Injection directe de puissance par médium EM

F. Poucheret[1,3], K. Tobich[2], M. Lisart[2], B. Robisson[3], P. Maurine[1]

[1]LIRMM Montpellier

[2]ST Microelectronics Rousset

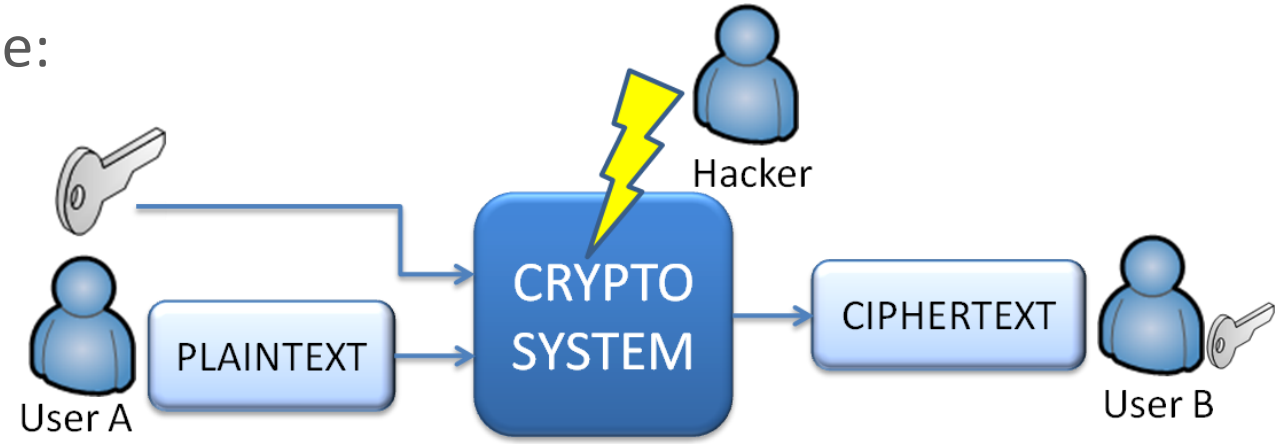
[3]CEA Gardanne

Plan

- 1/ Attaques en fautes
  - Contexte actuel.
  - Problématiques liées à l'EM.
- 2/ Travaux réalisés
  - Couplage EM dans les circuits intégrés.
  - Perturbations d'un circuit CMOS.
- 3/ Conclusion
  - Travaux actuels et perspectives.

ATTAQUES EN FAUTES: CONTEXTE ACTUEL

- Principe:



- **Perturber le calcul cryptographique afin d'en retirer de l'information.**
- Spécificités:
  - Très efficace sur CI non protégé.
  - Comportement imprévisible.
  - Difficile de s'en prémunir.

Moyens d'attaques et de protections

- Limites de fonctionnement.
- Impulsion sur alimentation.
- Front parasite sur horloge.
- Laser.
- **Attaques EM???**

Problématiques

Potentiel des attaques EM:

- *Propriétés de pénétration des ondes.*
- *Difficulté de détection.*
- *Peu d'échantillons, équipement abordable.*

