons
P	cm^{-3}	Densité de trous
P_{OPT}	δ	Puissance optique
Q_{IT}	$C.m^{-2}$	Charge due aux états d'interface
Q_{SC}	$C.m^{-2}$	Charge dans le semiconducteur
Q	?	Rayon de courbure du front d'onde
T	K	Température
T_{OX}	m	Epaisseur d'oxyde
V_{TH}	V	Tension de seuil d'une diode
W	m	Largeur de la grille d'un transistor MOS
w_0	m	« Col » d'un faisceau laser gaussien
Z_R	m	Longueur de Rayleigh
Z_{SC}	m	Distance confocal
A	m^{-1}	Coefficient d'absorption de l'onde lumineuse dans le silicium
Λ	m	Longueur d'onde
Z	rad	Déphasage de Gouy

Bibliographie

[Arc03] D. Agrawal, B. Archambeault, S. Chari, J. R. Rao and P. Rohatgi, Advances in Side-Channel Cryptanalysis". RSA Laboratories Cryptobytes, Vol. 6, No. 1, pp. 20-32, 2003.

[Ald03] J. Alda, Laser and Gaussian Beam Propagation and Transformation, Encyclopedia of Optical Engineering, 2003.

[Amu06] O. A. Amusan, A. F. Witulski, L. W. Massengill, B. L. Bhuva, P. R. Fleming, M. L. Alles, A. L. Stenberg, J. D. Black, D. R. Schrimpf, Charge collection and Charge sharing in a 130nm CMOS technology, IEEE Transactions on nuclear science, vol. 53, No. 6. Dec 2006.

[Amu07(b)] O. A. Amusan, L. W. Lloyd, M. P. Baze, B. L. Bhuva, A. F. Witulski, S. DasGupta, A. L. Stenberg, P. R. Fleming, C. C. Heath, M. L. Alles, Directional sensitivity of the Single Event Upsets in 90nm CMOS due to charge sharing, IEEE, transaction of Nuclear Science, vol. 54. No. 6, Dec 2007.

[Amu07] O. A. Amusan, A. L. Stenberg, A. F. Witulski, B. L. Bhurva, J. D. Black, M. P. Baze, and L. W. Massengill, Single event upsets in a 130 nm hardened latch design due to charge sharing, IRPS 2007.

[Amu08] O. A. Amusan, L. W. Lloyd, M. P. Baze, A. L. Stenberg, A. F. Witulski, B. L. Bhuva, J. D. Black, Single Event Upsets in deep-submicrometer technologies due to charge sharing, IEEE Transaction device and materials reliability, vol. 8, No. 3, Sept 2008.

[And01] R. Anderson, "Security engineering: a guide to building dependable distributed systems", Ed. Wiley, 2001.

[Bar07] M.A. Bajura et al, "Models and algorithmic limits for an ECC-based approach to hardening sub-100-nm SRAMs", IEEE Trans. Nucl. Sci., vol. 54, no. 4, pp. 935, Aug. 2007.

[Bec98] F. Beck : "Integrated Circuit Failure Analysis : A guide to preparation techniques", JohnWiley & Sons, 1998.

[Bie00] I. Biehl, B. Meyer and V. Müller. "Differential fault attacks on elliptic curve cryptosystems". In M. Bellare, editor, Advances in cryptology : Proceedings of CRYPTO'00, number 1880 of LNCS, pp. 131-146, Springer-Verlag.

[Bih97] E. Biham and A. Shamir, “Differential fault analysis of secret key cryptosystems”, presented at 17th annual International Cryptology Conference on Advances in Cryptology CRYPTO’97, vol. 1294, pp. 513-525, California, USA, 1997.

[Bih99] E. Biham and A. Shamir, “Power analysis of the key scheduling of the AES candidates”, presented at second AES Candidate Conference (AES2), Rome, Italy, March 22-23, 1999.

