



**HAL**  
open science

# Injection Electromagnétique Micro-onde jusqu'à 100 GHz. Susceptibilité, Détection non-linéaire, Microscopie champ proche

Jérémy Raoult

► **To cite this version:**

Jérémy Raoult. Injection Electromagnétique Micro-onde jusqu'à 100 GHz. Susceptibilité, Détection non-linéaire, Microscopie champ proche. Electronique. Université de Montpellier, 2019. tel-02171998

**HAL Id: tel-02171998**

**<https://hal.science/tel-02171998>**

Submitted on 3 Jul 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# **SYNTHESE DES ACTIVITES DE RECHERCHE POUR L'OBTENTION DE L'HABILITATION A DIRIGER DES RECHERCHES**

**En Électronique**

**Développées à l'IES, UMR 5214**

**Ecole Doctorale I2S**

## **Injection Electromagnétique Micro-onde jusqu'à 100 GHz**

**Susceptibilité, Détection non-linéaire, Microscopie  
champ proche**

**Présentée par Jérémy RAOULT**

**Le 01 juillet 2019**

**Devant le jury composé de**

**Philippe FERRARI, Professeur, RFIC Lab**

**Rapporteur**

**Geneviève DUCHAMP, Professeur, IMS**

**Rapporteuse**

**Philippe BESNIER, Directeur de recherche, IETR**

**Rapporteur**

**Christian PERSON, Professeur, Lab-STICC**

**Examineur**

**Christophe GAQUIERE, Professeur, IEMN**

**Examineur**

**Daniel DOLFI, Ingénieur HDR, TRT**

**Examineur**

**Laurent CHUSSEAU, Directeur de recherche, IES**

**Examineur**

**Jérôme BOCH, Professeur, IES**

**Examineur**



**UNIVERSITÉ  
DE MONTPELLIER**



# SOMMAIRE

## **Partie I : Curriculum vitae**

1) Etat civil, cursus universitaire et situation professionnelle .....	5
2) Encadrements scientifiques .....	6
3) Récompenses, Jurys de thèse, Activités complémentaires .....	8
4) Liste des publications et bilan scientifique .....	8
5) Activités d'enseignement .....	17

## **Partie II : Synthèse des activités de recherche**

<u>Introduction</u> .....	23
---------------------------	----

<u>Chapitre 1 : Perturbation de l'électronique par injection de signaux</u> .....	28
---	----

1) Mise en évidence de susceptibilité au niveau composant .....	31
a. Méthodologie de tests .....	31
b. Bancs de test mis en place et les principaux résultats .....	31
2) Moyens de calcul et de simulation .....	40
a. Calcul analytique .....	41
b. Simulation numérique .....	42
3) Expérimentations et calculs au niveau fonction électronique .....	45
a. Présentation des tests menés .....	46
b. Prédiction des effets par la simulation .....	51
4) Injection aux fréquences millimétriques .....	54
a. Mise en place du banc de test .....	55
b. Résultats d'injection sur un RF front-end Wifi .....	56
c. Vers une interprétation des résultats .....	59
d. Etude paramétrique de la sensibilité de puces RF front-ends .....	60
5) Bilan et perspectives .....	62

<u>Chapitre 2 : Détection d'une électronique RF à distance</u> .....	63
--	----

1) Radars déployés pour la détection de jonction, d'électroniques et de systèmes RF .....	63
2) Mise en place d'un banc de test radar à intermodulation .....	65
3) Performances attendues en matière de portée de détection .....	69

4) Perspectives : vers une identification de cibles inconnues .....	71
---	----

Chapitre 3 : Technique d'injection en champ proche – Optimisation de sonde en situation de couplage .....

1) Méthodologie d'optimisation de sondes magnétiques de champ proche .....	77
2) Modélisation du couplage sonde/ligne .....	79
a. Expériences d'injection en champ proche .....	79
b. Modèle de couplage par la mutuelle .....	80
c. Validation de l'injection en champ proche sur des test-chips .....	83

Chapitre 4 : Technique de champ proche aux fréquences millimétriques

Applications à la microscopie et à l'imagerie .....

1) Réflectométrie à haute résolution spatiale .....	87
a. Sonde et réflectomètre .....	87
b. Résultats d'imagerie .....	90
2) Réflectométrie vectorielle en champ proche .....	93
a. Principe de fonctionnement et premières images .....	93
b. Vers une caractérisation physique de matériaux .....	95
3) Discussion et perspectives .....	96

Bilan et perspectives .....

Bibliographie .....

Annexe : Sélection de publications .....

Partie I

CURRICULUM VITAE



## 1) Etat civil, cursus universitaire et situation professionnelle

### **Jérémy RAOULT**

Né le 14 décembre 1976 en France, à Toulouse

Nationalité Française

Situation familiale marié, 2 enfants

### **Coordonnées professionnelles**

IES, Institut d'Electronique et des Systèmes

CNRS UMR 5214

Université Montpellier

860, rue de St Priest

34090 MONTPELLIER

Tél : +33-(0)4-67-14-38-20

Mail : [raoult@ies.univ-montp2.fr](mailto:raoult@ies.univ-montp2.fr)

### **Parcours**

**Ingénieur ENSIL** : Ecole Nationale Supérieure des Ingénieurs de Limoges, Spécialité Electronique et Télécommunication

- **DEA de l'université de Limoges**, spécialité Electronique des hautes fréquences et optoélectronique  
**Stage DEA** : Etude et caractérisation de transistors bipolaires à hétérojonction Si/SiGe en vue de leur modélisation électrique, stage effectué au LPM (Laboratoire de Physique de la Matière) de l'INSA de Lyon, soutenu le 15 septembre 2000.
- **Docteur de l'Institut Nationale des Sciences Appliquées (INSA) de Lyon**, Spécialité Dispositifs de l'électronique intégrée  
**Thèse** : « Etude et modélisation de transistors bipolaires à hétérojonction SiGe, Application à la conception d'oscillateurs radiofréquences intégrés », soutenue le 16 décembre 2003, direction : Alain Poncet et Christian Gontrand. Co-encadrement : Jacques Verdier.
- **Monitorat** : INSA Lyon, département génie électrique, septembre 2000- septembre 2003
- **Attaché Temporaire de Recherche et d'Enseignement** : INSA Lyon, département Télécommunications Services et Usages, septembre 2003-septembre 2004
- **Recrutement Maître de Conférences** :  
Recrutement : 1<sup>er</sup> septembre 2004 à l'université Montpellier 2  
Titularisation : 1<sup>er</sup> septembre 2005  
**Etablissement** : IUT de Montpellier, département GEII  
**Laboratoire de recherche** : IES (Institut de l'Electronique et des Systèmes), UMR 5214  
**Section CNU** : 63- Electronique, Optronique et Systèmes  
**Habilitation** : confidentiel défense, depuis juillet 2014

## 2) Encadrements scientifiques

### a) Stages Master 2 et ingénieur

- [Stage1] Lionel SNADGY : « Etude et caractérisation de transistors bipolaires issus de technologies BiCMOS avancées », février 2005 – juin 2005
- [Stage2] Adrien DORIDANT : « Etude de l'impact d'une agression électromagnétique dans la gamme du GHz en zone de champ proche sur des amplificateurs opérationnels soumis à des radiations ionisantes », février 2009 – juin 2009
- [Stage3] Amable BLAIN : « Effet d'une agression électromagnétique sur les différentes caractéristiques d'un VCO », février 2009 – juin 2009
- [Stage4] Rachid OMAROUAYACHE : « Simulation électromagnétique de sondes de champ proche pour injection de fautes », mars 2011 – juillet 2011
- [Stage5] Pierre PAYET : « Imagerie et perturbation des circuits intégrés par ondes EM en champ proche jusqu'à 100 GHz », Mars 2014 – Août 2014
- [Stage6] Alexandre MARTORELL : « Comportement non-linéaire et changement d'état d'une carte de radiocommunication en téléphonie mobile 2G », Mars 2014- Août 2014
- [Stage7] Zohir FELLAH TOUTA : « Etude de l'interaction entre sondes de champ proche magnétiques et circuits intégrés », mars 2016 – août 2016.
- [Stage8] Mathieu GUERY : « Etude d'une agression électromagnétique hors-bande sur circuits électroniques », février 2017- juillet 2017.

### b) Thèses

- [Th1] Patrice BENOIT – « **Influence de paramètres technologiques sur le bruit basse fréquence des transistors bipolaires à hétérojonction Si/SiGe :C.** », octobre 2002 – décembre 2005.  
Thèse CIFRE à 50% chez ST Microelectronics Crolles  
Encadrement industriel : Jean Charles VILDEUIL, Pierre LLINARES, 40%  
Directeur de thèse : Fabien PASCAL, 20%  
Co-encadrement : Colette DELSENY, 20%  
Co-encadrement : Jérémy RAOULT, 20%
- [Th2] Tristan DUBOIS – « **Etude de l'effet d'ondes électromagnétiques sur le fonctionnement de circuits électroniques – Mise en place d'une méthode de test des systèmes** », octobre 2006- octobre 2009  
Thèse financée par une bourse DGA.  
Directrice de thèse : Sylvie JARRIX, 60%  
Co-encadrement : Jérémy RAOULT, 40%  
Tristan DUBOIS est actuellement Maître de Conférences à l'université de Bordeaux.
- [Th3] Amable BLAIN - « **Effets d'une agression électromagnétique sur le fonctionnement d'un oscillateur contrôlé en tension et d'une PLL 5 GHz** », Octobre 2009- Octobre 2012.  
Thèse financée par une bourse Ecole Normale Supérieure de Cachan.  
Directrice de thèse : Sylvie JARRIX, 20%  
Co-encadrement : Jérémy RAOULT, 80%  
Amable BLAIN est actuellement ingénieur études et essais chez Nuclétudes – Airbus (Defense and space).

- [Th4] Adrien DORIDANT – « **Effets de synergie entre susceptibilité électromagnétique et dose ionisante pour applications en électronique spatiale et de défense** » Janvier 2010 – Janvier 2013.  
Thèse CIFRE cofinancée par CEA-Gramat et Thalès Alenia Space, 100% du temps à l'IES  
Directrice de thèse : Sylvie JARRIX, 50%  
Co-encadrement : Jérémy RAOULT, 50%  
Adrien DORIDANT est actuellement Ingénieur de recherche CEM chez NXP.
- [Th5] Rachid OMAROUAYACHE- « **Imagerie et Injection électromagnétique en champ proche micro-onde et millimétrique** », Janvier 2013 - Décembre 2015  
Thèse financée par le projet ANR E-MATA-HARI  
Directeur de thèse : Laurent CHUSSEAU, 50%  
Co-encadrement : Jérémy RAOULT, 50%  
Rachid OMAROUAYACHE est actuellement Ingénieur R&D système champ proche chez NEXIO.
- [Th6] Clovis POUANT - « **Caractérisation de la susceptibilité électromagnétique des étages d'entrée de composants électroniques** », Octobre 2012- Octobre 2015,  
Thèse financée par le CEA Gramat ; 50% à Gramat, 50% à l'IES  
Encadrement industriel : Patrick HOFFMANN, 30%  
Directrice de thèse : Sylvie JARRIX, 10%  
Co-encadrement : Jérémy RAOULT, 60%  
Clovis POUANT est actuellement Ingénieur CDD au CEA Gramat.
- [Th7] Pierre PAYET – « **Injection électromagnétique et Microscopie en champ proche sur structures irradiées** », octobre 2015 – octobre 2018  
Contrat doctoral de l'I2S  
Directeur de thèse : Laurent CHUSSEAU, 60%  
Co-encadrement : Jérémy RAOULT, 40%  
Pierre Payet cherche actuellement un stage post-doctoral
- [Th8] Alexandre MARTORELL - « **Réponse de systèmes électroniques à une sollicitation radiofréquence** », Septembre 2015 – septembre 2018  
Thèse CIFRE ANRT THALES Communications & Security ; 20% à Thalès, 80% à l'IES  
Encadrement industriel : Robin MARIJON, Christian CAREL, 10%  
Directeur de thèse : Laurent CHUSSEAU, 10%  
Co-encadrement : Jérémy RAOULT, 80%  
Alexandre Martorell est actuellement Ingénieur R&D chez Thalès Communications & Security

c) Stages post-doctoral

- [PostDoc1] Tristan DUBOIS – « **Etude de formes d'onde d'agressions électromagnétiques hyperfréquences sur la vulnérabilité de circuits électroniques** », mars 2010 – mars 2011  
Financement DGA, stage réalisé au centre de recherche Poly-Grames de Montréal (Canada)  
Encadrement à Montréal : Jean-Jacques LAURIN, 40%  
Parrain scientifique en France : Sylvie JARRIX, 30%  
Co-encadrement, Jérémy RAOULT, 30%

[PostDoc2] Adrien DORIDANT – « **Etude de la susceptibilité électromagnétique en zone de champ proche des blocs d'une chaîne de réception dans la gamme micro-onde** », mars 2013 - mars 2014  
Financement DGA, stage réalisé au centre de recherche Poly-Grames de Montréal (Canada)  
Encadrement à Montréal : Jean-Jacques LAURIN, 40%  
Parrain scientifique en France : Sylvie JARRIX, 30%  
Co-encadrement, Jérémy RAOULT, 30%

### 3) Récompenses, Jurys de thèse, Activités complémentaires

#### a) Récompenses

[REC1] Prix régional SEE, Alexandre Martorell, sous la direction de J. Raoult, 2014

[REC2] Prix national SEE André Blanc-Lapierre 2014, Alexandre Martorell, sous la direction de J. Raoult, 2014

#### b) Jurys de thèse extérieurs à l'IES

[J1] Rachid HAMANI : “Characterization and modeling of devices and amplifier circuits at millimeter-wave band”, soutenue le 12/12/2014 à l'XLIM, université de Limoges, Examineur.

[J2] Maxime GIRARD : « Recherche de vulnérabilités des étages de réception aux agressions électromagnétiques de forte puissance : cas d'un LNA AsGa », soutenue le 12/12/2018, université de Bordeaux, Examineur.

#### c) Activités complémentaires

- Co-Organisateur de la journée thématique « Champ Proche : Applications pour la CEM et la sécurité des circuits électroniques », qui a eu lieu au LAAS-CNRS, à Toulouse, le 19 Juin 2015.
- Membre du comité de programme technique de la conférence internationale IEEE EMC compo (Electromagnetic Compatibility of Integrated Circuits), depuis 2016.
- Reviewing pour les revues Solid-State-Electronics (SSE) et Progress in Electromagnetics research Journal (PIER).
- Expertise pour des appels à projet régionaux, de soutien au programme de recherche

### 4) Liste des publications et bilan scientifique

#### a) Revue internationale

[R1] **J. Raoult, L. Militaru, J. Verdier and A. Souifi**  
“Time domain and frequency analysis of RTS noise in deep submicron SiGe HBTs”,  
Nuclear Instruments and Methods B 2002, Vol 186, N°1-4, pp. 435-440.

[R2] **C. Gontrand, J. Raoult, P. Girard, S. Latreche, L. Militaru, F. Miller, J. Verdier, K. Souifi, F. Calmon, P.J. Viverge, B. Bouazza**

- “Theoretical and experimental insights concerning ultra-submicronic Si/SiGe Heterojunction bipolar transistor specified for radio frequency range systems”, Recent Research Developments in Science and Technology of semiconductors, India Transworld Research Network, 2002, pp. 201-204.
- [R3] **P. Benoit, J. Raoult, C. Delseny, F. Pascal, L. Snadny, J.C. Vildeuil, M. Marin, B. Martinet, D. Cottin, O. Noblanc**  
 “Dc and Low Frequency Noise analysis of hot-carrier induced degradation of low complexity 0.13  $\mu\text{m}$  CMOS bipolar transistors”, Microelectronics Reliability, 45, p.p.1800-1806, 2005.
- [R4] **J. Raoult, F. Pascal, C. Delseny, M. Marin, M.J. Deen**  
 “Impact of Carbon Concentration on 1/f Noise and Random Telegraph Signal Noise in SiGe:C Heterojunction Bipolar Transistors”, Journal of Applied Physics, 103, June 2008.
- [R5] **J. Raoult, F. Pascal, C. Leyris**  
 “I-V and Low frequency noise characterization of Polysilicon and Amorphous Ti- and Co-salicide resistors”, Thin Solid Films, Volume 518, Issue 9, 26 February 2010, Pages 2497-2500.
- [R6] **T. Dubois, J. Raoult, S. Jarrix, A. Blain, A. Doridant**  
 “Optimal Electric Wave Propagation parameters on a transmission line – Schottky Diode System”, Progress in Electromagnetics Research Letters, vol. 27, pp. 125-132, 2011.
- [R7] **A. Doridant, S. Jarrix, J. Raoult, A. Blain, N. Chatry, P. Calvel, P. Hoffmann, L. Dusseau**  
 “Impact of Total Ionizing Dose on the Electromagnetic Susceptibility of a single bipolar transistor”, IEEE Transaction on Nuclear Science, Volume 59, issue 4, Part 1, 2012, pp 860-865.
- [R8] **A. Doridant, J. Raoult, S. Jarrix, A. Blain, N. Chatry, P. Calvel, P. Hoffmann, L. Dusseau**  
 “Combined effects of CO<sub>60</sub> Dose and High Frequency Interferences on a Discrete Bipolar Transistors”, IEEE Transaction on Nuclear Science, Volume 59, issue 6, Part 1, 2012, pp 3004-3010.
- [R9] **T. Dubois, J-J.Laurin, J. Raoult, S. Jarrix**  
 « Effect of Low and High Power Continuous Wave Electromagnetic Interference on a Microwave Oscillator System : From VCO to PLL to QPSK Receiver”, IEEE Transactions on Electromagnetic Compatibility, Volume 56 Issue 2, pp 286-293, 2014.
- [R10] **J. Raoult, A. Blain, A. Doridant, S. Jarrix**  
 “Interference Signal Effects on a High Frequency Monolithic Voltage-Controlled Oscillator: Experiments and Simulations”, IEEE Transactions on Electromagnetic Compatibility, volume 56, Issue 1, pp 51-59, 2014.
- [R11] **R. Omarouayache, P. Payet, J. Raoult, L. Chusseau**  
 “Millimeter-wave near-field imaging with bow-tie antennas”, Opt. Express, vol. 23, pp. 12144-12151, May 2015
- [R12] **L. Chusseau, P. Payet, J. Raoult**  
 « Optimization of near-field image capture with millimeter-wave bow-tie probes”, IEEE Transactions on Instrumentation and Measurement, vol 66, Issue 1, pp 61-68, 2017
- [R13] **P. Payet, J. Raoult, L. Chusseau**  
 “Remote extinction of a 2.4 GHz RF front-end using millimeter-wave EMI in the near-field”, Progress in Electromagnetics Research Letters, vol. 68, pp. 99-104, 2017.
- [R14] **P. Payet, M. Guery, J. Raoult, L. Chusseau**

“Out-of-band disturbance of mm-wave EMI on RF front-ends”, *Microelectronics Reliability*, vol. 76-77, pp. 670-673, 2017.

- [R15] **A. Martorell, J. Raoult, R. Marijon, L. Chusseau**  
“RF front-ends nonlinearity characterization using reflected power”, *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, Issue 6, pp. 1925-1931, 2017.
- [R16] **C. Pouant, J. Raoult, P. Hoffmann, L. Chusseau, F. Torrès**  
« Control of a MOS inverter by out-of-band pulsed microwave excitation », *Progress in Electromagnetics Research M*, vol. 61, pp. 185-195, 2017.
- [R17] **C. Pouant, F. Torrès, A. Reineix, P. Hoffmann, J. Raoult, L. Chusseau**  
« Modeling and analysis of Large signal RFI effects in MOS transistors », *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, Issue 1, pp. 111-120, 2019.

b) Conférences internationales

- [C1] **L. Militaru, J. Raoult, J. Verdier, G. Brémond, A. Souifi**  
“Low Frequency Noise Sources in Submicron SiGe-base Heterojunction Bipolar Transistors”, *Proc. ICNF, 16th International Conference on Noise in Physical Systems and 1/f Fluctuations*, Gainesville (Etats-Unis), pp. 201-204.
- [C2] **J. Raoult, L. Militaru, J. Verdier, A. Souifi**  
“Time domain and frequency analysis of RTS noise in deep submicron SiGe HBTs”, *E-MRS Strasbourg*, 5-8 june 2001.
- [C3] **J. Raoult, J. Verdier, P. Girard, F. Calmon, P.J Viverge, A. Pakfar, C. Gontrand,**  
“A noise and power analysis of SiGe HBTs for RF applications”, *ISTDM Nagoya, International SiGe Technology and Device Meeting*, 15-17 january 2003.
- [C4] **P. Benoit, J. Raoult, C. Delseny, F. Pascal, J.C. Vildeuil, B. Szlag, A. Monroy**  
“Influence of Carbon Incorporation on the Low Frequency Noise of Si/SiGe :C HBTs based on 0.25  $\mu\text{m}$  BICMOS Technology”, *Proceedings of 18<sup>th</sup> International Conference on Noise and Fluctuations*, Salamanca, 19-23 september 2005, p 257-260
- [C5] **P. Benoit, J. Raoult, C. Delseny, F. Pascal, L. Snadny, J.C. Vildeuil, M. Marin, B. Martinet, D. Cottin, O. Noblanc**  
“Dc and Low Frequency Noise analysis of hot-carrier induced degradation of low complexity 0.13  $\mu\text{m}$  CMOS bipolar transistors”, *ESREF European Symposium Reliability of Electron Devices*, Arcachon, 10-14 october 2005.
- [C6] **F. Pascal, J. Raoult, C. Delseny, P. Benoit, M. Marin, M. J. Deen**  
“Impact of technological parameters on the low frequency noise of advanced HBT”. *Proceedings of 19<sup>th</sup> international conference on noise in physical systems and 1/f fluctuations*, Tokyo, Japan, septembre 2007, pp. 77-82, ISBN 978-0-7354-0432-8.
- [C7] **J. Raoult, F. Pascal, M. Marin**  
“Low frequency noise spectroscopy of interfacial defects in advanced Si and Si/SiGe(C) bipolar transistors”, *E-MRS Strasbourg*, 26-29 may 2008.
- [C8] **J. Raoult, F. Pascal, C. Leyris**  
“I-V and Low frequency noise characterization of Polysilicon and Amorphous Ti- and Co-salicide resistors”, *E-MRS Strasbourg*, 8-12 June 2009.

- [C9] **F. Pascal, J. Raoult, C. Leyris**  
 “Study of the Low Frequency Noise of Metallic Emitter SiGeC Heterojunction Bipolar Transistors”, Proceedings of the 20<sup>th</sup> International Conference on Noise and Fluctuations, Pise, 15-19 june 2009.
- [C10] **F. Pascal, J. Raoult, B. Sagnes, A. Hoffmann, S. Haendler, G. Morin**  
 “Improvement of 1/f noise in advanced 0.13  $\mu\text{m}$  BiCMOS SiGe:C Heterojunction Bipolar Transistors”, 21<sup>th</sup> IEEE International Conference on Noise and Fluctuations, Toronto, 12-16 June 2011.
- [C11] **T. Dubois, S. Jarrix, J. Raoult, A. Pénarier, P. Nouvel, B. Azaïs et D. Gasquet,**  
 “Electromagnetic Susceptibility Studies of Op. Amp. and a VCO for a PLL Application”, Workshop International, EMC Compo, Toulouse, France, Novembre, 2009.
- [C12] **S. Jarrix, L. Dusseau, A. Doridant, T. Dubois, A. Blain, J. Raoult,** “Preliminary studies of the impact of dose radiation on the electromagnetic susceptibility of comparators”, European Workshop, EMC Europe, Wroclaw, Poland, sept 2010.
- [C13] **S. Jarrix, L. Dusseau, N. Chatry, P. Hoffmann, A. Doridant, A. Blain, T. Dubois, J. Raoult, P. Calvel,** "First studies of the impact of dose radiation on the electromagnetic susceptibility of bipolar transistors", 12<sup>th</sup> IEEE Latin American Test Workshop (LATW) 2011, 27 – 30 Mars, Recife (Brésil).
- [C14] **T. Dubois, J.J. Laurin, J. Raoult, S. Jarrix,** “On the effect of amplitude modulated EMI injected on a PLL active filter”, 8th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Dubrovnik, Croatia, 6-9 November 2011.
- [C15] **A. Blain, J. Raoult, A. Doridant, S. Jarrix, T. Dubois,** “ Effects of CW interference on a 5 GHz monolithic VCO” , 8th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Dubrovnik, Croatia, 6-9 November 2011.
- [C16] **A. Doridant, J. Raoult, A. Blain, J. Jarrix, L. Dusseau, N. Chatry, P. Hoffmann, P. Calvel,** “Electromagnetic Susceptibility of low frequency bipolar transistors subject to the total ionizing dose effect”, 8th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Dubrovnik, Croatia, 6-9 November 2011.
- [C17] **A. Doridant, S. Jarrix, J. Raoult, A. Blain, N. Chatry, P. Calvel, P. Hoffmann, L. Dusseau,** “Impact of Total Ionizing Dose on the Electromagnetic Susceptibility of a single bipolar transistor”, Conference on Radiation Effects on Components and Systems (RADECS), 19-23 September 2011, Seville, Spain.
- [C18] **S. Jarrix, A. Blain, A. Doridant, J. Raoult, C. Pouant**  
 «Electromagnetic Study of the Power and Radioboards of a Student Cubesat, ESA Workshop on Aerospace EMC”, 2012, Venise.
- [C19] **A. Blain, J. Raoult, A. Doridant, S. Jarrix**  
 “Effects of CW Interferences on a 5GHz Monolithic VCO, and on its associated PLL”, EUROEM, Toulouse, 2012.
- [C20] **A. Doridant, J. Raoult, S. Jarrix, A. Blain, N. Chatry, P. Calvel, P. Hoffmann, L. Dusseau**  
 “Combined effects of CO<sup>60</sup> Dose and High Frequency Interferences on a Discrete Bipolar Transistors”, Nuclear and Space Radiation Effects Conference (NSREC), Miami, 16-20 Juillet 2012.

- [C21] **R. Omarouyache, J. Raoult, S. Jarrix, L. Chusseau, P. Maurine**  
« Magnetic Microprobe Design for EM Fault Attack », EMC Europe, 2013, Bruges, pp 949-954
- [C22] **J. Raoult, A. Blain, S. Jarrix**  
“An Optimizing Technique to Lower both Phase Noise and Susceptibility of a Voltage-Controlled Oscillator”, 9th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Nara, Japan, 16-18 December 2013.
- [C23] **S. Jarrix, J. Raoult, A. Doridant, C. Clovis, P. Hoffmann**  
“Discrete Low-Frequency Transistors Subjected to High-Frequency CW and Pulse-modulated Sine Signals”, 9th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Nara, Japan, 16-18 December 2013
- [C24] **A. Doridant, J. Raoult, S. Jarrix**  
“Susceptibility of a low frequency bipolar transistor subject to a double aggression: dose irradiation and high frequency CW or pulse modulated signal”, in European Test and Telemetry Conference (ETTC), 11- 13 Juin 2013 Toulouse
- [C25] **L. Chusseau, R. Omarouyache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Boyer, B. Vrignon, J. Shepherd, T. Le, M. Berthier, L. Rivière, B. Robisson, A.L. Ribotta**,  
“Electromagnetic Analysis, Deciphering and Reverse Engineering of Integrated Circuits”, 22<sup>nd</sup> IEEE International Conference on Very Large Scale Integration VLSI-SoC, October 6-8 2014, Playa del Carmen, Mexico.
- [C26] **L. Chusseau, R. Omarouyache, P. Payet, J. Raoult**  
“Millimeter-wave near-field imagery with a bow-tie antenna”, in 8th Terahertz Days Conference, 31 march-2 april 2015 Arêches, France
- [C27] **R. Omarouyache, L. Chusseau, P. Payet, J. Raoult, S. Jarrix**  
“60 GHz Active Microscopy with a Bow-Tie Antenna as Near-Field Probe”, in International Instrumentation and Measurement Technology Conference (I<sup>2</sup>MTC), 11-14 Mai 2015, Pise.
- [C28] **R. Omarouyache, J. Raoult, P. Payet, L. Vrignon, A. Doridant, A. Boyer**  
“Electromagnetic near-field injection model on integrated circuit”, in Progress in Electromagnetic Research Symposium (PIERS), 6-9 July 2015, Prague.
- [C29] **L. Chusseau, R. Omarouyache, P. Payet, J. Raoult**  
“Near-Field imagery with bow-tie antenna probes at 60 GHz”, in Progress in Electromagnetic Research Symposium (PIERS), 6-9 July 2015, Prague.
- [C30] **C. Pouant, J. Raoult, P. Hoffmann**  
“Microwave-Rectification RFI Response in MOSFET Transistors”, in Progress in Electromagnetic Research Symposium (PIERS), 6-9 July 2015, Prague.
- [C31] **J. Raoult, P. Payet, R. Omarouyache, L. Chusseau**  
“Electromagnetic coupling circuit model of a magnetic near-field probe to a microstrip line”, in EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 10-13 November 2015, Edinburgh.
- [C32] **C. Pouant, J. Raoult, P. Hoffmann**  
“Large domain validity of MOSFET Microwave Rectification Response”, in EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 10-13 November 2015, Edinburgh.
- [C33] **A. Doridant, J.J. Laurin, J. Raoult, S. Jarrix, P. Hoffmann**

“Preliminary study of Automatic Control Loop subjected to Pulse-modulated radiofrequency interference”, in EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 10-13 November 2015, Edinburgh.

**[C34] P. Payet, L. Chusseau, J. Raoult**

« A low-cost millimeter-wave phase contrast imaging technique », 41<sup>st</sup> International Conference on Infrared, Millimeter and Terahertz waves (IRMMW), 25-30 september 2016, Copenhagen.

**[C35] L. Chusseau, P. Payet, J. Raoult**

« Millimeter-wave near-field imagery with micrometer spatial resolution », 41<sup>st</sup> International Conference on Infrared, Millimeter and Terahertz waves (IRMMW), 25-30 september 2016, Copenhagen.

**[C36] L. Chusseau, J. Raoult, P. Payet**

“Mm-waves near-field measurements”, in 9<sup>th</sup> Terahertz Days, Dunkerque, 13 june 2017.

**[C37] A. Martorell, J. Raoult, R. Marijon, L. Chusseau**

“ EMI functional vulnerability identification in RF Front-ends”, in EMC Compo 2017, 11<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 4-7 July 2017, St Petersburg.

**[C38] P. Payet, J. Raoult, L. Chusseau**

“Disruption of a RF front-end subject to an out-of-band signal”, in EMC Compo 2017, 11<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 4-7 July 2017, St Petersburg.

**[C39] P. Payet, M. Guery, J. Raoult, L. Chusseau**

“Out-of-band disturbance of mm-wave EMI on RF front-ends”, 28<sup>th</sup> European Symposium on Reliability of Electron Devices, failure physics and analysis (ESREF), 25-28 September 2017, Bordeaux.

**[C40] F. Torrès, C. Pouant, A. Reineix, P. Hoffmann, J. Raoult, L. Chusseau**

« Time-Domain Analysis and Modeling of Large-Signal RFI rectification in MOS transistors », EMC Europe, 27-30 August 2018, Amsterdam.

**[C41] J. Raoult, A. Martorell, L. Chusseau, C. Carel**

“Intermodulation Radar for RF Receiver Detection”, 15<sup>th</sup> European Radar Conference (EuRAD), 26-28 September 2018, Madrid.

c) Conférences invitées

**[CINV1] J. Raoult, C. Delseny, F. Pascal, M. Marin, M.J. Deen**

“Low frequency noise and random telegraph noise in SiGe:C HBT: impact of carbon concentration”, SPIE’s international symposium on fluctuations and noise, noise in devices, circuits and materials, Florence, Italy, may 2007, ISBN 9780819467379.

**[CINV2] J. Raoult**

« Perturbation de composants, circuits, systèmes par injection de signaux d’interférences », Journée thématique : Champ proche pour la CEM des composants et circuits, GDR Ondes (GT5), le 25 Juin 2013, Toulouse.

**[CINV3] J. Raoult**

« Modélisation du couplage magnétique par injection », Journée thématique « Champ Proche : Applications pour la CEM et la sécurité des circuits électroniques », sous l'égide du pôle de compétitivité OPTITEC et le GDR Ondes, 19 juin 2015 à Toulouse.

**[CINV4] J. Raoult**

« Injection électromagnétique en champ proche – Modélisation du couplage magnétique », Assemblée générale du GDR Ondes « Interférence d'Ondes », 19-21 octobre 2015 à Lyon

d) Conférences nationales

**[CN1] J. Raoult, L. Militaru, J. Verdier, A. Souifi, M. Mouis**

« Etude des transistors bipolaires à hétérojonction Si/SiGe submicroniques par bruit RTS », Congrès SFP Strasbourg 2001, 9-13 juillet.

**[CN2] J. Verdier, J. Raoult, C. Gontrand**

« Conception et optimisation d'un oscillateur contrôlé en tension à base de TBH SiGe fonctionnant à 5 GHz », 5<sup>ème</sup> journée d'étude faible tension faible consommation, 18-19 mai 2005, Paris.

**[CN3] P. Benoit, J. Raoult, C. Delseny, F. Pascal, J.C. Vildeuil, A. Mauroy, M. Laurens**

« Etude de la dispersion du bruit basse fréquence dans les transistors bipolaires à hétérojonction Si/SiGe », JNMO06, 4-7 avril 2006, Aussois.

**[CN4] F. Pascal, J. Raoult, M. Marin**

« Etude du bruit basse fréquence dans les TBH Si/SiGeC (noeud 0.13µm) à émetteur métallique », JNMO 08, 3-6 juin 2008, Ile d'Oleron.

**[CN5] A. Blain, A. Doridant, T. Dubois, J. Raoult, S. Jarrix**, « Impact d'une onde d'agression rayonnée sur un oscillateur contrôlé en tension en fonction du design de routage », GDR Ondes GT2 : Micro, nano-structures et dispositifs de l'optique aux micro-ondes, Lille, 11-12 mai 2010.

**[CN6] A. Blain, D. Pantel, A. Doridant, J. Raoult, F. Wrobel, S. Jarrix**, « Caractérisation électromagnétique d'une diode perturbée par des convertisseurs lors d'une campagne de mesures en ballon », Club Opto-Hyper, Toulouse, 2010.

**[CN7] A. Doridant, A. Blain, J. Raoult, L. Dusseau, S. Jarrix**, « Susceptibilité électromagnétique en champ proche de transistors bipolaires discrets : étape vers une méthode d'étude des effets combinés dose – compatibilité électromagnétique », Club Opto-Hyper, Toulouse, 2010.

**[CN8] R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, L. Chusseau**, « Sondes de champ proche pour l'injection de fautes », GDR Ondes Journée thématique du GT2 et GT5 : Antennes et interaction champ proche, mars 2011, Paris.

**[CN9] R. Omarouayache, J. Raoult, P. Payet, L. Chusseau, B. Vrignon, J. Shepherd, A. Boyer**  
« Modèle d'injection électromagnétique en champ proche sur circuit intégré, XIXème Journées Nationales Microondes (JNM), 2-5 Juin 2015, Bordeaux.

**[CN10] R. Omarouayache, L. Chusseau, P. Payet, J. Raoult**

« Réflectométrie champ proche à 60 GHz », XIXème Journées Nationales Microondes (JNM), 2-5 Juin 2015, Bordeaux.

**[CN11] C. Pouant, J. Raoult, P. Hoffmann**

« Etude de la susceptibilité électromagnétique d'un transistor MOSFET », Assemblée générale du GDR Ondes « Interférence d'Ondes », 19-21 octobre 2015, Lyon.

[CN12] **P. Payet, L. Chusseau, J. Raoult**

« Imagerie en onde millimétrique avec un guide d'onde rectangulaire », JNRDM, Toulouse, 11-13 mai 2016.

[CN13] **P. Payet, A. Martorell, J. Raoult, L. Chusseau**

“Susceptibilité d'un récepteur RF à un signal hors bande de faible puissance”, XXème Journées Nationales Microondes (JNM), 16-19 mai 2017, St Malo.

[CN14] **J. Raoult, P. Payet, Z. Fella Touta, L. Chusseau**

“Injection électromagnétique en champ proche sur circuit intégré », XXème Journées Nationales Microondes (JNM), 16-19 mai 2017, St Malo.

[CN15] **A. Martorell, J. Raoult, C. Carel, L. Chusseau**

“Conception d'un radar non-linéaire à intermodulation pour la détection de récepteurs RF”, Journées Electromagnétisme et guerre électronique (EMGE), 22-23 novembre 2017, Toulouse.

[CN16] **C. Pouant, F. Torrès, A. Reineix, P. Hoffmann, J. Raoult, L. Chusseau**

« Analyse et modélisation du redressement RF fort signal dans les transistors MOS », 19<sup>ème</sup> colloque international et exposition sur la compatibilité électromagnétique (CEM2018), 9-11 juillet 2018, Paris.

#### e) Rapports

[M1] **J. Raoult**

« Etude et caractérisation de transistors bipolaires à hétérojonction Si/SiGe en vue de leur modélisation électrique »  
Stage de DEA, INSA de Lyon, soutenu le 15 septembre 2000.

[M2] **J. Raoult**

« Etude et modélisation de transistors bipolaires à hétérojonction Si/SiGe, application à la conception d'oscillateurs radiofréquences intégrés »  
Thèse, INSA de Lyon, soutenue le 16 décembre 2003.

#### f) Rapports d'étude

[RE1] Etude pour le PEA DGA obtenu par le LIRMM: « Champ magnétique d'une sonde boucle en champ proche », **R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, Ph. Maurine**, juillet 2012.

✓ Programme de recherche national ANR 12-INSE-0005, projet E-MATA-HARI

[RE2] Rapport à mi-parcours, workpackage 2 : « Modélisation du couplage avec sonde ferrite », **J. Raoult, L. Chusseau**.

[RE3] Rapport final, workpackage 1 et 2: “Conception et simulation de sonde de champ proche optimisée, et modélisation du couplage sonde/circuit intégré”, **L. Chusseau, J. Raoult**

✓ Contrat avec Thalès Communications & Security n°128934 et n°133190 :

- [RE4] Etude bibliographique : « Réponse de systèmes électroniques à une sollicitation radiofréquence », **A. Martorell et J. Raoult**, octobre 2015.
- [RE5] Compte rendu semestriel n°1 : « Etude numérique d'un émetteur-récepteur RF à l'aide d'un logiciel de simulation type SPICE », **A. Martorell et J. Raoult**, mars 2016.
- [RE6] Compte rendu semestriel n°2 « Analyse des non-linéarités sur des cibles RF opérationnelles & protocole de détection », **A. Martorell et J. Raoult**, septembre 2016.
- [RE7] Compte rendu semestriel n°3 « Détection de récepteurs RF par la raie d'intermodulation d'ordre 3 », **A. Martorell et J. Raoult**, mars 2017.
- [RE8] Compte rendu semestriel n°4 « Développement du RADAR non-linéaire & expérimentation », **A. Martorell et J. Raoult**, septembre 2017.
- [RE9] Compte rendu semestriel n°5 « Intermodulation Radar for RF Receiver Detections », **A. Martorell et J. Raoult**, février 2018.

### Bilan scientifique

Depuis le début de ma thèse (2000), mes travaux de recherche ont fait l'objet de :

- 17 articles dans des revues internationales
- 41 communications dans des conférences internationales
- 4 communications dans des conférences données à l'invitation du comité d'organisation dans un congrès national ou international
- 16 communications dans des conférences nationales
- 2 récompenses (prix régional et national de la SEE, André Blanc-Lapierre en 2014)

Et m'ont permis de contribuer aux encadrements suivants :

- 2 stages post-doctoral d'un an
- 8 thèses
- 8 stages Master 2 et Ingénieur

dans le cadre des collaborations et actions suivantes :

- 2 programmes de recherche nationaux :
  - RNRT « ARGOS », janvier 1999 – décembre 2001
  - ANR Ingénierie numérique et sécurité « E MATA-HARI » dont l'IES est le coordinateur, octobre 2012 – décembre 2015.
- Collaborations industrielles :
  - o 1 contrat de recherche avec ST Microelectronics, octobre 2002-octobre 2005.

- 1 contrat de recherche conclu entre la société Thalès Communications & Security, l'ANRT et l'IES, dont je suis le responsable scientifique, septembre 2015 – septembre 2018.
- Collaborations avec le CEA
  - 2 contrats de recherche avec le laboratoire CEG du CEA à Gramat, janvier 2010-janvier 2013, et octobre 2012-octobre 2015.

## 5) Activités d'enseignement

Avant de présenter mes activités d'enseignement de manière factuelle, je souhaiterais exprimer mon réel plaisir à enseigner. A la fin de mes études d'ingénieur, j'ai voulu m'engager vers une thèse dans l'idée de découvrir le monde de la recherche, mais j'ai été également très attiré par l'enseignement. J'ai d'ailleurs avant le début de la thèse souhaité m'engager vers une mission de moniteur, me permettant d'assurer une charge d'enseignement fixe chaque année. Cette expérience de moniteur exercée à l'INSA de Lyon m'a vraiment plu, en particulier le contact avec les étudiants. Très tôt j'ai su qu'à l'issue de la thèse je souhaiterais me diriger vers une carrière d'enseignant-chercheur, et ainsi pouvoir m'investir dans la formation des étudiants. Aujourd'hui ce plaisir reste intact, et je reste persuadé qu'il faille porter un effort important sur la pédagogie dans les enseignements proposés. Cette approche me semble réellement judicieuse en vue d'intéresser les étudiants et ainsi leur fournir une formation qui leur sera utile et dans laquelle ils pourront s'épanouir. Ceci reste également vrai selon moi dans les activités de recherche au niveau de l'encadrement des stagiaires et des doctorants. Avoir le sens de l'écoute et participer activement à leurs travaux me semble être nécessaire afin de créer une bonne dynamique de groupe et de faire avancer les sujets.

A présent je vais présenter de manière factuelle les niveaux d'études sur lesquels je suis intervenu ou j'interviens toujours, les matières que j'enseigne et enfin les responsabilités passées ou en cours.

### - Niveaux d'étude concernés :

Actuellement mes interventions se portent davantage au niveau des filières technologiques. Cependant j'ai aussi voulu et eu l'opportunité d'enseigner à un niveau master :

- ✓ Ecole d'ingénieur : INSA de Lyon, de la 1<sup>ère</sup> à la 5<sup>ème</sup> année
- ✓ IUT Montpellier, 1<sup>ère</sup>, 2<sup>ème</sup> année et année spéciale
- ✓ Licence Professionnelle :
  - Chargé d'affaires en ingénierie électrique et électronique (CAIEE)
  - Mécatronique (MECATRO)
- ✓ Master 2 : université de Montpellier, spécialité composants, énergie et fiabilité

- Matières enseignées

Le cœur de l'enseignement effectué à l'IUT porte sur 3 disciplines : de l'EEA (électronique, électrotechnique et automatique), de la physique (électromagnétisme), et des télécommunications (filaire et hertzienne).

L'enseignement de l'EEA constitue le volume horaire annuel le plus important de mon service statutaire. Je suis responsable (cours/TD) des modules d'électronique analogique de base, traitant des composants et circuits intégrés et de leur utilisation les plus classiques. Cet enseignement s'appuie fortement sur des travaux pratiques, dont j'ai pris la responsabilité pour la 1<sup>ère</sup> année, et dont j'assure actuellement celle des étudiants de 2<sup>ème</sup> année. Ces TP couvre un large spectre de disciplines : électronique, automatique, électronique de puissance, énergie renouvelable, télécommunications et enfin hyperfréquence.

J'assure également un enseignement de physique, plus particulièrement orienté vers la compatibilité électromagnétique et l'intégrité du signal, ces problématiques devenant fondamentales dans les métiers du génie électrique, avec notamment l'essor d'une électronique de plus en plus embarquée et intégrée. Je souhaite continuer à développer cet enseignement, qui est d'ailleurs proche de mes activités de recherche, favorisant ainsi des échanges interactifs avec les étudiants. J'interviens également dans deux licences professionnelles du département, dans des versions plus détaillées et adaptées aux besoins de la formation.

Et enfin la dernière discipline dans laquelle j'interviens concerne un enseignement de télécommunications, au niveau matériel. Il est surtout orienté vers les communications filaires et hertziennes (antennes, et premiers étages d'émission et de réception).

- Responsabilités au sein du département

✓ TP EEA 1<sup>ère</sup> année IUT , de 2007 à 2011

✓ TP EEA 2<sup>ème</sup> année IUT, depuis 2014. En plus de ma fonction de responsable « administratif » je m'implique dans l'amélioration pédagogique des textes de TP et dans la réalisation de nouvelles maquettes, en bonne collaboration avec les collègues agrégés du département.

✓ Responsable de la formation année spéciale « DUT en 1 an », de 2011 à 2014.

Mon rôle a commencé par la sélection des étudiants (avec un niveau Bac+2), s'est poursuivi par l'organisation de l'année (emploi du temps, logistique, jurys) et s'est terminé par la rédaction des avis de poursuite d'études.

Un bilan récapitulatif de mes enseignements, depuis mes premières missions, est donné dans le tableau ci-dessous :

<u>Année et Lieu</u>	<u>Fonction</u>	<u>Niveau</u>	<u>Matières enseignées</u>	<u>Volume horaire par an</u>
De 2000 à 2004, INSA	Moniteur  ATER	1 <sup>ère</sup> année  3, 4, 5 <sup>ème</sup> année	- Mesures Physiques  - Propagation filaire et optique  - Antennes	64  80  16
Depuis 2004  IUT	Enseignant - chercheur	1 <sup>ère</sup> , 2 <sup>ème</sup> année, et année spéciale	- Electronique analogique  - Compatibilité Electromagnétique  - Télécommunications	200  21  45
De 2006 à 2011, UFR	Enseignant - chercheur	Master 2	Fiabilité des composants à semi-conducteurs	15
Depuis 2010  IUT	Enseignant - chercheur	Licence professionnelle CAIEE	Compatibilité électromagnétique	15
Depuis 2014  IUT	Enseignant - chercheur	Licence professionnelle MECATRO	Compatibilité électromagnétique	21



## Partie II

### Synthèse des activités de recherche



## Introduction

Dans l'introduction de ce mémoire je vais scinder de manière chronologique mes activités de recherche en deux périodes. La première commence avec mes travaux de thèse (2000-2003), se poursuit lors de mes premières activités à l'IES et se termine à mon changement d'équipe et de thématique (courant 2009). La seconde concerne mes activités actuelles (2009 et après...). La première période sera exposée ici dans les pages d'introduction de manière synthétique. La seconde période sera développée dans le corps du mémoire, en détaillant les activités en cours, les méthodes mises en œuvre, les résultats marquants, et les perspectives envisagées.

### **Période 2000-2009 :**

De 2000 à 2004, période du stage Master 2, de la thèse et du poste d'attaché temporaire d'enseignement et de recherche, j'ai travaillé au sein du laboratoire LPM (actuellement l'INL) à l'INSA de Lyon, CNRS UMR5511 dans l'équipe « Micro et nanoélectronique sur Silicium ». Mon travail s'inscrivait dans le cadre du démarrage d'une nouvelle activité de recherche au laboratoire axée sur les composants actifs et circuits radiofréquences intégrés sur Silicium. J'étais seul avec mon encadrant de thèse, Jacques Verdier, en charge du développement de cette activité RF. J'ai largement participé à la définition des besoins en matière de moyens de caractérisation et de simulation ainsi que les expertises scientifiques à acquérir en priorité. A mon arrivée le LPM était impliqué dans le projet RNRT ARGOS (ARchitecture et composants pour OScillateurs en bande Ka) dont le principal objectif était d'évaluer les performances de la filière technologique bipolaire à hétérojonction SiGe dans la réalisation d'oscillateurs intégrés, aux fréquences micro-ondes, et à très faible bruit de phase. L'implication du laboratoire dans ce projet était de faire des mesures de bruit basse-fréquence, auxquelles j'ai participé durant mon stage Master 2 et le début de ma thèse. J'ai aussi pu grâce au projet me rapprocher du CNET de Meylan et finalement orienter mes travaux plus spécifiquement vers la conception d'oscillateurs intégrés sur Silicium et l'optimisation du bruit de phase. J'ai en particulier fortement travaillé sur les mécanismes de conversion non-linéaire du bruit basse fréquence en bruit de phase et par conséquent sur la modélisation fort-signal de composants avancés.

Plusieurs thèmes de recherche ont ainsi été abordés:

- **Mesure du bruit basse fréquence des transistors bipolaires à hétérojonction**
- **Modélisation compacte non-linéaire et non quasi-statique des transistors**
- **Optimisation du bruit de phase dans la conception d'oscillateur intégré en technologie BiCMOS 0.35 $\mu$ m, fonctionnant à 5GHz.**

Le bilan des publications scientifiques est présenté ci-dessous :

#### ***Bilan (2000-2004)***

Publications

2	articles dans des revues internationales	[R1] et [R2]
3	communications internationales	[C1] à [C3]
2	communications nationales	[CN1] et [CN2]

A partir de 2004, grâce notamment aux compétences acquises au niveau de la métrologie du bruit basse-fréquence sur transistors, j’obtiens un poste d’enseignant-chercheur au sein de l’IES (université Montpellier, CNRS UMR 5214), dans l’équipe BOM « Bruit opto et microélectronique », dans laquelle je travaille avec Fabien PASCAL et Colette DELSENY. Cette équipe a une expérience reconnue dans la métrologie du bruit basse-fréquence de composants intégrés avancés (transistor bipolaires et à effet de champ). Elle entretient depuis de longue date des relations privilégiées avec le fondeur ST Microelectronics, lui permettant d’avoir accès aux composants les plus avancés tout en bénéficiant d’un échange direct avec les technologues. Une convention de recherche CIFRE était en cours à mon arrivée. Le principal objectif de cette collaboration est d’évaluer les performances en bruit basse-fréquence des filières technologiques à base de transistors bipolaires à hétérojonction (TBH) SiGe :C. La société cherche à développer à la fois des technologies de plus en plus avancées pour des applications vers les très hautes fréquences (millimétrique et térahertz) et aussi des filières « low-cost » pour des applications de téléphonie sans fil grand public. Le bruit basse-fréquence étant un indicateur de maturité d’une technologie, il est très utile aux fondeurs pour améliorer les étapes de process des composants. L’expertise de l’équipe BOM concerne la mesure et l’analyse physique des sources de bruit présentes dans les transistors. La problématique forte est de déterminer l’origine et la localisation physique au sein de la structure des défauts responsables des niveaux de bruit mesurés.

Durant les 5 années passées dans ce groupe de recherche j’ai abordé les principaux thèmes suivants :

- **Mesure des différents types de bruit basse-fréquence sur les technologies TBH les plus avancées, et analyse de l’origine et la localisation physique des défauts responsable du bruit en excès dans les composants**

De manière générale mes travaux ont consisté à identifier les paramètres technologiques qui dégradent le niveau de bruit en excès. Il fallait ici en particulier évaluer l’influence du carbone sur le bruit « en excès » (RTS,  $1/f$ ) des TBH avancées. A partir du nœud technologique  $0.25\mu\text{m}$  le carbone est utilisé dans la base des TBH afin de limiter la diffusion du dopant et ainsi réduire sa taille géométrique et donc augmenter le gain et la fréquence de transition du composant. Une forte présence de bruit RTS (Random Telegraph Signal) a été observée et corrélée aux défauts structurels induits par l’implantation du carbone [R4]. Les sources de bruit RTS ont pu être localisées et les processus de capture (électrons, trous) ont été étudiés selon la température et la polarisation. Le fondeur a pu ajuster la concentration en carbone et ainsi garantir un bon compromis gain, fréquence de transition et niveau de bruit.

L’utilisation d’émetteur monocristallin et métallique à la place d’un polycristallin classique a pu être évaluée et une réduction du bruit en  $1/f$  a été mise en évidence [C8], [C9].

- **Utilisation de la caractérisation en bruit pour l'analyse de la dégradation par porteurs chaud des TBH de technologie les plus avancés.**

Il s'agissait ici d'évaluer la dégradation de ces TBHs très avancés (0.25µm et 0.13µm) sous stress électrique par porteurs chauds, selon la présence d'une couche superficielle de dopage dans la base. Une approche originale a consisté à utiliser la mesure de bruit en complément avec une caractérisation statique plus classique [R3]. La mesure de bruit étant plus sensible que la mesure DC, l'évaluation d'une meilleure tenue à un stress électrique selon les paramètres technologiques d'un transistor a été facilitée. J'ai pris en charge cette étude de stress électrique, en particulier dans le cadre du stage Master de Lionel Snadgy.

- **Mise en place d'un banc de caractérisation en température du bruit, directement sur wafer**

J'ai été responsable de la mise en place d'un banc de test destiné à la caractérisation en température (-40°C ,+100°C) du niveau de bruit directement sur le wafer. L'idée était d'élargir les moyens de test disponibles au laboratoire pour une caractérisation fine du bruit des composants. Ce banc de test a répondu principalement à une demande industrielle, qui était de mesurer l'évolution avec la température du niveau de bruit en excès des TBH. L'évolution en température du bruit en excès n'était pas mesurée de manière fine, et directement sur le wafer. Habituellement une caractérisation en température nécessite un découpage des wafers et une mise en boîtier du composant. Ici, un système de refroidissement et de chauffage est directement intégré à la station sous pointe, laquelle doit être incorporée dans une boîte à gants dans lequel un vide d'air est nécessaire pour éviter la condensation sur le wafer. Ce nouveau savoir-faire a contribué à la participation de l'équipe au projet européen CATRENE.

***Bilan (2004-2009)***

Publications

3 articles dans des revues internationales	[R3] à [R5]
6 communications internationales	[C4] à [C9]
1 communication internationale invité	[CINV1]
2 communications nationales	[CN3] et [CN4]

Partenariat industriel

1 contrat de recherche avec ST Microelectronics

Encadrement

1	thèse, soutenue en 2005	[Th1]
1	stage master 2	[Stage1]

### **Période 2009-...**

À partir de 2009, j'intègre l'équipe RADIAC « RADIAtion et Composants » de l'IES, spécialisée dans l'étude de la fiabilité de l'électronique dans les environnements radiatifs. L'équipe souhaite développer un nouvel axe de recherche sur le thème de la susceptibilité électromagnétique des composants et des circuits. La problématique abordée m'a immédiatement intéressé et avait des liens directs avec les travaux développés durant ma thèse, en particulier au niveau des effets liés aux non-linéarités intrinsèques des composants.

À mon arrivée cette activité était portée par Sylvie Jarrix, enseignante-chercheuse à l'IES. Une thèse était en cours, réalisée par Tristan Dubois et financée par la Direction Générale de l'Armement (DGA), qui visait à étudier les effets d'une onde électromagnétique sur un composant commercial haute fréquence (diode Schottky) et sur une boucle à verrouillage de phase fonctionnant aux fréquences radio. J'ai rencontré Tristan Dubois et je lui ai communiqué mon intérêt scientifique à m'impliquer dans son travail, ayant déjà travaillé sur des oscillateurs. Ceci a été le point de départ de mon intégration dans l'équipe et une réorientation de mes activités de recherche.

Le cœur des travaux présenté dans ce manuscrit porte sur cette nouvelle thématique au laboratoire. Le but de la démarche proposée est de présenter les actions que j'ai portées et auxquelles j'ai participé depuis 2009, et ainsi de mettre en avant ma capacité à développer la visibilité et la pérennité de cette activité. Pour ce faire, j'ai travaillé avec plusieurs étudiants (stages master, thèses et post-doctorat), et avec deux collègues de l'IES, Sylvie Jarrix de 2009 à 2014, et Laurent Chusseau à partir de 2013.

Ce manuscrit est composé de cinq parties, ce qui permettra aux lecteurs d'avoir une vision plus claire et synthétique de mon apport sur les différents sujets abordés depuis 9 ans. Les quatre premières parties traitent des activités passées et en cours durant la période considérée, la dernière présente les projets et perspectives envisagées pour les années futures.

Sur cette période, mon activité de recherche s'est construite autour de quatre thèmes :

- **la perturbation de l'électronique par injection de signaux,**
- **la détection d'électronique à distance,**
- **l'imagerie et la microscopie millimétrique en champ proche,**
- **les effets de synergie dans la réponse de l'électronique soumise aux contraintes radiative et électromagnétique.**

Le synoptique présenté ci-dessous montre les quatre thèmes abordés ainsi que les thèses, les stages post-doctoral et les collaborations établies.

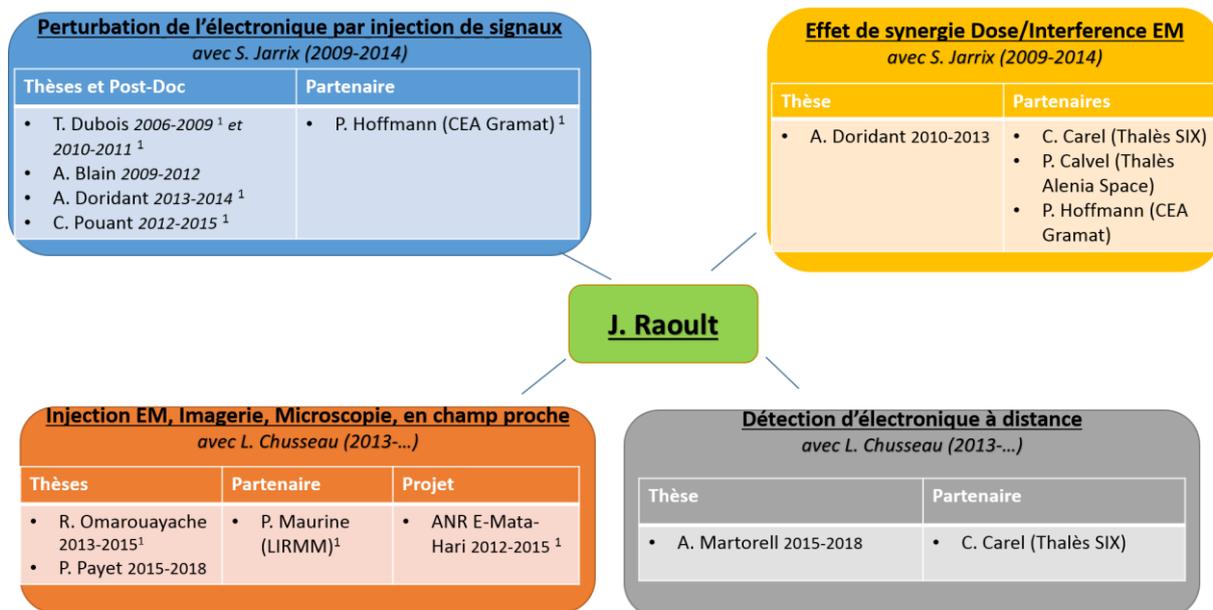


Fig. 1: Synoptique des activités de recherche développées depuis 2009

***Bilan (2009-...)***

Publications

- 12 articles dans des revues internationales [R6] à [R17]
- 31 communications internationales [C11] à [C41]
- 3 communications invité [CINV2] à [CINV4]
- 12 communications nationales [CN5] et [CN16]

Participation à 1 programme de recherche national (ANR)

Partenariat industriel

- 1 contrat de recherche avec Thalès Communication & Security
- 2 contrats de recherche avec le CEA Gramat

Encadrement

- 7 thèses [Th2] à [Th8]
- 7 stages master 2 [Stage2] à [Stage8]

## Chapitre 1. Perturbation de l'électronique par injection de signaux

Cette activité est la première sur laquelle je me suis engagé, dès mon arrivée dans l'équipe. J'ai participé activement, en collaboration ou seul, à l'encadrement de quatre thèses, de deux stages Master et de deux stages post-doctoral réalisés sur cette thématique.

Tous ces travaux traitent de la susceptibilité des composants électroniques actifs aux interférences EM. L'immunité de l'électronique a toujours été un problème majeur, d'autant plus que les progrès de la microélectronique conduisent à une augmentation de la densité d'intégration des composants, de la fréquence de fonctionnement des transistors et à une diminution des marges de bruit [1,2]. Cette proximité entre les circuits intégrés et leur montée en fréquence de fonctionnement favorisent les couplages EM au sein des cartes électroniques, induisant un signal susceptible de se propager à travers les systèmes. En outre, ces derniers baignent dans un environnement EM extérieur saturé d'ondes radio en raison d'une utilisation massive de systèmes communicants à distance. Cette énergie RF peut conduire à un dysfonctionnement du circuit.

Dans la littérature, les premières études des effets des interférences RF ont été menées, au niveau composant, sur des transistors discrets. Elles ont mis en évidence un mécanisme de base expliquant la perturbation d'un composant par un signal interférant RF. A cause de la non-linéarité de la caractéristique de transfert courant-tension du transistor, une excitation RF induit une distorsion du courant de sortie, menant entre autres à une variation du point de polarisation [3-5]. Le mécanisme de redressement explique cette modification de la valeur moyenne du courant. Ces premiers travaux précurseurs ont mis les non-linéarités au cœur de la problématique de la vulnérabilité d'un circuit électronique. Une compréhension des phénomènes passe donc forcément par une prise en compte des non-linéarités.

Finalement l'effet qui en résulte sur la fonction attendue que doit fournir l'électronique est divers et peut aller d'un faible dysfonctionnement à un dommage permanent [6, 7], y compris un redémarrage logique ou une réduction de la durée de vie de l'installation [8].

En plus du risque sur l'électronique dû aux interférences dites non-intentionnelles, les armes électromagnétiques [9], comme les microondes à bande étroite et à fortes puissance (HPM) [10] ou les rayonnements ultra-larges bandes [11], sont de plus en plus utilisées sur les théâtres d'opération et sont considérées comme de réelles menaces. Ces sources sont usuellement classées selon le niveau de puissance délivré et la bande de fréquence couverte. Dans la classification proposée par Giri [9], une source ultra large bande peut couvrir une bande passante de 1 GHz. Il a été montré que des interférences intentionnelles intenses dans la bande 100 MHz – 5GHz ont causé des perturbations et des dysfonctionnements sévères sur des circuits analogiques ou numériques [12, 13]. Des sources à champ rayonné à haute intensité produite par des faisceaux d'électrons atteignent même des fréquences de fonctionnement de 100 GHz [14]. La figure 1.2 illustre une situation où un signal de forte puissance est installé dans un véhicule et placé au milieu d'une ville. La grande différence par rapport au cas plus

classique des interférences non-intentionnelles est sur le niveau de puissance délivré par la source qui permet, même à des distances élevées, de transférer beaucoup plus de puissance sur une cible. Deux types de couplage sont possibles au niveau des équipements visés [15].

