Utilisation de méthodes d'analyse fréquentielle pour l'attaque de composants cryptographiques par canaux auxiliaires

Olivier MEYNARD, Sylvain Guilley, Denis Réal, Jean-Luc Danger.

[1] TELECOM-ParisTech , CNRS – LTCI (UMR 5141),
[2] DGA/MI (French DoD, information superiority).

Le 18 Mai 2011.

Présentation

Presentation Outline

Introduction aux **Canaux Auxiliaires** (*SCA*)

Les Composants Cryptographiques et Cibles Potentielles

- Carte à Puce,
- Microprocessor,
- FPGA.

Les Canaux Auxiliaires

Les composants cryptographiques nous livrent leurs secrets:

- Temps d'exécution
- Consommation de courant
- Rayonnement Électromagnétique

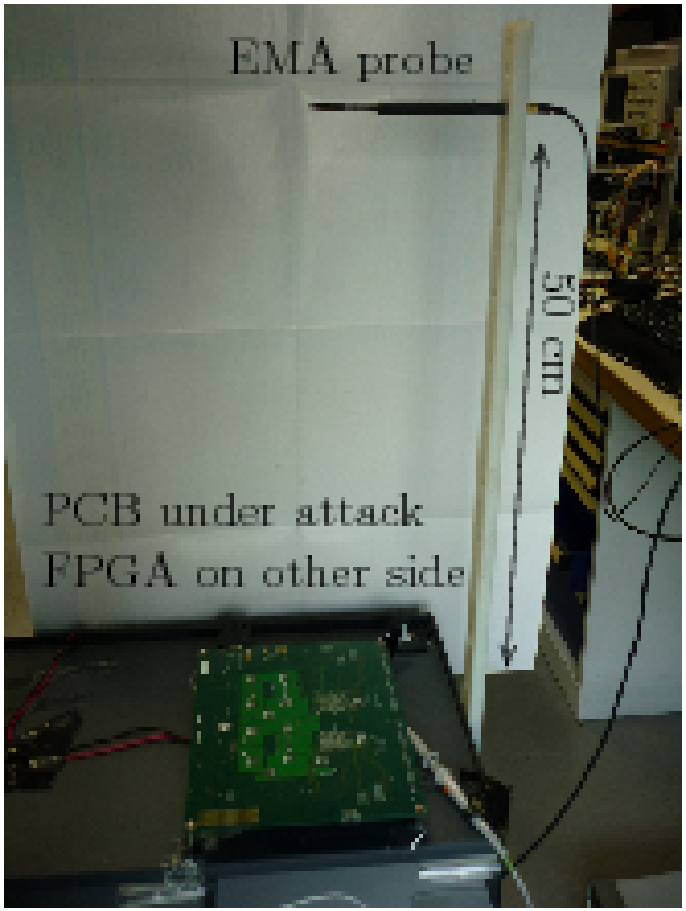
Comment réussir une attaque ?

Choix stratégiques pour une bonne Exploitation du SCA

Le succès d'une attaque dépend de différents paramètres :

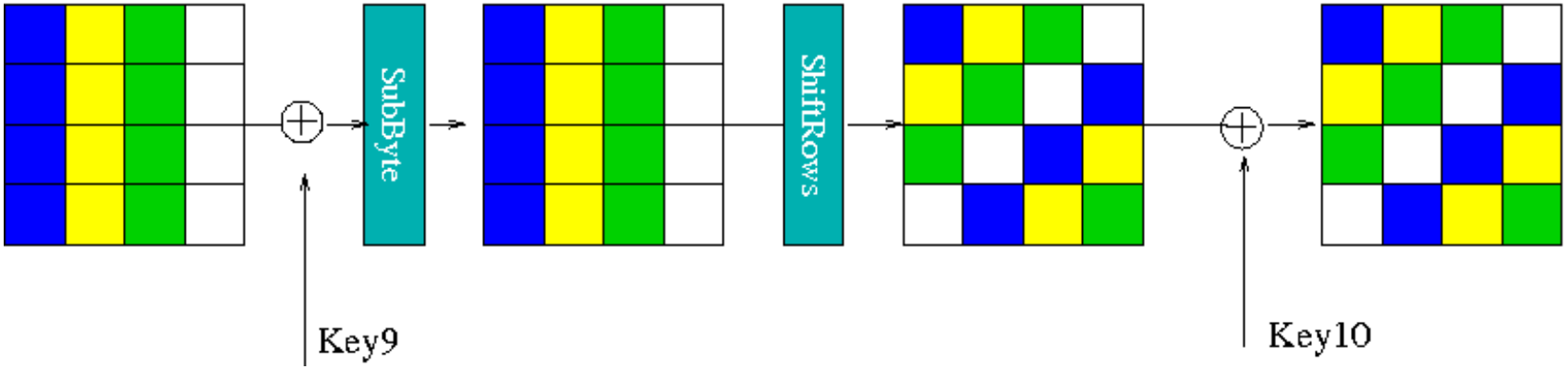
- Un tri pertinent des acquisitions selon un modèle de fuite, *i.e.* **leakage model** ;
- La sélection de points d'intérêts, *i.e.* **POI** ;
- **Un Distingueur** :
  covariance (DPA), *corrélation* (CPA), *information mutuelle* (MIA), *maximum de vraisemblance* (Template et Attaques Stochastiques).

Un contexte d'attaque (EM) particulier



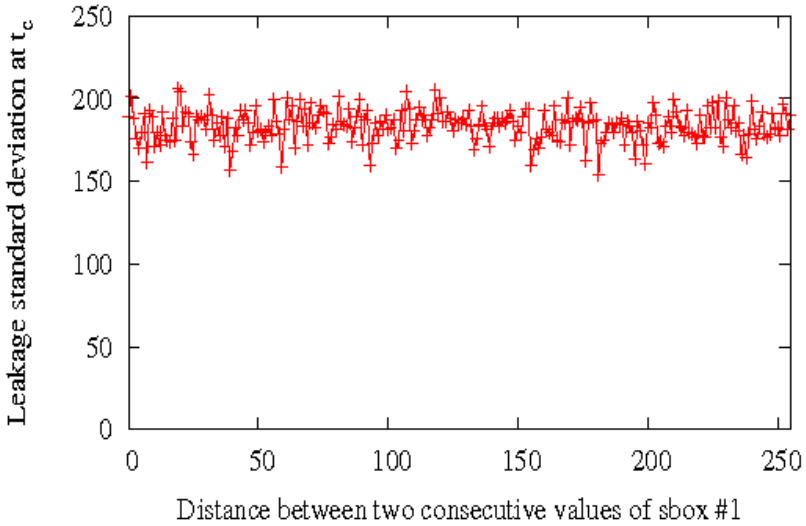
- Utilisation d'une carte SASEBO-G,
- Implémentation d'un AES 128-Bits Rijndael,
- Implémentation sans contremesure.

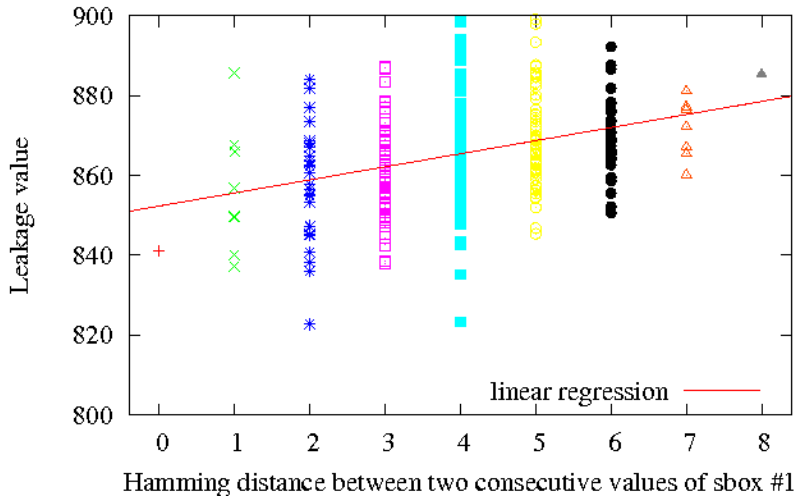
Choix d'un modèle de fuite et premiers résultats



- La fonction de sélection $\mathcal{L} = HW(\text{state}_9[sbox] \oplus \text{ciphertext}[sbox])$.
- Une anecdote : la première ligne des Sbox au dernier tour ne prend pas les 256 valeurs possibles.
- Le nombre de transitions possibles est donc réduit à $\#\{x \oplus \texttt{SubBytes}(x),\ \text{for } x \in [\texttt{0x00}, \texttt{0xff}]\} = 162$ valeurs sur les 256 attendues.
- la raison : $x \mapsto x \oplus \texttt{SubBytes}(x)$ n'est pas forcément bijective même si SubBytes l'est.

Premières observations : la détérioration du modèle de fuite à $d = 50$ cm





- La plus grande part d'information est contenue dans la moyenne des valeurs de fuite.
- Le modèle de fuite basé sur la distance de Hamming n'est plus optimal.

Comment améliorer les attaques EM dans des conditions de faible SNR ?

Recherche exhaustive des Points d'intérêts

Méthodes de recherche des points d'intérêt

- The *Sum Of Squared pairwise Differences* (sosd) Gierlichs *et al.* CHES'06
- The *Sum Of Squared pairwise (T-)Differences* (sost) Gierlichs *et al.* CHES'08
- The *Principal Component Analysis* (PCA)

Table 1: Quantité d'information et probabilité des poids de Hamming pour des mots aléatoires de 8-bit uniformément distribués.

Class index l	0	1	2	3	4	5	6	7	8
Information [bit]	8.00	5.00	3.19	2.19	1.87	2.19	3.19	5.00	8.00
Probability [%]	0.4	3.1	10.9	21.9	27.3	21.9	10.9	3.1	0.4

- l'estimation pour les sous groupes $l = 0$ ou 8 est moins précise.
- Conditions de mesures dégradées (faible SNR)...

Utilisation de matériel supplémentaire de type récepteur avant la numérisation du signal

Presentation Outline

Introduction au TEMPEST

Le programme TEMPEST

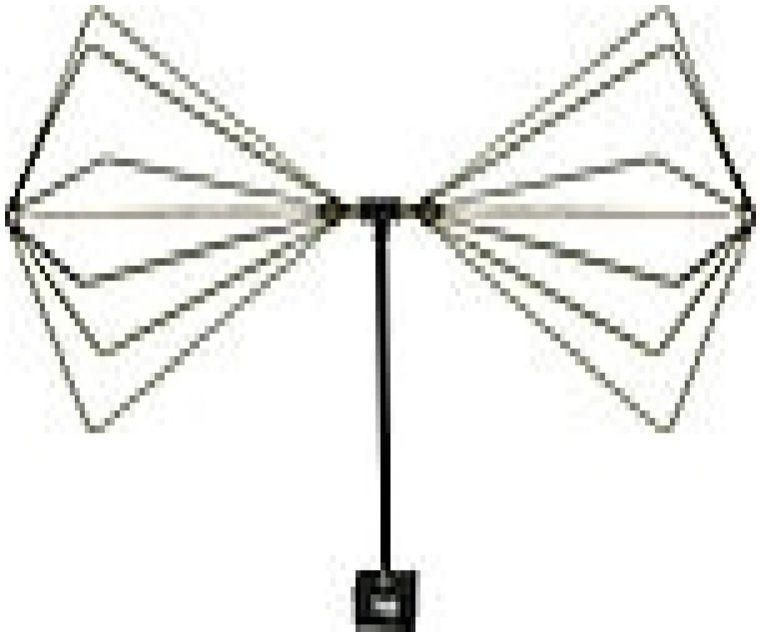
- depuis 1960 : pour analyse des compromissions électromagnétiques,
- définition d'une norme et de standards pour quantifier la quantité d'information compromettante dissipée,
- en 1990 une part importante de ces standards sont déclassifiés.