[Boc09] A. Bocquillon, Thèse de doctorat, Evaluation de la sensbilité des FPGA SRAM-based face aux erreurs induites par les radiations naturelles, Institut Polytechnique de Grenoble, pp.26.

[Boc09(b)] A. Bocquillon, Thèse de doctorat, Evaluation de la sensbilité des FPGA SRAM-based face aux erreurs induites par les radiations naturelles, Institut Polytechnique de Grenoble, pp.72.

[Bon97] D. Boneh, R. A. DeMillo, and R. J. Lipton, “On the importance of cheking cryptographic protocols for faults”, presented at EUROCRYPT’97, vol. 1233, pp. 37-51, Berlin, 1997.

[Bua07] Latchup effect in CMOS IC: a solution for crypto-processors protection against fault injection attacks ?, N. Buard, F. Miller, C. Ruby, R. Gaillard, IOLTS 2007.

[Cal96] T. Calin, M. Nicolaidis, R. Velazco, « Upset Hardened Memory Design for Submicron CMOS Technology », IEEE Trans. Nucl. Sci., 43, p. 2874, 1996.

[Cas02] K. Castellani-Coulié, « Recherche des paramètres déterminants pour la prévision des aléas logiques induits par les protons et les neutrons sur les technologies CMOS avancées. », Université Montpellier II, thèse soutenue en Décembre 2002.

[DebB12] A. Dehbaoui, J.M. Dutertre, et al., “Electromagnetic Transient Faults Injection on a hardware and a software implementations of AES,” Fault Diagnosis and Tolerance in Cryptography 2012, Leuven, Belgium.

[Det97] C. Detcheverry, C Dachs, E. Lorfèvre, C. Sudre, G. Bruguier, J.M. Palau, J. Gasiot, R. Ecoffet, “SEU Critical Charge and Sensitive Area in a Submicron CMOS Technology”, IEEE Trans. Nucl. Sci., vol. 44, no. 6, pp. 2266-2273, 1997.

[Dhe98] J. F. Dhem, F. Koeune, P. A. Leroux, P. Mestre, J. J. Quisquater, and J. L. Willems, “A pratical implementation of the timing attack”, presented at the

third International conference on smart card research and applications (CARDIS).

[Dod05] P. E. Dodd, Physics-Based Simulation of Single-Event Effects, , IEEE, Transactions on device and materials reliability, vol. 5, No. 3, Sept 2005.

[Dod95] P. E. Dodd, F. W. Sexton, “Critical Charge Concepts for CMOS SRAMs”, IEEE Trans. Nucl. Sci., vol. 42, no. 6, pp. 1764-1771, 1995.

[Dod96(b)] P.E. Dodd, F. W. Sexton, G. L. Hash, M. R. Shaneyfelt, B. L. Draper, A. J. Farino, R. S. Flores, “Impact of Technology Trends on SEU in CMOS SRAMs”, IEEE Trans. Nucl. Sci., vol. 43, no. 6, pp. 2797-2804, 1996.

[Dod96] P. E. Dodd, “Device Simulation of Charge Collection and Single-Event Upset”, IEEE Trans. Nucl. Sci., vol. 43, no. 2, pp. 561-575, 1996.

[Dou05] A. Douin, V. Pouget, F. Daracq, D. Lewis, P. Fouillat, P. Perdu, Influence of Laser Pulse Duration in Single Event Upset Testing

[Dou08] A. Douin, ph. D Thesis, Université Bordeaux I, 2008, Contribution à la modélisation et au développement de techniques de test et d’analyse dynamique de circuits intégrés par faisceau laser pulsé.

[Dut02] J.-M. Dutertre, « Circuits reconfigurables robustes », These de doctorat, Université de Montpellier II, pp. 25-26, 2002.

[Fip186] NIST, “Digital signature standard (DSS), “ National Institut of Standard and Technology FIPS PUB 186-2, Jan. 2000.

