Characterization and use of the EM radiation to enhance side channel attacks

Olivier Meynard

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2012-ENST-002

EDITE - ED 130

Télécom-ParisTech - PARIS
École Doctorale EDITE
Informatique Télécommunications et Électronique de Paris

Thèse de Doctorat

Mention : Électronique et Communications

Olivier Meynard

Caractérisation et utilisation du rayonnement électromagnétique pour l'attaque de composants cryptographiques

Le 18 Janvier 2012

Jury :

Rapporteurs :	Christophe Clavier	-	Université de Limoges
	Pierre-Alain Fouque	-	École Normale Supérieure Paris
Directeurs :	Jean-Luc Danger	-	Telecom-ParisTech
	Sylvain Guilley	-	Telecom-ParisTech
	Denis Réal	-	DGA-MI
Examinateurs :	Éliane Jaulmes	-	ANSSI
	Lionel Torres	-	Lirmm Montpellier
	Naofumi Homma	-	Tohoku University
Invité :	Frédéric Valette	-	DGA-MI.

THÈSE

à Nono

Remerciements

Cette thèse constitue pour moi une étape importante dans ma vie personnelle et professionnelle. Ce rapport expose les principales contributions que j'ai effectuées durant trois années au sein du Laboratoire COMELEC/SEN de Telecom-ParisTech et de la DGA/ MI à Bruz. Je voudrais tout d'abord remercier Pierre-Alain Fouque et Christophe Clavier qui ont accepté de relire et rapporter ce travail de thèse. Je remercie ensuite Naofumi Homma, Lionel Torres, Frédéric Valette, Éliane Jaulmes pour leur participation à mon jury de thèse.

J'adresse aussi mes vifs remerciements à Jean-Luc Danger, Sylvain Guilley et Denis Réal mes directeurs et encadrants de thèse. Merci à Jean-Luc pour avoir pris en considération mon dossier pour cette thèse et soutenu ma candidature pour un financement DGA-CNRS. Merci aussi à Denis et Frédéric pour m'avoir permis de réaliser certaines expériences au sein de DGA-MI et bénéficier de moyens techniques importants notamment avec le laboratoire TEMPEST. Je tiens à exprimer plus particulièrement ma profonde gratitude à Sylvain, pour la qualité de son encadrement et sa bienveillance tout au long de ce travail de recherche, et pour m'avoir transmis en quelque sorte, la passion de ce métier.

Mes remerciements vont aussi à nos amis Japonnais Naofumi et Yu-ichi, avec qui nous avons eu des échanges très enrichissants, sur le plan scientifique et humain. Je remercie les doctorants, maître de conférence et personnels de Telecom-ParisTech : Shivam, Florent, Aziz, Nidal, Chady, Youssef, Taoufik, Houssem, Laurent et en particulier Tariq Graba pour sa présence, ses bons conseils "trucs et astuces"... Je suis aussi reconnaissant aux équipes du CELAR pour leur bon accueil en terre bretonne pour ne citer qu'eux : Julien, Delphine, Denis, Pierrick, Yvon, Pascal, Daniel, Cyril ...

Enfin je n'oublierai pas ma famille et mes amis les plus proches toujours aussi fidèles ...

Résumé de la thèse en français

Ce manuscrit de thèse s'articule en quatre parties. Dans une première partie, nous exposons les bases de la cryptographie moderne et les différentes notions qui seront utilisées dans les parties suivantes. Dans une deuxième partie nous étudions plus spécifiquement le rayonnement électromagnétique, les différents modèles de fuite pour l'étude de canaux auxiliaires. Nous envisageons aussi l'analyse du rayonnement électromagnétique dans des conditions très dégradées de mesure, lors de mesures à distance du rayonnement électromagnétique émis par un composant électronique. Dans une troisième partie, nous utilisons une représentation dans l'espace des fréquences afin de retrouver des fréquences de compromission donc porteuses d'information, qui grâce à du matériel de démodulation nous permettra de retrouver une partie de l'information. Enfin en quatrième partie après avoir étudié la susceptibilité de matériel électronique cryptographique soumis à une onde électromagnétique, nous proposons des méthodes permettant de produire des attaques en fautes.

Première Partie

Chapitre 1 : Introduction

Du grec kryptos caché et graphein écrire la cryptographie trouve ses origines dans l'antiquité. La cryptographie a pour objectif principal de chiffrer de l'information, afin que deux interlocuteurs puissent communiquer sans qu'un intercepteur puisse déchiffrer et espionner cette communication. Pour cela en cryptographie moderne il existe des algorithmes mathématiques capables de sécuriser la communication et garantir :

- la confidentialité,
- l'authenticité
- et l'intégrité,

des échanges. Ces algorithmes reposent sur l'utilisation de secrets ou de clés. Il existe deux types d'algorithmes cryptographiques. Les plus anciens sont les algorithmes cryptographiques dits symmétriques : l'émetteur et le recepteur partagent la même clé. On parlera de chiffrement symmétrique ou à clé privée. La cryptographie morderne a vue naître au XX^e siècle le chiffrement à clé privée ou asymmétrique : émetteur et récepteur disposent chacun d'une clé privée et utilise une clé publique. La clé publique sera utilisée pour chiffrer un message, alors que la clé privée qui doit rester confidentielle sera utilisée pour le déchiffrer.

Dans la suite nous utilisons principalement l'AES Advanced Encryption Standard comme algorithme cryptographique symétrique et le RSA Rivest Shamir Adelman comme algorithme de chiffrement asymétrique.

Ces algorithmes cryptographiques réputés sûrs d'un point de vue mathématiques deviennent vulnérables du fait de leur implantation sur des composants électroniques comme par exemple les FPGA, les cartes à Puce : ces objets qui envahissent peu à peu notre vie quotidienne.

En effet l'étude de grandeurs physiques durant le calcul de chiffrement telles que :

- le temps de calcul,
- la consommation de courant,
- le rayonnement électromagnétique,

nous renseigne sur le fonctionnement du composant, et donne des indices à un attaquant pour retrouver les éléments secrets. On peut par exemple à l'aide d'une capture de consommation de courant retrouver les opérations effectuées par un composant exécutant un calcul de type RSA et par ce biais retrouver la séquence secrète de bit composant la clé privée. On nommera cette attaque SPA "Simple Power Analysis". Une autre méthode appropriée dans le cas de chiffrement symétrique est de collecter un nombre conséquent de mesures de consommation de courant et de réaliser des calculs statistiques basés sur l'utilisation du coefficient de Pearson. On pourra ainsi calculer un coefficient de correlation entre une hypothèse sur le secret et la mesure de consommation de courant produite par le composant traitant de l'information sensible. A partir de ces éléments nous serons en mesure d'identifier l'élément secret (*i.e* la bonne hypothèse ayant le coefficient de corrélation le plus élevé avec les mesures de consommation). On parlera dans ce cas de CPA "Correlation Power Analysis".

Ces méthodes sont qualifiées de passives ou par observations étant donné qu'il n'y a pas d'interaction directe avec le composant, a contrario il existe des attaques dites actives. Ces attaques ont pour objectifs de modifier le comportement du composant électronique chiffrant afin qu'il génère des fautes de chiffrements exploitables par un attaquant qui pourra déduire le secret. Ces attaques peuvent être réalisées en agissant sur la consommation, l'horloge ou encore en exposant le composant à des impulsions lumineuses notamment le laser. Face à ces menaces, les concepteurs et fabricants de composants électroniques sécurisés ont mis au point des parades ou contre mesures. Il existe des contre mesures algébriques comme par exemple l'échelle de Montgormery. Des contre mesures basées sur le masquage peuvent aussi être proposées : une valeur aléatoire générée est ajoutée aux calculs de chiffrement. La logique double rail est aussi une contre mesure efficace face aux attaques par canaux auxiliaires et attaques en fautes.

Deuxième Partie

Dans cette deuxième partie nous étudions le rayonnement électromagnétique. Nous présenterons tout d'abord les modalités et les outils mathématiques utilisés pour quantifier, caractériser ce rayonnement afin de retrouver des éléments secrets traités par le composant. Dans le Chapitre 3, nous exposons des résultats de recherche concernant des attaques par canaux auxiliaires à distance du composant électronique. Nous proposons différentes méthodes afin d'améliorer le rapport signal à bruit et augmenter le temps de calcul et de traitement de ces attaques.

Chapitre 2 : Fuite électromagnétique

Dans ce chapitre nous introduisons et décrivons le rayonnement électromagnétique. Nous distinguons deux types de rayonnement

- les émanations directes
- les émanations indirectes.

Les émanations directes ou intentionnelles proviennent de l'activité des bascules et portes logiques du composant électronique. Ces éléments commutent à de très hautes fréquences avec des temps de montée de l'ordre de 1 ns. On pourra collecter ce type d'émanation à très faible distance du composant avec un oscilloscope disposant d'une fréquence d'échantillonnage de l'ordre du GHz. Nous aurons ainsi une idée de la consommation du composant en bande de base.

Les émanations indirectes quant à elles, proviennent de modulations ou intermodulations intrinsèques au composant : par exemple l'horloge et ses harmoniques peuvent générer des phénomènes de couplage entre une donnée et une porteuse. Elles sont alors observables à distance du composant en créant des phénomènes de modulation d'amplitude. Dans le cas d'attaques statistiques : un attaquant peut modéliser le rayonnement électromagnétique en fonction des données calculées. Il utilise pour cela un modèle en distance de Hamming ou en poids de Hamming. Après avoir collecté un nombre conséquent de mesures et grâce à ce modèle, il établit en fonction de différentes hypothèses de clés un partitionnement de ces mesures. Ensuite grâce à un distingueur : le coefficient de Pearson dans le cadre de la CPA (Corrélation Power Analysis) ou encore l'information mutuelle en théorie de l'information, l'attaquant est en mesure de retrouver la bonne hypothèse de clé.

Afin d'améliorer ces attaques, différentes études ont été menées notamment sur l'amélioration des distingueurs mais aussi concernant des modèles de fuite. Des travaux au sujet de la combinaison des modèles de fuite sont proposés dans cette thèse.

Chapitre 3 : Attaques Electromagnétiques de composants crytpographiques à distance

Dans ce Chapitre nous décrivons une attaque statistique de type CEMA (Corre-

lation ElectroMagnetic Analysis) réalisée sur une carte SASEBO-G implémentant un AES à 50 cm. Nous réussissons avec un nombre conséquent de mesures du rayonnement électromagnétique à 50 cm à retrouver certains octets du secret sans matériel additionnel de type récepteur. Nous décrivons la dégradation du signal de fuite lié au secret en fonction de la distance et du bruit environnant. Ensuite nous proposons une étude de l'évolution du modèle de fuite en fonction de la distance. Nous constatons que le modèle en distance de Hamming se détériore avec la distance. Afin d'améliorer la qualité du signal nous proposons d'utiliser des méthodes de recherche de point d'intérêt publiées par Gierlich sosd, sost. Il apparaît que dans un contexte d'attaque électromagnétique à distance ces méthodes sont difficiles à mettre en place. Nous utilisons alors un calcul de corrélation de Pearson afin de déterminer ces points d'intérêts, nous vérifions aussi que ces échantillons temporels contiennent de l'information et qu'ils sont indépendants de la valeur du secret.

$$\hat{\rho}_{\text{combined}} \doteq \prod_{t \in \text{Sample}\{1,2,3,4\}} |\hat{\rho}_t|$$

Un calcul basé sur le produit des coefficients de corrélation obtenus en ces échantillons nous permet d'améliorer considérablement l'attaque en terme de taux de succès compte tenu du nombre de mesures.

Troisième Partie

Chapitre 4 : TEMPEST

Initialement le programme TEMPEST fut lancé par le gouvernement américain afin d'étudier, caractériser le rayonnement électromagnétique produit par les équipements électroniques et ensuite produire des méthodes d'évaluation et un standard. En effet les émanations produites par un équipement électronique peuvent donner des indices sur le signal rouge traitant de l'information confidentielle. Des recommandations de conception doivent être alors suivies par les fabricants d'équipements électroniques. Ces méthodes bien connues du monde de la compatibilité électromagnétique sont par exemple : le revêtement anti-rayonnement, le filtrage des signaux, l'isolation des bus de données. Les équipements doivent ensuite être soumis à une évaluation TEMPEST afin de vérifier la conformité de l'équipement avec la Norme TEMPEST. Durant ces évaluations, est mesurée la difficulté qu'aurait un attaquant à retrouver le signal de données confidentielles en captant une émanation électromagnétique. Ces évaluations sont réalisées à l'aide d'un récepteur TEMPEST. Lors de ces évaluations on considère les émanations en modulation d'amplitude et modulation de fréquence. Ces récepteurs large bande disposent d'étage de préamplification permettant d'affiner le réglage du Gain sur des bandes de fréquences allant de quelques kHz à 500 MHz, et nous pouvons

balayer le spectre de quelques kHz au GHz.

Chapitre 5 : Caractérisation des fréquences de compromission d'un clavier

Reconnaissance à distance des touches d'un clavier et adaptation de méthodes de cryptanalyse à la caractérisation de bandes de fréquences sensibles. Afin de comprendre ces phénomènes de modulation, nous avons adopté un modèle simple basé sur la reconnaissance des touches d'un clavier, à distance. Un clavier PS/2 est connecté à un ordinateur. Une antenne fouet est disposée à distance de ce dispositif et est connectée à un récepteur/ démodulateur comme représenté sur la figure 1. Nous sommes alors capables de retrouver la touche sur laquelle l'utilisateur a appuyé si le récepteur est réglé sur la bonne fréquence de démodulation. Pour mener à bien ce type d'évaluation, nous avons utilisé des récepteurs TEMPEST dans les laboratoires du CELAR. Nous avons aussi adapté les méthodes traditionnellement appliquées en cryptanalyse à ce modèle afin de détecter les plages de fréquences où l'information est présente, et donc les plages de fréquences où des compromissions sont potentiellement présentes.

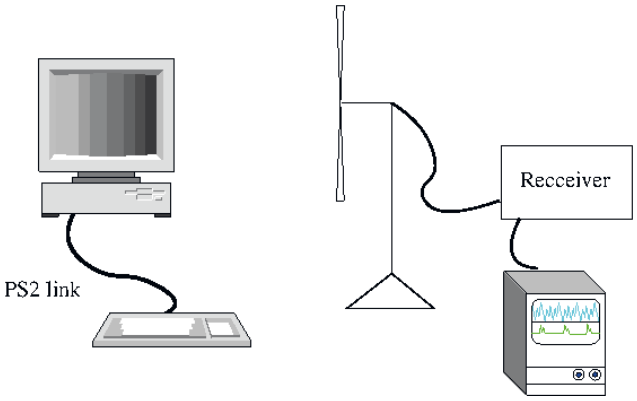


Figure 1: Dispositif expérimental : reconnaissance d'un mot de passe

Ainsi grâce à ces calculs statistiques basés sur la CPA (Corrélation Power Analysis), sur la théorie de l'information et la MIA (Mutual Information Analysis) nous réussissons à mettre en évidence ces plages de fréquences comme présenté sur la figure 2.

Un attaquant muni alors d'un dictionnaire établissant la correspondance entre les touches d'un clavier et leur signature électromagnétique est en mesure avec un récepteur réglé en démodulation d'amplitude de retrouver les touches tapées sur un clavier. Nous avons développé aussi un outil logiciel nous permettant d'émuler le fonctionnement du récepteur matériel (ou démodulateur), en effectuant un filtrage passe bande.