$\Rightarrow$ le monde civil et académique commence à s'intéresser au domaine

Travaux publiés :

- 1985 : RF eavesdropping of video displays [van Eck]
- 1990 : HF/VHF eavesdropping of RS-232 cables [Smulders]
- 2002 : The EM Side-Channel(s)[Agrawal]
- 2005 : Security limits for compromising emanations [Kuhn]
- 2009 : Compromising Electromagnetic Emanations of Wired and Wireless Keyboard [Vuagnoux]

Matériel utilisé



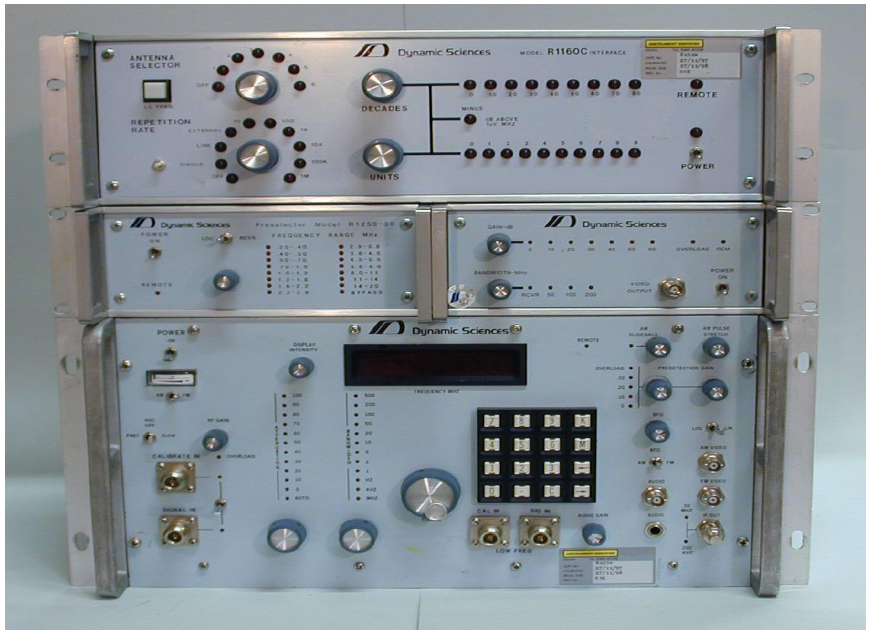


Figure 1: Antenne Biconique 20MHz-300MHz, Récepteur TEMPEST
(Photos extraites Kuhn CHES2005)

Les Compromissions Électromagnétiques

Les origines et les différents types de Compromissions

- Les émanations directes produites par des changements d'état rapides du courant
- Les émanations non intentionnelles produites par des phénomènes de couplage :
  - apparaissent comme la modulation d'une porteuse (les harmoniques de l'horloge) en AM ou FM
  - les signaux compromettants disponibles via démodulation

Un défi scientifique :
Caractériser les fréquences porteuses d'information

Notre Contribution

- Nous proposons différentes approches :
  1. **une méthode empirique**,
  2. **une méthode basée sur la PCA (analyse en composantes principales)**,
  3. **une méthode basée sur la théorie de l'information**.
- Validation de ces méthodes prédictives avec un récepteur TEMPEST.
- Cas d'étude du rayonnement émis par un clavier PS/2.
- Application de cette méthode sur une cible cryptographique.

Presentation Outline

Le Protocole PS/2

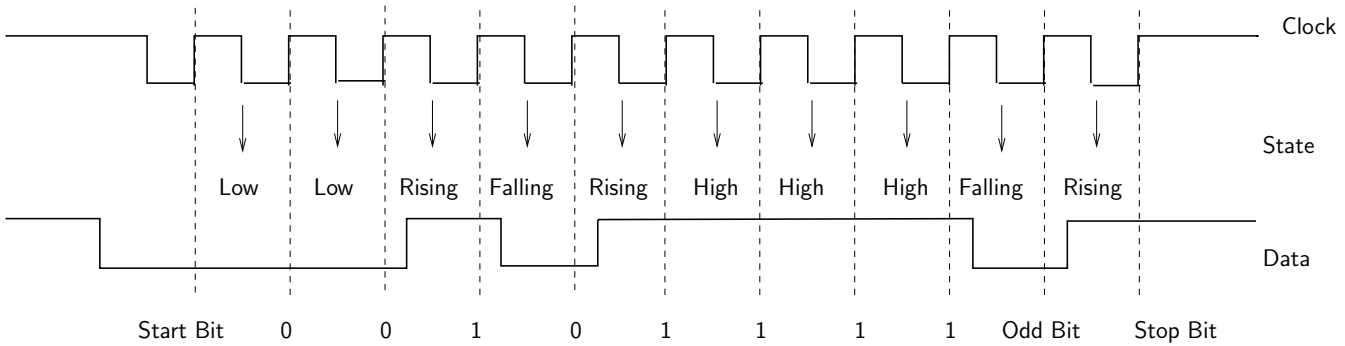
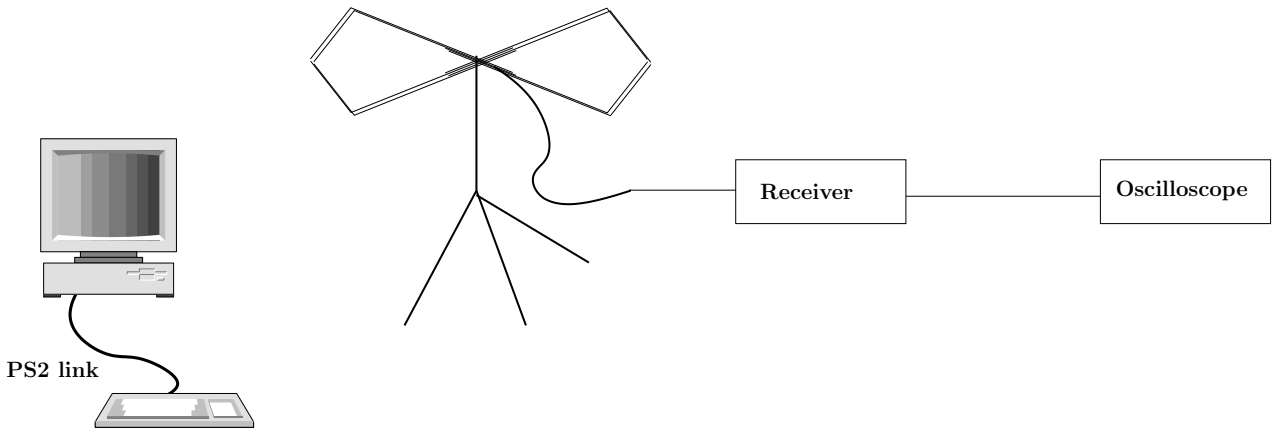


Figure 2: Protocole PS/2 entre un clavier et l'unité centrale d'un ordinateur

- Les lignes (données, horloge) sont montées en collecteur ouvert.
- Les données des trames de 11-bits.
- L'émission d'une trame déclenche l'horloge (F 10 kHz et 16.7 kHz).
- Les données sont lues sur les fronts descendants de l'horloge.

État de l'art et méthodologie des évaluations TEMPEST



Les principes de l'évaluation TEMPEST

- Système placé en cage de Faraday.
- Vérifier que les signaux "Rouge" et "Noir" sont bien séparés.
- i.e la difficulté pour un attaquant de reconstruire un signal "Rouge" à partir d'une interception du "Noir".
- Utilisation d'un analyseur de Spectre et d'un récepteur TEMPEST est requise.

Inconvénients

- Travail long et fastidieux
- dépend de l'acuité de l'évaluateur et de son expérience.

Attaque/Évaluation sans utilisation d'un récepteur TEMPEST

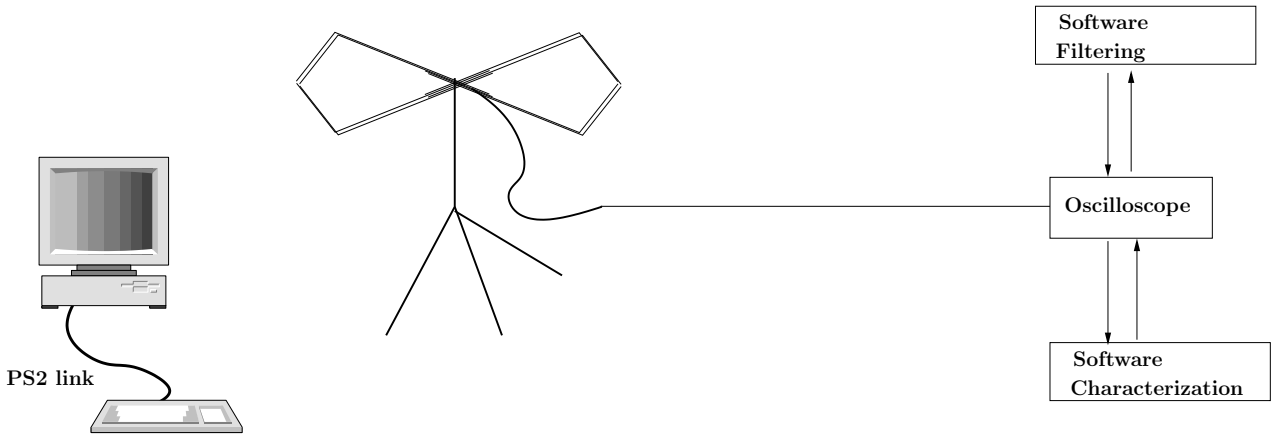
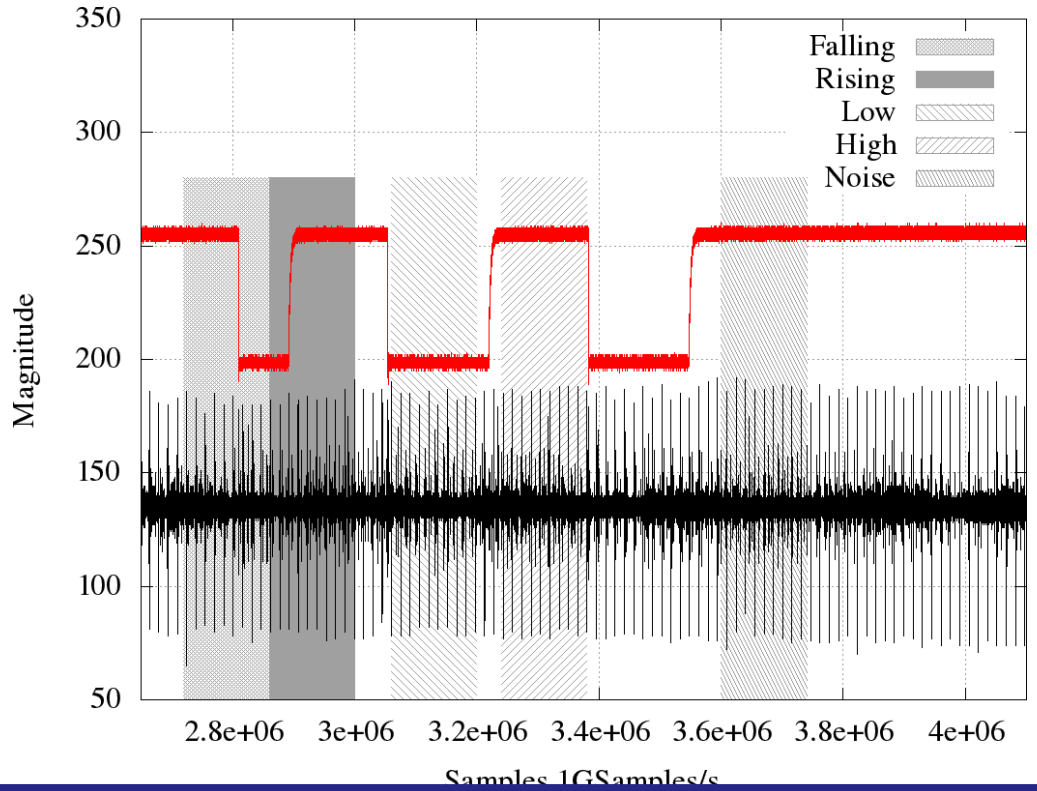


Figure 3: Dispositif d'attaque sans utiliser de récepteur TEMPEST

- Analyse des mesures dans le domaine fréquentiel.
- Accumulation des mesures pour améliorer la précision de la caractérisation fréquentielle.
- Ces résultats peuvent constituer une première évaluation TEMPEST.