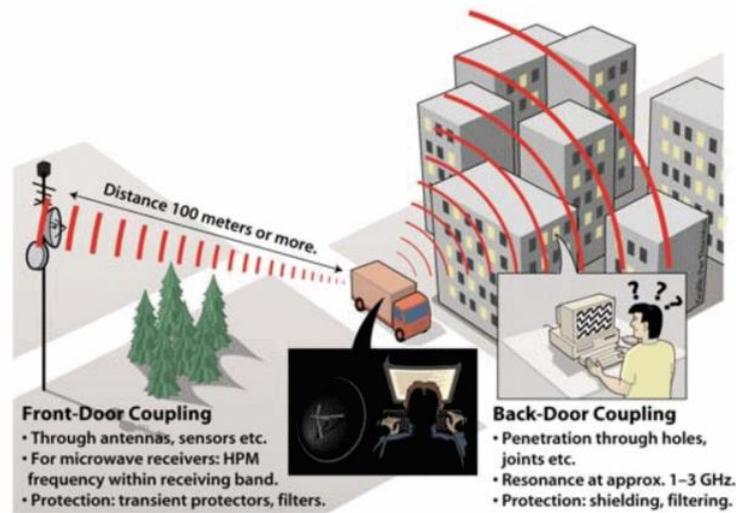


Fig. 1.2: Illustration du couplage front-door et du couplage back-door

Le couplage front-door se produit sur les antennes des ports de communication, induisant la pénétration d'un signal de forte puissance directement sur l'étage d'émission-réception de l'équipement. Toute la chaîne de communication radio-fréquence ou microonde, donc les fonctions analogiques RF, peuvent être impactées [16, 17]. L'efficacité de ce mode de couplage est optimale si la fréquence du signal agresseur se situe dans la bande de réception du système.

L'autre mode de couplage est le couplage back-door qui se produit sur les pistes, les câbles de l'équipement, à travers les ouvertures du blindage. Le niveau de signal résultant est souvent plus faible que dans le cas du couplage front-door, mais il peut engendrer des dysfonctionnements sur des circuits de contrôle-commande ou de traitement de l'information, donc en particulier pour des applications numériques ou analogiques. Même avec un blindage de protection d'efficacité 30 dB, il a été montré [16] que l'amplitude d'une interférence EM intentionnelle couplée sur un circuit imprimé peut être suffisamment élevée pour générer des défauts temporaires ou permanents. Pour de forts champs électriques incidents (plus de 100 V/m au niveau de l'équipement), le couplage back-door peut induire des signaux parasites de plusieurs centaines de Volt [12, 18, 19]. Cette fois la fonction électronique cible est la cellule inverseuse.

Pour évaluer la susceptibilité de l'électronique, il a donc été nécessaire de concevoir des expériences d'injection. Au-delà de cette phase de tests, nous avons voulu analyser les mécanismes de défaillance induits. La compréhension des mécanismes induits par des signaux interférents potentiellement de forte puissance et bande large, ont nécessité la mise en place des étapes de modélisation fort-signal et haute fréquence des composants. Cette activité m'a particulièrement motivé ayant déjà été confronté durant mes travaux de thèse à ce type de modélisation sur des technologies avancées de transistor. Ces

techniques d'injection et l'analyse associée trouvent leurs applications essentiellement dans le domaine de la défense et de la sécurité. La DGA puis le CEA Gramat et plus particulièrement l'équipe de Patrick Hoffmann ont été d'ailleurs nos principaux collaborateurs sur ce sujet.

Leur intérêt consiste à la fois à élargir la base de données des défaillances observées sur une large palette de circuits, mais aussi et surtout d'acquérir de la compréhension dans l'origine physique des susceptibilités aux signaux de forte puissance sur des « briques de base ». Tout l'équipement n'étant pas forcément susceptible à l'agression, certaines fonctions électroniques critiques fixent la vulnérabilité EM de l'équipement entier, d'où un intérêt à identifier les fonctions les plus vulnérantes.

La plupart des thèses et la totalité des post-docs ont été financées par le CEA dans le cadre de cette collaboration. Les études menées se sont concentrées sur les réponses sous agression EM de composants et de fonctions électroniques connues pour être des cibles potentielles dans un contexte de couplage front-door et back-door de signaux type HPM.

Des composants discrets fonctionnant en HF et en BF, avec des fréquences de transition  $f_T$  plus faibles que les fréquences injectées, ont été testés. Les premiers tests d'injection ont été menés lors de la thèse de Tristan Dubois sur un dispositif actif élémentaire, une diode Schottky HF fonctionnant jusqu'à quelques GHz. L'injection dans la bande de fréquence du dispositif a permis d'appréhender plus directement le mécanisme de redressement sur les caractéristiques statiques du composant [20].

Les tests puis l'analyse des effets forts-signaux se sont poursuivis dans les thèses d'Adrien Doridant et de Clovis Pouant sur des transistors cette fois BF, de technologie Bipolaire et MOSFET respectivement. Ces composants sont évidemment utilisés pour des applications analogiques et numériques, et aussi comme dispositifs de protection sur les étages d'entrée de circuits intégrés [21]. Les effets observés étaient fortement dépendantes de la fréquence du signal injecté et donc du régime de fonctionnement du composant [22, 23].

Au niveau des fonctions électroniques, la majorité des travaux s'est focalisée sur des systèmes asservis, testant ainsi entre autres la capacité de l'asservissement à résister à la présence d'un signal d'interférence. Une partie de la thèse et le post-doc de Tristan Dubois a consisté à étudier la réponse, d'oscillateurs contrôlés en tension HF et la boucle à verrouillage de phase associée, à des signaux de fréquence et de puissance variables [24-25]. Ces premiers travaux ont essentiellement été expérimentaux et ont été menés sur des composants commerciaux.

Ils ont été poursuivis dans la thèse d'Amable Blain sur ce même type de fonction, mais cette fois avec des circuits plus intégrés, de conception et de technologie connues. Ceci a été d'une grande aide pour mener les phases d'analyse et de modélisation des effets observés [26].

La dernière étude sur des circuits asservis a été réalisée durant le stage post-doctoral d'Adrien Doridant et a concerné un contrôle automatique de gain HF, couramment utilisé dans les récepteurs de communications sans fil, afin de maintenir constant le gain de l'amplificateur bas-bruit de la chaîne [27]. Les résultats ont montré la possibilité de mettre en défaut ces circuits asservis dans et en dehors de leur bande de fonctionnement.

Je vais dans la suite exposer de manière synthétique la démarche et les méthodes mises en place pour étudier la réponse des véhicules de test à un signal EM, et présenter les résultats les plus marquants.

### *1) Mise en évidence de susceptibilités au niveau composant*

#### **a) Méthodologie de test**

Le test au niveau composant est nécessaire pour mettre en lumière et analyser les mécanismes de perturbation de base. Être capable d'analyser ces mécanismes signifie une connaissance du ou des chemins pris par le signal d'agression au sein de la structure testée.

Dans la littérature, les travaux considèrent le composant sous test souvent comme une « boîte noire ». L'approche utilisée pour décrire les défaillances est surtout basée sur des caractérisations fonctionnelles, qui consistent exclusivement à mesurer des tensions à l'entrée et la sortie du composant [21]. Notre approche cherche davantage à décrire les effets observés avec un positionnement davantage axé sur la physique du composant. Nous avons ainsi voulu décrire au sein des transistors les variations de charges imposées par le signal agresseur de puissance pouvant être élevée. Une méthodologie basée sur la mesure des courants instantanés aux accès du transistor est par conséquent développée. Les formes d'onde des courants et des tensions à tous les accès du transistor ont ainsi permis d'observer la distorsion globale induite par l'interférence. Cette manière d'évaluer les susceptibilités, peu courante dans la communauté CEM, se rapproche de la démarche utilisée par les personnes qui cherchent à développer le modèle fort-signal de composants, où la physique du composant est nécessairement prise en compte.

J'ai initié et développé ces méthodes de travail au sein de l'équipe en m'appuyant sur les compétences acquises à la fois durant ma thèse au niveau de la caractérisation non-linéaire de composants, et dans l'équipe BOM au niveau de la physique et de la technologie des composants.

Les premiers tests menés durant les thèses de Tristan Dubois et d'Adrien Doridant se sont concentrés sur la mesure des valeurs moyennes des courants et tensions aux accès des composants. Puis plus récemment lors de la thèse de Clovis Pouant, nous avons voulu caractériser de manière globale la distorsion induite par l'agression et donc mesurer les courants et tensions instantanés à tous les accès d'un transistor NMOS. Dans cette partie je ne présente que les résultats expérimentaux de cette dernière thèse.

#### **b) Bancs de test mis en place et principaux résultats**

Le premier banc réalisé consiste à mesurer la réponse DC d'un composant à une excitation. Les fréquences porteuses classiquement utilisées dans les attaques EM type HPM s'étalent de 100 MHz à quelques GHz [9]. Lors de nos tests, les mesures ont été réalisées jusqu'à 1 GHz. Les transistors sous test choisis sont tous dédiés à des applications à plutôt moyenne fréquence. Dans la thèse d'Adrien Doridant, ce sont des transistors bipolaires très classiques (type 2N2222), à usage général, avec une

fréquence de transition de 100MHz. Dans la thèse de Clovis Pouant, les transistors NMOS sélectionnés sont plutôt utilisés en commutation, avec une fréquence de transition de 200 MHz. L'intérêt principal de ces mesures est d'observer la réponse de composants dont la fréquence de fonctionnement est inférieure aux fréquences de l'excitation. La figure 1.3 présente une configuration de test pour laquelle le signal est injecté en conduit sur l'entrée du composant.

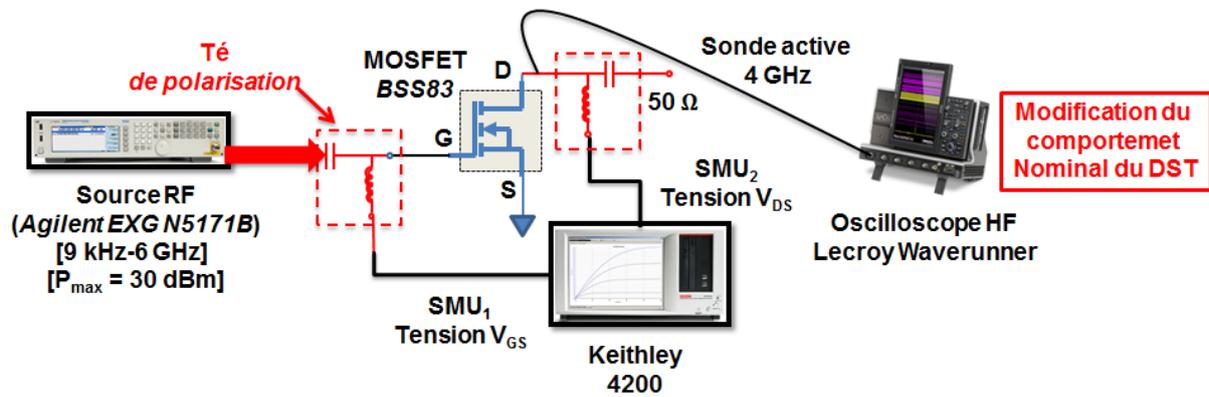


Fig. 1.3: Schéma du banc de test développé pour mesurer l'effet d'un signal RF sur les caractéristiques statiques d'un transistor

Le dispositif sous test en boîtier CMS a été monté sur un circuit imprimé avec un substrat hyperfréquence. Nous avons mené également des tests sur tous les accès du composant, avec des résultats similaires quant à la susceptibilité mise en évidence. Le signal délivré par le synthétiseur est un signal sinusoïdal CW. Les caractéristiques statiques du composant sous agression ( $I_D=f(V_{GS})$  et  $I_D=f(V_{DS})$ ) sont directement mesurées grâce aux deux SMU (Source Measure Unit) intégrées dans l'analyseur de paramètres de composants (Keithley 4200). Les té de polarisation assurent la superposition des voies DC et RF et une bonne isolation sur chacune des voies. Les signaux instantanés d'entrée  $v_{GS}(t)$  et de sortie  $v_{DS}(t)$  sont également mesurés grâce à une sonde active, de bande passante 4 GHz. La figure suivante présente un réseau de caractéristiques de sortie du transistor NMOS, sous agression EM. Les courbes en trait plein correspondent aux mesures sans agression, et celles en pointillés aux mesures sous agression.

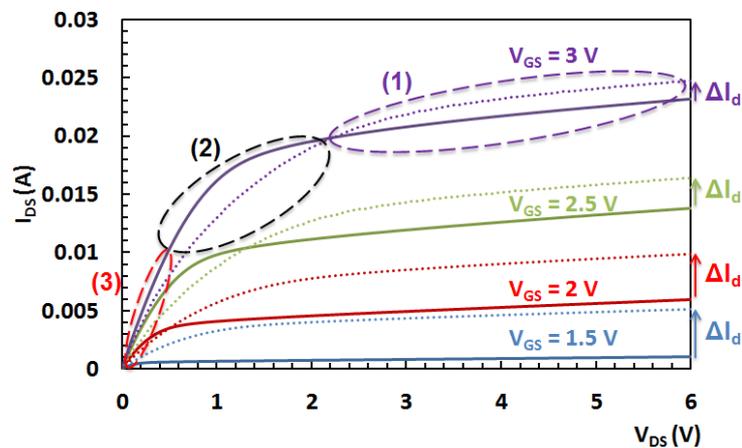


Fig. 1.4: Caractéristique de sortie  $I_D=f(V_{DS})$ , pour plusieurs tensions de commande  $V_{GS}$

La fréquence du signal injecté sur la grille est réglée à 10 MHz, et sa puissance est de 5 dBm. Une susceptibilité est ici révélée. Le premier effet induit par le signal d'agression est connu de la littérature sous le nom de phénomène de redressement [3- 5]. Quand un signal d'excitation alternatif est appliqué sur les accès d'une jonction électronique, une modification de son point de fonctionnement ( $I_D$ ,  $V$ ) apparaît, ceci en raison du comportement non-linéaire de la caractéristique courant-tension de la jonction. Ce décalage de la valeur moyenne du courant de drain, noté  $\Delta I_D$  sur la figure, est donc induit par la non-linéarité de la caractéristique d'entrée  $I_D=f(V_{GS})$  d'un transistor. Sur la figure 1.4 on voit clairement que la valeur de  $\Delta I_D$  dépend du choix de la tension de polarisation  $V_{GS}$ , mais également de la zone de fonctionnement du transistor :

- $\Delta I_D$  est positif dans la zone saturée (zone 1)
- $\Delta I_D$  est négatif dans la zone non-saturée (zone 2)
- $\Delta I_D$  est négatif mais faible dans la zone linéaire (zone 3)

La susceptibilité au redressement peut être caractérisée selon les paramètres du signal d'agression, en particulier en fonction de la puissance et de la fréquence du signal d'interférence. Ces évolutions sont particulièrement intéressantes à acquérir, puisqu'elles permettent de donner des ordres de grandeur des paramètres de l'interférence, qui assure un certain niveau de vulnérabilité du composant, sachant que dans un contexte d'attaque les caractéristiques du signal d'agression peuvent être optimisées. Le balayage en puissance du signal d'agression est mené, sur une plage de valeurs probables lors d'un couplage back-door [12]. Une valeur maximale réglée au synthétiseur de 10 dBm est utilisée.

Sur la figure 1.5, les traits pleins correspondent aux résultats de mesure, les pointillés correspondent à des résultats de calcul, dont le principe sera exposé dans la sous-partie 2. Le décalage du courant de drain tend à augmenter avec la puissance d'entrée. Selon la zone de fonctionnement du transistor, l'évolution pour les plus fortes puissances est différente ; dans la zone non-saturée ( $V_{GS}=4V$ ) un comportement linéaire (en dB) de pente constante est observé, alors que dans la zone saturée ( $V_{GS}=1.5V$  et  $V_{GS}=2V$ ) la pente diminue pour les plus forts niveaux de puissance utilisés. Notons qu'à une puissance de 10 dBm, la tension crête de commande  $V_{GS}$  est à 2V. Ce fort signal appliqué à l'entrée du composant induit un comportement fortement non-linéaire du transistor.

Le balayage en fréquence du signal d'agression est mené jusqu'à 1 GHz (figure 1.6). Sur cette figure les traits pleins correspondent aux résultats de mesure, les pointillés correspondent à des résultats de calcul.

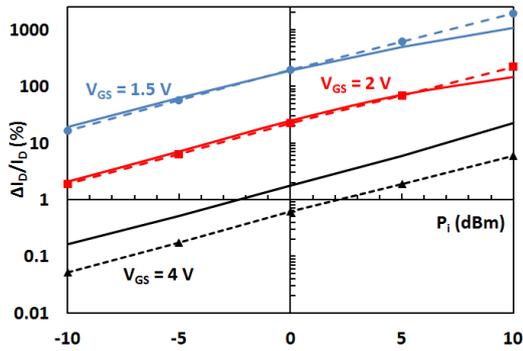


Fig. 1.5:  $\Delta I_D/I_D$  (%) en fonction de la puissance du signal agresseur, pour trois tensions de commande  $V_{GS}$ . La fréquence du signal est de 10 MHz.  $V_{DS}=2$  V

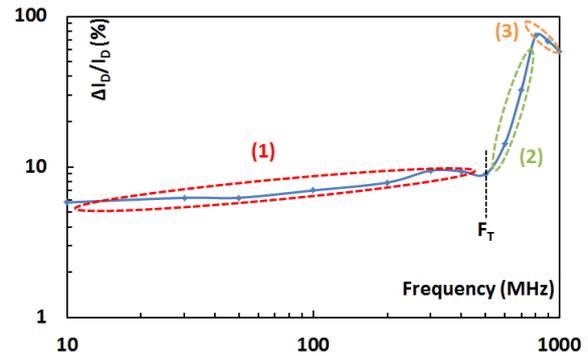


Fig. 1.6:  $\Delta I_D/I_D$  (%) en fonction de la fréquence du signal agresseur. La puissance absorbée sur la grille du transistor est maintenue à 5 dBm

L'impédance d'entrée d'un transistor MOS étant très capacitive, l'excursion  $v_{GS}(t)$  lorsque la fréquence de l'interférence est supérieure à  $f_T$  est faible, tendant ainsi à diminuer l'effet. Les mesures ont ainsi été réalisées en maintenant constante la tension crête  $V_{GS}$ , en ajustant pour chaque fréquence la puissance du signal d'entrée. Le redressement du courant de drain n'évolue pas avec la fréquence jusqu'à  $f_T$ . Puis quand la fréquence de l'interférence dépasse cette limite une augmentation forte du décalage en courant apparaît, suivie d'une légère diminution. Il semble donc évident que d'autres phénomènes entrent en jeu.

Pour expliquer ces comportements, les mesures des formes d'onde des tensions (entrée, sortie) proposées ne sont pas suffisantes. C'est ainsi que Clovis Pouant et moi-même, en accord avec Patrick Hoffmann du CEA Gramat, avons mis en place un banc de test visant à une analyse temporelle des courants, à tous les accès du composant (grille, drain, source et substrat), afin de visualiser les variations de charges imposées par le signal d'agression.

La figure ci-dessous représente le schéma du banc de test développé pour cette analyse temporelle des courants et tensions d'un composant non-linéaire.

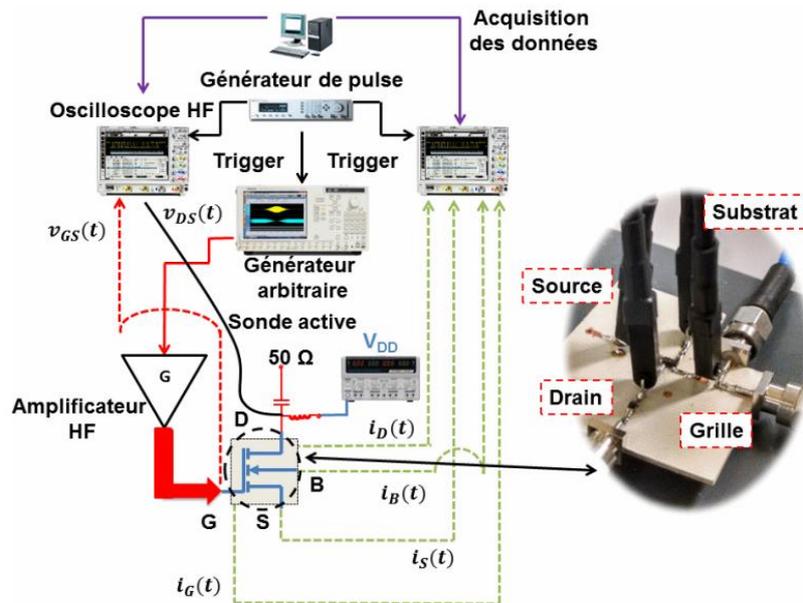


Fig. 1.7: Représentation schématique du banc d'expérimentation permettant de mesurer les courants et tensions instantanés aux accès du transistor

Un générateur de signaux arbitraires associé à un générateur de pulse est utilisé pour générer un signal d'agression de type impulsionnel avec porteuse. La durée du signal impulsionnel peut varier de 10 ns à 1  $\mu$ s, avec un taux de répétition des impulsions pouvant aller jusqu'à la ms [28, 29]. La limite haute de la fréquence porteuse utilisée sur ce banc est de 1 GHz. La mesure de chaque courant est réalisée par des sondes de courant HF, de bande passante 250 kHz – 2 GHz. Les tensions d'entrée et de sortie sont mesurées comme précédemment avec des sondes actives, haute impédance, jusqu'à 2 GHz. Le générateur de pulse synchronise à la fois les deux oscilloscopes (pour la mesure des 4 courants et des 2 tensions) et le générateur de signaux arbitraires. Les deux oscilloscopes sont déclenchés avec une grande attention pour que la mesure des formes d'onde de courant coïncide avec le signal d'agression impulsionnel. L'erreur temporelle de synchronisation entre les deux oscilloscopes est estimée à 500 ps.

Ce banc de test a été mis en place au CEA Gramat, pour des raisons de disponibilité de matériel. Cette méthode originale de test de susceptibilité a été publiée dans une revue internationale [30]. Les mesures ont été réalisées en configuration transistor seul et transistor monté en inverseur. Dans ce dernier cas, une résistance de charge  $R_D$  est insérée sur le drain du transistor. Sa valeur doit être choisie afin de garantir un gain du montage suffisant pour former une fonction inverseur logique.

Les expérimentations, présentées sur les figures 1.8 et 1.9, ont consisté à mesurer la réponse de l'inverseur à un signal impulsionnel de fréquences porteuses variables, de 10MHz à 1GHz, pour ainsi tester l'effet de la fréquence sur le comportement du transistor. A chaque fréquence testée, l'amplitude crête du signal d'agression appliquée sur la grille  $V_{GS}$  a toujours été maintenue constante.

Comme attendu, à basse fréquence le montage répond à la fréquence de l'excitation, et remplit sa fonction d'inverseur logique. Quand la fréquence du signal augmente, la réponse commence à s'altérer. La tension de sortie ne ressemble plus à un signal logique. Elle n'atteint plus sa valeur

maximale de  $V_{DD}=3V$ , sa valeur crête diminue fortement avec la fréquence. A partir de 400 MHz (figure 1.8 (c)) l'excursion de  $V_{DS}$  est faible et sa valeur moyenne est proche de 0, si bien que la sortie de l'inverseur est forcée à son niveau logique bas. Cet état se conserve durant l'application du signal impulsionnel.

Le résultat marquant est donc qu'il est possible de forcer un inverseur dans un état logique en appliquant un signal impulsionnel de fréquence porteuse judicieusement choisie. Cet état bloqué disparaît dès que la fréquence de l'excitation dépasse les 500 MHz. Au-delà de cette valeur, la tension de sortie devient sinusoïdale, et suit donc la forme du signal d'entrée (figure 1.9). Sa tension crête augmente fortement, et devient comparable à celle de l'entrée. L'inverseur est alors transparent vis-à-vis du signal interférant.

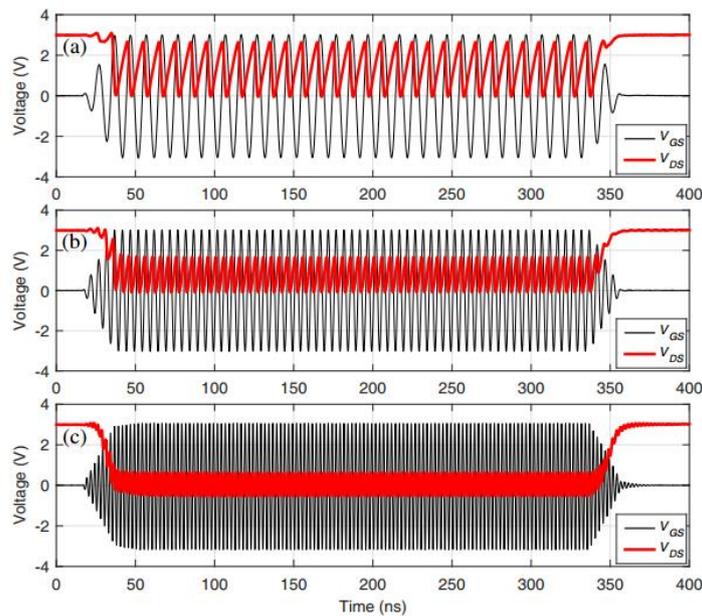


Fig. 1.8:  $V_{GS}(t)$  et  $V_{DS}(t)$  pour un signal d'agression de 3V crête, de fréquence : (a) 100MHz, (b) 200 MHz, (c) 400 MHz.  $V_{DD}=3V$

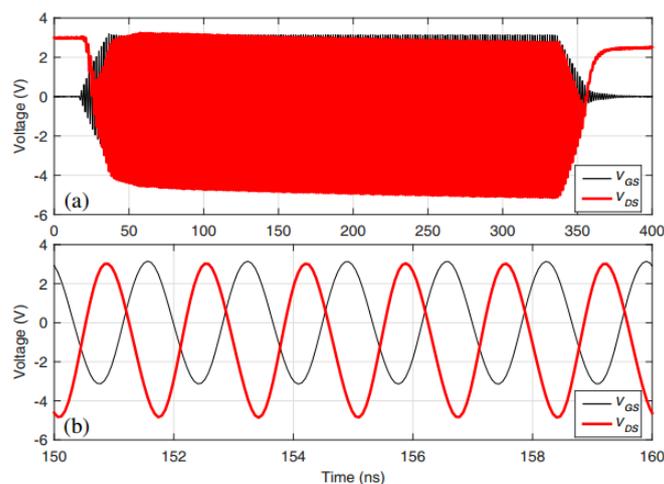


Fig. 1.9:  $V_{GS}(t)$  et  $V_{DS}(t)$  pour un signal d'agression de 3V crête, à 600 MHz, (a)  $V_{DD}=3V$ , (b) zoom de (a) entre 160 ns et 170 ns

Pour acquérir une description plus fine de l'origine physique de l'état bloqué, obtenu sous agression et dans une certaine bande de fréquence d'attaque, nous avons mesuré les courants instantanés, aux quatre accès du transistor. Les résultats sont présentés sur les figures 1.10, 1.11, 1.12 et 1.13.

Aux basses fréquences les formes d'ondes obtenues sont tout à fait cohérentes et représentatives d'un inverseur fonctionnant en commutation. La seule différence par rapport au cas classique est que le signal de commande est un signal sinusoïdal et non impulsionnel. Par conséquent, la distribution de la charge du transistor varie continuellement au rythme du signal d'agression. Ceci génère des courants dominés principalement par la partie extrinsèque du composant et en particulier au niveau des régions de déplétion (source-substrat et drain-substrat). La période du signal de commande est ici plus grande que les temps de commutation bloqué-passant, passant-bloqué. Par conséquent, dans la phase de conduction ( $v_{GS}(t) > V_T$ ), le courant de drain idéal (conduction dans le canal) parvient à s'établir à sa valeur DC. Dans la phase de blocage le courant de drain a le temps de s'annuler. Une description détaillée de ces formes d'onde a été proposée dans [30].

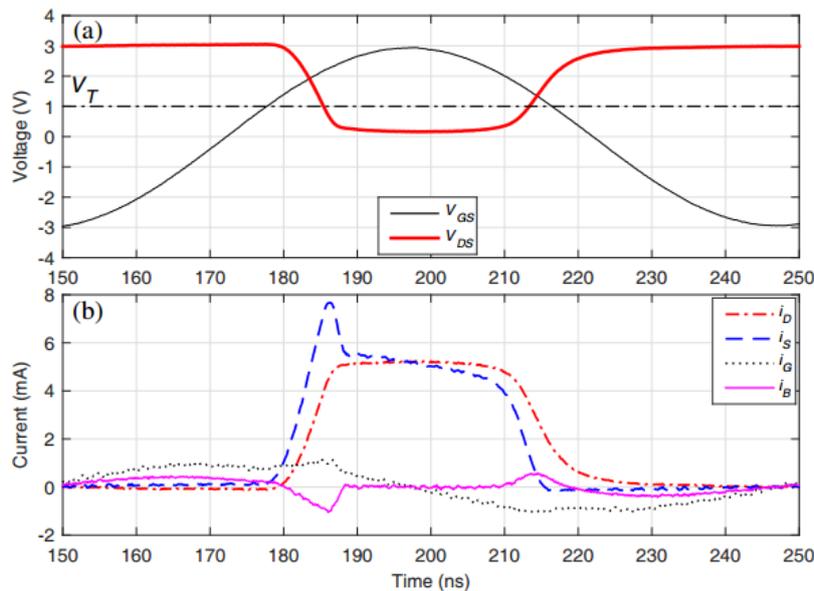


Fig. 1.10: Formes d'onde sur une période du signal d'agression, des tensions entrée/sortie, et des courants de l'inverseur NMOS, à une fréquence d'agression de 10 MHz

Lorsque la fréquence de l'agression augmente, les variations de charge imposées par ce signal de commande s'accroissent. Une augmentation des courants mesurés est alors nécessaire afin de suivre ces fortes variations de charge. Ceci est clairement visible sur les figures 1.11 et 1.12. Les courants de source, de grille et de substrat augmentent fortement. Le courant de drain atteint toujours sa valeur d'équilibre, mais il parvient à peine à s'annuler, avant une nouvelle phase de conduction. La tension de sortie n'atteint plus son état haut ( $V_{DS}=V_{DD}=3V$ ).

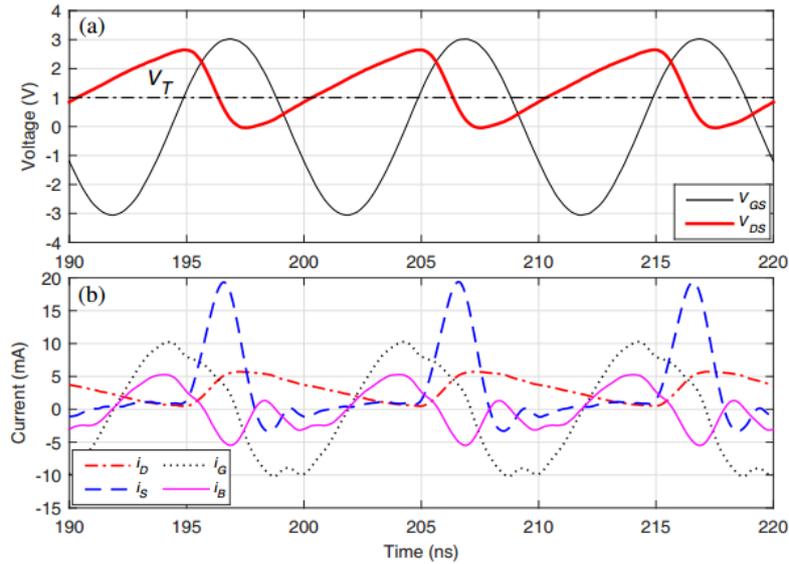


Fig. 1.11: Formes d'onde sur une période du signal d'agression, des tensions entrée/sortie, et des courants de l'inverseur NMOS, à une fréquence d'agression de 100 MHz

A 400 MHz la période des signaux devient plus faible que les temps de commutation de l'inverseur. Ainsi les formes d'onde évoluent beaucoup, et ressemblent de plus en plus à des sinusoïdes, à l'image du signal d'agression. Le courant de drain ne s'annule plus, sa valeur moyenne augmente. Or la droite de charge du montage lie les valeurs moyennes de  $i_D$  et de  $v_{DS}$ , avec des sens de variation opposés. Ceci explique la diminution de la valeur moyenne de  $v_{DS}(t)$ , qui tend vers 0, aboutissant ainsi à un état forcé de l'inverseur durant l'application du signal d'agression.

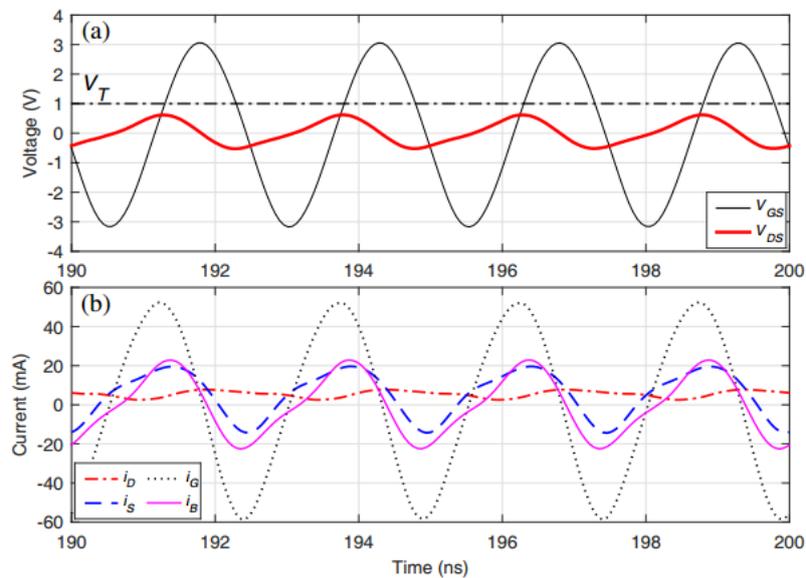


Fig. 1.12: Formes d'onde sur une période du signal d'agression, des tensions entrée/sortie, et des courants de l'inverseur NMOS, à une fréquence d'agression de 400 MHz

A 600 MHz, toutes les formes d'ondes sont sinusoïdales, à l'image du signal d'entrée du montage. Le fonctionnement de l'inverseur semble alors être complètement régi par des éléments passifs

(inductances, capacités). La majeure partie des courants circule à travers le transistor par des chemins apportés par des éléments extrinsèques au transistor et parasites (boîtier). L'effet transistor est inhibé.

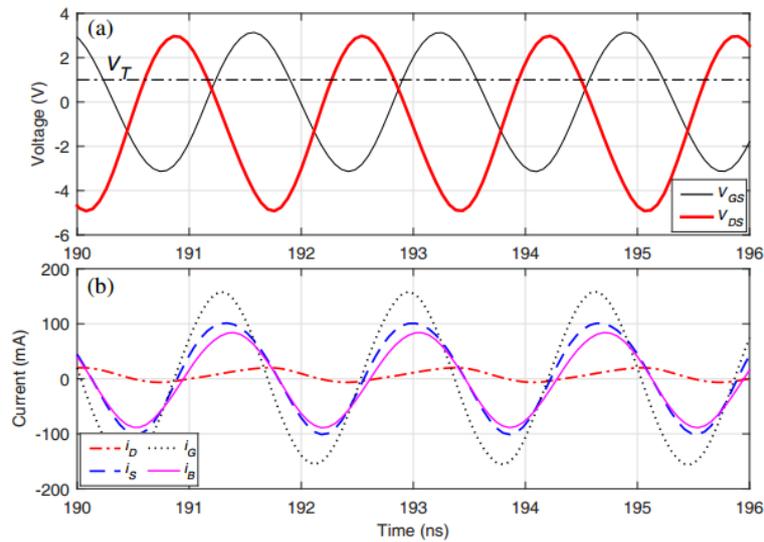


Fig. 1.13: Formes d'onde sur une période du signal d'agression, des tensions entrée/sortie, et des courants de l'inverseur NMOS, à une fréquence d'agression de 600 MHz.  $V_{DD}=3V$

Ces résultats montrent que les études de susceptibilité EM au niveau composant peuvent être menées en adoptant une méthodologie basée sur la mesure instantanée des tensions et des courants. Ces mesures amènent à la compréhension des mécanismes physiques mis en jeu. Cette méthode de test constitue donc un moyen judicieux pour une analyse plus fine de la susceptibilité EM.

Suite à ces premiers travaux, des tests sur d'autres références de transistors NMOS mais aussi PMOS ont été poursuivis durant le stage post-doctorat de Clovis Pouant, mené dans le laboratoire commun LEV3E entre le CEA Gramat et l'XLIM. La mise à l'état bloqué du transistor par le signal interférant a toujours été mise en évidence, dans des bandes de fréquences différentes, selon la vitesse de commutation du composant. J'ai été associé à ce travail de continuité, qui a donné lieu à un article dans une revue internationale [31] et une conférence internationale [32]. Il serait maintenant intéressant d'utiliser cette méthodologie sur une cellule inverseuse de technologie CMOS, et ainsi tester cette cellule de base largement répandue dans les circuits numériques. Pour l'instant pas de financement n'est prévu pour continuer ces actions.

Afin d'améliorer la compréhension et prédire les effets induits par un signal d'interférence, des outils de calcul analytique et de simulations numériques ont été mis en place, dès 2009 et les premiers travaux engagés sur ce thème de recherche. J'ai intégralement pris en charge le développement de ces outils, en m'appuyant notamment sur des compétences au niveau de la modélisation fort-signal, et haute-fréquence de composants, acquises durant ma thèse.

## 2) Moyens de calcul et de simulation

Afin d'analyser les comportements expérimentaux suite aux injections EM, j'ai voulu mettre en œuvre deux méthodes de calcul : le calcul analytique utilisant des fonctions mathématiques d'approximation des non-linéarités du composant, responsables des principaux effets induits, et le calcul numérique basé sur des simulations type SPICE à partir de modèles compacts, le plus souvent simplifiés pour conserver une maîtrise des outils.

Ces outils de calcul analytique et numérique ont été initiés dès la thèse de Tristan Dubois sur des diodes Schottky, puis ont été complétés et perfectionnés dans les thèses d'Adrien Doridant sur des transistors bipolaires, et de Clovis Pouant sur des transistors à effet de champ. Les simulations électriques développées à partir de calcul numérique permettent d'obtenir des résultats rapides et efficaces dans la prédiction des effets induits. Cependant, les modèles utilisés, même simplifiés, nécessitent des étapes de caractérisation (statiques, dynamiques petit et fort-signal) relativement fastidieuses [33, 34]. Plus généralement, la méthode utilisant les simulations ne permet pas de comprendre qualitativement de manière simple l'origine des phénomènes mis en jeu et les paramètres d'influence.

En revanche, un outil analytique conduit au développement d'expressions mathématiques des effets induits, et donc à une identification des grandeurs clés intervenant dans les mécanismes d'agression. Cette approche mathématique a essentiellement pour objectif de mieux comprendre les processus de conversion non-linéaire régnant au sein d'un composant actif soumis à une excitation. Dans un système supposé linéaire, une excitation mono-fréquence à son entrée produit uniquement un signal de sortie à la même fréquence. Cela n'est plus le cas avec un système non-linéaire. On parle alors de conversion ou de mélange induit par les non-linéarités propres au système considéré. Il faut donc être capable de mettre en équation ces processus de conversion pour comprendre l'origine des effets observés sous agression. C'est ce que j'ai voulu mettre en place dans l'équipe, en complément des simulations numériques.

La méthode de calcul s'appuie sur le développement en série de Taylor des non-linéarités courant-tension (I-V) et charge-tension (Q-V) du transistor. L'ordre de la série détermine l'étendue du domaine de validité de cette fonction d'approximation. Généralement des valeurs d'ordre faibles sont utilisées, afin de garder une certaine simplicité dans la mise en œuvre de l'outil. Le domaine de validité de cette technique est alors limité à de faibles excursions. Cette méthode n'est pas originale, mais j'ai souhaité la mettre en place et l'appliquer le plus largement possible à tous les cas d'étude rencontrés.

Elle a ainsi été utilisée pour le calcul du décalage du point de fonctionnement des composants discrets étudiés [22- 24]. Plus récemment dans la thèse d'Alexandre Martorell, elle a servi à calculer la distorsion d'intermodulation d'ordre 3 dans des amplificateurs faible bruit et des amplificateurs de puissance microonde, sous agression [35].

### a) Calcul analytique

Je vais présenter le principe du calcul analytique développé pour la thèse de Clovis Pouant en vue d'exprimer la variation du courant de drain induite par l'agression  $\Delta I_D$ , observée expérimentalement et présentée à la figure 1.4. Seules les non-linéarités associées au courant de transport dans les transistors et sans mémoire (les effets non quasi-statiques sont négligés) sont prises en compte. Un développement en série de Taylor de la non-linéarité d'entrée  $I_D$ - $V_{GS}$  et la non-linéarité de sortie  $I_D$ - $V_{DS}$ , est utilisé afin de calculer le décalage du courant de drain  $\Delta I_D$  dans toutes les zones de fonctionnement du transistor (saturée, non-saturée et linéaire). Il est en effet connu qu'en régime non-saturé et linéaire la conductance de sortie devient une importante source non-linéaire [36].

La valeur moyenne du courant de drain développé en série de Taylor, autour d'un point de fonctionnement  $V_{GS}$  et  $V_{DS}$  auquel on applique un signal d'entrée, s'exprime de la manière suivante :

$$\begin{aligned} & \overline{I_D(V_{GS} + \hat{V}_{GS} \cdot \sin(\omega t); V_{DS} + \hat{V}_{DS} \cdot \sin(\omega t + \phi))} = \\ & I_D(V_{GS}, V_{DS}) + \overline{\hat{V}_{GS} \cdot \sin(\omega t)} \cdot g_m + \overline{\hat{V}_{DS} \cdot \sin(\omega t + \phi)} \cdot g_d + \frac{\hat{V}_{GS}^2}{2!} \cdot \overline{\sin(\omega t)^2} \cdot \left. \frac{\partial g_m}{\partial V_{GS}} \right|_{V_{DS}} \\ & + \frac{\hat{V}_{DS}^2}{2!} \cdot \overline{\sin(\omega t + \phi)^2} \cdot \left. \frac{\partial g_d}{\partial V_{DS}} \right|_{V_{GS}} + \frac{\partial I_D}{\partial V_{GS} \partial V_{DS}} \Big|_{V_{DS}, V_{GS}} \cdot \overline{\hat{V}_{GS} \cdot \sin(\omega t) \cdot \hat{V}_{DS} \cdot \sin(\omega t + \phi)} \\ & + \dots + \frac{\hat{V}_{GS}^n}{n!} \cdot \overline{\sin(\omega t)^n} \cdot \left. \frac{\partial g_m^n}{\partial V_{GS}^n} \right|_{V_{DS}} + \frac{\hat{V}_{DS}^n}{n!} \cdot \overline{\sin(\omega t + \phi)^n} \cdot \left. \frac{\partial g_d^n}{\partial V_{DS}^n} \right|_{V_{GS}} \\ & + \frac{\partial I_D^{(n-1)}}{\partial V_{GS}^{(n-1)} \partial V_{DS}} \Big|_{V_{DS}, V_{GS}} \cdot \overline{\hat{V}_{GS}^{(n-1)} \cdot \sin(\omega t)^{(n-1)} \cdot \hat{V}_{DS} \cdot \sin(\omega t + \phi)} \\ & + \frac{\partial I_D^{(n-1)}}{\partial V_{GS} \partial V_{DS}^{(n-1)}} \Big|_{V_{DS}, V_{GS}} \cdot \overline{\hat{V}_{GS} \cdot \sin(\omega t) \cdot \hat{V}_{DS}^{(n-1)} \cdot \sin(\omega t + \phi)^{(n-1)}} \end{aligned}$$

Où  $g_m = \frac{\partial I_D}{\partial V_{GS}}$  est la transconductance,  $g_d = \frac{\partial I_D}{\partial V_{DS}}$  la conductance,  $g_{md} = \frac{\partial I_D}{\partial V_{GS} \partial V_{DS}}$  les termes croisés, et  $\Phi$  le déphasage entre les signaux  $v_{GS}(t)$  et  $v_{DS}(t)$ .

Si on limite le développement à l'ordre 2, la variation moyenne du courant de drain  $\Delta I_D$  s'exprime comme suit :

$$\begin{aligned} \Delta I_D & \approx \overline{I_D} - I_D(V_{GS}, V_{DS}) \\ & \approx \frac{\hat{V}_{GS}^2}{4} \cdot \left. \frac{\partial g_m}{\partial V_{GS}} \right|_{V_{DS}} + \frac{\hat{V}_{DS}^2}{4} \cdot \left. \frac{\partial g_d}{\partial V_{DS}} \right|_{V_{GS}} + \frac{1}{2} \cdot g_{md} \cdot \hat{V}_{GS} \cdot \hat{V}_{DS} \cdot \cos(\phi) \end{aligned}$$

$\Delta I_D$  dépend des dérivées de la transconductance et de la conductance de sortie du composant. Ces coefficients de la série de Taylor sont extraits de la dérivation jusqu'à l'ordre 2 des caractéristiques statiques expérimentales  $I_D=f(V_{GS})$  à  $V_{DS}$  constante et  $I_D=f(V_{DS})$  à  $V_{GS}$  constante. Le tracé de ces dérivées (première et seconde) est présenté sur les figures ci-après. Des variations plus ou moins marquées selon les zones de fonctionnement sont nettement mises en évidence. Dans la zone saturée du composant, la dérivée première de la conductance est proche de 0, elle est donc négligeable dans le calcul du  $\Delta I_D$ . Dans

les zones non-saturée et linéaire, les dérivées premières de  $g_m$  et  $g_d$  sont négatives, ce qui explique le signe négatif de  $\Delta I_D$  observé expérimentalement.

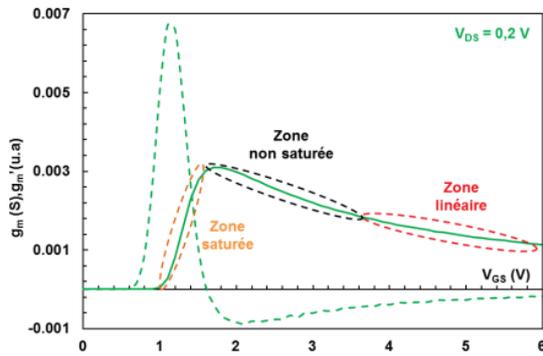


Fig. 1.14: Transconductance  $g_m$  (trait plein) et sa dérivée première selon la tension de grille-source (pointillés)

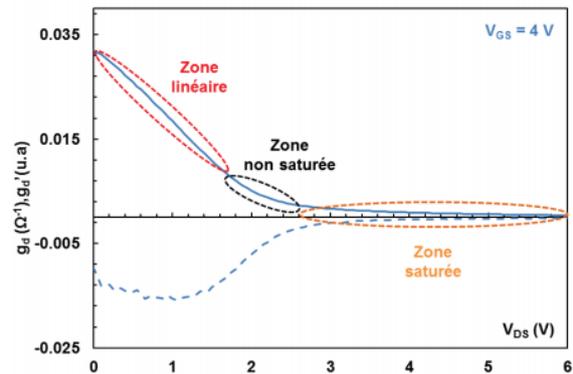


Fig. 1.15: Conductance de sortie  $g_d$  (trait plein) et sa dérivée première selon la tension de drain-source (pointillés).

Les valeurs calculées de  $\Delta I_D$  ont été comparées avec succès aux relevés expérimentaux, comme présenté à la figure 1.5. Une limite de validité en puissance d'entrée apparaît autour de 10 dBm. Elle est plus ou moins marquée selon la tension de polarisation  $V_{GS}$  choisie. Pour passer outre cette limite, il faut augmenter l'ordre de la série de Taylor, au-delà de 2.

Une limite en fréquence apparaît autour de la fréquence de transition du composant ( $f_T \approx 500$  MHz), comme présenté dans [23]. Au-delà de  $f_T$  le modèle analytique devient trop simpliste. En particulier, les valeurs crêtes des tensions  $v_{GS}(t)$  et  $v_{DS}(t)$  utilisées dans la formulation de  $\Delta I_D$  sont mesurées sur les plots, à l'extérieur du transistor. Or à de telles fréquences le boîtier et la partie extrinsèque du composant ont une contribution non négligeable à la réponse du dispositif.

Pour élargir notre expertise et dépasser ces limites de validité, j'ai voulu développer l'outil de calcul numérique basé sur des simulations électriques type SPICE.

## b) Simulation numérique

Les modèles compacts usuels [34] disponibles dans les logiciels de simulation et dont les paramètres sont parfois fournis sur le site des fondeurs ne sont pas utilisés. Ma démarche consiste à concevoir des modèles simplifiées, basés également sur les équations de la physique du composant. Un modèle compact simplifié peut tout à fait suffire, à condition d'avoir identifié les éléments qui ont un rôle prépondérant dans l'apparition des effets induits par le signal d'agression. Le modèle est ainsi modifiable, ce qui est utile pour garantir une meilleure compréhension des résultats. Rappelons également que les modèles compacts usuels ont été validés jusqu'à la fréquence de transition du composant. Or, nous testons la susceptibilité des composants avec des signaux de forte amplitude et de fréquences  $f > f_T$ . D'ailleurs le contexte des attaques EM tend et tendra à utiliser des signaux de

fréquences de plus en plus élevées. Les modèles intrinsèques restent-ils toujours valables avec des précisions acceptables pour des études avec des signaux hors-bande ?

Dans la thèse d'Adrien Doridant nous avons vu [37] que les effets induits par le signal d'agression mettent en jeu des phénomènes physiques spécifiques, qui ne sont pas forcément pris en compte dans les modèles compacts disponibles. Ainsi nous avons mis en évidence dans le cas d'un transistor bipolaire que l'application d'un signal de fréquence  $f > f_T$  induit une défocalisation des lignes de courant alternatif dans la jonction base-émetteur, si bien que la tension  $v_{BE}(t)$  varie latéralement dans la jonction. Si ce phénomène n'est pas pris en compte, la prédiction de la variation du courant collecteur  $\Delta I_C$  induite par le signal est faussée avec même une inversion de son signe. Un modèle distribué de la jonction est alors nécessaire [38], et a été détaillé dans la thèse d'Adrien Doridant.

Dans les études menées jusqu'à présent, nos modèles sont renseignés à partir de techniques d'extraction basées sur des mesures fréquentielles (paramètres S, load-pull) [39] et sont validés par des simulations utilisant des méthodes mixtes, de type équilibrage harmonique, avec une largeur de bande limitée. Cependant, les signaux d'attaque peuvent et pourront avoir des formes d'onde à bande très large, et avec de fortes variations de tension et/ou de courant ( $dV/dt$  et  $dI/dt$ ), ce qui va solliciter les fortes non-linéarités des composants actifs. Il faudra certainement, dans la suite des études, adapter nos modèles en essayant de toujours garder une proximité avec la physique du composant.

Je vais dans la suite détailler le modèle mis en œuvre pour simuler l'état bloqué présenté dans la partie précédente, lorsque le montage inverseur est soumis au signal impulsionnel avec porteuse. Le comportement du composant sous injection, mesuré sous certaines conditions expérimentales, doit être reproduit par simulation.

Il est donc nécessaire de modéliser chaque élément du banc de test considéré. Le composant actif est modélisé à partir d'un modèle compact adapté au nœud technologique utilisé. Ici un modèle de MOS fort signal valable en fonctionnement transitoire, basé sur la structure simplifiée proposée par [33] a été utilisé. Il inclut en plus des éléments intrinsèques non-linéaires, les capacités et résistances extrinsèques. Des étapes de caractérisations classiques (statiques, dynamiques) ont été menés afin d'extraire les valeurs des paramètres du modèle [40]. Autour de ce cœur non-linéaire sont ajoutés des éléments localisés résistifs et réactifs, prenant en compte les éléments parasites du boîtier, des pistes du circuit imprimé de test, et des sondes de mesure. Lors de la réalisation de la carte de test, nous avons utilisé des longueurs de pistes les plus faibles possible, afin de pouvoir utiliser des modèles simples de lignes, et non des modèles distribués. Les valeurs parasites du boîtier sont extraites à partir de mesures de paramètre S, à différents points de polarisation, et de techniques classiques « d'épluchage », en supposant que ces valeurs ne varient pas avec la polarisation. Le schéma électrique proposé est présenté à la figure 1.16.

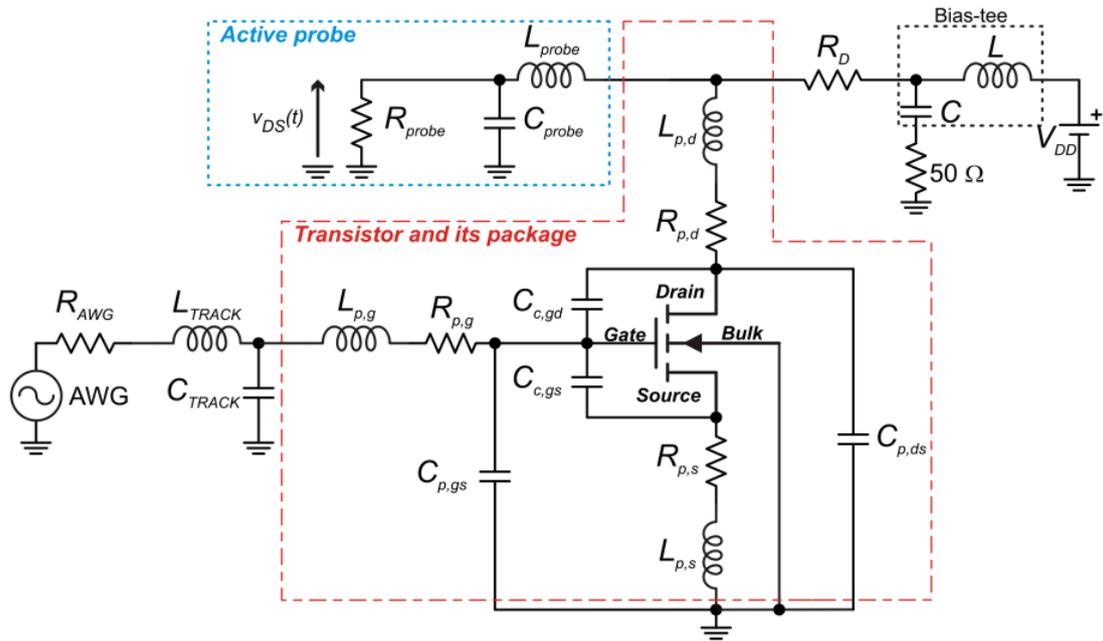


Fig. 1.16: Schéma électrique utilisé pour simuler la réponse d'un inverseur NMOS à un signal impulsionnel avec porteuse

La technique de simulation de type enveloppe est utilisée et appliquée à ce schéma électrique fort-signal et haute fréquence afin de calculer numériquement la forme d'onde de la tension  $v_{DS}(t)$ . Ce mode de simulation consiste en une analyse par la technique de l'équilibrage harmonique, limitée dans une fenêtre temporelle. Les amplitudes et phases au fondamental et aux harmoniques des signaux sont ainsi calculées et leur évolution est suivie temporellement, par exemple pendant la période de répétition du signal impulsionnel utilisé. La figure 1.17 compare les résultats simulés et mesurés des valeurs moyennes et crête-à-crête de la tension de sortie  $V_{DS}$ , extraites à partir des formes d'onde des tensions simulées, en fonction de la fréquence du signal d'entrée, jusqu'à 600 MHz.

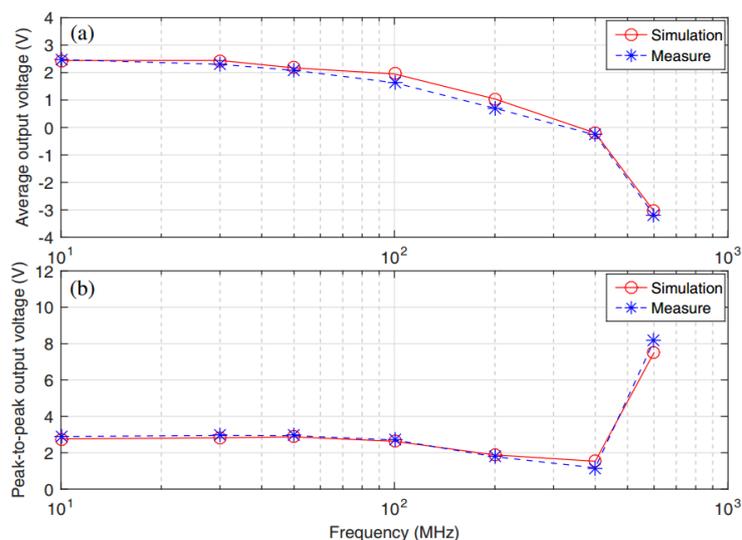


Fig. 1.17: Comparaison mesure, simulation des valeurs moyennes et des valeurs crête-à-crête de  $v_{DS}(t)$

Les résultats simulés et mesurés sont en très bon accord. La prise en compte des éléments parasites a été primordiale pour atteindre cet accord [30]. Ceci confirme le rôle important des éléments extrinsèques au composant (composant, boîtier, pistes), qui agissent ensemble à l'apparition de l'état bloqué. On voit clairement ici l'apport de la simulation par rapport au calcul analytique.

La simulation numérique permet également de calculer la réponse sous agression de composants non polarisés, ce qui est un intérêt évident dans le cas des circuits numériques. Cela ne peut être réalisé avec la méthode par calcul en série de Taylor car elle nécessite un point de polarisation autour duquel les dérivées sont calculées.

La simulation numérique peut aussi facilement être utilisée avec d'autres formes d'onde d'agression, afin d'anticiper et de prédire les effets, à condition que les modèles utilisés restent valides sur la bande d'occupation spectrale des signaux agresseur. L'attaquant dispose ainsi d'un moyen de prédiction des vulnérabilités, ainsi que d'une évaluation quantitative de l'ampleur des perturbations induites par des signaux de forme d'onde quelconque. Cela évite de procéder à certaines campagnes de tests, qui peuvent être coûteuses. Le concepteur de circuits peut quant à lui essayer de rendre moins sensible son circuit, et améliorer son immunité.

### 3) Expérimentations et calculs au niveau fonction électronique

Jusqu'à présent les études menées sur les circuits ont concerné les fonctions analogiques RF des chaînes d'émission-réception. Ces équipements sont massivement utilisés pour répondre à une demande croissante de systèmes de communications à distance. Etant placé juste après l'antenne de réception, cette électronique est soumise à des interférences par couplage de type front-door.

Notre intérêt en association avec la DGA puis le CEA Gramat a été de s'intéresser à des circuits asservis, en particulier la boucle à verrouillage de phase (PLL), qui est la principale fonction constituant l'oscillateur local du récepteur. Sa fréquence d'oscillation doit être stable, son bruit de phase le plus faible possible. Une étude de susceptibilité d'un récepteur radio a été réalisée durant le stage post-doctoral de Tristan Dubois financé par le CEA, menée à l'université de Montréal [25] et dont Sylvie Jarrix et moi étions les tuteurs académiques français. Un des résultats marquants est que lorsque l'oscillateur local est perturbé par un signal d'interférence la constellation mesurée en sortie du récepteur en modulation QPSK montre une forte dispersion des données reçues (figure 1.18). Cette illustration renforce le fait que l'oscillateur local est une fonction critique quant à sa susceptibilité.

Exemple :  
Modulation QPSK



Fig. 1.18: Exemple de constellation mesurée à la sortie d'un récepteur, sans et avec un signal injecté sur l'oscillateur local

Les premières études ont été réalisées en 2007 dans le cadre de la thèse de Tristan Dubois toujours financée par la DGA, et ont porté entre autres sur la mise en évidence des effets d'une onde EM sur une PLL. J'ai intégré l'équipe au cours de cette thèse pour travailler sur la fonction oscillateur contrôlé en tension (OCT), brique de base de la PLL pour laquelle j'avais l'expertise grâce à ma thèse.

Ces premiers travaux ont mis en évidence de façon expérimentale la plupart des comportements du circuit sous injection [24]. Peu de résultats en matière de calculs analytiques et de simulations prédictives ont été mis en place, à l'image de la plupart des travaux menés sur l'étude de la susceptibilité de systèmes de communications, qui concernaient essentiellement des interférences non-intentionnelles [41- 43] et ne présentaient que les phénomènes et leurs conséquences sur le fonctionnement complet du dispositif [44, 45].

Afin de poursuivre les études, une deuxième thèse a alors pu démarrer avec un financement de l'Ecole Normale Supérieure de Cachan. Les objectifs de la thèse d'Amable Blain ont été d'une part de continuer le travail expérimental de mise en lumière des perturbations, d'autre part d'approfondir la compréhension des mécanismes mis en jeu, et enfin de mettre en place des prédictions des comportements sous agression.

Pour ce faire, j'ai proposé de travailler sur les circuits utilisés durant ma thèse. Il me semblait très intéressant de travailler sur un circuit entièrement intégré (MMIC sur silicium), et j'avais en outre à disposition, les modèles des composants actifs et passifs ainsi que la topologie du circuit.

Je vais maintenant présenter les tests menés et les principaux résultats expérimentaux de perturbation sur ce type de circuit, en ciblant sur les comportements sous agression de l'OCT, puis de la PLL.

#### a) Présentation des tests menés

Le banc de test développé doit permettre d'injecter le signal sur un des accès de l'oscillateur. Trois accès sont disponibles à l'extérieur de la puce, deux entrées (alimentation et commande) et une sortie. Comme présenté sur la figure ci-dessous, le signal d'agression peut être injecté en mode conduit à travers un té de polarisation, placé sur les connecteurs. Les tés permettent d'éviter l'envoi des signaux agresseurs, pouvant être de forte puissance, sur les appareils de mesure. A l'aide d'un coupleur bidirectionnel nous mesurons la puissance injectée et la puissance réfléchiée, desquelles nous déduisons

la puissance réellement absorbée par le circuit. L'analyseur de spectre nous permet d'observer l'influence du signal d'interférence sur le spectre de l'OCT.