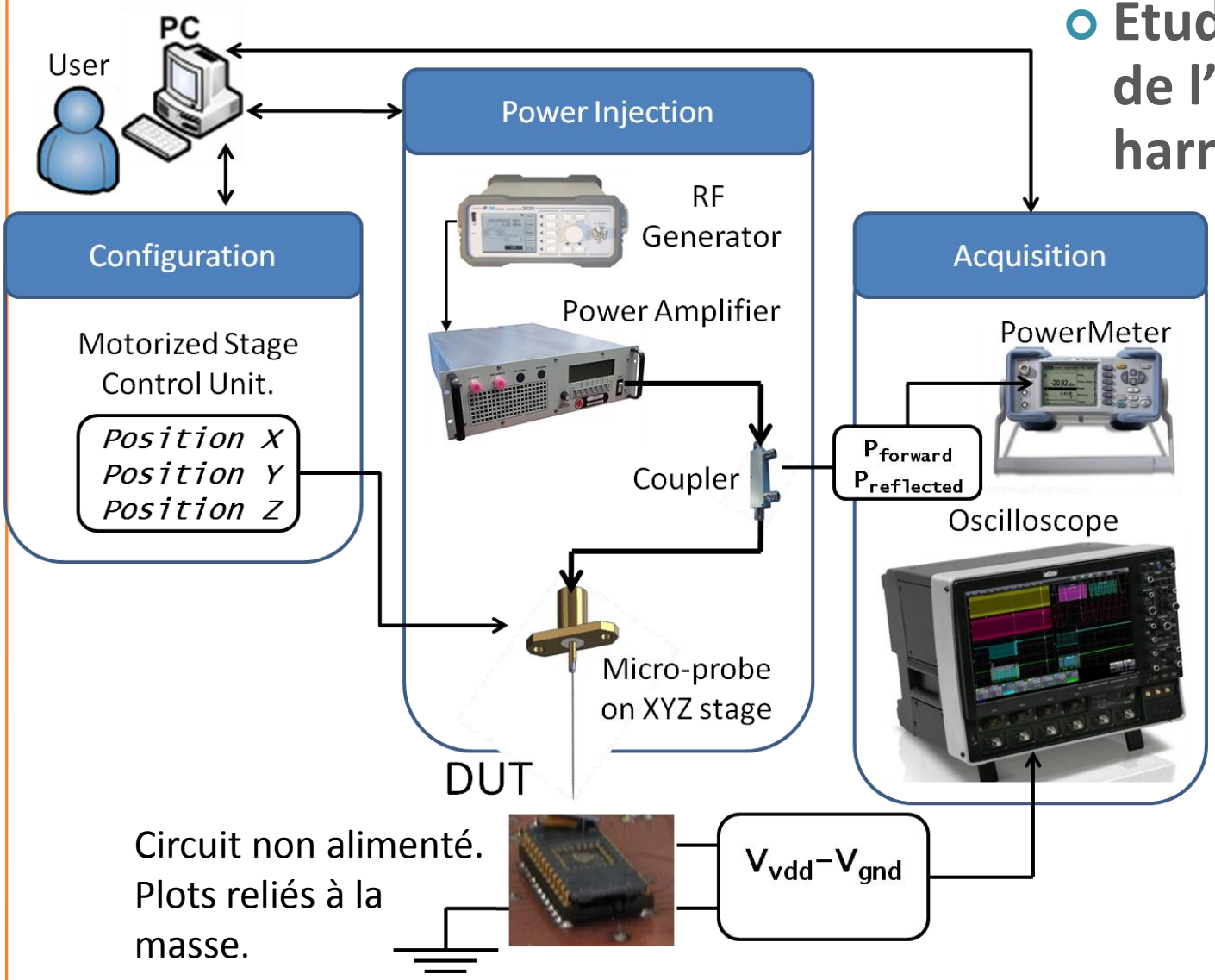
Etude de faisabilité des attaques EM.

- *Est-il possible de créer un couplage EM **local** dans un circuit CMOS ?*
  - Couplage EM sur ASIC 350nm.
- *Est il possible de perturber **à distance** un circuit CMOS?*
  - Perturbations d'un oscillateur en anneau 90nm.

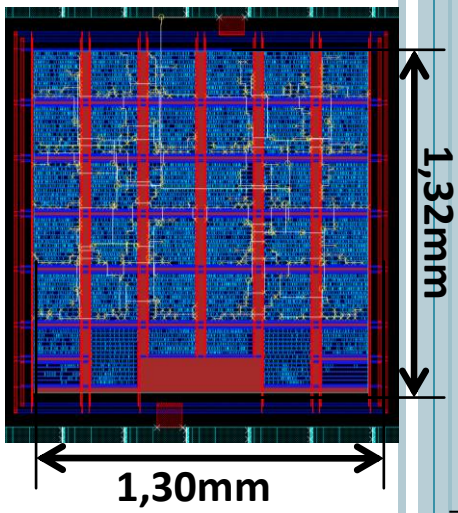
Couplage EM sur ASIC 350nm

MANIPULATION

- **Etude de l'impact de l'injection EM harmonique.**

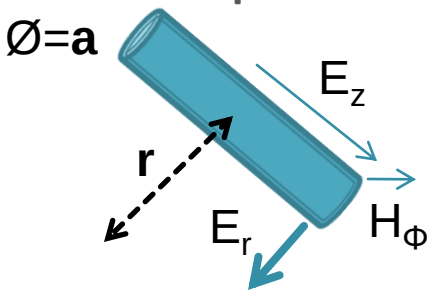


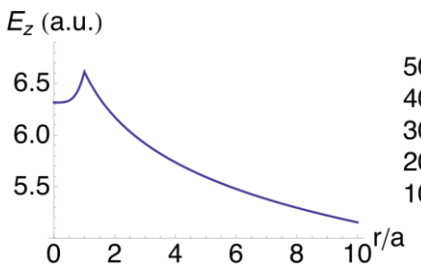
Techno c35b4
Metal1 enterré

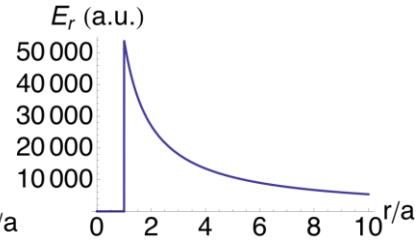


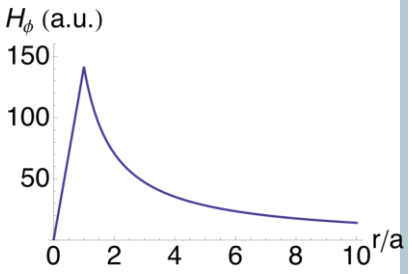
Modèle physique de l'injection EM

- Composantes EM (sonde cylindrique):