[Fou90] P. Fouillat, « Contribution à l’étude de l’interaction entre un faisceau laser et un milieu semiconducteur. Applications à l’étude du latchup et à l’analyse d’états logiques dans les circuits intégrés en technologie CMOS », Thèse de Doctorat de l’Université Bordeaux 1, N° 410, 1990.

[Gan01] K. Gandolfi et Al. “The Electromagnetic Analysis: concrete results”, CHES 2001, LNCS 2162, (2001) pp. 251-261.

[Ger93] J. Gervais, « Mesure du coefficient d’absorption optique dans le silicium multicristallin de type P pour photopiles solaires », Journal de Physique III, 3, p. 1489, 1993.

[Glo10(a)] A. Glowacki, Ph.D Thesis, “Expanding the scope of laser stimulation techniques for functional analysis and reliability of semiconductor devices by in-depth investigation of the optical interaction with the devices”, Berlin

University of Technology, 2010.

[Glo10(b)] A. Glowacki, S. K. Brahama, H. Suzuki, C. Boit. ―Systematic characterization of integrated circuit standard components as stimulated by scanning laser beam, ISTFA 2010.

[Hab65] D.H. Habbing, "The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits", IEEE Transactions on Nuclear Science, 1965.

[Ham11] Inverted Emission Microscope iPHEMOS Series Hamamatsu, « commercial brochure », 2011.

[Ish98] M .Ishida et al., "A novel 6T-SRAM cell technology designed with rectangular patterns scalable 183eyond 0.18µm generation and desirable for ultra high speed operation," Int Electron Device Meeting Tech. Digitest, 1998, pp.201-204.

[Jac75] J.D. Jackson, « Classical Electrodynamics », 2nd edition, J. Wiley & Sons, New York, 1975.

[Joh93] A.H. Johnston, « Charge Generation and Collection in p-n Junctions Excited with Pulsed Infrared Lasers », IEEE Trans. Nucl. Sci., 40, p. 1694, 1993.

[Koc96] P. Kocher, "Timing attacks on implementation of diffie-Hellman, RSA, DSS, and others systems", presented at 16th International cryptology conference on advances in cryptology (CRYPTO'96), vol. 1109, pp.104-113, Santa-Barbara, Calif.

[Koc99] P. C. Kocher, J. Jaffe, and B. Jun. 1999. Differential Power Analysis. In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '99), M. J. Wiener (Ed.) Springer-Verlag, London, UK, 388.397.

[Kog66] H. Kogelnik and T. Li, "Laser Beam resonators", Applied Optics, vol 5, no 10, pp 1550-1567, 1966.

[Kos88] G.N. Koskowich, R.B. Darling, M. Soma, « Effect of first-order phonon-assisted scattering on near-infrared free-carrier optical absorption in silicon », Phys. Rev. B, 38, p. 1281, 1988.

[Lal94] J. R. Lalanne, A. Ducasse, S. Kielich, « Interaction LASER molécule, physique du LASER et optique non linéaire moléculaire », Ed. Polytechnica, 1994.

[Lee93] T. W. Lee, S.V. Pabbisetty (eds.) : “Microelectronics Failure Analysis”, Desk Reference. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X.

[Lis12(a)] M. Lisart, A. Sarafianos, Device for detecting an attack in an integrated circuit chip, N° de publication: FR2976721, Dec 2012.

[Lis12(b)] M. Lisart, A. Sarafianos, O. Gagliano, M. Mantelli, Device for protecting an integrated circuit chip against attacks, N° de publication: FR2976722, Dec 2012.

[Lik94] J.P. Likforman, « Saturation sélective d’excitons et effets de cohérence dans des puits quantiques en arséniure de gallium », Thèse de Doctorat de l’Ecole Polytechnique, 1994.

[Lli12(a)] R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, V. Pouget, D. Lewis, J.M. Dutertre, A. Tria, Characterization and TCAD simulation of 90 nm technology NMOS transistors under continous photoelectric laser stimulation for failure analysis improvement, IPFA 2012.