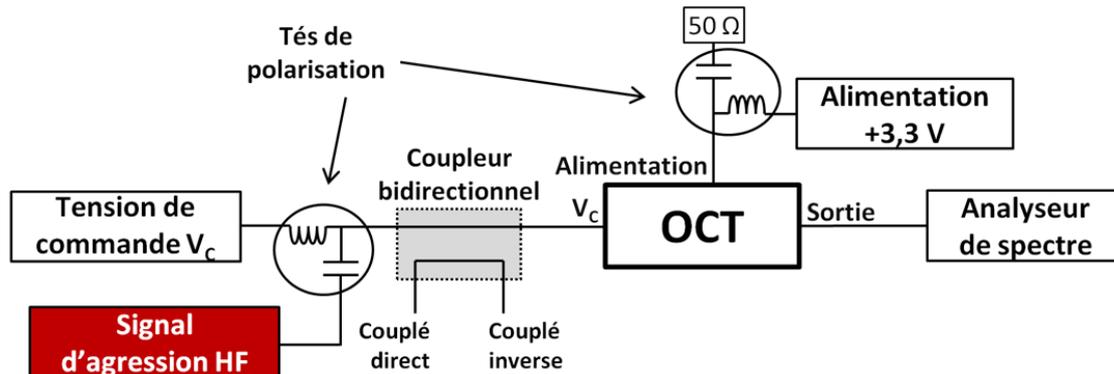


Fig. 1.19: Injection d'un signal sur l'entrée commande de l'OCT

Pour faciliter la compréhension et l'analyse des comportements, un signal d'injection de forme sinusoïdale CW est utilisé. Les niveaux de puissance sont balayés jusqu'aux limites du synthétiseur (30 dBm). Cette large plage de valeur couvre les niveaux de puissance représentatifs des signaux non-intentionnels (puissance relativement faible) et des signaux intentionnels (puissance généralement forte). La plage de fréquence sort largement de la bande de fonctionnement du circuit, qui par nature est très étroite pour un circuit asservi en phase.

Une des questions au cœur des préoccupations de cette thèse est de savoir si un signal d'injection hors bande par rapport aux caractéristiques fonctionnelles du circuit visé peut avoir un effet sur ses performances. Dans les parties précédentes nous avons montré, au niveau composant, une susceptibilité à des signaux de fréquences largement supérieures à leur fréquence de transition, ce qui laisse présager qu'au niveau circuit, des sensibilités en dehors de sa bande de fréquence de fonctionnement pourraient être révélées.

Les premiers tests fonctionnels consistent à injecter un signal de fréquence proche de la fréquence d'oscillation de l'OCT, et à mesurer le spectre de sortie. La fréquence d'injection est notée  $f_{inj}$  dans la suite. Le circuit est alimenté et commandé de telle sorte qu'il oscille à sa fréquence nominale ( $f_{oct} \approx 4.595\text{GHz}$ ). La figure 1.20 représente l'évolution du spectre dans une certaine bande de fréquence d'injection. Chaque ligne horizontale correspond à une image du spectre de sortie, obtenue à une fréquence particulière d'injection. Un changement de couleur signifie qu'une raie apparaît sur le spectre de sortie.

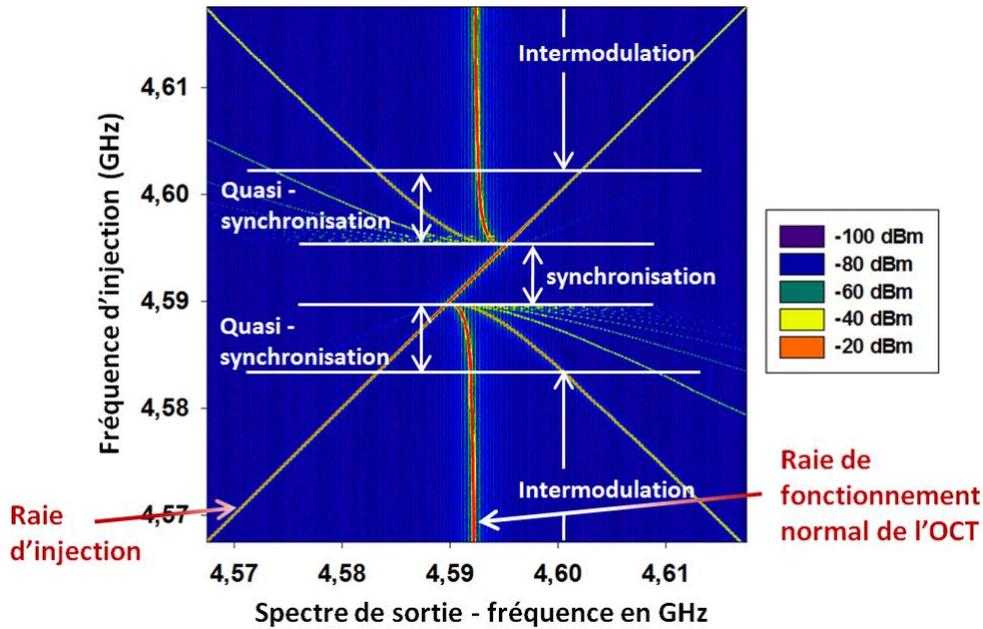


Fig. 1.20: Evolution du spectre de sortie de l'OCT sous injection sinusoïdale, à une puissance de 10 dBm

Trois comportements, tous résultant de mécanismes de conversion non-linéaire, peuvent être identifiés :

- $f_{\text{oct}}$  ne change pas si  $f_{\text{inj}}$  est loin de  $f_0$ . Seules des raies parasites d'intermodulation sont créées,
- $f_{\text{oct}}$  se déplace légèrement, avec un décalage de plus en plus marqué quand  $f_{\text{inj}}$  se rapproche de  $f_{\text{oct}}$ . De nombreuses raies latérales, générées par un phénomène de battement, polluent le spectre. On parle de quasi-synchronisation (ou pulling) [46],
- A partir d'une certaine fréquence injectée,  $f_{\text{oct}}$  et  $f_{\text{inj}}$  sont égales dans une bande de fréquence particulière, appelée plage de synchronisation [47]. L'OCT est alors piloté par le signal d'agression, sur une plage de plusieurs dizaines de MHz du signal d'attaque.

Ce dernier comportement, particulièrement intéressant dans un contexte d'attaque, a attiré notre attention, avec une volonté de quantifier la largeur de cette bande, et donc de déterminer les paramètres de l'agression et du circuit qui influent sur cette susceptibilité. Il s'explique par le fait que le signal parasite injecté introduit un déphasage supplémentaire dans la boucle. Pour garantir l'oscillation, le point de fonctionnement est modifié et la cellule résonante produit un déphasage qui compense celui introduit par le signal. La fréquence de résonance varie, et se cale donc sur celle du signal parasite. L'augmentation de la puissance de l'interférence élargit la plage de synchronisation.

En outre, nous avons cherché à savoir si une perturbation significative se produit si la fréquence de l'injection s'éloigne de cette fréquence de résonance. La figure 1.21 montre qu'une modification de la fréquence d'oscillation  $f_0$  est possible alors que  $f_{\text{inj}}$  est très éloignée de  $f_{\text{oct}}$ . Une synchronisation dite

secondaire de la fréquence d'oscillation a été possible avec une fréquence d'injection égale à une sous-harmonique de  $f_{oct}$  ( $\approx 2.25 \text{ GHz} = f_{oct} / 2$ ).

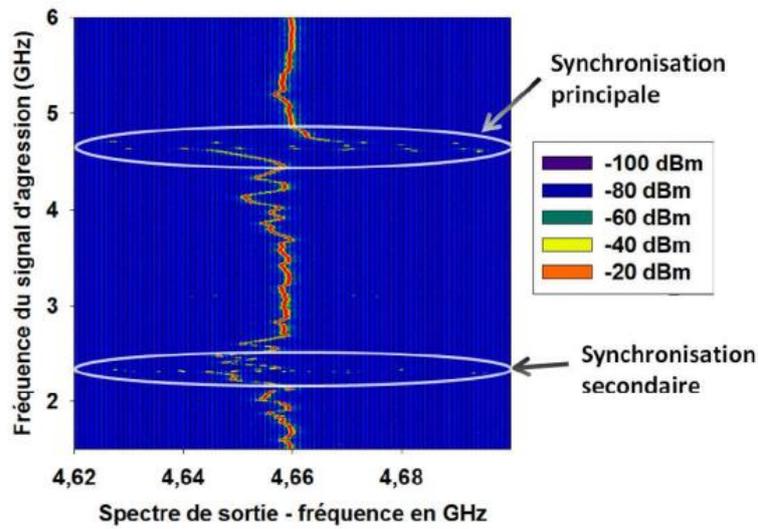


Fig. 1.21: Evolution du spectre de sortie de l'OCT sous injection sinusoïdale hors bande de fonctionnement de l'OCT, à une puissance de 20 dBm

Une étude approfondie a montré qu'à chaque fois que la fréquence d'injection se rapproche d'un produit d'intermodulation entre cette même fréquence et la fréquence d'oscillation, une modification de la fréquence d'oscillation apparaît ainsi qu'une synchronisation de la raie d'intermodulation considérée. Ceci est illustré sur les figures suivantes, où l'observation du spectre de sortie se fait sur une large bande. Des intersections entre  $f_{inj}$  et des produits d'intermodulation d'expression  $\alpha \cdot f_{oct} + \beta \cdot f_{inj}$ , où  $\alpha$  et  $\beta$  sont des entiers relatifs, ont été mises en évidence. La figure 1.23 montre un exemple de vue locale au voisinage de  $f_{oct} / 2$ , pour lequel les conditions sont respectées pour garantir une synchronisation de la raie d'intermodulation.

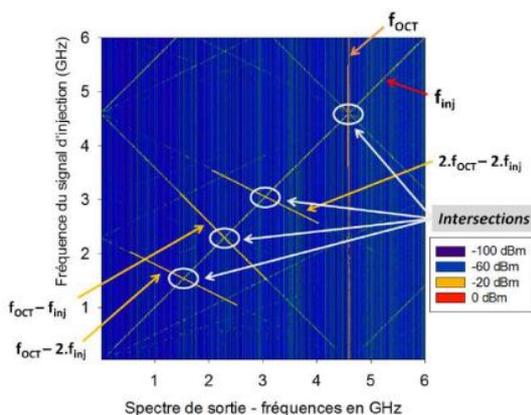


Fig. 1.22: Spectre de sortie de l'OCT sous injection large bande, de puissance 20 dBm

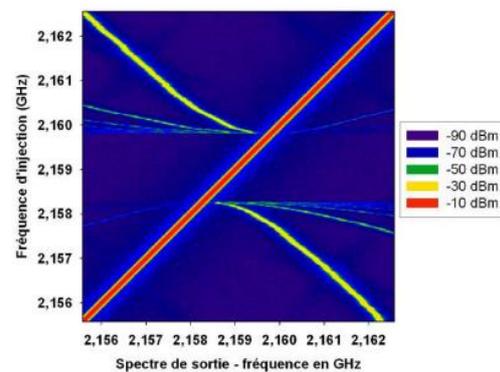


Fig. 1.23: observation du spectre au voisinage d'une raie d'intermodulation,  $f_{inj} \approx f_{oct} / 2$  (correspond au produit d'intermodulation  $f_{oct} - f_{inj}$ )

Des déviations de plusieurs dizaines de MHz ont pu être mises en évidence. Ces phénomènes sont évidemment exacerbés avec la puissance de l'injection. Les fréquences vulnérantes ont été identifiées, et doivent vérifier la relation suivante :

$$f_{inj} = \alpha \cdot f_{oct} + \beta \cdot f_{inj} , \text{ soit } f_{inj} = \frac{\alpha}{1-\beta} \cdot f_{oct} \text{ avec } (\alpha, \beta) \in \mathbb{Z}$$

Elles ne se limitent pas aux harmoniques et aux sous-harmoniques de  $f_0$ , mais peuvent intervenir sur des combinaisons rationnelles de  $f_{oct}$ .

Ces observations montrent une nouvelle fois le rôle fondamental des non-linéarités d'un circuit dans l'apparition et l'importance des effets induits par un signal d'interférence. Tous ces résultats d'injection dans et en dehors de la bande ont été publiés dans une conférence internationale [48].

Des expériences au niveau de la PLL ont été menées, avec les mêmes observables. Ce circuit PLL est un circuit mixte, il comporte une partie analogique (OCT), et une partie numérique (diviseur de fréquence et comparateur), comme illustré à la figure 1.24. Seul le filtre / correcteur n'est pas intégré au sein de la puce. La carte de test sur laquelle est soudée la puce est prévue pour sortir sur des connecteurs tous les signaux entrée et sortie de chaque bloc de la PLL (figure 1.25). Il est donc possible, de la même manière que pour l'étude de l'OCT, de placer des tés de polarisation sur les connecteurs afin d'injecter le signal d'interférence. Lors des travaux du stage post-doctoral de Tristan Dubois le circuit PLL était constitué de blocs discrets, regroupés sur un circuit imprimé. Les entrées et sorties des blocs n'étant pas accessibles par connecteurs, nous avons utilisé un banc de test avec injection en mode rayonné avec des sondes de champ proche [25].

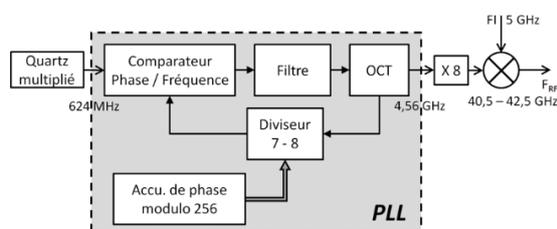


Fig. 1.24: Schéma fonctionnel du circuit PLL, fonctionnant à des fréquences autour de 5 GHz

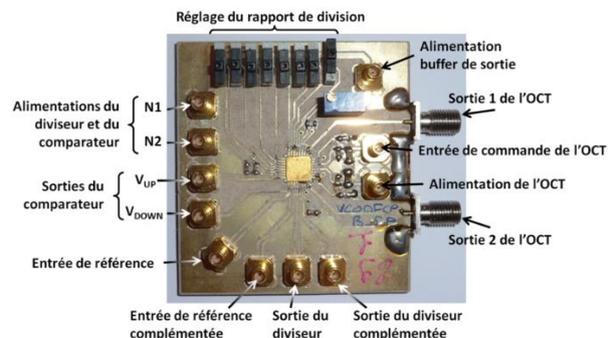


Fig. 1.25: Carte de test de la PLL

Les principaux résultats expérimentaux ont montré une disparition des phénomènes de synchronisation et de quasi-synchronisation du circuit, comme illustré sur la figure 1.26. Des raies d'intermodulation sont restées visibles. La PLL est parvenue à rester verrouillée à  $f_{oct}$  malgré la présence de l'interférence. Le déphasage supplémentaire induit dans l'OCT par le signal parasite a été corrigé par l'asservissement de la phase du circuit.

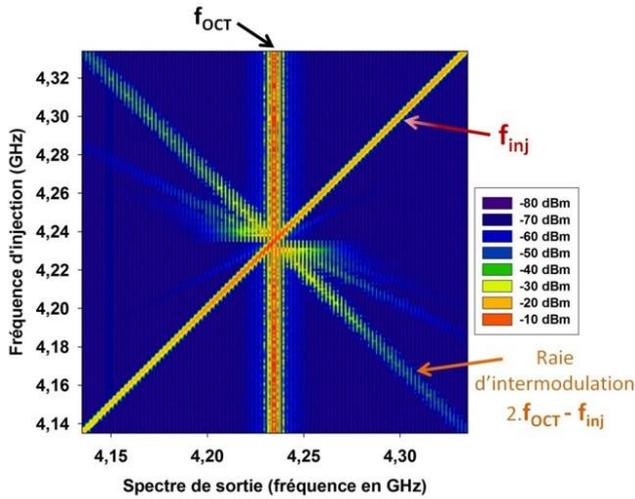


Fig. 1.26: Evolution du spectre de sortie de la PLL en fonction de  $f_{inj}$ , avec une puissance  $P_{inj}=15$  dBm

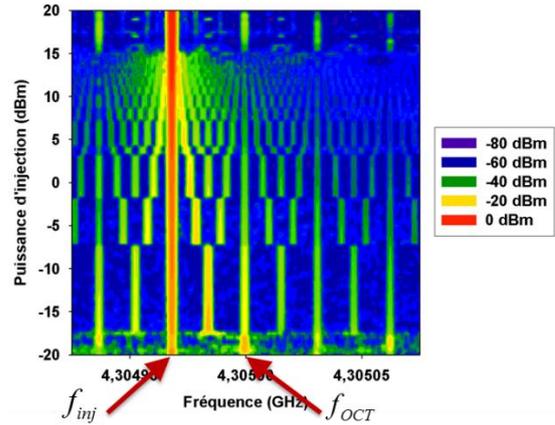


Fig. 1.27: Evolution du spectre de sortie de la PLL en fonction de la puissance de l'interférence  $P_{inj}$

Nous avons testé la susceptibilité de la PLL sous des injections de plus fortes puissances (voir figure 1.27), faisant apparaître de nouvelles raies. Leur nombre augmente avec le niveau de puissance injecté, et divise l'espace séparant la fréquence principale et la fréquence d'injection en deux subdivisions, puis quatre, et ainsi de suite jusqu'à atteindre un comportement erratique, voire chaotique [49].

Il a été montré durant le stage post-doctoral de Tristan Dubois que l'apparition de ces raies est reliée au facteur d'amortissement, pour un système d'ordre 2. Plus la PLL est amortie plus ces raies parasites sont atténuées. La figure 1.27 montre également clairement que le niveau de puissance de la fréquence  $f_{OCT}$  diminue au fur et à mesure que la puissance de  $f_{inj}$  augmente. L'énergie du système se répartie sur les très nombreuses nouvelles raies parasites. Dès que la puissance du signal injectée devient supérieure à celle de sortie, le comparateur de phase est en défaut puisqu'il va tenter de comparer la fréquence injectée à la fréquence de référence. Comme aucune correction n'est possible sur le signal injectée, la PLL s'est déverrouillée. Ceci met clairement en évidence un dysfonctionnement du circuit puisque ce dernier n'est plus parvenu à fournir un niveau de signal suffisant en sortie.

Ces expérimentations ont également été menées avec un signal impulsionnel avec porteuse, signal typique utilisé pour les armes électromagnétiques. Les mêmes phénomènes ont été mis en lumière. Le déverrouillage de la PLL a été possible durant le temps de l'impulsion. Sa susceptibilité a été réduite si la durée de l'impulsion est plus courte que la constante de temps du système.

### b) Prédiction des effets par la simulation

Comme pour les études composant, je me suis fortement impliqué dans la mise en place des outils de calcul analytique et numérique. L'objectif a été d'une part, de mettre en lumière les paramètres du circuit les plus influents sur sa susceptibilité, et d'autre part, de proposer des outils de simulation électrique permettant la prise en compte de certains critères de susceptibilité en accord avec les caractéristiques fonctionnelles du circuit (bruit de phase, réjection d'harmonique, consommation,...).

Dans le cas de l'OCT et d'après l'étude expérimentale, la largeur de la plage de synchronisation a été choisie comme critère de susceptibilité. La littérature apporte une formulation analytique de cette plage de fréquence, notée  $\delta f$ , dans laquelle la fréquence de l'OCT est complètement contrôlée par la fréquence du signal d'injection [46, 47] :

$$\delta f = \frac{f_{oct}}{Q} \cdot \sqrt{\frac{P_{inj}}{P_{oct}}}$$

La validité de cette expression impose un oscillateur simple conceptuel : un inverseur associé à une cellule résonante LC, une localisation de l'injection : le signal d'interférence est représenté par une source de courant équivalente appliquée en un point bien précis du circuit, et une injection de faible amplitude :  $P_{inj} \ll P_{oct}$ . Malgré ces hypothèses, qui ne correspondent pas rigoureusement à nos cas d'étude, la formulation simple proposée apporte un éclairage intéressant sur les paramètres clés du circuit responsables des effets. Afin de réduire cette plage de fréquence, il faut concevoir un circuit à fort facteur de qualité et à forte puissance de sortie. A partir de la topologie connue du circuit (figure 1.28), les paramètres internes au circuit permettant d'agir sur le facteur de qualité et la puissance de sortie sont le facteur de qualité des inductances ( $Q_L$ ), le courant de polarisation ( $I_{POLAR}$ ), et le taux de réaction imposé par le condensateur  $C_1$ .

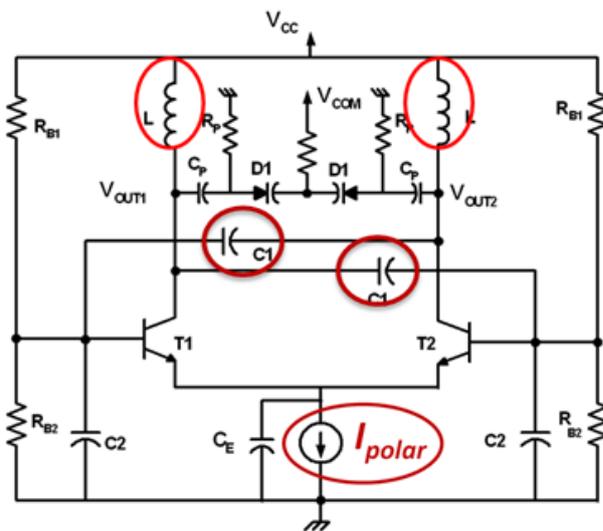


Fig. 1.28: Schéma électrique du l'OCT, basé sur une structure différentielle associée à un résonateur LC, indiquant les composants qui influencent le critère de susceptibilité

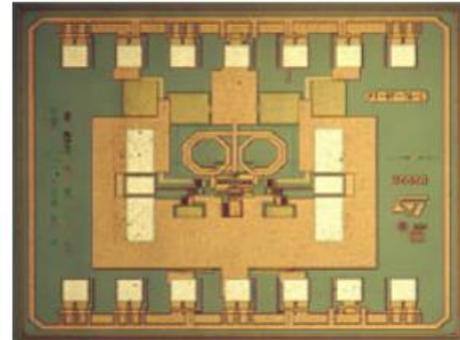


Fig. 1.29: Photographie du circuit intégré

La phase de simulation des effets induits a été menée en utilisant les modèles des composants passifs et actifs, validés en fort-signal, développés et validés durant ma thèse. Afin de reproduire le signal injecté, une source de puissance est placée sur les accès du circuit utilisés lors des expérimentations (commande, sortie, alimentation). La technique de simulation utilisée a consisté à faire varier linéairement la fréquence de la source, sur une plage autour de  $f_{oct}$ , et à mesurer pour chaque point de cette rampe de fréquence l'enveloppe du signal de sortie. En mode de synchronisation l'enveloppe

est quasiment continue, correspondant à la zone 2 de la figure 1.30, puisqu'il n'y a alors qu'une seule raie dans le spectre de sortie, et pas de phénomène de battement. La largeur de la plage de synchronisation est alors facilement extraite.

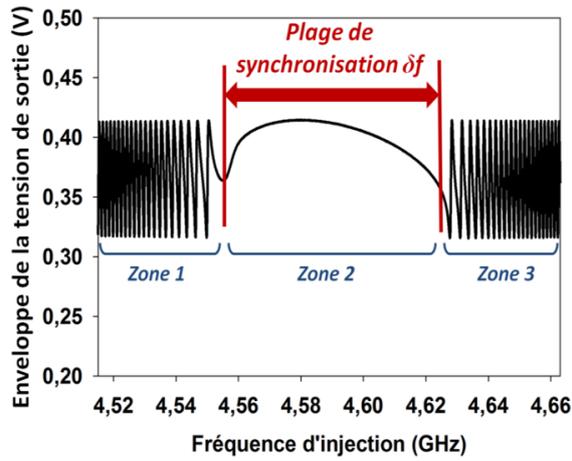


Fig. 1.30: Enveloppe de la tension de sortie sous injection, mettant en évidence la synchronisation et la quasi-synchronisation d'un OCT sous agression

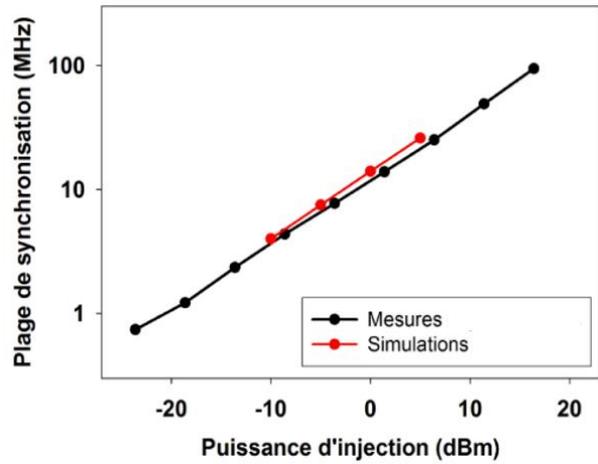


Fig. 1.31: Largeur de la plage de synchronisation, mesurée et simulée, en fonction de la puissance de l'agression, avec une injection sur la sortie de l'OCT

Cette méthode est efficace et rapide, et a été publiée dans une revue internationale [26]. Les résultats simulés et mesurés ont été comparés avec succès jusqu'à de fortes puissances d'injection, comme montré sur la figure 1.31.

Cet outil a ensuite été utilisé pour calculer l'évolution de la largeur de la plage de synchronisation avec les paramètres internes du circuit identifiés précédemment. Ceci permet d'obtenir des valeurs de paramètres qui optimisent la susceptibilité du circuit. Nous avons évalué l'influence des modifications envisagées sur les performances du circuit, en particulier sur le bruit de phase de l'OCT. L'évolution simulée de la largeur de la plage de synchronisation et du bruit de phase à 100 kHz de la porteuse,  $L(100 \text{ kHz})$  en dBc/Hz, en fonction du courant d'alimentation du circuit est présentée sur les figures 1.32 et 1.33.

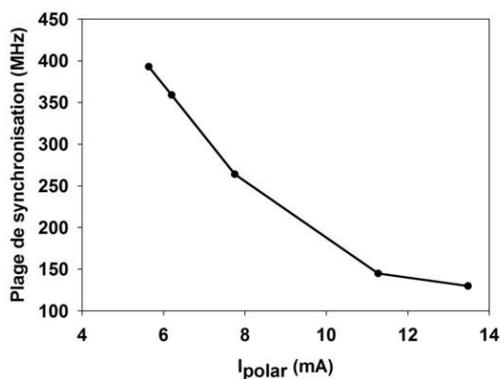


Fig. 1.32: Largeur de la plage de synchronisation en fonction du courant de polarisation

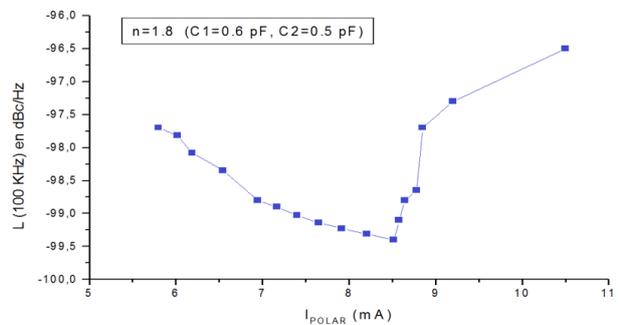


Fig. 1.33: Bruit de phase à 100 kHz de la porteuse en fonction du courant de polarisation

Les résultats de simulation de ces deux grandeurs en fonction des autres paramètres internes influents,  $Q_L$  et  $C_1$ , sont disponibles à la référence [50].

L'évolution du bruit de phase met clairement en évidence une valeur de courant de polarisation optimale, alors que la largeur de la plage de synchronisation diminue continuellement avec le courant de polarisation. Finalement, le concepteur de circuit a à disposition un outil de simulation lui permettant de prédire la susceptibilité du circuit, qu'il peut coupler avec les outils habituels de validation des performances fonctionnelles.

Les résultats présentés dans cette partie concernent des injections menées en mode conduit à des fréquences RF et micro-ondes sur des fonctions électroniques analogiques RF. Des effets ont été mis en évidence, même si les fréquences injectées sont relativement éloignées des fréquences de fonctionnement des circuits. Ceci a motivé la poursuite d'études de susceptibilité vers une montée en fréquence des signaux injectés.

#### 4) Injection aux fréquences millimétriques

Les travaux concernant la montée en fréquence de notre banc d'injection sont récents, ils ont débuté courant 2016 et ont fait l'objet d'une des deux parties de la thèse de Pierre Payet, qui a été soutenue fin 2018. Mathieu Guéry, stagiaire Master en 2017, a aussi participé à l'acquisition de nombreux résultats expérimentaux d'injection à très hautes fréquences, sur plusieurs échantillons de test. Ce banc est né de ma collaboration avec Laurent Chusseau, avec l'idée d'associer nos compétences, lui au niveau de l'instrumentation aux fréquences millimétriques, et moi sur les études de susceptibilité EM.

L'environnement électromagnétique actuel est principalement saturé par des ondes aux fréquences RF et micro-ondes [1]. Il va dans les années à venir s'enrichir davantage avec la recrudescence des communications aux fréquences millimétriques, comme le futur standard 5G ou la dernière génération wifi 802.11ad [51], qui sont en phase de développement. Les armes électromagnétiques tendent également à fonctionner jusqu'à des fréquences de 100 GHz [8, 14, 52], offrant ainsi une plus grande compacité. Ainsi les circuits actuels fonctionnant aux fréquences RF et micro-ondes devront cohabiter avec des signaux ayant des porteuses aux fréquences millimétriques. Ils n'ont évidemment pas été conçus et testés à des signaux de longueur d'onde de l'ordre du millimètre. Dans la littérature des premiers tests sur des bascules jusqu'à des fréquences de 40 GHz ont été conduits, mais à des niveaux de puissance relativement faibles [53]. La pénétration de ces ondes au niveau des puces peut être tout à fait facilitée car les défauts de blindage sont nettement plus importants à ces longueurs d'onde.

Nous avons ainsi voulu élargir la bande de fréquence de nos bancs de tests de susceptibilité, et envisager d'étudier les effets potentiels d'un signal d'interférence aux fréquences millimétriques.

Pour ce faire, nous avons mis en place un banc de test dédié à l'étude de la susceptibilité de l'électronique à une fréquence millimétrique.

### a) Mise en place du banc de test

Notre intention est de développer un banc de test dans lequel le signal d'interférence est injecté en mode rayonné au-dessus d'un circuit intégré. Cette méthode d'injection est sans contact, et donc ne nécessite aucune préparation particulière de la carte de test. L'injection au-dessus de la puce permet d'envisager un couplage de l'onde au plus près des non-linéarités, susceptibles de générer un effet.

Des calculs théoriques ont montré qu'une source à 60 GHz de puissance faible (20 dBm) rayonne à la sortie d'un guide d'onde [54- 56] un niveau de champ électrique tout à fait comparable à celui obtenu avec une source de forte puissance en champ lointain [16]. Une source utilisée en champ proche de l'objet sous test amène de la compacité au banc de test et un coût réduit. Un autre avantage est la possibilité d'injecter le signal localement dans la puce. Des cartographies peuvent alors permettre d'identifier les zones de la puce de plus grande vulnérabilité.

Nos premiers tests ont été conduits sur des circuits assurant l'amplification HF dans la chaîne d'émission-réception d'une communication sans-fil. Un seul circuit intégré, le front-end, placé juste derrière l'antenne et donc pouvant être particulièrement exposé à des signaux d'interférence réalise la fonction d'amplificateur bas bruit (LNA, Low-Noise Amplifier) pour la réception, celle d'amplificateur de puissance (PA, Power Amplifier) pour l'émission et celle de commutateur (switch) pour le choix de la configuration. Plusieurs front-ends commerciaux fonctionnant dans les bandes de fréquence usuelles grand public de 400 MHz à 5.1 GHz ont été testés.

La figure 1.34 présente le schéma du banc de test développé. Nous injectons une fréquence à 60 GHz à partir d'une source à oscillateur Gunn montée avec un guide d'onde rectangulaire WR15 (de taille 3.76 mm x 1.88 mm), au-dessus d'un circuit intégré, à des distances  $100 \mu\text{m} \leq h \leq 2 \text{ mm}$ , qui sont bien en-dessous de la longueur d'onde ( $\lambda \approx 5 \text{ mm}$  à 60 GHz). La puissance disponible au niveau de la puce est ainsi modulée selon la hauteur guide – puce. La source utilisée peut être modulée en tout-ou-rien, avec une fréquence de répétition maximale de 20 kHz, permettant de tester la susceptibilité du circuit en mode continu et en mode impulsionnel.

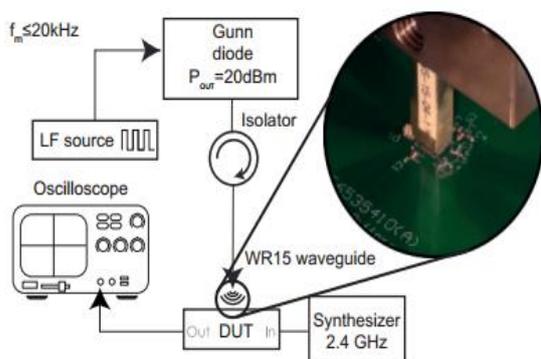


Fig. 1.34: Schéma du banc expérimental d'injection à 60 GHz sur un front-end RF fonctionnant à 2.4 GHz



Fig. 1.35: Photographie du banc (les appareils de mesure ne sont pas placés)

Les tests sont toujours menés avec le circuit en fonctionnement nominal. Un synthétiseur délivre le signal utile à 2.4 GHz, que le circuit doit amplifier soit avec le LNA soit avec la PA. Les caractéristiques fonctionnelles du circuit mesurées sont le courant d'alimentation du circuit (le multimètre n'est pas représenté sur la figure) et sa sortie observée en temporel avec un oscilloscope rapide pour suivre les comportements en régime transitoire et permanent.

Le positionnement 3D relatif du guide d'onde au-dessus du circuit est réalisé par des moteurs de résolution micrométrique, ce qui permet d'établir la cartographie des zones vulnérables du circuit. Pour évaluer l'influence de l'orientation du guide par rapport à la puce, une bague crantée de rotation est fixée sur l'axe Z. Le guide peut ainsi tourner avec une précision au degré par rapport à la puce. Ce degré de liberté amène de la compréhension pour appréhender le problème du couplage du champ rayonné en sortie de guide, qui est polarisé, sur la puce, dont les cibles potentielles (pistes) sont orientées.

### b) Résultats d'injection sur un RF front-end Wifi

Le mode opératoire consiste à déplacer le guide avec un pas faible devant les dimensions de la puce, au-dessus de l'intégralité de la surface de la puce en injectant le signal à 60 GHz, et à mesurer la sortie de la fonction testée. La figure ci-dessous présente un oscillogramme de la tension en sortie du PA à la position du guide pour lequel l'effet est le plus intense, et pour trois hauteurs guide-puce.

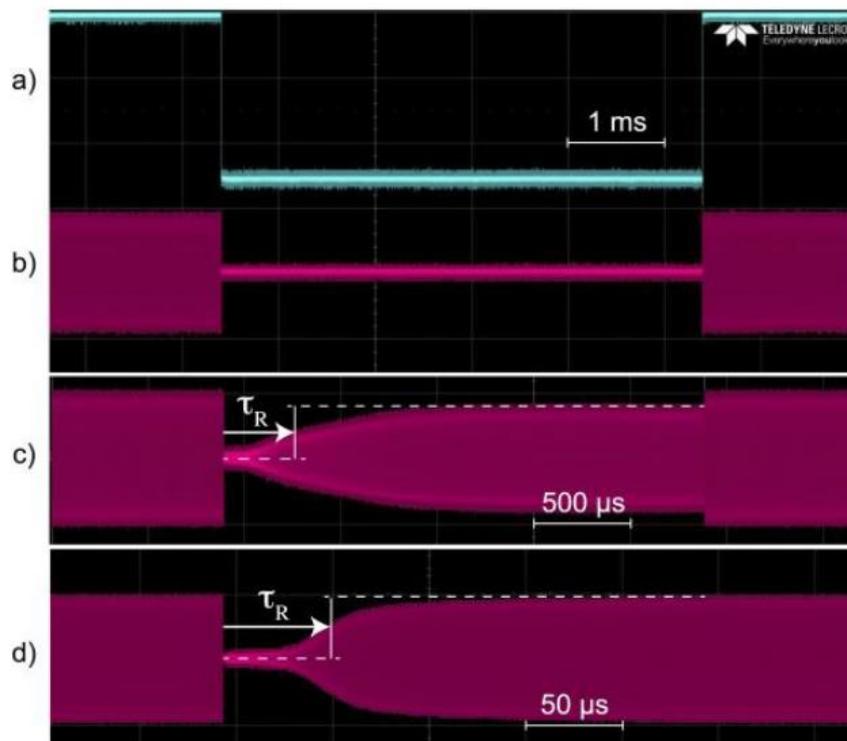


Fig. 1.36: Oscillogramme de la sortie du PA, à la position optimale, avec 3 hauteurs  $h$  guide-puce, a) signal de commande de la source, b)  $h=100 \mu\text{m}$ , c)  $h=1100 \mu\text{m}$  et d)  $h=1200 \mu\text{m}$ .

Le signal impulsionnel utilisé pour moduler la source est suffisamment lent pour observer le comportement en régime transitoire et permanent. A l'état bas de ce signal de commande, la source est activée, et la tension de sortie diminue jusqu'à éteindre complètement (figure 1.36 (b)) et de façon permanente la fonction d'amplification.

Quand la hauteur augmente, une plus faible puissance est injectée au niveau de la puce. Au moment du front d'activation de la source, l'extinction de la fonction est observée. Mais cet état ne dure pas, et l'établissement progressif à un niveau permanent inférieur au niveau normal sans l'injection apparaît. A la dernière hauteur testée, ce niveau permanent sous injection a presque rejoint la valeur de tension normale. Il reste cependant toujours l'effet transitoire qui apparaît au moment du front d'activation de la source 60 GHz. Un temps de récupération  $\tau_R$ , propre au circuit, défini comme le temps nécessaire pour récupérer 50 % du niveau permanent atteint sous injection, est mis en évidence. Plus  $\tau_R$  est élevé, plus la perturbation est efficace, et la cible est inhibée sur une échelle de temps plus longue. Ce temps  $\tau_R$  tend à diminuer avec la puissance injectée. Le détail de ces expérimentations a été publié dans une revue et une conférence internationale [56, 57]. Notons que dans tous les cas testés, le circuit fonctionne tout à fait normalement dès que la source est éteinte.

De ces résultats nous avons défini une grandeur, un taux d'extinction ( $\alpha_{CW}$ ), qui quantifie en mode CW le rapport entre l'amplitude de sortie sous injection ( $A_{UNP}$ ) et celle sans injection ( $A_P$ ). Cette grandeur, indicateur de l'effet de signal 60 GHz sur une fonction amplificateur HF, peut être comparée sur plusieurs autres circuits, de caractéristiques de fonctionnement différentes (fréquence, technologie, ...). Ce taux d'extinction  $\alpha_{CW} = 1 - \frac{A_P}{A_{UNP}}$  permet de caractériser les effets observés en fonction des conditions expérimentales : la hauteur guide-puce (figure 1.37), et l'angle de rotation du guide (figure 1.38), qui constituent des paramètres essentiels d'un couplage champ proche.

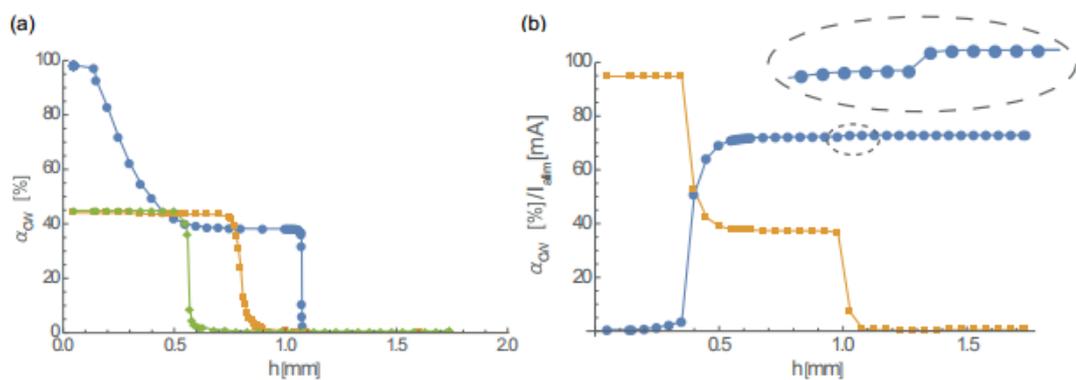


Fig. 1.37: (a)  $\alpha_{CW}$  (%) en fonction de la distance guide-puce, pour deux positions  $M_{OPT}(PA)$  ( $\bullet, \blacklozenge$ ),  $M_{OPT}(LNA)$  ( $\blacksquare$ ). (b)  $\alpha_{CW}$ (%) ( $\blacksquare$ ) et  $I_{alim}$  ( $\bullet$ ) en fonction de la distance guide-puce, pour la fonction PA

La fonction PA est la plus vulnérable sur cette puce, une extinction complète ( $\alpha_{CW}=100\%$  comparé à  $\alpha_{CW}=45\%$  pour le LNA) est possible à une position particulière. La sensibilité des fonctions diminue avec la hauteur mais pas avec une décroissance typique du champ rayonné par une sonde en

champ proche (en  $1/h^3$ ). Les paliers de sensibilité observés confirment le caractère non-linéaire de la conversion opérée entre le champ couplé sur la puce et la diminution de la tension de sortie, ou comme représenté sur la figure 1.37 (b), la diminution du courant d'alimentation du circuit ( $I_{\text{alim}}$ ).

D'ailleurs cet abaissement brutal du courant continu observé lorsque le guide est le plus proche de la puce fait fortement penser au phénomène de redressement déjà évoqué en début de ce chapitre. La baisse de la tension de sortie (donc du gain du montage) et celle du courant d'alimentation sont fortement corrélées, et apparaissent aux mêmes hauteurs. Notons qu'à partir du millimètre la puissance couplée sur la puce est trop faible pour induire un effet mesurable.

Ces tests d'injection ont montré que la sensibilité dépend de la position spatiale du guide au-dessus de la puce. Notre système d'injection en champ proche permet de générer des perturbations locales alors que l'ouverture du guide est sensiblement la même que la taille de la puce. Chaque fonction a une position spatiale à laquelle l'effet est optimal, notée  $M_{\text{OPT}}(\text{LNA})$  et  $M_{\text{OPT}}(\text{PA})$ . Ces 2 points sont espacés de  $300 \mu\text{m}$ , ce qui pourrait correspondre à la distance séparant les deux fonctions intégrées sur la puce. A la position  $M_{\text{OPT}}(\text{PA})$  nous avons mesuré l'effet sur le LNA (courbe  $\blacklozenge$ ). La sortie est impactée mais l'effet cesse pour des hauteurs plus faibles que dans le cas du positionnement optimal du guide.

L'influence de l'orientation du guide par rapport à la puce a été étudiée. Nous nous sommes placés à la position  $M_{\text{OPT}}(\text{PA})$  où une extinction de la fonction PA est complète, puis l'angle de rotation du guide  $\theta$  a été modifié (figure 1.38)

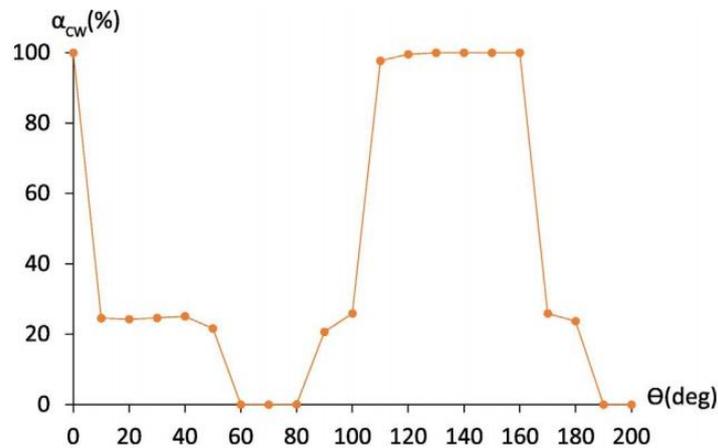


Fig. 1.38: Taux d'extinction en fonction de l'angle de rotation du guide

La sensibilité est très fortement dépendante de la polarisation du champ rayonné en sortie de guide. Le taux d'extinction peut évoluer de 100 % à 0% (pas d'effet), avec une périodicité proche de  $180^\circ$ . Ce comportement fait penser au couplage champ – ligne avec un champ de polarisation linéaire projeté sur un fil de bounding ou sur les rails d'alimentation. En tournant le guide, la projection du champ le long de la ligne est plus ou moins efficace quant au courant induit au sein du circuit, et/ou change d'une ligne à une autre. Une plus faible quantité de signal couplée et propagée dans les circuits induira après conversion par les non-linéarités intrinsèques des composants actifs une baisse de la sensibilité. Des

paliers sont une nouvelle fois observables, et rappellent le rôle des non-linéarités dans le processus de conversion du signal d'injection.

### c) Vers une interprétation des résultats

De manière très intuitive nous aurions pu penser que les conversions non-linéaires au sein du circuit seraient peu efficaces, sachant que le signal couplé fluctue à des fréquences très élevées comparativement aux fréquences de fonctionnement du circuit. Cependant dans les conceptions de circuit, il est maintenant courant d'intégrer des transistors ayant des fréquences de transition très élevées, de l'ordre de la centaine de GHz, même pour fonctionner beaucoup plus bas en fréquence.

Le signal induit à 60 GHz a certes de nombreux chemins possibles au cœur du circuit, cependant il n'y a aucune raison que les non-linéarités soient shuntés. De fortes variations de courant d'alimentation peuvent être ainsi générées par un mécanisme de redressement.

Pour confirmer ces comportements observés, j'ai commencé durant la thèse de Pierre Payet des premières simulations électriques. Comme le schéma interne et le dessin des masques du circuit sont inconnus, il est très ambitieux de viser une prédiction précise des effets observés. L'objectif est déjà de parvenir à reproduire de manière qualitative les comportements expérimentaux.

J'ai ainsi utilisé un schéma typique de LNA dont les caractéristiques électriques fonctionnelles ont été ajustées au circuit testé. N'ayant pas de modèle de couplage complet qui prend en compte la nature vectorielle du champ électromagnétique rayonné, un simple modèle de couplage capacitif entre la source et une piste d'alimentation du LNA a été utilisé.

Les premiers résultats montrent qu'il a été possible de reproduire en mode CW des variations du courant d'alimentation et du gain, avec des ordres de grandeur proches de ceux trouvés en expérimental, à condition d'utiliser un modèle de transistors ayant une  $f_T$  supérieure à 60 GHz, et d'injecter à des endroits particuliers du circuit.

Le principal point sensible a été identifié au niveau des pistes d'alimentation à l'entrée du miroir de courant du circuit, comme cela a été également observé sur des travaux d'injection en BF concernant la vulnérabilité de circuits analogiques [58]. Une fois le signal couplé (noté  $i_{HF}(t)$  sur la figure 1.39), le signal haute fréquence peut circuler dans les capacités parasites ou internes aux transistors (représentées par la capacité équivalente C sur la figure 1.39), créant ainsi une tension de commande du transistor M2, qui impacte le courant continu de sortie  $I_{OUT}$  en raison de la non-linéarité I-V de M2 [59, 60]. Le signal interférant peut ainsi se propager vers la sortie du miroir et corrompre le courant d'alimentation de l'amplificateur, entraînant une baisse du gain. Les inductances parasites du circuit peuvent induire des résonances particulièrement marquées aux très hautes fréquences, et qui par conséquent renforcent les effets comme observé sur la figure.

La figure 1.40 montre une simulation de la variation du courant de sortie du miroir  $\Delta I_{OUT}$  en fonction de la fréquence d'un signal d'interférence de forme sinusoïdale, et avec 2 niveaux d'amplitude (de valeur crête-à-crête  $i_{HF-c} = 8 \text{ mA}$  et  $i_{HF-c} = 10 \text{ mA}$ ).

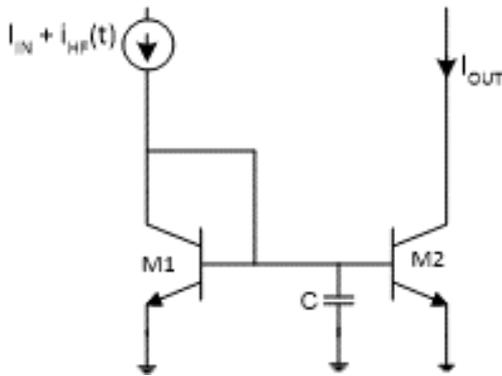


Fig. 1.39: Miroir de courant simplifié.  $I_{IN}$  est le courant continu de référence,  $i_{HF}(t)$  est le signal couplé sur une piste d'alimentation.  $I_{OUT}$  est le courant d'alimentation de l'amplificateur. C représente la capacité équivalente à l'entrée de M2

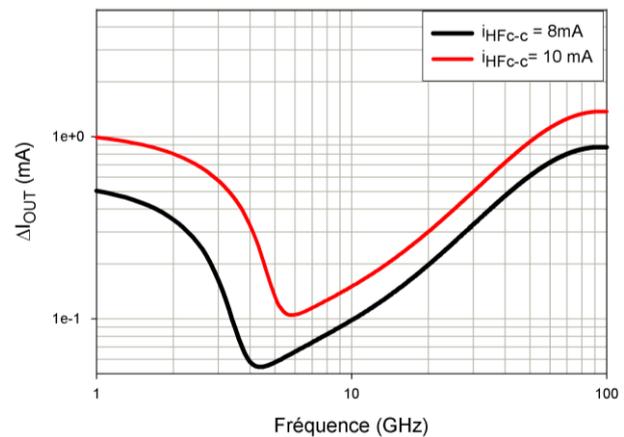


Fig. 1.40: Simulation de la variation du courant d'alimentation  $\Delta I_{OUT}$  en fonction de la fréquence du signal d'interférence.  $i_{HF}(t)$  est un signal sinusoïdal, d'amplitude crête-à-crête 8 mA et 10 mA

Avec ces niveaux d'amplitude du signal interférant à 60 GHz, il est possible par simulation de générer une variation de l'ordre du mA sur le courant d'alimentation du LNA ou du PA. Ces résultats préliminaires donnent des réponses intéressantes sur une des origines de la dégradation du gain observée.

Ces premiers résultats laissent présager une sensibilité accrue sur des circuits intégrant des technologies de composants de plus en plus rapides.

#### d) Etude paramétrique de la sensibilité de puces RF front-ends

Nous avons élargi l'étude à plusieurs circuits commerciaux, sélectionnés selon certaines caractéristiques techniques : la bande de fréquence de fonctionnement, l'épaisseur du boîtier, et le courant d'alimentation du LNA et celui du PA. Les particularités de chaque puce doivent permettre d'identifier et de trier des paramètres influents sur la susceptibilité à des interférences très haute fréquence. La fréquence de fonctionnement du circuit peut être un paramètre influent puisqu'à priori, plus la fréquence d'injection s'éloigne de la fréquence de fonctionnement d'un circuit meilleure est son immunité. De nombreux chemins sont proposés au signal couplé, pouvant ainsi l'empêcher de se propager vers les composants actifs. Une gamme significative de fréquence a été choisie, elle s'étend sur plus d'une décade, de 400 MHz à 5.1 GHz.

L'épaisseur du boîtier est un paramètre à considérer en raison de l'injection faite en champ proche. Toutes les puces sont surmoulées avec du plastique puis encapsulées dans des boîtiers type QFN. Une large épaisseur implique une augmentation de la distance guide-puce, donc une puissance du signal rayonné plus faible au niveau de la puce (zone active).

Enfin, le courant d'alimentation est un paramètre clé de la fonction considérée, il détermine la plupart de ses caractéristiques dynamiques et il fixe le régime de fonctionnement plus ou moins non-linéaire des composants actifs.

Sept front-end RF commerciaux du même fabricant (Qorvo) ont été testés selon le protocole défini précédemment. Ce travail expérimental a été confié à un stagiaire Master, et nous a permis d'avoir une étude de la sensibilité d'une famille de front-ends. Les taux d'extinction ont été relevés et comparés selon les paramètres choisis. Les résultats sont présentés sur la figure 1.41.

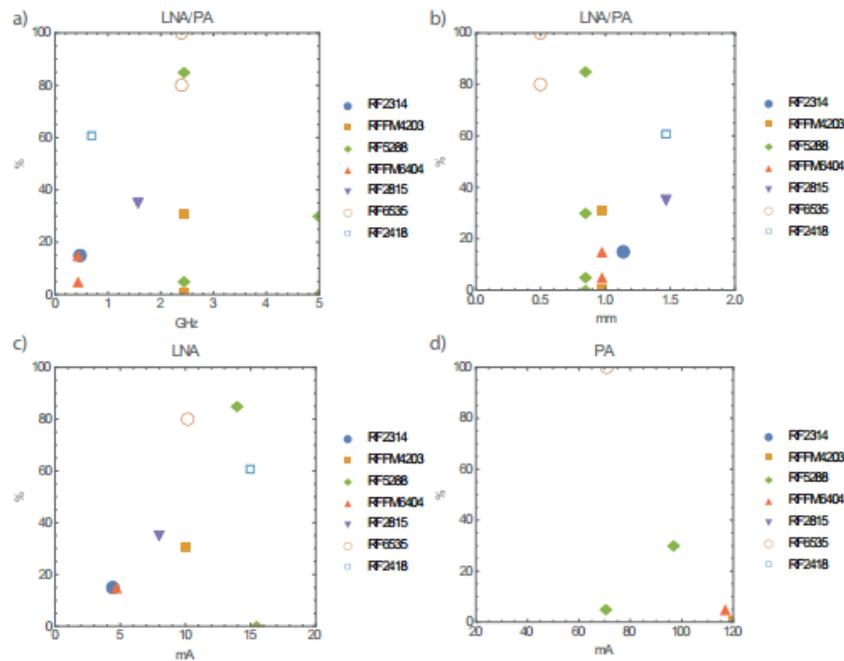


Fig. 1.41:  $\alpha_{CW}$  de 7 références de front-end en fonction de : a) la fréquence de fonctionnement, b) l'épaisseur du boîtier, c) du courant d'alimentation pour les LNAs, d) du courant d'alimentation pour les PAs

De ces tracés, publiés dans une revue internationale [61], nous pouvons tirer quelques règles générales de comportement, valables pour un même fabricant. Toutes les cartes ont été touchées, celles qui ont la plus grande sensibilité fonctionnent à 2.4 GHz (figure 1.41 (a)), et ont les épaisseurs de boîtier les plus faibles (figure 1.41(b)). La fonction LNA semble être la plus vulnérable comparativement aux PAs (figure 1.41 (c) et (d)). Les circuits les plus sensibles sont ceux dont le courant d'alimentation est le plus fort pour les LNAs et le plus faible pour les PAs.

Notons que d'autres paramètres auraient pu être pris en compte dans cette étude, comme la technologie des transistors intégrés, ou le matériau utilisé. Cela pourrait mettre en évidence une vulnérabilité accrue selon la filière et le nœud technologique. Les puces sont souvent constituées de modules à plusieurs puces (solution Multi-chip module). Les technologies et matériaux sont souvent différents, les principales filières technologiques utilisées sont les HBT en SiGe ou InGaP et des pHEMT en GaAs. Une classification des vulnérabilités selon les technologies pourrait amener des indications supplémentaires utiles lors de la conception du circuit. Quoiqu'il en soit, les effets révélés semblent être fortement dépendants de la topologie, du dessin des masques des circuits, et du choix des composants.

Finale­ment plus aller plus loin, une compréhension fine des mécanismes observés expérimentalement ne pourra être envisagée qu'avec une collaboration étroite avec un fondeur de circuits.

### 5) *Bilan et perspectives*

Ce chapitre met en avant les méthodes de travail que nous avons développées pour étudier la susceptibilité de composants et de fonctions électroniques. Une approche expérimentale est favorisée, avec la mise en place de bancs de tests où le signal d'interférence est injecté soit en mode conduit soit en mode rayonné en champ proche. Une fois la susceptibilité révélée et caractérisée j'ai mis en place des moyens de calcul théorique et de simulation électrique pour contribuer à une meilleure compréhension des phénomènes mis en jeu et tendre vers une prédiction des effets.

Une prise en compte des non-linéarités internes au dispositif testé est nécessaire puisque celles-ci sont à l'origine de distorsions qui affectent les performances fonctionnelles. L'analyse et la modélisation des effets induits restent bien évidemment une tâche très importante à mes yeux, et continuera à être développée dans la suite, sachant entre autres que la technologie des composants évolue et que les formes d'onde sont arbitraires.

L'injection à des fréquences millimétriques a été récemment menée et répond à une évolution de l'environnement électromagnétique qui s'enrichit des très hautes fréquences tant pour les communications sans fil à très haut débit que pour les armes à énergie dirigée destinées à neutraliser l'électronique.

A notre connaissance, nous sommes les premiers à avoir testé la sensibilité d'un front-end Wifi 2.4 GHz et 5.1 GHz à une fréquence de 60 GHz. Désormais ce banc d'injection millimétrique est opérationnel, et nous projetons de l'utiliser sur d'autres dispositifs, par exemple sur les systèmes de communication plus modernes, à échantillonnage direct où le convertisseur analogique/numérique se rapproche de l'antenne de réception, et peut ainsi devenir fortement exposé aux ondes EM.

Nous voulons également nous diriger vers des tests sur des circuits programmables. Des premiers tests ont été engagés sur des circuits type FPGA. Ce travail préliminaire a été réalisé lors du stage Master de Mathieu Guery auquel nous avons associé un collègue de l'équipe Radiac, Vincent Pouget, spécialiste des composants complexes. Deux structures de tests, un registre à décalage et un oscillateur à anneau, ont été implantées dans le circuit. L'injection du signal à 60 GHz n'a pas mis en évidence de perturbations franches dans le fonctionnement des circuits (modification du délai de propagation des portes, décalage de la fréquence d'oscillation, ...). Il est prévu de renouveler ces tests avec une puissance de la source plus élevée. Une campagne de mesure avec une source 60 GHz forte puissance (1W) est prévue fin 2018, avec un collègue de l'IMS à Bordeaux, et nous envisageons l'achat d'une extension en puissance de la source existante. Nous en attendons une plus grande efficacité dans l'évaluation de la sensibilité de tout type de circuit aux très hautes fréquences.

## Chapitre 2. Détection d'une électronique RF à distance en exploitant les susceptibilités

Les études de perturbations de circuit par injection de signaux présentées jusqu'à présent dans le mémoire, trouvent leur application dans le domaine de la défense, en particulier pour améliorer les techniques de brouillage des équipements. Cependant, en amont de la neutralisation de l'électronique, il peut y avoir un intérêt à la détecter, et si possible à distance. Le savoir-faire et l'expertise dans l'injection de signaux et l'analyse des effets induits sur l'électronique m'ont permis de démarrer une collaboration avec la société Thalès –SIX (Systèmes d'information et set de communications sécurisés) avec laquelle nous avons déjà collaboré durant la thèse d'Adrien Doridant soutenue début 2013.

Cette nouvelle activité de recherche, complémentaire de celle présentée jusqu'ici, vise à étudier et mettre en œuvre des solutions techniques pour détecter de l'électronique communicante cachée, et à distance. Elle a débuté en 2015 avec une collaboration entre l'IES et Thalès –SIX, et a donné lieu au stage de master 2 puis à la thèse CIFRE-ANRT d'Alexandre Martorell.

Thalès est fortement positionné sur le secteur d'activité de la sécurité des biens et des personnes. La détection d'électronique est cruciale dans de nombreuses applications, notamment lorsque la sécurité des personnes est engagée (colis suspect déclenché par un dispositif électronique, lutte anti-engins explosifs improvisés), ou dans le cadre de la guerre électronique (afin d'obtenir des informations à distance sur le dispositif adverse pour une meilleure efficacité du brouillage).

Thalès a d'abord travaillé dans le cadre d'un PEA avec la DGA sur la mise en place d'un système de détection basé sur un radar harmonique. Cependant, cette méthode s'avère incomplète car limitée dans sa capacité de discrimination. L'objectif principal de la collaboration est donc de développer une nouvelle méthode de détection particulièrement adaptée à la discrimination des récepteurs RF.

### *1) Radars déployés pour la détection de jonction, d'électroniques et de systèmes RF*

La première difficulté dans la détection d'électronique potentiellement portable réside dans la petite taille des cibles. Un radar conventionnel (ou linéaire) a trop peu d'efficacité dans la détection des objets à très faible surface équivalente radar [62]. Le radar non-linéaire exploite les propriétés non-linéaires de la cible à des fins de détection [63]. Or, tout système électronique étant non-linéaire, il va réémettre un signal de fréquence différente de celle de l'illumination. La récupération de ce signal permet de valider de la présence d'un objet ayant une caractéristique non-linéaire [64]. Comparé au radar conventionnel cette méthode garantit une meilleure réjection des réponses parasites de l'environnement.

Le radar à harmonique 2 (noté H2) est le radar non-linéaire le plus utilisé [65, 66]. Il a montré de bonnes capacités de détection d'êtres vivants (piétons, insectes) [67- 69], de dispositifs contenant des métaux (détection du degré de corrosion d'un métal) [70], des semi-conducteurs (détection de jonctions

pn) [71]. Il exploite la réémission de la cible à l'harmonique 2 de la fréquence d'illumination. Ces radars émettent à une fréquence fixe, qui n'est évidemment pas forcément comprise dans la bande passante de fonctionnement de la cible, surtout s'il s'agit d'un récepteur RF qui par nature a une bande passante très étroite. Le couplage de l'onde incidente se fait alors préférentiellement par les ouvertures (couplage « back-door »), et sur les pistes des circuits [72]. Le signal induit au cœur du circuit se propage jusqu'à des non-linéarités, qui génèrent une distorsion dont la composante à l'harmonique 2, rayonnée par les pistes, est captée à distance par le récepteur du radar.

Comparé à un radar conventionnel, la puissance à la cible nécessaire pour générer un rapport signal-à-bruit comparable est beaucoup plus élevée. Les puissances utilisées à l'émetteur du radar sont donc généralement très fortes. Des valeurs dépassant les 50 dBm sont fréquemment rencontrées dans la littérature [66, 73].

Dans le cas d'une détection d'objets communicants, il semble judicieux d'utiliser la voie de couplage la plus directe, c'est-à-dire par l'antenne du système. Le premier étage non-linéaire juste derrière l'antenne, le front-end génère une distorsion dont une partie peut être réémise par l'antenne [74], et finalement captée par le radar.

C'est cette technique qui a fait l'objet du travail de recherche que j'ai initié avec Thalès et réalisé avec Alexandre Martorell.

