Cartographie Électromagnétique pour la Cryptanalyse Physique

Laurent Sauvage

Institut TELECOM / TELECOM-ParisTech
CNRS – LTCI (UMR 5141)

Journée Sécurité du GdR SoC-SiP – Mercredi, 18 mai 2011

Sommaire

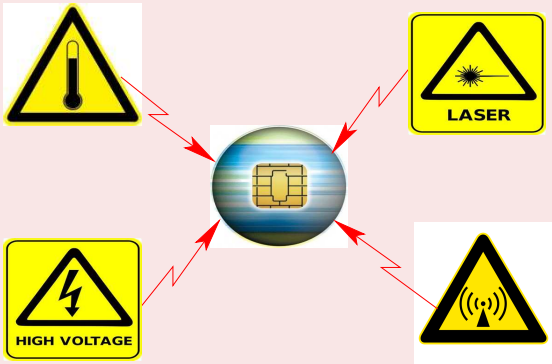
Sommaire

Des Systèmes Embarqués Omniprésents...

- iPad
- Smart Phones
- Cartes bancaires
- Télévision à péage
- Passe Navigo
- Téléphone portable chiffrant
- Drone militaire

...et Leurs Applications Cryptographiques Menacées.

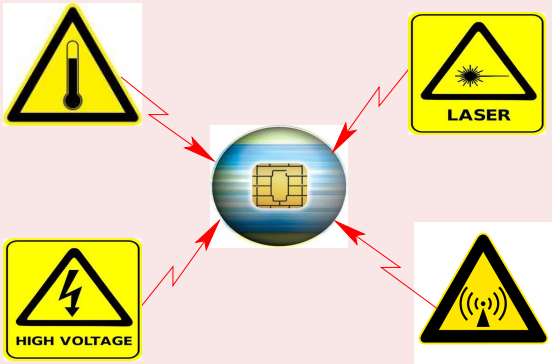
Attaques par Injection de Fautes



- Variation de la tension, fréquence, température
- Tir Laser
- Décharges électrostatiques

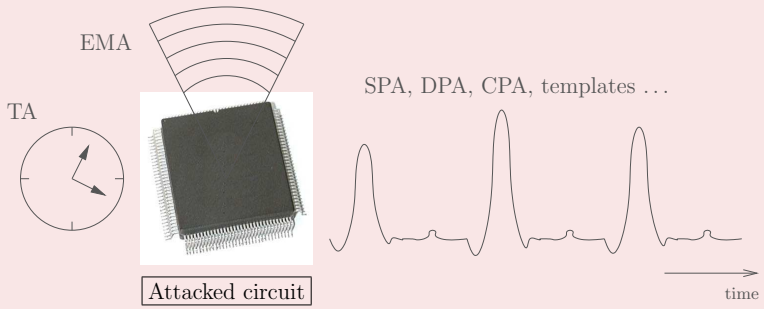
...et Leurs Applications Cryptographiques Menacées.

Attaques par Injection de Fautes



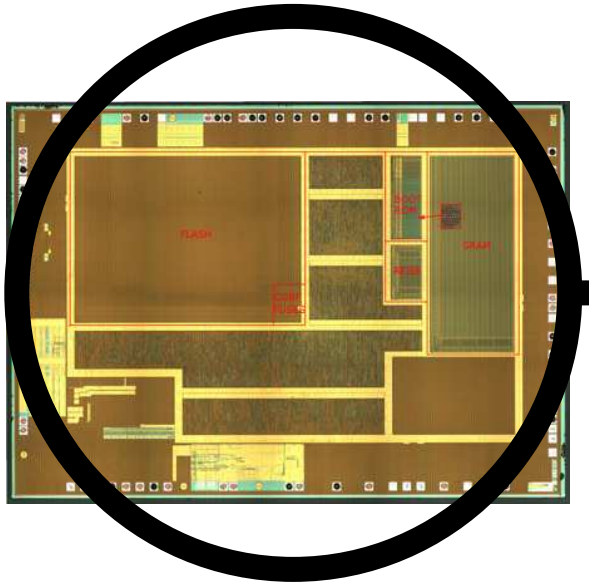
- Variation de la tension, fréquence, température
- Tir Laser
- Décharges électrostatiques

Attaques par Canal Auxiliaire



- Durée des opérations
- Consommation en courant
- Radiations électromagnétiques

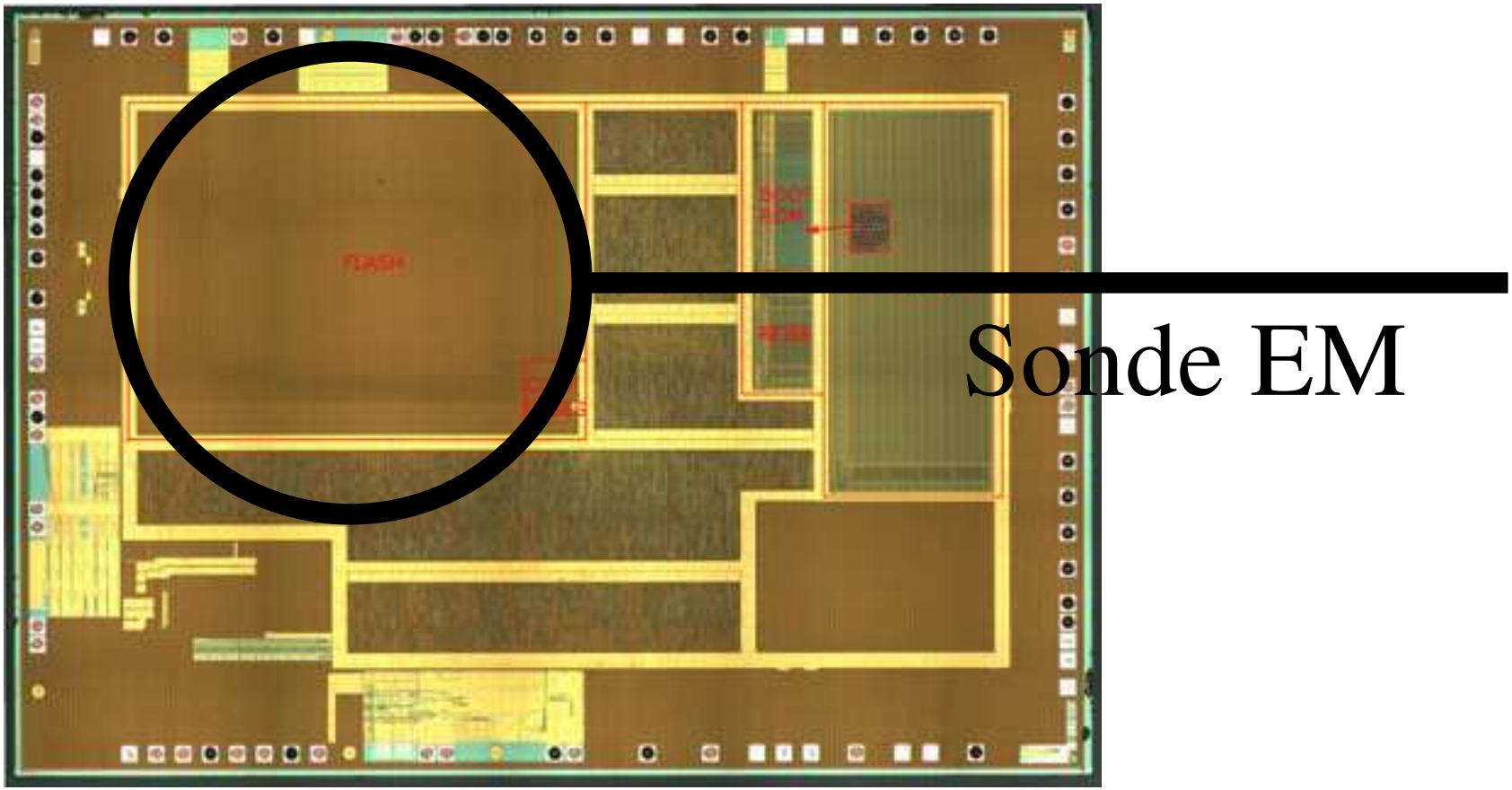
Globalité vs Localité



Sonde EM

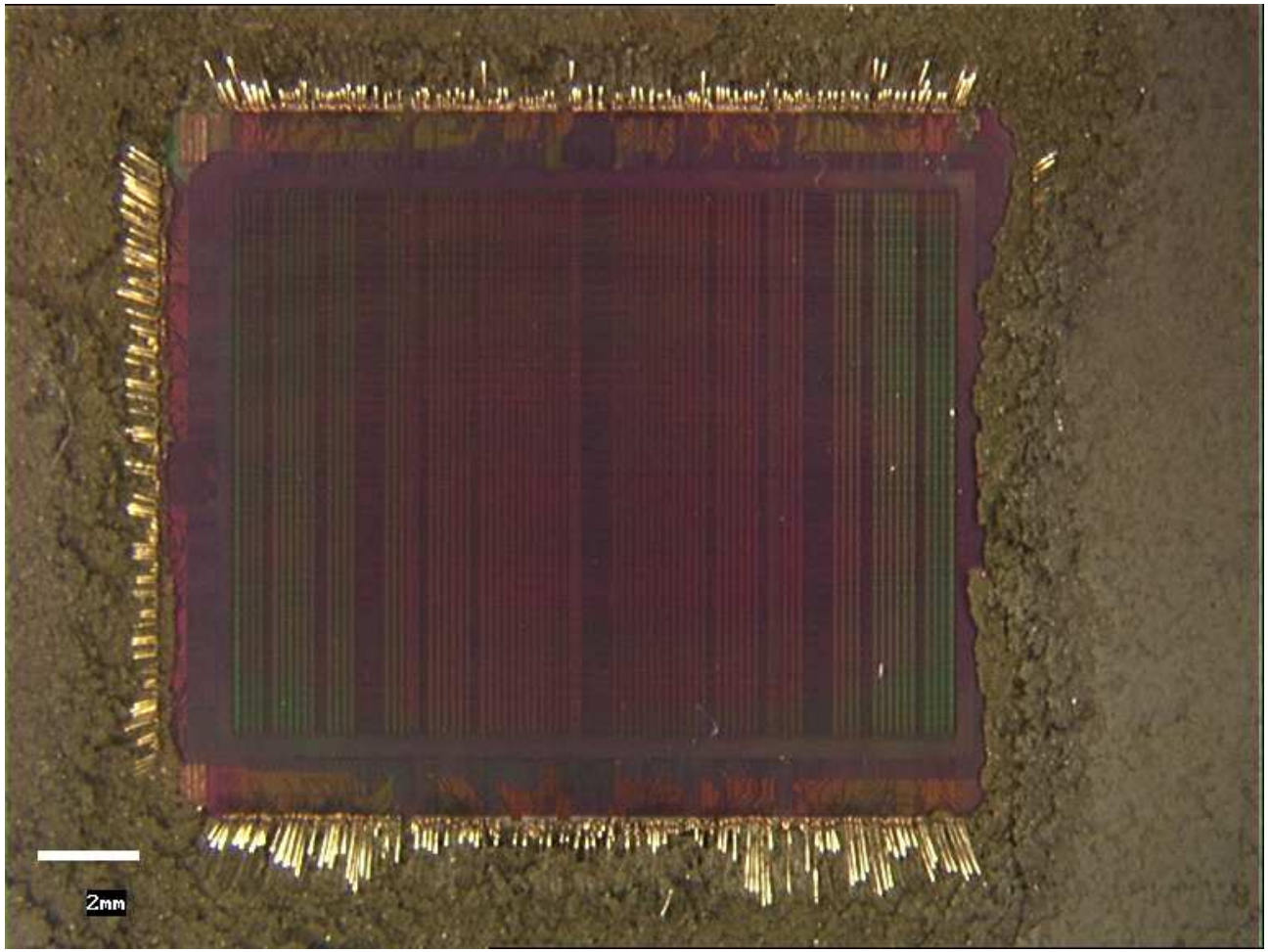
Mesure **globale** du rayonnement EM.