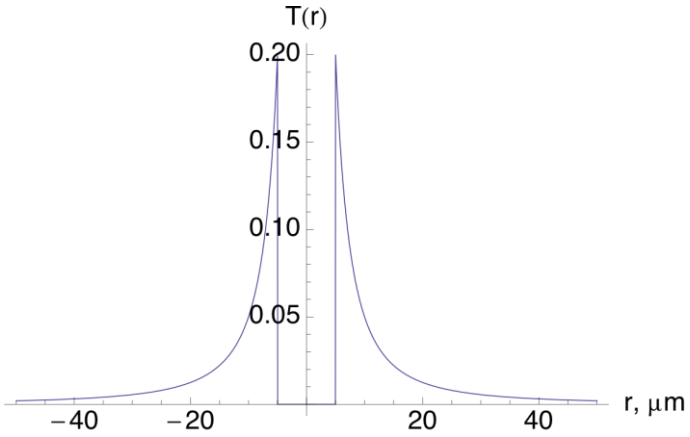


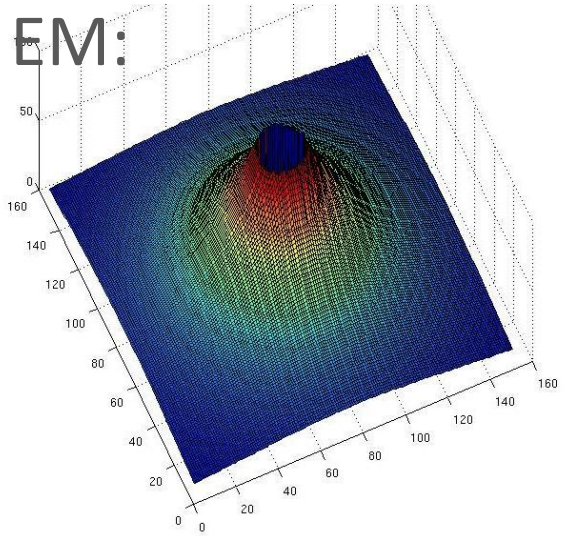






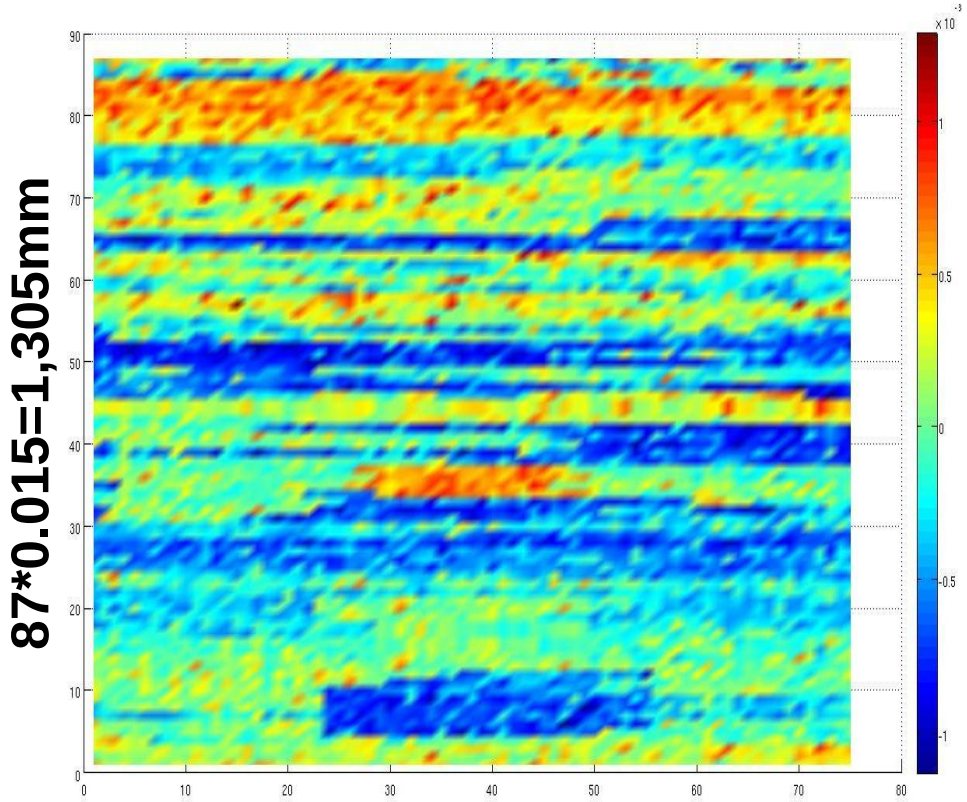
- Modélisation de l'illumination EM:





- 90% de la puissance concentrée dans un anneau Øint. 2*a et Øext. 5*a.
- Couplage électrique local.