Traitement des Données



Notre Méthode en Bref :

- Mettre en évidence les dépendances signal "Rouge" vs "Noir".
- Constituer un stock de courbes conséquent pour une même touche (Signature électromagnétique d'une touche)
- Découper le signal "Noir" connaissant le "Rouge".

Pseudo-code

Processing of the measurements

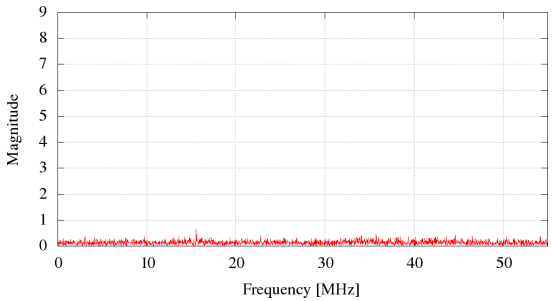
Input:	$O = (O_0, ..., O_{n-1}, O_n)$ Observation in time domain,
	$S = (S_0, ..., S_{n-1}, S_n)$ in $StateSet = \{High, Low, Falling, Rising, Noise\}$.
Output:	Result Characterization in frequency domain

1 : **for** $i = 0$ **to** n
2 : Sort O_i Observation according to the State S_i;
3 : Compute the FFT of each Observation O_i;
4 : **endfor**

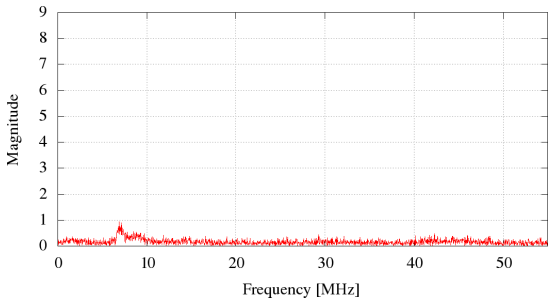
5 : Compute the mean for each state $E(f, State)$
6 : Compute the standard deviation for each state $\sigma(f, State)$,
7 : Compute the standard deviation of all the observations σ_{O_f}
8 : Apply the Distinguisher in Frequency domain.

Distingueur Empirique basé sur la CPA

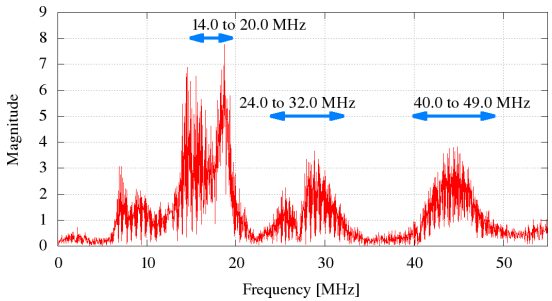
$\rho(f, LowState)$



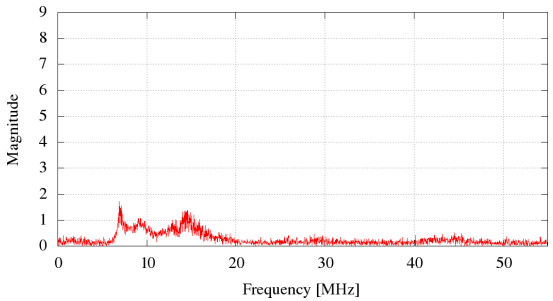
$\rho(f, HighState)$



$\rho(f, FallingEdge)$



$\rho(f, RisingEdge)$



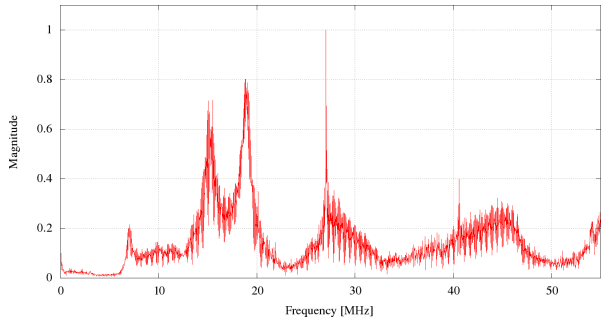
La Méthode Empirique : une différence entre deux moyennes

- spectre obtenu pour un état donné
- spectre obtenu pour le bruit i.e (aucune données ne transitent sur la ligne).

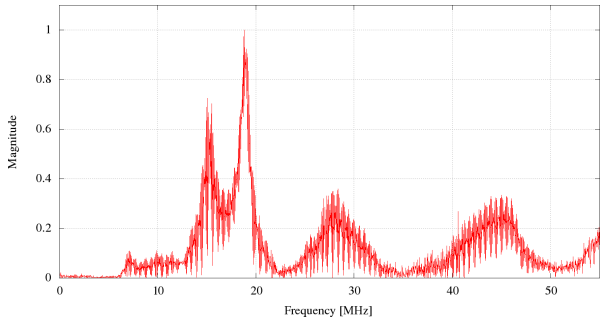
$$\rho(f, State) = \frac{E(f, State) - E(f, N)}{\sigma(f, N)}.$$

Distingueur basé sur l'analyse en composante principale

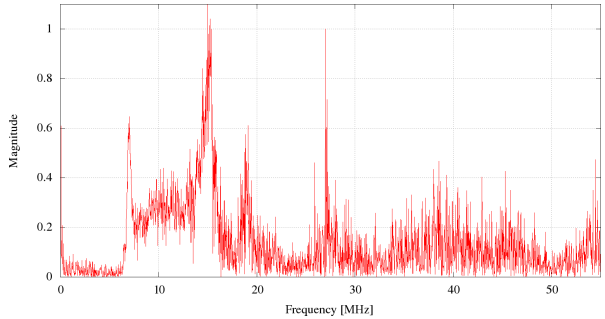
First eigenvector value=7.2×10^{14}



Second eigenvector value=2.3×10^{9}



Third eigenvector value=3.5×10^{7}



Fourth eigenvector value=2.0×10^{7}

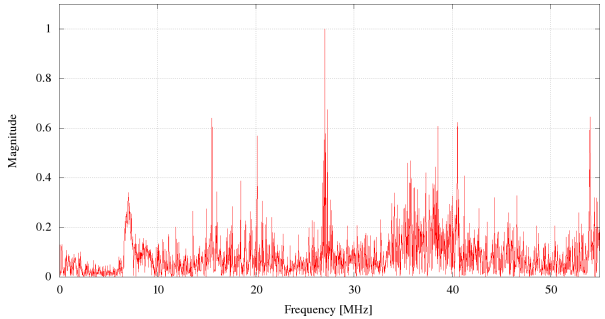
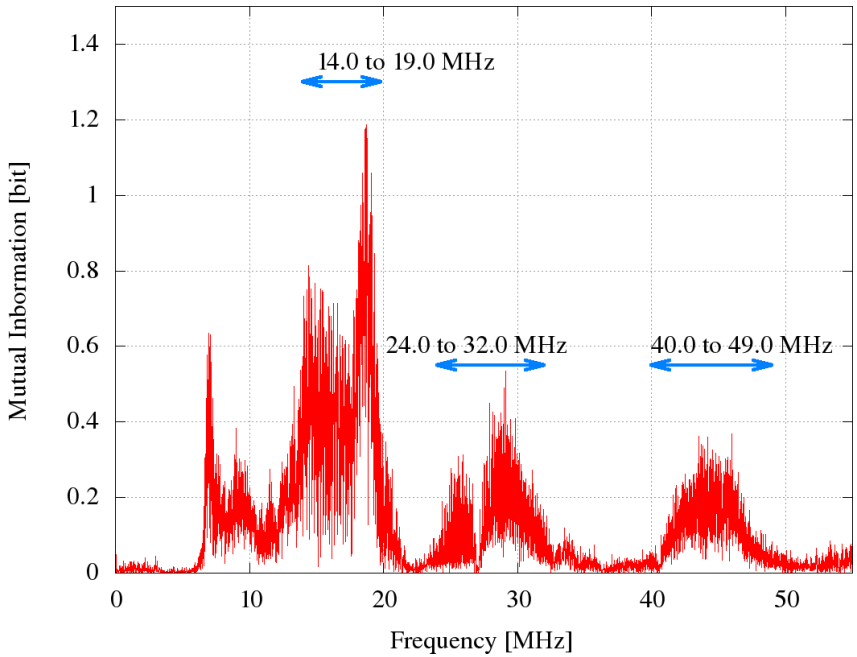


Figure 4: Les quatre vecteurs propres obtenus par PCA.

$$\Sigma_o = \frac{1}{4} \sum_{j \in StateSet} (\mu_j(f) - \mu(f))(\mu_j(f) - \mu(f))^{\mathsf{T}}$$

Un peu de Théorie de l'information...



- L'information Mutuelle est définie par : $\mathrm{I}(O_f; State) = \mathrm{H}(O_f) - \mathrm{H}(O_f|State)$.
- En approximant et en utilisant l'entropie paramétrique :

$$\mathrm{I}(O_f; State) = \frac{1}{4} \log_2 \frac{\sigma_{O_f}^4}{\sigma(f, High)\sigma(f, Low)\sigma(f, Rising)\sigma(f, Falling)}.$$

- Le bruit n'est pas considéré de la même façon.