Globalité vs Localité



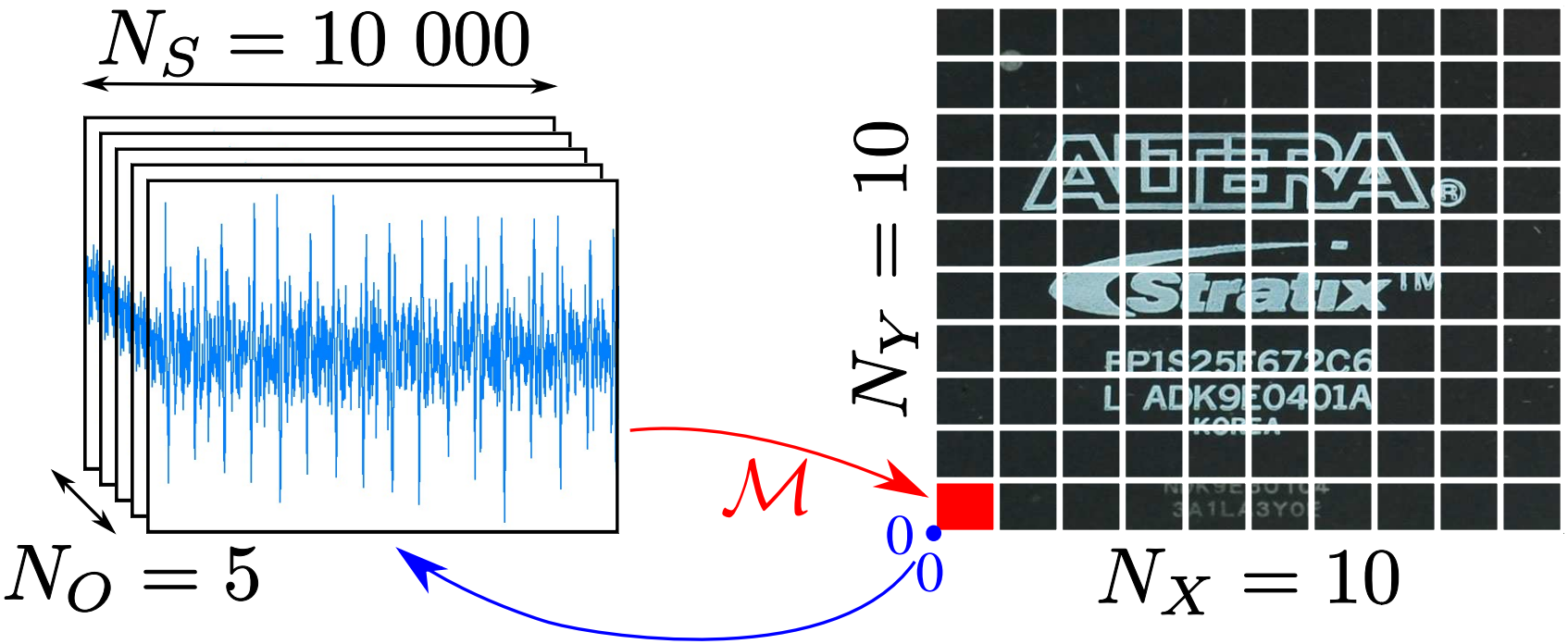
Mesure **locale** du rayonnement EM.

Des Méthodes de Localisation Nécessaires



FPGA Stratix décapsulé à l'aide de produits chimiques.

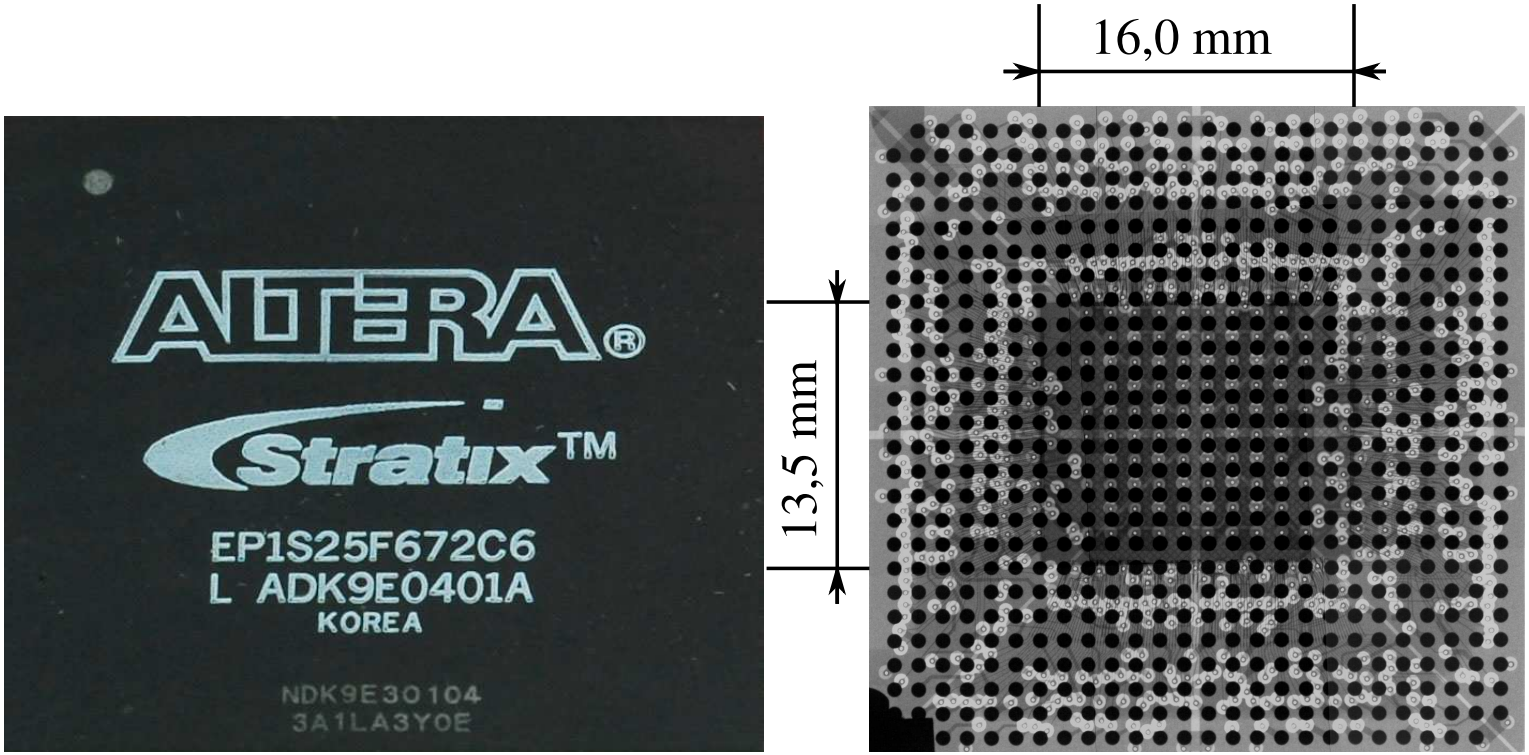
Principe de la Cartographie



En chacune des $N_P = N_X \times N_Y$ positions (x, y), N_O observations $O^o_{(x,y)}$ de N_S échantillons temporels n sont réalisées.