Résultats Cartographie ASIC 350nm



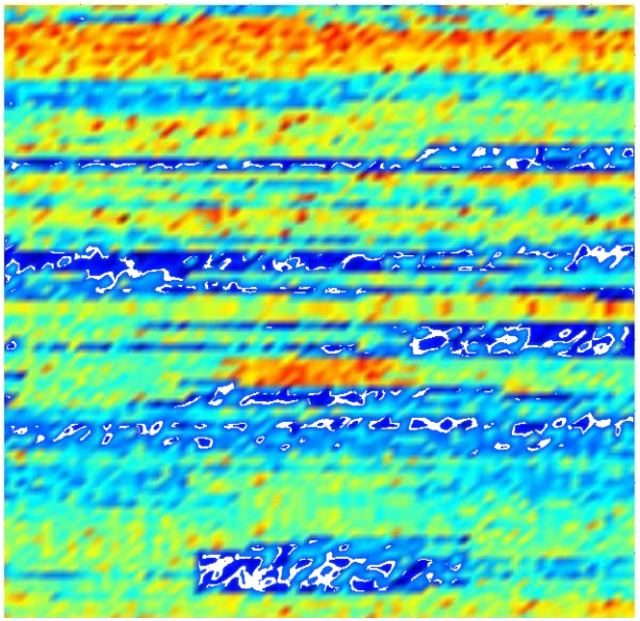
- **Paramètres:**
  - Injection harmonique.
  - Fréquence fixée 1GHz.
  - $P_{forward}$= 3dBm (=2mW).
  - Déplacement 15µm.
- Critère d'analyse:
  - **Valeur moyenne $V_{(vdd-gnd)}$.**
  - *Max, Min, FFT…*

Comparaison directe

- Extraction du MET1:

Met1

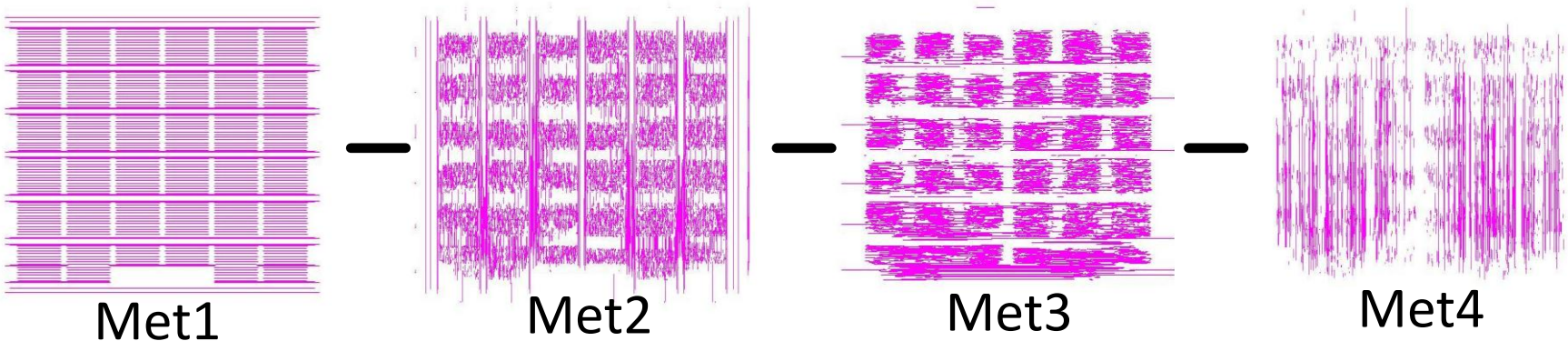
Cartographie



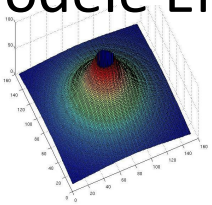
- Corrélation avec le réseau d'alimentation du MET1 loin d'être évidente (4%).
- Caractère local de l'injection EM.

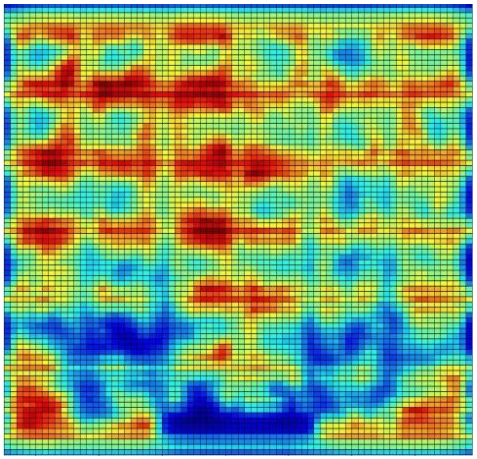
Illumination EM sur le circuit

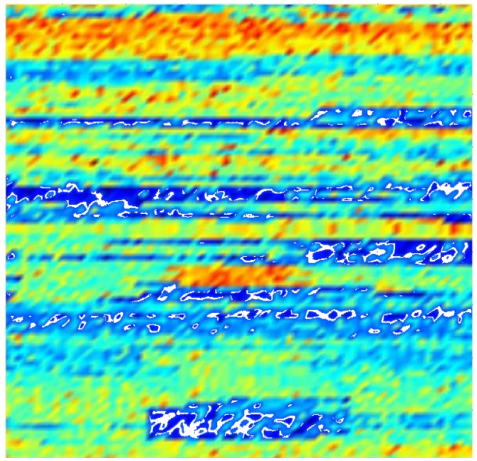
- Influence des couches supérieures (bouclier)



Modèle EM







Corrélation 2-D=35%.