Confirmation des Résultats de caractérisation avec un Récepteur Hardware

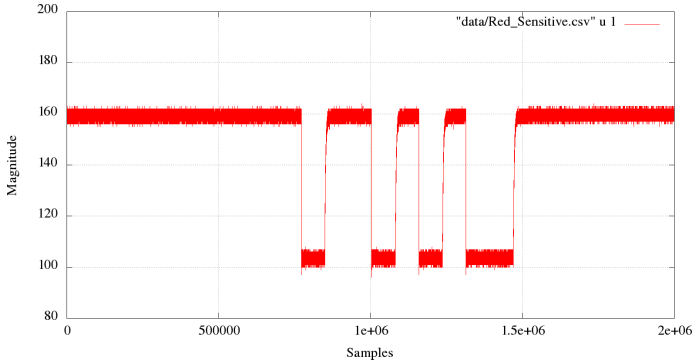
Les Caractéristiques d'un Récepteur TEMPEST

Décrit par Kuhn type R-1250 by *Dynamics Sciences* :

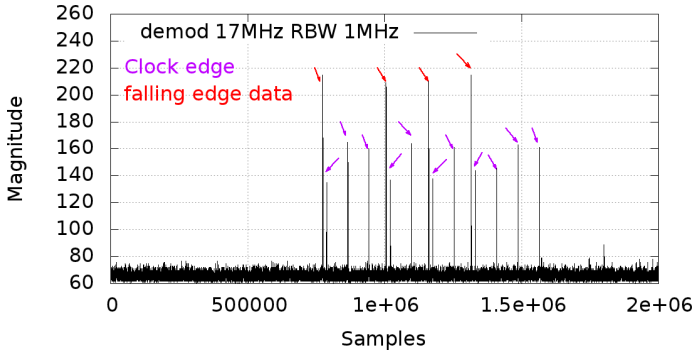
- super hétérodyne et large bande,
- balayage de façon continue des fréquences entre 100 Hz et 1 GHz avec une largeur de bande de 50 Hz à 200 MHz,
- plus de 21 filtres de présélection (atténuation et gain réglable).

Une démodulation réussie

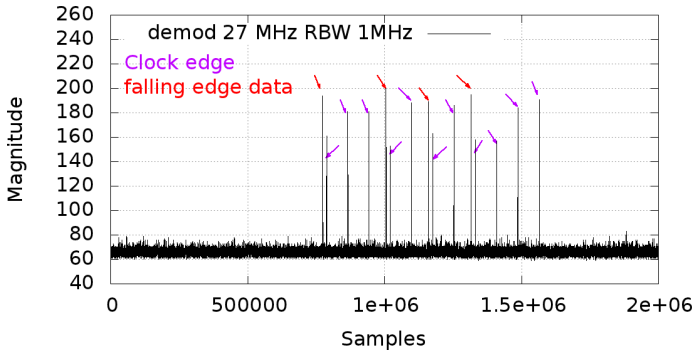
Signal Rouge



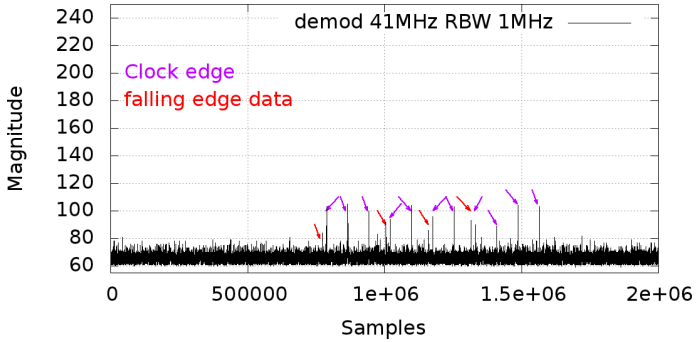
Démodulation à 17.0 MHz.



Démodulation à 27.0 MHz.



Démodulation à 41.0 MHz.



Le signal démodulé montre des particularités :

- la technique des "transitions sur front descendant",
- le front descendant du signal de données et de l'horloge apparents,
- les fronts descendants du signal de données apparaissent avant les fronts descendants d'horloge.

Technique de filtrage software

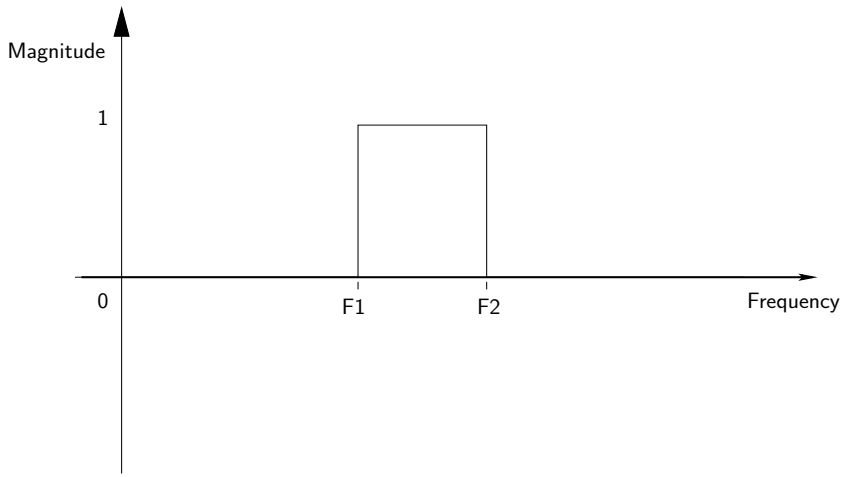


Figure 5: Conception du filtre passe bande.

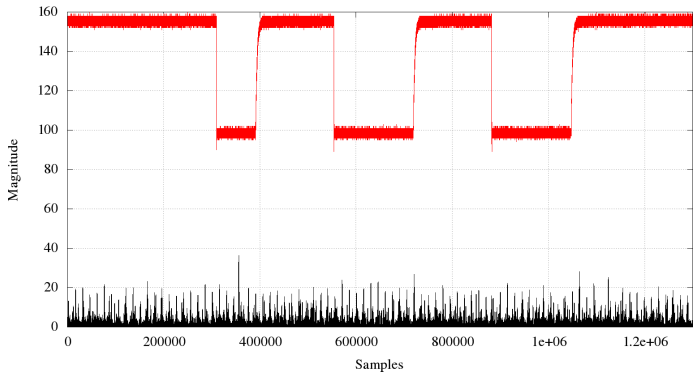
Traitement par filtre software

Démodulation par traitement software :

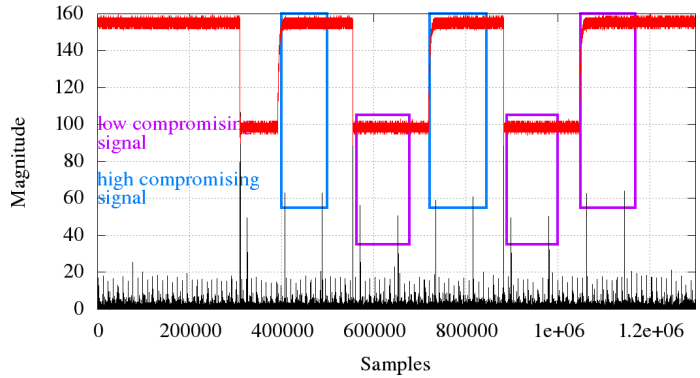
- appliquer la FFT sur le signal "Noir",
- effectuer le produit entre ce signal et le filtre passe bande,
- effectuer une IFFT.

Résultats de Démodulation software

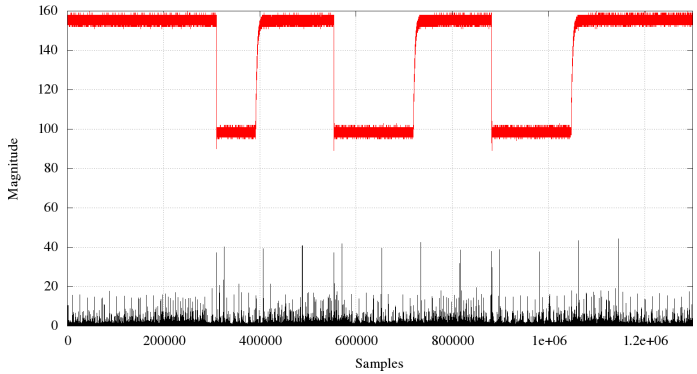
Bandpass filtering 21.0 – 27.0 MHz (No Signal)



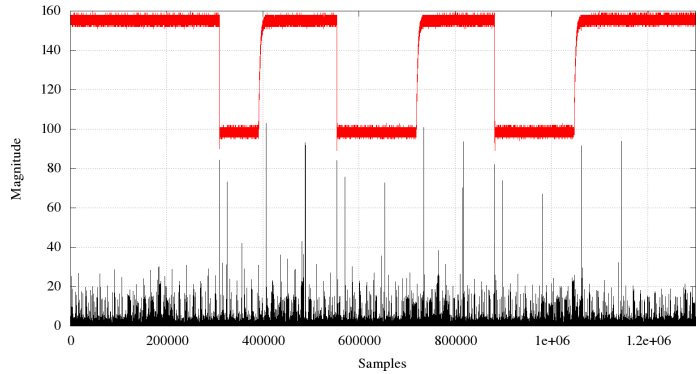
Bandpass filtering 14.0 – 20.0 MHz



Bandpass filtering 24.0 – 32.0 MHz



Bandpass filtering 40.0 – 49.0 MHz



- Obtention de façon approximative de l'enveloppe du signal avec une capture du Signal Noir
- Perte de précision (vs Hardware Démodulation) (BW plus importante).

Pré caractérisation fréquentielle sur des signaux

Cette technique est-elle applicable sur une cible cryptographique ?
Sur des Opérations ?

Presentation Outline

Problématiques & Motivations

- *Que faire pour améliorer une SEMA ?*

- SPA/SEMA bien connues d'un point de vue théorique,
- Développer l'aspect pratique de ces attaques,
- Montrer que la démodulation améliore considérablement la SEMA,
- Proposer une méthode pour retrouver les fréquences porteuses d'informations.

Le Cryptosystem RSA

Le RSA :

- Le RSA un crypto système à clé Publique :

$$\text{Encryption} \quad C = P^E \bmod N, \tag{1}$$

$$\text{Decryption} \quad P = C^D \bmod N. \tag{2}$$

- les opérandes sont de taille 1,024 bits.

L'implémentation RSA :

- Exponentiation Modulaire : left-to-right binary method,
- Opération de Multiplication et de mise au carré effectuée de façon séquentielle en fonction du bit de clé D ou E,
- Utilisation d'un Multiplieur de Montgomery (même chemin critique).

Implémentation : Exponentiation Modulaire

Input: X, N,
$E = (e_{k-1}, ..., e_1, e_0)_2$
Output: $Z = X^E \bmod N$

1: $Z := 1$;
2: **for** $i = k - 1$ **downto** 0
3: $Z := Z * Z \bmod N$; – squaring
4: **if** $(e_i = 1)$ **then**
5: $Z := Z * X \bmod N$; – multiplication
6: **end if**
7: **end for**