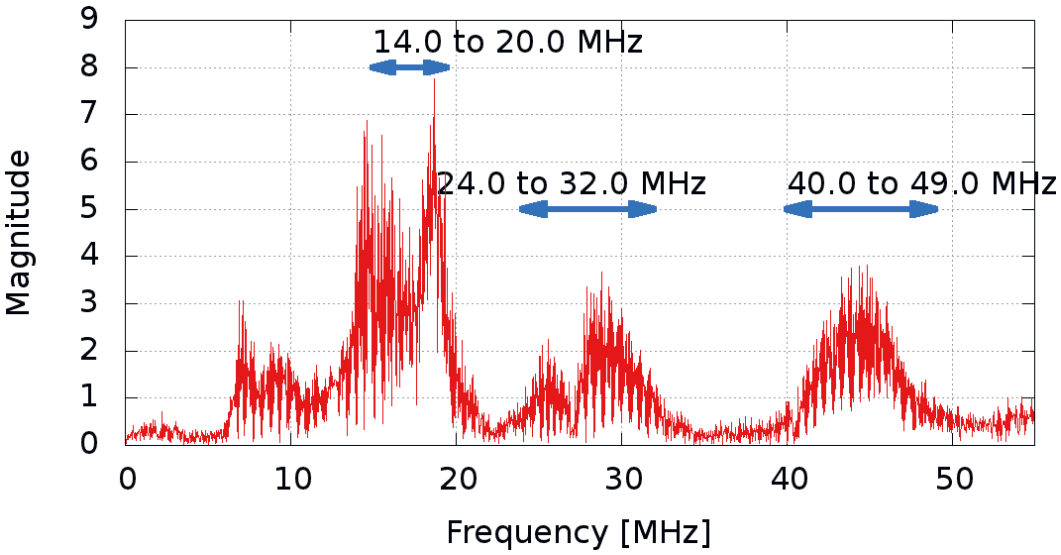


Figure 2: Caractérisation fréquenctielle du signal obtenu par Corrélation et par théorie de l'information.

Chapitre 6 : Caractérisation fréquentielle pour l'amélioration de la SEMA

Attaques par Démodulation, sur un algorithme de cryptographie asymétrique RSA Il s'agit d'étendre et d'appliquer les méthodes précédemment utilisées pour la caractérisation d'un système ; à un composant cryptographique. Nous avons alors adapté les techniques mises au point sur la reconnaissance des touches d'un clavier à une cible cryptographique. Nous avons pour cela choisi une implémentation du RSA implémentée sur la carte SASEBO-G. Le RSA est un algorithme de cryptographie asymétrique basé sur l'exponentiation modulaire caractérisée par deux opérations de mise au carré Square et de multiplication Multiply selon le bit de clé. Ainsi si nous distinguons les opérations de Square des opérations de Multiply nous sommes en mesure de retrouver la clé secrète comme représenté sur la figure 3.

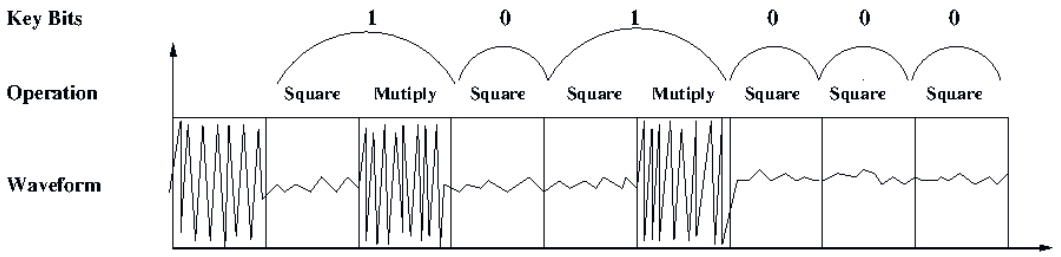


Figure 3: Schéma de principe RSA et ses opérations de Square & Multiply.

Nous avons utilisé la méthode basée sur la théorie de l'information afin de caractériser dans le domaine fréquentiel le signal de fuite du composant. Différentes bandes de fréquences porteuses d'information sont alors exhibées. Nous avons montré que la démodulation à la fréquence du composant apportait une réelle amélioration dans le cadre d'attaque par SEMA (Simple ElectroMagnetic Analysis). Différents types de compromission ont ainsi pu être mis en évidence :

- compromission en démodulant à la fréquence de fonctionnement du composant et à ses harmoniques,
- compromission à des fréquences différentes de celles liées au fonctionnement du composant.

Nous sommes ainsi en mesure d'établir le profil spectral d'une cible cryptographique.

Quatrième Partie

Chapitre 7 : Attaques ElectroMagnétiques actives de composants cryptographiques

Ce dernier chapitre est consacré à l'attaque active de composants cryptographiques par exposition du composant à un champ électromagnétique et/ou à une onde électromagnétique. Nous explorons différentes techniques d'exposition d'un composant cryptographique à un champ électromagnétique notamment avec l'utilisation de stripline. Ces techniques sont utilisées dans le domaine de la compatibilité électromagnétique. Nous avons aussi utilisé une sonde afin de générer une porteuse sur l'alimentation du composant cryptographique. Nous avons constaté qu'une onde électromagnétique générée sur les câbles d'alimentation d'un composant cryptographique pouvait générer des fautes exploitables au sens de Piret Quisquater pour déduire la clé secrète d'un AES. Cette méthode a été validée sur une carte SASEBO-G où le quartz de la carte était perturbé par l'onde générée. Une étude de caractérisation du composant a été menée afin de déterminer les fréquences sensibles du composant. Nous avons ensuite appliqué cette méthode sur un ASIC dédié au chiffrement DES. Nous générons des perturbations sur l'alimentation.

List of Figures

1 Dispositif expérimental : reconnaissance d'un mot de passe 9
2 Caractérisation fréquenctielle du signal obtenu par Corrélation et par théorie de l'information. 10
3 Schéma de principe RSA et ses opérations de Square & Multiply. . . 10

1.1 Feistel global structure 7
1.2 9th round of the AES. 9
1.3 RSA power supply consumption on a FPGA. 13
1.4 EM radiation of DES computation on an FPGA 14

2.1 Conventional side-channel: voltage drop. 22
2.2 Image of common-mode current. 23
2.3 CMOS Cell 25
2.4 Attack on the first round of DES with different models. 31
2.5 Mutual information estimated on each sample of the DES acquisition campaign. 32
2.6 Success rate comparison between mono-partitioning models M1, M2 and combined model M3 for 1,000 traces per class. 33

3.1 EM measurement test bench with its antenna on a plastic rod. . . . 36
3.2 Studied AES Architecture. 37
3.3 Quasi-homothetic downscale of the raw curves at different distances. 37
3.4 CEMA curves obtained for random cleartexts measurements at different distances and evolution of the maximal correlation value with distance. 39
3.5 Standard deviation of the signal and of the environmental noise. . . . 39
3.6 CEMA on sbox #1 at a distance $d = 50$ cm. 40
3.7 Hamming distance at 0 cm and at 15 cm. 40
3.8 Model at 50 cm for the Sbox #1. 41
3.9 Correlation traces for campaign at 0 cm and 25 cm,right key hypothesis 42
3.10 Sosd and Sost at 0 cm right key hypothesis 43
3.11 Sosd and Sost at 25 cm,right key hypothesis 44
3.12 I(O;l) for campaign at 0 cm and at 25 cm,right key hypothesis 44
3.13 Success rate of the CPA after PCA pre-processing at 0cm (*on the left*) at 25cm (*on the right*). 46
3.14 Correlation traces obtained for the right key hypotheses and for incorrect key hypotheses at 25 cm. 47
3.15 (a): Success rate of product of 2-samples correlation attack, and product of 4-samples of correlations attack; (b): Success rate of product of 3-samples correlation attack, and product of 4-samples of correlations attack. 49

3.16 Comparison of success rates between Eqn. (3.1) with (a) mono-sample attacks and (b) pre-treatment by PCA. 50
3.17 Differential traces obtained for the Sbox#2 using measurements from the DPA Contest v2 public database. 51
3.18 Success rate of Eqn. (3.1). 51

4.1 Level A Screen Monitor, Level A Power Supply (EMI suppression filter) *source www.sst.ws* 58
4.2 Bi-conical Antenna(20 MHz to 200 MHz), Double Ridge Horn Antenna (200 MHz to 2 GHz)(*source www.dynamicsciences.com*) 59

5.1 Setup used for the keyboard eavesdropping. 62
5.2 PS/2 protocol, involved in the keyboard to computer communication. 63
5.3 Spectrum of the black emanation. 64
5.4 Red signal/Black emanation. 65
5.5 Results of the Correlation for every state. 67
5.6 Result of Mutual Information Metric I(f; $State$). 69
5.7 The four eigenvectors obtained by PCA. 71
5.8 R-1250 wide-range receiver and its preselector and wide-band AM detector, *source M Kuhn Thesis* 73
5.9 Design of bandpass filter. 73
5.10 Results of demodulation (red signal, and black signal demodulated at 17.0 MHz, 27.0 MHz. 76
5.11 Results of demodulation (red signal, and black signal demodulated 41.0 MHz and 36.0 MHz). 77
5.12 Results of software demodulation between 14-20 MHz,21-27 MHz(No Signal) and 24-32 Mhz. 78
5.13 Results of software demodulation between 35.5-36.5 MHz(No Signal) and 40-49 MHz. 79

6.1 SEMA principle on RSA. 83
6.2 Overview of SASEBO-G. 83
6.3 EM measurement system. 84
6.4 EM-field map over FPGA2. 85
6.5 Frequency characteristics of EM radiation over four points over FPGA2. 86
6.6 EM-field maps: (a) 10-100 MHz, (b) 100-200 MHz, (c) 200-300 MHz, and (d) 300-400 MHz. 86
6.7 EM-field map at 24 MHz. 87
6.8 EM waveforms of: (a) point 1, (b) point 2, and (c) point 3. 88
6.9 Demodulated EM waveforms of: (a) point 1, (b) point 2, and (c) point 3. 89
6.10 EM loop on the SASEBO Board during an RSA computation. 90
6.11 Direct EM radiations emitted during an RSA computation. 90
6.12 EM measurement split into Square and Multiply parts. 91

6.13 Result of MIA in frequency domain. 93
6.14 One Single Demodulated EM waveform at 24 MHz. 94
6.15 One single Demodulated EM waveform at 34 MHz. 95
6.16 One Single Demodulated EM waveform at 54 MHz. 95

7.1 Schema of general experimental setup. 100
7.2 Real experiment with a stripline and attenuator configuration. 101
7.3 Spectrum of the working component without injecting wave. 102
7.4 Spectrum of the working component with injected wave. 102
7.5 Coil, FCC probe. 103
7.6 Fault injection experiment onto SecMatV1 DES, with separated power supply. 105
7.7 Schematic of the fault injection setup. 106
7.8 Transfer function. 106
7.9 Setup time violation. 107
7.10 Spectrum of one power measurement without injecting a carrier. . . 109
7.11 Setup of the power analysis with injected carrier and demodulation technique. 109
7.12 Power Measurement by injecting a carrier at 190 MHz and demodulating at 380 MHz. 110
7.13 Differential traces obtained for the right key hypothesis, by injecting a carrier at 190 MHz and demodulating at 380 MHz. 111

List of Tables

1.1 Montgomery Multiplication. 12

2.1 Correlations evolution and final waves after estimation with 2,000 traces. 30

3.1 Information and probability of the Hamming weight of an 8-bit uniformly distributed random variable. 46

5.1 Drawbacks and advantages of the three analyzed distinguishers. . . . 72

6.1 Measurement conditions 84
6.2 Comparison between the results. 95

7.1 Characteristics of the different setups used. 103
7.2 First results of fault injection onto the AES. 104
7.3 Experimental conditions and statistics. 107
7.4 Round statistics for the 9 MHz and clock-frequency injection. 108
7.5 Sbox statistics for the 9 MHz and clock-frequency injection. 108

Acronyms

AES Advanced Encryption Standard

ASIC Application Specific Integrated Circuit

CHES Cryptographic Hardware and Embedded Systems

CMOS Complementary Metal Oxide Semi-conductor

CEMA Correlation Electro-Magnetic Analysis

CPA Correlation Power Analysis

DEMA Differential Electro-Magnetic Analysis

DES Data Encryption Standard

DFA Differential Fault Analysis

DFF D Flip Flop

DPA Differential Power Analysis

DSP Digital Signal Processor

EMA Electro-Magnetic Analysis

EMC Electro-Magnetic Compatibility

FA Fault Analysis

FFT Fast Fourier Transform

FPGA Field Gate Programmable Array

GSM Global System for Mobile communications

HMAC Hash Message Authentication Code

IC Integrated Circuit

I/O Input/Output

IV Initialization Vector

LFSR Linear Feedback Shift Register

MDC Modification Detection Codes

MAC Message Authentication Codes

NIST National Institute of Standards and Technology

NSA National Security Agency

PC Personal Computer

pdf probability distribution function

PKCS Public Key Cryptographic Standards

PUF Physically Unclonable Functions

RAM Read-access Memory

RFID Radio Frequency IDentification

ROM Read-only Memory

RSA Rivest Shamir and Adleman

s-box substitution box

SCA Side Channel Analysis

SEMA Simple Electro-Magnetic Analysis

SHA Secure Hash Algorithm

SNR Signal on Noise Ratio

SPA Simple Power Analysis

SPN Substitution Permutation Network

S-SCA Statistical Side Channel Analysis

SSH Secure SHell

SSL Secure Socket Layer

TA Template Attacks

xor eXclusive OR

Contents

I Introduction **1**

1 Introduction **3**
1.1 Symmetric Cryptography . . . 4
1.1.1 Stream ciphers . . . 5
1.1.2 Hash Function . . . 5
1.1.3 Block Ciphers . . . 6
1.2 Asymmetric Cryptography . . . 9
1.2.1 The PKI System . . . 10
1.2.2 The RSA . . . 10
1.3 Attacks on Cryptographic Devices . . . 11
1.3.1 Timing Attack . . . 12
1.3.2 Power/ Electromagnetic Analysis Attacks . . . 13
1.3.3 Active Attack . . . 14
1.4 Countermeasures . . . 15
1.4.1 Algebraic Countermeasures . . . 16
1.4.2 Masking . . . 16
1.4.3 Dual Rail Logic . . . 16
1.5 Conclusion . . . 17

II Threats to cryptographic devices **19**

2 Leakage Modalities **21**
2.1 Electromagnetic Background . . . 21
2.1.1 Differential Mode . . . 22
2.1.2 Common Mode . . . 23
2.1.3 Direct Emanations and Indirect Emanations . . . 23
2.2 Cryptanalysis Point of View . . . 24
2.2.1 CMOS Leakage Modalities . . . 25
2.2.2 Distinguishers . . . 26
2.2.3 Leakage Model Enhancement . . . 29
2.3 Conclusion . . . 33

3 Electro-Magnetic Attacks on Cryptographic Device at Distance **35**
3.1 CEMA at Distance . . . 35
3.1.1 The Test Bench and Implementation of AES . . . 35
3.1.2 Leakage Indicator w.r.t. the Measurement Noise . . . 36
3.1.3 Leakage Model at Distance . . . 39
3.2 Techniques for Revealing the POIs . . . 42
3.2.1 The sosd *versus* sost . . . 42

3.2.2 Information Theoretic Metric . . . 44
3.2.3 The PCA . . . 45
3.3 Combining Time Samples . . . 47
3.3.1 Observations . . . 47
3.3.2 Sample Combination Principle and Results. . . . 47
3.3.3 POIs Independence with the Key . . . 48
3.4 Conclusion . . . 50

III Characterization of the electromagnetic Side channel and demodulation techniques 53

4 TEMPEST 55
4.1 Historic Background . . . 56
4.1.1 Military Issues . . . 56
4.1.2 TEMPEST Standard . . . 56
4.1.3 Academic Research . . . 57
4.1.4 Protections and Countermeasures . . . 58
4.2 TEMPEST Evaluation and Signal Acquisition . . . 59
4.2.1 Correlated Emanation . . . 59
4.2.2 State of the Art Methods for TEMPEST Evaluation . . . 59

5 Keyboard Emanation Methods to Detect Compromising Frequencies 61
5.1 Experimental Setup . . . 61
5.1.1 Measurement Setup . . . 62
5.1.2 PS/2 Protocol . . . 62
5.2 Frequency Distinguishers . . . 63
5.2.1 An Empirical Approach based on CPA . . . 65
5.2.2 Approach based on Mutual Information Analysis . . . 66
5.2.3 Frequency Distinguisher in Principal Subspaces . . . 69
5.3 Exploiting Compromising Emanation . . . 70
5.3.1 Confirmations of the Results with a Hardware Receiver . . . 70
5.3.2 Software Filtering . . . 73
5.4 Conclusion . . . 74

6 Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization and Demodulation Techniques 81
6.1 SEMA and Target Device Implementation . . . 82
6.1.1 SEMA on a RSA Implementation . . . 82
6.1.2 SASEBO-G and VirtexII . . . 83
6.1.3 Identification of the Information Leakage Spots . . . 84
6.2 Characterization of the EM Channel in Frequency Domain . . . 88
6.2.1 Windowing and Sample Preparation . . . 89
6.2.2 An Information Theory Viewpoint . . . 91

6.3 Demodulation Technique 93
6.3.1 Confirmation of the Results with a Hardware Receiver 93
6.3.2 Unintentional emanations 93
6.4 Conclusions 96

IV Intentional Electro-Magnetic Interference 97

7 Non Invasive Intentional Electro-Magnetic Interference Attacks 99
7.1 Radiative Intentional Electro-Magnetic Interference Attacks 100
7.1.1 Particular Experimental Setup 100
7.1.2 Results and Observations 101
7.2 Conductive/Radiative Intentional Electro-Magnetic Interference Attacks 102
7.2.1 Experimental setup 103
7.2.2 Fault Injection on Sasebo-G with AES 104
7.2.3 Fault Injection onto the DES SecMat-V1 105
7.3 Power Analysis in Frequency Domain 109
7.4 Conclusion 110

8 Conclusion 113

Bibliography 117

Part I

Introduction

Chapter 1

Introduction

In this chapter, we discuss about cryptography by describing the basic principles and algorithms. Then we present the cryptographic devices that are used nowadays and their different applications. We will see that these cryptographic algorithms which are recognized as safe and secure from a mathematical point of view become targets of physical attacks due to their implementation on electronic components. Therefore a theoretically secure cryptographic algorithm could give some clues about the secret data that are computed due to their physical behavior on an electronic device. We describe the main attacks and vulnerabilities of the component and give a brief overview of the main threats against cryptographic devices.