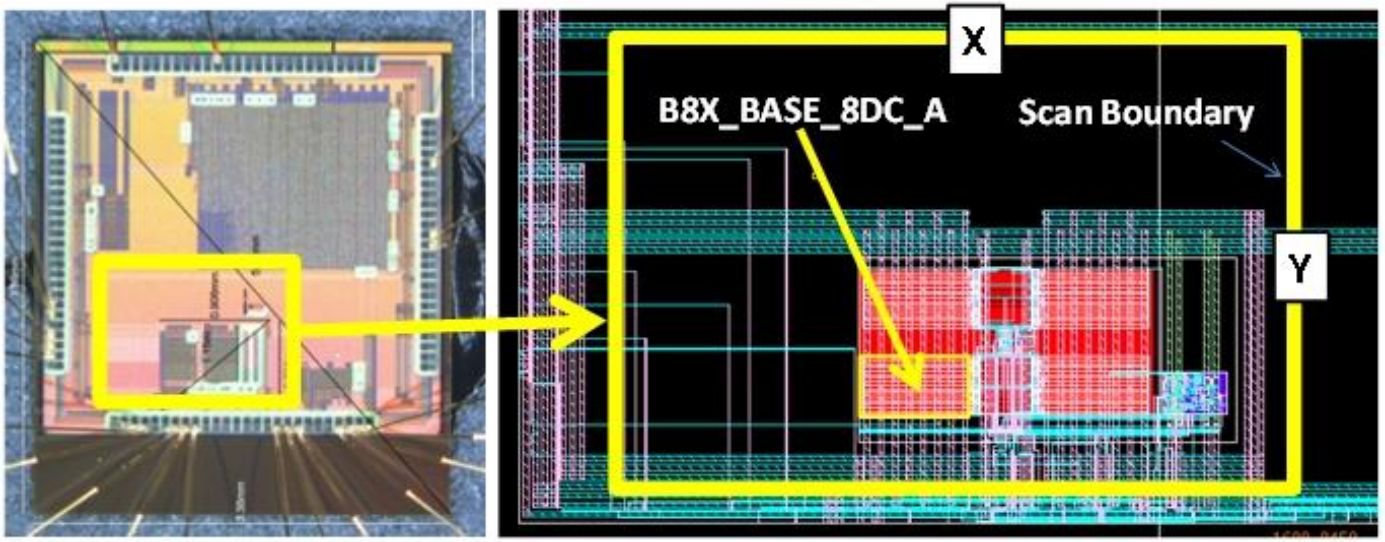
Résumé Couplage EM

- Couplage Electrique **local** avec le réseau d'alimentation d'un circuit (même enterré).
- Dépend:
  - Du circuit et de ses motifs.
  - Du type de sonde et son positionnement.
  - De chacun des éléments de la chaîne d'injection.
  - De la puissance injectée et de la fréquence d'injection.

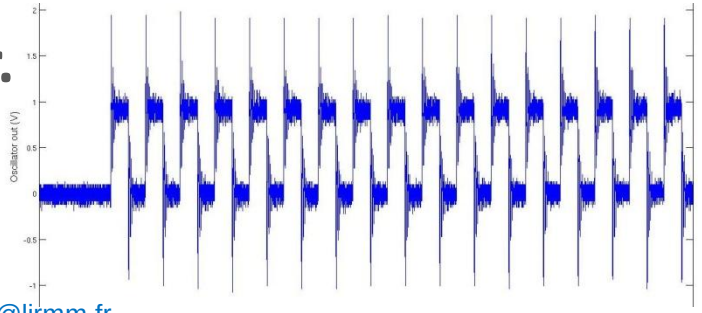
Perturbations d'un Oscillateur en Anneau par Injection EM