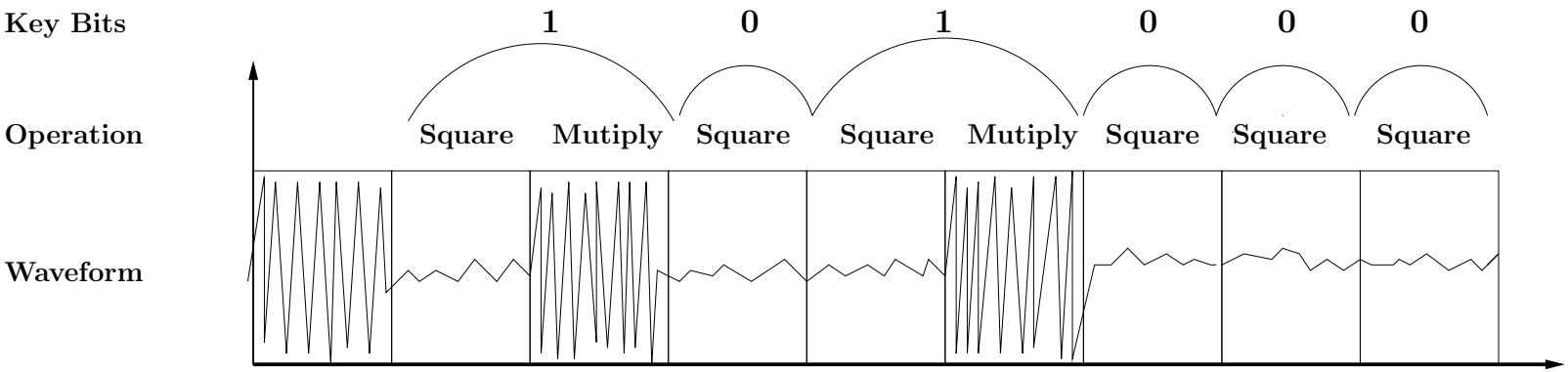
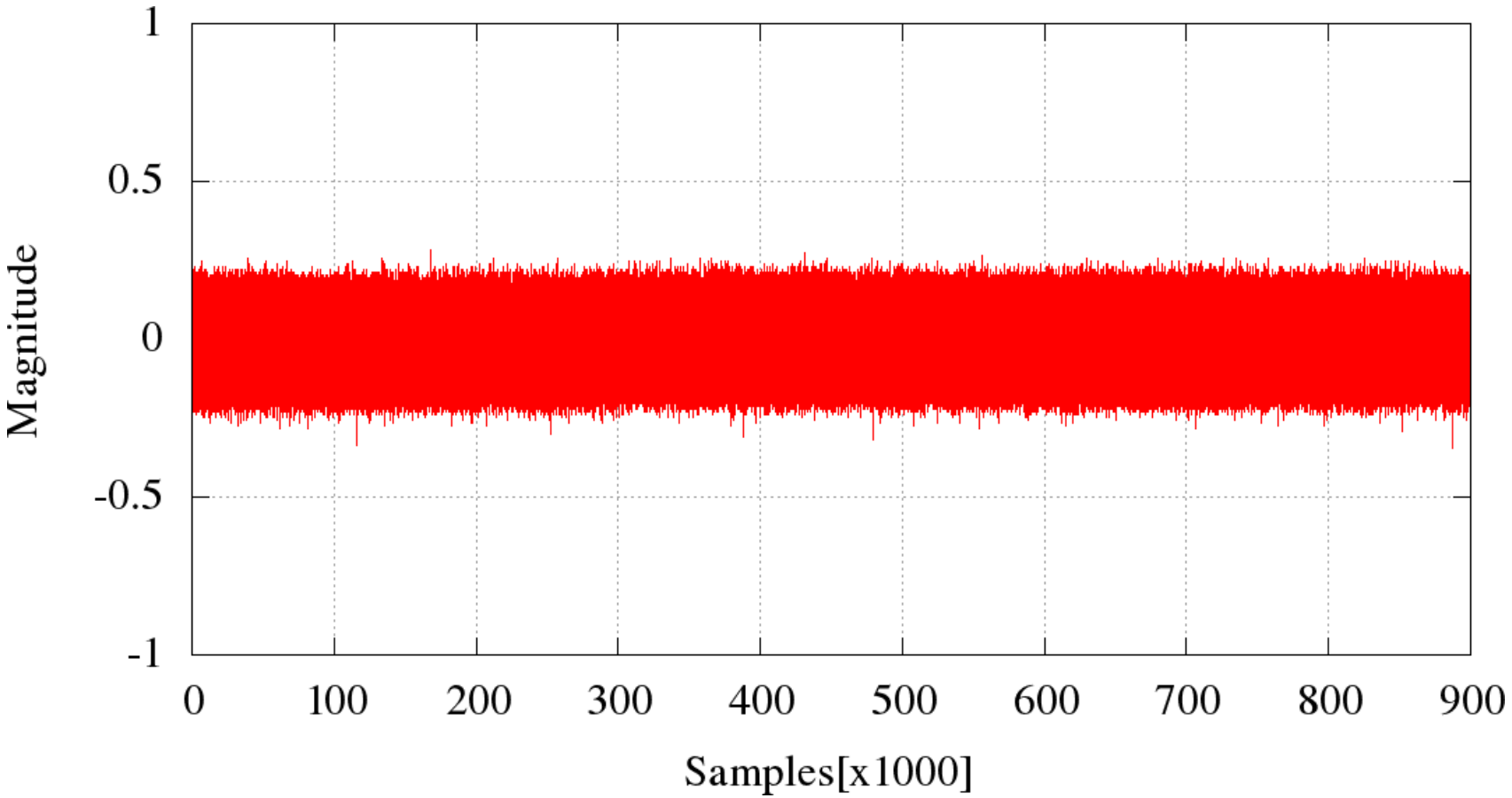


Figure 6: Principe de la SEMA sur le RSA.

Cible Cryptographique

RSA sur FPGA (Xilinx Virtex II) sur la carte SASEBO-G.

Une Mesure Brute



Questions

Y a-t-il de l'information contenue dans cette mesure brute ?

Notre Contribution

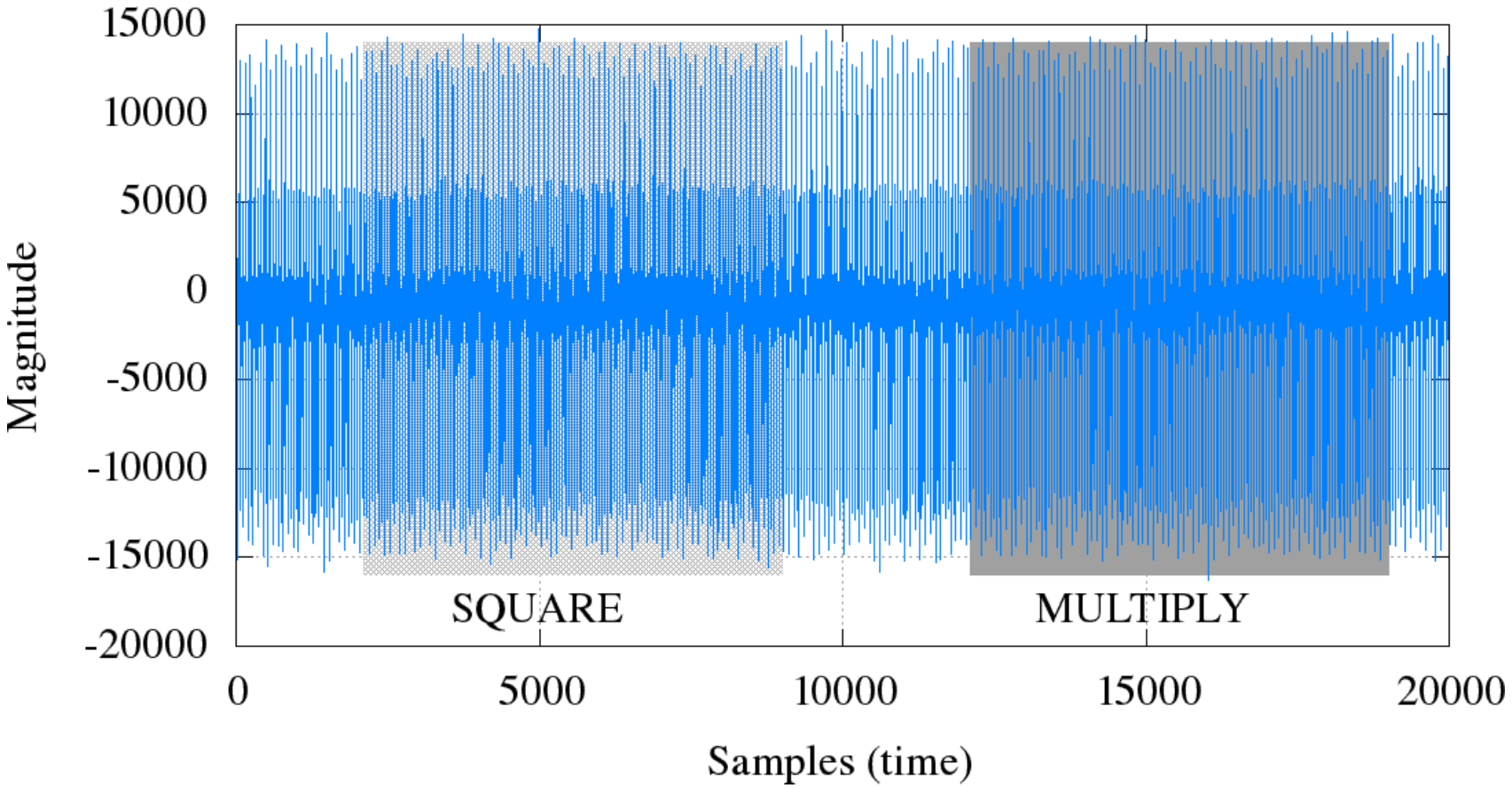
Nous proposons une caractérisation dans le domaine fréquentiel en utilisant la théorie de l'information.

Fenêtrage et Préparation des Echantillons

Méthodologie

1. Collecte d'un nombre conséquent de mesures (à Clé connue).
2. Choix d'une fenêtre où est exécutée une opération de Square et une opération de Multiply.
3. Découpe des mesures connaissant l'opération effectuée.
4. Obtentions de 2 jeux de courbes avec le même nombre de traces.

Traitement des Mesures EM



Pseudo-code

Input:	$O = (O_0, ..., O_{n-1}, O_n)$ Observation in time domain,
	$S = (S_0, ..., S_{n-1}, S_n)$ Secret (Operation)
Output:	Result of Mutual Information in frequency domain

1 : **for** $i = 0$ **to** n
2 : Sort O_i Observation according to the Secret S_i;
3 : Compute the FFT of each Observation O_i;
4 : **endfor**
5 : Compute the mean $(\mu_{Square}, \mu_{Multiply})$
and the variance $(\sigma^2_{Square}, \sigma^2_{Multiply})$
6 : Compute the Mutual Information in frequency domain.

Théorie de l'Information et Information Mutuelle

En bref

- Étude des dépendances entre le modèle de fuite et l'observation,
- Métrique utilisée pour évaluer la quantité d'information contenue à différentes fréquences f
- Pour chaque fréquence f calcule de la MI $\mathrm{I}(O_f; Operation)$.