Contents

1.1 Symmetric Cryptography 4
1.1.1 Stream ciphers 5
1.1.2 Hash Function 5
1.1.3 Block Ciphers 6
1.2 Asymmetric Cryptography 9
1.2.1 The PKI System 10
1.2.2 The RSA 10
1.3 Attacks on Cryptographic Devices 11
1.3.1 Timing Attack 12
1.3.2 Power/ Electromagnetic Analysis Attacks 13
1.3.3 Active Attack 14
1.4 Countermeasures 15
1.4.1 Algebraic Countermeasures 16
1.4.2 Masking 16
1.4.3 Dual Rail Logic 16
1.5 Conclusion 17

Cryptography from the Greek *kryptos* meaning hidden and *graphein* meaning writing refers to the art of ciphering a message. It means writing a message (*plaintext*) in an unintelligible form (*ciphertext*) for anyone unaware of the encryption process. Historically the use of cryptography dates back to the time of Julius Caesar who encrypted messages for military purpose with the famous encryption system called Caesar's cipher. More recently with the increase use of computer resources,

cryptography is even more used to protect confidential data, and consequently have become a widely used tool in communications, computer networks, and computer security to provide secure communications over an *insecure channel*. Cryptography is consequently becoming a branch of applied mathematics and computer sciences. The cryptography provides the following security properties:

- *authentication*: the proof that the sender of the ciphertext is not corrupted;
- *confidentiality*: the message is only intelligible by the receiver and the sender;
- *integrity*: the proof that the message has not been modified during its transfer;
- *non-repudiation*: property used in digital signature where the author of a signature can not deny afterwards.

Theoretically cryptographic algorithms can be broken by using a brute force attack, i.e an exhaustive key search. The attacker has to test every possible key and check if the plaintext encryption is similar to the ciphertext. But the cryptographic algorithms have been designed so that such exhaustive research can not be possible in reasonable time. For instance the key-length is chosen so that such exhaustive search is made impractical due to the huge computing time.

Cryptographic algorithms are sorted into two main branches: the symmetric cryptography and the asymmetric cryptography. According to Kerckhoffs principles [Ker83a, Ker83b], cryptographic system has to be public and only the key has to be kept secret. Therefore most of the time cryptographic algorithms are considered secure, if for several years of public existence, they remain without any relevant cryptanalysis attack. The robustness of symmetric algorithm is evaluated by this way. For the asymmetric cryptographic algorithm their security is based on hard problems from number theory such as factorization of large prime number or the discrete logarithm computation in a large multiplicative group. A problem is considered hard if it is computationally intractable.

1.1 Symmetric Cryptography

Historically, symmetric cryptography is the oldest manner used to encrypt the message. It is based on the assumption that Bob and Alice share the same secret key to encrypt and decrypt a message. In other words a key k is used as a parameter to cipher a message $c = E_k(m)$. Then to decipher the ciphertext the inverse function $m = E_k^{-1}(c)$ must be computed. This kind of ciphering technique is also called secret key cryptography. Two different types of secret key cryptography exist: the stream cipher and the block cipher. Due to their speed the stream ciphers are often used in Radio Frequency IDentification (RFID) like Mifare Crypto-1 or in Global System for Mobile communication (GSM A5/1).

1.1.1 Stream ciphers

Stream ciphers are based on Vernam cipher, in which the plaintext is XORed with a pseudo random cipher bit stream (keystream). Some stream ciphers used Linear Feedback Shift Register (*LFSR*) to initialize a fixed-length secret key k. It allows to derive a long pseudo random sequence from a short key. For each ciphering an Initialization Vector (IV) is used to make it independent from the others ciphering produced by the same key. We notice that the same key cannot be used for every encryption, that would destroy the stream cipher security. Therefore the usage of a different initialization vector for every encryption is mandatory for the stream cipher security.

1.1.2 Hash Function

A hash function is an algorithm that compresses a large data set into a smaller data set. Hash functions are required for many cryptographic algorithms or protocols for instance electronic signature, Message Authentication Codes (MAC), Pseudo Random Number Generator (PRNG)...

A hash function is defined as:

$$\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^n.$$

This function has to satisfy three main properties:

- $\mathcal{H}$ is considered as preimage-resistant if for the result y of a hash computation finding a preimage x such as $\mathcal{H}(x) = y$ is computationally hard,
- $\mathcal{H}$ has to be second-preimage resistant, if given a value x_1 and its hash value $\mathcal{H}(x_1)$ it is computationally hard to find $x_2 \neq x_1$ such that $\mathcal{H}(x_2) = \mathcal{H}(x_1)$,
- $\mathcal{H}$ is said to be collision-resistant $x_1 \neq x_2$
  $\mathcal{H}(x_1) = \mathcal{H}(x_2)$.

Therefore hash functions can be used if we want to compute a condensed version y of a message m. In this case, the digest is be specific to the message and can be used instead of the m. For authentication: a signature can be computed by Bob on y to prove that he is the author of m. Or during file sharing operation, Bob can provide y in order to help Alice to check the integrity of m.

There are two types of hash functions:

- without key used to ensure the integrity of a message, Modification Detection Code (MDC).
- with key used to verify the integrity and origin of the message simultaneously with the Message Authentication Code (MAC).

1.1.3 Block Ciphers

A block cipher is a bijective function parametrized by a key block $k \in K$ such as:

$$\begin{aligned} E : \{0,1\}^n \times K &\rightarrow \{0,1\}^n, \text{such that } \forall k \in K \\ m &\rightarrow E(m,k). \end{aligned}$$

It takes a n bit plaintext block as input and outputs a n bit block cipher. Respectively for deciphering the function $D_k = E_k^{-1}$ has to be used. Moreover it is possible to cipher block message of arbitrary length by splitting it in several n bit block $m_0, m_1, m_2, m_3, ...m_p$ that are each ciphered using a *mode of operation*. Different modes of operation exist such as the mains:

- ECB (Electronic CodeBook mode) each block is ciphered independently with the same key: $c_i = E_k(m_i)$, one permutation in cipher block corresponds to the same in plaintext block,
- CBC (Cipher Block Chaining), every ciphered block acts on the following plaintext block with a eXclusive-OR such as:

  $$c_i = \begin{cases} E_k(m_1 \oplus iv) \text{ if } i = 1 \\ E_k(m_i \oplus c_{i-1}) \text{ if } i > 1 \end{cases}$$

  In this mode an error can be propagated. One error in a cipher block affects two cipher blocks. Two faulty cipher blocks are required to retrieve a correct mode after.
- OFB (Output FeedBack mode) and CFB (Cipher FeedBack mode) a keystream is obtained from an Initial Vector iv and Xored with the plaintext, for instance for the OFB mode:

  $$\begin{aligned} O_0 &= iv \\ O_i &= E_k(O_{i-1}) \\ c_i &= m_i \oplus O_i, \end{aligned}$$

  and for CFB mode:

  $$\begin{aligned} c_0 &= iv \\ c_i &= E_k(c_{i-1}) \oplus m_i. \end{aligned}$$

A block cipher algorithm is composed of a number of iterations called rounds. It means that each round applies the repetition of key-dependent permutations and non-linear operation with substitutions, is called round transformation. The round sub-key used during these iterative rounds, is derived from a secret master key by applying a key scheduling function. In the following we present two types of block cipher: a Feistel Network with the Data Encryption Standard (DES) and a Substitution Permutation Network with the Advanced Encryption Standard (AES). Both standard block ciphers are widely used.

1.1.3.1 Feistel

A Feistel network is the application of a round transformation shown on the figure 1.1.

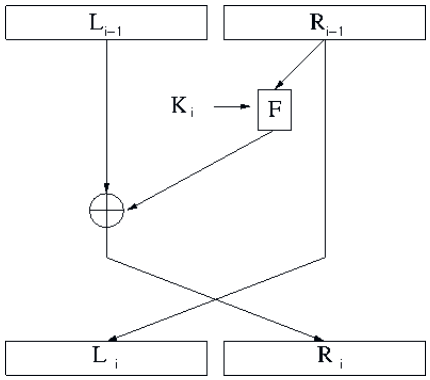


Figure 1.1: Feistel global structure

It operates on a fixed-length group of bits called a block. A Feistel processes two blocks of same length. The $2n$ bit plaintext is therefore divided into two n bit parts L_0 and R_0. If we consider a Feistel with r rounds, F the round function, and $K_1, ..., K_r$ the sub-keys for the round 1 to r. At the i-th round, we compute:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i), \end{aligned}$$

and by iterating this round transformation we obtain the ciphertext (R_r, L_r).

The Data Encryption Standard is the most famous Feistel scheme. It has been adopted by the NIST as a standard for data encryption in 1976. It processes cipher on 64-bit blocks with a 56-bit key. The DES is based on an iterative structure with 16 calls to the function F preceeded by an initial permutation IP and followed by a final permutation. The round function F takes a 48-bit round-key as a parameter. Firstly F applies an expansion function E, the 32-bit block is expanded to a 48-bit block by duplicating 16 of its bits. After a key mixing operation that consists in a eXclusive OR with the 48-bit round key derived from the master key using a key schedule algorithm. Then the 48-bit block is split into eight blocks of 6 bits, each entering into a different substitution box (S-box) that computes a 4-bit output according to a lookup table. Finally the 32-bit substitution sbox outputs are rearranged according to the Permutation operation. We can also summarize this algorithm by the following equation:

$$F(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i)),$$

where

- E is the expansion function from 32 bits to 48 bits,

- S is the substitution function composed of 8 different S-box from 6 bits to 4 bits,
- P is the permutation function on 32 bits.

Until 1999 DES was several times evaluated and kept as a standard. In 2004 it was considered unsecure since the bit-length of the key is too short. That is why NIST recommended to use the *Triple DES* with a 112-bit key (K_1, K_2) as illustrated below:

$$\begin{aligned} C &= DES_{K_1}(DES_{K_2^{-1}}(DES_{K_1}(M))) \text{ for encryption and,} \\ M &= DES^{-1}_{K_1}(DES_{K_2}(DES^{-1}_{K_1}(C))) \text{ for decryption.} \end{aligned}$$

1.1.3.2 Substitution Permutation Network

A Substitution Permutation Network is a series of mathematical functions such as Substitution Permutation. A SPN takes as input two blocks of a plaintext and a key. After applying several times a round function designed with S-boxes for substitution operation and P-boxes for permutation operation it produces the cipher block.

In 2002, after five years of competition the Rijndael algorithm was chosen as AES (Advanced Encryption Standard) by the National Institute of Standards and Technology as a successor to the Data Encryption Standard. Rijndael was designed by Joan Damen and Vincent Rijmen. The AES is specified by the NIST in US FIPS PUB 197 [14001], and can process 128 bit block size with key size of 128 bits, 192 bits or 256 bits. Obviously the number of rounds increases with the key size, thus we need 10 rounds for a key size of 128-bit length, 12 rounds for 192-bit and 14 rounds for 256-bit to compute the cipher. For the following we consider the AES-128. The plaintext, the key and the cipher can be represented by a 4-by-4 array of 8-bit words, the same for the intermediate values of the rounds that we call state matrix. The first nine rounds are composed of four stages:

- AddRoundKey,
- SubBytes,
- ShiftRows,
- MixColumns.

The tenth round omits the MixColumns operation. Before the first round an operation of **AddRounKey** is computed between the input key and the plaintext. The computations are realised in $GF(2^8)$ it means that each byte can be considered as an element of the finite field $GF(2^8) = \mathbb{F}_2[X]/m(x)$ where $m(x) = x^8 + x^4 + x^3 + x + 1$. During the **SubBytes** operation a non-linear bytes substitution is performed independently on each byte of the state using a substitution table (S-box). Contrary to the DES, the same S-boxes are used to compute Substitution operation, and each

byte is substituted by another one according to a lookup table. **ShiftRows** operation as the name suggests shifts bytes cyclically in different rows. For instance the shift value is 1 for the second row, 2 for the third row and 3 for the fourth row. Then a **Mixcolumns** transformation operates on the state column wise and each byte is replaced by a combination of the four bytes in its column. Finally the **AddRoundKey** is applied, in which a round key is added to the state by a simple bitwise Xor operation, knowing that each round key consists of Nb words from the key schedule. We noticed that the first row is left untouched by the ShiftRows operation on the last round of the encryption as illustrated on the figure 1.2.

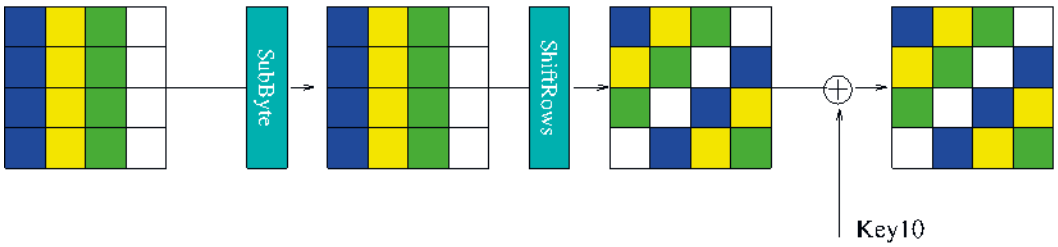


Figure 1.2: 9th round of the AES.

1.2 Asymmetric Cryptography

Symmetric cryptography is proving to be a very efficient tool. A major concern in symmetric cryptography is: How to share preliminary the secret data between two entities before to establish a secure channel? In 1976 Diffie and Hellman proposed the notion of public-key cryptosystem or asymmetric key cryptography in which a public and a private mathematically related keys are used to share confidential data. This system is based on one-way permutation with trapdoor. For instance Bob wants to communicate securely with Alice. To do so he builds a key K^B which is composed of two parts: $K^B = (K_p^B, K_s^B)$. K_p^B is the public-key of Bob and is transmitted to Alice, who uses it to encrypt. K_s^B is kept secret by Bob, and used as a trapdoor to recover the plaintext and inverse the one-way function. It is important to notice that the public key is publicly deployed so that anyone can use it to encrypt a message to Bob. In practice public-key cryptosystems are slower than symmetric encryption function and operate on a fixed length message. As a result, they are not used to encrypt-decrypt large messages, but rather to exchange securely a symmetric encryption key, that is relatively easy to encrypt due to its small size. Once this key exchange is done, with an interlocutor, it is possible to use an algorithm for fast block cipher to encrypt a large amount of data. However with this kind of asymmetric cryptosystem, it might be possible for an attacker to provide its own public key instead of Bob's one. The adversary will be in position to decrypt secret data that Alice had thought sending to Bob. To tackle this issue, a solution has been proposed based on certificate.