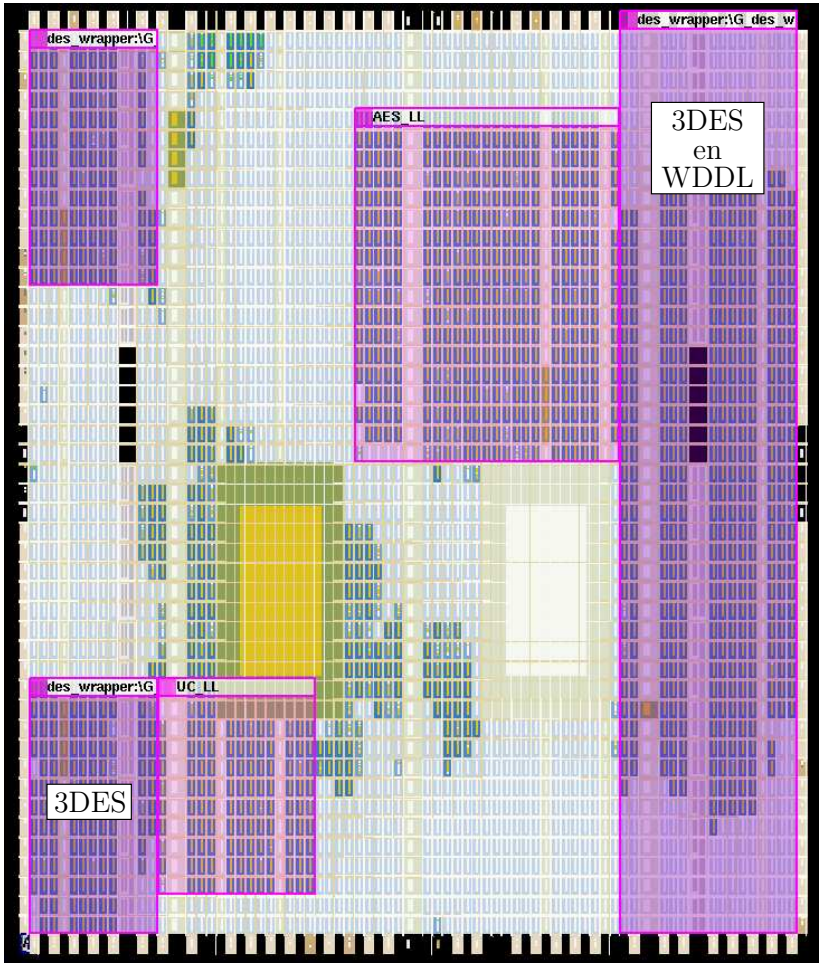
Sommaire

Photographie aux rayons X du boîtier du FPGA ALTERA Stratix EP1S25

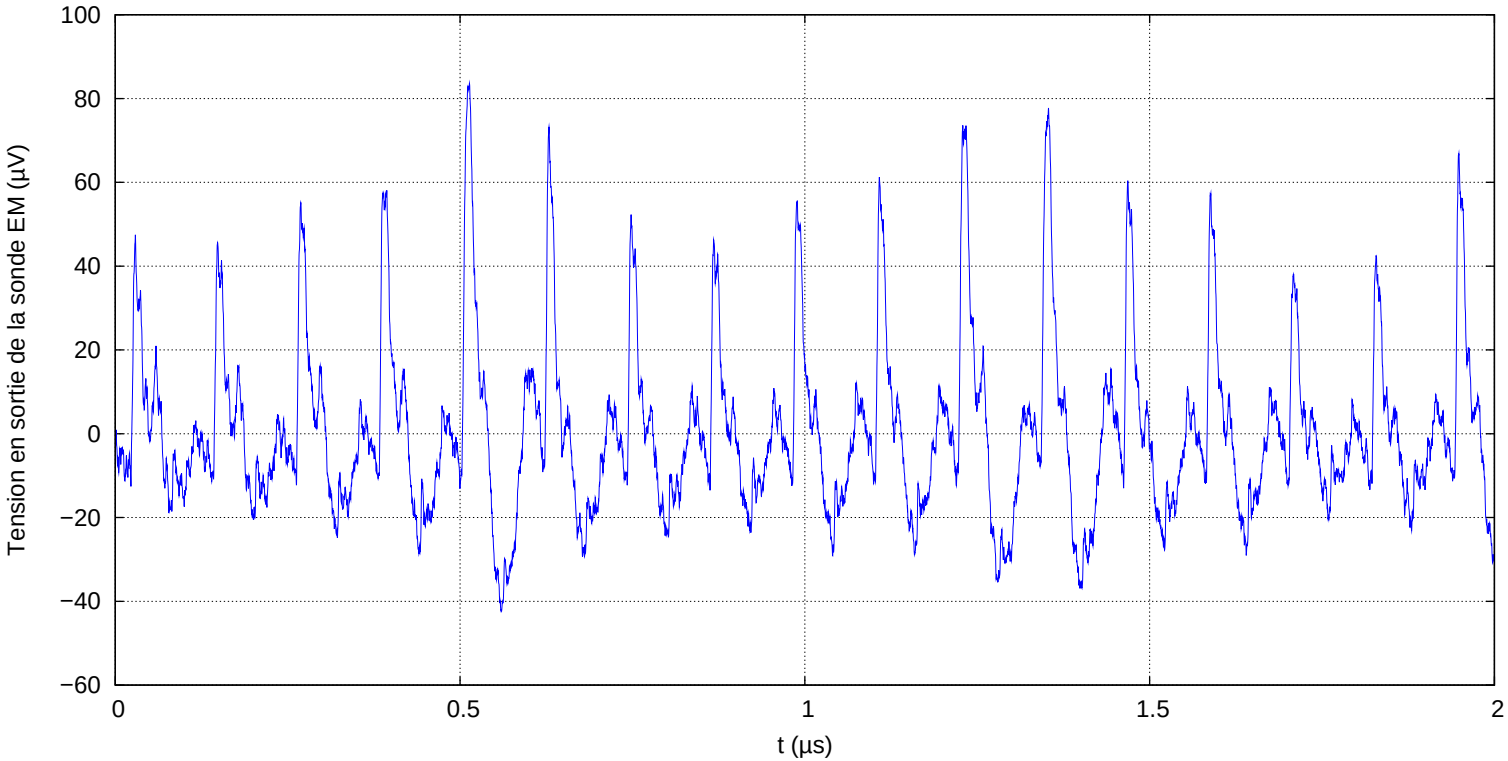


1 LAB est large de 205 μm, haut de 290 μm.

Floorplan du SoPC EveSoc programmé dans un Stratix



Attaque par EMA Globale

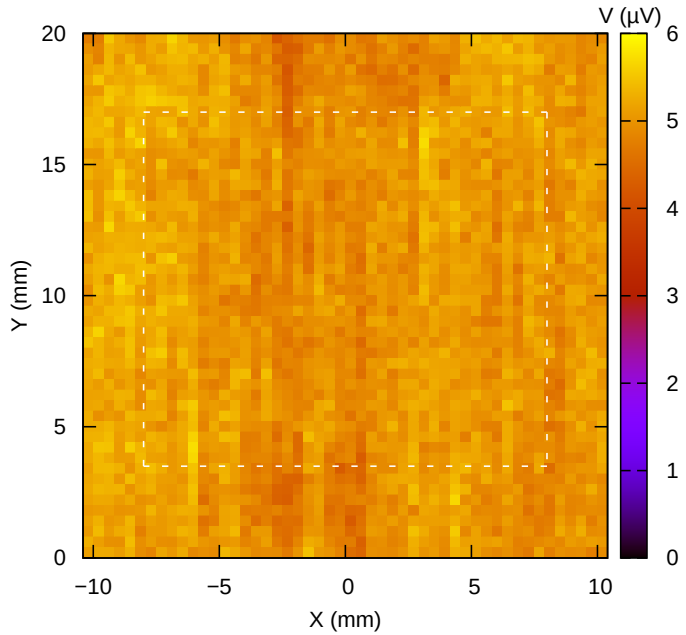


Trace des radiations EM au-dessus d'un condensateur de découplage.

Cartographie EM dans le Domaine Temporel

Valeur Moyenne

$$\begin{aligned} \mathcal{M} : \quad \mathbb{R}^{N_S} &\rightarrow \mathbb{R} \\ O^0_{(x,y)} &\mapsto \frac{1}{N_S} \sum_{n=0}^{N_S-1} O^0_{(x,y)}(n) \end{aligned}$$

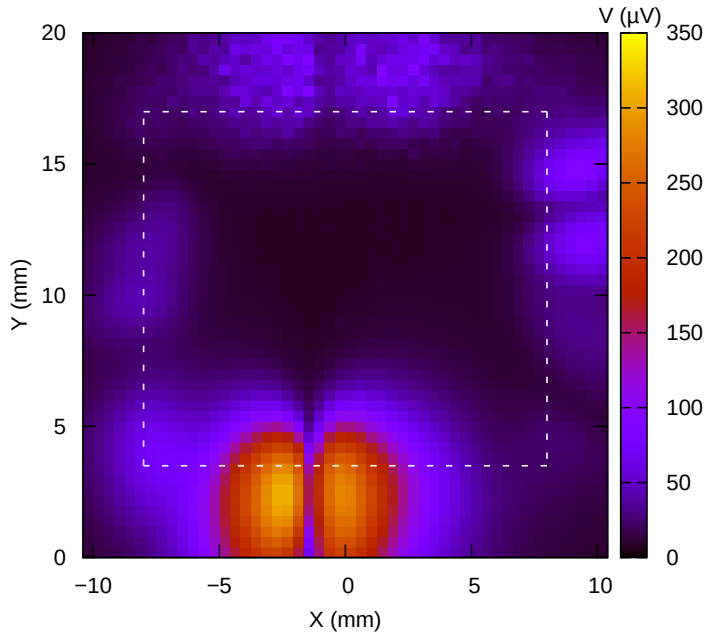


Composante continue non mesurée car la bande passante s'étend de 100 kHz à 3 GHz.

Cartographie EM dans le Domaine Temporel

Valeur Efficace (Moyenne Quadratique)

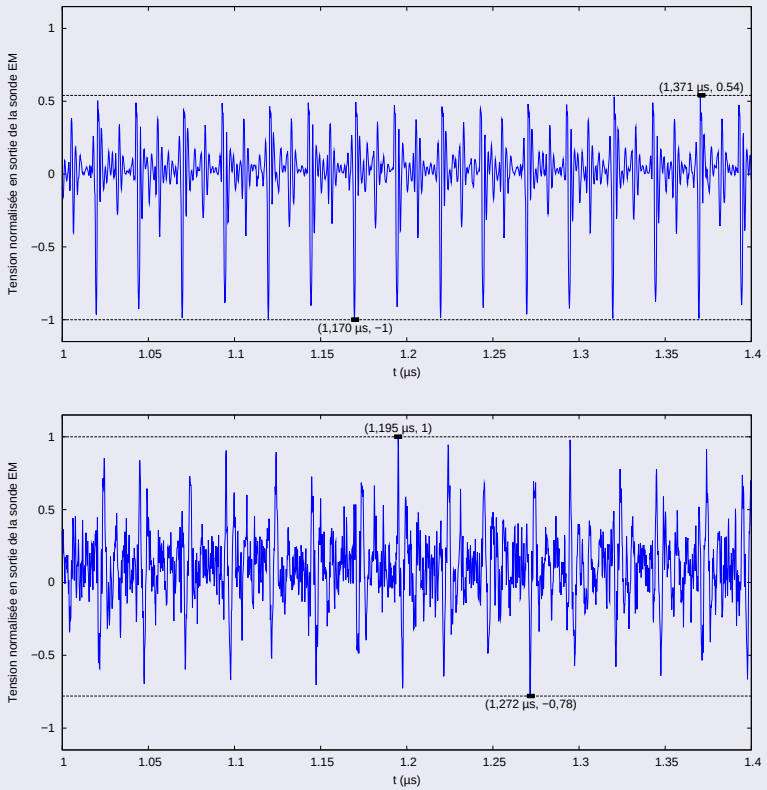
$$\begin{aligned} \mathcal{M} : \quad \mathbb{R}^{N_S} &\rightarrow \mathbb{R} \\ O^0_{(x,y)} &\mapsto \sqrt{\frac{1}{N_S} \sum_{n=0}^{N_S-1} O^0_{(x,y)}(n)^2} \end{aligned}$$



Perte de l'information sur la polarité du champ EM.