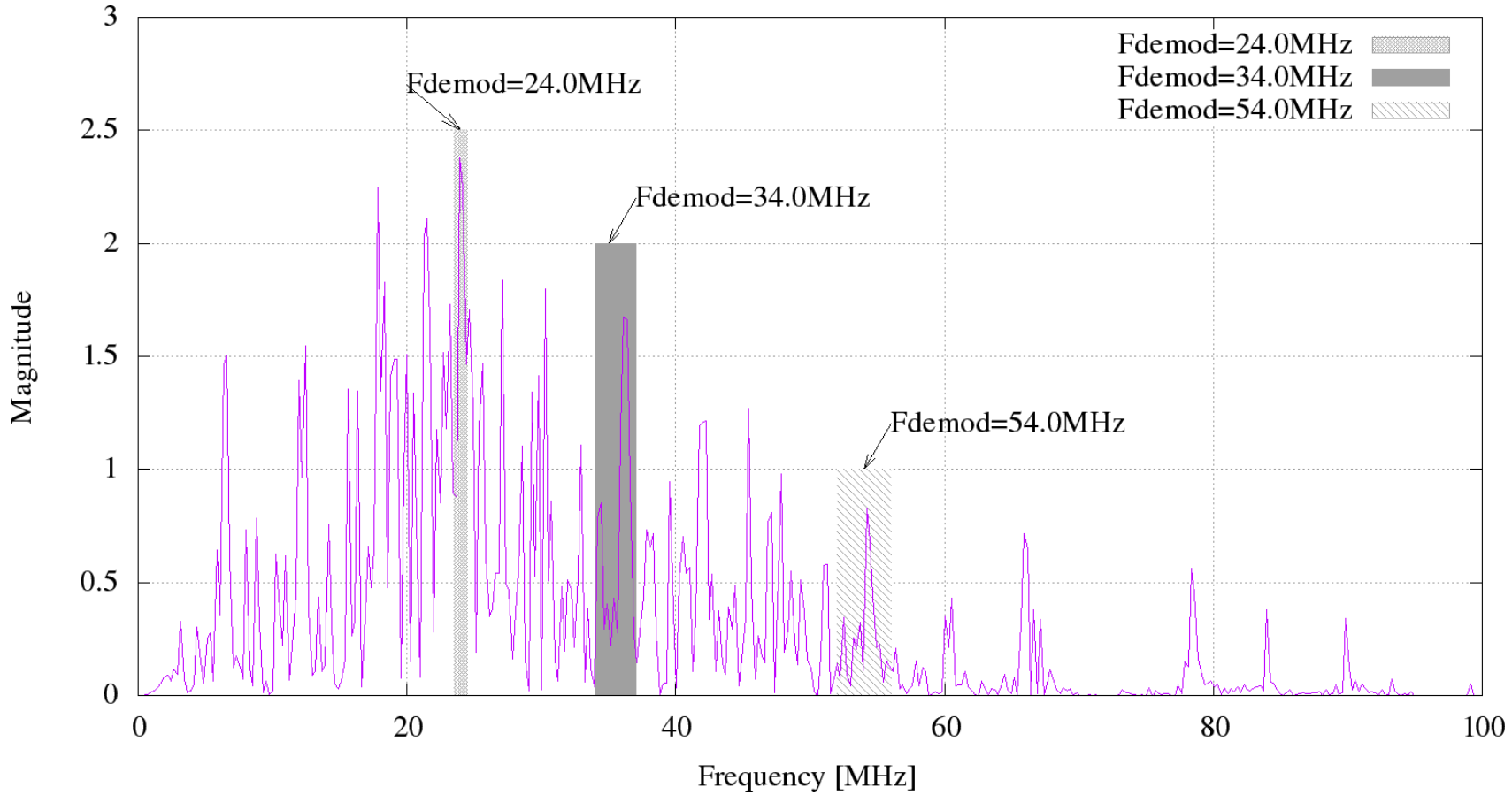
Comment calculer la MI ?

$$\mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) - \mathrm{H}(O_f|Operation),$$

$$\mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) - \frac{1}{2}\left(\mathrm{H}(f|Multiply) + \mathrm{H}(f|Square)\right),$$

$$\mathrm{I}(O_f; Operation) = \frac{1}{2}\log_2 \frac{\sigma^2_{O_f}}{\sigma_{O_f,Multiply} \times \sigma_{O_f,Square}}.$$

Résultat de MIA dans le Domaine Fréquentiel



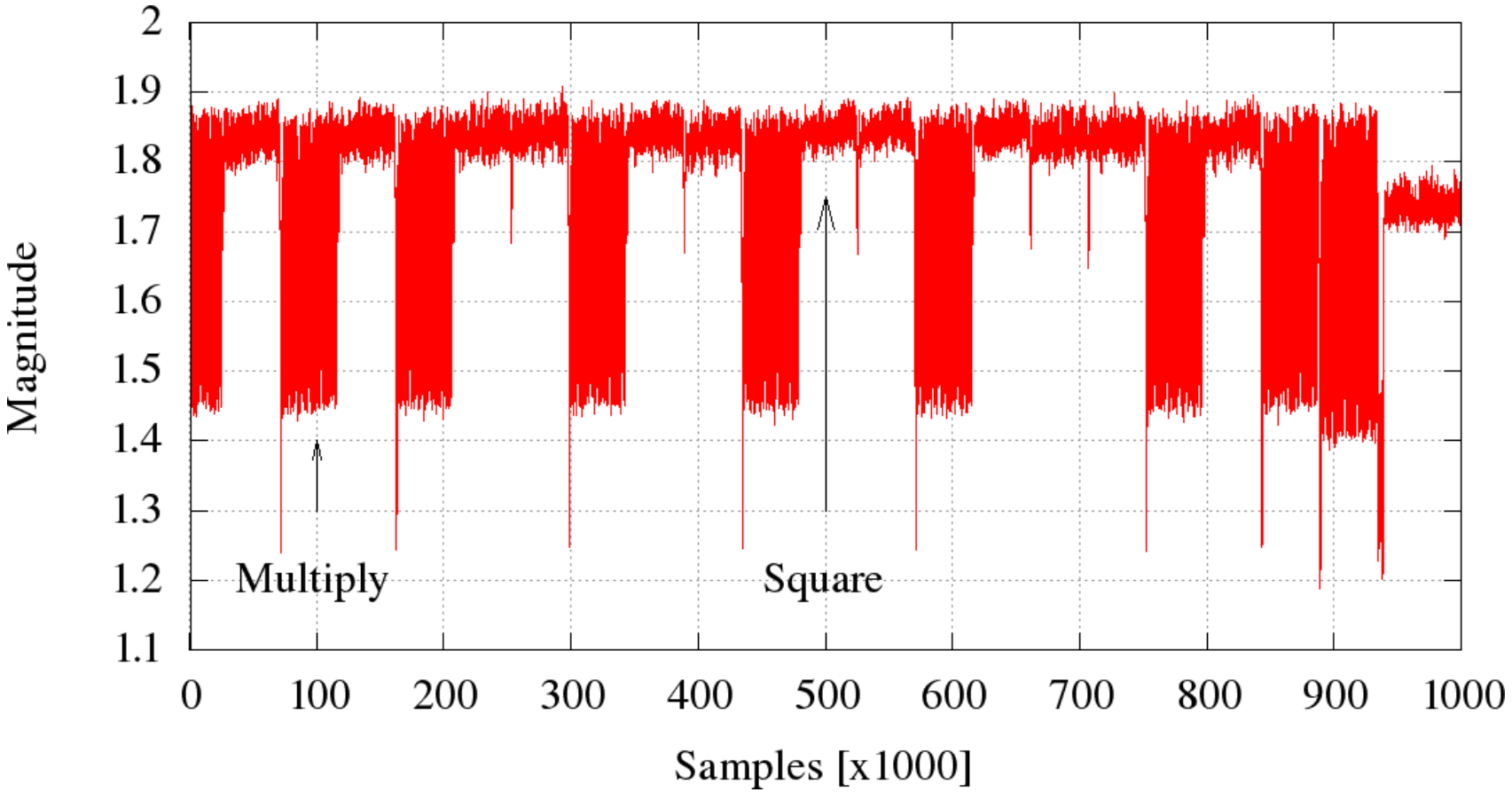
Démodulation à ces différentes fréquences

Émanations Non Intentionnelles

Décrites par Agrawal: Résultat d'une modulation entre une porteuse et l'information sensible.

$$Ms(t) = A \cdot \cos(2\pi f_c t) \cdot [1 + m \cdot v(t)],$$

où f_c la fréquence de porteuse, $v(t)$ le signal informatif A l'amplitude m le coefficient de modulation