1.2.1 The PKI System

Public Key Infrastructure, manages a set of digital certificates that are the proof that a public key belongs to a certain user. During a communication two users have to exchange their certificates and each user checks the signature of certificate with an authority. If the authority validates the certificate, they can exchange their public key in confidence. The public-key cryptosystem has therefore given rise to the concept of digital signature. This is the analogue of the handwritten signature that is affixed on a document in order to bind the responsibility of the signatory. It was created so that anyone can verify its authenticity.

1.2.2 The RSA

Proposed in 1978 by Ronald Rivest, Adi Shamir and Leonard Adleman is the first public-key cryptosystem. This algorithm is commonly named RSA that are the initials of the autors' names. It was the first algorithm suitable for signing as well as ciphering. This algorithm is based on the Fermat's theorem and calculation in the ring $\mathbb{Z}/n\mathbb{Z}$. The RSA is composed of three steps: key generation, encryption and decryption.

- *Key Generation* During the key generation a modulus N is obtained by the product $N = p \cdot q$ of two large secret prime numbers p and q. The large prime integers p and q must be chosen randomly and have a large bit-length. A primality test such as those proposed by Fermat can be efficiently used to find the prime integers. Then: $\varphi(N) = (p-1) \cdot (q-1)$ Euler's totient function is computed. After an integer e is chosen such that $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$, i.e e and $\varphi(N)$ are coprime, and e is defined as the public key exponent. Most of the time e takes the value 65537=0x10001, due to its short bit-length. Sometimes a value of 3 for e can be also taken. And finally d is determined as following: $d = e^{-1} \bmod \varphi(N)$ therefore d is the multiplicative inverse of $e \bmod \varphi(N)$, it is obtained by computing the extended euclidean algorithm. We obtain a couple of key: the public key is composed of the modulus N and of the exponent e. In other hand the private exponent d must be kept secret.

- *Encryption* To cipher a message $0 \leq m < N$ Alice has to compute:

$$c = m^e \bmod N.$$

- *Decryption* Bob receives the ciphertext and has to retrieve the plaintext by computing $m = c^d \bmod N$. The plaintext is recovered because:

$$\begin{aligned} c^d &\equiv m^{ed} \bmod N, \\ &\equiv m^{1+k\varphi(N)} \bmod N, \text{with } ed = 1 \bmod \varphi(N), \\ &\equiv m \bmod N, \text{ duetoEuler}'\text{sTheorem}. \end{aligned}$$

The RSA can also be used to provide a ***digital signature***. In this case Bob uses his private key to sign a document m and compute:

$$s = \mathcal{H}(m)^d \bmod N.$$

Therefore to check the authentication of Bob's signature, Alice has to compute:

$$\mathcal{H}(m) = s^e \bmod N,$$

Alice has to check that the hash value of the message is equal to the received hash. For security reason, we prefer to compute the signature of a hash value $h = \mathcal{H}(m)$ of the message, and check the signature of this value h instead of the original message. The use of the hash value avoids to compute the signature of very large messages. To make impossible the factorisation of the module N, we choose generally large prime numbers p and q of 1024 bit-length up to 2048 bits.

1.3 Attacks on Cryptographic Devices

Cryptographic modules (software or hardware implementations of cryptographic algorithms) are now essential for many electronic devices. Such modules are commonly used for secure communications and transactions to protect privacy and valuable data.

The most famous cryptographic device is probably the smart card. It was proposed for the first time in 1970 and resulted from several works and contributors, that can be cited such as the Americans Thomas Pomeroy, Jules Ellingboe, the Japanese Kunitaka Arimura, the Germans Jurgen Dethloff and Helmut Grottrup and the French Roland Moreno, Michel Ugon and Louis Guillou. Nowadays smart cards are used in different applications of everyone's daily life such as SIM (Subscriber Identity Module) card, credit card, electronic passport... That is why before deployment an electronic security product must be tested against various possible attacks. So whatever is the mathematical robustness of cryptographic algorithm, it has to be implemented on test device such as FPGA (*Field Programmable Gate Array*), DSP (*Digital Signal Processor*), to be evaluated against side channels attacks. In this thesis, we choose to implement cryptographic algorithm on FPGA, that we introduce in the following.

FPGA a programmable logic array consists of many logic cells which can be freely assembled. A logic cell is composed of a lookup table LUT and a flip-flop. A LUT can be seen as a small memory. It is generally used to implement combinatorial logic that has multiple inputs and one single output. Therefore it can be used as a multiplexer or a shift register. These logic blocks are interconnected according to a configurable routing matrix, that allows the configuration of the component by the user.

During the security evaluation, different attack scenarii can be imagined. An attacker can for instance use advantageously any imperfection of the implementation to recover the secret information. Now we propose an overview of the different published attacks.

HIGH-RADIX MONTGOMERY MULTIPLICATION (*MontMult*)

Input:	$X = (x_{m-1}, ..., x_1, x_0)_{2^r}$, $Y = (y_{m-1}, ..., y_1, y_0)_{2^r}$, $N = (n_{m-1}, ..., n_1, n_0)_{2^r}$, $W = -N^{-1} \bmod 2^r$
Output:	$Z = XY2^{-r \cdot m} \bmod N$

1: $Z := 0$;
2: **for** $i = 0$ **to** $m - 1$
3: $\quad C := 0$;
4: $\quad t_i := (z_0 + x_i y_0) W \bmod 2^r$;
5: $\quad$ **for** $j = 0$ **to** $m - 1$
6: $\quad\quad Q := z_j + x_i y_j + t_i n_j + C$;
7: $\quad\quad$ **if** $(j \neq 0)$ **then** $z_{j-1} := Q \bmod 2^r$;
8: $\quad\quad C := Q/2^r$;
9: $\quad$ **end for**
10: $\quad z_{m-1} := C$;
11: **end for**
12: **if** $(Z > N)$ **then** $Z := Z - N$;

Table 1.1: Montgomery Multiplication.

1.3.1 Timing Attack

Timing attack is a Side Channel Attack, in which an attacker, by considering the overall computation time, aims to recover secret information. Knowing that a cryptosystem takes time to execute a logical instruction depending of the input, an attacker can choose a set of sound plaintexts to observe a maximal difference of computation time. For instance in 1996 Kocher in [KJJ96] exhibits a flaw by considering an implementation of the RSA with computation of the modular exponentiation using a Montgomery modular multiplication [FZY+06].

In the Montgomery Multiplication algorithm presented in 1.1 final subtraction is performed depending on the operands value (line 12). Consequently the overall time of the RSA computation depends on each intermediate result of the exponentiation. The idea of chosen plaintexts seems to be consequently relevant. A simple countermeasure is to compute the same number of operations whatever the input value. Concerning the block cipher, timing attack is more subtle. In 2005 Bernstein *et al* showed in [Ber05] that a timing attack is possible by considering the cache memory and the time access for cache memory knowing that the S-box can be loaded in the cache memory.

1.3.2 Power/ Electromagnetic Analysis Attacks

Power analysis attacks, can be further categorized into two types of attacks. The first one is related to the observations of the power consumption of a device during the computation. This power consumption can be measured by using a resistor connected to the power supply of the device as described in Chapter 2. With an oscilloscope we can display the instantaneous consumption of the device and guess the secret information. The global power consumption of the device depends on the contribution of the logic cells that are changing state switching to the sequential operation. An attacker is therefore able to identify a secret dependent instruction or intermediate value. Figure 1.3 shows a typical example of SPA (Simple Power Attack) attack against an RSA implementation based on the square-and-multiply algorithm. In this algorithm every loop operation performs a square if the exponent bit key equals 0 or a square and multiply if the exponent bit key equals 1. Square and multiply operations have a different power consumption. In that case the leakage trace for a single RSA operation reveals the secret exponent.

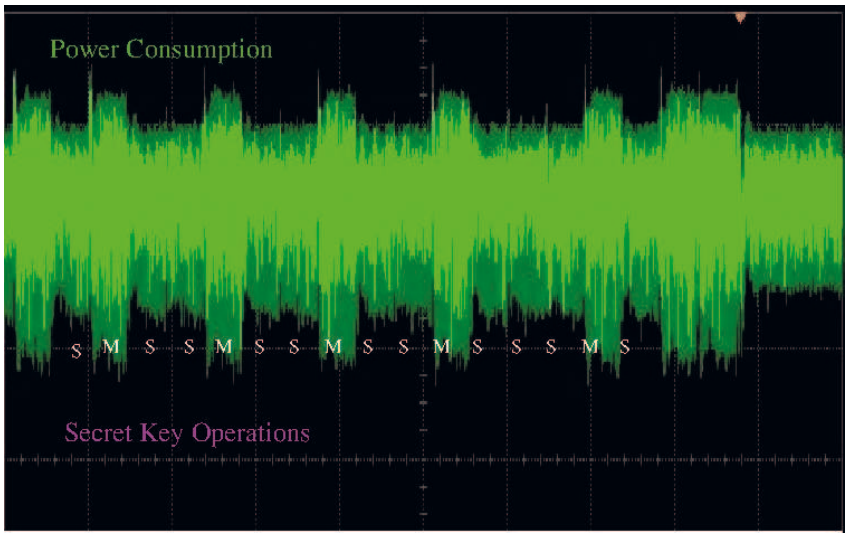


Figure 1.3: RSA power supply consumption on a FPGA.

We could see that the power consumption of a cryptographic device is dependent on the activity of the cryptographic computation as illustrated in figure 1.3. Quisquater was the first one to show that the electromagnetic emanations could also be used as a leakage source [QS01]. Such attacks are detailed in Chapter 6, and some improvements will be proposed. From this first observation, the overall consumption of a cryptographic device is the result of the consumption of its logic gates; and reflects the internal activity. This consumption depends on both the handled data and executed instruction. As we can see in the figure 1.4 the power consumption and the electromagnetic emanations depend on the intermediate variable being processed. The two EM traces show some differences that can be exploited by differential analysis. These differences depends on the sensitive varibles

that are manipulated.

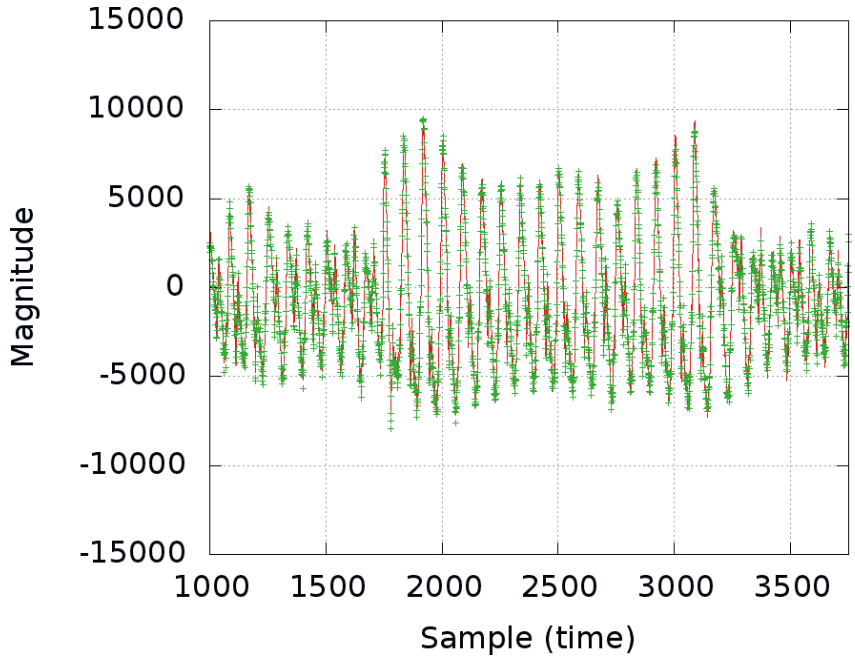


Figure 1.4: EM radiation of DES computation on an FPGA

An attacker has also to devise a suitable leakage model related to these sensitive variables. With a reliable estimation based on prediction of the sensitive values for several computations with different known inputs, the attacker with a correct guess can recover the part of the secret key. If the guess is correct a statistical relation is observed between the predicted values and the leakage measurements. This kind of attack is related to differential power analysis DPA, and has been described by Kocher in [KJJ99]. Several improvements have been proposed since the initial publication of Kocher. These improvements are related to the study of a fair leakage model, new powerful statistical tools, in other words, concerning the distinguisher and the selection function. In Chapter 2, we will introduce more details about the measurement techniques, the leakage models and the distinguishers that can be used. Chapter 3 is dedicated to the study of this type of differential attack with remote measurements. We will see how we can use these powerful attacks and improve them to perform attack at distance on a cryptographic device. Then we introduce a set of tools based on the state of the art distinguishers used in differential analysis to characterize the electromagnetic emanation in the frequency domain, and retrieve the frequencies that are carrying sensitive information.

1.3.3 Active Attack

In 1996, Dan Boneh *et al* introduced in [BDL97] new methods called fault analysis. With these attacks, we consider that the attacker is able to disrupt the behavior of a cryptographic device during computation. The faulty cipher obtained allows an

attacker to retrieve the secret data. Different ways to produce a fault attack exist, for example:

- power glitch,
- clock glitch,
- light pulse.

A power glitch is a sudden controlled variation of the power supply voltage that produces switching of logical gates. Similar effects are produced with the clock glitch technique. A sizeable increase of the clock frequency causes the early start for the execution of instruction. These techniques are relatively easy to mount and they do not require high cost equipment. However manufacturers introduce countermeasures in their device to avoid this kind of attack. For instance voltage threshold sensors and high frequency detectors can be included in the chip to protect them against glitches attacks. Light pulse is also a suitable technique to inject fault. Indeed it was noticed that an electronic device is sensitive to light. To allow this technique of fault injection, the device must be carefully depackaged without altering its integrity. Depackaging is a relatively delicate step that requires high-tech microelectronic equipment. The first light pulse attack was realized with an amplified camera flash and is described in [SA03] by Skorobogatov and Anderson. Nowadays this kind of attacks are realized with a laser beam, that is more effective and offers many advantages. A laser beam can bypass countermeasure that usually detect camera flashes. Moreover it allows to target accurately a local area of the device, and to select the wavelength of the pulse.

The different erroneous results produced by these fault attacks are then analysed by considering a *Fault model*. The *Fault model* describes how the data have been corrupted by the fault, and the effect of the perturbation onto the data. For instance we consider that a fault attack can change the value of one bit, a whole byte or more. This change in value occurs by switching randomly a state of one or several bits, or by erasing the data by a given fixed value most of the time $0x00$ or $0xFF$. This type of fault is named *stuck-at* fault model. Therefore the attacker in order to retrieve the secret key has to make some assumptions considering the fault model.

In Chapter 7 we will introduce a new technique of fault attack based on carrier injection on power cables.

1.4 Countermeasures

To protect cryptographic devices against the threat of Side Channel Attacks some research teams propose countermeasures. In this section we give an overview of the most usual countermeasures.

1.4.1 Algebraic Countermeasures

One of the most famous countermeasures against SPA is the Montgomery Ladder. This countermeasure was presented by Joye and Yen in [JY03], and consists in computing the same operations in the same order independently of the key bit value. These operations are often called dummy operations. This countermeasure is used for asymmetric cryptographic algorithm such as RSA or elliptic curve and is described for the RSA in the following algorithm.

Montgomery Ladder for RSA

Input:	C a message for RSA, N modulus for RSA, $D = (d_{k-1}, ..., d_1, d_0)_2$ an exponent
Output:	$M = C^D \bmod N$

1: $S[0] := 1$ $S[1] :=$ C
2: **for** $i = k - 1$ **downto** 0
3: $S[0] := S[0]^2 \bmod N$
4: $S[1] := S[0] \times C \bmod N$
5: $S[0] := S[d_i]$
6: **end for**
7: return S

1.4.2 Masking

The data masking countermeasure uses a randomly generated value called mask. This mask is used in the computation in such a way that the end result remains unaffected. The use of mask during computation makes the leakage correlated to the mask. Since the mask is randomly generated the leakage will give no or few useful information. This way, masking, makes the design more resistant against side channel attack.