Nous avons opté pour une détection d'une raie d'intermodulation car cette raie peut être très proche des deux fréquences d'excitation et donc peut être réémise par l'antenne du dispositif RF sans perte par désadaptation. Finalement, le principe de fonctionnement du radar retenu consiste à émettre deux fréquences de valeurs proches  $f_1$  et  $f_2$ , et à capter un produit d'intermodulation opéré au niveau du front-end RF de la cible et rayonné par l'antenne de la cible. La raie d'intermodulation d'ordre 3,  $2f_1-f_2$  ou  $2f_2-f_1$ , est privilégiée car elle a la plus grande amplitude à faible niveau de puissance d'excitation de l'étage non-linéaire. De plus si l'écart de fréquence  $\Delta f=f_2-f_1$  est petit, la raie d'intermodulation d'ordre 3, noté IM3, est également séparée de  $\Delta f$  de  $f_1$  ou de  $f_2$ , elle reste donc dans la bande passante du récepteur. Une illustration du principe de détection par l'harmonique 2 et de celle par l'intermodulation est présentée sur la figure 2.1.

Le mode de couplage par l'antenne impose l'utilisation de fréquences agiles à l'émission pour détecter plusieurs cibles placées dans l'environnement. Le système radar doit donc proposer un balayage en fréquence, à dimensionner selon les standards de communications à détecter.

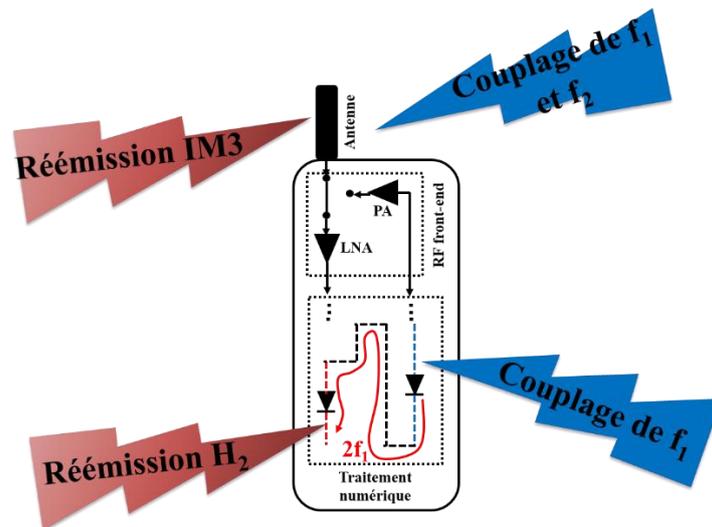


Fig. 2.1: Illustration des deux techniques de détection non-linéaire, utilisant l'harmonique 2 ou l'intermodulation d'ordre 3

En matière de portée de détection, le radar H2 a un bilan de liaison théorique en  $1/r^6$ , plus favorable que celui du radar IM3, qui lui, évolue en  $1/r^8$  [75]. Cependant, on peut espérer avoir une quantité de puissance susceptible de se coupler sur la cible bien supérieure avec le radar IM3. Les performances attendues vont donc évidemment dépendre de la quantité de puissance réémise à la fréquence de l'intermodulation, et donc finalement de la vulnérabilité du front-end de l'équipement à une excitation à 2 fréquences.

Cette susceptibilité à l'intermodulation de l'équipement se situe au cœur de la problématique d'un radar à détection de l'IM3 [76].

## 2) Mise en place d'un banc de test de radar à intermodulation

Le banc de test développé doit montrer la faisabilité d'une détection d'un récepteur RF par l'intermodulation. La bande de fréquence de travail actuelle s'étend de 300 MHz à 2.5 GHz. Elle correspond aux fréquences de fonctionnement typiques de la plupart des cibles RF.

Cette preuve de faisabilité passe d'abord par une étude préliminaire fondamentale portant sur la susceptibilité à l'intermodulation d'un récepteur RF, non pas en transmission mais cette fois en réflexion.

Il est connu qu'un front-end RF génère une distorsion d'intermodulation lorsqu'il est excité par deux fréquences. Les concepteurs de circuits de LNA ou de PA utilisent le test à deux fréquences pour caractériser ce type de distorsion et extraire des facteurs de mérite de la linéarité du circuit tel le point d'intersection d'ordre 3 (l'IP3) [77]. Cependant, ce test est toujours mené en mode transmis. Or la configuration de test du radar est basée sur la mesure d'une raie d'intermodulation réémise par le circuit.

La susceptibilité à l'intermodulation de récepteurs RF, cette fois en mode réfléchi, est donc à évaluer et à caractériser.

Ce travail a mené au développement d'un banc de test en mode conduit de l'intermodulation en réflexion (figure 2.2). La mise en place de ce banc et son utilisation sur un modem commercial ont été les principales activités que j'ai menées avec Alexandre Martorell durant son stage Master.

Ce travail original a abouti à deux récompenses, les prix régional et national Andrée Blanc-Lapierre en 2014. L'injection en mode conduit est privilégiée, afin de s'affranchir des pertes de couplage et donc de mesurer directement la raie d'intermodulation réfléchie à l'entrée du circuit sous test. Ce banc entièrement automatisé permet, à l'image d'un test à deux fréquences classiques, de mesurer l'amplitude de la puissance de la raie d'intermodulation d'ordre 3 (IM3) sur une plage large de puissance d'entrée aux fréquences  $f_1$  et  $f_2$ . Le coupleur bi-directionnel permet de diriger le signal de retour du circuit RF vers l'analyseur de spectre, réglé pour mesurer l'amplitude de la raie à l'IM3.

Afin d'expliquer la présence de cette raie à l'entrée d'un circuit non-linéaire alors que ce dernier est parfaitement adapté en impédance aux fréquences incidentes  $f_1$  et  $f_2$ , je me suis occupé, en y associant Alexandre Martorell, à la réalisation de calculs théoriques et de simulations électriques. Le détail de ces travaux a été publié dans une revue internationale [76] et une conférence internationale [73].

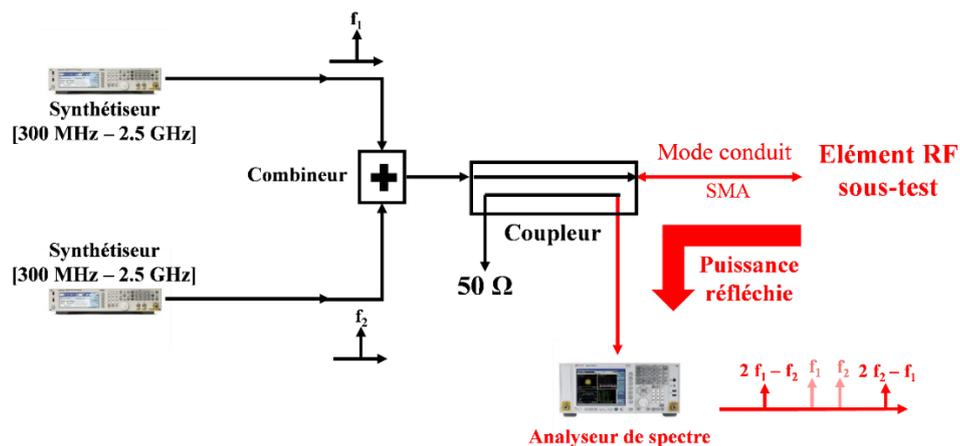


Fig. 2.2: Schéma expérimental permettant la mesure de la puissance réfléchie (au fondamental et à l'IM3) par les systèmes RF sous-test

De nombreux circuits ont été testés, du front-end intégré seul au système RF (talkie-walkie), dans le but d'évaluer la susceptibilité à l'intermodulation en mode réfléchi et de la comparer au mode transmis. Une très faible susceptibilité à l'intermodulation révélerait une difficulté d'utiliser la méthode de détection par l'intermodulation. Voilà pourquoi la mesure des niveaux de puissance possible en mode réflexion est fondamentale dans l'optique de la mise en place du radar.

Un exemple de mesure de la puissance à l'IM3 en mode transmis et en mode réfléchi sur un même front-end RF est présenté sur les figures 2.3 et 2.4.

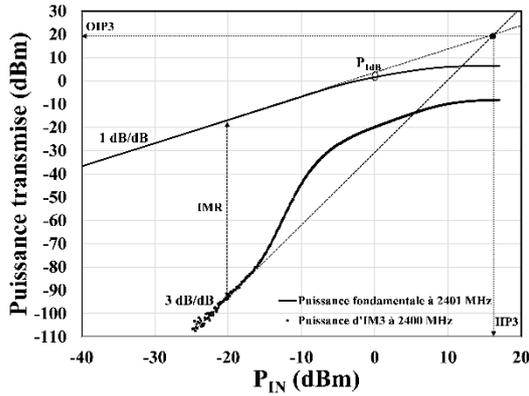


Fig. 2.3: Niveau de puissance de l'IM3 et du fondamental en mode transmis d'un front-end RF commercial, configuré en récepteur, en fonction de la puissance en sortie des synthétiseurs.  $f_1 = 2401$  MHz et  $f_2 = 2402$  MHz. La fréquence de l'IM3 est à 2400 MHz

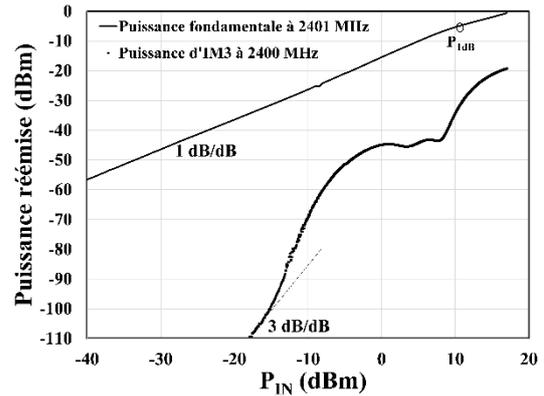


Fig. 2.4: Niveau de puissance de l'IM3 et du fondamental en mode réfléchi d'un front-end RF commercial, configuré en récepteur, en fonction de la puissance en sortie des synthétiseurs.  $f_1 = 2401$  MHz et  $f_2 = 2402$  MHz. La fréquence de l'IM3 est à 2400 MHz

Des comportements similaires sont observés, avec des niveaux de puissance à l'IM3 relativement proches. Les puissances d'entrée correspondant aux IP3 définis en mode réfléchi et en mode transmis sont du même ordre de grandeur. Ceci a aussi pu être vérifié sur d'autres dispositifs [76]. Ces résultats participent au dimensionnement du radar à détection de l'IM3 puisqu'ils informent sur les niveaux de puissance réémis, attendus au niveau de l'antenne de la cible.

Le banc de test du radar IM3 a ainsi été développé (figure 2.5). Le rayonnement champ lointain (incident et réfléchi) est assuré par deux antennes large-bande (type log-périodique), une pour l'émission du signal incident et une pour la détection du signal réémis.

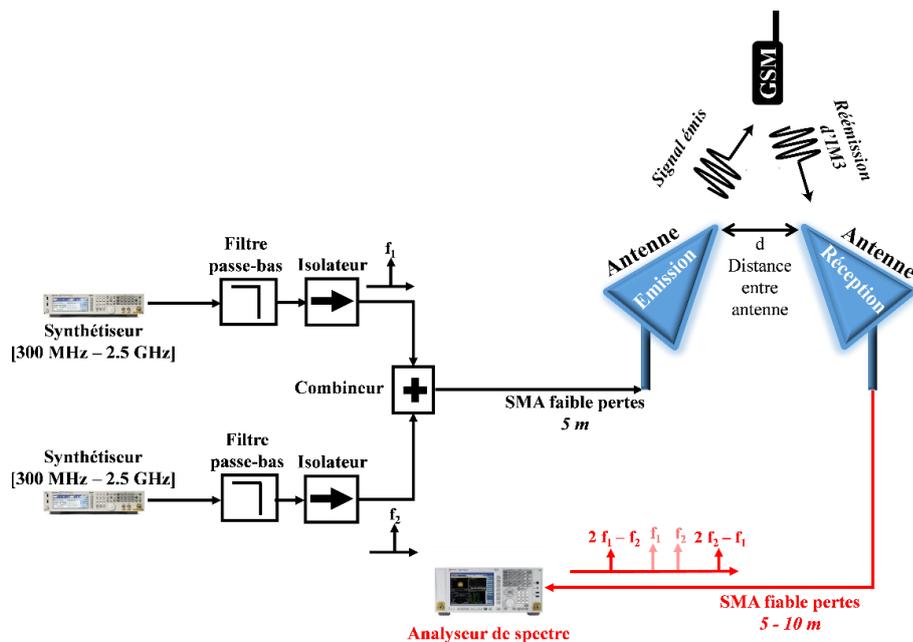


Fig. 2.5: Schéma du banc de test radar à intermodulation à deux antennes

Nous avons fait particulièrement attention à minimiser la contribution de la distorsion d'intermodulation parasite dont l'origine provient des appareils utilisés, afin d'optimiser la sensibilité du radar. L'IM3 résiduel est généré au niveau de la chaîne d'émission, par un mélange généré au niveau des étages d'entrée non-linéaires des synthétiseurs entre les deux fréquences incidentes  $f_1$  et  $f_2$  et leur harmonique, et est favorisé par une mauvaise isolation du combineur. Il peut ensuite se coupler directement sur l'antenne de réception par diaphonie et dégrader le seuil de détection du radar. De même le couplage direct des fréquences incidentes  $f_1$  et  $f_2$  peut également produire un niveau d'IM3 résiduel à cause du mélange au niveau de l'étage d'entrée non-linéaire de l'analyseur de spectre.

Pour pallier à ce problème nous avons opté pour une linéarisation sur l'émission par des filtres et des isolateurs [78], une polarisation croisée et une distance suffisante entre les deux antennes.

Le détail des mesures permettant une optimisation de ce niveau d'IM3 résiduel est présentée dans la thèse d'Alexandre Martorell [79] et a été publié à la conférence European Radar Conference [80].

Typiquement une distance de 2 m entre antennes permet l'obtention d'un seuil de détectabilité confortable à -110 dBm. Finalement le banc est optimisé pour avoir un seuil de mesure donné non pas par les contraintes harmoniques résiduelles, mais par le bruit de l'analyseur de spectre.

Une phase de caractérisation du radar a alors été menée sur un talkie-walkie fonctionnant dans la bande amateur à 400 MHz. Cette cible a l'avantage d'avoir une connectique adaptable qui permet de faire des mesures de l'IM3 réfléchi en conduit. Sa réponse sur une large plage de puissance d'excitation est alors connue, et pourra être comparée avec celle obtenue en mode rayonné avec le radar.

Le protocole de détection consiste à effectuer un balayage des fréquences incidentes  $f_1$  et  $f_2$  et de la puissance incidente à ces deux fréquences. Les résultats pour deux configurations de distance à la cible sont présentées sur les figures 2.6 et 2.7. La distance  $r_1$  est la distance entre l'antenne d'émission et la cible, et  $r_2$  est la distance de la cible à l'antenne de réception. Les fréquences  $f_1$  et  $f_2$  varient de 300 MHz à 600 MHz, avec une différence  $f_2 - f_1$  de 1 MHz. L'antenne d'émission a été positionnée afin d'adapter au mieux sa polarisation avec celle de la cible.

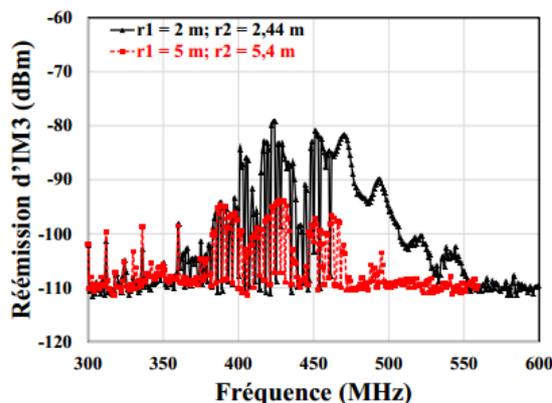


Fig. 2.6: IM3 réfléchi et rayonné par l'antenne de la cible, mesuré dans une bande de fréquence balayée, et pour 2 distances à la cible,  $P_{in}$  fixe

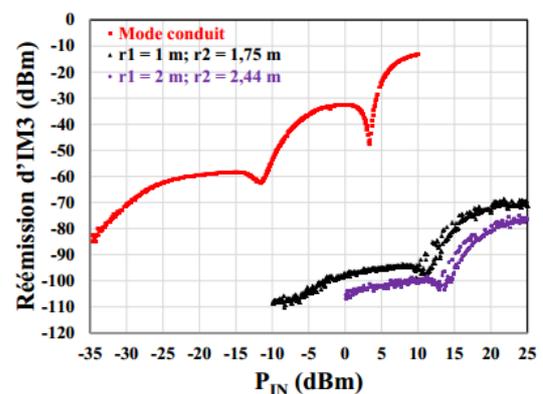


Fig. 2.7: IM3 réfléchi en fonction de la puissance transmise, mesuré en mode conduit et en mode rayonné, et pour 2 distances à la cible,  $f_1$  et  $f_2$  fixes

Le balayage en fréquence du radar à détection d'IM3 fait ressortir la bande de communication de la cible, validée par les données du constructeur. La ressemblance entre le niveau d'IM3 réémis en mode conduit et en mode rayonné est évidente. Un décalage en puissance est observé, dû aux pertes de propagation et de polarisation des antennes (émetteur-cible et cible-récepteur). La partie de la courbe en conduit pouvant être mesurée par le radar correspond à la réponse de la cible excitée aux plus fortes puissances, pour laquelle classiquement on observe de forts changements de pente et des minima [81]. La réponse à faible puissance (pente 3dB/dB) n'a pas pu être mesurée car les niveaux sont sous le seuil de détection du radar.

Ce protocole valide complètement la faisabilité d'un radar à détection d'IM3. Il reste ensuite à estimer ses performances.

### 3) Performances attendues en matière de portée de détection

La portée de détection a été évaluée à partir du bilan de liaison du radar IM3. Dans la littérature, l'équation d'un radar non linéaire utilise un modèle simplifié faiblement non-linéaire de la cible [75, 82]. Il considère que la puissance de l'IM3 réémise par la cible évolue en pente 3dB/dB selon la puissance incidente. Or cette évolution théorique simplifiée n'est pas vérifiée expérimentalement, d'après la figure 2.7.

Nous avons ainsi proposé un modèle beaucoup plus proche de la réalité où la réponse de la cible détectée est fortement non-linéaire. Une approche semi-empirique basée sur la formulation de Friis et les résultats expérimentaux obtenus en mode conduit a été préférée à une approche théorique basée sur un modèle fort-signal de la cible, qui s'avère être une tâche difficile en l'absence de connaissance interne du circuit.

La figure suivante illustre le chemin pris par le signal jusqu'à la détection de la réponse non-linéaire de la cible, et précise les grandeurs intervenant dans le modèle développé.

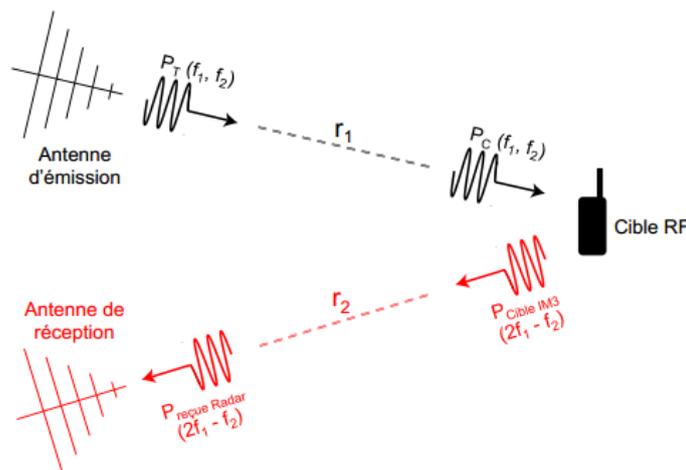


Fig. 2.8: Vue schématique du trajet du signal radar à détection d'IM3

L'équation de Friis permet de calculer la puissance  $P_c$  reçue par la cible à partir de la puissance transmise par l'émetteur, et la puissance de l'IM3 détectée à la réception  $P_{\text{reçue-radar}}$  à partir de la puissance réémise par la cible  $P_{\text{cible-IM3}}$ . Le modèle utilise la réponse expérimentale de la cible qui a été mesurée en conduit (figure 2.7).

Finalement le modèle semi-empirique s'exprime ainsi :

$$P_C = \beta_1 \cdot \frac{P_T \cdot G_T \cdot G_{\text{cible}}}{(4\pi)^2 \cdot r_1^2} \cdot \lambda_{f_1, f_2}^2$$

$$P_{\text{cible-IM3}} = f_{NL}(P_C)$$

$$P_{\text{Reçue-radar}} = \beta_2 \cdot \frac{P_{\text{cible-IM3}} \cdot G_R \cdot G_{\text{cible}}}{(4\pi)^2 \cdot r_2^2} \cdot \lambda_{2f_1-f_2}^2$$

$G_T$ ,  $G_{\text{cible}}$ ,  $G_R$  sont les gains des antennes de l'émetteur, de la cible et du récepteur respectivement.

Ce modèle a été utilisé avec des cibles dont le gain est connu et la réponse en mode conduit a été mesurée, soit un talkie-walkie et un récepteur radio télécommandé, fonctionnant dans des bandes de fréquence différentes (400 MHz et 2.4 GHz), afin d'estimer les portées de détection maximale du système radar proposé. Le modèle fait intervenir des facteurs de perte de polarisation ( $\beta_1$  et  $\beta_2$ ) entre les antennes.

Dans les expériences et de manière opérationnelle, afin d'optimiser le transfert de puissance de l'émetteur vers la cible, l'antenne de l'émetteur est toujours adaptée au mieux en polarisation par rapport à l'antenne de la cible, le terme  $\beta_1$  tend donc vers 1. Comme l'antenne de l'émetteur et celle du récepteur sont positionnées en polarisation croisée, le terme  $\beta_2$  est quant à lui beaucoup plus faible. Ces deux termes sont ajustés à partir des mesures réalisées avec le radar, dans une configuration de distance  $r_1$  et  $r_2$ , et des équations du modèle.

Le détail de la procédure d'extraction de ces paramètres est disponible dans la thèse d'Alexandre Martorell [79], et a été publié à la conférence EuRAD [80]. Des valeurs typiques de  $\beta_1 = -3$  dB et  $\beta_2 = -16$  dB ont été extraites pour le talkie-walkie. Ces valeurs semblent tout à fait cohérentes par rapport à des valeurs typiques de pertes de polarisation.

Une fois le modèle complet, il est possible d'estimer l'évolution de la portée de détection avec la puissance incidente du radar (figure 2.9). Un seuil de sensibilité de -110 dBm à l'analyseur de spectre a été utilisée. Le banc de test développé au laboratoire permet d'injecter des puissances incidentes maximales de 20 dBm. Jusqu'à cette valeur, le modèle semi-empirique proposé est en bon accord avec les résultats expérimentaux, contrairement à l'évolution théorique (en  $1/r^8$ ) qui surévalue la portée. Le modèle semi-empirique permet une extrapolation de la détection à des niveaux de puissance plus élevés.

A la valeur tout à fait envisageable en condition opérationnelle de 40 dBm une portée de détection d'environ 50 m semble être accessible. Ces cibles n'ont pas été testées avec un radar à harmonique 2. Néanmoins, d'après la littérature, les valeurs de portée obtenues avec les deux types de radar sont équivalentes, même si le radar H2 nécessite l'utilisation d'une puissance incidente supérieure [65].

Notons également qu'il reste des pistes d'amélioration des performances du radar IM3 par exemple en utilisant des antennes à plus fort gain.

Une solution de radar à une antenne (émission et réception) a aussi été testée. Le système devient plus compact mais le point bloquant est l'atténuation de couplage induit par le coupleur bidirectionnel nécessaire pour diriger le signal détecté vers l'analyseur de spectre. Les portées de détection sont moins intéressantes que dans le cas proposé. Cette solution reste néanmoins encore à explorer car elle offre une simplicité de mise en œuvre en milieu opérationnel.

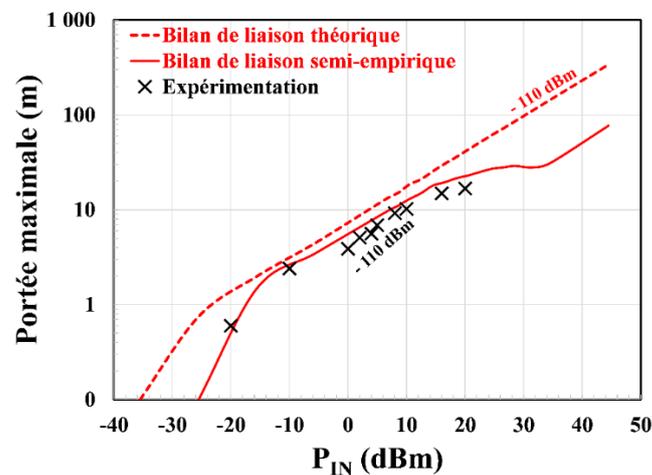


Fig. 2.9: Evolution théorique, semi-empirique et expérimentale de la portée de détection en fonction de la puissance à l'émission du radar, pour une cible fonctionnant autour de 400 MHz

Les tests sur les cibles fonctionnant en plus haute fréquence montrent des portées de détection plus faibles, bien que leur susceptibilité à l'intermodulation testée en mode conduit soit très proche. Une portée de 10 m avec un récepteur radio à 2.4 GHz a pu être mesurée. Les antennes du radar et l'antenne de la cible sont identiques quelle que soit la fréquence. La réduction des portées est probablement liée à un affaiblissement du signal lors de sa propagation en espace libre, qui est plus fort pour les plus hautes fréquences.

#### 4) Perspectives : vers une identification de cibles inconnues

D'après les résultats obtenus lors de la caractérisation de cibles connues, le radar à IM3 semble pouvoir remplir davantage de fonctions que la détection de cibles inconnues, en conditions opérationnelles.

Tout d'abord, il a montré sa capacité à mesurer la bande passante d'un récepteur radio grâce à l'utilisation d'un balayage en fréquence. L'identification de cette bande passante peut renseigner sur le type de communication de la cible, à savoir l'identification du standard de communication utilisé, ou sa fréquence de fonctionnement. Cette première classification par standard de communication corrélée avec l'environnement où la mesure a été effectuée, peut potentiellement amener une première hypothèse sur la mission de la cible. La détection d'une fréquence de fonctionnement dite amateur (2,4 GHz) en milieu urbain semble innocente, sachant la surcharge du spectre électromagnétique à cette fréquence. La détection de cette même fréquence de fonctionnement, sur un théâtre d'opération, est cette fois-ci synonyme d'un récepteur RF potentiellement menaçant.

Par la mesure de l'IM3 réémis avec un balayage en fréquence, une détection multi-cible a été réalisée (figure 2.10). Toutes ces données pourraient être implantées dans une base de données intelligente, qui s'enrichirait par l'expérience à partir de multiples scénarios opérationnels, et en y intégrant une estimation du danger selon le lieu de la détection. Ceci pourrait permettre d'améliorer la prise de décision et envisager si nécessaire une neutralisation de la cible.

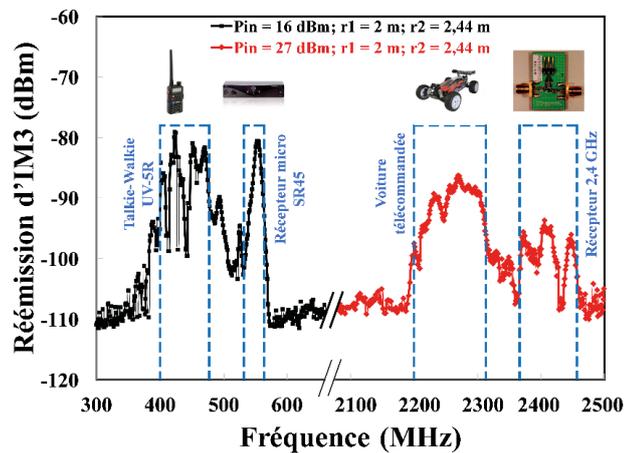


Fig. 2.10: Balayage en fréquence qui permet l'identification des bandes passantes de 4 cibles RF

Le balayage en puissance sur une cible qui émet et reçoit met en évidence une réponse de l'IM3 spécifique (figure 2.7). Des mesures en acquisition instantanée à l'analyseur de spectre montrent deux comportements bien distincts. L'étude sur de nombreux front-ends de la susceptibilité à l'intermodulation en conduit a montré que le LNA (mode réception) a un niveau réémis d'IM3 bien plus élevé que celui réémis par le PA (mode émission), en particulier car les deux fréquences incidentes attaquent le PA par sa sortie. Ceci a pu être validé par des simulations numériques. Ces deux niveaux de rémission d'IM3 bien distincts sont observés sur les résultats expérimentaux de la figure 2.11. Le premier tracé donnant le maximum de puissance à l'IM3 est caractéristique de la réémission du LNA et le deuxième tracé donnant le minimum de puissance à l'IM3 est caractéristique de la réémission du PA. Les points intermédiaires correspondent aux niveaux de puissance mesurés au cours de la commutation du système. Le switch du dispositif commute avec une certaine dynamique entre les fonctions émettrice

et réceptrice, qu'il est possible de mesurer en mode SPAN zéro de l'analyseur de spectre, à la fréquence de l'IM3 (figure 2.12).

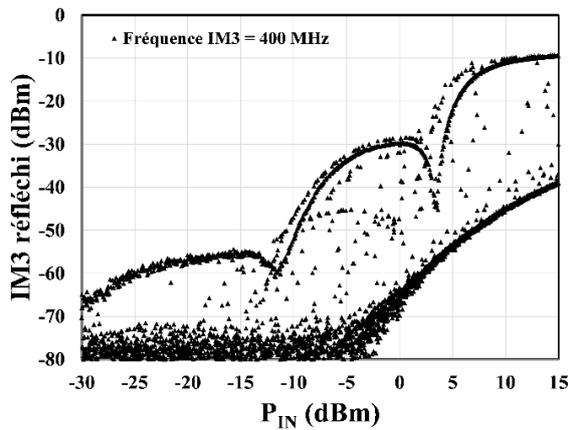


Fig. 2.11: Balayage en puissance réalisé sur un Talkie-Walkie

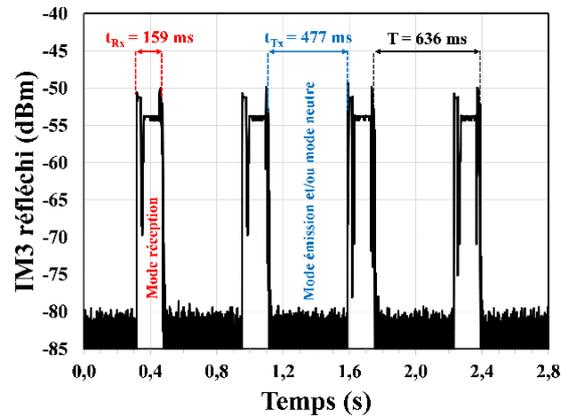


Fig. 2.12: Identification du temps de commutation du switch

Un switch avec une période de commutation de 636 ms a été détecté, identifiant le fonctionnement propre d'un front-end en commutation automatique.

Ainsi il apparaît qu'un balayage en puissance et en fréquence permet de discriminer les fonctions : récepteur, émetteur-récepteur et émetteur.

Les perspectives à ce travail s'orientent vers une meilleure capacité d'identification au niveau des récepteurs RF, en vue de leur classification selon leur dangerosité. Les courbes d'IM3 réémise par un récepteur présentent un comportement spécifique pour les plus fortes puissances incidentes. Un ou plusieurs minima sont observés, en conduit ou en rayonné. Dans tous les cas la pente théorique unique en 3 dB/dB n'est jamais observée sur toute la plage de puissance incidente.

Nos travaux en cours, expérimentaux et par simulation, montrent que ces comportements particuliers dépendent de la topologie et des paramètres internes du LNA du récepteur, et surtout de son point de fonctionnement. Ces minima sont connus dans la littérature et apparaissent en régime fort-signal du circuit. Leur origine vient des phénomènes de mélange créés par les non-linéarités, pouvant conduire à une diminution du niveau de puissance de la raie IM3 à cause des produits d'intermodulation d'ordre supérieurs (IM5, IM7, ...), qui deviennent prépondérant dans la distorsion générée.

Ils peuvent être vus comme des singularités, dont la position et l'intensité pourraient discriminer un récepteur.

Pour la suite il me semble judicieux de tester le protocole de détection proposé (balayage en fréquence et en puissance) sur les nombreuses cibles réelles, potentiellement présentes sur les théâtres d'opération. Ceci constituera une base de données riche pouvant contribuer à une classification (estimation du danger) de récepteurs RF.

En parallèle à cette phase de tests, il serait intéressant d'exploiter au mieux les comportements singuliers dans la réponse de l'IM3, mais aussi aux autres ordres, avec pour objectif la récolte d'informations sur les paramètres internes (architecture, point de fonctionnement, etc.) d'un récepteur inconnu, et ceci à distance. En particulier, la présence d'une singularité devrait permettre de définir le niveau de vulnérabilité d'un récepteur et à terme améliorer la prise de décision (leurage, brouillage, etc.).

Finalement ce travail pourrait permettre de répondre plus intelligemment à la présence d'un récepteur et à son niveau d'hostilité. Thalès reste notre collaborateur principal pour envisager la suite de ces travaux. La DGA, acteur institutionnel de la défense est un partenaire idéal, grâce entre autres à la connaissance acquise sur le terrain quant à la définition des cibles les plus intéressantes et des besoins opérationnels à développer. La thèse d'Alexandre Martorell a été soutenue en juillet 2018. La DGA a été fortement intéressé par les travaux présentés durant la soutenance de thèse d'Alexandre Martorell en juillet 2018, et souhaite poursuivre dans le cadre d'une thèse Cifre-défense. Je suis actuellement à la recherche d'un candidat, et espère débiter la thèse courant 2019.

### **Chapitre 3. Technique d'injection en champ proche – Optimisation de sonde en situation de couplage**

Le premier chapitre de ce mémoire présente des perturbations mises en évidence au niveau composant et circuits, suite à l'injection d'un signal. Dans un contexte réel d'attaque ou de pollution non intentionnelle, le signal interférent est émis en champ lointain. L'illumination du circuit est alors complète, il est donc impossible d'identifier localement les zones de plus forte vulnérabilité. La caractérisation de la susceptibilité en champ lointain impose également de fortes puissances à l'émission, en particulier pour tester la sensibilité des circuits à des signaux intentionnels.

Ainsi, pour injecter de façon locale avec des puissances raisonnables et tout en gardant l'avantage du test sans contact, nous avons voulu mettre en place dès le début des études de susceptibilités des expériences d'injection en champ proche [83]. Celles-ci nécessitent l'utilisation de sondes de champ proche généralement large bande qui doivent générer soit un champ électrique soit un champ magnétique au voisinage des composants [84]. Par les lois de l'électromagnétisme, une interaction entre ce champ et des lignes du circuit connues comme des récepteurs efficaces de champ [85, 86], engendre une tension ou un courant à l'intérieur du circuit, susceptible d'apporter une perturbation au niveau de la fonction électronique. La maîtrise de la chaîne complète d'injection en champ proche nécessite d'acquérir une compréhension de ces interactions. Ceci passe d'abord par une étude de la sonde seule, puis par une phase d'optimisation lorsque la sonde est placée en situation de couplage.

L'injection électromagnétique en champ proche est devenue une technique incontournable pour les études de susceptibilité de composants ou de circuits électroniques [1, 87]. Récemment, son application aux circuits intégrés cryptographiques a permis la production de fautes significatives visant à casser le crypto-système [88, 89]. Une des problématiques principales de l'injection en champ proche est de concevoir des sondes optimisées en matière de transfert d'énergie au niveau du circuit. L'efficacité d'injection de la sonde devient une figure de mérite primordiale à optimiser, et dans une moindre mesure, sa résolution spatiale, qui doit être suffisamment fine pour garantir une injection localisée. La géométrie de la sonde et les matériaux utilisés sont les paramètres clés à optimiser pour améliorer le transfert de puissance à la cible, idéalement sur une large bande de fréquence.

Dans l'équipe, les premières expérimentations de susceptibilité EM en champ proche étaient le plus souvent effectuées avec des sondes non optimisées, des sondes à pointes pour rayonner préférentiellement un champ électrique et des sondes à boucle pour rayonner un champ magnétique [83]. Ces sondes peuvent être placées au-dessus de pistes du circuit imprimé sur lequel est soudé le composant ou le circuit sous test. Les courants ou tensions couplées ne sont alors pas générés au cœur du circuit mais à l'extérieur de celui-ci. Dans ce cas, l'utilisation de la technique d'injection en champ proche n'est pas nécessaire, et une injection en conduit, comme présenté dans le premier chapitre, est souvent plus simple à mettre en œuvre.

En revanche, l'injection au-dessus d'un circuit intégré vise à créer des courants/tensions parasites à l'intérieur du circuit. Cette technique d'injection est la seule solution pour passer outre les protections intégrées sur la puce. Elle est capable d'induire des courants d'intensité suffisante pour qu'un circuit intégré embarquant un cristo-système numérique produise des résultats erronés, exploitable par des attaquants pour remonter aux clés cryptés [90].

Nos collègues du LIRMM, en particulier Philippe Maurine travaillent sur les effets de ces injections sur les circuits intégrés cryptés, et les moyens de s'en prémunir. Pour aller plus loin dans leurs travaux, ils ont eu besoin d'une expertise en électromagnétisme, au niveau de la compréhension du fonctionnement de la sonde et des mécanismes physiques de couplage.

Nous avons ainsi travaillé ensemble sur cette problématique, d'abord avec des sondes électriques à pointe, dans le cadre du stage Master de Rachid Omarouayache suivi d'un poste d'ingénieur en CDD d'une année. Puis nous avons continué à collaborer étroitement sur la problématique de la sécurité des circuits cryptés, dans le cadre d'un projet ANR E-MATA-HARI (Electromagnetic Analysis, Deciphering and Reverse Engineering of Integrated Circuits) sur l'appel d'offre « Ingénierie Numérique et Sécurité », validé en 2012, pour une durée de 3 ans, et regroupant les partenaires Freescale, Morpho et le LAAS.

Ce projet a été porté par Laurent Chusseau de l'IES et j'ai été responsable des workpackages concernant la conception et l'optimisation des sondes ainsi que la modélisation du couplage. Les principaux enjeux étaient d'évaluer et de quantifier les menaces EM sur des circuits intégrés sécurisés, et ensuite de protéger les circuits à venir contre les attaques EM. Pour cela des contre-mesures tant logicielles que matérielles devaient être envisagées.

Notre travail à l'IES a concerné l'optimisation de l'interaction physique de la sonde avec le circuit. L'objectif a été d'améliorer les sondes existantes [91] et d'en concevoir de nouvelles destinées à la gamme de fréquence de 1 MHz à 100 GHz [92], avec une résolution de quelques dizaines de microns. Les plus basses fréquences sont dédiées à l'injection de fautes et les plus hautes à l'imagerie des circuits encapsulés et au reverse engineering, permettant entre autres de cibler des zones susceptibles aux injections.

Pour des fréquences allant jusqu'à quelques GHz, les sondes sont souvent basées sur de petites boucles pour le champ magnétique et des pointes pour le champ électrique. En pratique, la perturbation la plus efficace au niveau circuit intégré est la modification de la tension d'alimentation  $V_{DD}$  induite par une variation brutale du champ magnétique capté par les lignes d'alimentation du circuit. En outre, la densité de métal est très forte sur les circuits intégrés, ce qui joue un rôle de blindage naturel, surtout contre les champs électriques, puisque les métaux utilisés dans la micro-électronique n'ont pas ou peu de propriétés magnétiques permettant de dévier ou d'écranter les lignes de champ magnétique.

Nous nous sommes ainsi surtout focalisés sur les sondes magnétiques, pour lesquelles nous avons cherché à proposer une méthodologie d'optimisation. Ces études des sondes et du couplage ont été particulièrement motivées par le projet ANR, mais ont contribué à enrichir notre expertise au niveau de

l'injection EM au sens large. Ici, cette collaboration avec le LIRMM permet d'élargir nos compétences sur les sondes magnétiques et de débiter des travaux sur le couplage en champ proche sur circuit intégré, dont j'ai été le principal acteur, en collaboration avec plusieurs étudiants. La thèse de Rachid Omarouayache a été financée sur le projet ANR, et trois stages Master (Rachid Omarouayache, Pierre Payet et Zohir Touta) ont également travaillé sur ce sujet.

### 1) Méthodologie d'optimisation de sondes magnétiques de champ proche

Afin d'estimer qualitativement la nature et la quantité de puissance qu'il est possible de récupérer en champ proche, nous avons observé la puissance rayonnée par un dipôle magnétique, en intégrant le vecteur de Poynting sur une sphère de rayon  $r$  avec pour centre le dipôle [93, 94]. Son expression est la suivante :

$$P = P_0 \cdot \left(1 + j \cdot \frac{1}{(kr)^3}\right)$$
, où  $P_0$  dépend de l'impédance du vide, du courant circulant dans le dipôle, du diamètre du dipôle et de la longueur d'onde, et  $k$  est la constante de propagation.

Cette relation montre qu'en champ proche ( $k \cdot r \ll 1$ ) la partie imaginaire prédomine, le terme propagatif peut être négligé et la puissance stockée autour de la sonde est inductive. Pour un dipôle électrique la puissance stockée autour de la sonde est cette fois capacitive. La relation indique une évolution en  $1/r^3$  de la quantité de puissance stockée. La distance sonde-cible est donc un paramètre limitant dans l'optimisation du transfert de puissance. En outre, cette puissance stockée est répartie autour de la sonde, ce qui est pénalisant pour avoir de bonnes résolutions spatiales. Enfin, la présence d'une puissance stockée réactive signifie forcément une forte désadaptation d'impédance de la sonde avec le générateur d'excitation. Pour les sondes de champ proche destinées à injecter sur de larges bandes de fréquences, l'adaptation d'impédance n'est pas envisagée car difficile à mettre en œuvre.

Finalement les sondes de champ proche magnétique et électrique sont des objets désadaptés, pour lesquelles la résolution spatiale et l'efficacité d'injection tendent à évoluer en sens opposé (une forte efficacité d'injection implique une dégradation de la résolution spatiale).

L'optimisation des sondes selon la résolution spatiale, l'efficacité d'injection, et la bande passante voulue pour l'application, a été menée. La sonde doit en effet délivrer un champ magnétique intense et localisé sur une large bande passante.

Des simulations électromagnétiques 3D ont été utilisées principalement pour ajuster les tailles géométriques des éléments constituant la sonde. Des calculs ont d'abord été menés sur une sonde à boucle classique. Ces travaux ont été réalisés durant le stage master de Rachid et ont donné lieu à une première publication dans une conférence internationale à l'EMC Europe 2013 [91]. Les résultats de calcul ont montré que la résolution spatiale de la sonde est limitée par son diamètre. Elles peuvent difficilement être miniaturisées (de l'ordre du mm) en raison de l'épaisseur du fil de la boucle qui doit être suffisante pour supporter les forts courants du signal d'injection.

La solution pour concentrer le champ magnétique et ainsi affiner la résolution spatiale consiste en l'utilisation d'un noyau de ferrite cylindrique taillé en pointe (figure 3.1). Le calcul du champ magnétique (figure 3.2) à une distance de  $20\ \mu\text{m}$  sous la pointe met en évidence une résolution de  $400\ \mu\text{m}$  (largeur à mi-hauteur du profil de champ magnétique), alors que le diamètre des boucles est ici de  $1.5\ \text{mm}$ . L'augmentation de l'efficacité d'injection définie pour la sonde seule par l'amplitude maximale du champ  $H$  nécessite l'utilisation de plusieurs boucles de fil, enroulées autour du noyau de ferrite.

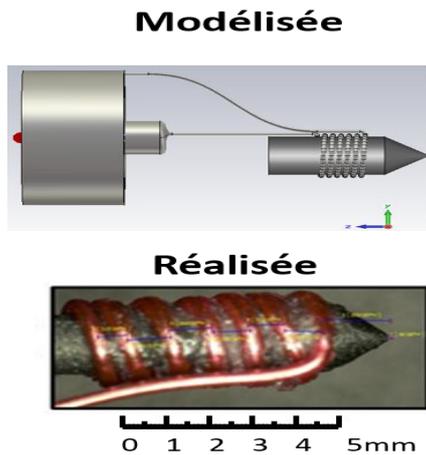


Fig. 3.1: Sonde magnétique avec noyau de ferrite, modélisée et réalisée

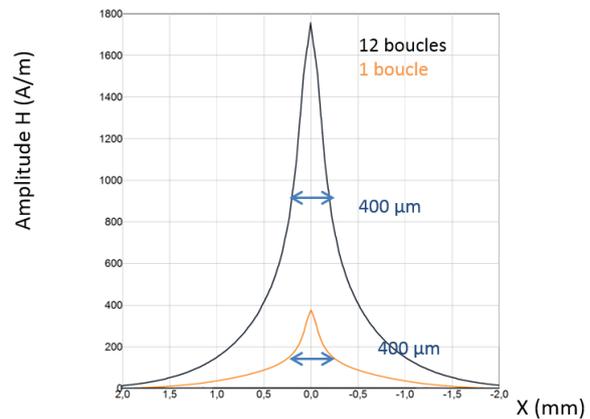


Fig. 3.2: Calcul numérique du champ magnétique rayonné à une distance de  $20\ \mu\text{m}$  de la pointe, pour 1 et 12 boucles

La perméabilité du ferrite est un paramètre fondamental dans le choix de ce matériau. Une forte partie réelle du  $\mu_R$  ( $\mu_R'$ ) favorise à la fois la quantité de champ  $H$  rayonné à un courant donné circulant dans la sonde, et la concentration locale de ce champ. Cependant l'évolution de  $\mu_R'$  avec la fréquence a un comportement passe-bas, et dans les matériaux de ferrite commun (NiZn, MnZn) le produit  $\mu_R' \cdot f_C$  (fréquence de coupure) est relativement constant [95]. Ainsi, un matériau à fort  $\mu_R'$  a une faible fréquence de coupure. Les pertes (partie imaginaire de  $\mu_R$ ) sont plus élevées autour et au-delà de la fréquence de coupure. Les performances en résolution spatiale et en efficacité d'injection doivent être mises en regard de la bande passante voulue.

En dynamique, ces sondes ont par nature un comportement inductif, jusqu'à une fréquence de résonance amenée par des capacités parasites, dont la principale est la capacité inter-spire. La valeur de l'inductance dépend surtout du nombre de boucles et de  $\mu_R'$ . Plus le nombre de boucles est important et le  $\mu_R'$  du ferrite est fort, plus l'inductance de la sonde a une valeur élevée, ceci au prix d'une diminution de sa fréquence de résonance (la sonde n'est plus purement magnétique) et de son aptitude à faire varier rapidement le courant magnétisant la traversant (par une augmentation de la constante de temps). Ainsi si la source d'attaque présente de fortes variations de tension la sonde a tendance à ralentir cette dynamique en lissant le courant, réduisant ainsi le transfert de puissance vers la cible.

A partir des règles de conception établies avec les simulations EM, un premier travail expérimental a été réalisé au début de la thèse de Rachid avec ma participation et celle de Laurent Chusseau. Il a consisté à fabriquer puis à caractériser des sondes avec un nombre de boucles variables et des matériaux ferrite du commerce, ayant différents  $\mu_R$  et différents diamètres de noyau. Des mesures d'impédance d'entrée des sondes jusqu'au GHz à partir d'un analyseur de réseau ainsi que des mesures en régime impulsionnel ont été menées, validant les comportements décrits précédemment. La fréquence de résonance obtenue varie selon les cas, et atteint dans le pire cas testé (12 boucles) la valeur d'environ 100 MHz, et dans le meilleur cas (3 boucles) 500 MHz, avec le matériau ferrite ayant la meilleure réponse en fréquence.

Par la suite j'ai pris en charge la modélisation de la sonde et du couplage sonde/ligne, avec la participation de Rachid et le stagiaire master Pierre Payet. Des modèles électriques à éléments localisés RLC, permettant de reproduire les comportements des sondes jusqu'à des fréquences du GHz (figure 3.8), ont été conçus, en s'appuyant sur la physique et la géométrie de la sonde. Les évolutions fréquentielles de l'inductance de la tige de ferrite bobinée et de sa résistance de pertes ont été considérés en utilisant le modèle dynamique de la perméabilité relative du ferrite  $\mu_R$ , trouvé dans la littérature [95, 96].

## 2) Modélisation du couplage sonde/ligne

### a) **Expériences d'injection en champ proche**

Les lignes sont connues pour être des récepteurs efficaces de champ électrique et magnétique [85]. Afin de caractériser et de modéliser ce couplage nous avons d'abord utilisé des lignes micro-ruban longues d'impédance caractéristiques  $50 \Omega$  et adaptées. Puis, pour nous rapprocher du contexte de l'attaque nous avons utilisé des lignes intégrées sur silicium, avec des dimensions géométriques réduites et fermées sur des blocs fonctionnels.

Expérimentalement un banc d'injection en champ proche a été utilisé pour caractériser le couplage. Ce banc avait été mis en place à l'origine des premiers travaux de l'équipe lors de la thèse de Tristan Dubois. Il est basé sur le même principe que le scanner présenté au chapitre 1 permettant les injections aux fréquences millimétriques. Ici un synthétiseur est utilisé avec une connexion par câble SMA jusqu'à la sonde. Des cartographies en injection (ou en capture) sont possibles avec un pas de  $1 \mu\text{m}$  en x, y et z. La sonde peut ainsi être mise en situation de couplage au-dessus d'une ligne. Le signal couplé est mesuré soit avec un oscilloscope soit avec un analyseur de spectre selon la forme du signal injecté.

Les figures 3.3 et 3.4 illustrent des expériences d'injection en champ proche avec une sonde magnétique sur des lignes et sur un circuit intégré. Les distances sonde-ligne sont nécessairement faibles pour pouvoir transférer de la puissance. Les valeurs typiques varient de  $10 \mu\text{m}$  jusqu'à quelques mm.



Fig. 3.3: Injection en champ proche sur ligne micro-ruban

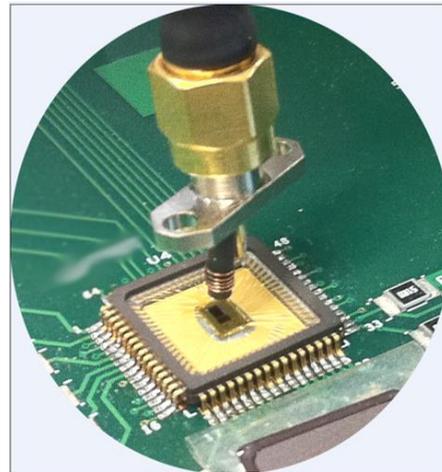


Fig. 3.4: Injection en champ proche sur circuit intégré

La puissance stockée autour de la sonde dans le champ proche étant inductive, l'interaction locale sonde-ligne a été décrit par la loi de Maxwell-Faraday : l'excitation de la boucle par un courant variable dans le temps rayonne un champ magnétique dont la variation temporelle génère une modification spatiale du champ électrique au voisinage de la ligne, d'où une modification de la tension dans la ligne.

#### b) Modèle de couplage par la mutuelle

J'ai construit le modèle de couplage en considérant que le système sonde-ligne couplé peut être assimilé à un transformateur, dont le primaire est la sonde et le secondaire la ligne. L'inductance mutuelle  $M$  est le paramètre quantitatif global décrivant l'efficacité du couplage. Sa valeur est variable, prenant ainsi en compte la variation spatiale des champs magnétiques mis en jeu, et dépend en particulier de la distance sonde-ligne et de la position relative de la sonde par rapport à la ligne.

Expérimentalement, les valeurs de  $M$  ont été extraites avec des cartographies d'injection. Ce travail a été réalisé lors du stage de Zohir Touta. Le protocole consiste à positionner la sonde à une hauteur  $h$  de ligne et à la déplacer perpendiculairement par rapport à la ligne, par pas fixe.

L'extraction de  $M$  repose sur une méthode de mesure temporelle, inspirée du papier de Johnson [97], et qui a été détaillée dans la thèse de Rachid et publiée dans la conférence nationale JNM en 2017 [98]. Le signal d'excitation est ainsi de type impulsif de temps de montée et descente typique de quelques dizaines de nanosecondes, choisis de telle façon que la fréquence équivalente soit plus faible que la fréquence de résonance de la sonde (limite de son comportement inductif). A chaque position de la sonde, la tension induite sur la ligne est mesurée avec un oscilloscope rapide. A partir des pics de surtension observés au moment des fronts montants ou descendants du signal d'excitation, une valeur de mutuelle est extraite. Une forte mutuelle indique une bonne efficacité d'injection.

Ce paramètre quantitatif du couplage sert à établir des règles de conception et d'optimisation de la sonde, cette fois en situation de couplage, et non seule comme présenté précédemment. L'évolution de

M avec la position relative de la sonde par rapport à la ligne met en lumière la zone spatiale de couplage au-dessus de la ligne (figure 3.5).

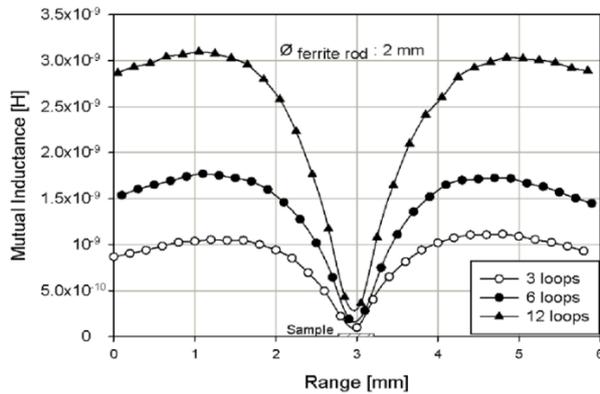


Fig. 3.5: Evolution de l'inductance mutuelle M en fonction de la position relative de la sonde par rapport à la ligne, pour 3, 6, 12 boucles de fil, et un diamètre de noyau de 2 mm

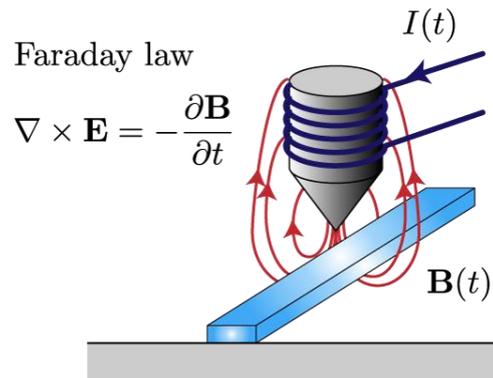


Fig. 3.6: Mécanisme de couplage magnétique sur une ligne

La figure 3.5 montre que quel que soit le nombre de boucles utilisé, le couplage est important même si la sonde est loin de la cible (plusieurs mm), et il est minimum au centre de la ligne. Le maximum de couplage est localisé à 2 mm de part et d'autre de la ligne. Cela est dû au fait que le champ magnétique émis par la sonde est essentiellement vertical (figure 3.6). Ce champ doit englober la ligne pour créer une tension induite dans la ligne.

Bien que la résolution spatiale de la sonde seule ait été optimisée, l'ensemble sonde+ligne est bien moins résolu, et ceci à cause d'une mauvaise adaptation entre l'émetteur (la sonde) et le récepteur (la ligne). L'adaptation sonde-cible est une problématique récurrente du champ proche. Il est possible de l'améliorer par une optimisation des paramètres géométriques de la sonde. Ceci valide bien le fait qu'une optimisation de la sonde seule ne suffit pas, il faut aussi la caractériser en situation de couplage.

Dans cette idée, j'ai voulu vérifier durant le stage de Zohir Touta l'intérêt réel de la forme conique donnée au noyau de ferrite. Des mesures comparatives de mutuelle avec et sans cette forme particulière ont révélé une plus faible mutuelle (donc transfert de puissance) avec la sonde appointée, expliquée par le fait que les boucles se retrouvent à une distance plus lointaine de la cible, et que les lignes de champ sur la forme appointée se dispersent et atteignent donc en moins grand nombre la cible.

Finalement les tests en situation de couplage nous ont permis de corriger la forme du noyau pour une meilleure efficacité d'injection. Le noyau magnétique garde sa forme cylindrique et le fil est bobiné le plus bas possible sur ce noyau.

D'après la figure 3.5, M croît avec le nombre de boucles. Cependant comme mentionné dans la partie sonde ceci est tempéré avec la forte décroissante de la fréquence maximale d'utilisation de la sonde avec le nombre de boucles. Le choix du nombre de boucles dépend donc de la rapidité du signal d'excitation.

Afin de miniaturiser la sonde et d'améliorer l'adaptation sonde-ligne, le diamètre de la sonde doit être optimisé et si possible réduit. La figure 3.7 présente l'effet du diamètre sur la valeur de la mutuelle inductance. Les noyaux magnétiques disponibles dans le commerce ont un diamètre minimal de 0.75 mm. La géométrie de la cible pour observer les effets du diamètre de la sonde sur le couplage a son importance, en particulier sa longueur, qui a été choisie faible ( $L \approx 500 \mu\text{m}$ ) et du même ordre de grandeur que celle rencontrée pour des lignes d'interconnexion dans les circuits intégrés. La surface sous la ligne, interceptant le champ magnétique, est donc d'autant plus réduite que le diamètre de la sonde est toujours plus grand que la longueur de la ligne (insert de la figure 3.7). Notons que dans ce type de couplage champ à boucle la hauteur du substrat modifie également la surface équivalente de capture du champ.

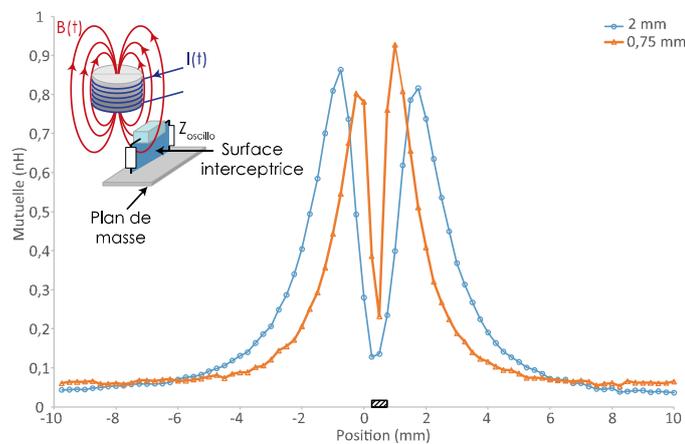


Fig. 3.7: Efficacité d'injection en fonction de la position relative de la sonde par rapport à la ligne, pour 2 diamètres de noyau magnétique non appointé

Ces résultats confirment un étalement à mi-hauteur de la mutuelle plus faible pour le plus petit diamètre, traduisant une meilleure résolution spatiale du système sonde+ligne. Les valeurs maximales de mutuelle sont assez similaires dans les deux cas. L'efficacité d'injection est limitée, non pas par le diamètre de la sonde, mais par la longueur de la ligne.

Ainsi l'injection sur circuit intégré semble donc être optimisée en utilisant des sondes de faible diamètre. De plus, ces noyaux cylindriques de ferrite utilisés voient leur perméabilité relative dépendre du rapport longueur-diamètre du barreau. Le  $\mu_R$  est supérieur pour les plus petits diamètres, ce qui confirme une nouvelle fois l'intérêt d'utiliser de petits diamètres de noyau de ferrite [98].

Preuve que nos travaux d'optimisation de sonde ont intéressé les industriels, la société allemande LANGER EMV-Technik GmbH, spécialisé dans la réalisation de sonde de champ proche vient de mettre sur le marché des sondes magnétiques de champ proche de forme et caractéristiques quasiment similaires à celles que nous avons proposées et publiées à l'issue du projet ANR.

La compréhension acquise lors de ces expériences a contribué à la réalisation d'un modèle électrique à éléments localisés du couplage sonde-ligne, valable jusqu'à des fréquences du GHz. Le modèle proposé type SPICE est donné à la figure suivante :

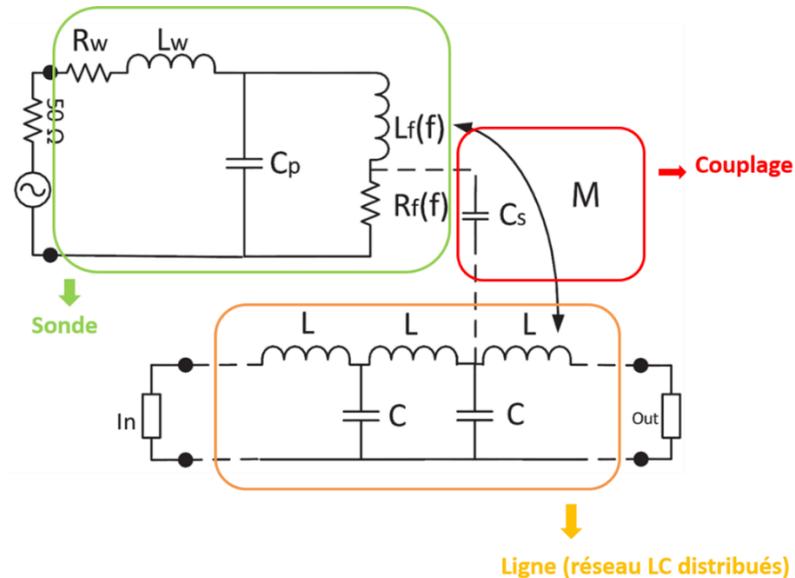


Fig. 3.8: Modèle électrique équivalent de la sonde, du couplage sonde-ligne et de la ligne réceptrice

La tige de ferrite bobinée est modélisée par une inductance  $L_f$  en série avec une résistance de perte magnétique  $R_f$ . Ces deux éléments sont dépendants de la fréquence, à partir du modèle physique de la partie réelle et imaginaire de la perméabilité de la tige de ferrite [95].  $C_p$  est la capacité inter-spire. Le modèle de couplage est décrit par la mutuelle inductance caractérisée expérimentalement, tandis qu'une capacité parasite  $C_s$  traduit le comportement capacitif du système sonde-ligne, non négligeable aux hautes fréquences [99]. La ligne est modélisée par un réseau distribué de cellules LC dont le nombre varie selon sa longueur, et terminée par deux impédances ( $In$  et  $Out$ ) qui peuvent être remplacées par les non-linéarités d'un circuit actif connecté sur la ligne.