[Lli12(b)] R. Llido, J. Gomez, V. Goubier, G. Haller, V. Pouget, D. Lewis, "Improving defect localization techniques with laser beam with specific analysis and set-up modules", IEEE International Reliability Physics Symposium (IRPS), FA2.1, FA2.5.

[Lli12(c)] R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, V. Pouget, D. Lewis, J.M. Dutertre, A. Tria, Characterization and TCAD simulation of 90 nm technology PMOS transistors under continous photoelectric laser stimulation for failure analysis improvement, ISTFA 2012.

[Mat06] A. Matthews, "Low Cost Attacks on Smart Cards, the Electrognetic Side-Channel", NGSSoftware Insight Security Research (NISR) white paper, September, 2006.

[Min06] R. Minixhofer, “TCAD as an integral part of the semiconductor manufacturing environment", Simulation of Semiconductor Processes and Devices, vol. issue pp. 9-16, 2006.

[Mon99] T. Monnier, F.M. Roche, J. Cosculluela, R. Velazco, « SEU Testing of a Novel Hardened Register Implemented Using Standard CMOS Technology », IEEE Trans. Nucl. Sci., 46, p. 1440, 1999.

[Mul05] E. De Mulder, P. Buysschaert, S. B. örs, P. Delmotte, B. Preneel, G. Vanderbosch and I. Verbauwhede, "Electromagnetic Analysis Attack on FPGA Implementation of an Elliptic Curve Cryptosystem", presented at

EUROCON 2005, Belgrade, Serbia & Montenegro, November, 22-24, 2005.

[Mus91] O. Musseau, J.L. Leray, V. Ferlet, A. Umbert, Y.M. Coic and P. Hesto, "Charge collection mecanisms in MOS/SOI transistors irradiated by energetic heavy ions", IEEE Transaction on Nuclear Science vol 38 n°6 Dec 1991 pp 1226-1233.

[Ord10] T. Ordas, PhD Thesis, Analyse des emissions électromagnétiques des circuits intégrés, Université de Montpellier II, 2010.

[Ols05] B. D. Olson, D. R. Ball, K. M. Waren, L. W. Massengill, N. F. Haddad, S. E. Doyle and D. McMorrow, Simultaneous Single Event Charge Sharing and Parasitic Bipolar Conduction in a Highly-Scaled SRAM Design, IEEE transactions on nuclear science, vol. 52, No. 6, Dec 2005.

[Ott04] M. Otto, Ph Thesis, Fault Attacks and Countermeasures, Fakultat fur Elektrotechnik, Informatik und Mathematik, Institut fur Informatik, Universitat Paderborn, 2004.

[Per93] S. Perkowitz, « Optical Characterization of Semiconductors : Infrared, Raman and Photoluminescence Spectroscopy », Academic Press, 1993.

[Pir03] G. Piret, J.-J. Quisquater, " A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD", In C. Walter, C. K. Koc, C. Paar, editors, Fifth International Workshop on Crypto-graphic Hardware and Embedded Systems (CHES 2003), Vol. 2779 of Lecture Notes in Computer Science, pp. 291-303, Springer.

[Pou00(a)] V. Pouget, "Simulation expérimentale par impulsions laser ultra-courtes des effets des radiations ionisantes sur les circuits intégrés.", Thèse, Université de Bordeaux 1, n°.2250, 2000, pp. 121-124.

[Pou00(b)] V. Pouget, ph. D Thesis, Université Bordeaux I, 2000, "Simulation expérimentale par impulsions laser ultra-courtes des effets des radiations ionisantes sur les circuits intégrés.", n°.2250, 2000, p. 122.

[Pou00(c)] V. Pouget, ph. D Thesis, Université Bordeaux I, 2000, "Simulation expérimentale par impulsions laser ultra-courtes des effets des radiations ionisantes sur les circuits intégrés", n°.2250, 2000, p. 82.