1.4.3 Dual Rail Logic

The other way to protect cryptographic implementation is data hiding. Unlike data masking, the main purpose of this countermeasure is to make the activity of the device constant at all times. Some of the attacks are based on the fact that a CMOS cell consumes when it changes its states at the first order. This difference is exploited by power analysis or electromagnetic analysis of the design. The constant activity will provide constant leakage and there will not be much to exploit. Therefore data hiding serves as a countermeasure against attacks. The hiding technique consists in obtaining a constant power consumption whereas masking aims to mask the power consumption. One way to get a constant activity is to use differential logic characterized by the fact that each variable is made up of two complementary signals. This logic is such that if one signal switches the other does not switch and vice

versa. This allows the design to be balanced in term of power because in CMOS Technology the main power consumption comes from the switching rate. To make sure the number of transitions (0→1 or 1→0) is constant, the computation has two distinct phases:

1. A **Precharge** phase to reset all the signals in a known state, and
2. An **Evaluation** phase where the computation is performed with a fixed number of transitions.

The differential logic is also called "Dual Rail with Precharge Logic" (DPL) as the two signals of the same variable need twice as much logic and routing resources. Therefore the complexity is at least doubled w.r.t. a non-protected implementation. From this DPL principle many styles have been devised specifically for ASIC or FPGA technologies. This countermeasure may be also relevant to protect circuits against fault attack as explained by Selmane *et al* in [SBG+09].

1.5 Conclusion

In this chapter we have introduced some bases in cryptography as a preliminary. We have presented the most used cryptographic algorithms and primitives. Then we described the Side Channel Attacks, that can be divided into passive and active attack. During passive attacks the power consumption or the electromagnetic radiations are observed and gathered to compute statistical analysis and retrieve secret key. On an other hand, with active attacks, power glitch, clock glitch, light pulse are generated to disrupt the working of a cryptographic device. To tackle these different threats, we have presented an overview of countermeasures based on hiding, masking and algebraic computation.

Part II

Threats to cryptographic devices

Chapter 2

Leakage Modalities

In this chapter we demonstrate, how the electromagnetic radiation can be exploited to recover a secret key and perform Side Channel Analysis. We enumerate firstly the origins of the different electromagnetic emanations: the common mode and differential mode; that induce two kinds of emanation: direct radiations and the unintentional radiations. Then we explain how to discover and exploit the electromagnetic leakage by using statistical tools and leakage models.

Contents

2.1 Electromagnetic Background 21
2.1.1 Differential Mode 22
2.1.2 Common Mode 23
2.1.3 Direct Emanations and Indirect Emanations 23
2.2 Cryptanalysis Point of View 24
2.2.1 CMOS Leakage Modalities 25
2.2.2 Distinguishers 26
2.2.3 Leakage Model Enhancement 29
2.3 Conclusion 33

2.1 Electromagnetic Background

At the beginning, just some power consumption measurement were needed to retrieve the secret key. For the attacker it was relatively easy to insert a resistor (1Ω and 50Ω) between the Vdd bias input and the ground line as illustrated on the figure 2.1.

The attacker can easily observe the activity of the cryptographic component. This current is proportional to the current flowing into the device assuming that the power supply voltage is kept constant. Since long time, the insertion of a resistor into the power supply line of the cryptographic device stands to be the easiest way of building a side channel attack, but in 2001 Gandolfi *et al* proposed in [GMO01] the first measurement method for EM field. This method was largely used and described in [QS01] and in [SBM+05]. This passive attack was later improved by considering Electro-Magnetic radiation and a non-invasive technique. To perform contactless measurements electromagnetic probes are used to measure the magnetic field H and the electric field E component. Depending on the size and on the position of the

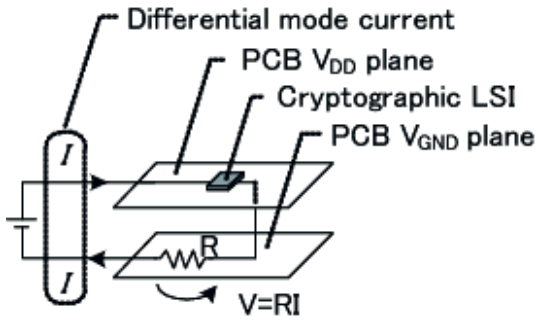


Figure 2.1: Conventional side-channel: voltage drop.

probe, the electromagnetic field of the attacked device can be measured. This field is proportional to the power consumption of the device as described by the following equations:

$$V = -N\frac{d\Phi}{dt},$$

where Φ represents the magnetic flux within the closed loop composing the probe, N is the number of the loops. Knowing that: $\Phi \propto I$, it follows that $V \propto dI/dt$. Therefore the output of the magnetic field probe is proportional to dI/dt. With this measurement technique we can get a fair estimation of the electrical current flowing the component. These vectorial fields are different depending on the probe and on its position onto the component.

Historically the electromagnetic emanations were studied for the Electro-Magnetic Compatibility (EMC), in order to characterize and suppress them if they disturb the operating of other components. The main purpose of the EMC was consequently to analyse the Electro-Magnetic Interference (EMI). We adopt for this reason similar methods for the signal detection and analysis.

EMC considers two types of unwanted emissions:

- **the conductive coupling** that requires physical support to transmit interference through the system (for instance a wire);
- **the radiative coupling** that occurs when a part of the internal circuit acts as a loop antenna.

In the following Chapters 5, 6 we will illustrate more precisely the radiative coupling, and in chapter 7 we will detail the conductive coupling. Concerning the radiative coupling EMC distinguishes two kinds of radiations depending on the source: the differential mode and the common mode.

2.1.1 Differential Mode

The differential mode is the normal way to transmit electrical signals. The current of the differential mode flows through a conductor and come back to the origin by

the others. The power supply and the digital signal on 2 wires are in differential mode. The voltage in differential mode is measured between the two wires. The differential mode radiation is therefore generated by loops formed with components printed circuit, ribbon cables. These different elements act as an antenna and the magnitude of the radiation is very low. To thwart this phenomena, a simple shield can be placed onto the FPGA. This kind of radiation is not easily influenced by external radiations.

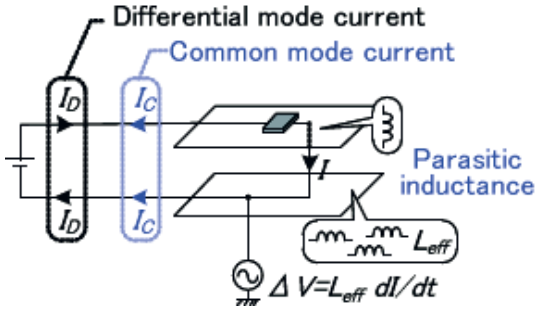


Figure 2.2: Image of common-mode current.

2.1.2 Common Mode

Common mode current is the result of internal voltage drops in the circuit which usually appears in the ground loop. In common mode, the current propagates on all the components in the same way and comes back through the ground plane due to parasitic inductance as shown on figure 2.2. Consequently common-mode radiations are created from the electro-magnetic fields of the current pair that are not cancelled since their directions are the same. The fluctuation of the voltage containing the information leakage is therefore emitted by the peripheral circuits interconnected to a cryptographic module that acts as an antenna. These phenomenas are due to internal clock signal and its harmonics, crosstalk, ground pollution or power supply DC pollution.

From the attacker's point of view this is a simpler way to describe these radiations. Indeed, the attacker has no real interest to determine the source of the emanations, since he aims only at exploiting them. He may look for correlations between the signal carrying the sensitive information and the compromising emissions. Thus, we redefine the classification of these compromising electromagnetic emanations accordingly.

2.1.3 Direct Emanations and Indirect Emanations

If we consider the leakage information, cryptanalysis distinguishes two types of emanations:

- *Direct Emanations* Direct Emanations result from intentional current flowing in the component. In digital devices and more largely in hardware components, each clock cycle, sharp falling and rising edges generate short bursts.

Therefore this kind of emanation is related to the activity of D Flip Flop (DFF). DFF commute at high frequency around 1 ns, and consequently the electromagnetic waves are emitted at high frequency related to the duration of the Rise/Fall edge duration. These compromising radiations are straight produced by the wires transmitting sensitive data, they are only detectable at very short distance, with a high sampling rate tuned on the scope. By analysing the direct emanations we get an image of the power consumption of the device in base band.

- *Indirect Emanations* With recent progress and new technologies aiming at reducing drastically the size of the component, a new type of radiation appears: unintentional or indirect emanation. Small components are supposed to work at short distance from each others that induces unintentional radiation. More precisely these indirect emanations are caused by different physical phenomena such as modulations or inter-modulations (phase, amplitude or frequency), carrier signals for instance clock signal and its harmonics, and cross-talk. Cross-talk phenomena is generally caused by an undesired coupling between two parts of the circuit. This coupling has different origins such as capacitive, inductive or conductive from one part to another of the circuit. For instance ground pollution can create a coupling current that generates unintentional radiation. On the opposite of the direct emanations, assuming that the indirect emanations are the result of a modulation between a confidential data and a carrier, they can be observed at distance form the component. Non-linear coupling between the sensitive signal and the carrier manifests as amplitude modulation, and allows a better propagation than the direct emanations. Hence they can be captured at a large distance. In the next chapter we will see a case where the attacker can manage an attack at 50 cm from the cryptographic device. In Chapter 5 and in Chapter 6 we will present different techniques to predict the frequencies that are carrying information. Indeed the prediction of these emanations and of the carrier frequencies is extremely difficult, because they are mainly based on common-mode radiation and on non-linear coupling.

2.2 Cryptanalysis Point of View

In general, the component is shielded by coatings to protect it from malevolent manipulations. However, it has been noted that despite this protection, some externally measurable quantities can be exploited without touching the component. Typically, without special care, internal data are somehow modulating the computation timing, the instant current drawn from the power supply, and the radiated fields. Thus, those unintentional physical emanations can be analyzed in a view to derive from them some sensitive information. The fact that the observed measurements are affected by the internal data is *a priori* unknown by the attacker, although in some cases an hypothetical, hence imperfect, physical model can be assumed. The link

between the data and the side-channel is called the leakage model.

2.2.1 CMOS Leakage Modalities

Complementary Metal-Oxide-Semiconductor (CMOS) logic gates are designed to minimize their energy usage when their output does not change. Energy is dissipated essentially in case one gate change states. Therefore, at first order, we expect the change of states to be the primary leakage cause of a CMOS circuit.

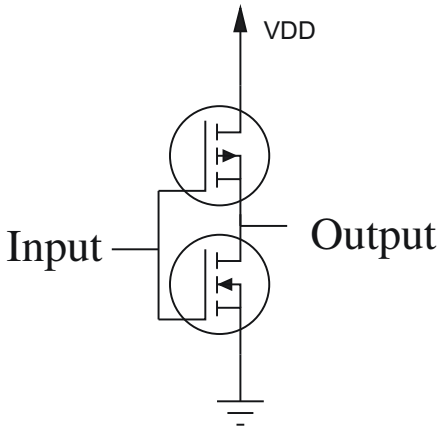


Figure 2.3: CMOS Cell

We consider as an assumption that each transition $1 \to 0$, $0 \to 1$, $1 \to 1$, $0 \to 0$ provokes different current from the power supply to the ground pin. In addition these transition currents generate electro-magnetic radiations. As a result there is a strong correlation between the electro-magnetic radiations and the data manipulated by the component. Therefore it may be interesting for an attacker to compute the number of bit flips.

Let us model the leakage $\mathcal{L}$ in a CMOS netlist as:

$$\mathcal{L} = \sum_{n \in \text{nets}} \xi_n^{\uparrow} \cdot \overline{n_0} \cdot n_1 + \xi_n^{\downarrow} \cdot n_0 \cdot \overline{n_1}\,, \tag{2.1}$$

where n is a net, taking successively the Boolean values n_0 and n_1, and $\xi_n^{\{\uparrow,\downarrow\}} \in \mathbb{R}$ is respectively its leakage (ergodic, *i.e.* independent on the date $t = 0$ or $t = 1$) when it has a rising or falling transition. But we can consider that the gates are designed to have similar characteristics whatever their transition edge. And in most setups, the attacker does not have sensors accurate enough to distinguish between the edges. We can assume $\xi_n^{\uparrow} \approx \xi_n^{\downarrow} \doteq \xi_n$. In this case, equation (2.1) can be rewrite as:

$$\mathcal{L} = \sum_{n \in \text{nets}} \xi_n \cdot n_0 \oplus n_1\,. \tag{2.2}$$

In 2.2 we have define the Hamming Distance model (HD). If we consider in the same equation 2.2 that n_0 the reference state is equal to 0, this particular case is

named Hamming Weight model (HW). This model is particularly suitable to evaluate Dual rail counter measure with a pre-charge logic or the combinatorial part of the design for instance the input of the S-box or the data bus of a microcontroler. In these model an additive gaussian noise has to be considered. This model can be refined and enriched for instance by considering explicitly rising and falling transitions. After introducing the distinguishers we will discuss about enhanced leakage model and sensitive variables.

2.2.2 Distinguishers

Most side-channel attacks start by a tentative partitioning of the measurements, indexed by key hypotheses [SGV08]. Then, the adversary assesses the quality of each partitioning. This information is typically summarized by a figure of merit. This figure of merit can be a difference of means (in case there are only two partitions [KJJ99]), a correlation (case of the CPA [BCO04]), a likelihood (case of template attacks [CRR02]) or a mutual information (case of the MIA [GBTP08]), to cite only the few most widespread. In the following we adopt the idea that the security of a circuit is assessed by the amount of information given by a leakage function. Thus S_K is the random variable representing the secret (ideally the key values), $\mathbf{L}$ is the random variable representing the values of the leakage function, and $\mathbf{M}$ designed the Electro-Magnetic or Power measurement.

2.2.2.1 Correlation Power Analysis

An attacker uses an hypothetical model of the device under attack to predict its electromagnetic radiation. These predictions are correlated with the measured samples. We consider that $\mathbf{L}$ and $\mathbf{M}$ are two real-valued random variables, and we compute Pearson coefficient for every measurment denoted $\rho(\mathbf{L}, \mathbf{M})$, that estimates the linear correlation between $\mathbf{L}$ and $\mathbf{M}$ defined as:

$$\rho(\mathbf{L}, \mathbf{M}) \doteq \frac{\mathrm{cov}(\mathbf{L}, \mathbf{M})}{\sigma(\mathbf{L}) \cdot \sigma(\mathbf{M})}.$$

For every pair, we notice that $\rho(\mathbf{L}, \mathbf{M})$ follows the Cauchy-Schwarz inequality:

$$-1 \leq \rho(\mathbf{L}, \mathbf{M}) \leq +1.$$

$\rho(\mathbf{L}, \mathbf{M}) = 1$ (resp. $= -1$) if $\mathbf{L}$ is an increasing (resp. decreasing) affine function of $\mathbf{M}$. $\mathbf{L}$ and $\mathbf{M}$ are independent when $\rho(\mathbf{L}, \mathbf{M}) = 0$.

Therefore for every key hypothesis a leakage model is predicted and Pearson correlation coefficient is computed. The right key S_K is consequently obtained when $\mathbf{L}$ is strongly correlated with $\mathbf{M}$. For the maximal value of Pearson correlation factor the right key is obtained.

2.2.2.2 Information Theoretic Metric

In information theory **H** is the entropy introduced by Claude E. Shannon [SMY09, EG10]. Intuitively the Entropy corresponds to the quantity of information given by a source. If we consider a source as a discrete random variable X composed of b symbols of data, assuming that a symbol i has the probability $\Pr_i$ to be realized we can formally define the Entropy as:

$$\mathbf{H}(X) = -\mathbf{E}[\log_b \Pr_i] = \sum_{i=1}^{n} \Pr_i \log_b \left(\frac{1}{\Pr_i}\right) = -\sum_{i=1}^{b} \Pr_i \log_b \Pr_i.$$

where **E** stands for the mean.