Les Émanations Directes

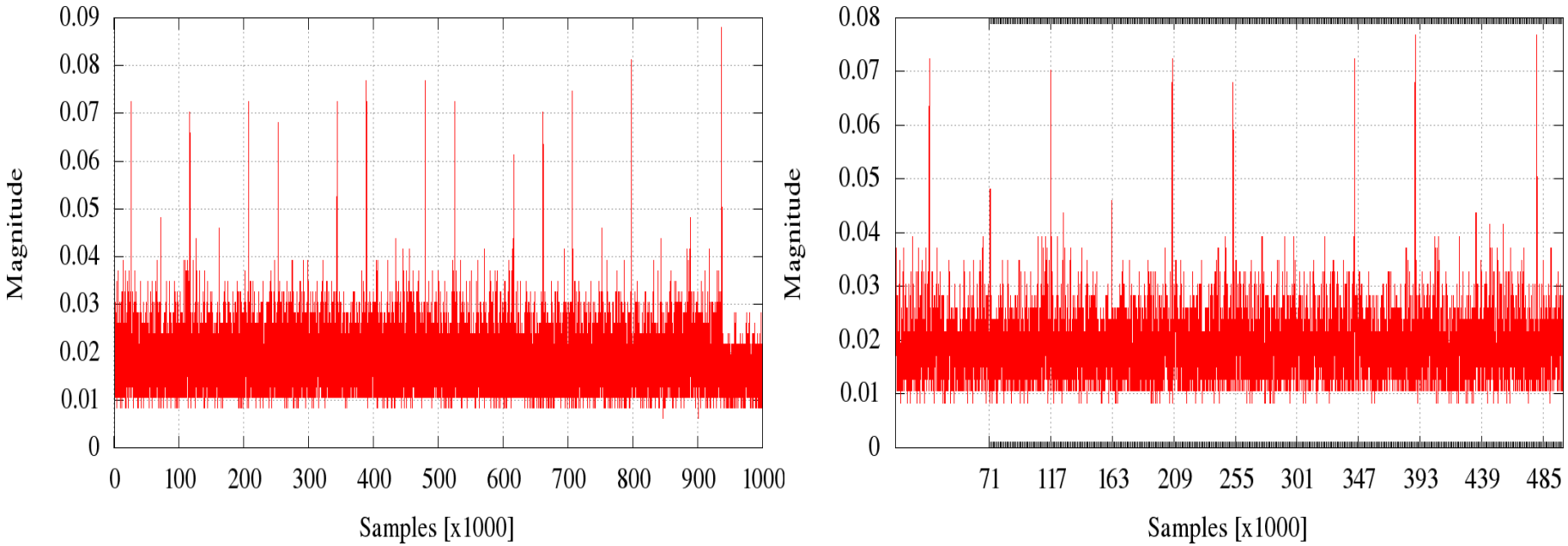


Figure 7: Démodulation à 34MHz

Les Émanations Directes

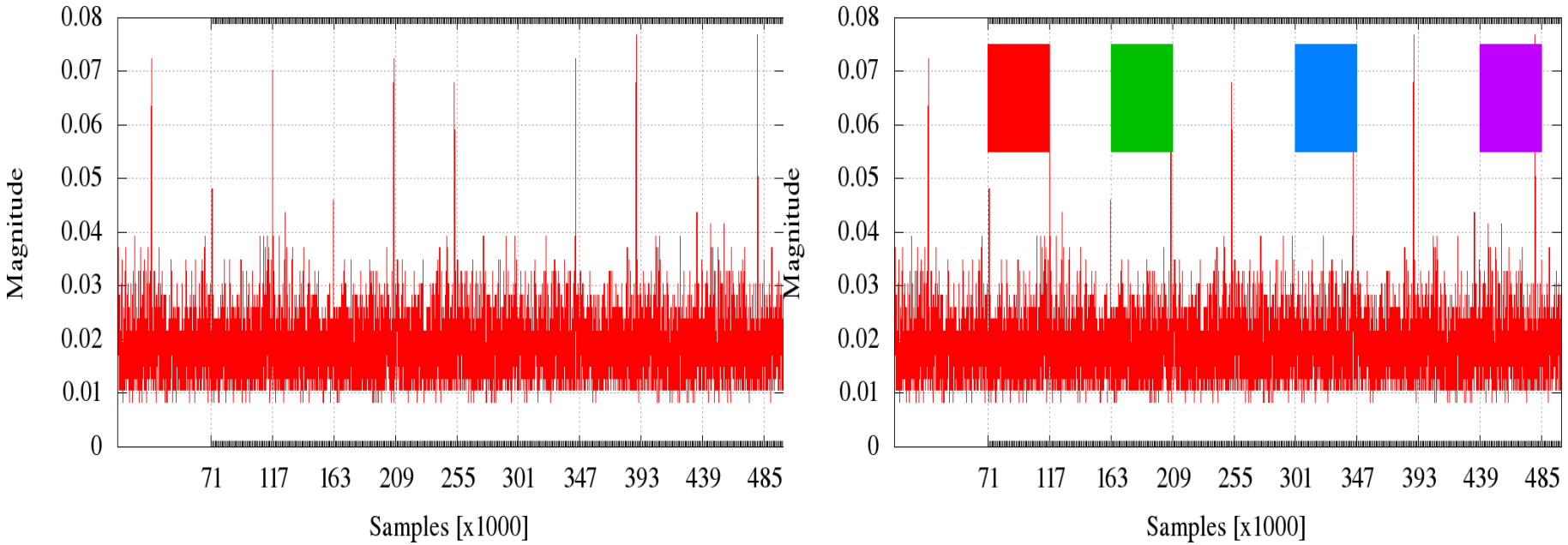


Figure 8: Démodulation à 34MHz

Les Émanations Directes

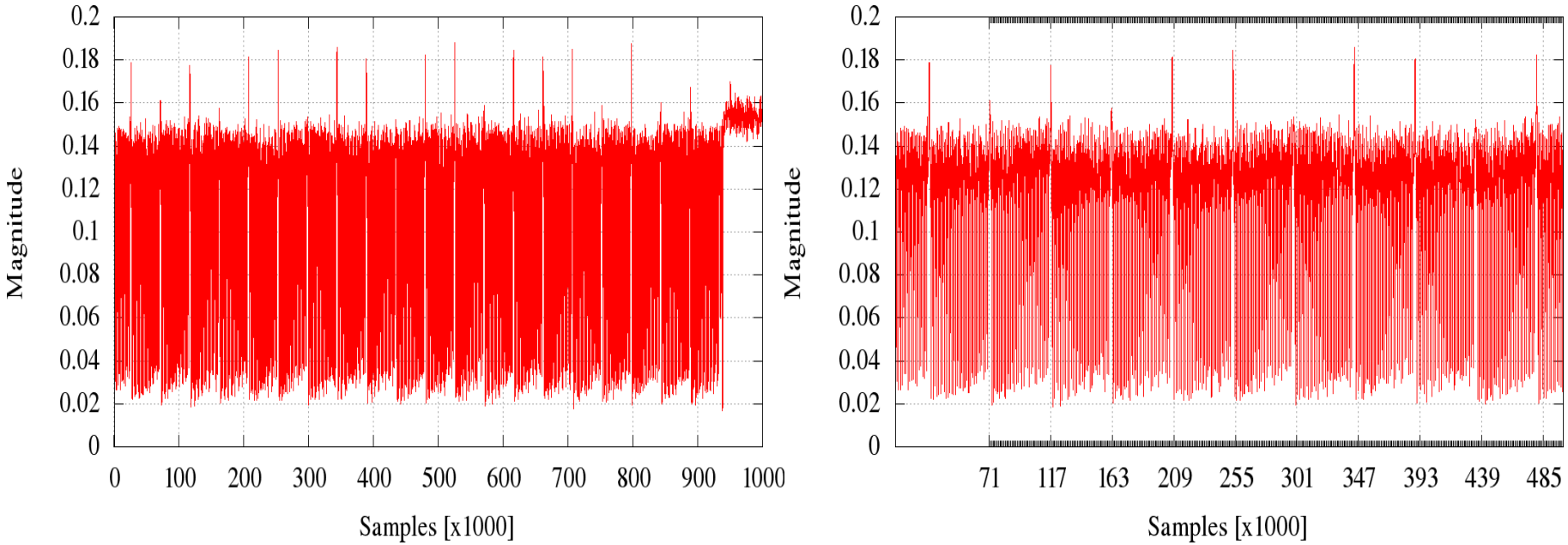


Figure 9: Démodulation à 54MHz

Les Émanations Directes

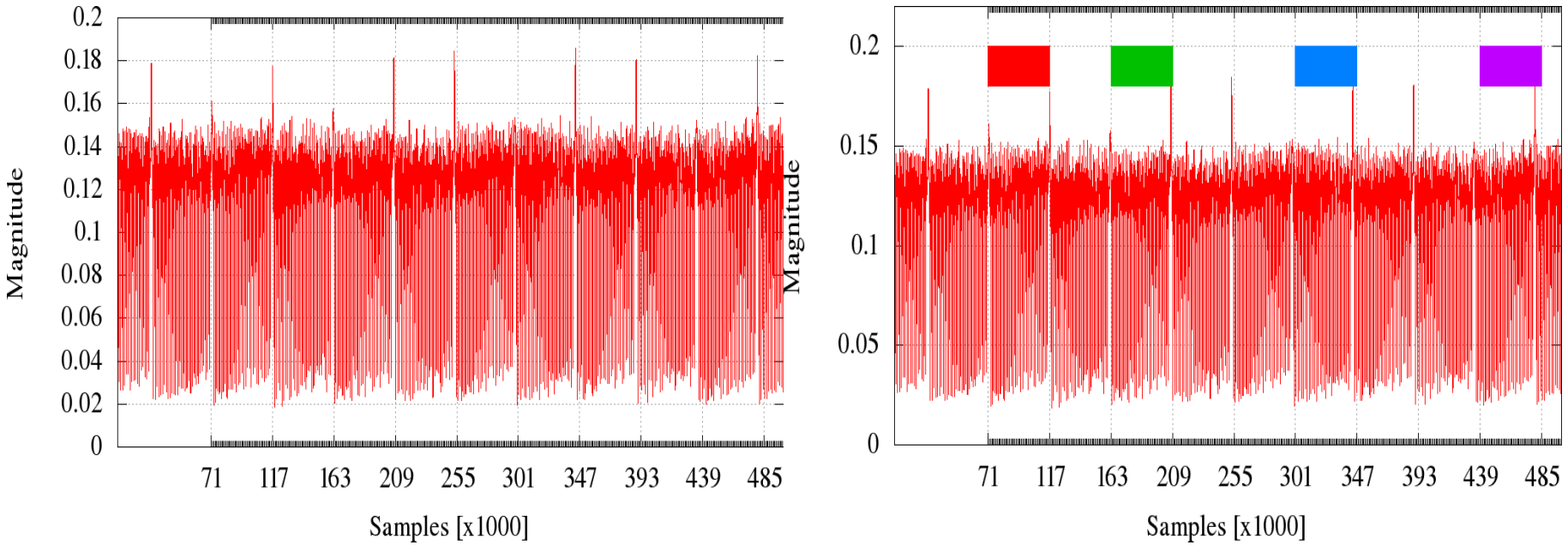


Figure 10: Démodulation à 54MHz

Presentation Outline

Travaux en cours : Origines de ces Fréquences Sensibles

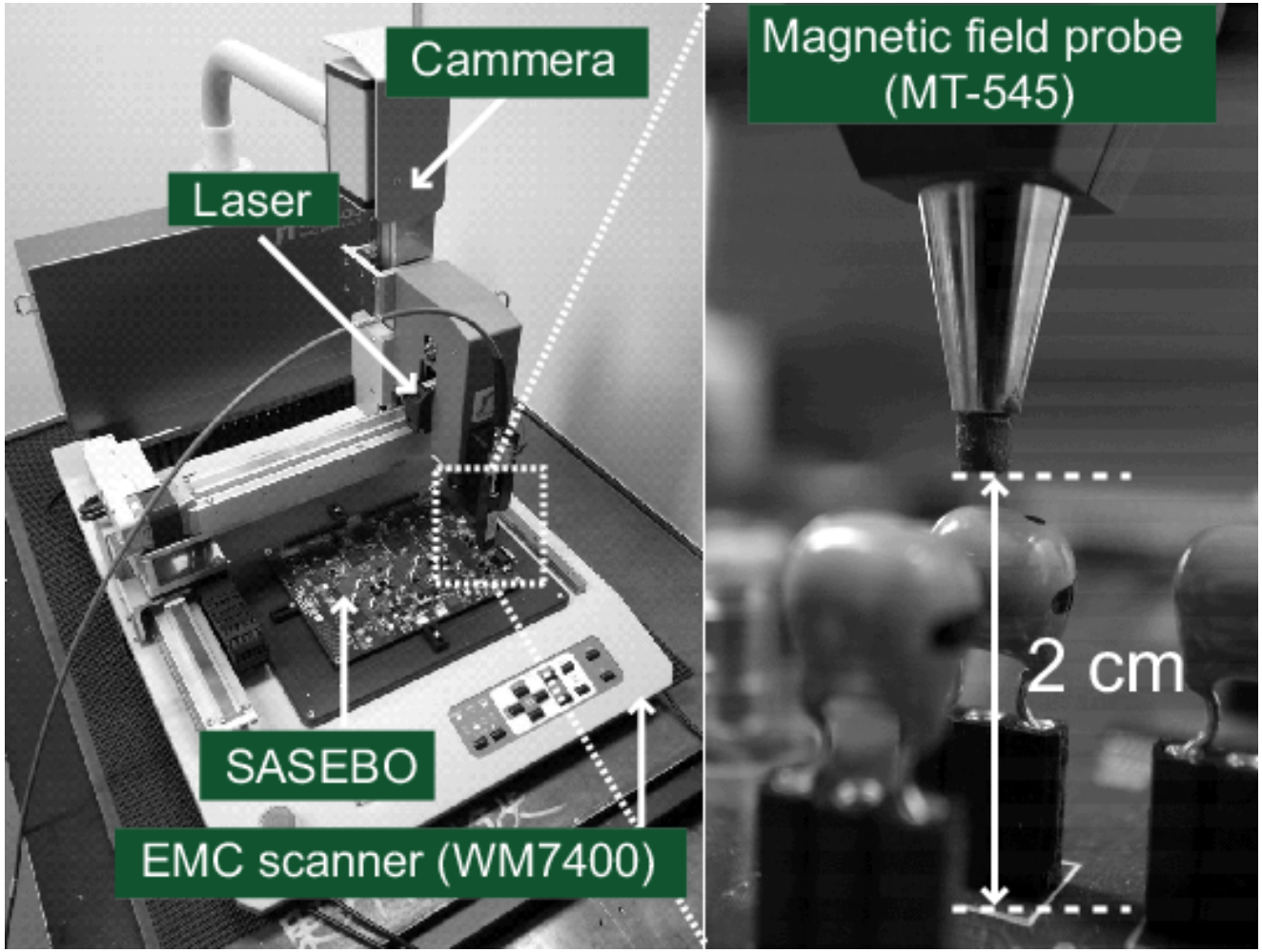
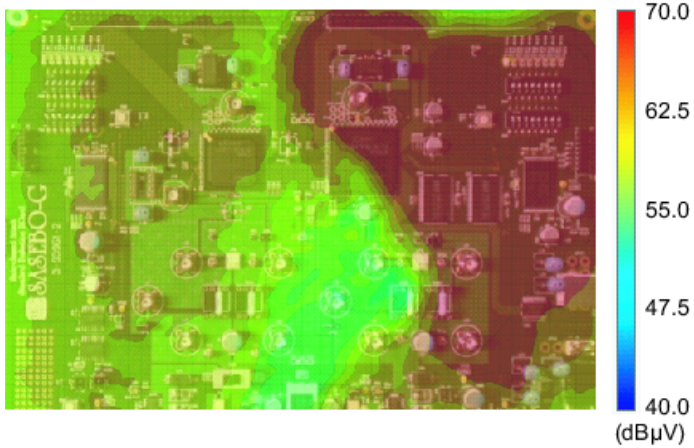


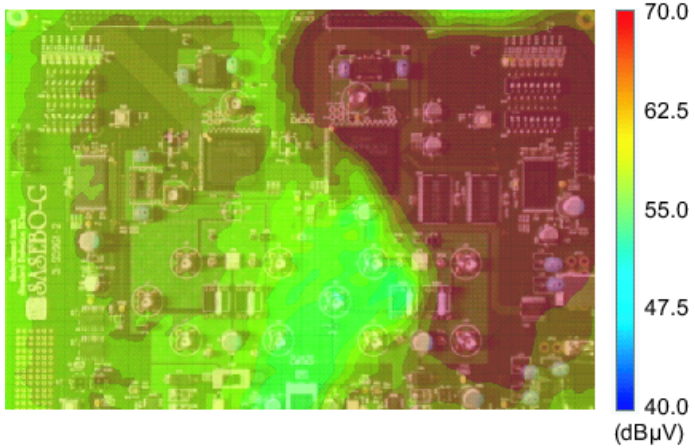
Figure 11: EM measurement system.