[Qui01] J.J. Quisquater and D. Samyde, “Electromagnetic analysis (EMA): Measures and counter-measures for smard cards,” Proceedings of Esmart' vol. 2140 of LNCS, pp. 200-210, Springer-Verlag, 2001.

[Roc92] L.R. Rockett, « Simulated SEU Hardened Scaled CMOS SRAM Cell Design Using Gated Resistors », IEEE Trans. Nucl. Sci., p. 1532, 1992.

[Roc98] P. Roche, J. M. Palau, K. Belhaddad, G. Bruguier, R. Ecoffet, J. Gasiot, “SEU Response of an Entire SRAM Cell Simulated as one Contiguous Three Dimensionnal Device Domain”, IEEE Trans. Nucl. Sci., vol. 45, no. 6, pp. 2534-2543, 1998.

[Sar12] A. Sarafianos, R. Llido, O. Gagliano, J.M. Dutertre, V. Serradeil, M. Lisart, V. Goubier, A. Tria, V. Pouget, D. Lewis, Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90 nm technology, ESREF 2012.

[Sar12(b)] A. Sarafianos, R. Llido, O. Gagliano, J.M. Dutertre, V. Serradeil, M. Lisart, V. Goubier, A. Tria, V. Pouget, D. Lewis, Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90 nm technology, ISTFA 2012.

[Sar13] A. Sarafianos, J.M. Dutertre, O. Gagliano, V. Serradeil, A. Tria, Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology, IRPS 2013.

[Sar13(b)] A. Sarafianos, J.M. Dutertre, O. Gagliano, V. Serradeil, A. Tria, Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology, IPFA 2013.

[Sar13(b)] A. Sarafianos, C. Roscian, J. M. Dutertre, M. Lisart, A. Tria, Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell, "in press", ESREF 2013.

[SarI87] M. Saritas and H.D. McKell, "Absorption coefficient of Si in the wavelength region between 0.8-1.16 μm", J. of Applied Physics., vol. 61, pp. 4923, 1987.

[Sen] TCAD Sentaurus user’s manual (Synopsys).

[Sie86] Siegman, A.E. Lasers; Oxford University Press: Mill Valley, CA, pp. 682–685 1986.

[Sko02] S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks", Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), LNCS, vol. 2523, Springer-Verlag, 2002, pp. 2-12.

[Sti96] D. Stinson, Cryptographie : "Théorie et Pratique", International Thomson Publishing ed. Paris: International Thomson Publishing France, 1996. 2-

84180-013. pp. 106.

[Vol05] S. Voldman, E. Gebreselasie, M. Zierak, D. Hershberger, D. Collins, N. Feilchenfeld, S. St. Onge, and J. Dunn, Latchup in merged triple well structure, IRPS 2005.

[Woo93] R.L. Woodruff and P.J. Rudeck, "Three-Dimensionnal Numerical Simulation of Single Event Upset of an SRAM cell", IEEE Transaction on Nuclear Science, vol. 40, no. 6, Dec. 1993, pp. 1795-1803.

[Yar97] A. Yariv, "Optical Electronics in Modern Communications", filth edition, Oxford, 1997.

[Yen02] S.-M. Yen, S. J. Moon and J. C. Ha. "Hardware fault attacks on RSA with CRT revisited". In P. J. Lee and C. H. Lim, editors, Proceedings of the 5th International Conference on Information Security and Cryptology - (ICISC), number 2587 of LNCS, pp. 374-388.

[Yen03] S.-M. Yen, S. J. Moon and J. C. Ha. "Permanent fault attack on the parameters of RSA with CRT". In R. Safavi-Naini and J. Seberry, editors, Proceedings of the 8th Australian Conference on Information Security and Privacy (ACISP), No. 2727 of LNCS.