Ce modèle permet de reproduire le comportement électrique du couplage magnétique en champ proche. Il est facilement simulable dans un logiciel de type SPICE et peut être associé avec le schéma du circuit actif sur lequel se fait l'injection, pour prédire les effets du signal sur le circuit attaqué en champ proche.

Ce travail de modélisation dont j'ai été le principal acteur a été publié dans une conférence internationale [100] et aux journées nationales microondes en 2015 [101].

### c) Validation de l'injection en champ proche sur des tests-chips

Dans l'idée d'étudier l'injection en champ proche sur les interconnexions typiques des circuits intégrés, une puce de test dédiée a été conçue par la société Freescale dans le cadre du projet (figure 3.10). Ce véhicule de test, utilisant une technologie  $0.25 \mu\text{m}$  SmartMOS avec quatre couches de métallisation, contient des lignes sur substrat silicium, au bout desquelles des capteurs de tension rapides

ont été intégrés [87, 102]. Leur rôle est de mesurer les fluctuations de tension in-situ induites localement par l'injection EM.

Plusieurs structures de tests sont disponibles et donnent la possibilité de tester la résolution spatiale des sondes et d'évaluer le couplage pour des lignes soit fermées sur  $50\Omega$ , soit reliant des blocs fonctionnels numériques (buffer).

La mutuelle inductance dans chaque cas peut être obtenue à partir de la mesure instantanée de la tension induite issue des capteurs sur puce, avec la même méthode que celle utilisée sur les lignes sur circuit imprimé.

Les tests d'injection sur ces lignes intégrées ont mis en évidence des comportements similaires à ceux observés précédemment, avec des valeurs de mutuelle proches de celles trouvées avec un couplage sur ligne de circuit imprimé. Ceci semble tout à fait cohérent puisque les grandeurs géométriques de la ligne sont très proches de celles mesurées précédemment, à la fois au niveau de la longueur et de la hauteur entre la ligne (en métal 3) et la masse du circuit (en bas de la puce), comme illustré à la figure 3.9.

A une position de la sonde au-dessus de la puce, la figure 3.10 montre l'allure de la tension couplée sur une ligne à partir d'un signal d'excitation impulsif ayant des caractéristiques conformes à celles utilisés pour les attaques, de tension crête-à-crête de 10 V, avec des temps de montée et de descente de 4 ns, et un temps à l'état haut de 50 ns. A partir de la tension mesurée, la mutuelle inductance est extraite, et renseignée dans le modèle électrique.

Les résultats expérimentaux et simulés montrent un très bon accord, ce qui valide le modèle de couplage.

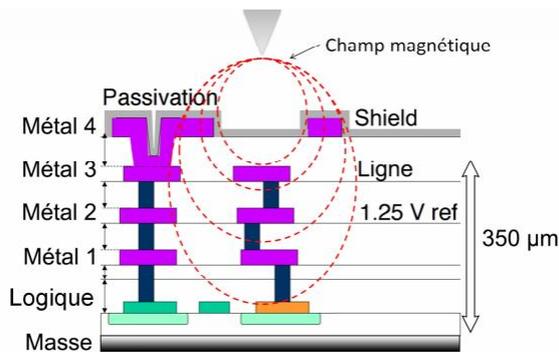


Fig. 3.9: Vue en coupe du circuit intégré, avec un schéma de la sonde, et des lignes de champ associées

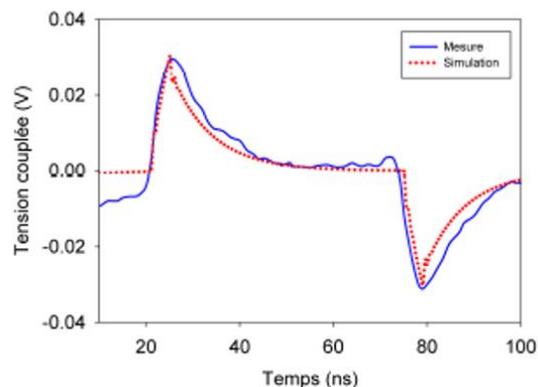


Fig. 3.10: Tension couplée instantanée sur une ligne du circuit intégré. Comparaison mesure-simulation. La sonde est placée à 100 µm de la puce

Pour montrer le caractère local de l'injection magnétique sur une puce, des tests d'injection ont été réalisés durant la thèse de Rachid sur des lignes relativement proches, avec des distances variables jusqu'à 320 µm (figure 3.11). Un déplacement latéral de la sonde au-dessus de ces lignes a été mené, et la comparaison des niveaux de la tension couplée, mesurés simultanément sur chaque ligne, a montré des décalages correspondant aux distances réelles entre les lignes (figure 3.12).

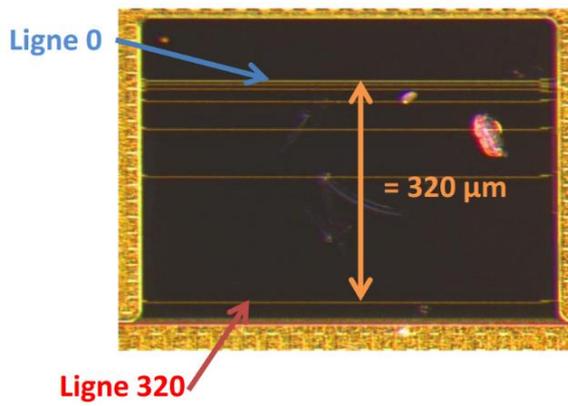


Fig. 3.11: Photographie d'une partie du véhicule de test, contenant les lignes intégrées

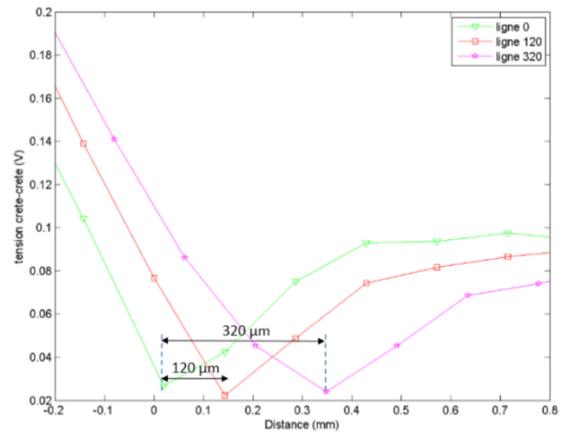


Fig. 3.12: Mesure de la tension induite sur 3 lignes de tests selon la distance de déplacement latéral de la sonde

Finalement le travail mené a été une contribution à l'évaluation et à l'optimisation quant à la résolution spatiale, à l'efficacité d'injection et à la bande passante de la technique d'injection magnétique en champ proche. Ceci a nécessité de comprendre le fonctionnement de la sonde de champ proche et son interaction avec une cible. Nous avons certainement pu atteindre les limites des performances pour ce type de sonde et dans une bande de fréquence jusqu'au GHz.

## **Chapitre 4. Techniques de champ proche aux fréquences millimétriques. Applications à la microscopie et l'imagerie**

L'activité « technique de scan en champ proche aux fréquences millimétriques » a été développée au laboratoire. Elle a été initiée et portée par Laurent Chusseau à partir de 2006, et a jusqu'à présent été en partie financée par deux projets ANR, le projet ANR Terascope (2006-2009) et le projet ANR E-Mata-Hari (2012-2015).

J'ai eu l'occasion de m'impliquer sur ce sujet nouveau pour moi, au cours de ce dernier projet, et suite à mon rapprochement avec Laurent Chusseau, j'ai participé aux discussions et à l'encadrement des étudiants, et je compte dans la suite, m'investir et faire vivre cette activité qui exploite le champ proche, mais cette fois à des fins de microscopie et d'imagerie.

Les thèses de Rachid Omarouyache et Pierre Payet dont j'ai été co-encadrant, ont porté pour moitié sur ce thème. Une a été financée sur le projet E-Mata-Hari, et a été soutenue en 2015, et l'autre a été financée par une bourse ministérielle, a été soutenue octobre 2018.

Dans ce chapitre je présente les techniques en champ proche millimétrique mises en œuvre au laboratoire et leurs applications en microscopie et en imagerie.

Une des motivations premières dans l'utilisation de techniques de champ proche aux fréquences millimétriques ou térahertz était de réaliser de l'imagerie sur circuits intégrés, afin d'identifier les zones les plus vulnérantes avant injection EM. Les ondes millimétriques et térahertz ont en effet des caractéristiques uniques en spectroscopie. La plupart des matériaux utilisés dans les boîtiers des puces sont transparents à ces fréquences. Il devient alors possible de faire du contrôle non-destructif et de l'espionnage d'électronique intégrée.

En outre, le champ proche donne la possibilité de sonder les échantillons de manière locale, avec une résolution spatiale beaucoup plus petite que la longueur d'onde [103- 106]. Des résolutions de l'ordre du  $\mu\text{m}$  voire du nm peuvent être obtenues, selon la distance sonde-échantillon et la taille de la sonde.

Dans la littérature la technique de microscopie en champ proche aux fréquences micro-ondes et millimétriques utilise presque toujours un analyseur de réseau vectoriel [107, 108]. Le principe de base est de mesurer avec précision une modification d'impédance apportée par un échantillon placé dans le champ proche de la sonde (souvent une pointe) [109]. La technique la plus efficace consiste à faire résonner cette pointe, placée juste au-dessus de l'objet à imager. L'image est obtenue par le tracé du décalage de la fréquence de résonance induit par le couplage champ proche avec la pointe [110, 111]. Cette technique est basée sur un couplage capacitif sonde-échantillon et n'exploite pas la nature vectorielle du champ proche électromagnétique, ce qui pourrait pourtant enrichir l'image formée. La meilleure résolution est atteinte avec des pointes les plus fines et le meilleur coefficient de qualité de la cavité résonante.

Cette méthode est par exemple utilisée pour détecter des structures enterrées sous des surfaces pouvant aller jusqu'à l'échelle du nm [112, 113]. Cet appareillage certes très performant a néanmoins l'inconvénient d'avoir un coût très élevé, surtout dans les bandes millimétriques, et encore davantage dans le térahertz.

Notre intention au laboratoire est de nous orienter vers des solutions moins onéreuses, et inspirées des techniques de microscopie en champ proche optique, à savoir le SNOM (Scanning Near-field Optical Microscopy) [114, 115]. L'interaction champ proche est ici obtenue en faisant vibrer la sonde illuminant l'objet, puis en détectant le signal réfléchi. La modulation de la distance sonde-échantillon permet de rejeter les sources secondaires de champ lointain et avoir ainsi la possibilité de mesurer le « vrai » champ proche de l'objet imagé.

Cette technique a montré de très bonnes performances en matière de résolution spatiale (quelques dizaines de nm), aux fréquences optiques. Notre approche consiste donc à transposer les techniques les plus efficaces du SNOM dans le domaine des fréquences millimétriques, pour lequel il est possible notamment de bénéficier d'équipements fiables, efficaces, moins chers (guides d'onde, sources) et de procédés de fabrication simplifiés des sondes.

Ceci a conduit au développement d'un banc de microscopie en champ proche basé sur des expériences de réflectométrie [92, 116]. Les points les plus sensibles de ce banc concernent le choix de la sonde et son interaction avec l'échantillon. Il a fallu travailler sur les meilleurs réglages au niveau des conditions expérimentales afin d'optimiser la sensibilité et la résolution spatiale de la détection en champ proche.

## 1) Réflectométrie à haute résolution spatiale

### a) Sonde et réflectomètre

Un premier réflectomètre a été développé durant le projet Terascope. La sonde utilisée est un fil fin terminé par une pointe sur lequel une onde peut être guidée, et rayonne à sa pointe une composante longitudinale  $E_z$ . Cette sonde électrique a été utilisée pour capter le champ  $E_z$  d'un objet métallique en réflexion [117]. L'image obtenue correspond à cette composante longitudinale et non aux autres composantes. Cette première expérience a mis en évidence une résolution spatiale estimée à  $85 \mu\text{m}$  ( $\approx \lambda/33$ ).

Dans la thèse de Rachid Omarouayache, ces travaux ont été poursuivis en utilisant non plus un champ longitudinal  $E_z$  mais un champ transverse  $E_t$ . L'intérêt de tester ces sondes transverses est d'avoir à terme des sondes dédiées à la détection de toutes les composantes du champ proche. La sonde de champ transverse peut être utilisée dans la direction X et la direction Y par rotation de  $90^\circ$  de la sonde.

Nous avons utilisé une sonde de type nœud papillon (bow-tie) pour créer un champ transverse (figure 4.1 (a)). Ces sondes sont fabriquées à la main, en soudant deux triangles équilatéraux de tungstène ou d'or à la sortie d'un guide d'onde WR15. Une pièce de plastique (PLA) est utilisée pour

aider à la tenue mécanique des deux triangles. L'écart entre les pointes des triangles est un paramètre d'optimisation de la sonde en matière de sensibilité et de résolution spatiale, il s'étale typiquement de  $18\ \mu\text{m}$  à  $200\ \mu\text{m}$ . La principale difficulté dans le montage de ces sondes réside dans le positionnement en vis-à-vis des pointes des triangles.

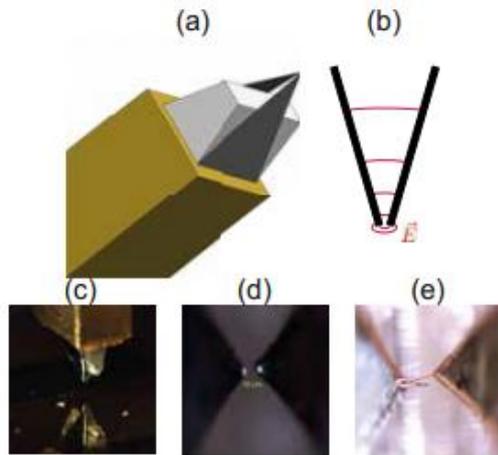


Fig. 4.1: (a) Dessin de la sonde bow-tie, (b) Profil du champ électrique dans la sonde et à son extrémité, (c) Vue générale d'une sonde en position de mesure, (d) Photographie d'une sonde en tungstène avec un écart  $e=30\ \mu\text{m}$ , (e) Photographie d'une sonde en or avec un écart de  $e=200\ \mu\text{m}$

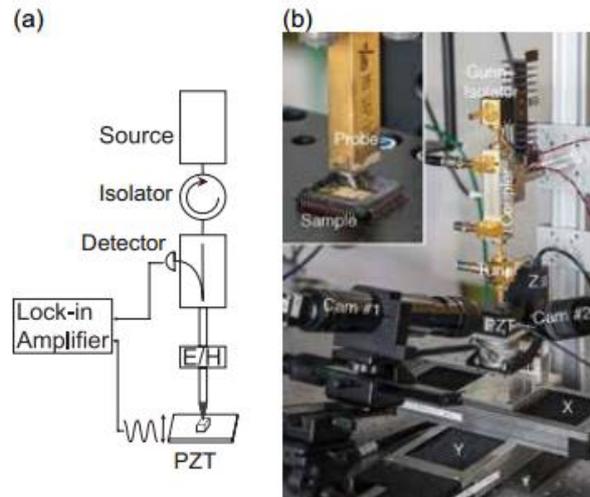


Fig. 4.2: (a) Vue schématique du réflectomètre, (b) Photographie du banc

La figure 4.1 (b) montre la polarisation du champ électrique calculé par un simulateur électromagnétique, elle est bien transverse entre les deux pointes des triangles avec un maximum d'intensité juste entre les deux, à l'image d'un dipôle transverse.

Le réflectomètre présenté à la figure 4.2 a été développé durant la thèse de Rachid Omarouyache [118], en transposant les techniques du SNOM. La sonde est fixe et l'échantillon vibre par l'intermédiaire d'un actionneur piézo dont la position verticale peut être modulée. Tout comme pour les expériences d'injection millimétrique présentées au chapitre 1, une source 60 GHz est utilisée. Elle est protégée par un isolateur. Un tuner E/H est réglé pour rendre la sonde résonante à 60 GHz, permettant d'améliorer le transfert de puissance. La puissance stockée en champ proche autour de la sonde permet une interaction avec l'échantillon qui se traduit par un signal réfléchi, qui lui est modulé à la fréquence mécanique du piézo. Le coupleur à forte isolation dirige ce signal utile vers une diode Schottky de détection puis vers une détection, synchrone avec la fréquence de modulation du piézo. L'intensité du champ proche modulé est ainsi mesurée. La sensibilité et la résolution spatiale du réflectomètre sont à optimiser en ajustant au mieux les paramètres au niveau de la sonde et de l'amplitude de la vibration du piézo.

L'optimisation de ces critères passe par une caractérisation de la sonde en situation de couplage. La mesure de courbes d'approche de la sonde à des distances variables au-dessus d'un échantillon de

référence (wafer de silicium) permet de régler l'amplitude de l'oscillation du piezo, ainsi que l'écart entre les pointes des deux triangles, et de choisir le matériau des triangles de la sonde.

La figure 4.3 présente des courbes d'approche expérimentales. Toujours dans l'idée d'avoir des images les plus résolues possibles, nous avons utilisé la détection synchrone à la fréquence fondamentale (fréquence de modulation du piézo) mais également à des ordres supérieurs, en nous limitant à l'ordre 3.

Dans le chapitre précédent nous avons précisé que la puissance stockée en champ proche autour d'un dipôle varie en  $1/r^3$ , où  $r$  est la distance sonde-échantillon. Dans l'expérience cette distance est modulée à la fréquence du piézo avec une certaine amplitude. Cette dépendance spatiale non-linéaire en  $1/r^3$  de la puissance stockée avec la distance, implique que le signal réfléchi que nous cherchons à détecter contient des composantes spectrales aux harmoniques de la fréquence de modulation, qui sert de fréquence de référence de la détection synchrone. Détecter sur les ordres supérieurs peut amener à exacerber le contraste sur l'image, et donc au final améliorer la résolution spatiale.

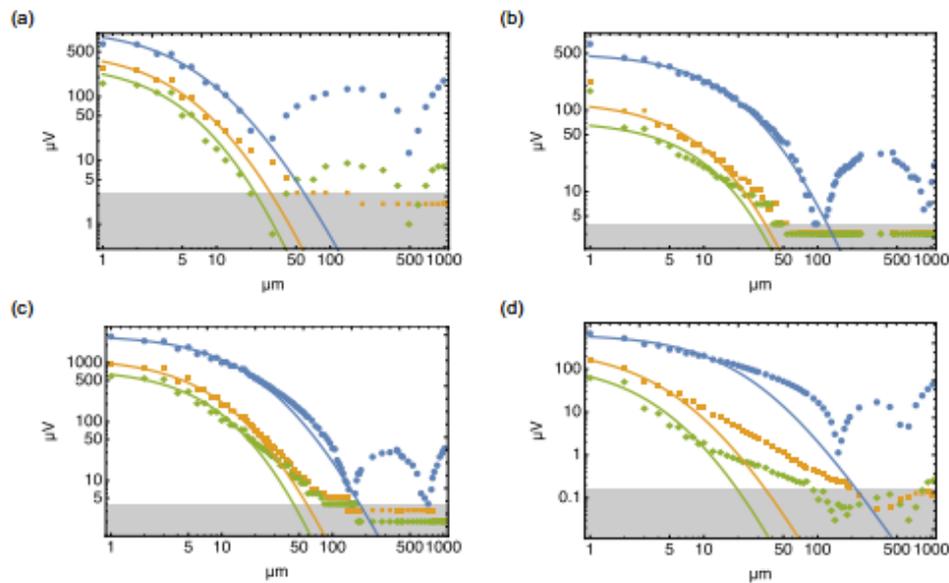


Fig. 4.3: Intensité du champ réfléchi en fonction de la distance sonde-échantillon (courbe d'approche), la détection synchrone mesure au fondamental et au deux premiers harmoniques de la fréquence de modulation du piezo, le fondamental (●), l'harmonique 2 (■), et l'harmonique 3 (◆). (a) sonde en or avec  $e=200 \mu\text{m}$ , (b) sonde en or avec  $e= 80 \mu\text{m}$ , (c) sonde en tungstène avec  $e= 30 \mu\text{m}$ , (d) sonde en tungstène avec  $e= 18 \mu\text{m}$ . Les points sont les mesures, les lignes sont issus d'un modèle développé dans [93]. Les zones grises délimitent le niveau de bruit de la détection

Un modèle théorique a été développé et présenté dans [93], en supposant que la sonde est assimilable à un dipôle électrique. La tension détectée est calculée à partir du développement en série de Fourier de la puissance stockée théorique valable dans le champ proche d'un dipôle électrique en fonction de la distance sonde-échantillon, et qui varie de manière sinusoïdale à la fréquence de modulation du piézo.

D'après la figure 4.3 les données calculées sont en bon accord avec les courbes d'approche expérimentale, jusqu'à une distance limite de  $50 \mu\text{m}$  environ. La variation en  $1/r^3$  n'est pas visible dès

le début des tracés (pour les plus faibles distances) mais survient à partir d'une certaine hauteur. Ceci semble indiquer que le dipôle équivalent à la sonde n'est pas localisé rigoureusement au bout des pointes mais est légèrement décalé en-dessous. Dans le modèle théorique la prise en compte de ce décalage valide cette hypothèse.

De manière générale, le bon accord valide le fait qu'à faible distance le signal détecté correspond à un signal de champ proche d'un dipôle électrique, quel que soit le rang de l'harmonique choisi. Les niveaux détectés diminuent selon le rang de l'harmonique. Ils restent néanmoins nettement supérieurs au plancher de bruit du banc.

Cette mesure indique également qu'une image en champ proche avec une sensibilité acceptable ne pourra être obtenue que sur une distance limitée, à moins d'augmenter fortement la puissance à la sonde.

Au-delà de cette distance, des rebonds apparaissent, révélant probablement des composantes de champ lointain qui peuvent dégrader le contraste de l'image. Ces rebonds ont d'ailleurs été fortement liés à la forme et la taille de la pièce en plastique en PLA sur la sonde. Une réduction de sa taille diminue fortement leur amplitude. Aucun rebond n'est visible pour la détection aux harmoniques 2 et 3. Ceci montre l'avantage certain de ce type de détection dans la dynamique de mesure, donc d'obtention de meilleurs contrastes.

Plusieurs sondes ont été fabriquées et testées. Les niveaux détectés changent selon le matériau des triangles utilisés, et selon l'écart entre les pointes des triangles (à part pour l'or). L'épaisseur du tungstène utilisé est beaucoup plus faible, permettant d'ailleurs d'atteindre des écarts entre triangles plus faibles qu'avec l'or.

Finalement une courbe d'approche est un bon moyen de caractérisation de la sensibilité d'une sonde, en situation de couplage. Cependant pour améliorer la résolution il est nécessaire de réduire l'écart entre les pointes. Les sondes en tungstène semblent donc mieux adaptées à notre besoin. Même si le fait de réduire l'écart (figure 4.3 (d)) diminue le niveau détecté, la comparaison avec l'écart le plus élevé (figure 4.3 (c)) montre une dynamique de mesure identique (un contraste de  $10^3$  est atteint pour la détection aux harmoniques 2 et 3).

Comme déjà observé en SNOM [115], la détection aux ordres supérieurs permet de mieux exacerber le champ proche, avec une meilleure dynamique de mesure et malgré une intensité mesurée réduite.

## **b) Résultats d'imagerie**

Après cette phase d'optimisation des paramètres clés de la sonde, nous avons imagé une partie d'un circuit intégré, et une antenne bow-tie sur substrat silicium (figures 4.4 et 4.5).

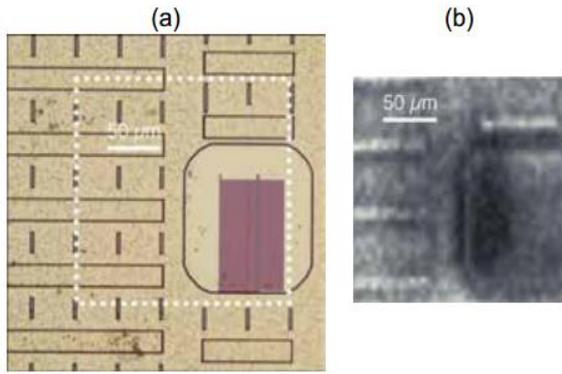


Fig. 4.4: Image de la surface d'un circuit test fourni par la société Freescale. (a) Image au microscope optique, (b) image avec notre microscope de champ proche à 60 GHz, dans la zone délimitée par les tirets

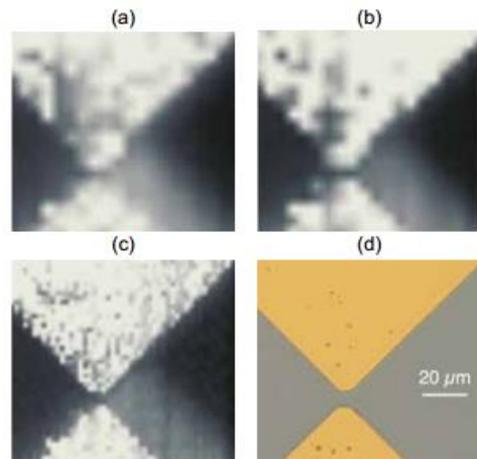


Fig. 4.5: Images avec notre microscope de champ proche à 60 GHz d'une antenne bow-tie sur substrat Si, selon le rang de l'harmonique détecté, (a) fondamental, (b) harmonique 2, (c) harmonique 3, (d) image optique

Nous avons envisagé obtenir une image, à travers le boîtier d'un circuit intégré, en raison de la transparence des plastiques aux ondes millimétriques. Cependant, d'après les courbes d'approche, au-delà de 50  $\mu\text{m}$  (avec la puissance de la sonde utilisée), aucun niveau ne peut être détecté. Or la distance typique entre la surface du boîtier et la puce est de l'ordre de 800  $\mu\text{m}$ . L'acquisition d'une image nécessite donc d'enlever le boîtier, et placer la sonde à une distance très faible.

L'image présentée à la figure 4.4 a été réalisée avec la détection réglée sur la fréquence de modulation du piézo, avec une sonde en tungstène d'écart  $e=30\mu\text{m}$ , un pas de mesure de 5  $\mu\text{m}$  et une hauteur sonde-échantillon de 5  $\mu\text{m}$ . Rappelons que la longueur d'onde à la fréquence de travail de 60 GHz est  $\lambda=5\text{ mm}$ . La plupart des structures visibles sont des plans métalliques servant de blindage.

Dans la partie inférieure droite de l'image (rectangle violet) le blindage est ouvert pour insérer une structure de test (lignes intégrées sur silicium). Des ouvertures (vias) apparaissent comme des rectangles sur l'image optique. Les rectangles les plus larges de largeur 20  $\mu\text{m}$  sont bien résolus avec au moins deux pixels. La résolution spatiale peut ainsi être estimée à 10  $\mu\text{m}$ , c'est-à-dire  $\lambda/500$ , ce qui est déjà un résultat tout à fait intéressant.

À la figure 4.5 nous avons imagé la partie centrale d'une antenne bow-tie d'espacement entre triangles de 5  $\mu\text{m}$ . Cet objet a l'avantage d'être une cible à fort contraste, comparé à l'objet précédent. Nous avons ici utilisé notre meilleure sonde en tungstène d'écart  $e=18\mu\text{m}$ , et un pas de mesure de 2  $\mu\text{m}$ . Comme observée en SNOM, l'image est de mieux en mieux résolue en utilisant une détection sur les rangs d'harmonique croissants. L'espacement entre les triangles est parfaitement visible (sur plus de 2 pixels) à l'harmonique 3.

La résolution spatiale atteint alors une valeur à l'état de l'art de 2  $\mu\text{m} \approx \lambda/2500$ , et a été publié dans la revue IEEE Transactions Instrumentation and Measurement [93].

Suite à cette phase de caractérisation et d'optimisation des sondes, du processus d'acquisition des images, nous avons testé des objets avec des profils topographiques marqués. Un coin de matériau (GaSb) a ainsi été imagé (figure 4.6), dans les deux polarisations de la sonde du plan de l'objet (direction X et direction Y). Changer de polarisation consiste concrètement à tourner la sonde de 90°. Ceci a un intérêt car cette sonde transverse n'est pas isotrope dans le plan de mesure, les images peuvent donc être différentes, contrairement à une sonde à polarisation longitudinale.

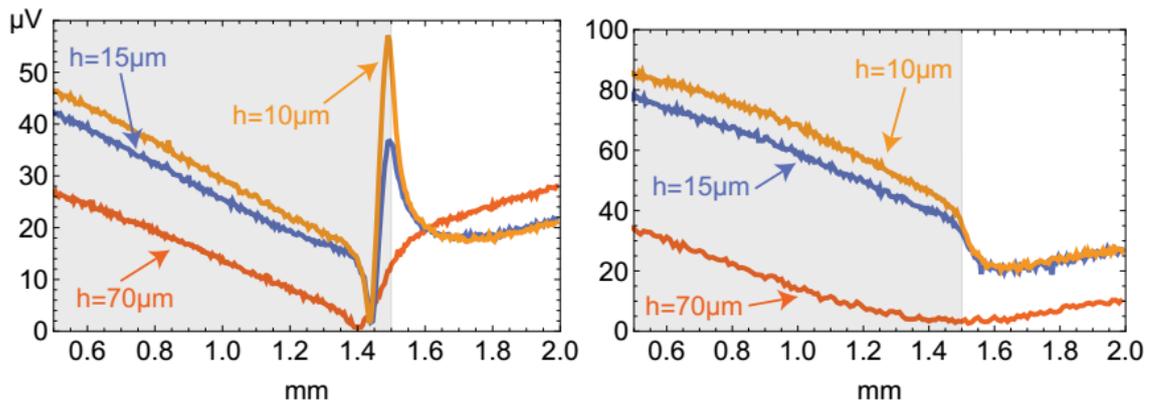


Fig. 4.6: Niveau détecté en fonction du déplacement de la sonde, selon la direction X (figure de gauche) et selon la direction Y (figure de droite), et ceci pour plusieurs hauteurs sonde-échantillon. La zone grisée correspond au matériau GaSb, et la zone blanche à du vide

Les tendances sont assez similaires dans les deux directions du plan de mesure. La polarisation du champ de la sonde dans la direction X présente au bord du matériau de fortes oscillations, d'autant plus marquées que la hauteur de la sonde est faible.

Ces oscillations témoignent probablement d'une interaction sonde-matériau particulière et forte en champ très proche [120]. Elles contribuent à confirmer qu'une image champ proche ne reflète pas la réalité (tout comme dans le domaine du visible d'ailleurs), et nécessite impérativement une interprétation. Imager un objet en se rapprochant de plus en plus près ne signifie pas en faire un grossissement. Le déplacement de la sonde dans la direction Y n'amène pas ce genre de comportement, ce qui prouve que selon la hauteur sonde-échantillon et l'orientation du dipôle, la physique de l'interaction mise en jeu est différente, mais reste complètement exploitable.

Ces expériences valident donc la faisabilité pour des objets à forte topographie d'utiliser des sondes à polarisation transverse dans les deux directions du plan de mesure.

Finalement en matière d'imagerie très haute résolution, nous avons montré un fort contraste sur des objets métalliques déposés sur un substrat silicium (figure 4.5).

Au-delà des acquisitions d'image, nous aimerions maintenant utiliser le banc en vue d'obtenir des informations physiques plus quantitatives sur la nature du matériau, comme sa conductivité, et sa constante diélectrique complexe.

Cependant cette expérience ne fait ressortir que le module du coefficient de réflexion. Pour proposer une caractérisation complète en champ proche de matériaux (partie réelle et imaginaire des constantes physiques), nous avons alors étendu le réflectomètre en vue d'obtenir des mesures vectorielles.

## 2) Réflectométrie millimétrique vectorielle en champ proche

### a) Principe de fonctionnement et premiers résultats d'imagerie

Nous souhaitons caractériser des matériaux en nous focalisant sur des mesures ponctuelles et quantitatives dans le champ proche. Dans la littérature la mesure de permittivité complexe a été mise en place dans le domaine des micro-ondes, à quelques GHz [111]. Cependant, la montée en fréquence des circuits modernes impose de transférer ce savoir-faire dans le domaine millimétrique.

La mesure de la phase de l'onde réfléchi est alors nécessaire. Les moyens mis en œuvre sur le réflectomètre en intensité pour améliorer la résolution et la sensibilité de détection sont conservés sur le nouveau banc de test.

La solution simple utilisée pour faire une mesure vectorielle repose sur une détection hétérodyne réalisée par un mélangeur I/Q. Le principe de l'expérience est présenté sur la figure 4.7, et la photographie du système sur la figure 4.8. La source Gunn 60 GHz a été remplacée par une source synthétisée de très bonne pureté spectrale, afin de réduire fortement le bruit de la mesure sachant que le signal est modulé à la fréquence d'oscillation du piézo de 40 Hz. Les avantages de la source synthétisée sont sa pureté spectrale et son accordabilité, ce qui permet d'élargir la bande de fréquence de caractérisation des matériaux. Le signal incident (de puissance 13dBm au synthétiseur) est rayonné par la sonde en champ proche, puis réfléchi par l'échantillon dont la position est modulée à la fréquence du piézo. Le signal arrivant à l'entrée du mélangeur est composé d'un signal de plus forte puissance non modulé venant directement de la désadaptation de la sonde, et du signal utile de faible puissance modulé et réfléchi par l'échantillon. La puissance délivrée par le synthétiseur doit donc être dimensionnée par rapport au niveau de puissance limite, avant la compression du mélangeur. Un atténuateur (non représenté sur la figure) permet de diminuer le niveau de puissance parasite réfléchi directement par la sonde. Le mélangeur transpose en bande de base le champ réfléchi et sort la composante en phase (I) et en quadrature de phase (Q). Deux détections, synchrones avec la fréquence de modulation du piézo, mesurent ces deux composantes. Un traitement des données de sortie des détections synchrones est nécessaire pour extraire la partie réelle et la partie imaginaire du coefficient de réflexion du matériau.

Tous les éléments de la chaîne ont été dimensionnés par nos soins et assemblés par la société LTEQ Microwave. D'après les limites en fréquence de chaque élément de la chaîne, le système complet peut fonctionner théoriquement dans une bande s'étalant de 55 GHz à 65 GHz.

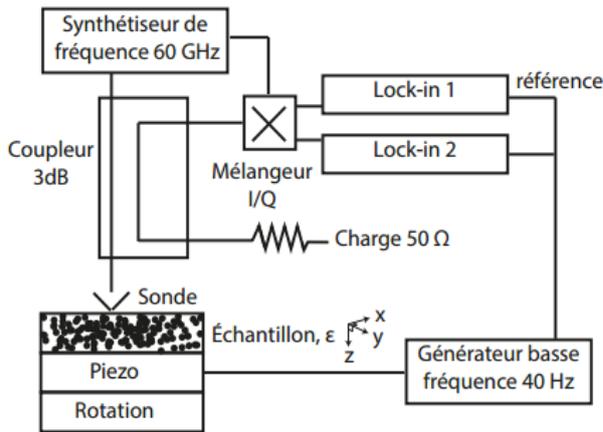


Fig. 4.7: Schéma de principe de l'expérience champ proche vectorielle



Fig. 4.8: Photographie de l'expérience

Les détections synchrones donnent accès à quatre grandeurs : les parties réelles ( $x_I$ , et  $x_Q$ ) et les parties imaginaires ( $y_I$ , et  $y_Q$ ) des voies I et Q. Leur combinaison permet de calculer les tensions complexes sur les voies I et Q, et pour finalement obtenir le module et la phase du champ électrique réfléchi  $E_{REF}$  sur l'échantillon. Le détail de l'exploitation des résultats est présenté dans la thèse de Pierre Payet [118].

À partir de cette exploitation nous avons réalisé une première image vectorielle d'une capacité intégrée (figure 4.9). Les mesures ont été faites à 59 GHz, avec une détection sur l'harmonique 3 et un pas de 10  $\mu\text{m}$ .

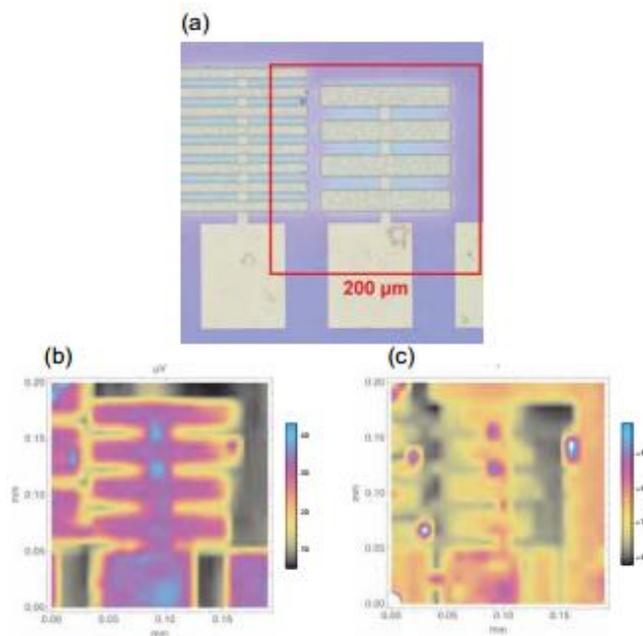


Fig. 4.9: Image vectorielle en champ proche (a) image optique de capacités interdigitées, (b) Module de  $E_{REF}$  dans la zone encadrée de (a), (c) Phase de  $E_{REF}$  dans la zone encadrée de (a)

La résolution spatiale estimée est meilleure que 10  $\mu\text{m}$ . Les images en module et en phase ont clairement montré des contrastes différents. L'image en intensité est bien résolue au niveau du peigne à 4 brins, ce qui est moins vrai pour le peigne à 8 brins. En revanche, l'image en phase a plutôt montré le contraire. L'image en phase permet d'améliorer la résolution par une dynamique plus grande.

### b) Vers une caractérisation physique de matériaux

Pour espérer pouvoir faire des mesures quantitatives (partie réelle et partie imaginaire de la permittivité) et si possible sur une large bande de fréquence, il a fallu, à l'instar d'un analyseur de réseau prévoir une procédure de calibration, pour corriger des erreurs systématiques du banc, car nous avons observé des images différentes selon la fréquence de mesure.

L'échantillon de référence choisi est de l'or. Ce métal de coefficient de réflexion connu, très proche de -1, a une rugosité très faible, et ne s'oxyde pas, contrairement aux autres très bons conducteurs. L'épaisseur de la couche d'or a été choisie supérieure à l'épaisseur de peau à 60 GHz ( $\approx 300\text{nm}$ ).

La mesure du champ réfléchi au réflectomètre d'un matériau inconnu est alors normalisée avec celle de l'échantillon de référence, et le coefficient de réflexion du matériau inconnu est déduit simplement avec la relation suivante :

$$\Gamma = \frac{E_{REF}^{inc}}{E_{IN}} \approx -\frac{E_{REF}^{inc}}{E_{REF}^{con}}$$

où  $E_{IN}$  est le champ incident avant la réflexion sur l'échantillon,  $E_{REF}^{inc}$  est le champ réfléchi mesuré du matériau inconnu, et  $E_{REF}^{con}$  est celui de la référence. Le signe négatif vient de la réflexion totale ( $\Gamma = -1$ ) au niveau de l'échantillon de référence.

Des mesures ponctuelles de champ réfléchi sur l'échantillon de référence ont été menées sur toute la bande 55 GHz – 65 GHz du système. Les quatre grandeurs  $x_I$ ,  $x_Q$ ,  $y_I$ ,  $y_Q$  des détections synchrones présentent des oscillations en amplitude et en phase non constantes le long de la bande de fréquence, comme illustré à la figure 4.10.

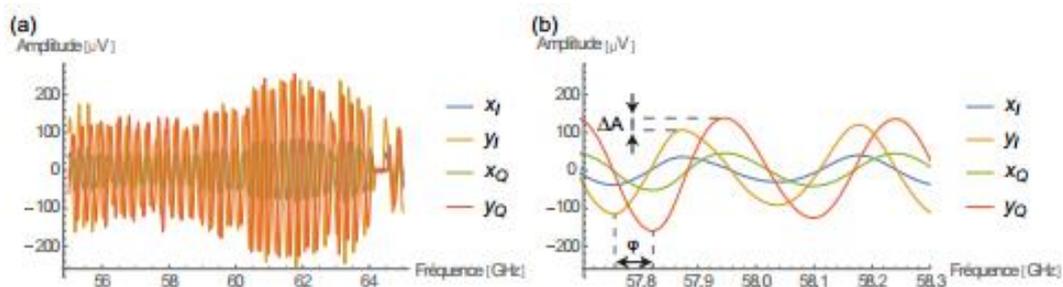


Fig. 4.10: Mesure de tensions réfléchies en champ proche sur l'échantillon d'or à la sortie des détections synchrones  $x_I$ ,  $y_I$ ,  $x_Q$ ,  $y_Q$ , (a) mesures sur la bande complète, (b) mesures sur un zoom en fréquence

Nous avons montré que l'origine de ces oscillations est directement liée à la longueur électrique du guide d'onde utilisé, que doit parcourir l'onde après réflexion sur le matériau. La fréquence d'oscillation mesurée à partir des données de la figure 4.10 (b) est de l'ordre de 290 MHz.

L'écart en amplitude et en phase observé entre les paires de données  $(x_I, x_Q)$  et  $(y_I, y_Q)$  (noté  $\Delta A$  et  $\phi$ ) met en lumière les imperfections du mélangeur I/Q, alors qu'idéalement à la sortie d'un mélangeur I/Q les amplitudes sur les 2 voies sont identiques ( $\Delta A=0$ ) et le déphasage est de  $90^\circ$ . L'équilibrage du mélangeur sur les deux voies n'est pas parfait, et il dépend de la fréquence de travail.

Une modélisation théorique des quatre grandeurs détectées prenant en compte l'imperfection du mélangeur sur l'amplitude et la phase entre les deux voies a permis de mettre au point une méthode pour compenser les erreurs induites [118].

Finalement la solution proposée a été de mesurer ces quatre grandeurs sur une période entière d'oscillation (autour de 290 MHz), pour l'échantillon de référence et l'inconnu, puis de déterminer le coefficient de réflexion avec la relation précédente, et enfin de moyenner la partie réelle et imaginaire de ce coefficient.

Toutefois cette méthode de compensation ne fonctionne pas sur la bande de fréquence complète du système (55-65 GHz), ce qui révèle simplement les limites du modèle utilisé. Nous avons donc restreint la bande de fréquence sur laquelle l'extraction du coefficient de réflexion est envisagée.

Avec la référence de mélangeur utilisé, la bande 56.5 GHz – 57.5 GHz convient pour mener la méthode. Cette plage de mesure de 1 GHz est déjà intéressante pour caractériser des matériaux peu dispersifs.

Finalement, un protocole de mesure a été mis en œuvre, et utilisé pour extraire les coefficients de réflexion en champ proche de matériaux simples et homogènes déposés en couche mince sur du verre. Des métaux (Au, Pt) et des diélectriques ( $\text{SiO}_2$ ,  $\text{Si}_3\text{N}_4$ ) rencontrés typiquement en micro-électronique ont été utilisés [118].

### 3) *Discussions et perspectives*

Le réflectomètre vectoriel permet d'envisager l'extraction de la permittivité diélectrique  $\epsilon$  locale, à partir de la connaissance du coefficient de réflexion, à condition de décrire l'interaction en champ proche réalisé. Le modèle de dipôle électrique proposé dans la littérature [103], cohérent avec une approximation quasi-statique a été utilisé.

Il est illustré à la figure 4.11. La sonde bow-tie est assimilée à un dipôle électrique parallèle au plan de l'échantillon dans son champ proche. Le champ total réinjecté dans la sonde peut être calculé comme la somme du champ du dipôle original et du dipôle image, dont l'intensité dépend des relations de passage à la surface du matériau  $\frac{\epsilon-1}{\epsilon+1}$ . Le champ réfléchi détecté sur une des harmoniques de la fréquence de modulation du piézo contient l'information de la permittivité  $\epsilon$ , dont on peut extraire la partie réelle et imaginaire. Ce modèle a été appliqué aux échantillons de test.

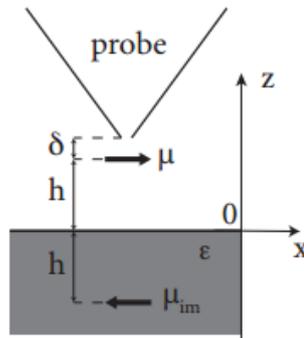


Fig. 4.11: Schéma d'interaction de la sonde bow-tie avec une interface diélectrique de permittivité relative  $\epsilon$ , basé sur le principe du dipôle image

Des valeurs de permittivité ont été extraites. Les résultats sont assez concluants. La partie imaginaire pour les métaux est bien supérieure à celle des diélectriques. Ces résultats ont été comparés avec les indices optiques mesurés par ellipsométrie. Les parties réelles sont plutôt très concordantes. Les parties imaginaires le sont moins, pour ces premiers résultats.

Notre expérience montre que les pertes sont plus élevées que celles auxquelles on peut s'attendre. Les échantillons testés ont été déposés sur du verre en couche mince, le modèle d'interaction en champ proche utilisé considère que le dipôle image est localisé dans le matériau. Les expériences sont menées à des hauteurs sonde-échantillon de l'ordre de quelques microns. Cette distance est supérieure à la taille de la couche. Dans notre cas le verre tend certainement à renforcer les pertes mesurées.

Quoiqu'il en soit, nous avons l'intention de poursuivre la fiabilisation de ce banc, en travaillant aussi davantage sur le modèle d'interaction en champ proche, qui nous permettra d'extraire des valeurs quantitatives fiables de permittivité du matériau. Nos sondes n'étant pas parfaitement transverses, la composante longitudinale induite par un décalage dans l'altitude des deux pointes de triangles peut être considérée dans le modèle d'interaction.

Les résultats actuels restent néanmoins très encourageants et montrent la faisabilité d'extraire la permittivité locale complexe d'un matériau, en champ proche et aux fréquences millimétriques. D'ailleurs l'équipe de F. Keilmann vient de publier des travaux de caractérisation, uniquement de conductivité de semi-conducteurs faiblement dopés, utilisant un banc de mesure basé sur le même principe que le nôtre et fonctionnant à 750 GHz [121].

Dans l'idée de mesurer les composantes vectorielles des champs électriques et magnétiques en champ proche, nous avons également l'intention de développer des sondes magnétiques pour chaque composante, aux fréquences millimétriques. Nous améliorerons ainsi la capacité du banc à distinguer des matériaux magnétiques, et nous pourrions envisager la mesure de perméabilité.

Nous avons d'ailleurs commencé des expérimentations sur des matériaux paramagnétiques complexes conçus par notre collègue Fériat Terki du laboratoire Charles Coulomb à Montpellier. Ces matériaux sont sensibles à un champ magnétique polarisant et nous avons montré que leur réflectivité

en champ proche à 60 GHz change selon l'intensité et l'orientation du champ. Ces résultats préliminaires soulignent la capacité du banc à caractériser des matériaux magnétiques.

## Bilan et perspectives

Depuis 2009, j'ai pu participer, animer et initier des sujets de recherche dans l'optique de construire une nouvelle thématique au laboratoire autour de l'injection électromagnétique. La démarche consiste à privilégier la mise en place au sein du laboratoire de plateformes de test et de méthodes d'analyse, d'optimisation, et de procédures de validation basées sur des outils de calcul et de simulation numérique.

Dans ce mémoire j'ai essayé de faire ressortir les méthodes de travail et les résultats majeurs obtenus, sachant que ces travaux vont continuer à se développer, et ainsi permettre de nouvelles collaborations et contrats. J'ai d'ailleurs exprimé le plus souvent en fin de chaque chapitre les principales perspectives à plus ou moins court terme.

J'aimerais récapituler brièvement les bancs de test désormais disponibles au laboratoire, et dont certains restent encore à fiabiliser :

- Nous avons mis au point des bancs dédiés à la caractérisation de la susceptibilité de composants et circuits, avec une injection du signal d'interférence en mode conduit et en mode rayonné (champ proche), et sur une bande de fréquence très large, jusqu'aux fréquences millimétriques. Ces bancs, ainsi que les méthodes d'analyse associées, sont particulièrement utiles dans les domaines de la défense et de la sécurité, aussi bien pour l'attaquant que pour le concepteur de circuits. La très récente montée en fréquence de nos bancs, jusqu'à la bande millimétrique, permet de nous positionner pour répondre aux futures menaces électromagnétiques. En complément à l'expertise au niveau de la susceptibilité EM, nous avons lancé une activité portant sur la détection à distance de systèmes avec port radio, avec le développement d'un banc de test d'un nouveau type de radar fonctionnant sur la détection de la réponse non-linéaire d'une cible. Nous pouvons ainsi apporter aux acteurs industriels et institutionnels de la défense un savoir-faire et une expertise sur la détection et la neutralisation de cibles.

- Nous avons également développé plusieurs bancs d'injection utilisant le champ proche millimétrique pour des applications d'imagerie et de microscopie. Des expériences de réflectométrie sont mises au point pour les applications suivantes :

- Imagerie à fort contraste en intensité et en phase. Le banc propose une grande dynamique de mesure. Il est basé sur une détection interférométrique sans sonde de champ proche donc avec une résolution de la taille du guide ( $\approx 2$  mm), mais avec un transfert de puissance sur l'échantillon optimisé. L'image en contraste de phase est formée avec une source d'illumination à fréquence variable (chirp), et est particulièrement intéressante car elle révèle la non-homogénéité des matériaux. Il est prévu de construire un nouveau banc de test à 100 GHz utilisant une source avec une plus grande variation de fréquence afin de distinguer encore mieux la dispersion des matériaux.

- Imagerie à haute résolution spatiale, utilisant des sondes dédiées. Une résolution au niveau de l'état de l'art, de  $2 \mu\text{m}$  à 60 GHz, a pu être atteinte avec une sonde bow-tie. Ceci est possible grâce à la vibration de l'échantillon et à la détection sur une harmonique de la fréquence de vibration.

Ce banc peut être utilisé pour caractériser et identifier des matériaux. Un réflectomètre vectoriel vient d'être mis au point dans l'optique d'améliorer la capacité de distinction des matériaux et d'extraire quantitativement et localement des constantes physiques du matériau comme la permittivité diélectrique et la perméabilité complexe.

Lors de la mise en place des bancs de test, nous essayons de limiter l'utilisation de systèmes commerciaux, qui par nature sont complètement fermés. Les techniques utilisées en champ proche (vibration de l'échantillon, détection synchrone) ne nous donnent d'ailleurs pas le choix. Nous les concevons dans l'optique d'acquérir une maîtrise dans le dimensionnement de tous les éléments de la chaîne de mesure, du signal d'injection aux données mesurées. Une phase de fiabilisation des outils est donc envisageable, en particulier pour le réflectomètre vectoriel pour lequel il nous faut tester d'autres échantillons afin de mieux appréhender les possibilités ainsi que les limites d'utilisation.

Par la suite mon intention est de continuer à faire évoluer les plateformes d'injection, ce qui contribuera à élargir leur champ d'action.

Il me semble en particulier cohérent de mettre ces moyens de tests au service de l'équipe Radiac, en essayant d'utiliser nos bancs avec des échantillons irradiés d'intérêt. L'équipe travaille à la compréhension et à la prédiction des effets du rayonnement ionisant sur l'électronique. Des outils de simulation physique sont utilisés pour aider à la compréhension des mécanismes de défaillance induits par l'irradiation. Les signaux fonctionnels des composants ou circuits avant et après irradiation sont mesurés.

Nos outils pourraient permettre une caractérisation des couches irradiées, et ainsi compléter ou affiner leurs connaissances sur les effets de l'irradiation, par exemple en leur donnant des données d'entrée pour la simulation physique. Nos expériences d'imagerie pourraient mettre en évidence des modifications physiques dues à la dose ionisante stockée dans les couches, et identifier des zones où les défauts sont davantage présents. Ainsi, pour l'équipe, ce rapprochement des thématiques serait probablement l'occasion d'utiliser de nouveaux outils de diagnostic, et également de développer des compétences et des savoir-faire, utiles à la recherche de nouvelles collaborations et contrats industriels.

J'envisage également de relancer une activité sur la problématique des effets de synergie dose ionisante et interférence EM. Nous avons réalisé un travail préliminaire dans le cadre de la thèse Cifre-défense d'Adrien Doridant (2010-2013), financée par le CEA Gramat et Thalès Alénia Space, où nous avons commencé à étudier les effets combinés de la dose ionisante et des interférences EM sur un transistor bipolaire discret. L'analyse de la susceptibilité EM du composant a été menée selon le niveau de dose déposée (rayon X et gamma). Ce premier travail a mis en évidence la réponse de composants qui sont à la fois soumis à la contrainte radiative et électromagnétique. Il s'est focalisé exclusivement sur un transistor, ce qui ne nous a pas permis de mettre en évidence des effets de synergie ou de compensation que l'on pourrait rencontrer au niveau circuit. Dans tous les cas, ces travaux originaux et précurseurs dans les deux communautés compatibilité électromagnétique et rayonnement ionisant ont

donné lieu à de nombreuses publications. Nous n'avons pas eu l'occasion de poursuivre ce sujet, les financeurs de la thèse ont préféré lancer d'autres actions, et nous nous sommes également dirigés vers d'autres sujets.

Cependant, désormais de plus en plus d'acteurs du spatial prennent conscience que l'électronique doit être évaluée sous des environnements plus complexes que ce qui se fait classiquement. La société Nuclétudes (filiale d'Airbus) envisage d'inclure la contrainte EM dans l'environnement de test. La miniaturisation et la densité croissante des composants, l'augmentation des fréquences de fonctionnement, la diminution des tensions d'alimentation, sont autant de facteurs qui renforcent la nécessité de considérer de plus en plus l'environnement EM pour tester l'électronique embarquée aux radiations. Comment évolue la susceptibilité du composant et du circuit lorsqu'il est dans un environnement radiatif ? La même question peut aussi se poser cette fois concernant son émission EM. Les zones de plus fort rayonnement EM au sein de la puce évoluent elles avec la dose déposée ?

Les moyens de tests développés récemment ainsi que les moyens d'irradiation désormais accessibles au laboratoire nous apportent davantage de solutions techniques pour répondre plus efficacement à cette problématique. Nous pouvons mener des tests d'injection jusqu'aux fréquences millimétriques, en mode conduit et rayonné au-dessus de la puce avec des sondes locales optimisées en résolution et en efficacité, d'injection ou de capture (pour l'émission EM de la puce). Nous pourrons aussi compléter nos outils de calcul en y intégrant des effets de l'irradiation.

En conclusion, ce sujet m'intéresse particulièrement, et je pense qu'il constituera pour moi une voie de recherche privilégiée dans les prochaines années.

## Bibliographie

- [1] Ramdani M. and al., The electromagnetic compatibility of integrated circuits---Past, present, and future, IEEE Trans. Electromagn. Compat., 2009, 51, pp. 78—100.
- [2] E. Sicard, S.B. Dhia, M. Ramdani, J. Catrysse, M. Coenen, “Towards an EMC roadmap for integrated circuit”, IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Torino, 2007.
- [3] R.E. Richardson, V.G. Puglielli, R.A. Amadori, “Microwave interference effect in bipolar transistors”, IEEE Transaction on Electromagnetic Compatibility, pp. 216-219, 1975.
- [4] R.E. Richardson, “Quiescent operating point shift in bipolar transistors with AC excitation”, IEEE Journal of Solid-State Circuits, vol. 14, pp. 1087-1094, 1979.
- [5] M.L. Forcier, R.E Richardson, “Microwave-rectification RFI response in field-effect transistors”, IEEE Transaction on Electromagnetic Compatibility, pp. 312-315, 1979.
- [6] R. Hoad, N.J. Carter, D. Herke, S.P. Watkins, “Trends in EM susceptibility of IT equipment”, IEEE Transaction on Electromagnetic Compatibility, vol. 46, pp. 390-395, 2004.
- [7] R. Thottappillil, D. Mansson, M. Backstrom, “Response of electrified railway facilities to intentional electromagnetic interference”, Asia-Pacific Symposium on Electromagnetic Compatibility, pp. 291-294, 2008.
- [8] W. A Radasky. and al., “Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)”, IEEE Trans. on Electromagn. Compat., vol. 46, no. 3, pp. 314–321, 2004.
- [9] D.V. Giri, F.M. Tesche, “Classification of intentional electromagnetic environment” (IEMI)”, IEEE Transaction on Electromagnetic Compatibility, vol. 46, pp3 322-358, 2004.
- [10] J. Benford, J.A. Swegle, E. Shamiloglu, “High power microwaves”, 3<sup>rd</sup> ed. CRC Press, 2015.
- [11] D. Nitsch, M. Camp, F. Sabath, J.L. ter Haseborg, H. Garbe, “Susceptibility of some electronic equipment to HPEM threats”, IEEE Transaction on Electromagnetic Compatibility, vol. 46, pp.380-389, 2004.
- [12] IEEE Recommended Practice for protecting publicly accessible computer systems from intentional electromagnetic interference (IEMI)”, IEEE Standard 1642-2015, pp. 1-39, 2015.
- [13] M. Dagys, Z. Kancleris, P. Ragulis, R. Simniskis, “Investigation of susceptibility of routers to high power microwave pulse radiation”, International Conference microwave, radar and wireless communications, pp. 1-3, 2010.
- [14] E. Schamiloglu, “High Power Microwave Sources and Applications”, Microwave Symposium Digest, 2004 IEEE MTT-S International, vol. 2, pp. 1001–1004, 2004.
- [15] M.G. Backstrom, K.G. Lovstrand, “Susceptibility of electronic systems to high power microwaves: Summary of test experience”, IEEE Transaction on Electromagnetic Compatibility, vol. 46, pp. 396-403, 2004.
- [16] Mansson D. and al., “Vulnerability of european rail traffic management system to radiated intentional EMI”, IEEE Trans. on Electromag. Compat., vol. 50, no. 1, pp. 101–109, 2008.
- [17] F. Fiori, S. Benelli, G. Gaidano, V. Pozzolo, « Investigation on VLSIS input ports susceptibility to conducted RF interference », IEEE Internationale Symposium on Electromagnetic Compatibility, pp. 326-329, 1997.
- [18] C. Lertsirimit, D.R. Jackson, D.R. Wilton, D. Erricolo, D.H.Y. Yang, “EMC coupling to a circuit board from a wire penetrating a cavity aperture”, IEEE Antennas and Propagation Society International Symposium, vol. 1, pp. 375-378, 2004.
- [19] F. Brauer, F. Sabath, J.L. Ter haseborg, “Susceptibility of IT network systems to interferences by HPEM”, IEEE International Symposium on Electromagnetic Compatibility, pp. 237-242, 2009.
- [20] T. Dubois, J. Raoult, S. Jarrix, A. Blain, A. Doridant, “Optimal Electric Wave Propagation parameters on a transmission line – Schottky Diode System”, Progress in Electromagnetics Research Letters, vol. 27, pp. 125-132, 2011.
- [21] M.A. Holloway, Z. Dilli, N. Seekhao, J.C. Rodgers, “Study of basic effects of HPM pulses in digital CMOS integrated circuit inputs”, IEEE Transaction on Electromagnetic Compatibility, vol. 54, pp. 1017-1027, 2012.
- [22] S. Jarrix, J. Raoult, A. Doridant, C. Clovis, P. Hoffmann, “Discrete Low-Frequency Transistors Subjected to High-Frequency CW and Pulse-modulated Sine Signals”, 9th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Nara, Japan, 16-18 December 2013.

- [23] C. Pouant, J. Raoult, P. Hoffmann, “Large domain validity of MOSFET Microwave Rectification Response”, in EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 10-13 November 2015, Edinburgh.
- [24] T. Dubois, S. Jarrix, J. Raoult, A. Pénarier, P. Nouvel, B. Azaïs et D. Gasquet, “Electromagnetic Susceptibility Studies of Op. Amp. and a VCO for a PLL Application”, Workshop International, EMC Compo, Toulouse, France, Novembre, 2009.
- [25] T. Dubois, J.-J. Laurin, J. Raoult, S. Jarrix, « Effect of Low and High Power Continuous Wave Electromagnetic Interference on a Microwave Oscillator System: From VCO to PLL to QPSK Receiver”, IEEE Transactions on Electromagnetic Compatibility, Vol. 56, Issue 2, pp 286-293, 2014.
- [26] J. Raoult, A. Blain, A. Doridant, S. Jarrix, “Interference Signal Effects on a High Frequency Monolithic Voltage-Controlled Oscillator: Experiments and Simulations”, IEEE Transactions on Electromagnetic Compatibility, volume 56, Issue 1, pp 51-59, 2014.
- [27] A. Doridant, J.-J. Laurin, J. Raoult, S. Jarrix, P. Hoffmann, “Preliminary study of Automatic Control Loop subjected to Pulse-modulated radiofrequency interference”, in EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 10-13 November 2015, Edinburgh.
- [28] E.M. Walling, “High power microwave weapons: Strategic and operational implications for warfare”, DTIC Document, Tech. Rep., 2000.
- [29] G. Ni, B. Gao, J. Lu, “Research on high microwave weapons”, IEEE Microwave Conference Proceedings, APMC, vol. 2, 2005.
- [30] C. Pouant, J. Raoult, P. Hoffmann, L. Chusseau, F. Torrès, « Control of a MOS inverter by out-of-band pulsed microwave excitation », Progress in Electromagnetics Research M, vol. 61, pp. 185-195, 2017.
- [31] C. Pouant, F. Torrès, A. Reineix, P. Hoffmann, J. Raoult, L. Chusseau, « Modeling and analysis of Large signal RFI effects in MOS transistors », IEEE Transactions on Electromagnetic Compatibility, vol. 61, pp. 111-120, 2019.
- [32] F. Torrès, C. Pouant, A. Reineix, P. Hoffmann, J. Raoult, L. Chusseau, « Time-Domain Analysis and Modeling of Large-Signal RFI rectification in MOS transistors », EMC Europe, 27-30 August 2018, Amsterdam.
- [33] Y. Tsividis, “Operation and Modeling of the MOS transistor, 3<sup>rd</sup> ed., New York, Oxford University Press, Inc, 2012.
- [34] W. Liu, “MOSFET Models for Spice simulation including BSIM3v3 and BSIM4”, NY, John Wiley & Sons, 2001.
- [35] A. Martorell, J. Raoult, R. Marijon, L. Chusseau, “EMI functional vulnerability identification in RF Front-ends”, in EMC Compo 2017, 11<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 4-7 July 2017, St Petersburg.
- [36] S. Kang, B. Choi, B. Kim, “Linearity analysis of CMOS for RF application”, IEEE Transaction on Microwave Theory and Techniques, vol. 51, 2003.
- [37] A. Doridant, S. Jarrix, J. Raoult, A. Blain, N. Chatry, P. Calvel, P. Hoffmann, L. Dusseau, “Impact of Total Ionizing Dose on the Electromagnetic Susceptibility of a single bipolar transistor”, IEEE Transaction on Nuclear Science, Volume 59, issue 4, Part 1, 2012, pp 860-865.
- [38] F. Fiori, V. Pozzolo, « Modified Gummel-Poon for susceptibility prediction », IEEE Transaction on Electromagnetic Compatibility, vol. 42, pp. 206-213, 2000.
- [39] E. Bouhana, “Analyse du comportement petit-signal du transistor MOS : contribution à une nouvelle approche d’extraction et modélisation pour des applications RF », Thèse de doctorat, Université de Lille, 2007.
- [40] C. Pouant, « Caractérisation de la susceptibilité électromagnétique des étages d’entrée de composants électroniques », Thèse de doctorat, Université de Montpellier, 2015.
- [41] L.B. Green, “Electromagnetic compatibility of radio telecommunications”, IEEE Proceeding – Science, Measurement and Technology, vol 141, pp. 244-247, 1994.
- [42] K. Yazbek, O. Harfoush, “Practical EMC considerations in designing PCB for RF and microwave systems”, IEEE International RF and Microwave Conference, pp. 148-152, December 2008.
- [43] M. Capstick, D. Pearce, “EMC susceptibility of low power radio receivers”, IEEE International Symposium on Electromagnetic Interference and Compatibility”, vol. 2, pp. 1293-1296, 2003.
- [44] M. F. Karsi, W. Lindsey, “Effects of CW interference on phase locked loop performance”, IEEE Transactions on Communications”, vol. 48, pp. 886-896, 2000.