Cible: Oscillateur en Anneau

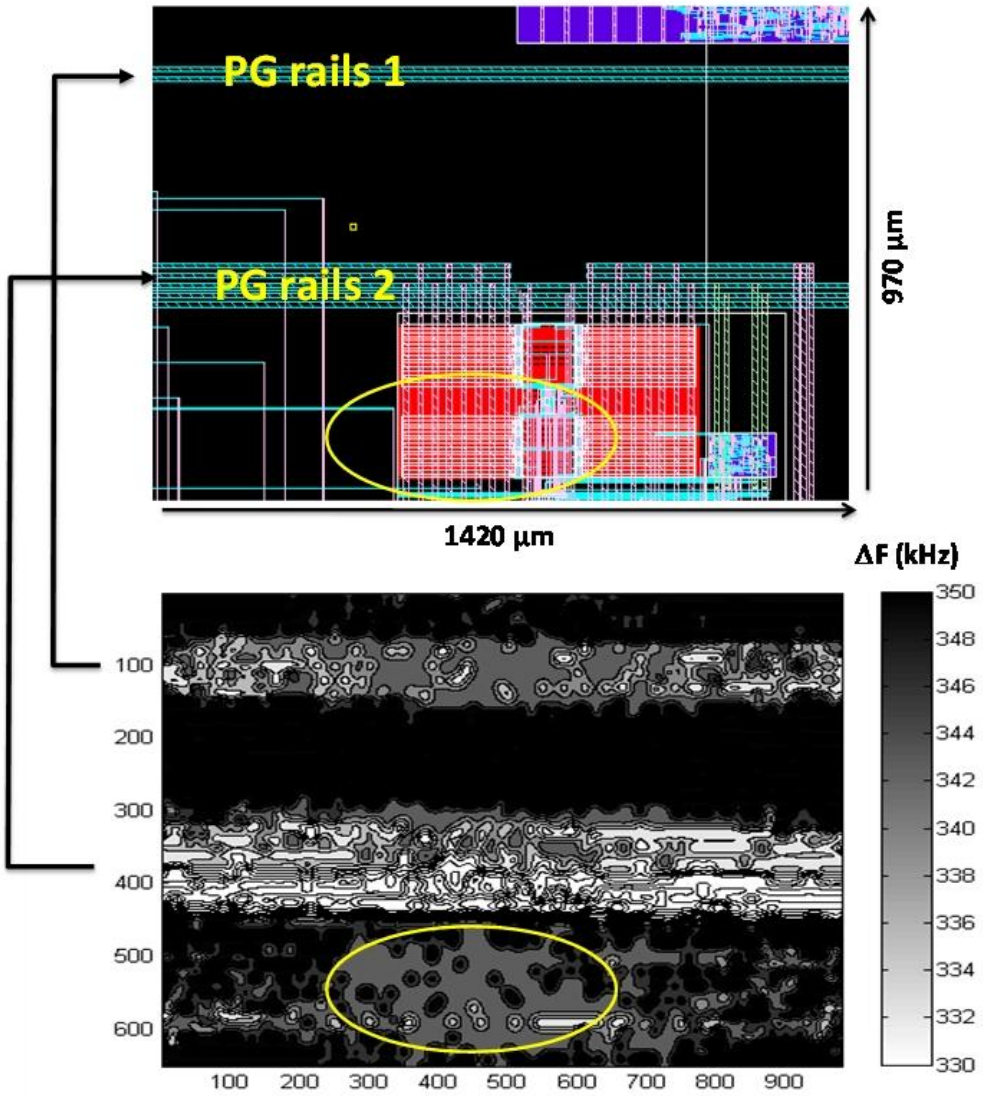
- **Choix d'un oscillateur en anneau:**
  - Caractérisation de la logique CMOS.
  - Générateurs de nombres aléatoires, générateurs internes d'horloge.