We adopt the idea that the quality of a circuit is assessed by the amount of information given by a leakage function. Thus, if S_K is the random variable representing the secret (ideally the key values), and **L** is the random variable representing the values of the leakage function.
The residual uncertainty on S_K knowing **L** is given by $\mathbf{H}(S_K \mid L)$. **H** is the conditional entropy introduced by Claude E. Shannon [SMY09, EG10]. Note that this value will depend on sensitive variables chosen, and thus the quality of the leakage function. The more the sensitive variable leaks, the smaller is the entropy and more vulnerable is the circuit. For this purpose we use the concept of conditional entropy introduced by Claude E. Shannon. Let S_K the target key class discrete variable of a side-channel attack, s_K a realisation of this variable, **L** a random variable denoting the side-channel observation generated with inputs of the target device, and l a realisation of this random variable. The conditional uncertainly $\mathbf{H}(S_K \mid L)$ is defined as:

$$\mathbf{H}(S_K \mid \mathbf{L}) = \sum_{s_K} \Pr(s_K)\ \mathbf{H}_{s_K, s_K}\ ,$$

where $\mathbf{H}_{s_K, s_K}$ is the conditional entropy matrix [SMY09].

2.2.2.3 Template Attacks

Template attacks are able to break implementations and countermeasures which assume that the attacker cannot get more than a very small number of samples extracted from the attacked device. To this end, the adversary needs to target an identical hardware, which allows him to obtain some information under the form of leakage realizations. The main step is to perform a modeling process; its goal is to build classes for side-channel traces that will help the attacker to identify the secret values during the on-line phase of the attack. The information collected by profiling is used to classify some part of encryption key. Actually, the full round key has obviously too many bits to be guessed in one go by exhaustive search. In general, the key bits at the input of substitution boxes (sboxes) are targeted. In fact, they all contribute to activate the same logic, which explains why it is beneficial to guess them together. An adversary can also select other key bits if they are more vulnerable. In other words, the attacker itself selects the bits of the best

key for his attack. Guessing the correct key is a problem of decision theory. To solve it, we introduce a statistical model that is directly applicable in principle to the problem of classification. This application is mainly based on Bayes' rule, which allows to evaluate an *a posteriori* probability (that is after the effective observation), knowing the conditional probability distributions *a priori* (*i.e.* independent of any constraint on observed variables). The maximum likelihood approach provides the most appropriate model. Template attacks are composed on two steps. The first one is the Profiling Process.

- *Profiling Process:* For this step, we need a set of traces $\mathcal{S}_o, o \in [0, N'[$ corresponding to each N' operations that are also values of the sensitive variable. Traces, denoted by t, are vectors of N dimensions related to random values of plaintext and keys needed by the encryption algorithm. These observations are then classified according to functions of leakage $\mathcal{L}$. These leakage functions must depend on the configuration of the circuit, and on the implemented algorithm. This provides a framework for the estimation of the leakage during encryption. For each set $\mathcal{S}_o, o \in [0, N'[$ the attacker computes the average

$$\mu_o = \frac{1}{|\mathcal{S}_o|} \sum_{t \in \mathcal{S}_o} t,$$

  and the covariance matrix

$$\Sigma_o = \frac{1}{|\mathcal{S}_o| - 1} \sum_{t \in \mathcal{S}_o} (t - \mu_o)(t - \mu_o)^\mathsf{T}.$$

  The ordered pair (μ_o, Σ_o) associated with value o of the leakage function outputs, is called *template* and will be used in the attack to retrieve subkeys. It allows to build the ideal probability density function (PDF) of a multivariate Gaussian distribution. The second step is the Online Attack.

- *Online Attack and Success Rate* The *online attack* consists in first capturing one trace t of the target device during an encryption using the secret key κ. Knowing that each trace corresponds to one leakage value, the secret key will be retrieved from this trace by using maximum likelihood:

$$\kappa = \text{argmax}_{s_{Kc}} Pr(s_{Kc} \mid t),$$

  where s_{Kc} is the candidate key. Indeed, for each key candidate, we estimate the value of leakage by using the message or the ciphertext that is *a priori* known. The success rate is given by the average number of times where the adversary succeeds to retrieve the key $s_{Kc} = \kappa$. For each attempt the adversary can use one trace corresponding to one query, or a set of traces corresponding to different queries.

Such figures of merit are often referred to as distinguishers, as they are able to successfully distinguish between the key candidates to select the correct one.

Two approaches are traditionally considered in a view to build oracles. Either a deterministic model pre-exists and the correlation with this model is computed, or a pre-characterization of the leakage is computed and the most suitable key is selected. The comparison of these distinguishers on the same acquisition set has been already discussed in some papers [CKN00, MOP06, LCC08, GDMPV09, VCS09]. It appears that for a given partitioning, some distinguishers are better than the others to rank the correct key first, other distinguishers are better to optimize the average rank of the correct key [GDMPV09]. Moreover, the conclusions depend on the target, since the leakage structure is inherent to each device. The definition of new distinguishers is an active research area. Each new distinguisher contributes to feed a battery of attacks suitable to be launched in parallel on a device under test.

2.2.3 Leakage Model Enhancement

Another active research area is to optimize the leakage value, and devise sensitive variables. For instance, we illustrate in the Tab. 2.1 the fact that:

- a CPA [BCO04] succeeds in retrieving the secret key on an unprotected DES processor if the model with which the traces are correlated to is the Hamming distance, which is physically relevant for the device under analysis;
- a CPA with a less adapted leakage function, the Hamming Weight at the output of the substitution box, fails.

However, we notice that even if the Hamming Weight model is chosen, the correct key hypothesis does not yield the largest correlation, its correlation waveform is different from that of the incorrect key guesses.

With this example we notice that a large difference between the efficiency of leakage models exists, the success of a Side Channel Attack depends largely on the leakage model and consequently different improvements can be proposed. One first direction to explore might be to consider the sensitive variable. We call sensitive a variable, if it depends on the secret. Therefore some leakage model can be devised.

Having been convinced that both the initial and the final value of a sensitive variable shall be taken into account, we now carry out an overview of the different models by considering the acquisition campaign from DES computation. We propose to analyze the measurements sample per sample with a mutual information metric (MIM). By considering the figure 2.4, we can propose different selection functions or leakage models.

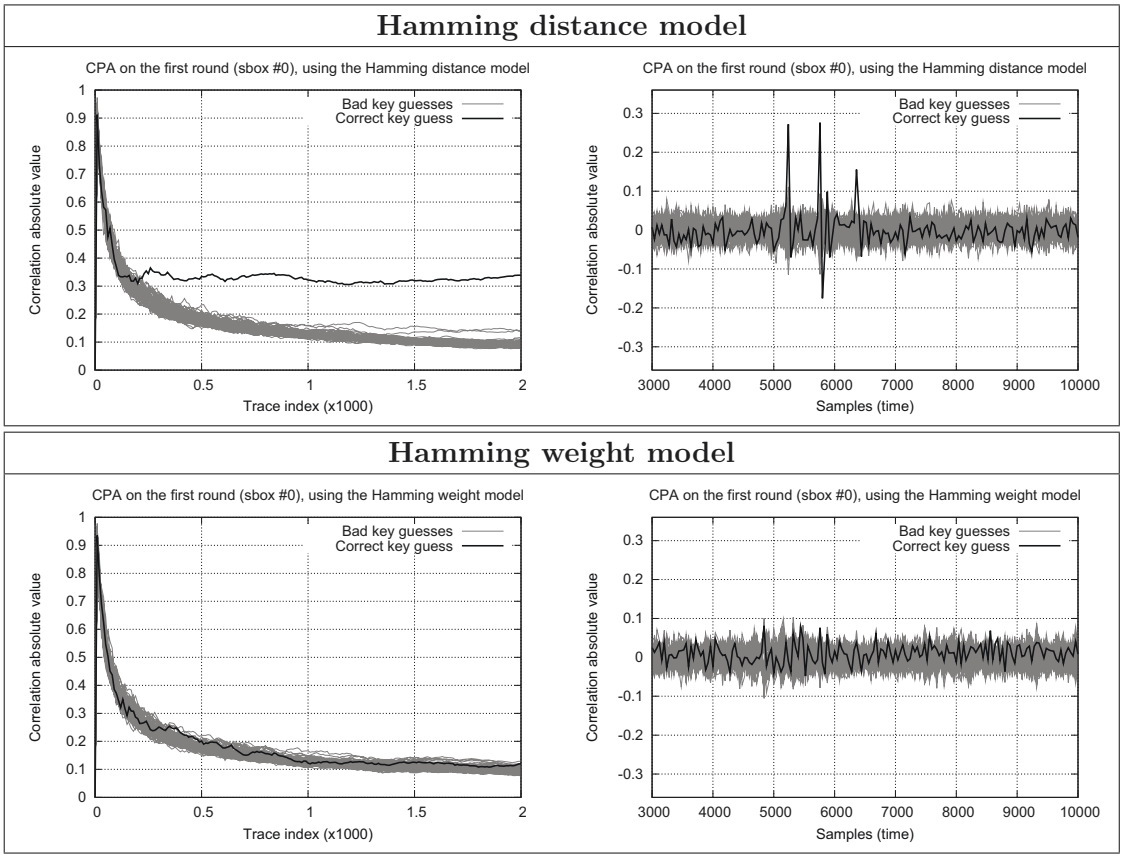
At each point of the curve, the average and the variance have been estimated for all the 2^4 following classes:

$$\mathrm{P}^{-1}(R0 \oplus R1)[4 \times n, 4 \times n + 4[\quad \in \quad \{0,1\}^4\,, \tag{2.3}$$

where:

- $R0$ and $R1$ are the initial and first round half words (made up of 32-bit) held in the right-hand side state register,

Table 2.1: Correlations evolution and final waves after estimation with 2,000 traces.



- $n \in [0, 8[$ is the substitution box ('sbox') index,
- P is the datapath permutation, that implements the diffusion.

This metric (2.3) is called `R0_XOR_R1`. Also, some non-distance mutual information metrics have been computed. Actually, three of them are used:

$$(\mathrm{E}(R0) \oplus K1)[6 \times n, 6 \times n + 6[\quad \in \quad \{0,1\}^6, \quad \text{called } \texttt{SBOX\_INPUT}, \tag{2.4}$$

$$\mathrm{S}(\mathrm{E}(R0) \oplus K1)[4 \times n, 4 \times n + 4[\quad \in \quad \{0,1\}^4, \quad \text{called } \texttt{SBOX\_OUTPUT}, \tag{2.5}$$

$$\mathrm{P}^{-1}(R1)[4 \times n, 4 \times n + 4[\quad \in \quad \{0,1\}^4, \quad \text{called } \texttt{R1}. \tag{2.6}$$

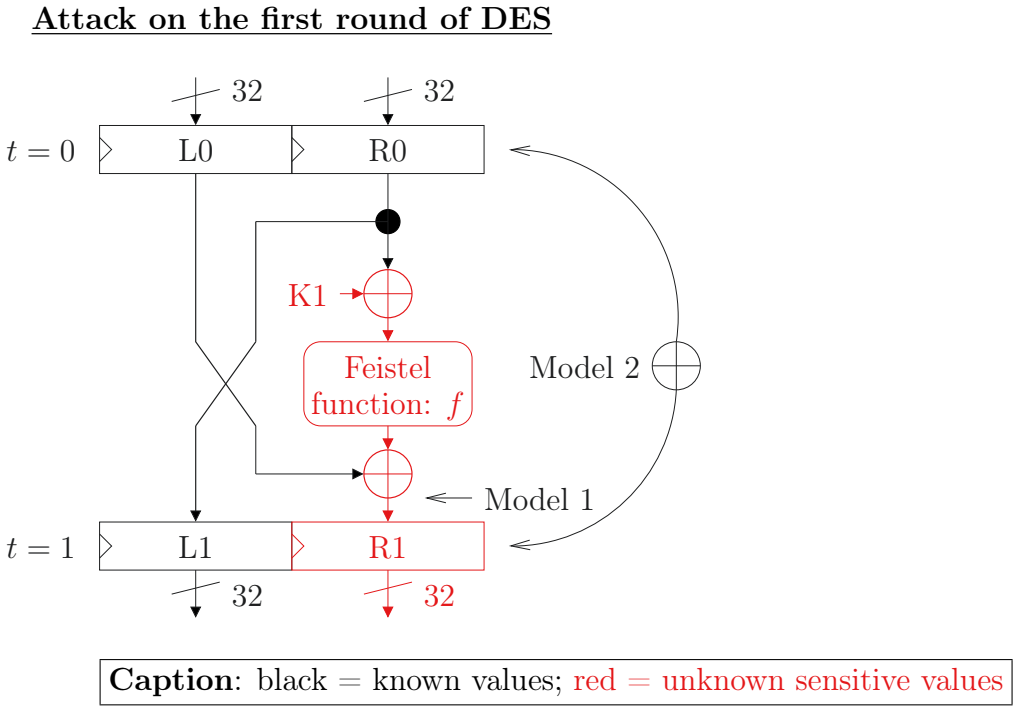


Figure 2.4: Attack on the first round of DES with different models.

In those equations, E is the expansion/permutation, S is the sbox layer and $K1$ the 48-bit key involved in the first round. Based on these data, the mutual information with the ideal value, *i.e.* equations (2.3), (2.4), (2.5) and (2.6), has been computed. The results are plotted in figure 2.5 for $n = 0$.

We can see that the distance (model `R0_XOR_R1`) leaks more than states. As a cautionary note, we indicate that this observation might be specific to the technological node of the circuit under investigation: in our case, it was designed in a 130 nanometer process; however, as underlined for instance in this article [QS07], the leakage might behave differently in very deep sub-micronic technologies.

Additionally, we observe that for the states, the information decreases with the logical depth of the probed word: (2.4) leaks about 0.05 bit, (2.5) about the half, and (2.6) only one fifth. We notice that `R1` is similar to `R0_XOR_R1`, but that only the later shows the dissipation of the DFF input latch. The MI distributions for `SBOX_INPUT` and `SBOX_OUTPUT` are close to identical; their most leaking samples almost coincide. With these examples we observe that an unprotected device might leak differently for different partitioning. However model-based attacks, such as the DPA [KJJ99], CPA [BCO04] or variants (enhanced CPA [LCC+06], *etc.*) attempt to match the measurements with a Hamming-distance model, this model is questioned by some authors like Peteers in [PSQ07a]. In multi-bit attacks, the relevance of weighting each bit by the same coefficient is indeed arbitrary. Also, weighting equally the rising and falling transitions in [PSQ07b] is not always relevant. Therefore, we can

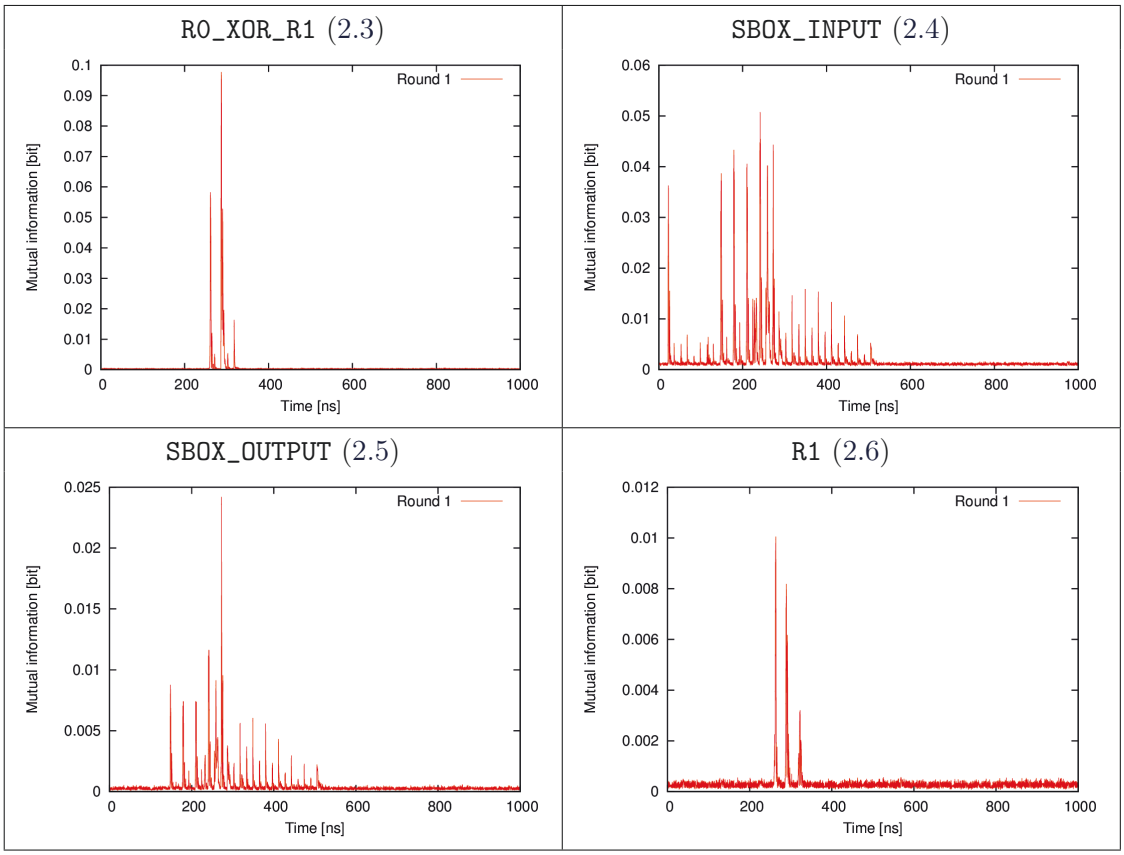


Figure 2.5: Mutual information estimated on each sample of the DES acquisition campaign.

propose some models which are more precise to estimate the leakage.