- [45] A. Blanchard, "Interferences in phase locked loop", IEEE Transaction on Aerospace Electronic systems, vol. AES-10, pp. 686-697, 1974.
- [46] B. Razavi, "A study of injection locking and pulling in oscillators", IEEE Journal of Solid State, vol. 39, pp. 1415-1424, 2004.
- [47] K. Kurokawa, "Injection locking of microwave solid-state oscillators", Proceeding of the IEEE, vol. 61, pp. 1386-1410, 1973.
- [48] A. Blain, J. Raoult, A. Doridant, S. Jarrix, T. Dubois, "Effects of CW interference on a 5 GHz monolithic VCO", 8th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Dubrovnik, Croatia, 6-9 November 2011.
- [49] B. Sarkar, R. Hati, "Chaos from second-order pll in presence of CW interference", Electronics Letters, vol. 35, pp. 1217-1218, 1999.
- [50] J. Raoult, A. Blain, S. Jarrix, "An Optimizing Technique to Lower both Phase Noise and Susceptibility of a Voltage-Controlled Oscillator", 9th IEEE International Workshop on Electromagnetic Compatibility of Integrated Circuits, Nara, Japan, 16-18 December 2013.
- [51] Perahia E. and al., "IEEE 802.11 ad: Defining the Next Generation Multi-Gbps Wi-Fi", 7th IEEE Consumer Communications and Networking Conf., 2010, pp. 1-5.
- [52] Baryshevsky V. G. and al., "A compact high power microwave (HPM) source, Pulsed Power Conference", 2009 IET European, 2009.
- [53] Perdriau R. and al., "Exploration of radiated electromagnetic immunity of integrated circuits up to 40 GHz", Electron. Lett., 2011, 47, pp. 589-590.
- [54] Jackson, J. D., "Electrodynamics", Wiley, 1975.
- [55] Baudrand H. and al., "Study of radiating properties of open-ended rectangular waveguides", IEEE Trans. Antennas Propag., 1988, 36, pp. 1071-1077.
- [56] P. Payet, J. Raoult, L. Chusseau, "Remote extinction of a 2.4 GHz RF front-end using millimeter-wave EMI in the near-field", Progress in Electromagnetics Research Letters, vol. 68, pp. 99-104, 2017.
- [57] P. Payet, J. Raoult, L. Chusseau, "Disruption of a RF front-end subject to an out-of-band signal", in EMC Compo 2017, 11<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits, 4-7 July 2017, St Petersburg.
- [58] M.T. Abuelma'atti, "Radio frequency interference by demodulation mechanisms present in bipolar operational amplifiers", IEEE Transactions on EMC, vol. 37, may 1995.
- [59] R.A.H. Balmford, W. Redman-White, "New high-compliance CMOS current-mirror with low harmonic distortion for high-frequency circuits", Electron. Lett., vol. 29, 1993.
- [60] Redouté J.-M. and Steyaert M., "Current mirror structure insensitive to conducted EMI", Electron. Lett., Oct. 2005, vol. 41, no. 21, pp. 1145-1146.
- [61] P. Payet, M. Guery, J. Raoult, L. Chusseau, "Out-of-band disturbance of mm-wave EMI on RF front-ends", Microelectronics Reliability, vol. 76-77, pp. 670-673, 2017.
- [62] V. Vlasak, J. Pidanic, "The analysis of small RCS target detection in primary radar system", International Symposium ELMAR, Zadar, 2016, pp. 141-145.
- [63] L. Rong and W. Hai-yong, "The re-radiation characteristics of nonlinear target in harmonic radar detection," in *Microwave Conference, 2008 China-Japan Joint*, 2008, pp. 661-664.
- [64] P. M. Danzer and M. J. Brienza, "Radar target signature detector," US PATENT 5,191,343, 10-Feb-1992.
- [65] A. F. Martone, K. I. Ranney, K. D. Sherbondy, K. A. Gallagher, G. J. Mazzaro, and R. M. Narayanan, "An overview of spectrum sensing for harmonic radar," in *Fundamentals of Electrical Engineering (ISFEE), 2016 International Symposium on*, 2016, pp. 1-5.
- [66] G. J. Mazzaro, A. F. Martone, K. I. Ranney, and R. M. Narayanan, "Nonlinear Radar for Finding RF Electronics: System Design and Recent Advancements," *IEEE Trans. Microw. Theory Tech.*, vol. 65, no. 5, pp. 1716-1726, May 2017.
- [67] K. A. Gallagher, R. M. Narayanan, G. J. Mazzaro, K. I. Ranney, A. F. Martone, and K. D. Sherbondy, "Moving target indication with non-linear radar," in *Radar Conference (RadarCon), 2015 IEEE*, 2015, pp. 1428-1433.
- [68] V. Viikari *et al.*, "Technical solutions for automotive intermodulation radar for detecting vulnerable road users," in *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th*, 2009, pp. 1-5.

- [69] B. G. Colpitts and G. Boiteau, "Harmonic Radar Transceiver Design: Miniature Tags for Insect Tracking," *IEEE Trans. Antennas Propag.*, vol. 52, no. 11, pp. 2825–2832, Nov. 2004.
- [70] F. Crowne and C. Fazi, "Nonlinear radar signatures from metal surfaces," in *2009 International Radar Conference "Surveillance for a Safer World" (RADAR 2009)*, 2009, pp. 1–6.
- [71] H. Aniktar, D. Baran, E. Karav, E. Akkaya, Y. S. Birecik, and M. Sezgin, "Getting the Bugs Out: A Portable Harmonic Radar System for Electronic Countersurveillance Applications," *IEEE Microw. Mag.*, vol. 16, no. 10, pp. 40–52, Nov. 2015.
- [72] K. Wincza, S. Gruszczynski, and J. Borgosz, "Dual-band capacitive feed antenna for nonlinear junction detection device," in *Microwave Techniques, 2008. COMITE 2008. 14th Conference on*, 2008, pp. 1–4.
- [73] G. J. Mazzaro, A. F. Martone, and D. M. McNamara, "Detection of RF Electronics by Multitone Harmonic Radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 1, pp. 477–490, Jan. 2014.
- [74] A. Martorell, J. Raoult, R. Marijon, and L. Chusseau, "EMI functional vulnerability identification in RF Front-Ends," in *Electromagnetic Compatibility of Integrated Circuits (EMCCompo), 2017 11th International Workshop on the*, 2017, pp. 15–20.
- [75] C. Fazi, F. Crowne, and M. Ressler, "Link budget calculations for nonlinear scattering," in *Antennas and Propagation (EUCAP), 2012 6th European Conference on*, 2012, pp. 1146–1150.
- [76] A. Martorell, J. Raoult, R. Marijon, and L. Chusseau, "RF Front-Ends Nonlinearity Characterization Using Reflected Power," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 6, pp. 1925–1931, Dec. 2017.
- [77] J. C. Pedro and N. B. Carvalho, *Intermodulation distortion in microwave and wireless circuits*. Boston: Artech House, 2003.
- [78] K. A. Gallagher, R. M. Narayanan, G. J. Mazzaro, and K. D. Sherbondy, "Linearization of a harmonic radar transmitter by feed-forward filter reflection," in *Radar Conference, 2014 IEEE*, 2014, pp. 1363–1368.
- [79] A. Martorell, "Détection à distance d'électroniques par l'intermodulation », thèse, Université Montpellier, 2018
- [80] J. Raoult, A. Martorell, L. Chusseau and C. Carel, "Intermodulation Radar for RF receiver Detections," *2018 European Radar Conference (EURAD)*, Madrid, 2018.
- [81] N. B. De Carvalho and J. C. Pedro, "Large-and small-signal IMD behavior of microwave power amplifiers," *IEEE Trans. Microw. Theory Tech.*, vol. 47, no. 12, pp. 2364–2374, 1999.
- [82] K. A. Gallagher, G. J. Mazzaro, A. F. Martone, K. D. Sherbondy, and R. M. Narayanan, "Derivation and validation of the nonlinear radar range equation," 2016, p. 98290P.
- [83] T. Dubois, S. Jarrix, A. Penarier, P. Nouvel, D. Gasquet, L. Chusseau, « Near-field electromagnetic characterization and perturbation of logic circuits », *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 11, pp. 2398-2404, 2008.
- [84] H. Whiteside, R.W.P. King, "The loop antenna as a probe", *IEEE Transactions on Antennas and Propagation*, vol.12, no. 3, pp. 291-297, May 1964.
- [85] C. Taylor et al., "The response of a terminated two-wire transmission line excited by a nonuniform electromagnetic field", *Ant. And Propag.*, *IEEE Trans. On*, vol. 13, 1965.
- [86] M. Spang, M. Albach, G.Schubert, "Response of a Magnetic Loop Probe to the Current and Voltage on a Microstrip Line", *Electromagnetic Compatibility, 2008, EMC 2008, IEEE International Symposium on*, 18-22 August 2008, Detroit, USA.
- [87] A. Boyer, B. Vrignon, J. Shepherd, M. Cavarroc, "Evaluation of the near-field injection method at integrated circuit level", *EMC Europe, Dresden*, 2014.
- [88] A. Dehbaoui, J.M. Dutertre, B. Robisson, A. Tria, « Electromagnetic transient faults injection on a hardware and a software implementations of aes », *Fault Diagnosis and Tolerance in Cryptography, 2012 Workshop on*, *IEEE*, 2012, pp. 7-15.
- [89] F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, P. Maurine, « Local and direct EM injection of power into CMOS integrated circuits », *Fault Diagnosis and Tolerance in Cryptography, 2011 Workshop on*, *IEEE*, 2011, pp. 100-104.
- [90] J.J. Quisquater, D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards", *Smart Card Programming and Security*, Springer, 2001, pp. 200-210.
- [91] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, P. Maurine, « Magnetic Microprobe Design for EM Fault Attack », *EMC Europe, 2013, Bruges*, pp 949-954.

- [92] R. Adam, L. Chusseau, T. Grosjean, A. Penarier, J.P. Guillet, D. Charraut, "Near-field wire-based passive probe antenna for the selective detection of the longitudinal electric field at terahertz frequencies", *Journal of Applied Physics*, vol. 106, p. 073107, 2009.
- [93] L. Chusseau, P. Payet, J. Raoult, « Optimization of near-field image capture with millimeter-wave bow-tie probes », *IEEE Transactions on Instrumentation and Measurement*, vol 66, Issue 1, pp 61-68, 2017.
- [94] C. A. Balanis, *Antenna Theory – Analysis and Design*. New York: Wiley, 1982, 2<sup>nd</sup> ed.
- [95] N. Hamilton, "The Small-Signal Frequency Response of Ferrites", *High Frequency Electronics*, June 2011.
- [96] Q. Yu, T.W. Holmes, K. Naishadham, "RF Equivalent Circuit Modeling of Ferrite-Core Inductors and Characterization of Core Materials", *IEEE Transactions on Electromagnetic Compatibility*, vol. 44, no. 1, February 2002.
- [97] H. Johnson et al., "High speed digital design: a handbook of black magic", *Modern Semiconductor design*. Prentice Hall, 1993.
- [98] J. Raoult, P. Payet, Z. Fellah Touta, L. Chusseau, "Injection électromagnétique en champ proche sur circuit intégré », *XXème Journées Nationales Microondes (JNM)*, 16-19 mai 2017, St Malo.
- [99] C. Carobbi, L. Millanta, "Analysis of the common-mode rejection in the measurement and generation of magnetic fields using loop probes", *Instrumentation and Measurement, IEEE Trans. On*, vol. 53, pp. 514-523, 2004.
- [100] J. Raoult, P. Payet, R. Omarouayache, L. Chusseau, "Electromagnetic coupling circuit model of a magnetic near-field probe to a microstrip line", in *EMC Compo 2015, 10<sup>th</sup> International Workshop on Electromagnetic Compatibility of Integrated Circuits*, 10-13 November 2015, Edinburgh.
- [101] R. Omarouayache, J. Raoult, P. Payet, L. Chusseau, B. Vrignon, J. Shepherd, A. Boyer, « Modèle d'injection électromagnétique en champ proche sur circuit intégré, XIXème Journées Nationales Microondes (JNM), 2-5 Juin 2015, Bordeaux.
- [102] S. Ben Dhia, A. Boyer, B. Vrignon, M. Deobarro, T.V. Dinh, "On-chip noise sensor for integrated circuit susceptibility investigations", *Instrumentation and Measurement, IEEE Trans. On*, vol. 61, pp. 696-707, 2012.
- [103] L. Novotny, B. Hecht, "Principles of nano-optics", Cambridge, MA, USA, 2006.
- [104] A.J.L. Adam, "Review of near-field terahertz measurement methods and their applications", *J. Infr., Millim. Terahertz Waves*, vol. 32, pp. 976-1019, 2011.
- [105] B.T. Rosner, D.W. van der Weide, "High-frequency near-field microscopy", *Rev. Sci. Instrum.*, vol. 73, pp. 2505-2525, 2002.
- [106] A. Imitaz, T.M. Wallis, P. Kabos, « Near-field scanning microwave microscopy : An emerging research tool for nanoscale metrology », *IEEE Microw. Mag.*, vol. 15, pp. 52-64, 2014.
- [107] A. Imitaz, S.M. Anlage, "Effect of tip geometry on contrast and spatial resolution of the near-field microwave microscope", *J. Appl. Phys.*, vol. 100, pp. 044304, 2006
- [108] S. Gu, K. Haddadi, A. El Fellahi, T. Lasri, "Setting parameters influence on accuracy and stability of near-field scanning microwave microscopy platform", *IEEE Trans. Instrum. Meas.*, vol. 65, pp. 890-897, 2016.
- [109] A.N. Reznik, "Quasistatics and electrodynamics of near-field microwave microscope", *J. Appl. Phys*, vol. 115, pp. 084501, 2014.
- [110] K. Haddadi, T. Lasri, "60 GHz near-field six-port microscope using a scanning slit probe for subsurface sensing", *IEEE Sensors Journal*, vol. 12, pp. 2575-2576, 2012.
- [111] A. Gregory, J. Blackburn, T. Hodgetts, R. Clarke, K. Lees, S. Plint, G. Dimitrakis, "Traceable measurement and imaging of the complex permittivity of a multiphase mineral specimen at micron scales using a microwave microscope", *Ultramicroscopy*, vol. 172, pp. 65-74, 2017.
- [112] C. Plassard et al, "Detection of defects buried in metallic samples by scanning microwave microscopy", *Phys. Rev. B*, vol. 83, pp. 121409, 2011.
- [113] K. Moon et al., "Subsurface nano-imaging by broadband terahertz pulse near-field microscopy", *Nano Lett.*, vol. 15, pp. 549-552, 2014.
- [114] A.J.L. Adam, N.C.J. van der Valk, P.C.M Planken, "Measurement and calculation of the near-field of a terahertz apertureless scanning optical microscope", *J. Opt. Soc. Amer. B*, vol.24, pp. 1080-1090, 2007.
- [115] B. Knoll, F. Keilmann, "Enhanced dielectric contrast in scattering-type scanning near-field optical microscopy", *Opt. Commun.*, vol. 182, pp. 321-328, 2000.

- [116] J.P. Guillet, L. Chusseau, R. Adam, T. Grosjean, A. Penarier, F. Baida, D. Charraut, « Continuous-wave scanning terahertz near-field microscope », *Microwave and Optical Technology Letters*, vol. 53, pp. 580-582, 2011.
- [117] J.P. Guillet, “Développement d’un système de microscopie en champ proche terahertz”, Thèse, Université de Montpellier, 2010.
- [118] Rachid Omarouayache « Imagerie et Injection électromagnétique en champ proche micro-onde et millimétrique », Thèse de l’Université de Montpellier, soutenue le 16 décembre 2015.
- [119] Pierre Payet, « Injection électromagnétique et Microscopie en champ proche sur structures irradiées », Thèse à l’Université Montpellier, soutenue le 1 octobre 2018.
- [120] J.J. Greffet, R. Carminati, “Image formation in near-field optics”, *Prog. Surf. Sci.*, vol. 56, pp. 133-137, 1997.
- [121] C. Liewald, S. Mastel, J. Hesler, A. J. Huber, R. Hillenbrand, F. Feilmann, “All-electronic terahertz nanoscopy”, *Optica*, vol. 5, 2018.

**ANNEXE**

**SELECTION de PUBLICATIONS**

# Intermodulation Radar for RF Receiver Detections

Jérémy Raoult<sup>\*1</sup>, Alexandre Martorell<sup>\*#</sup>, Laurent Chusseau<sup>\*</sup>, Christian Carel<sup>#</sup>

<sup>\*</sup>IES, University of Montpellier, France

<sup>#</sup>Thales Communications & Security, TCS, France

<sup>1</sup>raoult@ies.univ-montp2.fr

**Abstract** — Nonlinear radars are often used to detect the presence of RF electronics. In the state-of-art most of researchers has chosen to exploit the second-harmonic response of target. But its antenna is usually not impedance-matched at these harmonics, requiring that the useful signal is radiated by unintentional antennas formed by traces on the circuit board. A strong incident power is therefore required to guarantee a detection with an acceptable range. In this paper we propose an intermodulation radar whose incident and reflected signals are both captured and emitted by the antenna of the target.

**Keywords** — Nonlinear radar, Intermodulation, RF receivers, Semi-empirical radar range equation.

## I. INTRODUCTION

The increase of hostile electronic devices on both theatres of operation and urban environments mandatory require an efficient detection system. These enemy devices are triggered remotely via an EM wave emitted by an operator. The aim of this work is to detect these devices by revealing the presence of a hidden RF receiver. RF systems are readily available on the market, and can be found in large numbers in an hostile context [1], [2]. A RF system is difficult to detect by a conventional linear radar measuring the reflection of a target by the same frequency that has been emitted [3]. Its small size and geometry drastically reduce its radar cross-section, making detection extremely difficult. That is why nonlinear radar is used. Its specificity is to detect an electronic target manufactured by man in a surrounding clutter by relying on the non-linear properties of the target. The harmonic radar is mainly used for the detection of RF electronics [4] [5], [6]. A RF receiver is known to be highly non-linear and its front-end is particularly exposed to electromagnetic interference since it is placed just behind the antenna [7]. The excitation of these nonlinearities by an EM signal can cause a significant harmonic reemission. Conventional harmonic radars transmit a wave containing a single frequency  $f_0$ , which is not necessarily within the operating band of the device. A RF receiver is naturally narrowband and its antenna is not impedance-matched at both  $f_0$  and its harmonics. As a result, the reflected signal at these new frequencies is radiated by traces within the device, and not by the antenna [8]–[10]. A large incident power and a very low receiver sensitivity are thus required to guarantee the detection of the target. This led to the development of intermodulation radars [4].

Exploiting the intermodulation response of targets could be a solution with many advantages, like a more efficient detection of wireless communicating systems or an easier implementation of the radar. The intermodulation radar transmits two frequencies  $f_1$  and  $f_2$  and receives the intermodulation product whose frequencies are inside the bandwidth of the RF receiver. The

frequency-of-interest is here the third intermodulation product (IM3), which can be in the receiver bandwidth if the two incident frequencies are very close. So, IM3 is radiated by the target antenna. We can therefore expect a better sensitivity of this detection technique, and the constraint on incident power could be more flexible.

In this work, the implementation of an intermodulation radar is presented. We emphasize on design principles relevant to detecting and identifying RF receivers. The main problems due to the design of such radar are exposed, in particular we point out the main contribution of parasitic intermodulation distortion in the useful signal, and the way to minimize it. Experiments results on several targets are then shown. The nonlinear link budget is presented. The detection range is estimated using the true nonlinear response with respect to the large power level of the incident signal, and not only using extrapolations from the weak non-linear response of the target.

## II. INTERMODULATION RADAR TEST BENCH

The wideband intermodulation radar test bench is shown in Fig. 1. Its bandwidth ranges from 300 MHz to 2500 MHz Two Keysight N5171B synthesizers are used to generate the CW frequencies  $f_1$  and  $f_2$  with the same amplitude at a variable incident power ranging up to 27 dBm. The aim is to receive and sense the IM3 tone ( $2f_2 - f_1$ ) produced by the nonlinearities of the receiver under test. During the implementation of the test-bench we paid attention to minimize the contribution of parasitic intermodulation distortion in the useful signal. The reduction of the residual intermodulation allows a decrease in the minimum IM3 level detectable. An isolator is inserted in each channel in order to linearize the emission signal of the radar and avoid any mixing product between the two incident frequencies  $f_1$  and  $f_2$ .

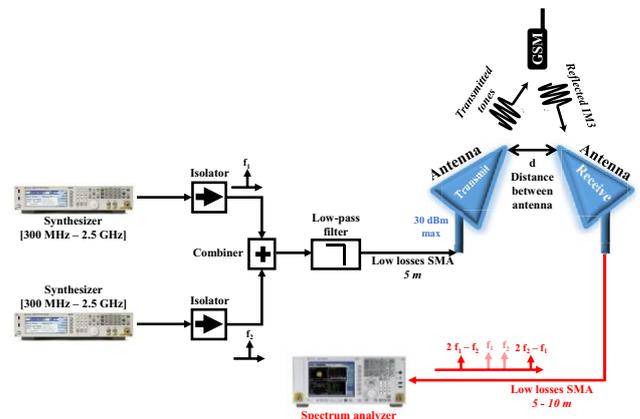


Fig. 1. Intermodulation radar test-bench.

The isolation of the power combiner was selected as high as possible thereby preventing one RF source to inject into the other and thus perturb its normal operation. A low-pass filter removes second-order harmonic components ( $2f_1$ ,  $2f_2$ ) that are likely to create an intermodulation product via indirect mixing on the RF target [11], [12]. Far-field radiation is obtained with two wideband antennas (AARONIA HyperLOG 4025), one for emission of the incident signal, and one for detection.

The IM3 tone generated by the target is detected by the radar receiver antenna. The distance  $d$  between the transmitter and receiver antennas must be chosen carefully. It must be large enough to avoid coupling between the antennas. In fact the receive chain is non-linear and able to create additional IM3 distortion that lowers drastically the detection threshold if too powerful incident power is directly coupled. To reduce more efficiently this crosstalk the antennas are used in a cross-polarization configuration. A 2 m distance was shown experimentally to ensure a comfortable detection threshold of -110 dBm at an incident power of 27 dBm. The active part of the receive chain is provided by a spectrum analyser that quantifies the IM3 tone emitted by the RF target. The spectrum analyser is settled to take advantage as much as possible of its dynamic range and sensitivity. This is achieved by lowering the bandwidth resolution, which must be accompanied by a correspondent increase in sweep time and a reduction in frequency span. To accord with usual narrowband RF front-ends, the difference in tones' frequency  $f_2 - f_1$  is chosen at 1 MHz. In the same time a span of 10 kHz and a resolution bandwidth of 100 Hz are used. The typical measurement time is about 5 minutes and a smallest power level detectable of -120 dBm obtained by averaging. Different targets whose operating bands fall within the radar frequency bandwidth (GSM, walkie-talkie, remote-controlled car...) are tested.

### III. EXPERIMENTAL RESULTS

The experiments are conducted in an external environment as close as possible to a theatre of operation. We experienced the radar on a walkie-talkie, which is a target-of-interest operating in the 400 MHz frequency band. Our RF receiver detection method require to inject the two incident frequencies within the frequency band of the system. Transmission using stepped-frequency CW waveforms is thus required. The tones' frequency difference  $f_2 - f_1$  remains constant. A fixed incident power level is used. The polarization of the transmission antenna is matched to that of the target in order to enhance the amount of incident wave captured. Fig. 2 depicts the IM3 power received by the radar when the frequencies varies from 300 MHz to 600 MHz. Two standoff-distances (between the radar and the target) are considered and  $r_1$  is the distance between the transmitter antenna and the target and  $r_2$  is the distance between the receiver antenna and the target. These results evidence an interesting property of the radar which reveal the operating bandwidth of a receiver, ranging here from 400 MHz to 470 MHz. Notice first that no IM3 signal can be detected if  $f_1$  and  $f_2$  are not included in the target bandwidth, and second that the IM3 level detected are relatively high and easily measurable. The latter is worth to be pointed out because it occurs in spite

of the weak incident power as compared to values typically used in the harmonic radar [2], [4], [6]. As expected when the distance-to-target goes up the results are noisier but even at a distance of 5 m the bandwidth identification can be performed. Once the walkie-talkie bandwidth is identified, we fix the incident frequencies  $f_1$  and  $f_2$  within the operating band and sweep the transmitter power from low to high level. Fig. 3 shows the evolution of the walkie-talkie IM3 power received as a function of the incident power. Incident frequencies  $f_1$  and  $f_2$  are chosen at 401 MHz and 402 MHz respectively, the resulting IM3 frequency is at 400 MHz. Two distance-to-target are tested. The measurements at a distance  $r_1$  of 1 m and 2 m are compared to those performed in the conducted mode [12]. This mode provides the susceptibility to intermodulation of the target, on a wide incident power range. It directly measured the IM3 power on the antenna port. As seen on the Fig. 3, the IM3 power measured in the conducted mode reflected exhibits a slope of 3dB/dB at low incident power which corresponds to the classical evolution for an RF receiver operating in a weakly nonlinear regime [12]. At higher incident powers the nonlinear behavior of the system become stronger, and the IM3 response exhibits strong changes of slope and minima. If we compare with the results obtained in the radiated mode (radar operation) we observe similarities in shape but not in amplitude. This is mainly due to the attenuation of power in the free space associated with the propagation of the incident and the reflected wave, and to a lesser extent to the polarization mismatch between antennas (transmitter-target, and target-receiver). This is confirmed when we observe results on the two distance-to-target, for  $r_1 = 1$  m and  $r_1 = 2$  m. The two curves are very similar but are just shifted in radiated power. Moreover we observe that only the stronger nonlinear behavior of the target is revealed. At -110 dBm which corresponds to the detection threshold of the radar, the typical slope of 3dB/dB for the IM3 response is not reached. This is crucial if we want to derive a realistic link budget for this radar.

### IV. NON-LINEAR LINK BUDGET AND DETECTION RANGE

In this section we derive the intermodulation radar range equation. In the literature the nonlinear radar equation considers a simplified nonlinear model of the target.

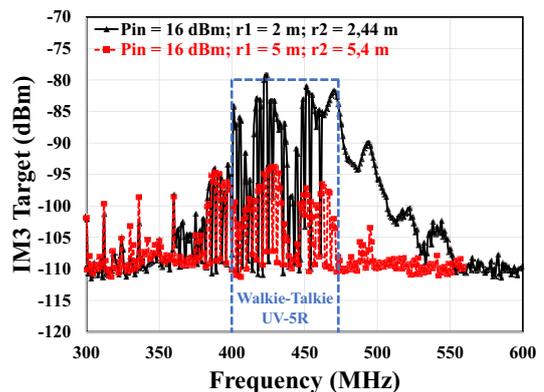


Fig. 2. IM3 power reflected and radiated by the target antenna, in two distances-to-target. Incident frequencies varies from 300 MHz to 600 MHz, with a 1 MHz tone's difference  $f_2 - f_1$ .

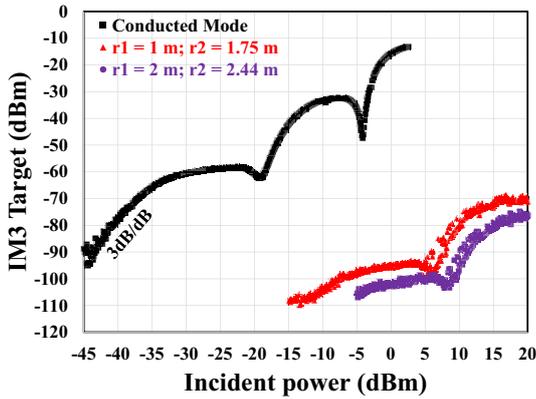


Fig. 3. IM3 power versus the transmitter power, measured in the conducted and the radiated mode. Two distance-to-target are tested.

It assumes that the RF system always operate in a weakly nonlinear regime, whatever the incident power level involved [13]. A simple power series is used to model the nonlinear behavior of the system. This approach is qualitatively interesting because it proposes a simple prediction of the nonlinear response to various input conditions, and is simple to implement.

In this case the output to input relationship for the intermodulation tone follows a 3:1 ratio, on a wide input power. This monotonous evolution is not consistent with the experimental results depicted in the Fig. 3, where many change of slope and minima are visible. Considering this simplified nonlinear behavior leads to a false estimation of the radar detection range. In this paper we do not propose a theoretical approach based on a large-signal model of the target, which is generally a difficult task, especially without the knowledge of internal details of the system. A semi-empirical approach is preferred, based on the experimental results obtained in the conducted mode.

Now consider a schematic view of the radar to introduce the quantities involved in the radar equation. The Fig. 4 illustrates the path taken by the signal to receive a response from a nonlinear target. The transmitter emits  $f_1$  and  $f_2$ , with a power  $P_T$ . The wave travels a distance  $r_1$  to the target, which captures a power  $P_C$  at the two tones via its antenna. This energy generate an in-band intermodulation distortion at the first nonlinear stage of the system, which are partly reflected at the input, and further radiated by the antenna. The power reflected by the receiver  $P_{IM3 \text{ Target}}$  at the IM3 frequency ( $2f_2 - f_1$ ) travels a distance  $r_2$  to the radar receiver.  $P_R$  is the IM3 power emitted by the target and captured by the receiver antenna. Based on the Friis equation  $P_C(f_1, f_2)$  can be written as:

$$P_C(f_1, f_2) = \beta_1 \frac{P_T G_T G_{Target}}{(4\pi)^2 r_1^2} \lambda_{f_1, f_2}^2 \quad (1)$$

Where  $G_T$  is the gain of the transmitter antenna,  $G_{Target}$  the gain of the target, and  $\lambda_{f_1, f_2}$  is the wavelength of incident frequencies ( $f_1$  et  $f_2$  are very close).  $\beta_1$  is the polarization loss factor, which is extremely dependent on the orientation of the transmitter antenna.

$P_{Target-IM3}$  corresponds to the real nonlinear response of the target, measured in a conducted mode, as depicted in Fig. 3. We introduce a function  $f$  such as:

$$P_{Target-IM3} = f(P_C(f_1, f_2)) \quad (2)$$

The function  $f$  represents the IM3 power level when varying the power  $P_C$  received by the target antenna. Fig. 3 shows a plot of this function for the walkie-talkie.

Finally the received power  $P_R$  can be written as:

$$P_R(2f_1 - f_2) = \beta_2 \frac{P_{Target-IM3} G_R G_{Target}}{(4\pi)^2 r_2^2} \lambda_{2f_1 - f_2}^2 \quad (3)$$

Where  $G_R$  is the gain of the receive antenna,  $\lambda_{2f_1 - f_2}$  is the wavelength of the IM3 tone, and  $\beta_2$  is the polarization loss factor. These three equations form a semi-empirical radar equation valid both in weakly and strongly nonlinear operation regimes. We can use this set of equations to estimate the detection range, for two RF targets: a walkie-talkie, and a 2.4 GHz receiver.

Fig. 5 shows the maximum range  $r_1$  as a function of the transmitter power  $P_T$ , for two targets. This maximum range corresponds to the distance-to-target  $r_1$  such as the receive power  $P_R$  equal the detection threshold of -110 dBm.

The polarization loss factors  $\beta_1$  and  $\beta_2$  are extracted with the experimental results depicted in Fig. 3, for distance-to-target  $r_1 = 1$  m and  $r_2 = 1.75$  m. Knowing ( $P_T$ ,  $P_R$ ,  $r_1$ ,  $r_2$ ),  $\beta_1$  and  $\beta_2$  can easily be calculated with the equations (1) and (3). Table 1 depicts the values used to compute the range shown in the Fig. 5, for the walkie-talkie.

Table 1. Antenna gain and polarization loss factors used for the walkie-talkie.

$G_T$ [dBi]	$\beta_1$ [dB]	$G_{Target}$ [dBi]	$\beta_2$ [dB]	$G_R$ [dBi]
4	-3	2	-16	4

The transmitter antenna is experimentally set to the optimum polarization with respect to the target, hence the weaker loss is obtained on the transmit path. But the transmitter and receiver antennas have to be cross-polarized to reduce the crosstalk, so the polarization loss factor in the receive path  $\beta_2$  is large. In Fig. 5 the transmitter power has been limited to 40 dBm leading to a detection range of approximately 50 m for the walkie-talkie and 10 m for the 2.4 GHz receiver. These results depend strongly of the susceptibility of the target to intermodulation. In addition, the target operating in the highest frequency band has a reduced maximum detection range because of a shortened wavelength.

## V. MULTI-TARGET DETECTION

Now we extend our study to others devices. A remote-controlled car and a microphone receiver are added to the systems previously tested. These systems are placed side-by-side and a sweep in incident frequencies from 300 MHz to 2.5 GHz are used. Fig. 6 shows the intermodulation response of the targets as a function of the transmitter frequencies at a distance-to-target of 2 m.

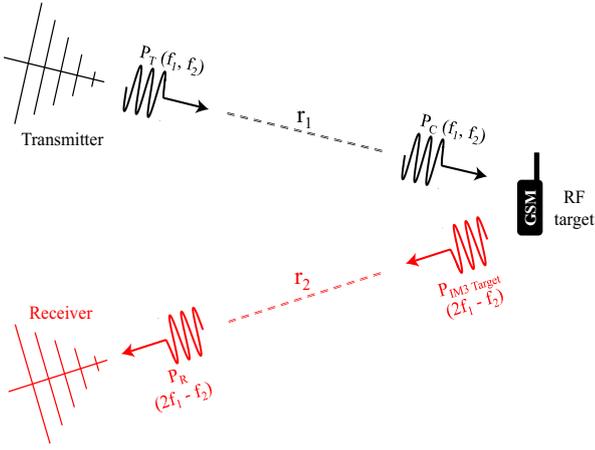


Fig. 4. Schematic view of radar signal path.

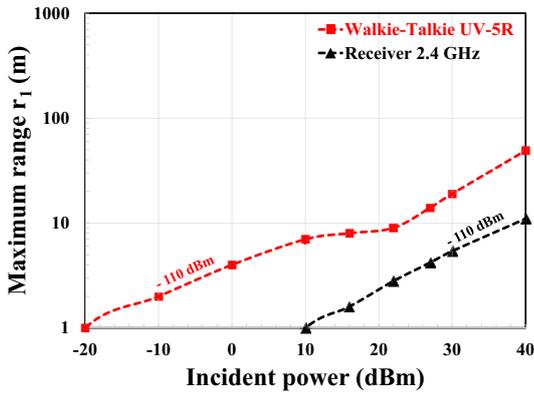


Fig. 5. Maximum range versus transmitter power for two nonlinear targets.

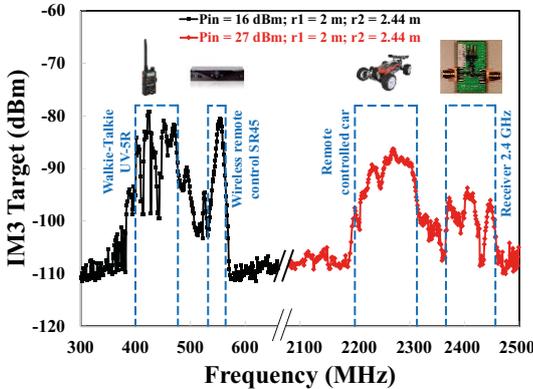


Fig. 6. Detection of many targets. The IM3 power received by the radar versus the transmitter frequencies.

For the systems operating in the highest frequency band the incident power is increased up to 27 dBm, in order to improve the sensitivity. As an evidence, the system reveals the operating bandwidth of each target.

## VI. CONCLUSION

This paper details the implementation of a nonlinear radar for detecting the presence of RF receivers. The proposed radar exploits target intermodulation responses. Unlike to the conventional harmonic radars, the transmitter frequencies are captured by the target antenna which re-emits the resulting intermodulation tone created by the nonlinearities of the device. Transmission using stepped-frequency CW waveforms is thus required. An identification of the bandwidth of the receiver under test is revealed. A reduced incident power can also be used, with an acceptable range of detection. Further development will involve other radar with a single antenna to take benefit of the very close transmitted and received frequencies.

## REFERENCES

- [1] G. J. Mazzaro, A. F. Martone, and D. M. McNamara, "Detection of RF Electronics by Multitone Harmonic Radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 1, pp. 477–490, Jan. 2014.
- [2] A. F. Martone, K. I. Ranney, K. D. Sherbondy, K. A. Gallagher, G. J. Mazzaro, and R. M. Narayanan, "An overview of spectrum sensing for harmonic radar," in *Fundamentals of Electrical Engineering (ISFEE), 2016 International Symposium on*, 2016, pp. 1–5.
- [3] V. Vlasak, and J. Pidanic, "The analysis of small RCS target detection in primary radar system," presented at the 2016 International Symposium ELMAR, Zadar, 2016, pp. 141–145.
- [4] G. J. Mazzaro, A. F. Martone, K. I. Ranney, and R. M. Narayanan, "Non-linear Radar for Finding RF Electronics: System Design and Recent Advancements," *IEEE Trans. Microw. Theory Tech.*, vol. 65, no. 5, pp. 1716–1726, May 2017.
- [5] L. Rong and W. Hai-yong, "The re-radiation characteristics of nonlinear target in harmonic radar detection," in *Microwave Conference, 2008 China-Japan Joint*, 2008, pp. 661–664.
- [6] H. Aniktar, D. Baran, E. Karav, E. Akkaya, Y. S. Birecik, and M. Sezgin, "Getting the Bugs Out: A Portable Harmonic Radar System for Electronic Countersurveillance Applications," *IEEE Microw. Mag.*, vol. 16, no. 10, pp. 40–52, Nov. 2015.
- [7] A. Martorell, J. Raoult, R. Marijon, and L. Chusseau, "EMI functional vulnerability identification in RF Front-Ends," in *Electromagnetic Compatibility of Integrated Circuits (EMCCo), 2017 11th International Workshop on the*, 2017, pp. 15–20.
- [8] R. Hstger, "Harmonic radar systems for near-ground in-foilage nonlinear scatterers," *IEEE Trans. Aerosp. Electron. Syst.*, no. 2, pp. 230–245, 1976.
- [9] M. A. Flemming et al., "Harmonic radar detection system," presented at the Proceedings of the International Radar Conference on Radar, London, UK, 1977, pp. 552–554.
- [10] K. Wincza, S. Gruszczynski, and J. Borgosz, "Dual-band capacitive feed antenna for nonlinear junction detection device," in *Microwave Techniques, 2008. COMITE 2008. 14th Conference on*, 2008, pp. 1–4.
- [11] J. C. Pedro and N. B. Carvalho, *Intermodulation distortion in microwave and wireless circuits*. Boston: Artech House, 2003.
- [12] A. Martorell, J. Raoult, R. Marijon, and L. Chusseau, "RF Front-Ends Nonlinearity Characterization Using Reflected Power," *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 6, pp. 1925–1931, Dec. 2017.
- [13] K. A. Gallagher, G. J. Mazzaro, A. F. Martone, K. D. Sherbondy, and R. M. Narayanan, "Derivation and validation of the nonlinear radar range equation," 2016, p. 98290P.

# Optimization of Near-Field Image Capture With Millimeter-Wave Bow-Tie Probes

Laurent Chusseau, *Member, IEEE*, Pierre Payet, and Jérémy Raoult

**Abstract**—A 60 GHz high-spatial resolution millimeter near-field scanning microwave microscope system is developed. Like in scanning near-field optical microscopy, it involves a modulation of the probe-sample distance. An analytical model of the near-field detection versus the minimum probe-sample distance is derived as a function of the harmonic rank used for lock-in detection. The model is validated owing to various probe sizes and materials. Both the model and experiments exhibit the filtering out of low spatial frequencies, the best efficiency being obtained at highest harmonics. It yields a resolution of  $\approx 2 \mu\text{m}$  (i.e.,  $\lambda/2500$ ) with an  $18 \mu\text{m}$  gap bow-tie probe and an optimized detection setup operating on the third harmonic.

**Index Terms**—Bow-tie antenna, microwave imaging, millimeter waves, near-field microscopy, near-field probe.

## I. INTRODUCTION

NEAR-FIELD scanning techniques with electromagnetic waves have been developed intensely at optical frequencies, because the highest resolution is expected for the shorter wavelengths [1], it is called near-field optical microscopy (SNOM) and is coupled to an atomic force microscope (AFM) that exhibits a probe of nanometer size. Simultaneously, numerous works were proposed in the far infrared or terahertz range [2] and in the RF [3], [4]. At microwave frequencies, the technique is often called near-field scanning microwave microscope (NFSMM) and was already demonstrated as a helpful tool to characterize the surface and material properties [5], [6], capacitances [7], metallic patterns [8], [9], dielectric patterns and metallic lines on a chip [10], electronic circuit boards [11], small biological samples [12], or concealed corrosion precursor in aircraft structures [13]. In these works, the higher resolutions are obtained by coupling the system with an AFM, while the higher sensitivity arose with resonant probes.

Owing to the transparency of many materials at gigahertz and terahertz frequencies, part of this research moved to the detection of subsurface buried structures either at

the nanoscale [14], [15], the micrometer scale [16], [17], or the millimeter scale [13]. Most experiments involve vector network analyzers (VNAs) to measure with high accuracy any impedance modification brought by a sample in the near field of a tip [18], eventually including a resonant probe [19], or an interferometric compensation of the very high reflectivity of the near-field probe [20], [21]. Since VNAs are very expensive in the terahertz, more affordable solutions derived from SNOM [3], [22], [23] could be preferred.

In SNOM experiments, the modulation of the distance to sample is mandatory to reject perturbations brought by probe emissions not belonging to near field, especially for apertureless probes. The detection process is thus part of the image formation [24]–[28]. We recently developed an NFSMM experiment operating at 60 GHz with a bow-tie near-field probe that interact mostly by a tangential electric field [29] instead of the longitudinal field of more classical tips [30]. Like in SNOM, we use the modulation of the probe-sample distance to get rid of far-field components. A lock-in amplifier operating on a given harmonic rank of this modulation obtains the detection. In this paper, we question about the best setting of these experimental conditions to optimize the sensitivity and spatial resolution of the near-field detection. The influence of these parameters on the bow-tie to sample interaction must then be understood and modeled to evaluate their counterparts on the measured images.

Our purpose is to provide guidelines for near-field detection with bow-tie probe. The experimental setup is described in Section II. Section III focuses on probe-sample interaction owing to approach curves. The model of the near-field detection with a vibrating sample is derived from the linear dipole approximation and described in Section IV as a function of the distance modulation and the harmonic detection rank. Finally, the imaging properties of these probes as applied to ICs and simple metallic samples are given in Section V.

## II. EXPERIMENTAL SETUP

The experimental setup is organized like a reflectometer (see Fig. 1). It has been described elsewhere [29], [31] so only the most important features are recalled here. The source is a Gunn diode of 20 mW output power attached to a 20 dB directional coupler. The direct path of the coupler feeds the probe. The intensity detection is provided by a Schottky diode on the reflected signal. The probe is connected in series with an E/H tuner that makes it resonant and matches the source. A low-frequency sinusoidal modulation of the probe-sample

Manuscript received June 16, 2016; revised September 17, 2016; accepted September 27, 2016. Date of publication November 4, 2016; date of current version December 7, 2016. This work was supported by the French Agence Nationale de la Recherche through the E-MATA HARI under Contract ANR-12-INSE-0005. The Associate Editor coordinating the review process was Dr. Sergey Kharkovskiy.

The authors are with the Institut d'Electronique et des Systèmes, University of Montpellier, 34095 Montpellier, France (e-mail: laurent.chusseau@umontpellier.fr).

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TIM.2016.2618960

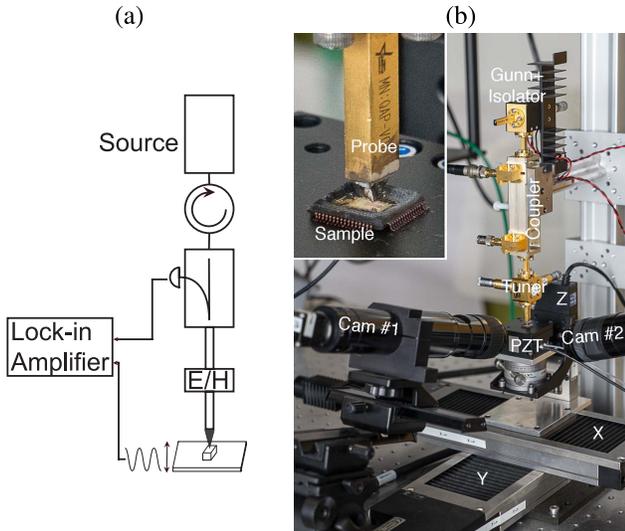


Fig. 1. (a) Schematic view of the experiments. (b) Photograph of the actual setup with close-up view in inset.

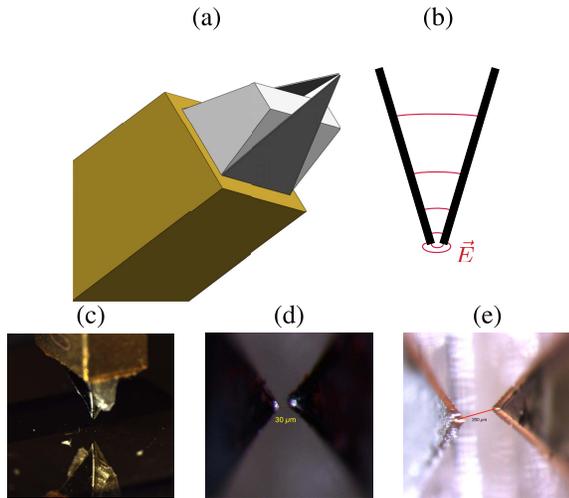


Fig. 2. (a) Schematic view of a probe: the two metal triangles are glued to a plastic add-on inserted in the WR15 open end. (b) Electric field in the probe and at its end. (c) General view of a probe in measurement position and its reflection in the Si substrate used as target. (d) Microscopic view of the tungsten probe with gap  $g = 30 \mu\text{m}$ . (e) Microscopic view of the gold probe with gap  $g = 200 \mu\text{m}$ .

distance is applied using a piezo actuator. This modulation serves as reference signal of a lock-in amplifier whose signal input is the detected Schottky voltage.

Homemade 60 GHz bow-tie probes are fabricated by soldering two equilateral triangles cut with a femtosecond laser at the WR15 end. Both gold and tungsten triangles were used for the probes considered in this paper. Gap  $g$  between tips is ranging from 18 to  $230 \mu\text{m}$ . The fabricated probes are represented in Fig. 2, metal triangles, plastic add-on piece, and gap measurements are illustrated. From a polarization point of view, Fig. 2(b) draws the resulting  $E$ -field with its two components: the first is transverse and applies in the direction joining the two facing triangle tips, with a maximum intensity just in-between, while the second of far less intensity

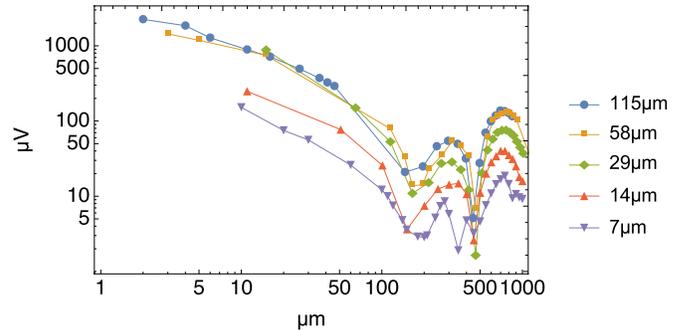


Fig. 3. Experimental approach curves for various dither amplitudes. Gold probe  $g = 230 \mu\text{m}$ .

is longitudinal along the waveguide and is significant only in the very close vicinity of the tips, not in-between.

### III. PROBE CHARACTERIZATIONS

We first measured the approach characteristics of our probes in various conditions. A 4 in polished Si wafer is the plane target of these experiments; its surface figures a perfect reference plane that avoids any pattern effects while changing the probe-sample distance  $h$ . Starting from the touchdown  $h = 0$ , the detected signal is collected when  $h$  increases using the calibrated motorized  $z$ -stage. In practice, the touchdown is validated owing to two video cameras arranged at right angles and equipped with 12 times zoom lenses to achieve a micrometer resolution [see Fig. 1(b)].

#### A. Effect of Dither Amplitude

The first approach curve (Fig. 3) was recorded at the reference frequency of the lock-in amplifier by varying the amplitude voltage applied to the piezoelectric sample holder. Results involve a bow-tie probe build using two gold triangle plates exhibiting a separation of  $g = 230 \mu\text{m}$  and the overall look of all curves is similar: at very short distance, there is a rapid decrease followed by some bounce between 200 and  $500 \mu\text{m}$  and between  $500 \mu\text{m}$  and 1 mm. Such a behavior was already observed in SNOM [24], [26] and explained by interference effects along the tip shaft of the SNOM probe. Calculations in such cases [28] have shown that bounce amplitudes and periods depend on the tip shaft length and are always close to the half of the wavelength with big probes. The case is not exactly the same here with a wavelength of 5 mm and submillimeter bounce periods. This discrepancy comes probably from the large geometric difference between the bow-tie and the tip, which results in an  $E$ -field strengthening that occurs for components at right angle. Nevertheless, bounces in the response versus distance are obviously the result of some interference, which probably occur between different radiating parts on both sides in-between the two triangles of the bow-tie probe.

Also worth to note in Fig. 3 are the superimposed curves for the three biggest considered dither amplitudes. This is not surprising because the abscissa records the minimum

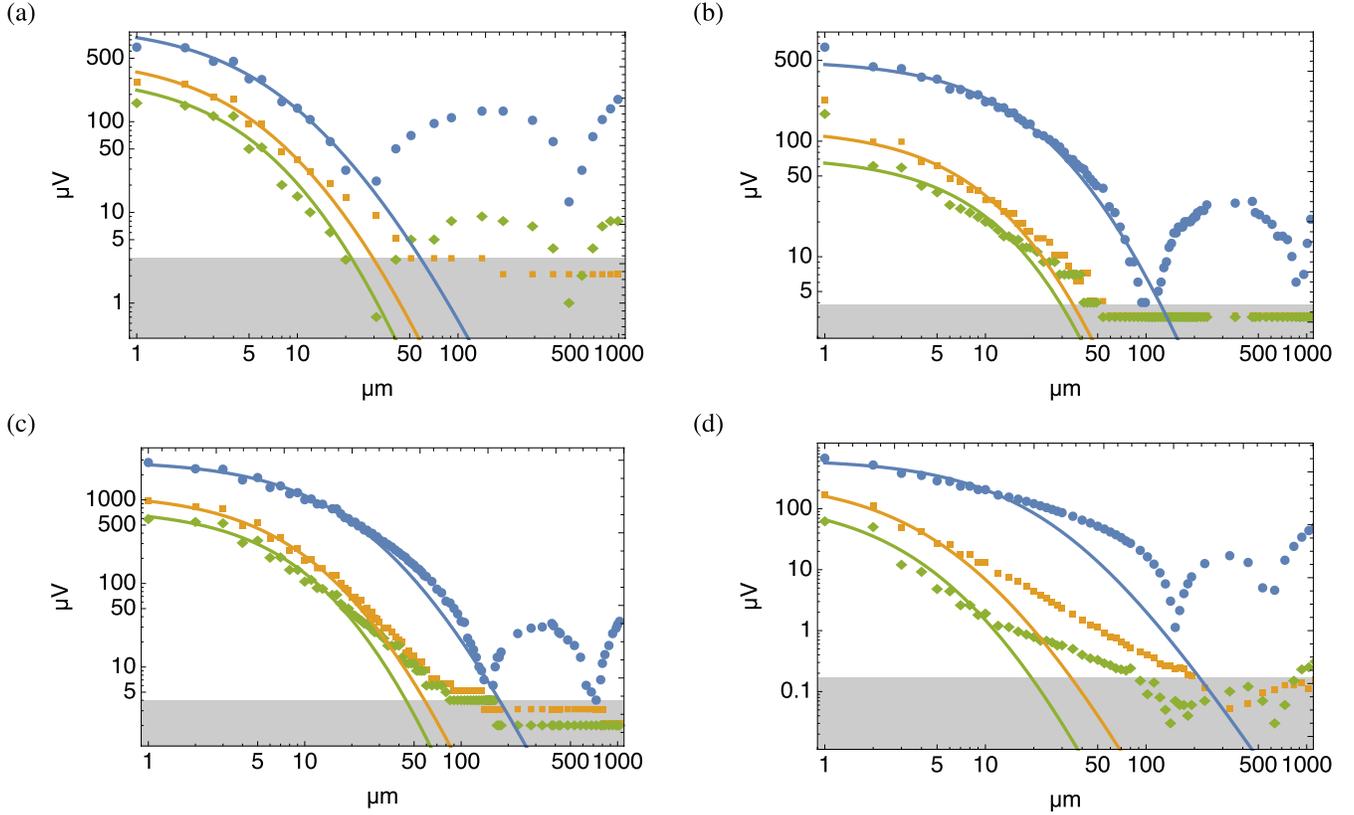


Fig. 4. Experimental approach curves: the lock-in amplitudes measured for the first three harmonics  $\mathcal{H}_1$  ( $\bullet$ ),  $\mathcal{H}_2$  ( $\blacksquare$ ), and  $\mathcal{H}_3$  ( $\blacklozenge$ ) of the dither frequency  $f$  are plotted as a function of probe-sample distance. (a) Gold probe  $g = 200 \mu\text{m}$ . (b) Gold probe  $g = 80 \mu\text{m}$ . (c) Tungsten probe  $g = 30 \mu\text{m}$ . (d) Tungsten probe  $g = 18 \mu\text{m}$ . Dots are measurements and lines are fits from the model of (4). Gray areas are the estimated noise level regions.

probe-sample distance during a modulation period. In the near field, the rapid decrease of the signal with the distance focuses mainly on the shorter distances to the detriment to the largest. According to the measurements, dither amplitude beyond  $\approx 30 \mu\text{m}$  seems inefficient. We will, therefore, always consider  $z$  variations lower than that limit in the sequel.

### B. Higher Harmonic Rank Approach Characteristics

In a second time, approach curves were recorded as a function of the lock-in detection harmonic rank for four different probes. Results are shown in Fig. 4 for two gold probes with gaps  $g = 200 \mu\text{m}$  and  $g = 80 \mu\text{m}$  and two tungsten probes with gaps  $g = 30 \mu\text{m}$  and  $g = 18 \mu\text{m}$ . Because of the higher ductility of gold as compared with tungsten, the metal sheets of the triangles in the former case were twice thicker ( $50 \mu\text{m}$  instead of  $25 \mu\text{m}$ ), this explains why it was more difficult to obtain low- $g$  probes with gold.

All four probes characterized in Fig. 4 exhibit similar behaviors, whatever the  $g$ -value and the metal nature. We first remark a rapid signal decrease with the minimum probe-sample distance and then bounces at greater distances. For higher harmonics, signals are lower and bounces are less visible and may even become less than the noise detection level. For all probes, the measured ratios between harmonic intensities at shorter distances are within similar ranges  $2.5 \leq \mathcal{H}_1/\mathcal{H}_2 \leq 8$  and  $5 \leq \mathcal{H}_1/\mathcal{H}_3 \leq 14$ , these ratios being approximately constant up to the first bounce whose

occurrence appears at very different distances as a function of the probe. As seen in Fig. 4(a), it can be as short as  $30 \mu\text{m}$  although it exceeds  $100 \mu\text{m}$  in Fig. 4(c) and (d). This intriguing difference was correlated with the probe fabrication that requires a plastic add-on to support the triangles while soldering to the WR15 waveguide end [29]. In practice, these supports are adjusted manually in length and width during the bow-tie probe mount. Recalling that interferences occurring between different radiating parts in-between the two triangles are responsible of these bounces and comparing the results of Fig. 4 with actual probes, we derive the rule: the bigger and the more protruding the plastic add-on is, the shorter the bounce distance, resulting in a reduced useful range of measurement for the probe.

The occurrence of marked bounces in Fig. 4 is a drawback for the usefulness of the probes. It reveals the probe ability to capture simultaneously near field and far field whatever the dither amplitude. Correspondingly, the lock-in detection mixes both contributions although only near-field components were expected. For instance, with the  $g = 200 \mu\text{m}$  gold probe of Fig. 4(a), an  $\mathcal{H}_1$  near-field signal produced by an object at a distance of  $10 \mu\text{m}$  is equivalent to a far-field signal of objects located at 200 to 400  $\mu\text{m}$  and even more from objects beyond 1 mm. This mixture is very harmful for the expected contrast during future image captures. In the sequel, we quantify this effect by means of what we call the ‘‘probe dynamic.’’ It was evaluated for the three harmonics and all

TABLE I  
“PROBE DYNAMIC” VERSUS LOCK-IN HARMONIC RANK

Probe Material	Probe Gap ( $\mu\text{m}$ )	$f$	$2f$	$3f$
Gold	200	4	80	18
Gold	80	21	39	43
Tungsten	30	75	185	145
Tungsten	18	15	1200	1200

probes. Referring to the data of Fig. 4, the so-called “probe dynamic” of the  $i$ th harmonic is calculated as the ratio of the  $\mathcal{H}_i$  amplitude at very short distance to its maximum amplitude occurring in bounces, or to the noise level if no bounce is observed. Results given in Table I show that higher harmonics exhibit better dynamic in each case, and that gold probes are the worst, especially if wide. In the special case of the smaller tungsten probe, very high contrasts exceeding  $10^3$  are reached for  $\mathcal{H}_2$  and  $\mathcal{H}_3$ . Both latter two harmonics are thus expected very efficient for high-resolution imaging in the near field. Nevertheless, for this probe, the  $\mathcal{H}_1$  contrast remains low because of the far field that increases at  $\approx 1$  mm. The same feature is far less noticeable with the very similar  $g = 30 \mu\text{m}$  tungsten probe, perhaps because the triangle metal thickness of  $25 \mu\text{m}$  is lower than tip separation at  $g = 30 \mu\text{m}$  and not at  $g = 18 \mu\text{m}$ , other parts of the bow-tie probes being exactly the same.

In practice, the measurement sensitivity is dependent of both the accuracy of the  $z$ -position with respect to the sample and the probe itself. On the one hand, the stepping motor with a micrometer resolution and repeatability controls the  $z$ -position. Plots of Fig. 4 confirm that it is not limitative. On the other hand, the probe gap  $g$  seems to be an important parameter for the sensitivity. The comparison between the two tungsten probes exhibits a signal level one order of magnitude lower with  $g = 18 \mu\text{m}$  than that with  $g = 30 \mu\text{m}$ . This feature is straightforwardly understood from the lower reactive power stored in the near field of the smallest probe. Nevertheless, it is worth noting that the dynamic range to the electronic noise shown by gray areas in Fig. 4 is the same and reaches  $\approx 10^3$ , both probes being then equivalent from the point of view of their use.

Subtler is the difference identified between gold probes and tungsten probes. Since gold probes of Fig. 4(a) and (b) are wider than tungsten probes, we should expect from the previous statement a greater signal at touchdown. Both are rather around  $500 \mu\text{V}$ , whereas more than  $1$  mV was obtained with the biggest tungsten probe. We believe that this difference is mostly due to the metal thickness ( $50 \mu\text{m}$  for gold and  $25 \mu\text{m}$  for tungsten) rather than to the difference of conductivity.

As a first rule of thumb of probe choice solely derived from measurements, one can emphasize that thinner metals are preferred together with small plastic support whose protruding parts must be removed in order to obtain little radiations in the far field.

#### IV. DIPOLE MODEL OF BOW-TIE NEAR-FIELD PROBES

To improve our understanding of the bow-tie operation in the near field, we model it as a linear electric dipole

parallel to the sample surface. Previous measurements on high-contrast samples [29] have shown high similarities with earliest SNOM interpretations [32] that were correctly interpreted with this hypothesis. Within this dipolar framework, the emitted  $\mathbf{E}$  and  $\mathbf{H}$  fields in polar coordinates are given by [33]

$$E_\phi = H_r = H_\theta = 0 \quad (1a)$$

$$E_r = \eta \frac{I_0 l \cos(\theta)}{2\pi r^2} \left(1 + \frac{1}{jkr}\right) \exp(-jkr) \hat{\mathbf{A}} \quad (1b)$$

$$E_\theta = j\eta \frac{kI_0 l \sin(\theta)}{4\pi r} \left(1 + \frac{1}{jkr} - \frac{1}{(kr)^2}\right) \exp(-jkr) \quad (1c)$$

$$H_\phi = j \frac{kI_0 l \sin(\theta)}{4\pi r} \left(1 + \frac{1}{jkr}\right) \exp(-jkr) \quad (1d)$$

where  $\eta$  is the vacuum impedance,  $I_0$  is the current fed into the dipole,  $k$  is the wavevector,  $r$  is the distance to dipole center, and  $\theta$  is the azimuth angle. In the very near field,  $kr \ll 1$ , the most important terms are the imaginary  $1/r^3$  terms in  $E_r$  and  $E_\theta$ .