- **101 inverseurs rebouclés + compteur.**
- **Sortie Fout=3,81MHz.**

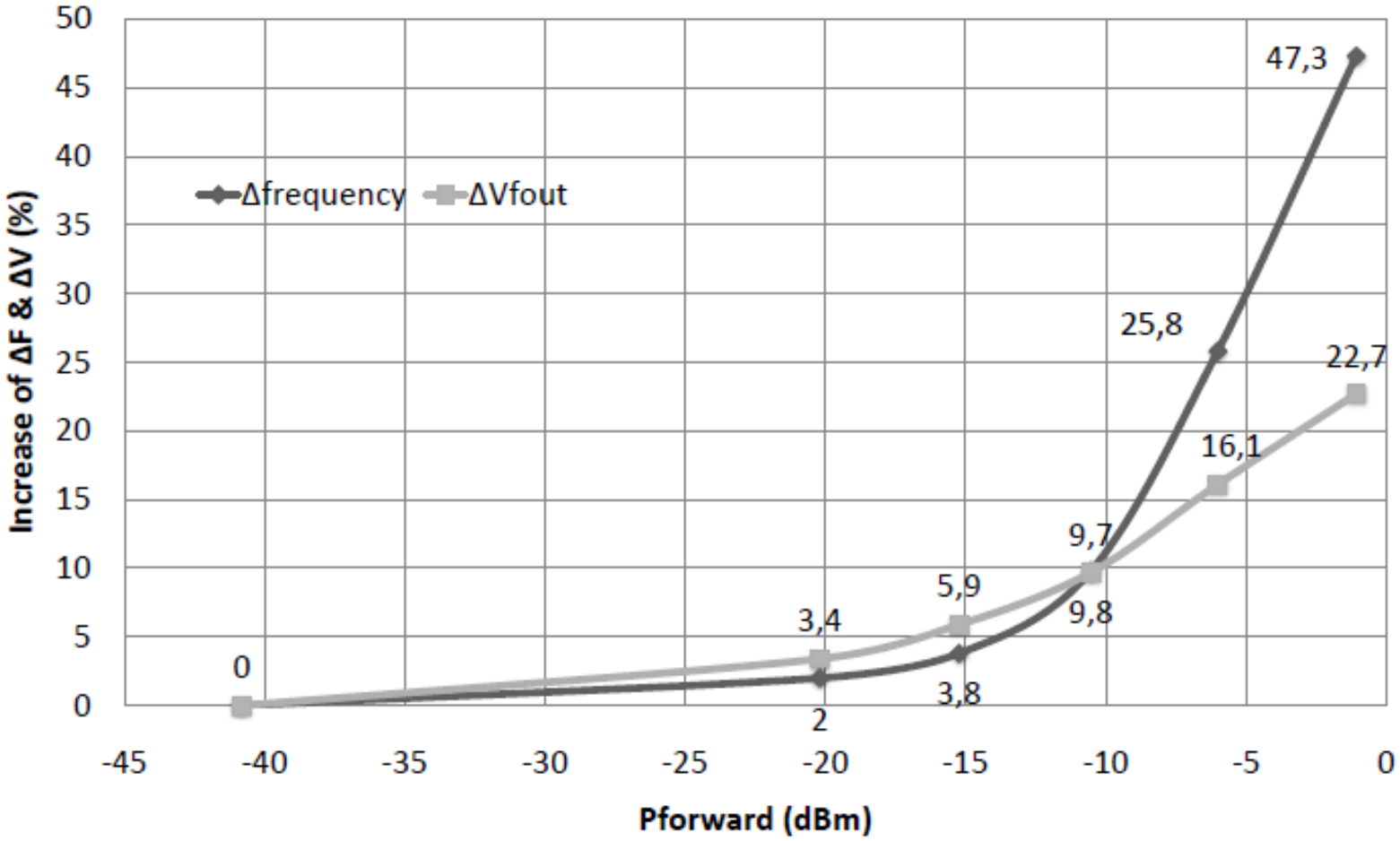


CARTOGRAPHIE ΔF SUR CI DÉPACKAGÉ



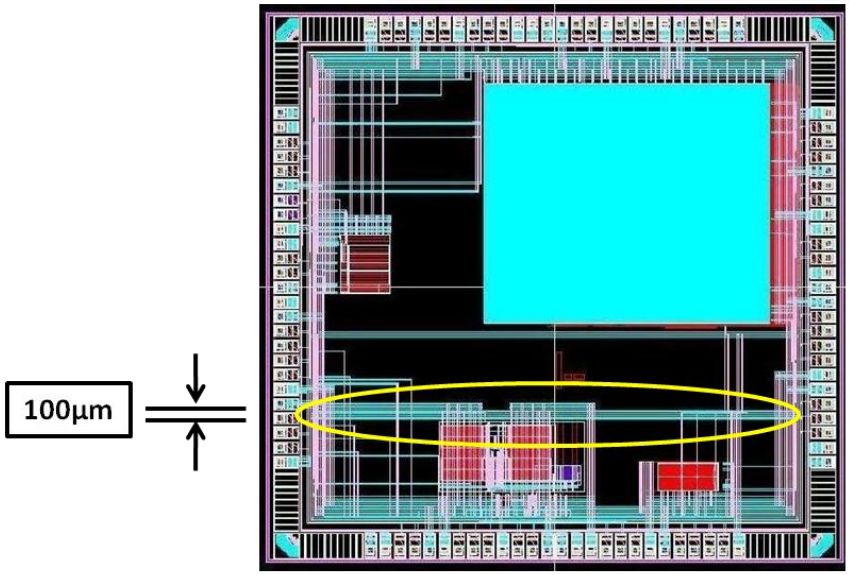
- **Paramètres:**
  - Injection harmonique.
  - Sinus 1GHz.
  - $P_{forward}$ = -10.53dBm (≈0,1mW).
  - Distance sonde/CI = 50µm.
- Augmentation globale de la fréquence de 350kHz (9.2%).
- Variations locales 310-380kHz sur certaines zones.