Cartographie EM dans le Domaine Temporel

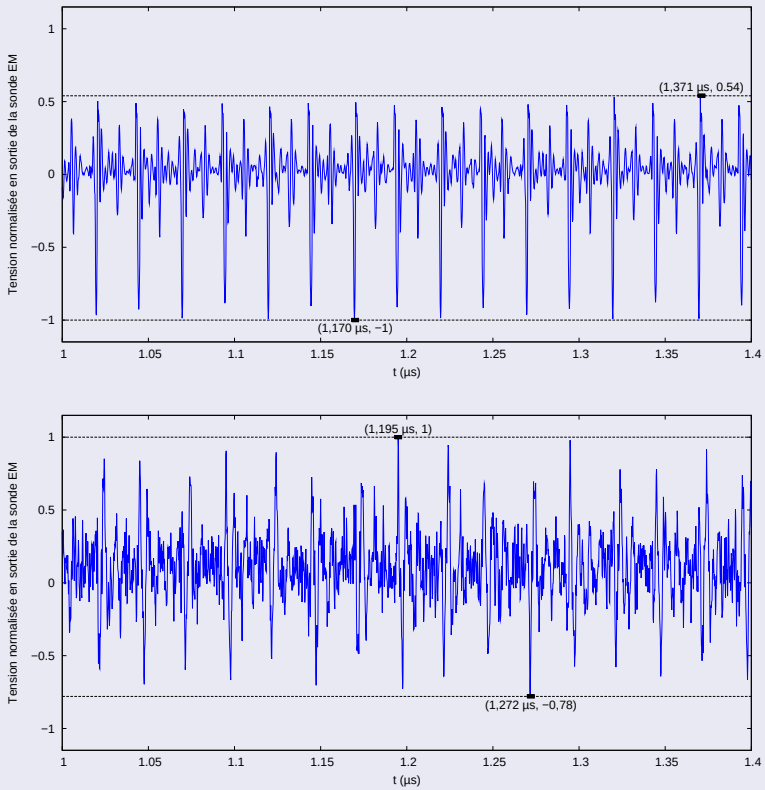
Champ EM majoritairement négatif (*haut*) et bipolaire (*bas*)



Ces deux observations sont identiques en valeur absolue pour une fonction de recherche de maximum.

Cartographie EM dans le Domaine Temporel

Champ EM majoritairement négatif (*haut*) et bipolaire (*bas*)

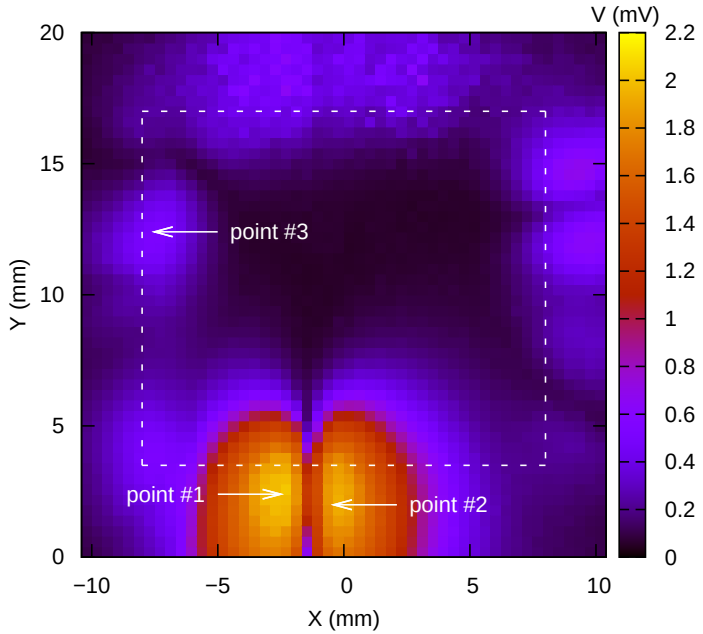


Dynamiques de -0,46 et 1,78 : les valeurs absolues passent d'un écart nul à un écart de 1,32.

Cartographie EM dans le Domaine Temporel

Dynamique du signal EM

$$\begin{array}{rccl} \mathcal{M}: & \mathbb{R}^{N_S} & \rightarrow & \mathbb{R} \\ & O^0_{(x,y)} & \mapsto & \max(O^0_{(x,y)}) - \min(O^0_{(x,y)}) \end{array}$$



Cartographie EM dans le Domaine Temporel

Différence des dynamiques du signal EM

$$\begin{array}{rccl} \mathcal{M}: & \mathbb{R}^{2N_S} & \rightarrow & \mathbb{R} \\ & (O^0_{(x,y)}, O^1_{(x,y)}) & \mapsto & \mathcal{D}(O^1_{(x,y)}) - \mathcal{D}(O^0_{(x,y)}) \end{array}$$

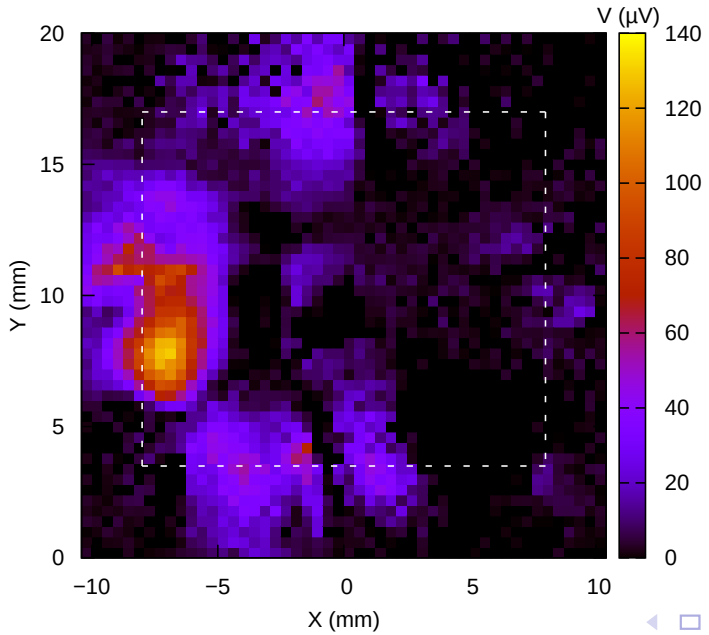
Module inactif durant $O^0_{(x,y)}$, actif durant $O^1_{(x,y)}$.

Cartographie EM dans le Domaine Temporel

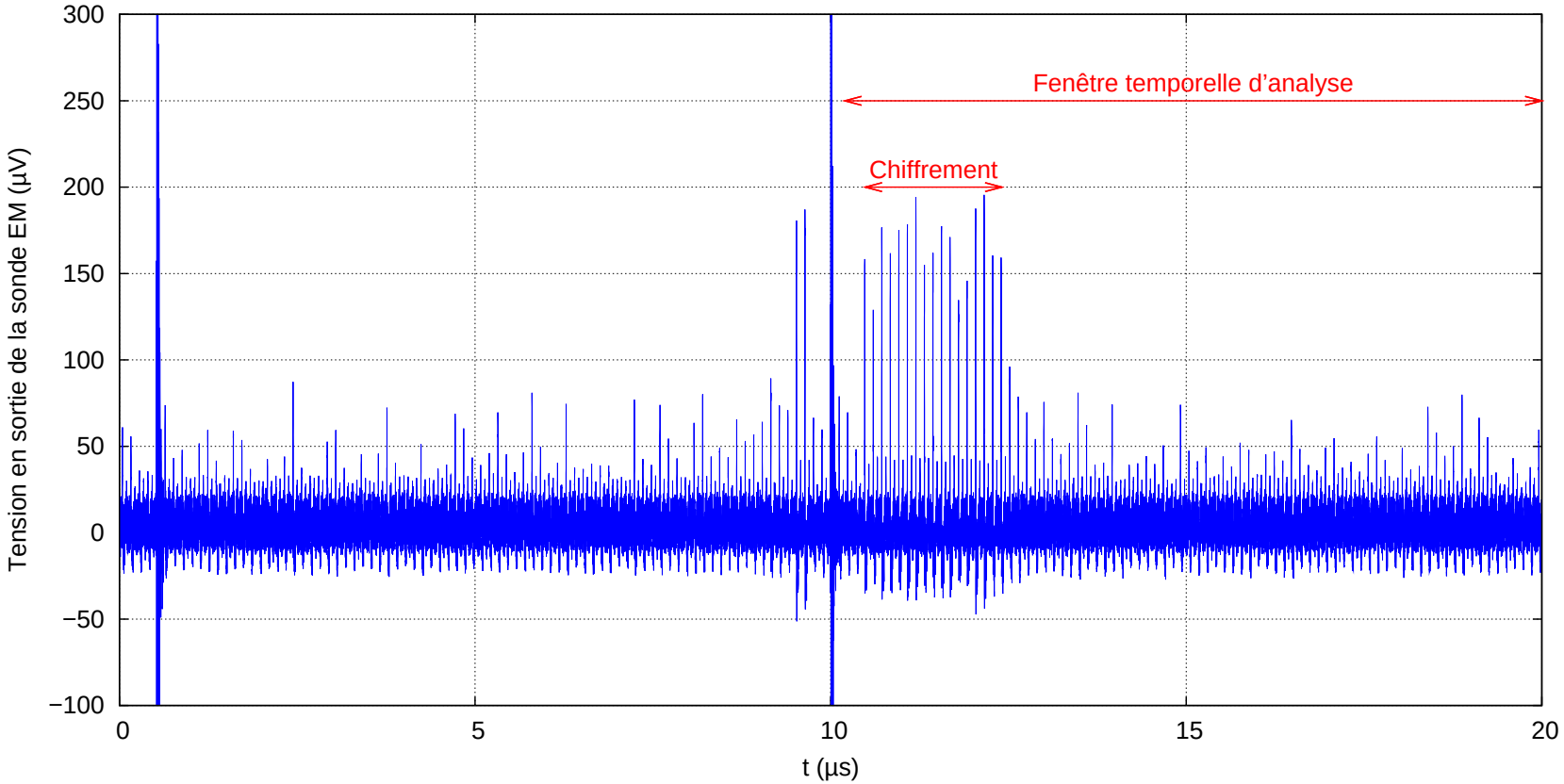
Différence des dynamiques du signal EM

$$\begin{array}{rccl} \mathcal{M}: & \mathbb{R}^{2N_S} & \rightarrow & \mathbb{R} \\ & (O^0_{(x,y)}, O^1_{(x,y)}) & \mapsto & \mathcal{D}(O^1_{(x,y)}) - \mathcal{D}(O^0_{(x,y)}) \end{array}$$

Module inactif durant $O^0_{(x,y)}$, actif durant $O^1_{(x,y)}$.



Cartographie EM dans le Domaine Temporel



Trace complète des radiations EM au-dessus du cryptoprocesseur 3DES non protégé.

Inconvénients

- Le rapport signal à bruit (SNR) de mesure doit être suffisamment grand ;
- Les instants d'activité / repos de la cible doivent être connus.

Inconvénients

- Le rapport signal à bruit (SNR) de mesure doit être suffisamment grand ;
- Les instants d'activité / repos de la cible doivent être connus.