From (1), it is easy to derive the power emitted by the dipole by integrating the Poynting vector  $\mathbf{W} = (1/2)(\mathbf{E} \times \mathbf{H}^*)$  on the sphere of radius  $r$  centered at the dipole. This extremely simple result accounts for emission in all directions

$$P = \oint_S \mathbf{W} \cdot d\mathbf{s} = \mathcal{P} \left(1 - \frac{j}{(kr)^3}\right) \quad (2)$$

with  $\mathcal{P} = \eta(\pi/3) |I_0 l / \lambda|^2$ . In near field, the imaginary term is predominant and the stored power is capacitive. The propagative term can be neglected. A similar calculation with a small loop antenna would have led to an inductive stored power in the near field [33]. These behaviors are well known and exploited in NFSMM, for example, by a capacitance change detected with a VNA [34].

In our NFSMM experiment, we seek micrometer resolutions by dithering the probe-sample distance to create a modulation of the stored reactive energy at probe tip. According to experiments, we write the instantaneous position and amplitude as a function of two parameters  $h$  and  $\Delta h$  plus the pulsation  $\Omega$  so as the minimum value is always  $h$ . This figures out our experimental adjustment where we want to compare modulation conditions with the same minimum probe-sample distance

$$z = h + \frac{\Delta h}{2} (1 + \sin(\Omega t)). \quad (3)$$

If this modulation is substituted to the  $r$  distance in (2), it results in a picture of the variation of the local electromagnetic energy in time. Since the useful experiment signal is the back reflection of the incident power, such calculation is a crude approximation of the true probe-sample interaction, because (2) integrates the dipole field over the whole space and not solely on the solid angle subject to the local interaction. We, however, expect from that a general and approximate behavior rather than an accurate quantitative description of approach curves.

Fig. 5 clearly shows the nonlinear effect of the dither amplitude with large spikes each time  $h$  is reached. The outcome is a rich spectral content suitable for detection at

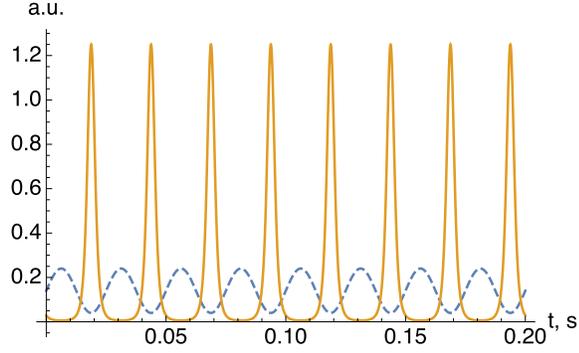


Fig. 5. Plot of  $P$  as a function of time (solid line) and the corresponding voltage applied to the  $z$ -piezoelectric stage (dashed line).  $h = 2 \mu\text{m}$ ,  $\Delta h = 10 \mu\text{m}$ , and  $\Omega = 80\pi \text{ Hz}$

various harmonic ranks of  $\Omega$ , which give the image of what should be detected with the lock-in [25]. In practice, they are calculated using a Fourier series expansion of (2) after the insertion of the variable distance of (3). We have done this analytically for the first three harmonics. After straightforward but somewhat lengthy manipulations, it yields

$$\frac{\mathcal{H}_1}{\mathcal{P}} = \frac{3(H^2 - h^2)}{4(Hh)^{5/2}} \quad (4a)$$

$$\frac{\mathcal{H}_2}{\mathcal{P}} = \frac{3(H - h)^2}{4(Hh)^{5/2}} \quad (4b)$$

$$\frac{\mathcal{H}_3}{\mathcal{P}} = \frac{\mathcal{H}_1}{\mathcal{P}} + \frac{64}{(H - h)^3} - \frac{6(h + H)^5}{4(H - h)^3(Hh)^{5/2}} - \frac{8hH(H + h)(2H - h)(2h - H)}{(H - h)^3(Hh)^{5/2}} \quad (4c)$$

with  $h$  and  $H = h + \Delta h$ , the minimum and the maximum probe to sample distances.

The analytic forms of (4) are surprisingly simple for the first two harmonics while the third harmonic and all subsequent ranks are much more complicated. Calculation results using these formulas are shown in Fig. 6 as a function of the dither amplitude  $\Delta h$  and minimum distance  $h$ .

Plots of Fig. 6(a) are for the selected  $\Delta h = 2 \mu\text{m}$  value. Calculated  $\mathcal{H}_i$  amplitudes fall rapidly when  $h$  increases and it comes along with a greater steepness when the harmonic rank is higher. This is in perfect agreement with the highest near-field sensitivity observed when detecting at higher harmonic ranks, and consequently it is expected to be less sensitive to any background far-field signal captured by the probe. However, this is achieved at the cost of a weaker useful signal although calculations are here far more optimistic than the measurements of Fig. 4. This discrepancy is a probable result of the crude approximation inherent to our model that otherwise depicts quite accurately the signal slopes when  $h$  increases.

At a fixed  $h = 2 \mu\text{m}$  minimum height, Fig. 6(b) shows that the calculated harmonic intensities grow very rapidly up to an optimum  $\Delta h$ -value and then decreases slowly. Such an optimum is present for all three harmonics and occurs, respectively, at  $1.24 h$  for  $\mathcal{H}_1$ ,  $4 h$  for  $\mathcal{H}_2$ , and  $8.53 h$  for  $\mathcal{H}_3$ . The higher the harmonic rank is, the bigger the

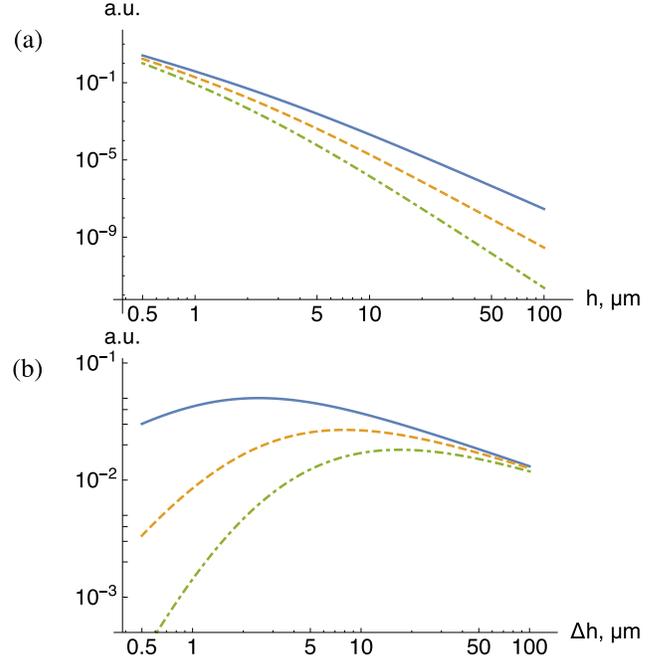


Fig. 6. Plot of harmonic amplitudes given by (4) versus minimum height  $h$  and dither amplitude  $\Delta h$ . Solid line:  $\mathcal{H}_1/\mathcal{P}$ . Dashed line:  $\mathcal{H}_2/\mathcal{P}$ . Dashed-dotted line  $\mathcal{H}_3/\mathcal{P}$ . (a)  $\Delta h = 2 \mu\text{m}$ . (b)  $h = 2 \mu\text{m}$ .

dither amplitude to reach this optimum. This feature was not observed during experiments, probably because it arises at very low  $\Delta h$  values that were not explored experimentally since they are associated with poor signal/noise ratios. Nonetheless, the increase of  $\mathcal{H}_1$  subsequently followed by a collapse of all measurements at high  $\Delta h$  values was observed in Fig. 3. Analytical expressions of (4) also show that beyond the maximum all  $\mathcal{H}_i$  decrease and tend to zero with the same asymptote of value  $3/(4h^{(5/2)}\Delta h^{(1/2)})$ . Again, this was not observed experimentally, because it would have appear only if the range of  $\Delta h$  values has been much larger than that explored in Fig. 3.

We then used the analytical formulas of (4) to fit the experimental results of Fig. 4. It is obvious that experimental  $\mathcal{H}_i(h)$  curves are not as monotonic as calculated ones. We suggest solving this question by taking as fitting parameter the relative dipole position with respect to the actual probe end. Within this framework the experimental curves are well fitted by the proposed analytical model up to the occurrence of the first bounce (see solid lines in Fig. 4). Considering the first three probes, the dipole model is very efficient to describe the probe-sample interaction in the near field up to the distance at which interference effects become evident. Such restriction is straightforward since any far-field effects due to a large source emission have been omitted in the model.

Considering the last tungsten probe with  $g = 18 \mu\text{m}$ , the fitting model seems to be less efficient and the discrepancy between measurements and theory progressively increases when  $h \geq 10 \mu\text{m}$ . One should notice that a change in  $d\mathcal{H}_i/dh$  arises at that latter distance whatever  $i$ , which causes this difference. The origin of these slope breaks remains

TABLE II  
POSITION OF THE EQUIVALENT DIPOLE IN FRONT OF PROBE TIP

Probe Material	Probe Gap ( $\mu\text{m}$ )	Dipole Position ( $\mu\text{m}$ )
Gold	230	25.8
Gold	200	8.9
Gold	80	27.4
Tungsten	30	18.1
Tungsten	18	10.3

unknown but recalling that the tungsten sheets used to build the probes have a thickness  $e = 25 \mu\text{m}$ , the tip end exhibits here a very different geometry with a ratio  $g/e \approx 0.7$  that is noticeably below unity, whereas it exceeds unity for all other probes. Our crude model with only one dipole becomes probably inaccurate. Nonetheless, at very short distances, and particularly  $\lesssim g$  the model accuracy is quite satisfactory.

Distances of the equivalent dipole position with respect to probe end as extracted from fitted data are given in Table II for the four probes considered in Fig. 4. As seen they are all positive, thereby locating the equivalent dipole in front of the bow-tie tips in a range from  $\lesssim 10$  to  $\approx 30 \mu\text{m}$  depending on the probe material and gap. At first glance, no rule can be given that may link such distance with  $g$  or with the triangle metal. Nevertheless, if one except the surprising gold  $g = 200 \mu\text{m}$  case it seems that the thinner metal sheets of tungsten probes and their lower  $g$  may shorten this distance, according to a rough vision of the electric field lines that links the two tips at bow-tie end.

## V. IMAGERY

We have used these probes to image integrated circuits. Owing to the transparency of plastics to millimeter-waves one may expect to gain information from a visualization of the die through the package or even more of an identification of the various functions from their layout implementation on the Si chip in view of further electromagnetic attacks [35]. Recalling the  $\approx 800 \mu\text{m}$  typical distance from package surface to die surface and referring to the curves of Fig. 4 such an expectation is an illusion as the main part of the signal detected at this distance comes from the far field and would not contain any high spatial frequency. Nevertheless, it is possible to image these ICs with the package removed and this has been done with the  $g = 30 \mu\text{m}$  tungsten probe at very short distance  $h \approx 5 \mu\text{m}$ .

The microscopic image of the IC and the millimeter-wave image are given in Fig. 7. A dashed square rectangle surrounds the targeted IC area in Fig. 7(a). Most of the visible structures are shields built in upper metallization and protected by SiN passivation. In the lower right part of the image, the shield has been opened to insert a test structure with  $50 \Omega$  lines that serve as coupling targets in electromagnetic compatibility tests [35]. This area is darker because the frontmost material is dielectric and  $50 \Omega$  lines of width  $1.75 \mu\text{m}$  are distinguished in the middle. On the other hand, the metal recesses created when opening vias between metal levels is of a few micrometers in depth and appear on the top metallic surface as rectangles in the optical image. Such targets are low contrast objects as compared with lines or metallic patterns deposited on

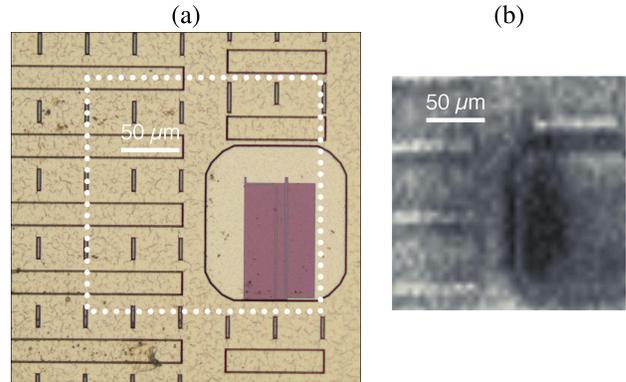


Fig. 7. Imaging of the surface of a test circuit provided by Freescale. (a) Microscopic image. (b) Near-field millimeter-wave image of the area surrounded by the dashed square in (a).

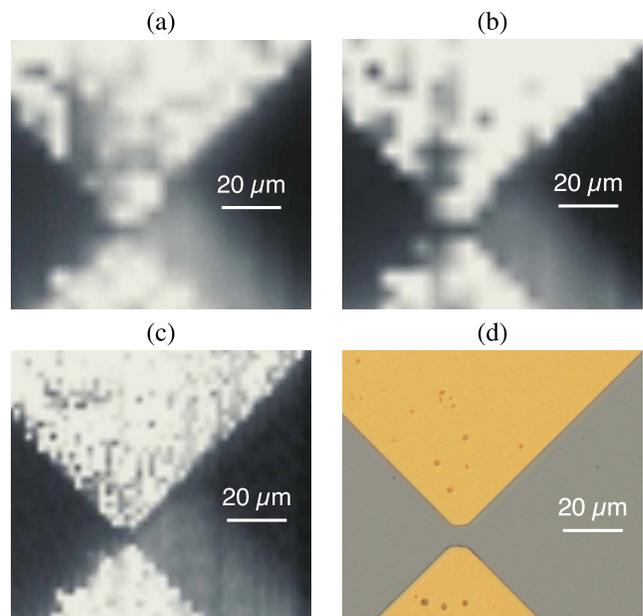


Fig. 8. Millimeter-wave near-field images of a gold bow-tie antenna on Si substrate as a function of harmonic rank on the lock-in. (a)  $f$ . (b)  $2f$ . (c)  $3f$ . (d) Microscopic view of the antenna.

semiconductor substrates that we used previously [31]. The near-field 60 GHz image of Fig. 7(b) was acquired at the fundamental frequency of the modulation using the  $g = 30 \mu\text{m}$  tungsten probe with a stepsize of  $5 \mu\text{m}$ . It exhibits most of the details previously identified on the optical image, even if their sizes are far lower than the wavelength of 5 mm. For example, the largest rectangles in the shield whose width is  $20 \mu\text{m}$  are well resolved with at least two pixels in spite of the low contrast associated with their depth of a few micrometers. This allows an estimate of the spatial resolution of  $\approx 10 \mu\text{m}$ , i.e.,  $\lambda/500$ . The smallest rectangles of size  $3 \times 20 \mu\text{m}^2$  and the  $50 \Omega$  lines are, however, not seen, not because of the too big stepsize but instead of the inadequate spatial resolution.

Our best tungsten probe with  $g = 18 \mu\text{m}$  was subsequently used to image a gold bow-tie antenna fabricated on a Si wafer. The optical image of this antenna is given in Fig. 8(d). The available free space between the two triangles is  $5 \mu\text{m}$ ,

i.e., half of the previously observed spatial resolution. Using such a high contrast target is favorable to evaluate the impact of the harmonic-rank of the lock-in detection on the images, because it allows high level of detection signal. Fig. 8(a)–(c) gives the images obtained while choosing lock-in detection at  $f$ ,  $2f$ , and  $3f$  with a stepsize of 5, 5, and 2  $\mu\text{m}$ , respectively. As previously observed in SNOM [24], a higher harmonic rank allows a better spatial resolution by rejecting more efficiently the lower spatial frequencies. This is also in perfect agreement with our previous model and yields the increase in both contrast and sharpness observed in Fig. 8(a)–(c). Such effects goes with an impressive increase of the resolution that reaches  $\approx 2 \mu\text{m}$  at  $3f$  in Fig. 8(c) since 2 pixels are clearly resolved in-between the bow-tie antenna tips. Correspondingly, the resolution is thus  $\lambda/2500$  instead of  $\lambda/130$  measured previously [29], [31]. Such a huge improvement is related to the previous characterization of that probe [see Fig. 4(d) and Table I], namely, the highest sensitivity to the near field at  $3f$  and the high increase in the dynamic capability of the probe that attenuates the blur observed at  $f$  and  $2f$ .

## VI. CONCLUSION

We have presented a 60 GHz high spatial resolution millimeter-wave NFSMM system and focused on the probe-sample detection and its influence on image formation and spatial resolution. To increase the spatial resolution and keep only the near-field components captured by the probe, a modulation of the probe-sample distance is set up like in SNOM, thereby filtering out most far-field contributions with the help of a lock-in detection.

Many probes involving a WR15 rectangular waveguide to bow-tie adiabatic transition have been fabricated using both gold and tungsten triangles soldered at an open WR15 end. These probes were characterized experimentally by approach curves recorded for the first three harmonic ranks of the lock-in detection. It was observed first that gold probes realized with a thicker metal sheet produce a lower signal, and second that bounces may appear on the approach curves reducing their measurement range and contrast. The latter bounces have been linked to excess in far-field emission provided by a small plastic add-on used for the probe mounting. As a result, very efficient probes have been realized with gaps between tips as short as 18  $\mu\text{m}$ . This was achieved by choosing thinner metal sheets with less ductile material like tungsten, and by reducing the protruding parts of the plastic add-on.

An analytical model of the probe detection versus the minimum probe-sample distance and the harmonic rank used for lock-in detection has been proposed. It simply relies on the emission of a transverse dipole in the near field. Using the model we succeed to explain the more and more efficient selection of the high spatial frequencies when the harmonic rank of the lock-in detection increases. Very efficient fits of the experimental approach curves were also obtained.

Finally, we use tungsten probes to image real objects, such as an integrated circuit and a gold bow-tie on Si substrate. High quality images with very high subwavelength resolutions were demonstrated in both cases. In agreement with both the

probe characterization and the model, a very high resolution was achieved using the third harmonic yielding a minimum observed dimension of  $\approx 2 \mu\text{m}$  (i.e.,  $\lambda/2500$ ).

## ACKNOWLEDGMENT

The authors would like to thank B. Vrignon from Freescale for the circuit sample and D. Marty for the help during experiments.

## REFERENCES

- [1] L. Novotny and B. Hecht, *Principles of Nano-Optics*. Cambridge, MA, USA: Cambridge Univ. Press, 2006.
- [2] A. J. L. Adam, "Review of near-field terahertz measurement methods and their applications," *J. Infr., Millim., Terahertz Waves*, vol. 32, nos. 8–9, pp. 976–1019, 2011.
- [3] B. T. Rosner and D. W. van der Weide, "High-frequency near-field microscopy," *Rev. Sci. Instrum.*, vol. 73, no. 7, pp. 2505–2525, 2002.
- [4] A. Imtiaz, T. M. Wallis, and P. Kabos, "Near-field scanning microwave microscopy: An emerging research tool for nanoscale metrology," *IEEE Microw. Mag.*, vol. 15, no. 1, pp. 52–64, Jan./Feb. 2014.
- [5] A. Imtiaz *et al.*, "Frequency-selective contrast on variably doped p-type silicon with a scanning microwave microscope," *J. Appl. Phys.*, vol. 111, no. 9, p. 093727, 2012.
- [6] E. Brinciotti *et al.*, "Probing resistivity and doping concentration of semiconductors at the nanoscale using scanning microwave microscopy," *Nanoscale*, vol. 7, no. 35, pp. 14715–14722, 2015.
- [7] T. Dargent *et al.*, "An interferometric scanning microwave microscope and calibration method for sub-fF microwave measurements," *Rev. Sci. Instrum.*, vol. 84, no. 12, p. 123705, 2013.
- [8] C. P. Vlahacos, R. C. Black, S. M. Anlage, A. Amar, and F. C. Wellstood, "Near-field scanning microwave microscope with 100  $\mu\text{m}$  resolution," *Appl. Phys. Lett.*, vol. 69, no. 21, pp. 3272–3274, 1996.
- [9] M. Kim *et al.*, "Nondestructive high spatial resolution imaging with a 60 GHz near-field scanning millimeter-wave microscope," *Rev. Sci. Instrum.*, vol. 75, no. 3, pp. 684–688, 2004.
- [10] M. Tabib-Azar, D.-P. Su, A. Pohar, S. R. LeClair, and G. Ponchak, "0.4  $\mu\text{m}$  spatial resolution with 1 GHz ( $\lambda = 30 \text{ cm}$ ) evanescent microwave probe," *Rev. Sci. Instrum.*, vol. 70, no. 3, pp. 1725–1729, 1999.
- [11] T. Dubois *et al.*, "Near-field electromagnetic characterization and perturbation of logic circuits," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 11, pp. 2398–2404, Nov. 2008.
- [12] O. Fawole and M. Tabib-Azar, "A novel near-field terahertz imaging probe for biological imaging," in *Proc. IEEE SENSORS*, Busan, South Korea, Nov. 2015, pp. 1–3.
- [13] M. T. Ghasr, S. Kharkovsky, R. Zoughi, and R. Austin, "Comparison of near-field millimeter-wave probes for detecting corrosion precursor pitting under paint," *IEEE Trans. Instrum. Meas.*, vol. 54, no. 4, pp. 1497–1504, Aug. 2005.
- [14] C. Plassard *et al.*, "Detection of defects buried in metallic samples by scanning microwave microscopy," *Phys. Rev. B*, vol. 83, no. 12, p. 121409, Mar. 2011.
- [15] K. Moon *et al.*, "Subsurface nanoimaging by broadband terahertz pulse near-field microscopy," *Nano Lett.*, vol. 15, no. 1, pp. 549–552, 2014.
- [16] K. Haddadi, D. Glay, and T. Lasri, "A 60 GHz scanning near-field microscope with high spatial resolution sub-surface imaging," *IEEE Microw. Wireless Compon. Lett.*, vol. 21, no. 11, pp. 625–627, Nov. 2011.
- [17] J. D. Chisum and Z. Popovic, "Performance limitations and measurement analysis of a near-field microwave microscope for nondestructive and subsurface detection," *IEEE Trans. Microw. Theory Techn.*, vol. 60, no. 8, pp. 2605–2615, Aug. 2012.
- [18] A. N. Reznik, "Quasistatics and electrodynamics of near-field microwave microscope," *J. Appl. Phys.*, vol. 115, no. 8, p. 084501, 2014.
- [19] A. Imtiaz and S. M. Anlage, "Effect of tip geometry on contrast and spatial resolution of the near-field microwave microscope," *J. Appl. Phys.*, vol. 100, no. 4, p. 044304, 2006.
- [20] M. T. Ghasr, K. P. Ying, and R. Zoughi, "Wideband millimeter wave interferometer for high-resolution 3D SAR imaging," in *Proc. IEEE Instrum. Meas. Technol. Conf. (I2MTC)*, Pisa, Italy, May 2015, pp. 925–929.

- [21] S. Gu, K. Haddadi, A. El Fellahi, and T. Lasri, "Setting parameters influence on accuracy and stability of near-field scanning microwave microscopy platform," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 4, pp. 890–897, Apr. 2016.
- [22] K. Wang, D. M. Mittleman, N. C. J. van der Valk, and P. C. M. Planken, "Antenna effects in terahertz apertureless near-field optical microscopy," *Appl. Phys. Lett.*, vol. 85, no. 14, pp. 2715–2717, 2004.
- [23] H.-G. von Ribbeck *et al.*, "Spectroscopic THz near-field microscope," *Opt. Exp.*, vol. 16, no. 5, pp. 3430–3438, 2008.
- [24] B. Knoll and F. Keilmann, "Enhanced dielectric contrast in scattering-type scanning near-field optical microscopy," *Opt. Commun.*, vol. 182, nos. 4–5, pp. 321–328, Aug. 2000.
- [25] P. M. Adam, J. L. Bijeon, G. Viardot, and P. Royer, "Analysis of the influence of the tip vibration in the formation of images in apertureless scanning near-field optical microscopy," *Opt. Commun.*, vol. 174, nos. 1–4, pp. 91–98, Jan. 2000.
- [26] F. Formanek, Y. De Wilde, and L. Aigouy, "Analysis of the measured signals in apertureless near-field optical microscopy," *Ultramicroscopy*, vol. 103, no. 2, pp. 133–139, May 2005.
- [27] A. J. L. Adam, N. C. J. van der Valk, and P. C. M. Planken, "Measurement and calculation of the near field of a terahertz apertureless scanning optical microscope," *J. Opt. Soc. Amer. B*, vol. 24, no. 5, pp. 1080–1090, May 2007.
- [28] R. Esteban, R. Vogelgesang, and K. Kern, "Tip-substrate interaction in optical near-field microscopy," *Phys. Rev. B*, vol. 75, p. 195410, May 2007.
- [29] R. Omarouayache, P. Payet, J. Raoult, and L. Chusseau, "Millimeter-wave near-field imaging with bow-tie antennas," *Opt. Exp.*, vol. 23, no. 9, pp. 12144–12151, May 2015.
- [30] J.-P. Guillet *et al.*, "Continuous-wave scanning terahertz near-field microscope," *Microw. Opt. Technol. Lett.*, vol. 53, no. 3, pp. 580–582, Mar. 2011.
- [31] R. Omarouayache, L. Chusseau, P. Payet, J. Raoult, and S. Jarrix, "60 GHz active microscopy with a bow-tie antenna as near-field probe," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (I2MTC)*, Pisa, Italy, May 2015, pp. 1189–1193.
- [32] J.-J. Greffet and R. Carminati, "Image formation in near-field optics," *Prog. Surf. Sci.*, vol. 56, no. 3, pp. 133–237, Nov. 1997.
- [33] C. A. Balanis, *Antenna Theory: Analysis and Design*, 2nd ed. New York, NY, USA: Wiley, 1982.
- [34] K. Lee *et al.*, "Label-free DNA microarray bioassays using a near-field scanning microwavemicroscope," *Biosensors Bioelectron.*, vol. 42, pp. 326–331, Apr. 2013.
- [35] L. Chusseau *et al.*, "Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (E-MATA HARI)," in *Proc. 22nd Int. Conf. Very Large Scale Integr. (VLSI-SoC)*, Playa del Carmen, Mexico, Oct. 2014, pp. 189–194.



**Laurent Chusseau** (M'15) received the Degree from the École Normale Supérieure de Cachan, Cachan, France, in 1983, and the Ph.D. degree from the University of Paris XI, Orsay, France, in 1986.

He held either an academic position with the Institut d'Électronique Fondamentale, Orsay, France, where he was involved in the microwave and optical domains, or was a Research Engineer with the Laboratoire Central de Recherche of Thomson-CSF, Center National d'Étude des Télécommunications of France Télécom, Lannion, France. In 1994, he joined the Institut d'Électronique et des Systèmes, Montpellier, France, where he developed research on laser modeling and electromagnetic near field. He is currently the Directeur de Recherche of the Center National de la Recherche Scientifique, Paris, France. He has authored over 200 articles and communications in technical journals or international conferences.

Dr. Chusseau is a member of the IEEE-MTT.



**Pierre Payet** received the B.Sc. degree and the M.Sc. degree in electrical engineering from the University of Montpellier, Montpellier, France, in 2012 and 2015, respectively, where he is currently pursuing the Ph.D. degree with the Institut d'Électronique et des Systèmes.

His current research interests include the near-field electromagnetic measurement and injection on material, device, and system, including irradiated devices.



**Jérémy Raoult** was born in Toulouse, France, in 1976. He received the Ph.D. degree in radio-frequency electronics from INSA of Lyon, France, in 2003.

Since 2004, he has been an Associate professor with the Institut d'Électronique et des Systèmes, University of Montpellier, Montpellier, France. Since 2008, he has been studying high-frequency electromagnetic compatibility and susceptibility of electronic components and systems. The main goal is to highlight the failure mechanisms induced by an interference signal, and to implement numerical simulation tools to predict these effects. He also focuses on the physical modeling and characterization of probes for near-field injection, and coupling between the probes and integrated circuits. His current research interests include noise in SiGe devices, and Si-based RF/microwave/millimeter-wave devices and circuits.

# Electromagnetic Coupling Circuit Model of a Magnetic Near-Field Probe to a Microstrip Line

Jérémy Raoult, Pierre Payet, Rachid Omarouyache, Laurent Chusseau  
IES, Université de Montpellier, 860 rue de Saint Priest, 34095 Montpellier, France  
Email: jeremy.raoult@ies.univ-montp2.fr

**Abstract**—Electromagnetic (EM) injection experiments require an accurate and quantitative knowledge of the voltage effectively coupled to a target line or circuit in order to predict disruptive behavior or sensitivity of digital IC circuits to EM threats. To answer this question we derive here a complete quantitative model of the coupling of our magnetic probe to a microstrip line. The novelty of this model is to consider the coupling by analogy with a transformer and then to deduce the corresponding mutual inductance as a function of probe to target relative positions. Its inputs are  $S$ -parameter measurements of the actual probe coupled to a  $50\ \Omega$  microstrip line and its output is an electric equivalent circuit that can be implemented in any circuit simulator. Validity of the model extends up to GHz frequencies.

**Index Terms**—Electromagnetic injection, Electromagnetic coupling model, Electrical circuit model, Magnetic near-field probe.

## I. INTRODUCTION

Electromagnetic injection (EMI) is a technique that has proven its effectiveness in studying the susceptibility of integrated circuits (ICs) [1], [2] and has found recently applications in fault-injection combined with side-channel attack as a new physical technique to break a cryptosystem [3]. Such new usages of EMI drive optimizations of the attacks that in practice rely on the optimization of the probe and on an enhanced understanding of its coupling with the possible on-chip receivers that are known to be mostly the long supply voltage lines and eventually the long signal lines [4].

The EMI optimization is two-fold. The probes must be optimized to deliver an intense and localized magnetic field that is most efficiently coupled to on-chip long lines. In a previous study an injection near-field probe has been improved considering only its radiative properties [5]. We then intend in this work to understand and quantify as accurately as possible the coupling between the probe and the IC. In fact this is now theoretically possible using 3D electromagnetic softwares, but such a method is quite long and tedious. Another possibility is to calculate analytically the coupling using formalisms like that of Ref. [6], but the subtle details of the probe geometry seems impossible to account for. Here we chose to derive an equivalent circuit model that will be probe dependent but very accurate and include by essence the probe as a whole. It fits our final goal that is to build an electrical circuit model suitable for implementation in classical circuit simulators. By the way EMI attacks could be taken into account at the early stage of the IC layout design and eventually one can then prevent

against such EMI threats. Notice that the method employed can be easily transposed to another magnetic probe design.

The §II of the paper recalls the magnetic ferrite probe design and optimization and propose an equivalent electrical circuit model validated against  $S$ -parameters measurements. The §III details the near-field probe to line coupling and supports the coupling model *via* mutual inductance, like in a ideal transformer. Optimization guidelines relative to probe-line relative position as well as number of loops wound around the ferrite core are given. The §IV deals with an application of the deduced electrical model to a realistic coupling situation with a pulse input.

## II. THE PROBE

### A. Geometrical Description

Let us first recall the geometrical parameters of the magnetic ferrite probe already designed and realized [5]. In that latter study we focused on the optimization of the field concentration at probe tip end and this was obtained with a ferrite core conically machined so as to exhibit a tip of a few tenths of  $\mu\text{m}$  radius ( $150\ \mu\text{m}$  typical for practical realizations and  $20\ \mu\text{m}$  for simulation). The magnetic field is produced by winding  $N$  loops of  $50\ \mu\text{m}$  diameter Cu wire around a ferrite rod of 2 mm diameter made of MnZn alloy (see Fig. 1).

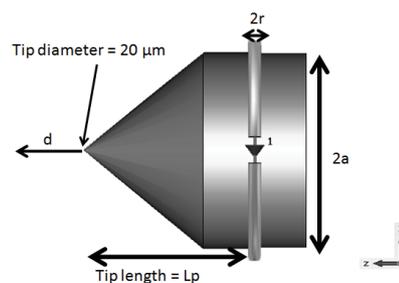


Fig. 1. Design view of the modeled ferrite with a conical cut.

Owing to the magnetic guiding properties of the ferrite core the field generation and its guiding and concentration up to the interaction with the target are fully decoupled. By using CST Microwave Studio [7], we have optimized this probe following the two criteria of spatial resolution and injection efficiency. According to electromagnetic simulations, this geometrical configuration should provide a spatial resolution of  $\lesssim 200\ \mu\text{m}$  for a tip-sample distance of  $20\ \mu\text{m}$  together with a maximum field intensity that is proportional to  $N$ , the number

of loops. This characteristic holds if the following conditions are satisfied: the field remains below the saturation field of the ferrite core, the frequency does not exceed  $\approx 1$  GHz and the loop count is not too high so as the parasitic capacitance between loops remains sufficiently low.

### B. Electrical Model of the Probe

A better understanding of the probe-circuit interaction require an accurate characterization. This was done owing to  $S$ -parameters with the same methodology as in Ref. [1]. Focusing on  $S_{11}$  in the frequency range of 1 MHz to 1 GHz allows to derive an electric model with lumped elements by means of the known transformation of  $S$ -parameters to  $Z$ -parameters. The proposed electrical SPICE model of the probe is given in Fig. 2.

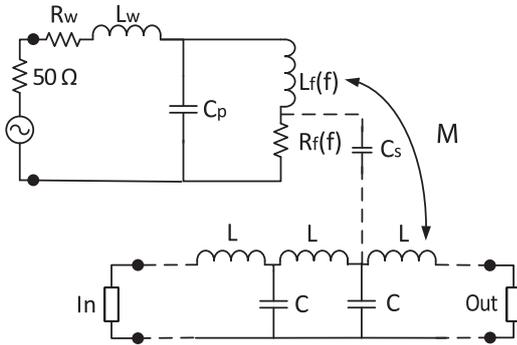


Fig. 2. Equivalent electrical circuit model of the magnetic probe and of the coupling to the line. The probe lumped equivalent circuit is given in the upper part with  $R_w$ ,  $L_w$ ,  $R_f$ ,  $L_f$  and  $C_p$ , the generator and  $50\ \Omega$  load figuring the input signal fed into the probe. The coupling model is described by  $M$  and  $C_s$ . The line is modeled by distributed  $LC$  cells ended by input and output devices ( $50\ \Omega$  load, transistor, ...).

This model is intended to replicate the electrical behavior of the sensor while being close to the physics and geometry of the probe. The wire connecting the  $N$  loops wound around the ferrite core to the SMA connector is modeled by a resistance in series with an inductance whose values are set proportional to their true length and known resistivity. The ferrite with its  $N$  loops is accounted for by the  $RLC$  circuit,  $C_p$  corresponding to the inter-loop winding capacitance. The resistance  $R_f$  that accounts for magnetic losses and the inductance  $L_f$  are frequency dependent and they both come from the physical model of the real and imaginary part of the ferrite rod [8]. Figure 3 depicts the known evolution of  $\mu_{\text{rod}} = \mu'_{\text{rod}} - j\mu''_{\text{rod}}$  of our MnZn ferrite rod in the entire frequency band of interest.

The real part of the relative permittivity of the ferrite rod,  $\mu'_{\text{rod}}$ , is the multiplicative factor entering the calculation of the coil inductance,  $L_f(f)$ . It is almost constant and maximum at low frequency and decreases rapidly beyond 200 MHz, thereby reducing the efficiency of the probe. In the same time the imaginary part,  $\mu''_{\text{rod}}$ , increases regularly inducing corresponding increasing losses,  $R_f(f)$ , as the frequency rises. The optimum frequency band for a magnetic sensor using this ferrite rod material is thus from 1 MHz to 200 MHz.

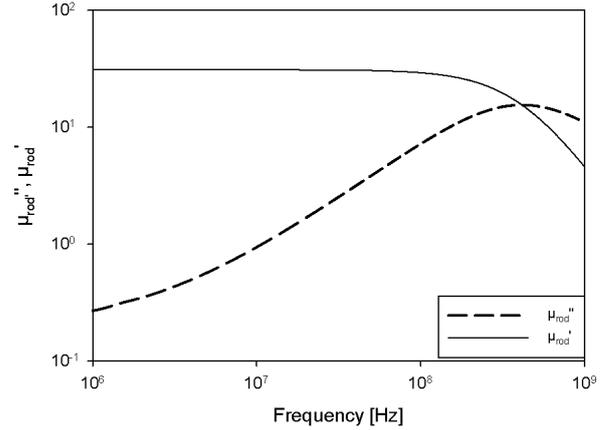


Fig. 3. Real and imaginary part of the MnZn ferrite rod permeability.

With this model in hands, an adjustment of the circuit element values to measurement data has been done. Values are given in Tab. I for three probes with different  $N$ . Figure 4 then gives the comparison, in magnitude and phase of  $Z_{11}$ , between the calculated probe model impedance and the corresponding measurement. The increase of  $|Z_{11}|$  proportionally to the frequency arising together with a constant  $90^\circ$  phase corresponds to an inductive behavior up to 200 MHz. The resonance occurring at 400 MHz indicates a change in the electrical behavior of the probe that can not anymore be assimilated to a perfect inductance. The excellent agreement between model and measurements, over three decades in frequency extending up to 1 GHz, validates the high capability of our model to model electrically this probe.

TABLE I  
PARAMETERS OF THE PROBE MODEL.

	$N = 3$	$N = 6$	$N = 12$
$R_w$ ( $\Omega$ )	0.3	0.25	0.15
$L_w$ (nH)	42	38	23
$C_p$ (pF)	0.7	0.7	1.6
$L_f$ @ 10 MHz (nH)	137	910	2150
$R_f$ @ 10 MHz ( $\Omega$ )	0.3	2	8

### III. COUPLING MODEL OF A NEAR-FIELD PROBE TO A LINE

Let us now consider the coupling between the probe and the circuit under test. Since long lines were identified as the most interesting targets of our injection application, we will consider here a known  $50\ \Omega$  microstrip line on PCB. Note that in practice there is no loss of generality to consider only a  $50\ \Omega$  microstrip line because the voltage coupled to a line is given by the Maxwell-Faraday law and the knowledge of the magnetic field produced by the probe [6]. As long as the emitted field does not depend of the target, a feature verified here because it is valid except in the extreme near-field region (Rayleigh or reactive near-field region [9]), the coupling will

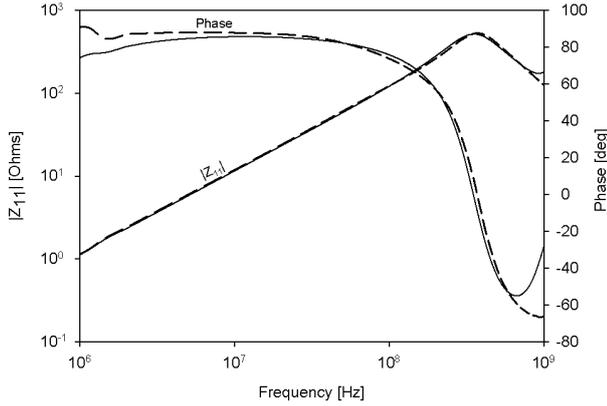


Fig. 4. Modulus and phase of the measured and modeled probe input impedance. The probe has  $N = 3$  loops.

be modified only according to the line geometry in terms of the area under the microstrip. It thus follows that a simple proportionality rule holds when changing the line geometry.

In the following we will study both the influence of  $N$  and the relative location of the probe with respect to the target line. An optimization of the probe is looked for in terms of spatial resolution and injection efficiency. Characterizations have been performed on a  $50\ \Omega$  characteristic impedance, 5 cm long and  $500\ \mu\text{m}$  wide microstrip PCB line. Magnetic probes with three different loop counts of  $N = 3, 6$  and  $12$  have been fabricated and considered.

#### A. The Ideal Transformer Picture

Our probe is designed for magnetic coupling. The natural picture for the coupling of this probe to any target is thus the ideal transformer. The input of the transformer is the probe and its output is the target, here the line. Both are linked through a mutual inductance to be determined. Assuming that the probe is at port 1 and the line at port 2, one can characterize experimentally the system by measuring its  $S$ -parameters then subsequently converted to  $Z$ -matrix. As a consequence the mutual inductance  $M$  is directly obtained from the  $Z_{21}$  parameter by

$$Z_{21} = jM\omega \quad \rightarrow \quad M = \frac{Z_{21}}{j\omega} \quad (1)$$

The novelty and key parameter of our model lies in this  $M$  mutual inductance whose extraction is performed by measuring  $Z_{21}$  in the 1 MHz–1 GHz frequency band. This is done by connecting a network analyzer to our near-field injection bench (see Fig. 5). The probe position is adjusted in the three  $XYZ$  directions using motorized stages controlled by computer. Relative motions, including height and lateral displacement of the line with respect to the probe, are then considered to seek for optimal coupling conditions by maximizing  $M$  from  $Z_{21}$  measurements. Similarly one can compare probes with various characteristics at a given position with respect to the line.

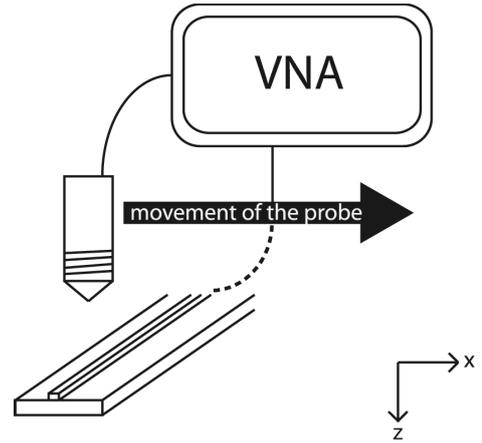


Fig. 5. Experimental setup for near-field EMI. Probe motion across the line is shown.

#### B. Extraction of $M$

In a first attempt we chose a probe positioning at height of  $100\ \mu\text{m}$  over the circuit with the probe tip slightly away from the line, just like it was drawn in Fig. 5.  $M$ -values were extracted over the whole 1 MHz–1 GHz frequency range for two probes differing by the number of loops, namely  $N = 3$  and  $N = 12$ . A tremendous result of Fig. 6 is the constant  $M$ -values obtained at low frequencies for both probes. This emphasizes our model picture of an ideal transformer. The  $N = 3$  probe exhibits a constant  $M = 0.9\ \text{nH}$  up to 300 MHz while the  $N = 12$  probe has a  $M = 2\ \text{nH}$  constant value up to  $\approx 30\ \text{MHz}$ . Beyond these limits a cutoff behavior is observed together with an overshoot that is more or less pronounced depending on  $N$ . For sure at such high frequencies the transformer is no more ideal for two reasons. First the receptive line is no more a pure inductance, and second the capacitive coupling between the probe and the line increases with the frequency [10]. A simple model improvement was to include these two factors of non-ideality: the microstrip line is practically modeled using distributed  $LC$  elements [11], and the capacitive coupling is taken into account in the model by adding the fitted stray capacitance  $C_s$  between the probe and the line. The now complete electrical scheme of probe to line coupling is given in Fig. 2 and is used in the following for optimization as a function of loop count and position.

#### C. Coupling vs Loop Count

The mutual inductance being the key value of the coupling, we decide first to compare various probes on this sole criteria as a function of the lateral position with respect to the target line, the height being prescribed at  $h = 100\ \mu\text{m}$ . For each probe at each position the  $M$ -value is obtained as an average over the lower frequencies like it was shown in Fig. 6. Results are given in Fig. 7 for three probes having  $N = 3, 6$  and  $12$  loops around a ferrite core of 2 mm diameter. Important features appear on these plots:

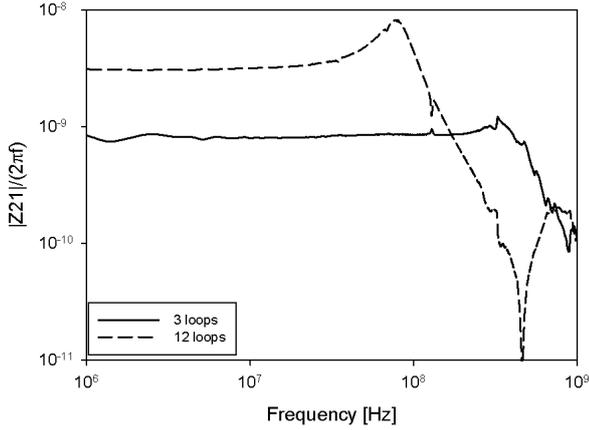


Fig. 6.  $M = |Z_{21}|/\omega$  extraction vs frequency at a given position for two probes with  $N = 3$  and  $N = 12$  loops.

- First the coupling is found important even far from the target, but surprisingly it is minimum just over the line and maximum 2 mm away on both sides! This comes from the field emitted by the probe which is mainly vertical in our scheme and that must encompass the line to create an induced voltage by mean of Maxwell-Faraday law. As a result, our  $M$  determination, that is the convolution of the intrinsic resolution of the probe with the intrinsic resolution of the detecting line, is poorly spatially localized. Although the spatial resolution of the probe alone has been optimized (see §II), the whole system becomes less accurate because of a bad matching between emitter and receiver.
- Second the coupling is found highly dependent of  $N$ . Quantitatively it is almost proportional to  $N$  since the maximum values measured are  $M \approx 1.05, 1.8,$  and  $3.1$  nH for  $N = 3, 6$  and  $12$  loops. However, this must be tempered with the strong decrease of the maximum usable frequency observed as  $N$  increases (see Fig. 6). Thus the choice of  $N$  is highly application dependent and must be put in accordance with the speed of the EMI excitation signal.

#### D. Coupling vs Height

Similarly the  $M$ -value is relevant to compare the coupling of one specific set of probe–line as a function of probe height. This has been done for several probes but only the results obtained with the  $N = 6$  loops probe crossing the line at the three constant heights of  $h = 50, 100$  and  $200 \mu\text{m}$  are given in Fig. 8.

The height has a minor role on the injection efficiency. Indeed a very small decrease (less than 10%) is observed when  $h$  is multiplied by 4. One can imagine that the change in  $h$  used here is quite negligible as compared to the mm-scale resolution of the coupled probe–line system with the simultaneous consequence of a very weak influence on both the coupling resolution and efficiency.

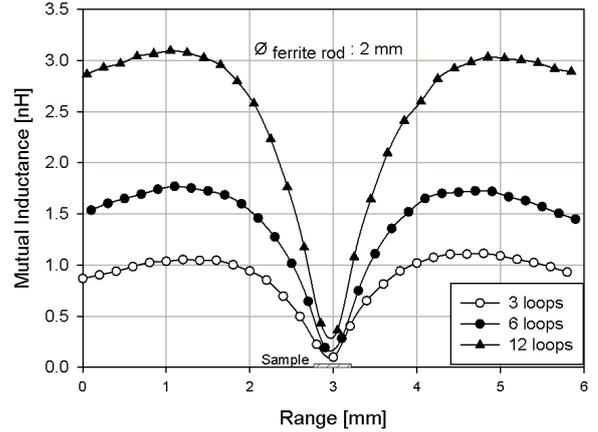


Fig. 7. Evolution of  $M$  vs the lateral position of the probe with respect to the line. The line position and size is sketched on the graph. Plots are given for three probes with different loop counts of  $N = 3, 6$  and  $12$ .

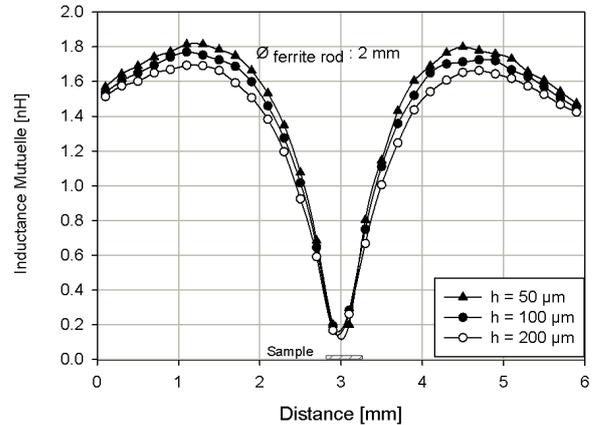


Fig. 8. Evolution of  $M$  vs the lateral position of the probe with respect to the line. The line position and size is sketched on the graph. Plots are for a  $N = 6$  at heights  $h = 50, 100$  and  $200 \mu\text{m}$ .

#### IV. COUPLING MODEL APPLICATION

As an illustration of our model usage, we calculate the EMI coupling signal on the supply voltage of a bipolar transistor in  $0.25 \mu\text{m}$  BiCMOS technology. Namely the electrical scheme of Fig. 2 is used with a pulse signal at probe input. Simulation was performed using ADS with the excitation depicted in Fig. 9 and has a voltage excursion of  $\pm 5$  V, a repetition frequency of 10 MHz, risetime and falltime of  $\tau_r = \tau_f = 3$  ns. Also given in Fig. 9 is the voltage across the ferrite coil which is almost the derivative of the current in the probe, and therefore a quantity proportional to the expected voltage coupled to the target owing to the Maxwell-Faraday law.

The simulation is intended to illustrate a realistic supply voltage line in  $0.25 \mu\text{m}$  BiCMOS technology. Both ends of the target line are therefore loaded by a voltage source with its capacitance at  $I_n$  port and by a bipolar connected as

## V. CONCLUSION

The coupling between a magnetic near-field probe and a line has been experimentally studied and modeled. The probe is built from a ferrite core machined in conical form with few wire loops wound to produce the magnetic field that is concentrated at ferrite tip end. This design was intended to optimize the injection efficiency and spatial resolution. The interaction between the probe and the line was experimentally characterized up to 1GHz. Experiments were used to derive an original lumped-elements equivalent coupling-model suitable for an implementation in electrical-circuit simulators. Within the framework of this model we show that the coupling is quantified by a mutual inductance extracted by analogy with an ideal transformer. As a consequence optimization guidelines have been defined for the coupling in term of number of loops, position, depending on the bandwidth of the signal to be coupled. Finally the model is used in a case study to evaluate the perturbation brought on the supply line of a BiCMOS technology.

## ACKNOWLEDGMENT

We kindly acknowledge the French Agence Nationale de la Recherche for funding this research under the E-MATA HARI contract n°ANR-12-INSE-0005.

## REFERENCES

- [1] T. Dubois, S. Jarrix, A. Penarier, P. Nouvel, D. Gasquet, L. Chusseau, and B. Azaïs, "Near-field electromagnetic characterization and perturbation of logic circuits," *IEEE Trans. On Instrumentation and Measurements*, vol. 57, pp. 2398–2404, 2008.
- [2] L. Chusseau, R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Boyer, B. Vrignon, J. Shepherd, T.-H. Le, M. Berthier, L. Rivière, B. Robisson, and A.-L. Ribotta, "Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (E-MATA HARI)," in *IEEE International Conference on Very Large Scale Integration, VLSI-SOC 2014*, Playa del Carmen, MX, 2014.
- [3] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of AES," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*. IEEE, 2012, pp. 7–15.
- [4] F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, and P. Maurine, "Local and direct EM injection of power into CMOS integrated circuits," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*. IEEE, 2011, pp. 100–104.
- [5] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine, "Magnetic microprobe design for EM fault attack," in *EMC Europe*, Brugge, 2013.
- [6] C. Taylor, R. Satterwhite, and C. Harrison Jr, "The response of a terminated two-wire transmission line excited by a nonuniform electromagnetic field," *Antennas and Propagation, IEEE Transactions on*, vol. 13, no. 6, pp. 987–989, 1965.
- [7] "CST Microwave Studio." <http://www.cst.com/>
- [8] N. Hamilton, "The small-signal frequency response of ferrites," *High frequency electronics*, pp. 36–52, June 2011.
- [9] C. A. Balanis, *Antenna Theory - Analysis and Design*, 2nd ed. John Wiley & Sons Inc., 1982.
- [10] C. F. Carobbi and L. M. Millanta, "Analysis of the common-mode rejection in the measurement and generation of magnetic fields using loop probes," *Instrumentation and Measurement, IEEE Transactions on*, vol. 53, no. 2, pp. 514–523, 2004.
- [11] D. M. Pozar, *Microwave engineering*. John Wiley & Sons, 2009.

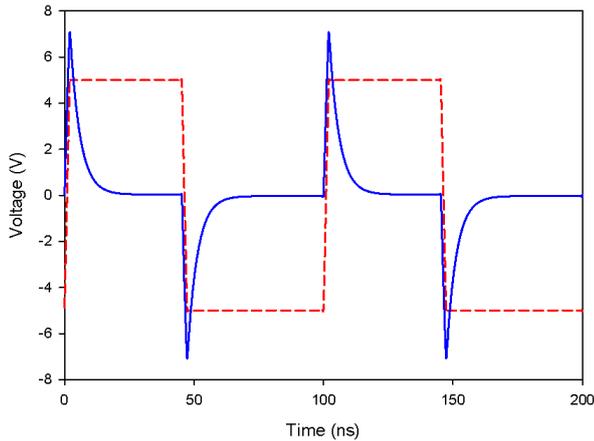


Fig. 9. Input signals. The dashed curve is the prescribed signal at probe input. The solid curve is the voltage across  $C_p$ .

an inverter at Out port. The Fig.10 gives the calculated voltage at that port. One can observe that more than 10 mV peak-to-peak voltage excursion are induced at that point and superimposed to intrinsic oscillations brought by the internal bipolar dynamics. These values are not sufficient to perturb the internal logic of an IC but the excitation considered here was at least ten times lower than what is usually considered for that purpose [3]. This application example of our coupling model also shows that induced perturbations are not easily predictable: for instance, if the transistor and voltage source are replaced by  $50\Omega$  loads the coupled signal is two times less in amplitude and does not exhibit rapid oscillations. In the future, it is thus expected that our model can help in identifying the inner mechanisms of EMI fault injection by accounting of the exact layout of logic ICs.

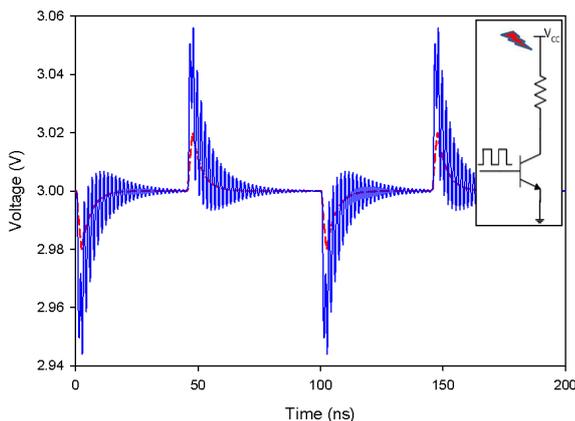


Fig. 10. Output signals coupled to the line measured at the Out port. The dashed curve is for a  $50\Omega$  loaded line at both ends. The solid curve is for a supply voltage line loaded by a BiCMOS bipolar transistor. Inset is a schematic of the circuit simulated, the lightning symbol figures out the injection on  $V_{cc}$  line.

## Control of a MOS Inverter by Out-of-Band Pulsed Microwave Excitation

Clovis Pouant<sup>1, 2, 3</sup>, Jérémy Raoult<sup>1, \*</sup>, Patrick Hoffmann<sup>2</sup>,  
Laurent Chusseau<sup>1</sup>, and François Torrès<sup>3</sup>

**Abstract**—An intentional focusing of High-Power Microwave (HPM) energy on microelectronic systems can produce effects that will potentially upset or damage the target. However, the physical mechanisms at work within the device are not often well understood. We provide a detailed understanding of the physical mechanisms involved in a common-source Metal Oxide Semiconductor (MOS) transistor inverter when Pulsed Microwave Excitation (PME) in a frequency range from 10 MHz to 1 GHz is applied on the gate terminal. Our study is based on the measurements of the current waveforms on all transistor access and explains the MOS response with and without the Radio-Frequency (RF) interference.

### 1. INTRODUCTION

The intentional use of High-Power Microwave (HPM) sources to disturb electronic systems is a major threat to civil and military infrastructures. Overall, HPM sources are able to produce at least 100 MW of peak RF power within the frequency range of 1 MHz to 100 GHz, with pulse duration ranging from 10 ns to 1  $\mu$ s [1]. HPM couple to electronic systems many ways [2]:

- (i) *Front door coupling*: The electromagnetic interference couple to systems through ports intended to transmit or receive signals for communication with other systems, such as antennas or sensors.
- (ii) *Back door coupling*: The electromagnetic energy uses any parts of the system not intended to transmit or receive RF signals, such as apertures, seams, wires, power sockets or printed circuit boards traces.

HPM interferences are classified according to their severity, such as destruction, permanent damage or a variety of non-destructive failures [3, 4]. Nonetheless, it is often difficult to trace an upset to a particular individual component or circuit mechanism. It is necessary to study the electromagnetic susceptibility of each sub-system constituting the target in order to determine which physical mechanisms are at work. The aim of the present paper is to provide a physical analysis of a MOS transistor inverter under Pulsed Microwave Excitation (PME) by means of an experimental setup and methodology.

Various susceptibility effects may take place when an RF interference is superimposed on transistor pins [5–10]. Their intensity and dangerousness depend on RF power level, frequency and operating regime. Anyway, intrinsic transistor non-linearities, especially considering the current-voltage characteristic, are the main causes of distorted current waveform induced by RF excitations, which finally leads to a bias point shift. This modification of the nominal current is called the rectification effect [11].

The most recent research efforts were focused on circuits including electrostatic discharge (ESD) protection and stressed by HPM [12]. Because of their own saturation mechanism, these protections

---

Received 31 May 2017, Accepted 8 August 2017, Scheduled 30 October 2017

\* Corresponding author: Jérémy Raoult (jeremy.raoult@ies.univ-montp2.fr).

<sup>1</sup> IES, UMR CNRS 5214, 860 rue St Priest, 34095 Montpellier, France. <sup>2</sup> CEA, DAM, GRAMAT, F-46500 Gramat, France. <sup>3</sup> Xlim, UMR CNRS 7252, 123 avenue Albert Thomas, 87060 Limoges, France.

were thought to bring some extra protection against HPM that one must quantify. However, it was shown that an HPM excitation having a sufficiently large voltage amplitude can induce — through ESD protections — a significant DC voltage at the input pin of a CMOS IC, which finally leads to a change of the logic state at its output [12]. Unfortunately, this study does not propose any physical understanding on the underlying mechanisms affecting the circuit via interference.

By using another MOS technology that also includes ESD protections, but with larger triggering thresholds, we conduct here PME attacks on a MOS common-source inverter without activating its ESD protection devices. The effective PME is the result of HPM coupling onto printed circuit board (PCB) traces (back door coupling) [13]. It is observed that a MOS inverter that initially follows the interference may switch to a state where it is totally inhibited and pinned down to the lower logic level. As a major outcome, we develop a methodology to clearly understand the EMI effect. It is based on the measurement of the transient currents on all access of the transistor, bringing many informations about average values, distortion, peak values. . . With the support of these measurements, the physical understanding of the response of the device under excitation becomes possible and may help to explain the system susceptibility at frequencies up to 1 GHz.

The paper is organized as follows. Section 2 describes the experimental setup used to apply the direct injection and assess all transistor instantaneous currents up to 1 GHz. Section 3 provides detailed results when the device’s gate is stressed by a typical PME. We analyze the input/output voltage waveforms and their evolutions versus frequency to identify the conditions where PME causes the dramatic effect of gain inhibition and logic level pinning, which could upset digital circuits. The Section 4 details all the transistor’s input/output current waveforms to provide a physical analysis of the occurrence of this dramatic effect. A first numerical approach is proposed in Section 5 to confirm and identify the elements that drive the observed response. Conclusion follows in Section 6.

## 2. RF INJECTION EXPERIMENTS SETUP AND METHODOLOGY

The test setup used for the direct injection experiments [14] and the measurement of all transistor currents waveform up to 1 GHz is described in Fig. 1. The Device Under Test (DUT) is mounted on a printed circuit board (PCB) made from Rogers RO3010 substrate, and the short 50 ohm microstrip tracks ( $< 2$  cm) allow neglecting parasitic elements up to 1 GHz. Each ground connections to the chip is made through a via to the ground-plane. The commercial transistor (DUT) is a BSS83, an enhancement n-channel MOSFET from NXP, with a 140- nm gate oxide thickness and a threshold voltage of 1.2 V. It is designed for RF switching applications, and its peak transition frequency is around 500 MHz. This transistor has also been chosen because of its 4-pin SOT-143 package providing access to the bulk terminal, thus allowing direct bulk current measurement. DC measurements were used to extract the threshold voltage, see Table 1.

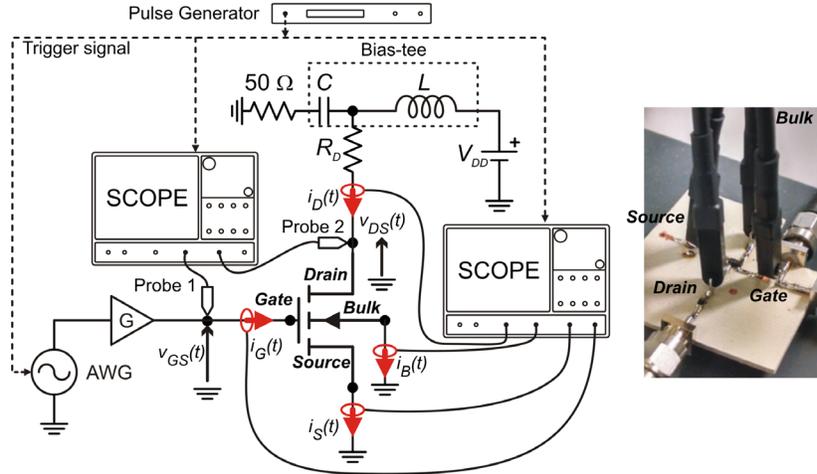
**Table 1.** Useful parameters from the NXP MOSFET datasheet.

Gate Length ( $L$ )	6 $\mu\text{m}$
Gate Width ( $W$ )	1200 $\mu\text{m}$
Oxide Thickness ( $t_{ox}$ )	140 nm
Threshold Voltage ( $V_T$ )	1.2 V

Fig. 1 shows the measurement circuit when a PME is injected into the nMOS gate, which is the most likely entry for the RF signal. A Tektronix AWG 7122B arbitrary waveform generator is used to generate the PME, subsequently fed into an RF amplifier to raise the desired power output capability.

Four Tektronix CT6 high-frequency (2 GHz) current probes provide a stable measurement of all transistor currents, which are probed on a small 20-gauge wire, and measured using a first high-bandwidth DSO9254A oscilloscope, whose averaging mode was used to reduce noise on the recorded currents.