École Nationale Supérieure des Mines

de Saint-Étienne

NNT : *2013 EMSE 0703*

Alexandre SARAFIANOS

FAULT INJECTIONS BY LASER IMPULSIONS IN SECURED MICROCONTROLLERS

Speciality : Microelectronics

Keywords : Secured microcontrollers, laser injection, electrical modelling, countermeasures

Abstract :

From time immemorial, human beings have been forced to protect the fruits of their creativity and ensure the security of their property. This information is very often strategic, in particular in political and commercial relationships. Also the need to protect this information by keeping it concealed in regards to enemies or competitors soon appeared. From ancient times, the methods used for masking and eventually encrypting information were numerous. Protection techniques have only advanced grown since the industrial era and have led to the precursor of electro-mechanic machines (such as the famous Enigma machine). Nowadays, new protection circuitry embeds very efficient algorithms. Despite these protections, they remain a prime target for « attackers » who try to break through all means of securing structures, for fraudulent uses. These « attackers » have a multitude of attack techniques. One of them uses a method of fault injections using a laser beam.

From the beginning (Chapter I), this manuscript describes the state of the art of fault injections, focusing on those made using a laser beam. It explains these intrusive methods and provides information on how to protect even the most secure microcontrollers against these types of attacks. It is necessary to understand the physical phenomena involved in the interaction between a coherent light wave, such as lasers, and the physicochemical material that makes up a microcontroller. To better understanding these phenomena, an electrical modeling of CMOS gates under laser illumination was implemented to predict their behavior (Chapter II). Good correlations have been obtained between measurements and electrical simulation. These results can be used to test the laser sensitivity of CMOS gates through electrical cartographies. Due to the better understanding of the phenomena and the developed simulator, many countermeasures have been developed. The techniques presented in this manuscript offer new possibilities to increase the robustness of CMOS circuits against laser attacks. This work has already enabled the implementation of efficient counter-measures on embedded laser sensors and significantly enhanced product security against different laser attacks.

École Nationale Supérieure des Mines

de Saint-Étienne

NNT : *2013 EMSE 0703*

Alexandre SARAFIANOS

INJECTION DE FAUTES PAR IMPULSION LASER DANS LES CIRCUITS SÉCURISÉS

Spécialité: Microélectronique

Mots clefs : Microcontrôleurs sécurisés, injection laser, modélisation électrique, contre-mesures.

Résumé :

De tout temps, l'Homme s'est vu contraint de protéger les fruits de sa créativité et les domaines concernant sa sécurité. Ses informations sont souvent sensibles, dans les relations politiques et commerciales notamment. Aussi, la nécessité de les protéger en les rendant opaques au regard d'adversaires ou de concurrents est vite survenue. Depuis l'Antiquité, les procédés de masquages et enfin de cryptages furent nombreux. Les techniques de protection, depuis l'époque industrielle n'ont fait que croître pour voir apparaître, durant la seconde guerre mondiale, l'archétype des machines électromécaniques (telle l'Enigma), aux performances réputées inviolables. De nos jours, les nouveaux circuits de protection embarquent des procédés aux algorithmes hyper performants. Malgré toutes ces protections, les produits restent la cible privilégiée des « pirates » qui cherchent à casser par tous les moyens les structures de sécurisation, en vue d'utilisations frauduleuses. Ces « hackers »

disposent d'une multitude de techniques d'attaques, l'une d'elles utilise un procédé par injections de fautes à l'aide d'un faisceau laser.