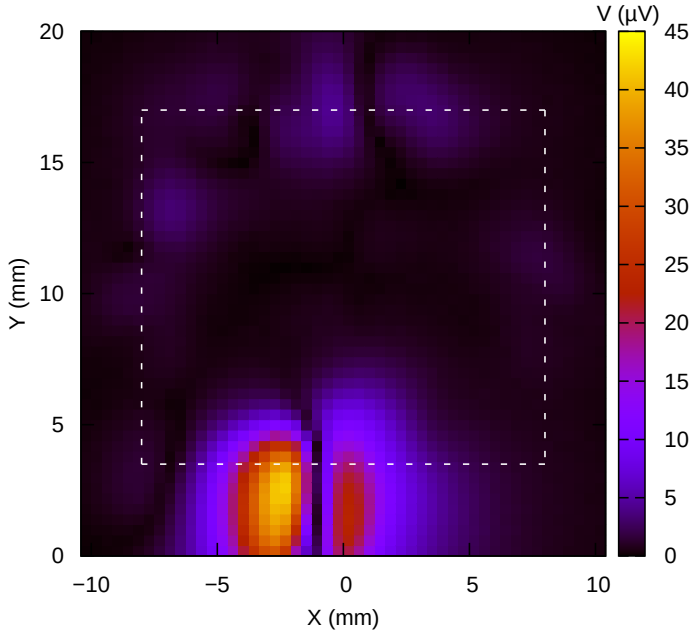
Domaine fréquentiel

- Limitation à une bande de fréquence où le SNR est satisfaisant ;
- Parfaite synchronisation inutile.

Cartographie EM dans le Domaine Fréquentiel

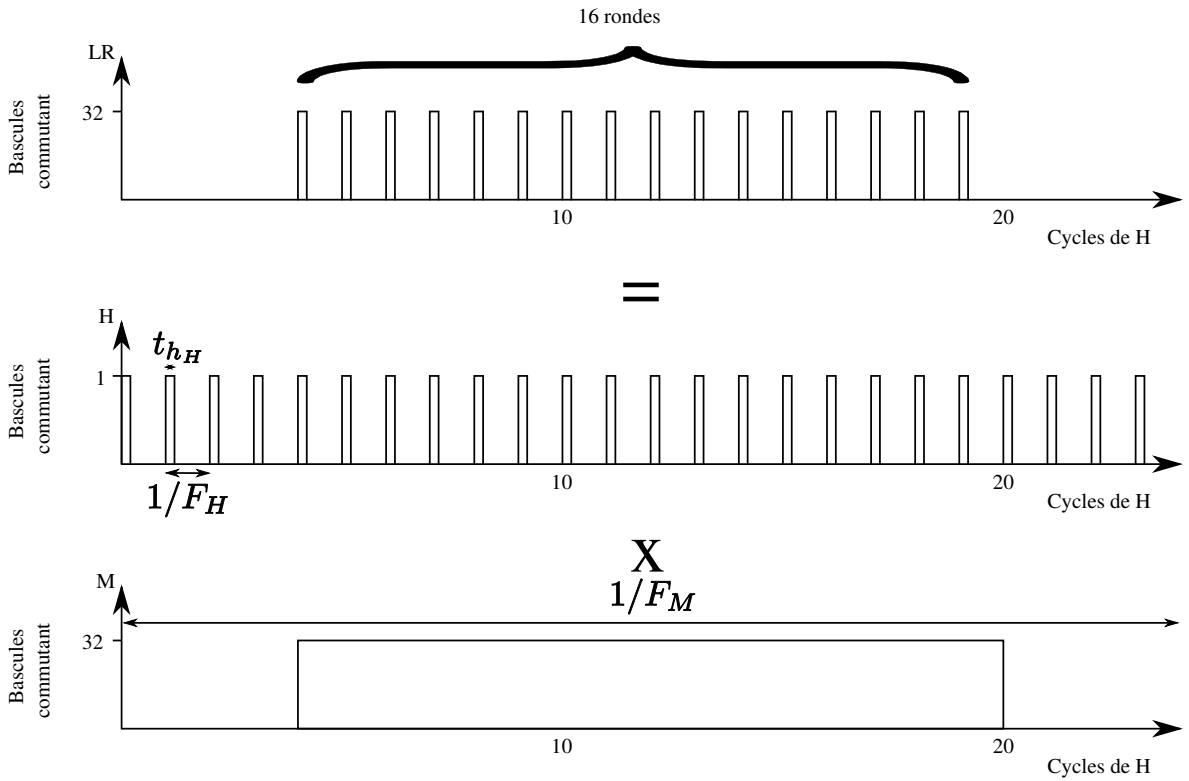
Module de la Transformée de Fourier Discrète

$$\begin{array}{rccl} \mathcal{M} : & \mathbb{R}^{N_S} & \rightarrow & \mathbb{R} \\ & O^0_{(x,y)} & \mapsto & \left| \sum_{n=0}^{N_S-1} O^0_{(x,y)}(n) \cdot e^{-2i\pi k \frac{n}{N_S}} \right| \end{array}$$



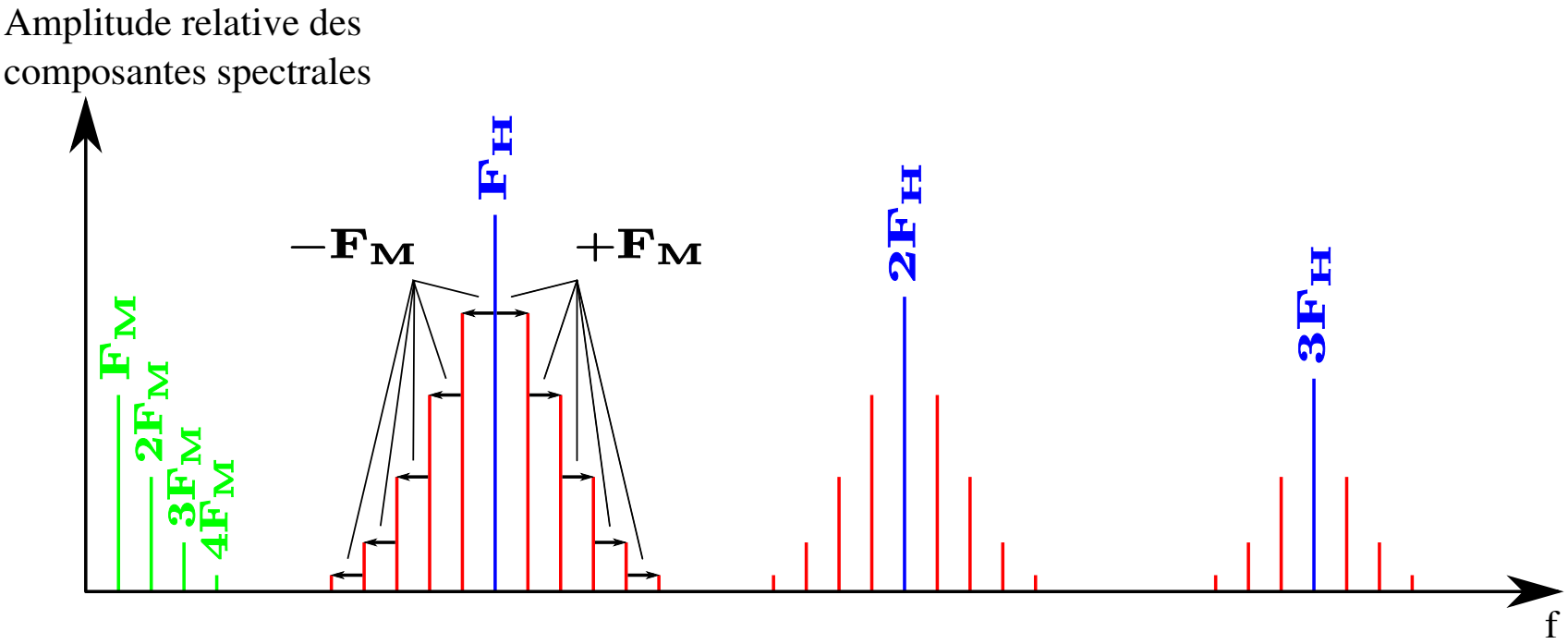
Composante à 20 MHz (k=2097), module de test en position NO.

Cartographie EM dans le Domaine Fréquentiel



Décomposition de l'activité du module 3DES en le produit algébrique de deux autres activités.

Cartographie EM dans le Domaine Fréquentiel

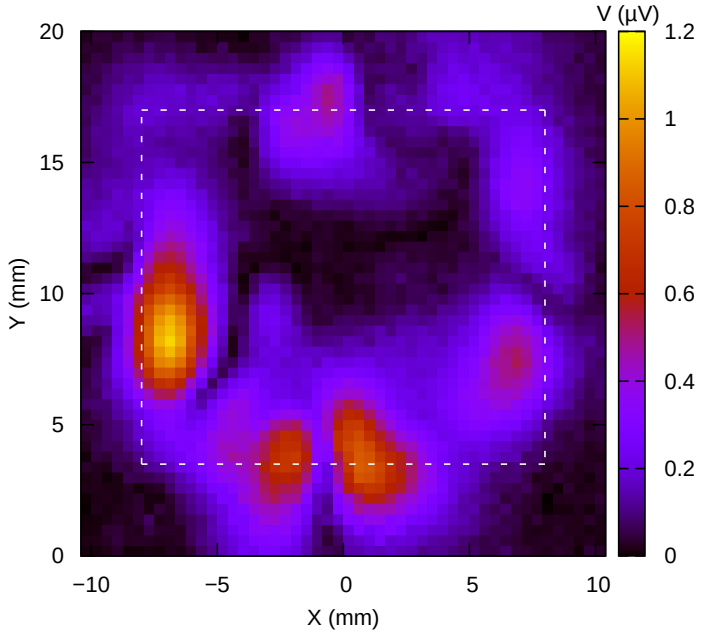


Spectre fréquentiel d'un signal modulé en amplitude.