A high impedance active probe N2796A senses the instantaneous drain-source voltage  $v_{DS}(t)$  across the 510 ohm drain resistor  $R_D$ . This probe introduces a load capacitance of 1.2 pF and has



**Figure 1.** Block diagram of the measurement setup for transistor currents and voltages, with a photograph of the test PCB design and the current probes.

a measurement bandwidth of 2 GHz. The N2796A is provided with connections maintaining the probe head as close as possible to the measurement point, thereby greatly reducing any excess parasitic inductance. The probe is connected to a second DSO 9254A oscilloscope as shown in Fig. 1. The gate-source voltage  $v_{GS}(t)$  is probed through an SMA cable and a T-junction, and measured with the same oscilloscope. A de-embedding of the T-junction and SMA cable allows to assess the gate voltage at the exact same point where the gate current is measured.

A bias-tee is connected to the MOS drain terminal to separate the RF signal and the supply path. A 50 ohm resistor was connected to the RF output of the bias-tee. This is important to minimize reflections at higher frequencies, which otherwise impair the measurements.

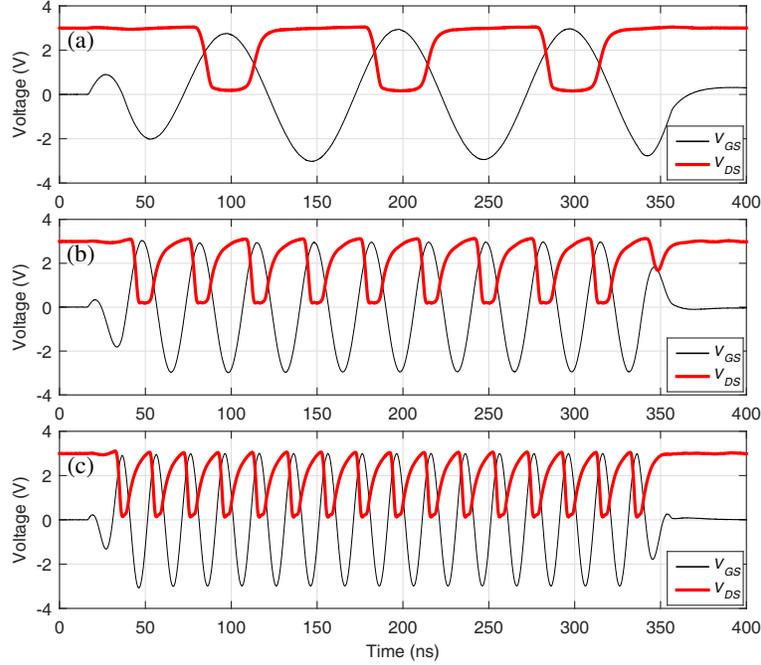
An 8110A pulse generator synchronizes both the two oscilloscopes and the arbitrary waveform generator (AWG). The two oscilloscopes were triggered with great precaution so that the current waveform measurement coincided with the injected RF pulse. Oscilloscopes and AWG were computer-controlled. The input signal was pulse modulated in order to prevent thermal effects in the DUT and the modulation pulse width was set to 300 ns with a repetition period of 1 ms. The fall and rise times of the modulation are 20 ns. The output voltage from the RF amplifier was maintained constant at 3 V over the frequency range of [10 MHz–1 GHz].

In the next section we will present the measurements when the inverter is stressed by typical PME.

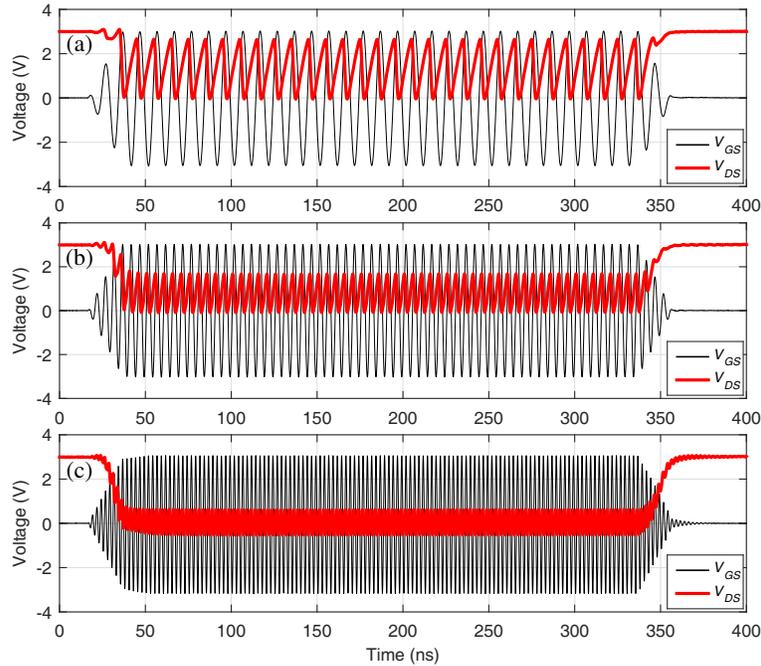
### 3. RESPONSE OF A MOS INVERTER TO A PME

The effect of the PME is functionally observed on the measurement of the output voltage of the MOS inverter shown in the center part of Fig. 1. The curves in Fig. 2 are input/output voltage waveforms for frequencies of 10 MHz, 30 MHz and 50 MHz with the same peak value of 3 V of the PME applied to the gate terminal. These plots depict  $v_{DS}$  voltages exhibiting a logic waveform in response to the PME excitation. In essence, the inverter follows the input frequency.

Figs. 3(a) and (b) show the alteration of the inverter response when the frequency is increased to 100 MHz or 200 MHz. The output voltage  $v_{DS}$  no longer looks like a logic waveform and the  $v_{DS}$  voltage swing decreases with frequency. At the frequency of 400 MHz (see Fig. 3(c)) this voltage swing is so reduced that the inverter output is a sine signal between  $-0.7$  V and  $+0.7$  V. In fact, as the carrier frequency increases, the inverter response tends to reproduce the opposite of the pulse envelope with a small amount of the RF signal superimposed, the latter being so small at 400 MHz that the output signal is always below the commutation threshold of a classic logic gate. As a main result, the input of any logic block following the inverter will be totally inhibited and pinned on the lower logic level. We get a blocking of the output state, while we were expecting a tracking of the control voltage. This effect will be hereafter referred to as the “blocked state” of the inverter. This blocked state occurs

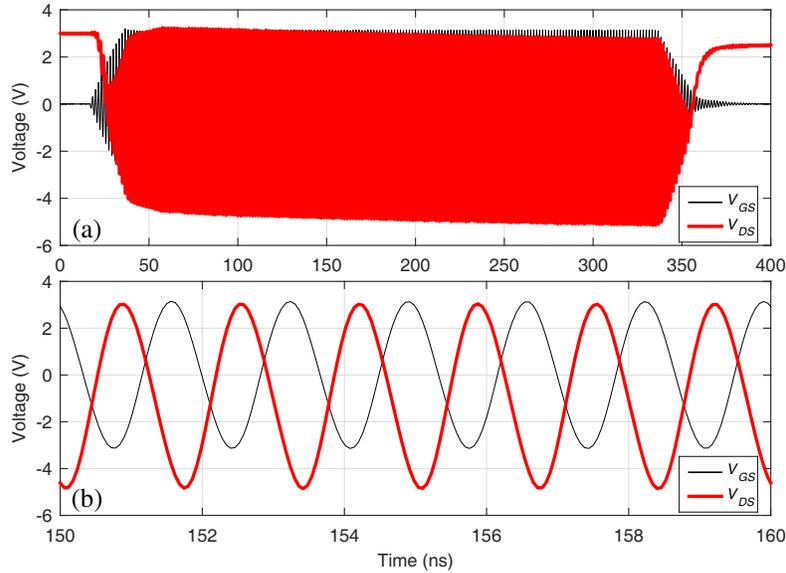


**Figure 2.** Input/Output voltages for an input PME of 3 V at 10 MHz (a), 30 MHz (b) and 50 MHz (c).  $V_{DD} = 3$  V.



**Figure 3.** Input/Output voltages for an input PME of 3 V at 100 MHz (a), 200 MHz (b) and 400 MHz (c).  $V_{DD} = 3$  V.

up to a PME frequency of 500 MHz. Beyond this value, this phenomenon disappears, as illustrated in Fig. 4. For such a high frequency, the output voltage  $v_{DS}$  again follows the input voltage and exhibits an increased peak amplitude of  $\hat{v}_{DS} \approx 3$  V, behaving as if the input voltage  $v_{GS}$  directly ends up to the inverter output.



**Figure 4.** Input/Output voltages for an input PME of 3 V at 600 MHz (a).  $V_{DD} = 3$  V. (b) Zoom of (a) from 160 ns to 170 ns.

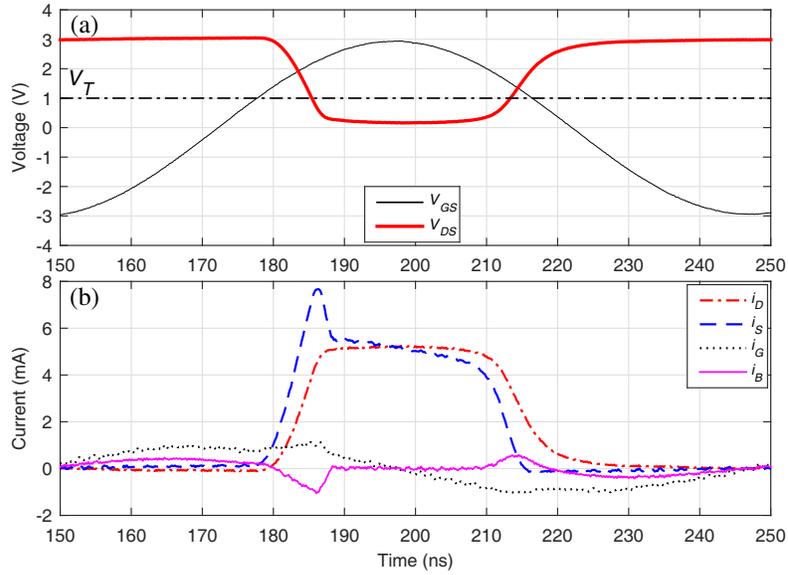
In the next section, an in-depth analysis will be carried out to explain these observed behaviours with the help of the measured currents.

#### 4. INPUT/OUTPUT CURRENT WAVEFORMS UNDER PME

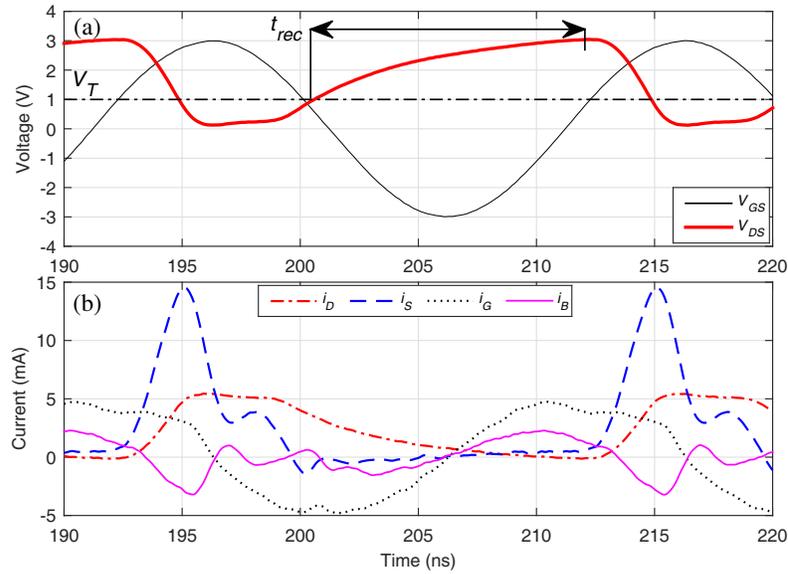
The study of current waveforms during switching operation aims at getting insights of the “blocked state” of the MOS inverter induced by the PME. In this section, input/output voltage and current waveforms are given in Figs. 5 to 9 for increasing frequencies from 10 MHz to 600 MHz, and with the same PME peak value of 3 V applied to the gate terminal. As the input impedance of the circuit decreases with frequency rise, the power of the PME has to be increased in order to maintain the input voltage constant.

For the lower frequencies, classical current-waveforms measured on an NMOS inverter under switching operation are obtained. Actually in our experiments, the switching of the MOS inverter is caused by a sinusoidal gate control signal, unlike the conventional square input. At 10 MHz,  $v_{DS}$  follows the input signal  $v_{GS}$ , and looks like a normal logic waveform (Fig. 5(a)). Corresponding currents (Fig. 5(b),  $i_D$ ,  $i_S$ ,  $i_G$  and  $i_B$  are the drain, source, gate and bulk currents, respectively) show a device operating in a switched mode driven by a sinusoidal input. As a result, the transistor charge distribution varies continually, generating charging currents dominated by the extrinsic part of the device, particularly the one associated with the depletion regions [15].

When  $v_{GS}$  exceeds the threshold voltage  $V_T$ ,  $i_S$  starts flowing; the device turns on; the output voltage  $v_{DS}$  tends to switch from  $V_{DD}$  to 0 V. Overshoots observed on  $i_S$  and  $i_B$  with a relatively large peak value are explained by these charging currents caused by the large-signal dynamic operation of the MOS transistor. Once the peak input value is reached ( $v_{GS} = 3$  V), the DC steady-state is reached with  $i_S = i_D = 5.5$  mA. The subsequent decrease of  $v_{GS}$  drives a corresponding decrease of  $i_S$  and a change in the inversion layer charge distribution. When the control voltage falls below  $V_T$ , the device tends to turn off and  $v_{DS}$  grows back to its higher value. As observed on Fig. 5(b), the time required to turn-off is longer than the turn-on time. During the turn-on process the device operates in a non-saturation region and the resulting low channel resistance speeds up the switching, to the contrary of the turn-off process where the drain resistance limits the return to zero of  $i_D$ . The time to turn-off, here named the recovery time,  $t_{rec}$ , is depicted in Fig. 6. Its measured value  $t_{rec} = 11$  ns is of tremendous importance in the interpretation of the experimental results of this paper because it is associated with the slower



**Figure 5.** Zoom of Input/Output voltages and currents of a MOS inverter with a 10 MHz/3 V PME applied ( $V_{DD} = 3$  V). (a) Voltages. (b) Currents.

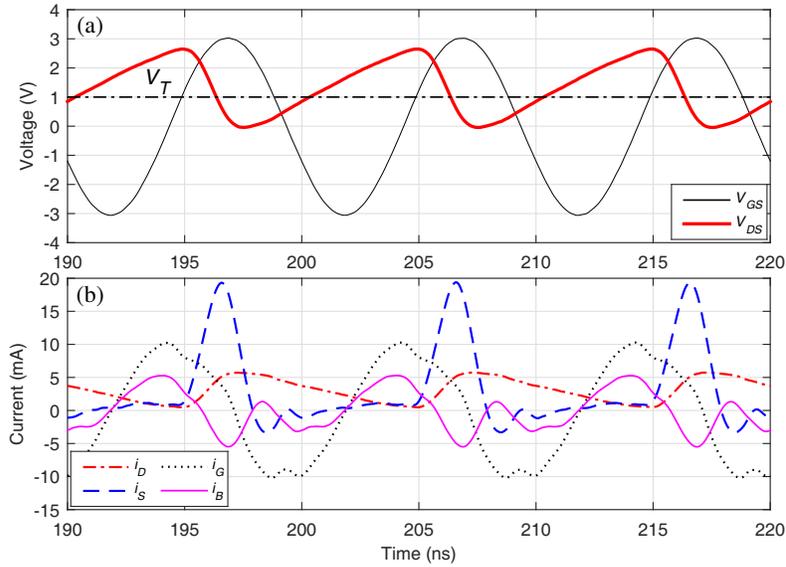


**Figure 6.** Zoom of Input/Output voltages and currents of a MOS inverter with a 50 MHz/3 V PME applied ( $V_{DD} = 3$  V). (a) Voltages. (b) Currents.

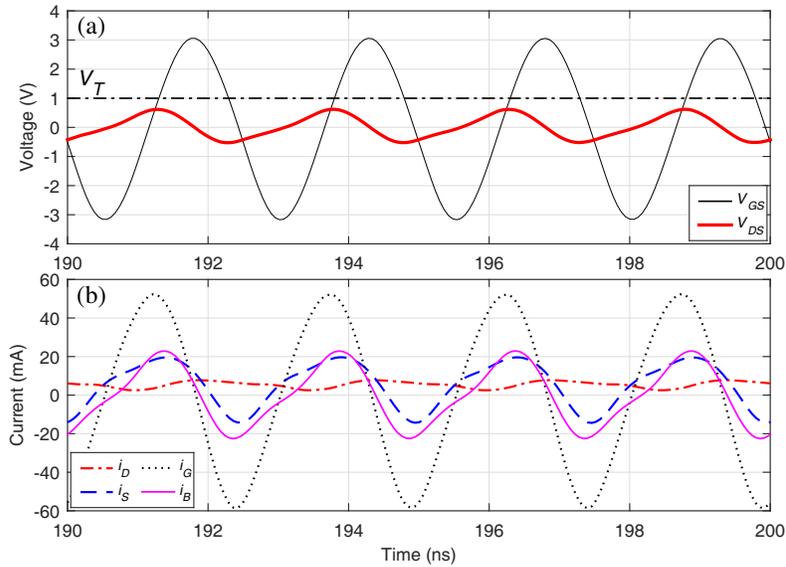
process.

At 50 MHz (see Fig. 6), the qualitative behaviour of the switching process is similar to that observed at lower frequency. All currents exhibit shapes similar to that obtained at 10 MHz. Once the peak input value is reached, the drain current reaches its DC steady state value  $i_D = 5.5$  mA, with the same turn-on time. Overshoots of source and substrate currents are more intense because of the larger  $dv_{GS}/dt$  that drives higher charging currents. Let us note that the off-state of the transistor is barely reached.

Increasing further the PME frequencies lead to a non-logic waveform for  $v_{DS}$ , close to a sawtooth, with a peak-to-peak drain voltage that tends also to decrease. The input voltage period,  $T \approx 10$  ns, now smaller than  $t_{rec}$ , indeed limits the  $v_{DS}$  increase rate and its previous maximum value  $V_{DD} = 3$  V is no longer reached (see e.g., Fig. 7(a) at 100 MHz). At the same time the DC steady-state value



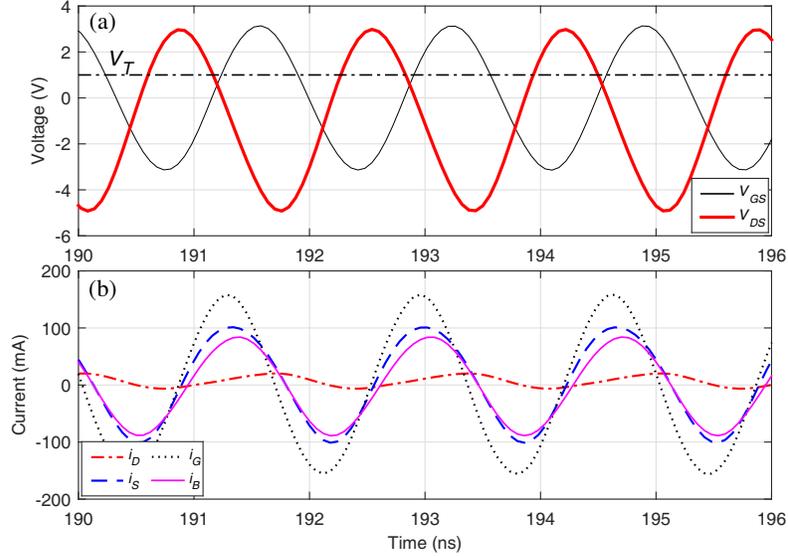
**Figure 7.** Zoom of Input/Output voltages and currents of a MOS inverter with a 100 MHz/3 V PME applied ( $V_{DD} = 3$  V). (a) Voltages. (b) Currents.



**Figure 8.** Zoom of Input/Output voltages and currents of a MOS inverter with a 400 MHz/3 V PME applied ( $V_{DD} = 3$  V). (a) Voltages. (b) Currents.

$i_D = 5.5$  mA is still reached, but during the turn-off process. Since the drain current never vanishes, the device is never off. The  $i_D$ -waveform now differs from the half-wave rectified current observed at low frequencies, where  $i_D$  flows only when  $v_{GS} \geq V_T$ . The consequence is an increase of  $\overline{i_D}$ , the mean value of  $i_D$ , and according to the load-line of the inverter, a decrease of  $\overline{v_{DS}}$ , the mean value of  $v_{DS}$ .

When switching to 400 MHz (Fig. 8), the effects previously pointed out are reinforced. The  $v_{DS}$ -waveform is very close to a sine of 1 V peak voltage superimposed to a DC component. Waveforms of Fig. 8(a) correspond to a “blocked state” of the inverter, lasting as long as the pulsed RF signal is applied. The period of the driven voltage  $v_{GS}$  is 2.5 ns, a value nearly four time shorter than  $t_{rec}$ . As already mentioned  $i_D$  no more vanishes and consequently  $\overline{i_D}$  further increases while  $\overline{v_{DS}}$  decreases. In the same time,  $v_{DS_{p-p}}$ , the  $v_{DS}$  swing, also tends to decrease with the PME frequency. To the contrary,



**Figure 9.** Zoom of Input/Output voltages and currents of a MOS inverter with a 600 MHz/3 V PME applied ( $V_{DD} = 3$  V). (a) Voltages. (b) Currents.

we observe a noticeable increase in the amplitude of source, gate and bulk currents. Moreover  $i_D$  is delayed with respect to the control voltage and its peak value of 7.5 mA is slightly higher than the DC steady-state value of 5.5 mA. The frequency of the control signal is now so high that the device reacts more to the time-variation of the input voltage than to its absolute value. At such high frequency, the impedances associated with the strong extrinsic capacitances of the device become so small that they lead to a “blocked state” of the MOS inverter.

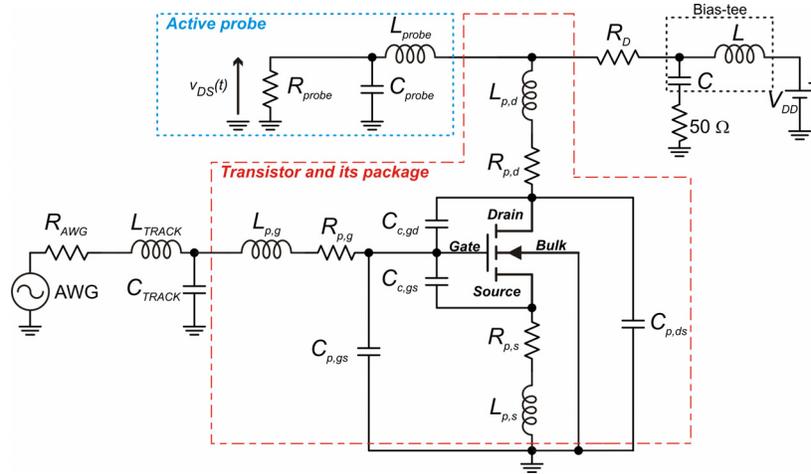
A further increase of frequency to 600 MHz together with a constant peak value of 3 V applied to the gate produces the waveforms given in Fig. 9. The inverter is no more in its “blocked state” and all currents are almost sinusoidal. Reasons are the too fast  $v_{GS}$  changes with respect to the MOS charges that are unable to follow such a rapid variation. The major part of the current flows through the inverter using shortcuts brought by the parasitic and external elements. Above 600 MHz new paths for the electromagnetic interference are opened by these parasitics, which shunt any transistor action, namely the classical intrinsic non-linearities associated with the transport current.

## 5. NUMERICAL SIMULATION

SPICE-like simulations were performed with Keysight ADS software to bring additional information, particularly regarding extrinsic parasitics that are believed mandatory to understand the circuit disruption. Note that our purpose here is not to reach a perfect fit between experimental and simulated results, but instead to confirm and identify the parasitics that drive the observed response of our inverter.

Lumped elements models are used for the transistor, package, tracks and active probe measuring  $v_{DS}$ . They are all represented in Fig. 10 with values in Table 2, and will be discussed step by step.

The MOS inverter is simulated using the compact model Philips MOS Model 9. This choice is fully appropriate to the present device. This model is simplified in that only few input parameters are required and should be determined from experiments. As for the intrinsic MOS, parameters values are obtained from the measured DC characteristics and the gate-to-channel capacitance. All charge storage provided by the extrinsic part of the MOS are modeled via bias-dependent and layout-dependent capacitances. They account for the overlap of the gate over both source and drain extensions ( $C_{gs,e_0}$  and  $C_{gd,e_0}$ ), the body-source and body-drain junctions ( $C_{bs,e}$  and  $C_{bd,e}$ ), and for layout-dependent capacitances because of the large source and drain contacts ( $C_{c,gs}$  and  $C_{c,gd}$ ). The only extrinsic resistance taken into account is the gate resistance because of its importance for high speed and RF signals. Bias-dependent capacitances and gate resistance are included in Philips MOS Model 9, and contact capacitances are added outside this model (cf Fig. 10). Parameters describing the DC characteristics and storage effects



**Figure 10.** Schematic diagram used to simulate the response of a MOS inverter to a PME.

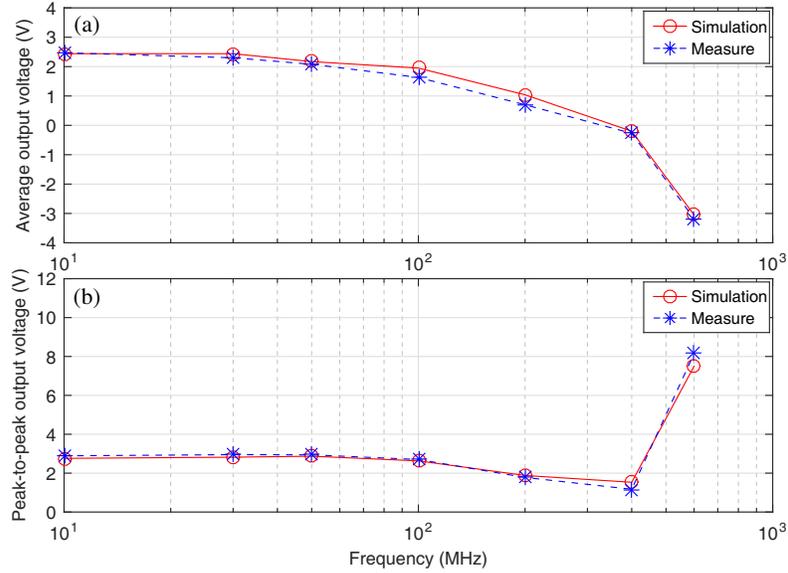
**Table 2.** Circuit model lumped elements values.

Circuit part	Element	Value
MOS extrinsic	$C_{gd,e0}, C_{gs,e0}$	0.6 pF
	$C_{bd,e}, C_{bs,e}$	3.5 pF
	$C_{c,gd}, C_{c,gs}$	0.5 pF
Package	$R_{p,g}, R_{p,s}, R_{p,d}$	1 $\Omega$
	$L_{p,g}, L_{p,d}$	0.6 nH
	$L_{p,s}$	1 nH
	$C_{p,gs}$	0.15 pF
	$C_{p,ds}$	0.1 pF
Active probe	$L_{probe}$	5 nH
	$C_{probe}$	1.2 pF
Track	$L_{track}$	9 nH
	$C_{track}$	4 pF

were extracted from static characteristics and from S-parameters at various bias conditions in the frequency range of interest [16, 17]. Once intrinsic and extrinsic parts of the transistor have been modeled, its SOT-143 package is considered. Because the excitation frequency exceeded the normal operating frequency of the device, the parasitic elements from the die to the external pads of the device cannot be ignored. New parasitic capacitances ( $C_{p,gs}, C_{p,ds}$ ), inductances ( $L_{p,g}, L_{p,d}, L_{p,s}$ ), and resistances ( $R_{p,g}, R_{p,d}, R_{p,s}$ ) such as pin-to-pin capacitance, as well as bond wire inductances and resistances, were added to the equivalent circuit of the MOS transistor.

In the considered frequency range, connections between package pins and chip are assumed as regular wires and not transmission lines. A simplified model based on few lumped elements is thus used. Package parasitics are extracted from S-parameters at various bias points and for an extended frequency range (compared to the nominal frequency band of operation). A set of parasitics can be found using a conventional de-embedding process with the reasonable hypothesis that they do not change with bias. Finally, the active probe electrical model is added to the schematic diagram of the inverter under PME. Again, it is extracted from measurements, namely the input impedance characteristics over the whole frequency range of interest. Owing to the knowledge of  $L_{probe}$  and  $C_{probe}$ , the drain-source voltage  $v_{DS}$  is numerically obtained in a way similar to what we did on the high impedance input of the oscilloscope.

The time-variation of the output voltage  $v_{DS}$  is computed using circuit envelope simulation mode



**Figure 11.** Comparison between measured (stars) and calculated (circles) outputs of the inverter as a function of the PME frequency, (a) average output voltage, (b) peak-to-peak output voltage.

of ADS. This technique consists in an harmonic balance analysis with time-varying envelop that particularly suits the PME modulated excitation signal used here. Note that a classical transient simulation-mode could also be used. The steady-state output of the nonlinear circuit is thus computed over a specified duration chosen in accordance with the repetition time of the PME. To compare with experiments we summarized the experimental time traces of Figs. 2–4 during the application of the PME with  $v_{DS_{p-p}}$  and  $\overline{v_{DS}}$ . These two values were also calculated with the numerical model and the results are both plotted for comparison in Fig. 11 as a function of  $f$ , the carrier frequency of the PME.

Both the measured and computed results show a regular decrease of  $\overline{v_{DS}}$  with  $f$ . The evolution of  $v_{DS_{p-p}}$  is a little bit more complicated and exhibits a sudden regrowth above 400 MHz according to the resonance brought by parasitics, the latter being estimated  $\approx 700$  MHz from values of Table 2. The internal gate voltage is thus far much higher than the one externally fed to the device. Again, both the experimental and computed curves compare favorably. The “blocked state” of the inverter is thus highlighted for frequencies between approximately 100 MHz and 400 MHz. In fact, the correspondence between calculations and experiments was only possible when accounting for all the parasitics surrounding the ADS Philips MOS Model 9. It confirms the tremendous role played by all MOS extrinsic elements but also by the parasitics brought by the package and the PCB tracks, that act together in the occurrence of the circuit disruption observed experimentally.

## 6. CONCLUSION

In this paper, we have experimentally studied the electromagnetic susceptibility of the MOS transistor to PME. The methodology and equipment setup for direct injection experiments and acquisition of all transistor instantaneous currents/voltages developed here have helped to get insights of the understanding of PME effects on MOS technology at the device level.

Experimental results have highlighted the dramatic effect of electromagnetic interferences that may lead to a “blocked state” of a MOS inverter. In this particular state, the output is maintained in a constant low state as long as the RF pulse is applied, and the transistor no more follows the control voltage  $v_{GS}$ . It was shown to occur if the excitation frequency is set within a bandwidth just beyond the maximum switching frequency of the inverter.

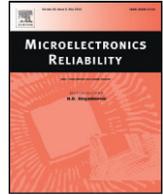
The analysis of current waveforms during this “blocked state” has led to the conclusion that the MOS transistor’s extrinsic elements and the PCB parasitics play a very important role in the occurrence of this effect. Numerical simulations have confirmed this point, as the phenomenon only appeared if

these elements were taken into account.

This “blocked state” could potentially generate upset events in larger electronic systems and will certainly also appear on more recent MOS technologies, but probably at higher frequencies because intrinsic and extrinsic capacitances are indeed reduced when shortening the gate length. The knowledge of the involved physical mechanisms is the basis to accurately understand the EM susceptibility. From the defender viewpoint, this study may help to predict how PME can upset circuits and thereby help in designing more robust electronic systems. From the attacker side, it can be useful to upset the targeted system more efficiently.

## REFERENCES

1. Ni, G., B. Gao, and J. Lu, “Research on high power microwave weapons,” *IEEE Asia-Pacific Microwave Conference*, 10–14, 2005.
2. Backstrom, M. and K. Lovstrand, “Susceptibility of electronic systems to high-power microwaves: summary of test experience,” *IEEE Trans. Electromagn. Compat.*, Vol. 46, No. 3, 396–403, 2004.
3. Hwang, S.-M., J.-I. Hong, and C.-S. Huh, “Characterization of the susceptibility of integrated circuits with induction caused by high power microwaves,” *Progress In Electromagnetics Research*, Vol. 81, 61–72, 2008.
4. Wang, H., J. Li, H. Li, K. Xiao, and H. Chen, “Experimental study and spice simulation of CMOS inverters latch-up effects due to high power microwave interference,” *Progress In Electromagnetics Research*, Vol. 87, 313–330, 2008.
5. Tsai, H.-C., “Reliable study of digital IC circuits with margin voltage among variable DC power supply, electromagnetic interference and conducting wire antenna,” *Microelectron. Reliab.*, Vol. 43, No. 12, 2001–2009, 2003.
6. Forcier, M. and R. Richardson, “Microwave-rectification RFI response in field-effect transistors,” *IEEE Trans. Electromagn. Compat.*, Vol. 21, No. 4, 312–315, 1979.
7. Richardson, R., “Quiescent operating point shift in bipolar transistors with AC excitation,” *IEEE J. of Solid-State Cir.*, Vol. 14, No. 6, 1087–1094, 1979.
8. Richardson, R., “Modeling of low-level rectification RFI in bipolar circuitry,” *IEEE Trans. Electromagn. Compat.*, Vol. 21, No. 4, 307–311, 1979.
9. Richardson, R., V. Puglielli, and R. A. Amadori, “Microwave interference effect in bipolar transistors,” *IEEE Trans. Electromagn. Compat.*, Vol. 17, No. 4, 216–219, 1975.
10. Jović, O., C. Maier, and A. Barić, “High-voltage PMOS transistor model for prediction of susceptibility to conducted interference,” *IEEE Trans. Electromagn. Compat.*, Vol. 53, No. 1, 53–62, 2011.
11. Pouant, C., J. Raoult, and P. Hoffmann, “Large domain validity of MOSFET microwave-rectification response,” *IEEE 10th International Electromagnetic Compatibility of Integrated Circuits*, 232–237, 2015.
12. Holloway, M., Z. Dilli, N. Seekhao, and J. Rodgers, “Study of basic effects of HPM pulses in digital CMOS integrated circuit inputs,” *IEEE Trans. Electromagn. Compat.*, Vol. 54, No. 5, 1017–1027, 2012.
13. Op’t Land, S. T., M. Ramdani, R. Perdriau, M. Leone, and M. Drissi, “Simple, Taylor-based worst-case model for field-to-line coupling,” *Progress In Electromagnetics Research*, Vol. 140, 297–311, 2013.
14. Sicard, E. and J. Dienot, “Issues in electromagnetic compatibility of integrated circuits: emission and susceptibility,” *Microelectron. Reliab.*, Vol. 45, No. 9, 1277–1284, 2005.
15. Tsvividis, Y. and C. McAndrew, *Operation and Modeling of the MOS Transistor*, Oxford Univ. Press, 2011.
16. Cheng, Y., M. Deen, and C.-H. Chen, “MOSFET modeling for RF IC design,” *IEEE Trans. Elect. Dev.*, Vol. 52, No. 7, 1286–1303, 2005.
17. Kwon, I., M. Je, K. Lee, and H. Shin, “A simple and analytical parameter-extraction method of a microwave MOSFET,” *IEEE Trans. Microw. Theory Tech.*, Vol. 50, No. 6, 1503–1509, 2002.



## Out-of-band disturbance of mm-wave EMI on RF front-ends



P. Payet, M. Guery, J. Raoult \*, L. Chusseau

IES, UMR 5214, Université de Montpellier, 860 rue St Priest, 34095 Montpellier, France

### ARTICLE INFO

#### Article history:

Received 23 May 2017

Received in revised form 27 June 2017

Accepted 17 July 2017

Available online 25 July 2017

#### Keywords:

Out-of-band disturbance

Millimeter wave

RF front-end

Electromagnetic coupling

### ABSTRACT

The effects of highly out-of-band electromagnetic interference (EMI) on a RF front-end are experimentally evaluated. Signal at 60 GHz with a moderate power is produced in the near-field owing to an open-ended WR15 waveguide fed by a Gunn diode. Due to the nonlinear behavior of active devices, we observed a gain quenching leading to complete extinction of either the transmitter or the receiver of the front-end subject to EMI. The paper proposes a detailed analysis of both CW and chopped EMI by varying almost all experimental conditions, namely the polarization, the target distance, and the chopping mode.

© 2017 Elsevier Ltd. All rights reserved.

### 1. Introduction

The electronic immunity of integrated circuits (IC) is of major concern with the increasing density of components and systems able to communicate [1]. Disturbances are usually considered within the nominal operating bandwidth where it is feared that they are the most dangerous. Transistors that operate at frequencies much higher than the circuit make it sensitive outside the designed operating bandwidth (out-of-band signals) [2]. Although high frequencies do not contribute to the output signal, they may induce DC offsets and low frequency amplitude variations at the output, mainly because of the non-linear behavior of the active devices [3]. Out-of-band investigations thus have to be performed with both analog and digital circuits.

In practice, interferences may be either unwanted or targeted by an attacker. On the one side, unwanted disruptions may result from the multiplication of communicating devices that fill the electromagnetic environment with growing operating frequencies. As an example, a laptop can disrupt a medical device or even tools onboard of an aircraft [4]. This arises because operating frequencies of such unintentional interferers are constantly increasing to reach now the millimeter-wave bands for example with the emergence of the future 5G standard or last Wifi generation 802.11ad [5]. On the other side, a lot of intentional sources exist such as jammers but also military sources dedicated to intentional EMI attack. These sources are usually classified according to their power and/or frequency band, for example in narrow band high power microwave (HPM) sources or high-intensity radiated fields (HIRF) sources produced by electron beam [6] and operating in the 1–

100 GHz band. High-power broadband sources use the ultra-wide band (UWB) or radar technologies with pulsed high-voltage generators [7]. The effects of intentional EMI by such sources have been examined in [8]. They are mainly used on front door targets where the coupling path uses available ports for the propagation of electromagnetic energy and communication with the external environment, for example antennas or sockets [9].

In [10] digital circuits of clock frequencies in the MHz range were tested in the GHz band. Susceptibility was characterized either by a prescribed threshold change on the output voltage or on the timing jitter. Although no upset was observed, perturbation criteria were reached at discrete frequencies up to  $\approx 12$  GHz followed by a sudden decrease with no more occurrences up to the 40 GHz limit of the setup. Even if such a lower susceptibility at high frequency is commonly observed, we decided to irradiate a commercial analog circuit with a millimeter-wave source operating at 60 GHz to evaluate its electromagnetic susceptibility. To the best of our knowledge, no EMI study has been conducted yet involving a millimeter-wave source and usual RF front-ends operating in typical communication bands.

### 2. Experimental setup

The experimental arrangement is given in Fig. 1. The mm-wave source is a Gunn oscillator (Quinstar, QTM-602001SV) delivering 20 dBm at 60 GHz. This source has the advantage of both compactness and cheapness for such high frequency. This source can be switched on and off using a TTL signal whose frequency  $f_m$  is limited to 20 kHz and a 35 dB isolator of 1.3 dB insertion losses ensures a stable operation whatever its load. An open-ended rectangular WR15 waveguide of size  $3.76 \times 1.88$  mm<sup>2</sup> radiates the signal onto the device under test (DUT).

\* Corresponding author.

E-mail addresses: [payet@ies.univ-montp2.fr](mailto:payet@ies.univ-montp2.fr) (P. Payet), [raoult@ies.univ-montp2.fr](mailto:raoult@ies.univ-montp2.fr) (J. Raoult).

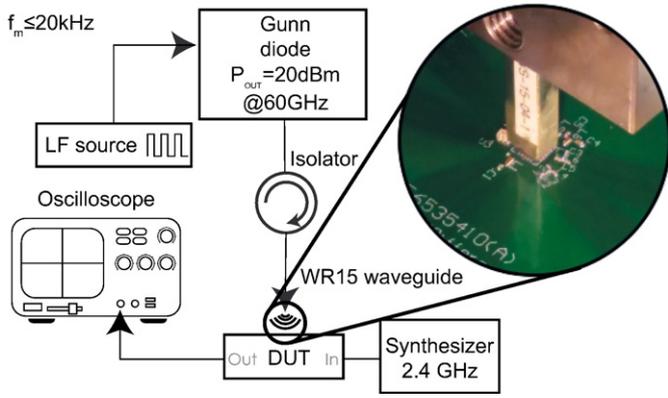


Fig. 1. Scheme of the experimental setup.

The relative 3D positioning of the waveguide above the circuit package is achieved via motorized stages. A graduated rotation ring attached to the Z-stage allows the positioning of the waveguide with a 1° accuracy. To overcome the relatively low power of the source, the DUT package is placed as close as possible, in the near-field, at typical distances  $100 \mu\text{m} \leq h \leq 2 \text{ mm}$  that are well below the  $\lambda = 5 \text{ mm}$  wavelength. In practice, it was not possible to move to smaller distances because of the respective dimensions of the guide and of the circuit package and because of a risk of short-circuiting. Such a small  $h$  hereby guarantees that the maximum energy is transferred locally in a small region of the circuit. As a rough estimate, the 75 mW microwave power travelling into the waveguide induces a maximum field intensity of  $E_{\text{TM}} = 4.6 \text{ kV/m}$  [11]. The transverse electric field radiated by the open-end of the waveguide was subsequently calculated using a method proposed in [12]. It is plotted in Fig. 2 as a function of  $h$  and a 2D view of the diffracted field profile is given in inset. A rapid decrease of the maximum field strength is observed with distance. With a typical distance of  $h_d = 800 \mu\text{m}$  between IC and package surface, the maximum field impinging onto the IC is calculated in between 2.7 kV/m and 1.2 kV/m for distances  $h = 100 \mu\text{m}$  and  $h = 2 \text{ mm}$ , respectively. Such field intensities are of the same order of magnitude of what is usually produced by high-power microwave tests [13].

The Fig. 3 illustrates the compact design of a typical IC package and its relative dimension with respect to the open-end waveguide. The height noted  $h$  corresponds to the sample-guide distance. The height noted  $h_d$  is the distance of the die under the package.

DUTs are specifically COTS circuits incorporating a LNA or the combination of a LNA and a PA (front-end). The choice of these circuits was motivated by their frequency ranges covering from 400 MHz to 5.1 GHz. The second criterion was the thickness of the package that influences the true power received by the die. Front-ends include a switch

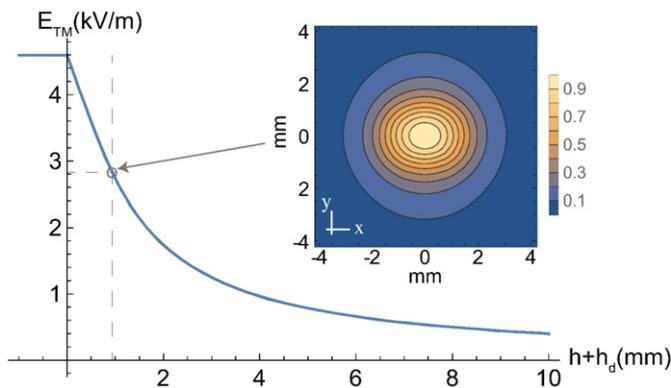


Fig. 2. Calculated 60 GHz transverse field intensity as a function of the distance to the open-ended waveguide with its smallest dimension on  $y$  axis. Inset is a 2D field profile at  $900 \mu\text{m}$ .

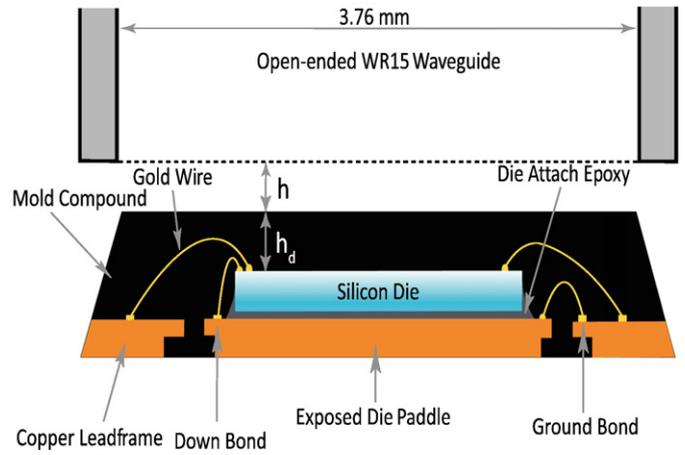


Fig. 3. Scheme of DUT package construction and dimension with respect to DUT.

for selecting the transmission path (TX) or the receive path (RX). Whatever the mode selected, the DUT operates in the linear regime and at the nominal frequency. The frequency signal is obtained from a Keysight synthesizer N5171B. The output signal is monitored in the time domain using a Lecroy oscilloscope ZI610. The average supply current is monitored by an amperemeter to evaluate the consumption of the device.

### 3. Experimental result

#### 3.1. CW injection

The first device tested is a commercial Front-End module (RF6535) enabling Wifi and Zigbee applications in the 2.4 GHz band. In TX mode, the power amplifier (PA) is selected and a typical 26 dB gain is achieved at the supply current  $I_s = 72 \text{ mA}$ . The PA output is limited to a maximum of 23 dBm. During the experiments the output power is set at  $-6 \text{ dBm}$ , operating in its linear regime. In RX mode, the low noise amplifier (LNA) exhibits a typical 10.5 dB gain with  $I_s = 10.7 \text{ mA}$ . Preliminary experiments were conducted with the Gunn diode operated in CW mode. PA and LNA were successively activated while the IC package was placed just below the waveguide. By monitoring the output of the selected function, a reduction in the amplitude of the 2.4 GHz signal was measured as a function of position and orientation. The extinction ratio is expressed by

$$\alpha_{\text{CW}} = 1 - \frac{A_p}{A_{\text{unp}}} \quad (1)$$

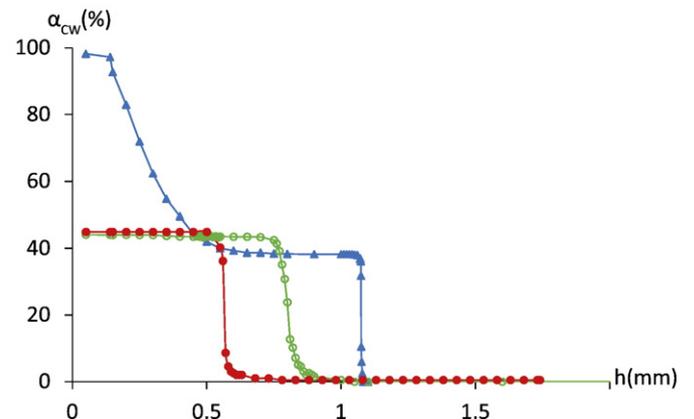


Fig. 4. CW extinction ratio  $\alpha_{\text{CW}}$  versus  $h$ .  $\blacktriangle$ : PA at  $M_{\text{opt}}^{\text{PA}}$ ,  $\circ$ : LNA at  $M_{\text{opt}}^{\text{LNA}}$ ,  $\bullet$ : LNA at  $M_{\text{opt}}^{\text{PA}}$ .

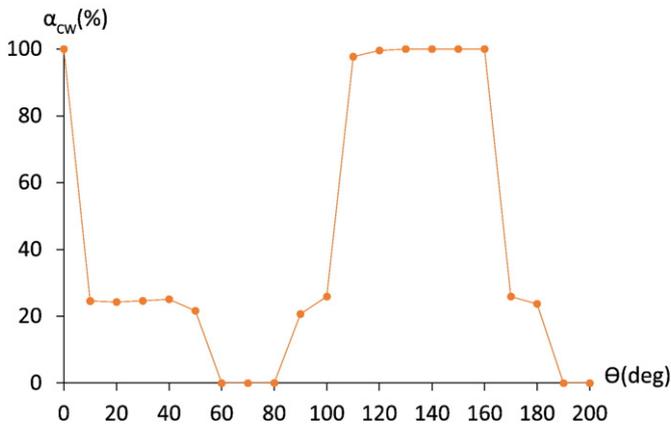


Fig. 5. CW extinction ratio  $\alpha_{CW}$  versus  $\theta$ .

where  $A_p$  is the output signal amplitude when the DUT is submitted to the perturbation, and  $A_{unp}$  is the output signal amplitude in normal operation (without any perturbation). The position of the optimum sensitivity with the function PA or LNA are called  $M_{opt}^{PA}$  and  $M_{opt}^{LNA}$  respectively in the sequel.

As evaluated separately, the  $E$ -field intensity decreases by a factor  $\approx 2.5$  as a function of  $h$ , which ranges from  $100 \mu\text{m}$  to  $2 \text{mm}$ . The amount of the perturbation is reported in Fig. 4 where  $\alpha_{CW}$  is plotted as a function of  $h$ . The PA and the LNA are affected in that range because  $\alpha_{CW}$  is zero at great distances and suddenly undergoes an important increase at a specific distance. For the three cases considered here: i) the PA, ii) the LNA at  $M_{opt}^{PA}$  and iii) the LNA at  $M_{opt}^{LNA}$ , it occurs in the range  $0.5 < h < 1.1 \text{mm}$ . Beyond that threshold both PA and LNA outputs are attenuated by almost 50% over a wide  $h$ -range. For the PA,  $\alpha_{CW}$  increases further up to  $\approx 100\%$  when  $h$  is reduced. This is not observed for the LNA, which shows a maximum perturbation of  $\approx 45\%$  for the two positions considered. Notice that these two measurement points,  $M_{opt}^{PA}$  and  $M_{opt}^{LNA}$ , were separated by  $\approx 300 \mu\text{m}$ , the possible distance separating the implantation of both functions on the die.

Starting from  $M_{opt}^{PA}$  where a complete extinction was observed we rotate the waveguide axis with respect to the DUT, the rotation being measured by the angle  $\theta$ . The amount of the perturbation vs  $\theta$  is represented in Fig. 5. As seen the perturbation switch from nearly complete to almost null as a function of  $\theta$  with a periodicity which is  $90^\circ$ . As a rough interpretation one can imagine that the linearly polarized electric field is projected either on power rails of the die or on a bounding wire. By turning the waveguide, the projection of the field along that line is more or less efficient and/or change from one line to another, thereby changing the coupled EMI that is converted into voltage changes into

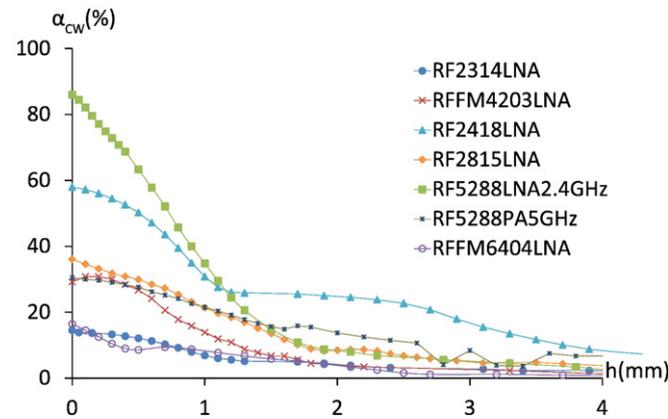


Fig. 6. CW extinction ratio  $\alpha_{CW}$  versus  $h$  at  $\theta_{opt}$ .

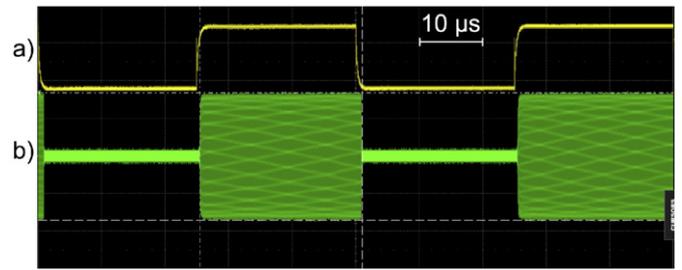


Fig. 7. a) TTL Gunn control voltage at  $f_m = 20 \text{kHz}$ . b) LNA output under chopped mode at position  $M_{opt}^{LNA}$ , and  $h = 100 \mu\text{m}$ .

the IC by its intrinsic nonlinearities. Indeed, polarization is a parameter closely related to the observed sensitivity.

The first outcome of CW tests is the proof of a local perturbation of the IC, and even with a spatial resolution which goes to the inside of the IC, owing to the near-field 60 GHz EMI injection. A higher sensitivity of the PA to such EMI attack as compared to the LNA is also observed for the sample considered here (RF6535). A second outcome of CW tests is that a 60 GHz field may perturb a common RF electronic device depending on its polarization.

As shown in Fig. 6, all ICs are disturbed and we observed that the LNA seems to be the most sensitive function. There is a significant impact at  $h = 0 \text{mm}$  since we observed drop out of the CW sample outputs ranging from about 20% to 85%. These results were obtained at the optimum position and angle.

In a second time the TTL chopper was applied to the Gunn diode and the output of the Front-End RF6535 was observed on the sampling scope. The Fig. 7 shows the LNA output at  $h = 100 \mu\text{m}$  and  $f_m = 20 \text{kHz}$ , the Gunn diode being active when the TTL control voltage is zero. The LNA output appears as shaded areas.

It exhibits very strong variations that follow the chopper with an extinction ratio that is almost complete when the 60 GHz EMI is applied. Notice that for the same conditions in CW mode, we had only  $\alpha_{CW} \approx 45\%$ . The chopper, even if it is at very low frequency as compared to both the operating frequency and the Front-End bandwidth, enforces considerably the perturbation. The underlying mechanism has yet to be elucidated.

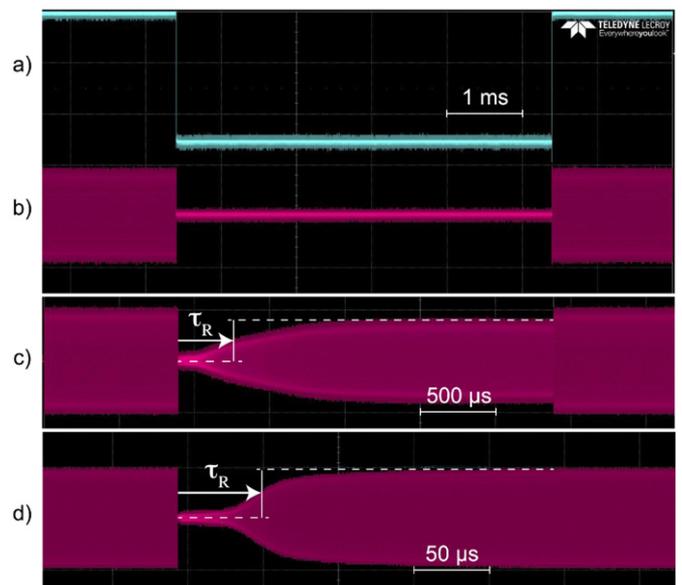


Fig. 8. PA output under chopped mode at position  $M_{opt}^{PA}$ . X-axis is stretched so as every square pulse is of the same size whatever  $f_m$ . a) TTL Gunn control voltage. b)  $h = 100 \mu\text{m}$ . c)  $h = 1100 \mu\text{m}$ . d)  $h = 1200 \mu\text{m}$ . The higher  $\tau_R$ , the most efficient the perturbation, because the target is affected on a more longer timescale.

**Table 1**  
Sensitivity of measured output devices to many input parameters.

Reference	Function	f (GHz)	TP (mm)	Impact (%)
RF2314	LNA	0,48	1,14	15
RFFM4203	LNA	2,45	0,975	30
RF5288	LNA	2,45	0,85	85
RF5288	LNA	5	0,85	0
RFFM6404	LNA	0,44	0,975	15
RF2815	LNA	1,575	1,47	35
RF6535	LNA	2,4	0,5	80
RF2418	LNA	0,7	1,47	60
RF6535	PA	2,4	0,5	100
RFFM4203	PA	2,45	0,975	0
RF5288	PA	2,45	0,85	5
RF5288	PA	5	0,85	30
RF6404	PA	0,44	0,975	5

### 3.2. Pulse injection

The Fig. 8 shows PA outputs at the three heights  $h = 100, 1100$  and  $1200 \mu\text{m}$ . The complete switching of the output signal at  $h = 100 \mu\text{m}$  follows exactly the TTL Gunn driven voltage, this is not surprising since we already measured  $\alpha_{\text{CW}} = 100\%$  in CW mode at that height. The two other traces (Fig. 8c and d) corresponds however to points where we had  $\alpha_{\text{CW}} \approx 20\%$  and  $\alpha_{\text{CW}} \approx 0\%$ , respectively. The temporal evolution of the PA output does not reproduce the chopped Gunn output. A sudden complete extinction of the function just follows the rising edge of the source and then one observes a slow trumpet-shape recovery toward the 2.4 GHz amplitude given by  $\alpha_{\text{CW}}$ . This dynamical behavior is here particularly evidenced by the choice of low  $f_m$  values for each  $h$  allowing to recover the steady-state. It allows to define the recovery time  $\tau_R$  as the time to recover 50% of the level reached in CW (see Fig. 8). Notice that in Fig. 7 we chose a high  $f_m$  with aim to show a possible complete extinction with the LNA. Nevertheless with a lower  $f_m$  we would also get this function recovery up to the  $\alpha_{\text{CW}} = 45\%$  value corresponding to that experimental conditions. The EMI attack dynamic is characterized by the recovery time  $\tau_R$  whose determination from oscillograms is drawn for a non-zero  $\alpha_{\text{CW}}$  in Fig. 8c and for  $\alpha_{\text{CW}} = 0$  in.

## 4. Discussion and conclusion

Experiments have illustrated the possible remote extinction of several Front-Ends modules over a wide frequency band using an EMI produced by a mm-wave Gunn diode. The following table summarizes the various DUTs with features like their thickness packages called TP, and their operating frequency called f. It also contains the impact of EMI disturbance for all tested boards.

The first observation made is that nearly all modules are affected. The second is that no obvious parameter emerges to favor the impact of mm-wave EMI on a specific device. The most sensitive samples have thicknesses that can vary by a factor of two with the same impact. The frequency of operation is not a good observable to determine the sensitivity of a sample. For a package thickness and an identical operating frequency, the impact can vary between 30 and 80%. The sensitivity seems rather design-dependent (Table 1).

The efficiency of the perturbation is considerably enhanced with a chopped microwave signal. Both the LNA and the PA have been

aggressed, preliminary results showed a higher sensitivity of the latter on the RF6535 sample. Further study with other IC showed that it was an isolated case whose the cause remains to be determined. The observation of the dynamic recovery on the two functions of the RF6535 is very similar. According to, and without any knowledge of the physical implantation on the die, this is the proof that attacks have induced effects of the same kind on the same type of targets, probably the supply voltage lines because of their large size and because of the proven sensitivity to polarization of waveguide.

When we highlighted these effects for the first time, we were very surprised because they were not foreseen in the literature [10]. In addition, it was quite astonishing that a Wifi module, otherwise known as very robust toward an EMI attack [14], could be so easily upset. This is probably because of the strong out-of-band character of the attack performed at mm-waves for a GHz circuit. Moreover a variation of the consumption current was measured. This is certainly due to a rectification phenomenon generated by non-linearities of the circuit [3]. In order to confirm the observed experimental behavior, first SPICE-simulations are in progress. Although the physical coupling between our mm-wave source and the DUT arises because of the vectorial nature of the electromagnetic field, we model it in a first attempt using a simple capacitive coupling between field intensity and induced current. Studies raise the possibility that coupling takes place on the power supply rail and the induced current which propagates toward the active function like current mirror [15]. Nonetheless, all details on the physical mechanisms involved will certainly be unveiled only with a perfect knowledge of the layout, and thus a close collaboration with a founder.

## References

- [1] M. Ramdani, et al., The electromagnetic compatibility of integrated circuits—past, present, and future, *IEEE Trans. Electromagn. Compat.* 51 (2009) 78–100.
- [2] C. Pouant, et al., Large Domain Validity of MOSFET Microwave - Rectification Response, *EMC Compo*, 2015 232–237.
- [3] M.J. Van der Horst, A. Linnenbank, Amplitude-modulation detection in single-stage negative-feedback amplifiers due to interfering out-of-band signals, *IEEE Trans. Electromagn. Compat.* 47 (1) (2005) 34–44.
- [4] S. Bandopadhyay, J. Varkey, EMI susceptibility characteristics of electromedical equipment in a typical hospital electromagnetic environment with particular reference to electrocardiography, *IEEE Int. Conf. Electromagn. Compat.* (1995) 266–272.
- [5] E. Perahia, et al., IEEE 802.11 ad: Defining the Next Generation Multi-Gbps Wi-Fi, 7th IEEE Consumer Communications and Networking Conf, 2010 1–5.
- [6] E. Schamiloglu, High Power Microwave Sources and Applications, *Microwave Symposium Digest, 2004 IEEE MTT-S International*, vol. 2, 2004 1001–1004.
- [7] Baryshevsky V. G. and et al., A Compact High Power Microwave (HPM) Source, *Pulsed Power Conference, 2009 IET European*, 2009.
- [8] W.A. Radasky, et al., Introduction to the special issue on High-Power Electromagnetics (HPM) and Intentional Electromagnetic Interference (IEMI), *IEEE Trans. Electromagn. Compat.* vol. 46 (3) (2004) 314–321.
- [9] D. Mansson, et al., Vulnerability of European rail traffic management system to radiated intentional EMI, *IEEE Trans. Electromagn. Compat.* vol. 50 (1) (2008) 101–109.
- [10] R. Perdriau, et al., Exploration of radiated electromagnetic immunity of integrated circuits up to 40 GHz, *Electron. Lett.* 47 (2011) 589–590.
- [11] J.D. Jackson, *Electrodynamics* Wiley, 1975.
- [12] H. Baudrand, et al., Study of radiating properties of open-ended rectangular waveguides, *IEEE Trans. Antennas Propag.* 36 (1988) 1071–1077.
- [13] D. Mansson, et al., Vulnerability of European rail traffic management system to radiated intentional EMI, *IEEE Trans. Electromagn. Compat.* vol. 50 (1) (2008) 101–109.
- [14] L. Palisek, L. Suchy, High Power Microwave Effects on Computer Networks, *EMC Europe*, 2011 18–21.
- [15] J.-M. Redouté, M. Steyaert, Current mirror structure insensitive to conducted EMI, *Electron. Lett.* vol. 41 (21) (Oct. 2005) 1145–1146.