Travaux en cours : Origines de ces Fréquences Sensibles

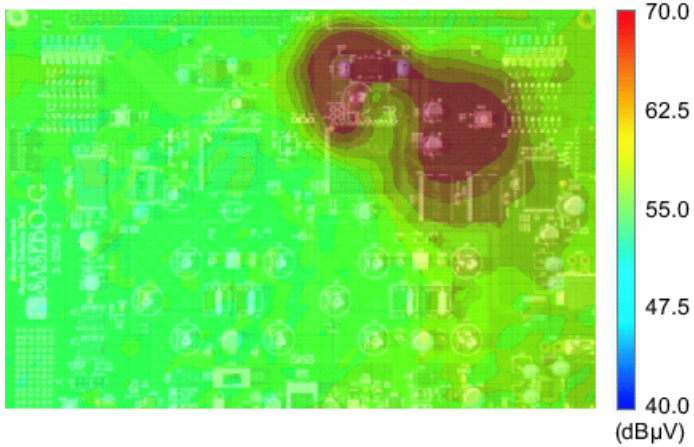
EM-field maps: 10-100 MHz



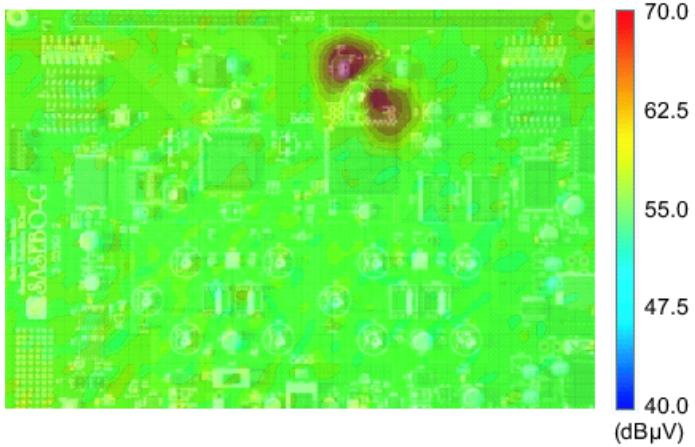
EM-field maps: (a) 100-200 MHz



EM-field maps: (a) 200-300 MHz

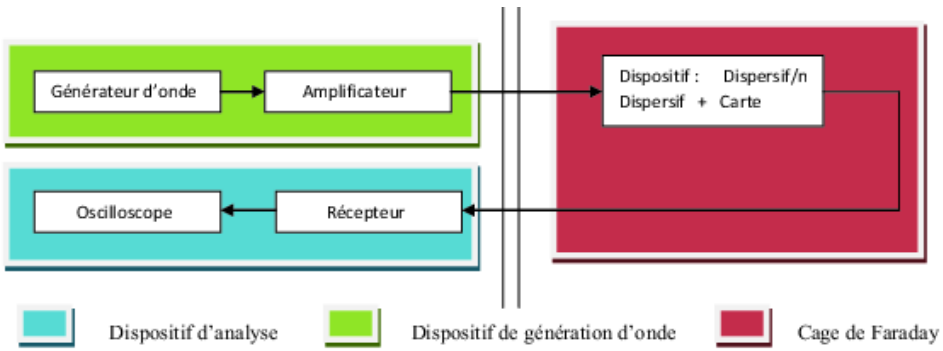


EM-field maps: (a) 300-400 MHz



Travaux en cours: Utilisations des Fréquences Sensibles en Rayonné

Schéma de Principe



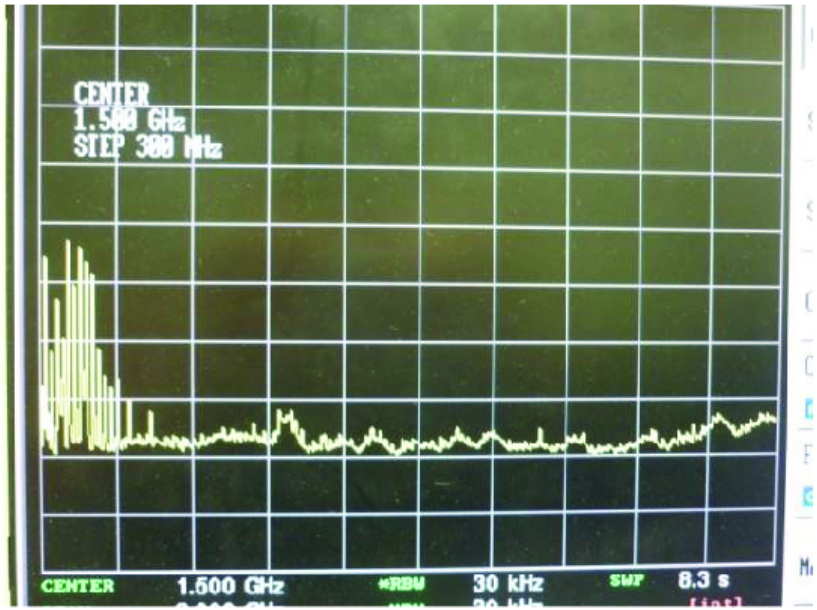
Dispositif Réel

Dispositif expérimental

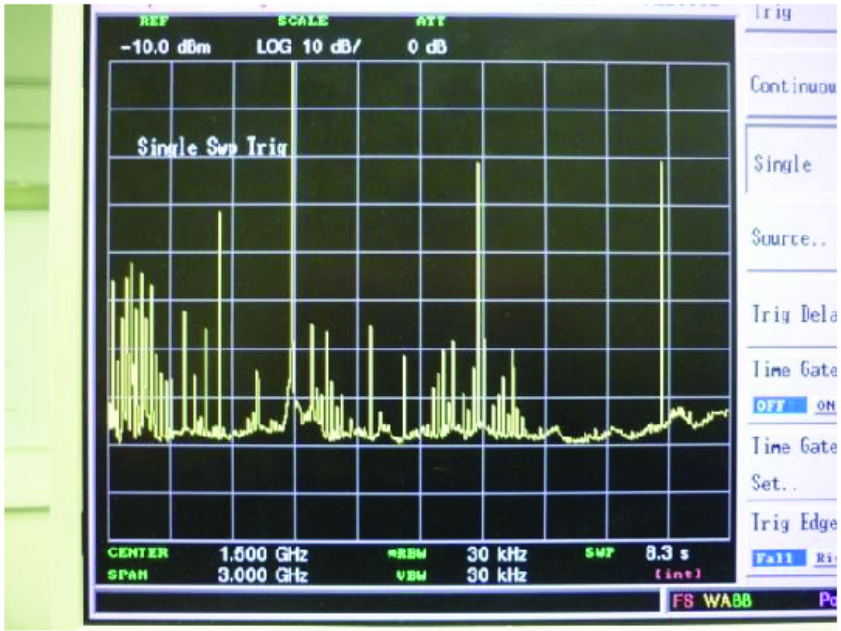
- Utilisation d'une stripeline,
- Utilisation d'un coupleur,
- Champ généré de l'ordre de 150V/m, 12dBm. (Fatal au composant)

Travaux en cours : Utilisations des Fréquences Sensibles en Rayonné

Spectre en passif



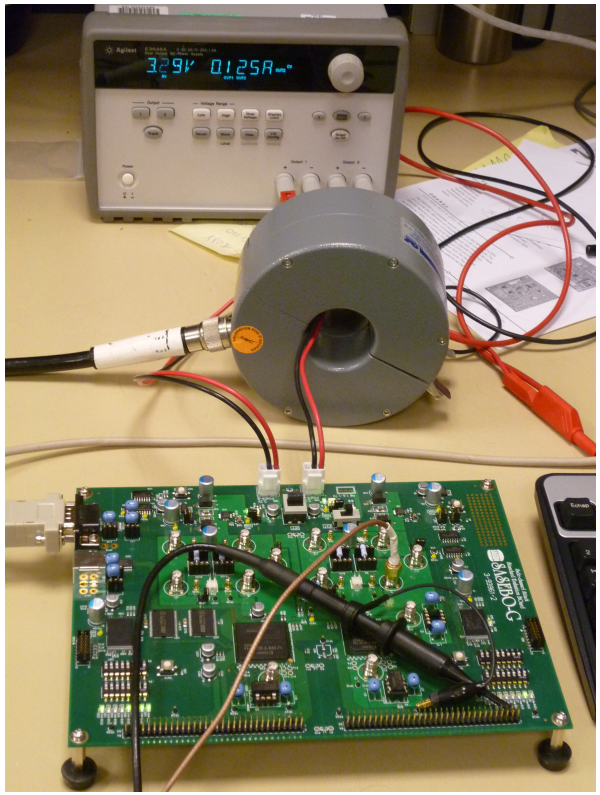
Spectre en injectant une porteuse



Puissance injectée trop forte $\Rightarrow$ détérioration du composant, impossibilité de démoduler.

Un compromis : Puissance Injectée / Réaction du composant ?

Travaux en cours : Utilisations des Fréquences Sensibles en Conduit



Dispositif expérimental

- Porteuse injectée sur l'alimentation continue
- Puissance nécessaire de l'ordre de $130 dB\mu V$
- Attaques en fautes, amélioration de l'EMA ...

Presentation Outline

Conclusion

- Nous avons montré à travers ces 2 exemples l'intérêt de démoduler des signaux brutes
- Nous proposons une méthode générique que nous pouvons appliquer sur un système et sur un composant.
- Cette méthode ne se substitue pas à une évaluation TEMPEST mais livre un diagnostique rapide de l'état de compromission potentiel des cibles,
- Nous illustrons cette méthode par une étude fréquentielle sur des signaux et sur des opérations.
- Il est maintenant intéressant d'étudier les causes de ces phénomènes et les fréquences de sensibilité de ces composants.
- Utilisation de fréquences de sensibilité des composants pour les mettre en défaut attaque par injection de Fautes, amélioration de l'EMA.

Collaborations

- **DGA MI (CELAR) Bruz**, Denis REAL
- **Université de Tohoku, Sendaï, Japon, Projet SPACES,** Naofumi HOMMA, Yu-ichi HAYASHI
- **ANSSI** Karim KHALFALLAH, Emmanuel DUPONCHELLE

MERCI
DES QUESTIONS ?