Cartographie EM dans le Domaine Fréquentiel

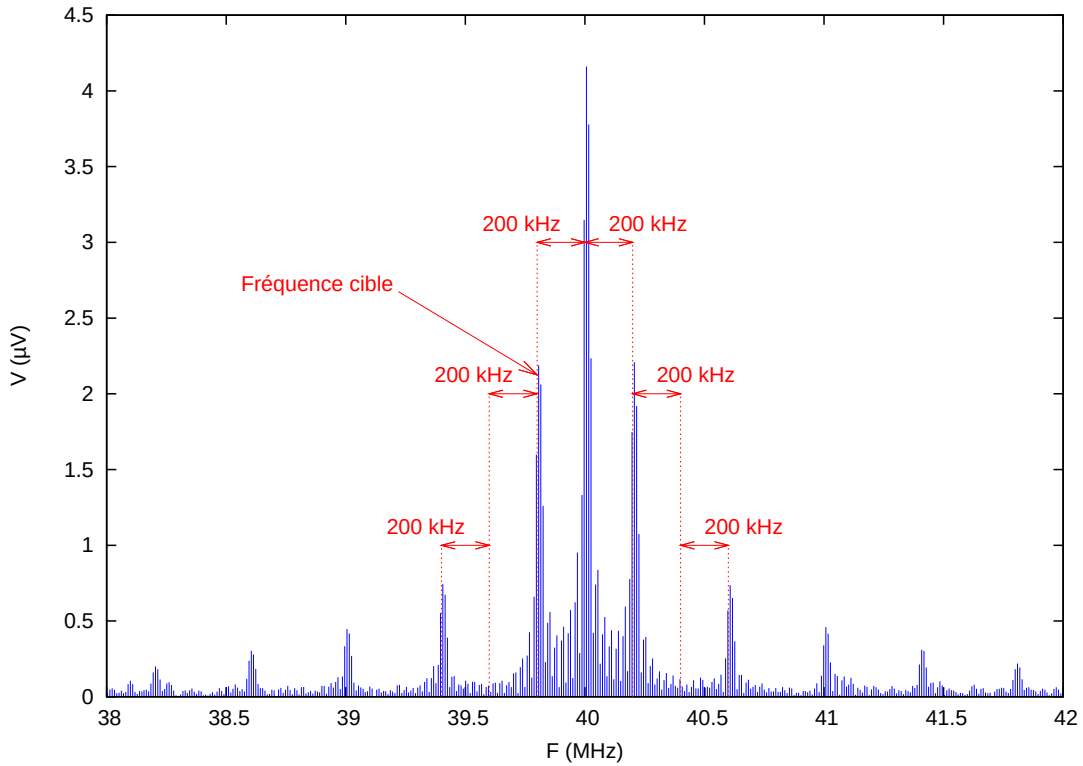
Module de la Transformée de Fourier Discrète

$$\begin{aligned} \mathcal{M} : \quad \mathbb{R}^{N_S} &\rightarrow \mathbb{R} \\ O^0_{(x,y)} &\mapsto \left| \sum_{n=0}^{N_S-1} O^0_{(x,y)}(n) \cdot e^{-2i\pi k \frac{n}{N_S}} \right| \end{aligned}$$



Composante à 19,800 MHz.

Cartographie EM dans le Domaine Fréquentiel



Spectre fréquentiel autour de la fréquence cible pour le point d'intérêt.

Cartographie EM par Corrélations Croisées

Inconvénients des méthodes précédentes

- Nécessité de connaître l'activité du module à localiser (description matérielle, SPA / SEMA) ;
- En conséquence, analyse partielle.

Cartographie EM par Corrélations Croisées

Inconvénients des méthodes précédentes

- Nécessité de connaître l'activité du module à localiser (description matérielle, SPA / SEMA) ;
- En conséquence, analyse partielle.

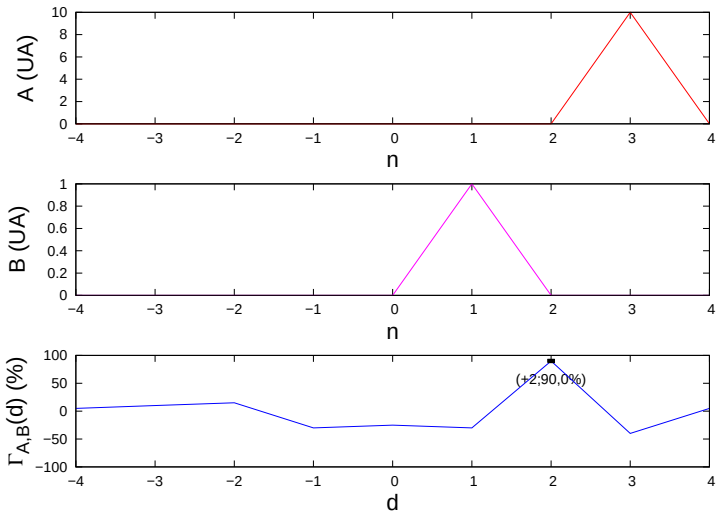
Objectifs

- Localisation **exhaustive** des sources EM ;
- **Sans connaissances préalables**.

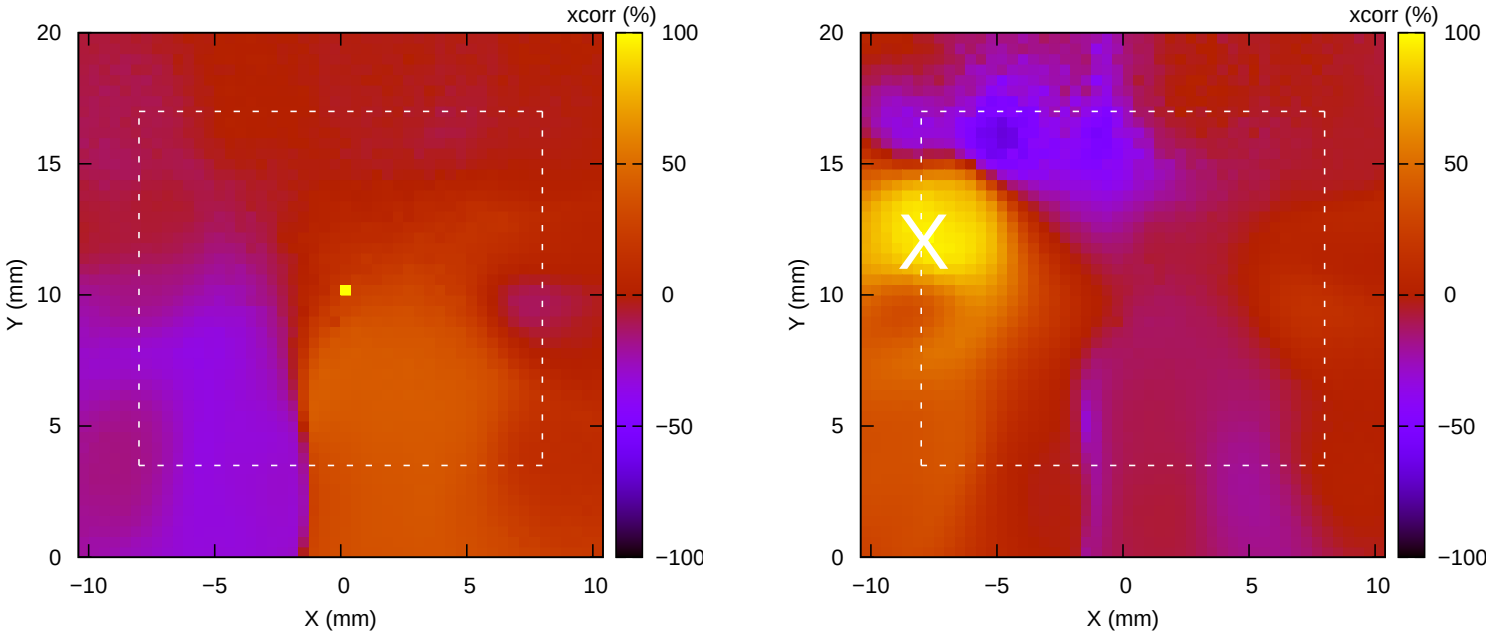
Cartographie EM par Corrélations Croisées

Fonction de corrélation croisée normalisée

$$\Gamma_{A,B}(d) = \frac{\mathrm{cov}(A,B_{-d})}{\sigma_A \cdot \sigma_B} = \frac{\sum_{n=d}^{d+\inf(n_A,n_B)-1} \left(A(n)-\overline{A(n)}\right)\cdot\left(B(n-d)-\overline{B(n)}\right)}{\sqrt{\sum_{n=0}^{n_A-1}\left(A(n)-\overline{A(n)}\right)^2}\cdot\sqrt{\sum_{n=0}^{n_B-1}\left(B(n-d)-\overline{B(n)}\right)^2}}$$



Cartographie EM par Corrélations Croisées



Le point de référence est le centre (*à gauche*) ou au-dessus du module de test en position NO (*à droite*).

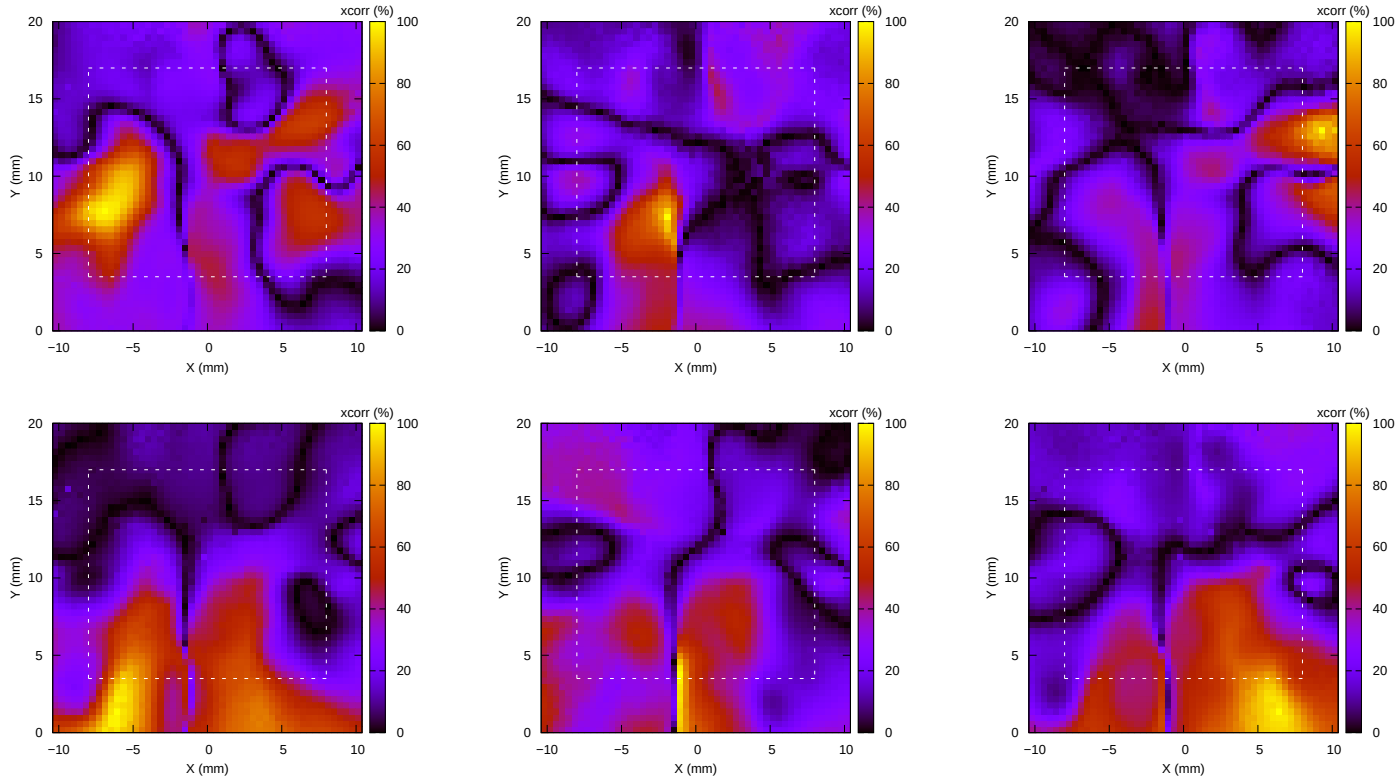
Cartographie EM par Corrélations Croisées

Fonction de corrélation croisée normalisée 2D

$$\Gamma^{2D}_{M,N}(p,q) = \frac{\mathrm{cov}(M, N_{(-p,-q)})}{\sigma_M \cdot \sigma_N}$$

$$= \frac{\sum_{x=p}^{p+\inf(N_{X_M},N_{X_N})-1} \sum_{y=q}^{q+\inf(N_{Y_M},N_{Y_N})-1} \left(M(x,y) - \overline{M(x,y)}\right) \cdot \left(N(x-p,y-q) - \overline{N(x,y)}\right)}{\sqrt{\sum_{x=0}^{N_{X_M}} \sum_{y=0}^{N_{Y_M}} \left(M(x,y) - \overline{M(x,y)}\right)^2} \cdot \sqrt{\sum_{x=0}^{N_{X_N}} \sum_{y=0}^{N_{Y_N}} \left(N(x-p,y-q) - \overline{N(x,y)}\right)^2}}$$

Cartographie EM par Corrélations Croisées



Zones principales identifiées par corrélations croisées pour le cryptoprocesseur 3DES non protégé.