2.2.3.1 Combined Models

Assuming that those leakages are statistically independent, we propose to combine them to take advantage by using multiple partitionings simultaneously. Indeed we propose to devise a new model that is evaluated by using template attacks. Can an adversary that combines models be considered as "higher order" [Mes00]? Will he be able to recover the secret key faster? The experiment described in this section attempts to address these issues.

Let

1. **Model M1** be the value of the first round corresponding to the fanout of the first sbox. It is a 4-bit model, and

2. **Model M2** be the first bit transition of model M1. It is a mono-bit model, belonging to the general class of "Hamming Distance" models.

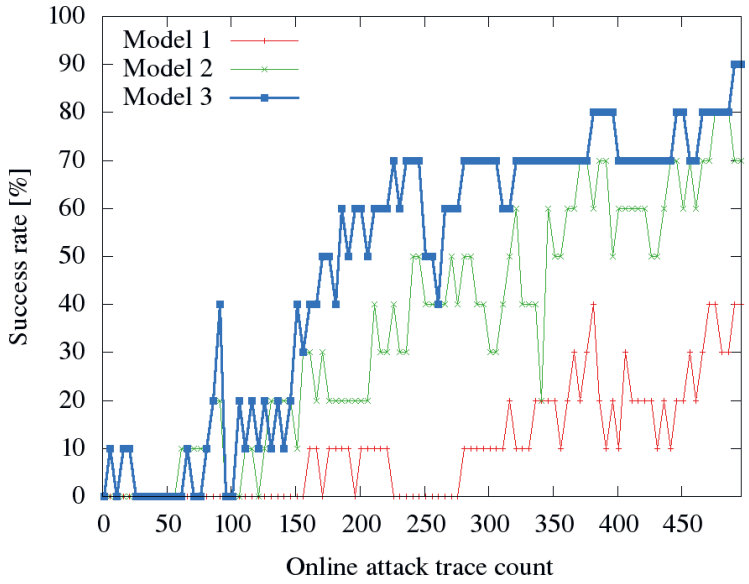


Figure 2.6: Success rate comparison between mono-partitioning models M1, M2 and combined model M3 for 1,000 traces per class.

From those two models, we derive a third one referred to as **Model M3**. M3 combines the 4-bit model M1 and the 1-bit model M2 as illustrated on figure 2.4. Therefore M3 is considered as a "bit-field structure" where the value of the most significant bit (MSB) is the model M2. The others 4 bits correspond to the model M1. M3 is the concatenation of M1 and M2, and we note M3 $\doteq$ (M1, M2). Hence M3 is a $4 + 1 = 5$ bits model, which means that M3 is based on 32 partitions. The partitioning for M3 is equal to the Cartesian product of M1 and M2 partition. The fair comparison between the models is not a trivial operation. We propose to use template attack with these models to evaluate the relevance of our partitioning. Typically, the number of templates for models M1, M2 and M3 differs. We take the same number of traces for each partition. Therefore, in total, much or less training traces are used for mono-partition models; but this is really the case when models are evaluated with as similar conditions as possible. We use an equal number of traces per class. In our experiment we take 1,000 traces per class for models **M1**, **M2**, and **M3**. Is our circuit very vulnerable against an attacker who combines models? The figure 2.6 attempts to answer this question, indeed we notice that the combine model is more efficient; with less traces for a higher success rate.

2.3 Conclusion

In this chapter we describe the main source of leakage for power and Electo-Magnetic leakage. After having introduce the most common leakage model used in litterature, we call back the state of art statistical methods and information theory methods used to evaluate the leakage in order to recover secret data from a crypto-system. Then we

detail some examples that illustrate the fact that the leakage model can be improved. Indeed it is proved that there are circuits for which those leakages are statistically independent; therefore, it is profitable to combine them, since the result of the attack will certainly be improved by using multiple partitionings simultaneously. Combined models are thus an opportunity to discover new leakage modes, as already noted for multi side-channel (power+EM) combination in [SA08a]. This note is actually a warning to security evaluators: the robustness of an implementation can be underestimated if the models are either inappropriate (since incomplete, and thus should be completed with another or some other models) or contain too few partitions.

Chapter 3

Electro-Magnetic Attacks on Cryptographic Device at Distance

In this Chapter, we will demonstrate that Correlation based on Electro-Magnetic Analysis (CEMA) on a high-performance hardware AES module is possible from a distance as far as 50 cm. Therefore we aim at mounting a successful Correlation Power Analysis (CPA [BCO04]) and retrieve cryptographic elements, without any additional device, such as a receiver or demodulator. We follow a systematic methodology that consists in leading attacks at different distances from the chip, so as to derive general laws in terms of leakage characteristics evolution. Then we notice that these attacks can be considerably improved by a strategic choice of the points of interest *(POIs)*, and by an efficient preprocessing of noisy measurements.

Contents

3.1 CEMA at Distance 35
3.1.1 The Test Bench and Implementation of AES 35
3.1.2 Leakage Indicator w.r.t. the Measurement Noise 36
3.1.3 Leakage Model at Distance 39
3.2 Techniques for Revealing the POIs 42
3.2.1 The sosd *versus* sost 42
3.2.2 Information Theoretic Metric 44
3.2.3 The PCA 45
3.3 Combining Time Samples 47
3.3.1 Observations 47
3.3.2 Sample Combination Principle and Results. 47
3.3.3 POIs Independence with the Key 48
3.4 Conclusion 50

3.1 CEMA at Distance

3.1.1 The Test Bench and Implementation of AES

The device whose EM emanations are studied is cadenced by a clock running at 24 MHz. The material is placed on a plastic table that limits the reflection of EM radiation and avoids the conducted radiation. A plastic rod is placed perpendicularly

to the board and is considered as a vertical axis to move the antenna by steps of 5 cm, as shown in the figure 3.1.

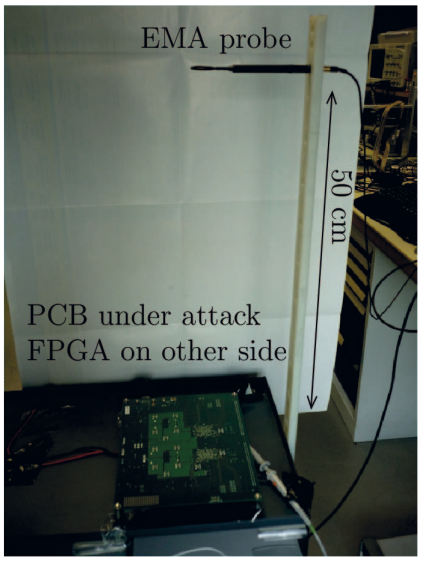


Figure 3.1: EM measurement test bench with its antenna on a plastic rod.

For each position of the antenna, we performed the same encryption and stored in a database the set of measurements. We take care of keeping away the power supply from the chip board, in order to avoid any coupling between the radiated waves and the power supply. We also record the emanations on the side of a decoupling capacitors, because the signal on this part of the board has the best quality. The targeted device is a Field Programmable Gate Array (FPGA) *Xilinx Virtex II*. It embeds an AES core supporting 128-bit keys. We study a high-performance hardware implementation of the Advanced Encryption Standard (AES). This means that all operations are done in parallel, at the rate of one AES round per clock cycle. Thus, the number of bit transitions during every clock cycle is multiplied (128 for the message and another 128 for the key state). Obviously a considerable computation noise is generated. The attacked chip has no specific countermeasure against EMA.The architecture of the AES implemented in the FPGA is depicted in figure 3.2.

Moreover an output is triggered each time an encryption begins, to facilitate traces synchronisation. This extra output could be easily removed and the synchronisation done using for instance a phase-only correlation [HNI+06].

3.1.2 Leakage Indicator w.r.t. the Measurement Noise

Firstly we check that for different distances, the curves for the same plaintext are scaled down, according to an inverse power law, as illustrated in figure 3.3. We use

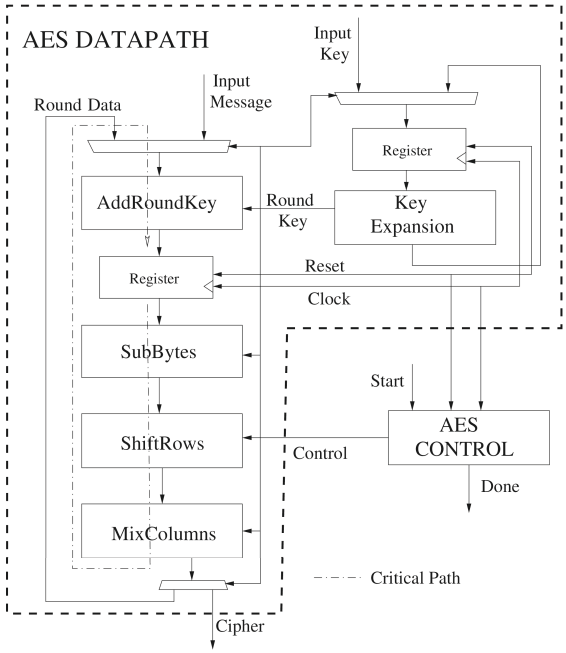


Figure 3.2: Studied AES Architecture.

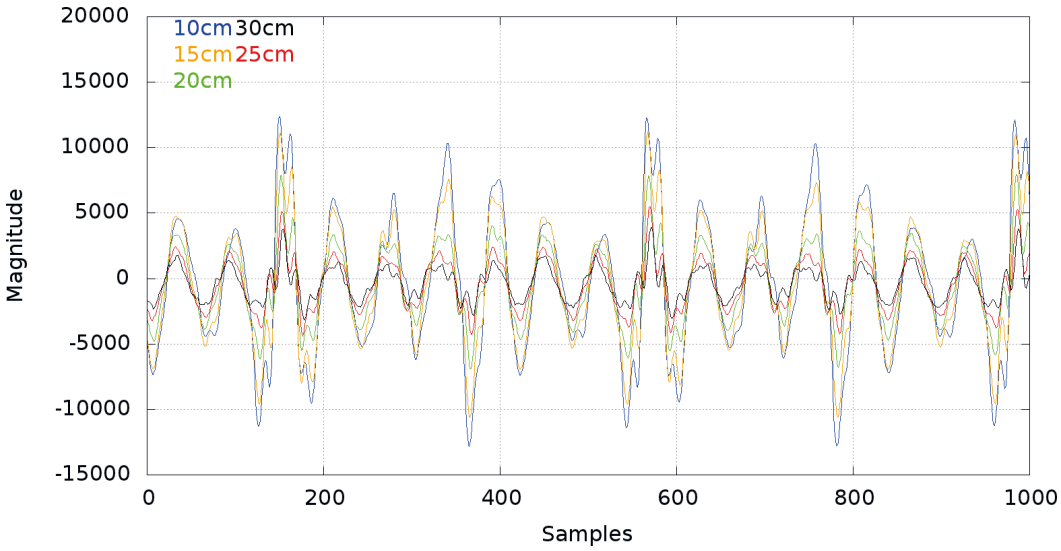


Figure 3.3: Quasi-homothetic downscale of the raw curves at different distances.

the SNR defined in [SPRQ06, Man04, CCD00] as:

$$\text{SNR} = \frac{Var(\frac{E_{leakage}}{d^i})}{Var(\mathcal{N})}$$

where $E_{leakage}$ stands for the emanation related to the secret, d^i for the distance and attenuation law ($i = 2or3$), and $\mathcal{N}$ the environmental noise. We consider that greater is the SNR, fewer traces are needed to retrieve the secret key [MOP06]. As a cautionary notice, we mention that in general, a variance does not necessarily contain information. For instance, if the variance was caused by a random number generator (RNG), it would not convey any single bit of information about the secrets. But given that we study a device without RNG, we can be assured that some information is present when the variance is non-zero. In order to estimate the SNR, we take advantage of the fact that we are able to choose the plaintexts and the key. This allows to create chosen plaintexts that activate only one substitution box (sbox). More precisely, we recorded the EM radiation of each sbox for all 256 inputs, while keeping the others at `0x00`, repeating for each distance $d \in \{0, 5, 10, 15, 20, 25\}$ cm. Our implementation of the AES is very straightforward, and has the specificity that for the first round of the encryption, the result of the key eXclusive-ORed (XORed) with the plaintext is reloaded into the same register, as sketched in figure 3.2. Due to this peculiarity, we can manage different measurements in order to evaluate the behavior of the radiated waves.

To evaluate the environmental noise $\mathcal{N}$, we performed another set of measurements. For this one, we recorded 1000 measurements without any averaging, and for every measurement the same key and the same plaintext: $K = 00x00..00$ $P = 0x00..00$. Then we caught one measurement by minimizing the activity of the 16 bytes of the register. To do so we averaged this measurement by 4 096 in a view to reduce the noise due to the other bits activity and to the environmental noise. After we compute the ratio between the mean of the 1000 measurements and the averaged trace.

Like Mangard in [Man04], we assume that the EM radiation E_{capt} of a device captured at the time t_c(Time sample when the correlation occurs) by the antenna can be written as:

$$E_{capt,t_c} = \frac{E_{leakage}}{d^i} + \mathcal{N}\,,$$

where $E_{leakage}$ corresponds to the useful part of the EM radiations caused by the attacked intermediate result and $\mathcal{N}$ is the environmental noise. In our case, we introduce another parameter: the distance between the EM sensor and the FPGA. Consequently $E_{leakage}$ at the distance d can be expressed as:

$$E_{leakage,d} = \frac{E_{leakage}}{d^i}\,,$$

where i corresponds to the attenuation law (typically, $i = 2$ or 3) [Pee06].

On one hand, we notice, as expected, that the useful signal decreases following a $1/d^i$ law of attenuation, plotted in figure. 3.5, and the noise reaches a limit when the distance increases: it stabilizes at 40^2 $\mu\mathrm{V}^2$ for $d \geq 5 \ldots 25$ cm.

Indeed, the closer we get to the electronic board, the more the noise level increases, because we capture the perturbations from the board components in addition to the ambient noise. To confirm these observations, we have performed an

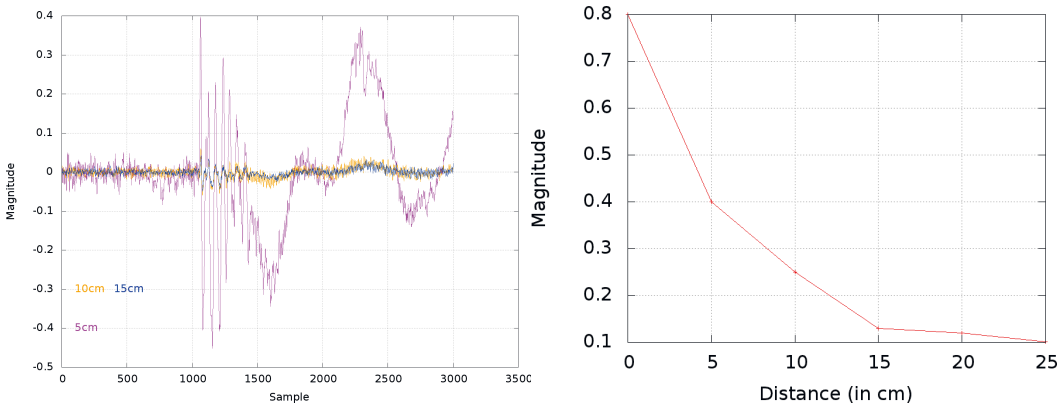


Figure 3.4: CEMA curves obtained for random cleartexts measurements at different distances and evolution of the maximal correlation value with distance.