Dès le début de ce manuscrit (Chapitre I), l'état de l'art de l'injection de fautes sera développé, en se focalisant sur celles faite à l'aide d'un faisceau laser. Ceci aidera à bien appréhender ces procédés intrusifs et ainsi protéger au mieux les microcontrôleurs sécurisés contre ces types d'attaques. Il est nécessaire de bien comprendre les phénomènes physiques mis en jeu lors de l'interaction entre une onde de lumière cohérente, tels les lasers et le matériau physico-chimique qu'est le silicium. De la compréhension de ces phénomènes, une modélisation électrique des portes CMOS sous illumination laser a été mise en œuvre pour prévoir leurs comportements (chapitre II). De bonnes corrélations ont pu être obtenues entre mesures et simulations électrique. Ces résultats peuvent permettre de tester la sensibilité au laser de portes CMOS au travers de cartographies de simulation. De cette meilleure compréhension des phénomènes et de ce simulateur mis en place, de nombreuses contre-mesures ont été imaginées. Les nouvelles techniques développées, présentées dans ce manuscrit, donnent déjà des pistes pour accroître la robustesse des circuits CMOS contre des attaques laser. D'ores et déjà, ce travail a permis la mise en œuvre de détecteurs lasers embarqués sur les puces récentes, renforçant ainsi sensiblement la sécurité des produits contre une attaque de type laser.

Liste des brevets:

[1] N° de publication: FR2976721 - Device for detecting an attack in an integrated circuit chip.

[2] N° de publication: FR2976722: Device for protecting an integrated circuit chip against attacks.

[3] N° d'enregistrement national de l'I.N.P.I.: FR1250787 - Device for protecting an integrated circuit against backside attacks.

[4] N° d'enregistrement national de l'I.N.P.I.: FR1251151 – Detection of a laser attack in an integrated circuit chip.

[5] N° d'enregistrement national de l'I.N.P.I.: FR1261066 – Protection of an integrated circuit against attacks.

Revues

[1] Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90nm technology, A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart, V. Goubier, J.M. Dutertre, A. Tria, V. Pouget, D. Lewis, Microelectronics Reliability 2012.

[2] Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell, A. Sarafianos, C. Roscian, J.-M. Dutertre, M. Lisart, A. Tria, Microelectronics Reliability 2013.

Liste des publications:

[1] Characterization and TCAD Simulation of 90nm Technology NMOS Transistor Under Continuous Photoelectric Laser Stimulation for Failure Analysis Improvement, R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, G. Haller, V. Pouget, D. Lewis, J.M. Dutertre, A. Tria, IPFA 2012.

[2] Characterization and TCAD Simulation of 90nm Technology PMOS Transistor Under Continuous Photoelectric Laser Stimulation for Failure Analysis Improvement, R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, G. Haller, V. Pouget, D. Lewis, J.M. Dutertre, A. Tria, ISTFA 2012.

[3] Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90nm technology, A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart, V. Goubier, J.M. Dutertre, A. Tria, V. Pouget, D. Lewis, ESREF 2012.

[4] Building the electrical model of the Photoelectric Laser Stimulation of an NMOS transistor in 90nm technology, A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart, V. Goubier, J.M. Dutertre, A. Tria, V. Pouget, D. Lewis, ISTFA 2012.

[5] Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology, Alexandre Sarafianos, Jean-Max Dutertre, Olivier Gagliano, Valérie Serradeil, Mathieu Lisart, Assia Tria, IRPS 2013.

[6] Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology, Alexandre Sarafianos, Jean-Max Dutertre, Olivier Gagliano, Valérie Serradeil, Mathieu Lisart, Assia Tria, IPFA 2013.

[7] Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell, A. Sarafianos, C. Roscian, J.-M. Dutertre, M. Lisart, A. Tria, ESREF 2013.

[8] Robustness improvement of an SRAM cell against laser-induced fault injection, A. Sarafianos, C. Roscian, J.-M. Dutertre, M. Lisart, O. Gagliano, V. Serradeil, A. Tria, DFTS 2013, « in press ».

[9] Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells, FDTC 2013, C. Roscian, A. Sarafianos, J.-M. Dutertre, A. Tria, M. Listart, Cosade 2013 “in press”.

Communication:

[1] Discussion on the Model of Laser-Induced Faults in SRAM Memory Cells, C. Roscian, A. Sarafianos, J.-M. Dutertre, A. Tria, M. Listart, Cosade 2013.