Performance des attaques sur le cryptoprocesseur 3DES non protégé, en milliers de chiffrement

Analyse	S1	S2	S3	S4	S5	S6	S7	S8	Gain
CPA (globale)	478,7	197,0	464,1	614,7	418,9	709,1	348,3	134,0	÷ 1
CEMA globale	4,9	7,5	16,6	16,8	23,6	14,9	30,2	13,7	÷ 23
CEMA temporelle	1,9	7,6	1,5	3,8	2,1	1,2	1,2	0,2	÷ 93
CEMA fréquentielle	2,9	6,2	1,1	4,7	3,1	0,7	1,5	0,6	÷ 114
CEMA horloge 20 MHz		44,4	34,3		28,7				-

■ >100 000 chiffrements.

Logique Double-rail à Précharge

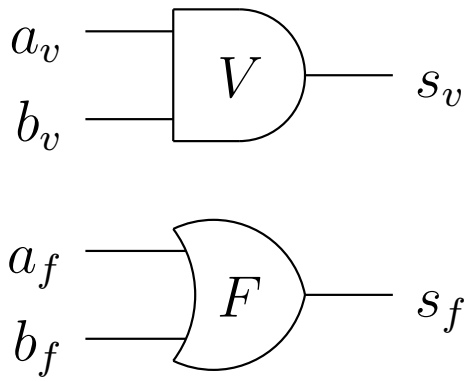
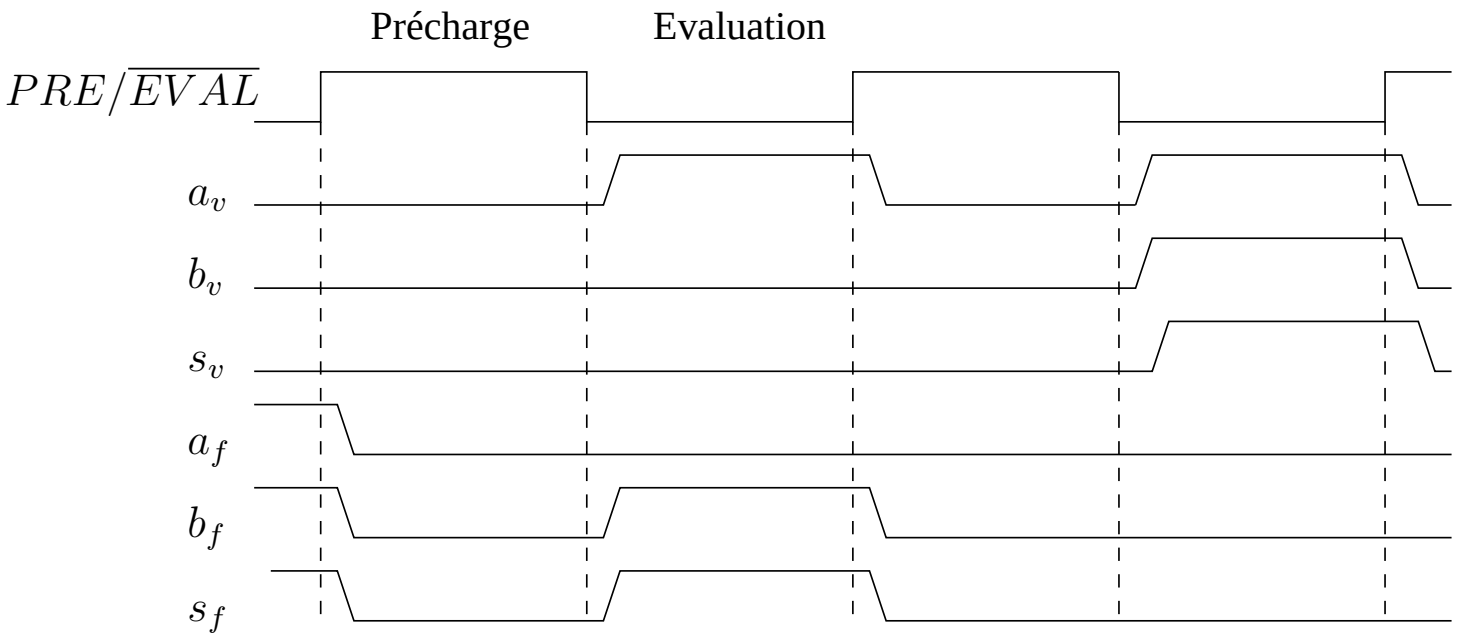


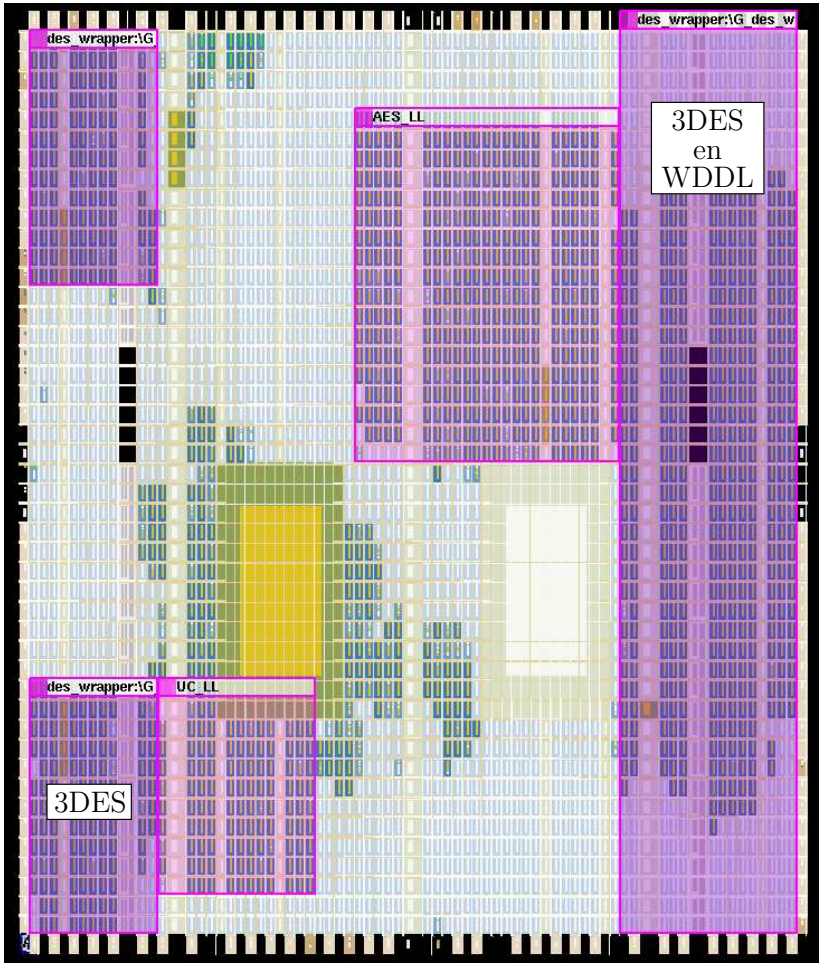
Schéma d'une porte logique ET en WDDL.

Logique Double-rail à Précharge

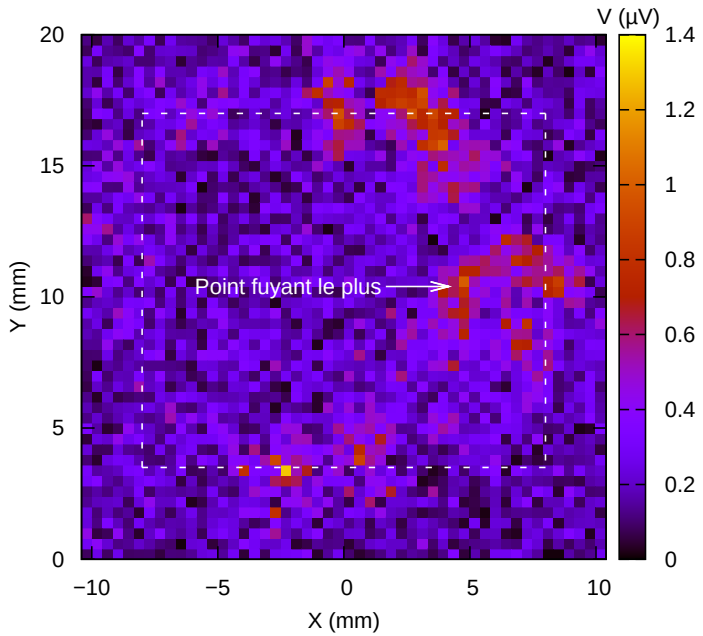


Chronogrammes de fonctionnement d'une porte logique ET en WDDL.

Floorplan du SoPC EveSoc programmé dans un Stratix



Attaque par Analyse Fréquentielle



Distribution de la composante fréquentielle à 4,333 MHz au-dessus du cryptoprocesseur 3DES WDDL.