Evolution Fréquence et Amplitude sur CI Dépackagé

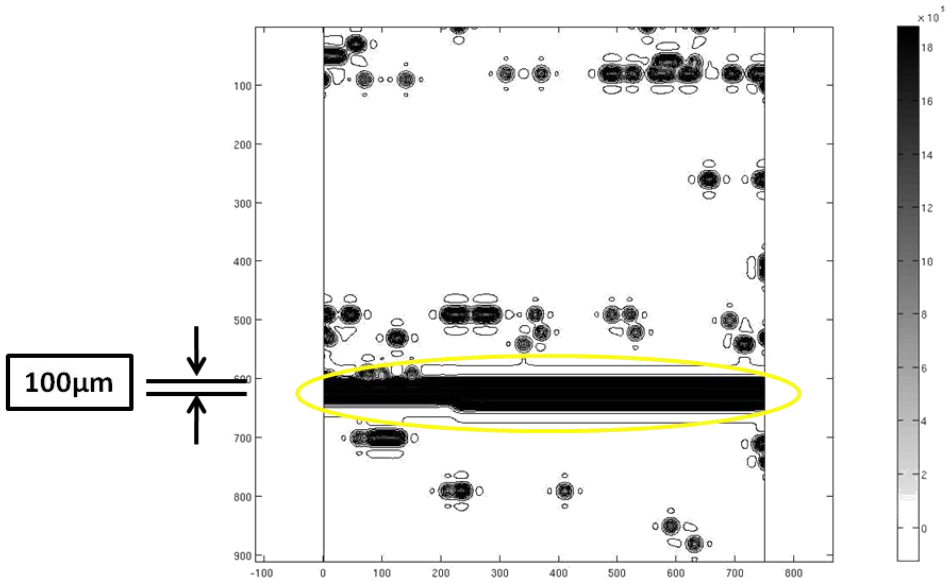


- Proportionnelle à $P_{forward}$.
- Augmentation de V_{dd} moyen par apport direct d'énergie.

Cartographie ΔF sur CI packagé



- **Paramètres:**
  - Injection harmonique.
  - Sinus 1GHz.
  - $P_{forward}$ = 8.22dBm. (≈6,63mW).
  - Distance sonde/CI = 2mm.



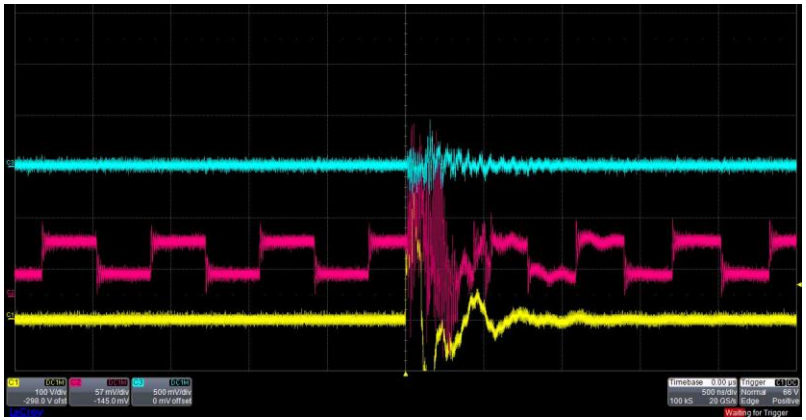
- Augmentation locale de 1.8 MHz (46,6%).
- Détection de motifs (largeur≈100µm).
- À travers package et à 2mm de distance.

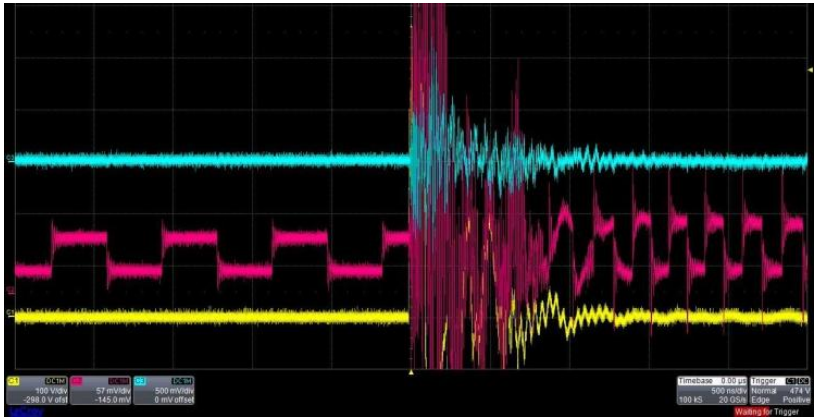
Résumé Perturbation EM sur CI

- **Injection EM harmonique sur circuits CMOS:**
  - Apport direct d'énergie au circuit.
  - Augmentation de V_{dd} moyen.
  - Sans contact et à plusieurs mm de distance.
  - Motif ciblé 100µm (dépend du couplage).
  - Attaques en limites de fonctionnement?
    - Sans préparation du circuit.
    - Contournement de certaines protections?

Conclusion & Perspectives

- **Injection EM harmonique:**
  - Validation sur structure type TRNG, générateur d'horloge.
  - Utilisation de sondes « cheveu » Ø=1µm.
  - Fréquences plus élevées.
- **Développement d'une plateforme d'Impulsion EM:**
  - Nouvelles sondes.
  - Etude des propriétés d'injection EM Impulsionnelle.





Merci de votre attention.
Questions?