Performance des attaques sur le cryptoprocesseur 3DES WDDL, en milliers de chiffrement

Analyse	S1	S2	S3	S4	S5	S6	S7	S8	Gain
CEMA HD 4 bit 3DES simple	2,6	5,4	1,4	4,9	3,1	3,6	2,8	0,6	$\times$ 1
CEMA HW 1 bit 3DES WDDL	62,9	32,8	45,3	14,6	27,1	3,8	37,1	27,6	$\times$ 12

Gain en sécurité : 12

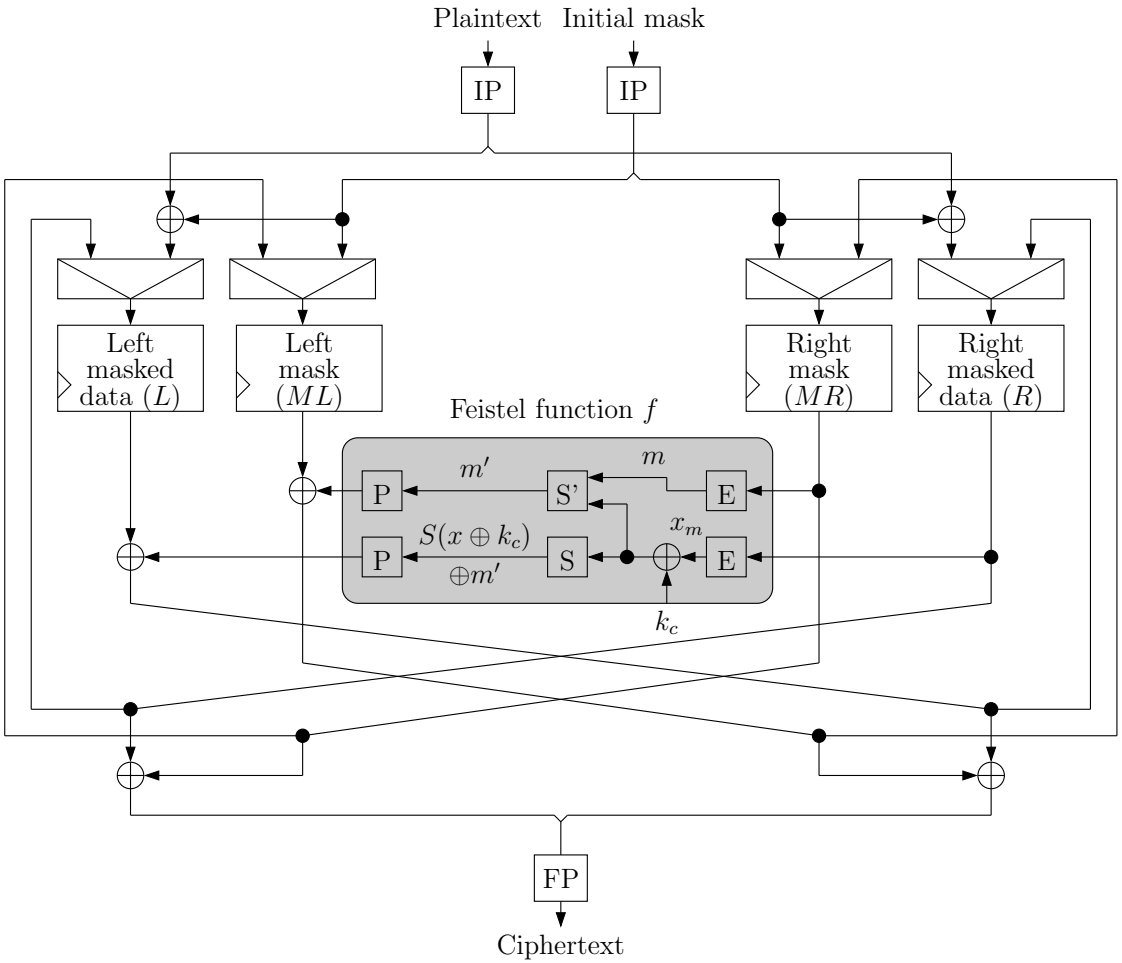
Masquage à base de partage de secret

Un bit sensible b qui doit rester secret est séparé en plusieurs parts : un bit masqué b_m et d bits de masque $m_1, m_2, ...m_d$ aléatoires, reliés entre eux par une relation de groupe $*$: $b = b_m * m_1 * m_2....$

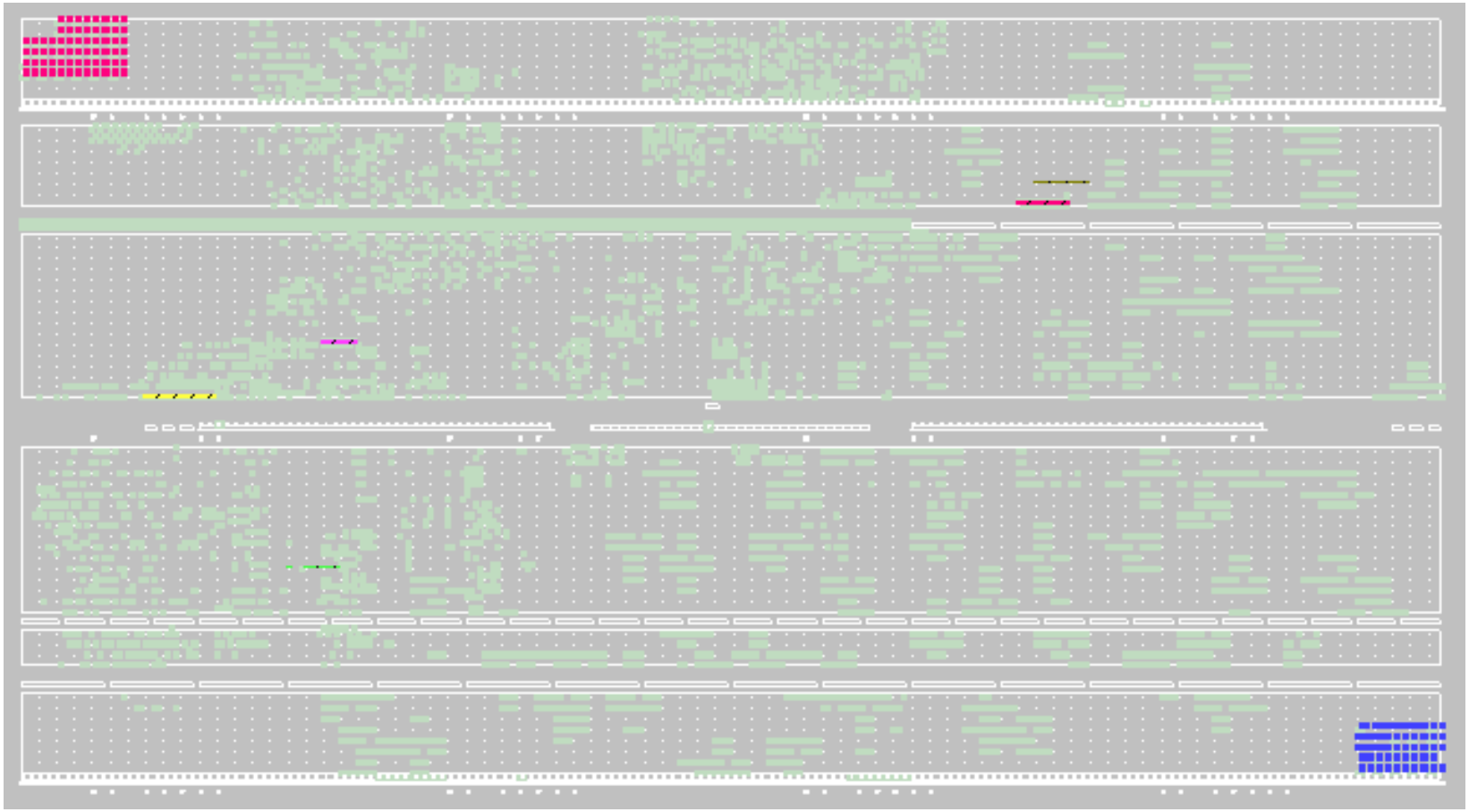
Attaques d'Ordre Élevée

Combiner les instants de fuites $L(t_i)$ où sont manipulés la valeur masquée et les différents masques (produit, valeur absolue de la différence, valeur absolue de la différence élevée à une puissance, sinus, ...).

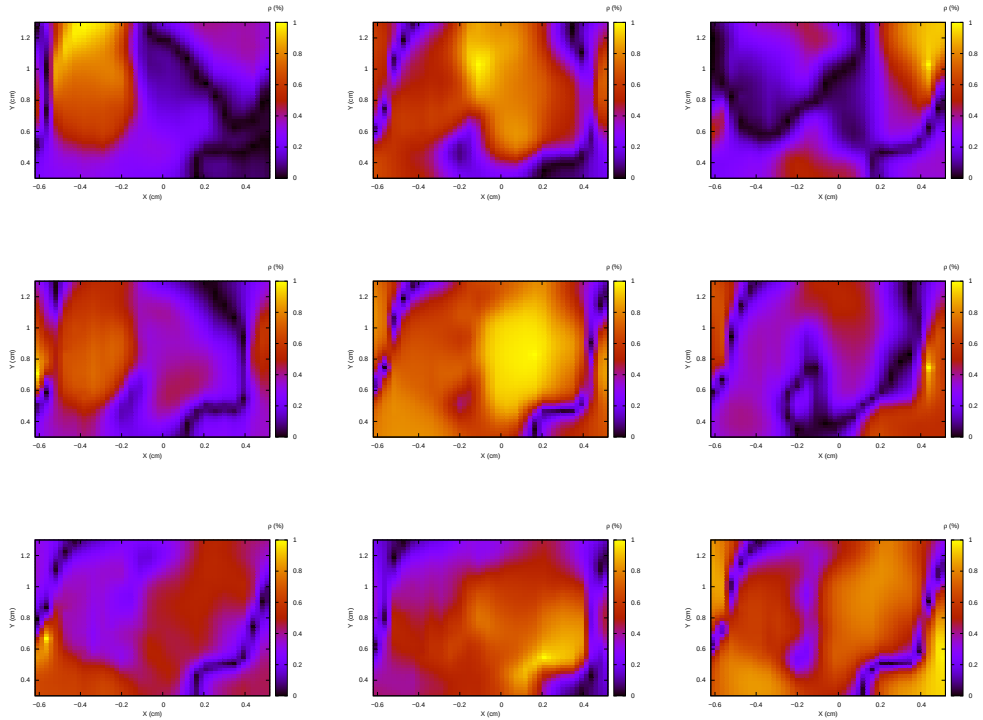
Chemin de données de notre implémentation 3DES protégée par masquage booléen



Placement des registres LR (*bleue*) et MLMR (*rouge*)



Cartes obtenues par corrélations croisées



La complexité passe de C_{625}^2 dans notre cas à $C_{11}^2 = 55$.

Sommaire

Conclusion

- 3 méthodes de localisation proposées
  - Temporelle : nécessite la connaissance des phases d'activité
  - Fréquentielle : nécessite de modéliser l'activité pour trouver une fréquence cible
  - Corrélations croisées
- Amélioration de la force des attaques
- 1 attaque du 2e ordre spatiale

Perspectives

- Corrélation : à reproduire dans le domaine fréquentiel
- WDDL : analyse à reproduire avec P&R vraiment différentiel
- Masquage : analyse à reproduire sans P&R

Merci pour votre attention, des questions ?