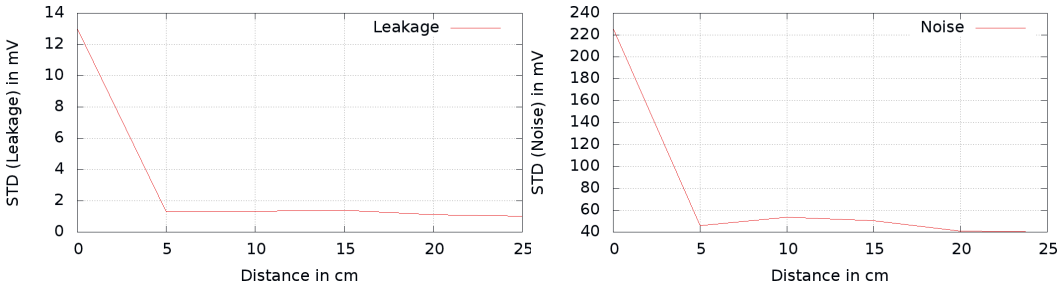


Figure 3.5: Standard deviation of the signal and of the environmental noise.

attack on the AES, when the antenna was placed much further away, at 50 cm from the FPGA board.

In practice, the signal was amplified by 60 dB and averaged by a factor of 4 096. The attack needs 51 519 measurements to recover the first byte of the key entering, whereas only 1,000 are required at $d = 0$ cm. The correlation curve is represented in figure. 3.6. The correlation does not clearly stand out. We assume that the attack requires so many traces to fully disclose the key because the Hamming weight model is not valid anymore at this large distance. Then we will study the distortion of the leakage model with the Hamming distance variation.

3.1.3 Leakage Model at Distance

It has already been noticed in the literature that the Hamming distance is not the best model in the case of very near-field analyses. For example, authors in [PSQ07b] proves that under some circumstances, an ASIC can have a transition-dependent leakage. In this section, we show that the Hamming distance model is adequate for intermediate distance fields EM analyses, but that it distorts seriously for far-field analyses.

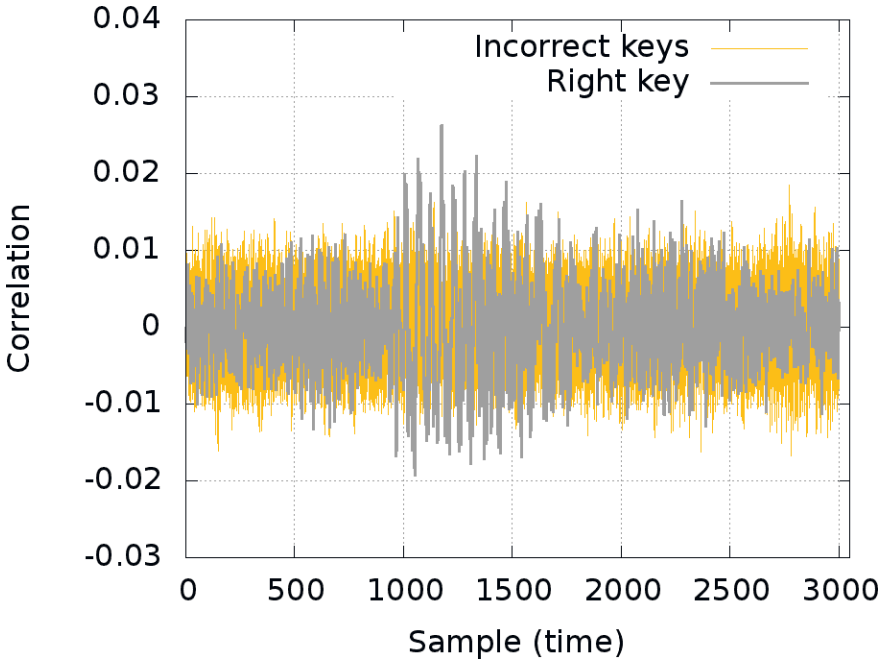


Figure 3.6: CEMA on sbox #1 at a distance $d = 50$ cm.

In near-field the leakage obeys a Hamming distance model: it is an affine function of the number of bit transitions between two consecutive states. The Hamming distance is confirmed at $d = 0$ cm, as attested by figure. 3.7, at 15 cm, the model is chaotic and not consistent.

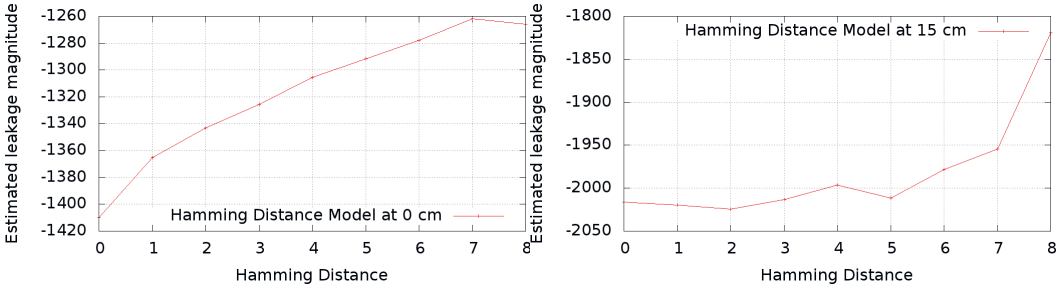


Figure 3.7: Hamming distance at 0 cm and at 15 cm.

We propose to characterize the leakage to disclose the Sbox #1 on the tenth subkey of the AES. We search the index t_c of the maximal correlation, that corresponds to the moment when the data are stored in the register on the last round. We compute for this index the mean and the variance for the 256 possible Hamming weight, the key and the message being known. The figure 3.8 depicted the leakage model at 50 cm.

We observe that the standard deviation is almost independent of the byte dis-

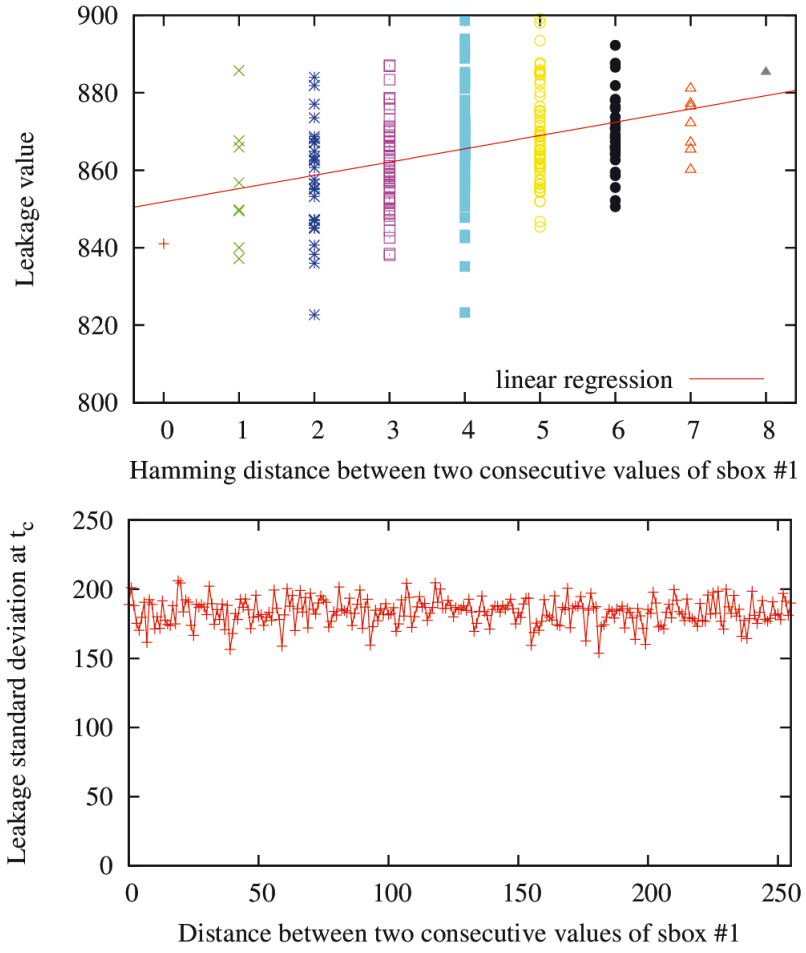


Figure 3.8: Model at 50 cm for the Sbox #1.

tances. Therefore, most of the model information is contained in the mean leakage value. We discover that the leakage model distorts more and more with the distance. Therefore, we show that the leakage models change according to thresholds. We identify three regions: in near-field, the switching distance is the most suited, as initially observed in the article [PSQ07b]; in medium-distance ($d \in [0, 5]$ cm), the Hamming distance model is suitable; then in long-distance ($d > 5$ cm), it becomes less relevant.

Also it has been underlined that the various samples garnered during the same acquisition can carry complementary information. In this context there is an opportunity to study how to best combine different samples from a single source. Different questions arise from these observations. Can we say that the leakage model depends on the temporal samples? However, we target in this topic situations where the difference of nature is not artificially due to a countermeasure, but naturally by the distortion into the communication channel between the leaking device and the side-channel sensor.

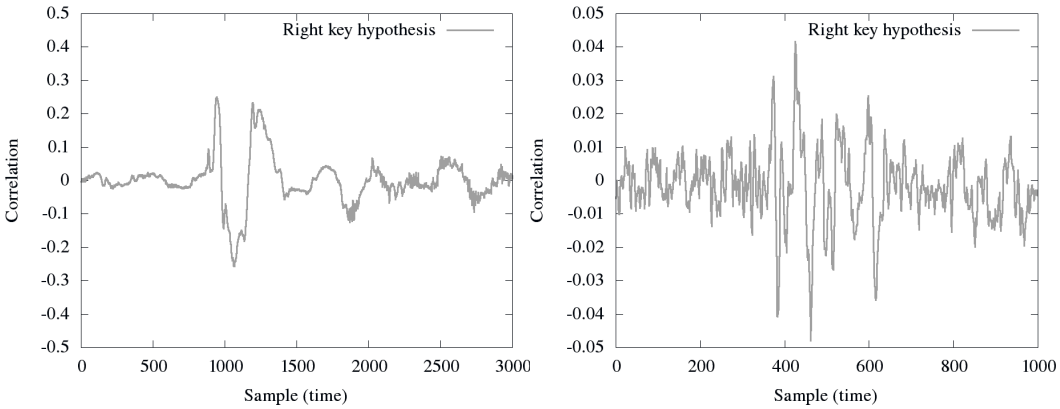


Figure 3.9: Correlation traces for campaign at 0 cm and 25 cm,right key hypothesis

3.2 Techniques for Revealing the POIs

One difficulty for improving the side channel analysis or the template attack in presence of large noise is to identify the leaking samples, also called *Points Of Interest* (POIs). They correspond to the points in time when the sensitive data is indeed processed and leaking the most. This characterization is crucial to succeed with a template attacks or an enhanced Correlation Power Analysis. The attacker has to take some care to find out the right POI because the more of them are selected, the more information is collected, but the more noise is kept. There is consequently an obvious trade-off in the selection process for POIs and the difficult task consists in separating the signal from the noise.

Several techniques have been proposed to identify the POIs and are most of the time an heuristic. The *Sum Of Squared pairwise (T-)Differences* (or sosd [GBTP08] and sost in [GLRP06]), and the *Principal Component Analysis* (PCA [APSQ06]) are four widespread examples. In this section, we study these methods and compare their efficiency, by applying them on two sets of measurements, one at short distance from the chip and an other one more noisy, at 25 cm from the chip.

For these two sets of electromagnetic measurements $\mathbf{O}(t)$ we notice that a CPA can be successfully performed, by using the Hamming distance model between the penultimate and the last round state of the AES as shown on figure 3.9.

3.2.1 The sosd *versus* sost

The computation of the sosd leakage indicator metric requires to average the traces in a given partitioning. We decide to restrict the values of the leakages to the interval $[0, 8]$, according to $\mathcal{L} = HW(\text{state}_9[sbox] \oplus \text{ciphertext}[sbox])$, where $sbox \in [0, 16[$ is the substitution box index. If we denote $o_i(t)$ all the samples (t) of the i^{th} realization of observation $\mathbf{O}(t)$, then the averages $\mu_j(t)$ in each class $j = \mathcal{L} \in [0, 8]$ is given by the mean of set $\{o_i(t) \mid l_i = \mathcal{L}\}$. Then their squared pairwise difference is summed

up to yield the sosd.

The sost is based on the T-Test, which is a standard statistical tool to meet the challenge of distinguishing noisy signals. This method has the advantage to consider not only the difference between their means $\mu_j, \mu_{j'}$ but as well their variability $(\sigma_j^2, \sigma_{j'}^2)$ in relation to the number of samples $(n_j, n_{j'})$. The definition of the sosd and sost is given below:

$$\text{sosd} \doteq \sum_{j,j'=0}^{8} \left(\mu_j - \mu_{j'}\right)^2$$

$$\text{sost} \doteq \sum_{j,j'=0}^{8} \left(\frac{\mu_j - \mu_{j'}}{\sqrt{\frac{\sigma_j^2}{n_j} + \frac{\sigma_{j'}^2}{n_{j'}}}} \right)^2 .$$

The sosd and the sost for the two EM observation campaigns are plotted in figure 3.10. We notice that the correlation trace, the sosd and sost curves are matching for the measurement at 0 cm, and the attacks based on sosd and sost work on these measurements as shown on figure 3.10.

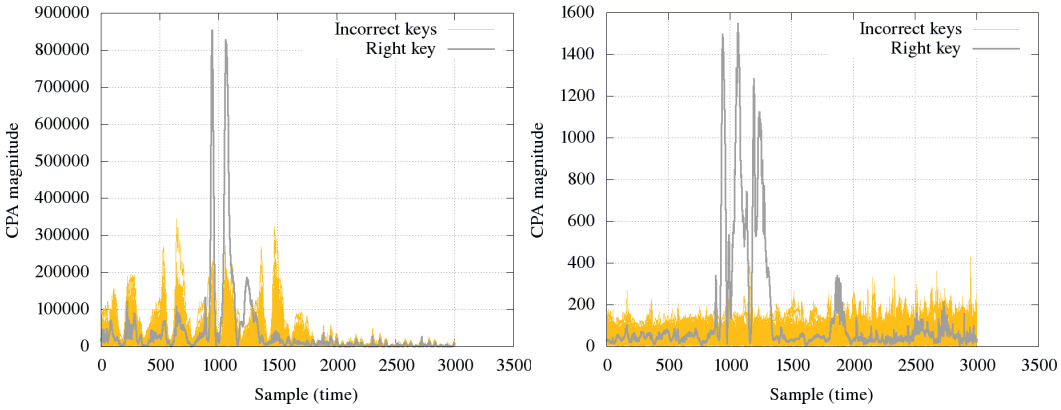


Figure 3.10: Sosd and Sost at 0 cm right key hypothesis

We use for the partitioning the same leakage function $\mathcal{L}$ and although we find the right key with a CPA on the measurement at 0 cm, the sosd and the sost curves do not highlight the time samples where the key can be retrieved by CPA. Moreover, it is important to notice that we can use these heuristics as an attack, *i.e* we have done in the case of the AES, 256 key hypotheses, and the n highest points for the measurements at 0 cm are outlined by the sosd and sost and can serve as point of interest. These n points are the highest in comparison with the level of noise obtained for the right key, and are higher than the points obtained for the bad key hypotheses. The curves obtained for the sosd and sost at 25 cm does not highlight the right POIs, the level of noise is too high, and the attack based on these heuristics do not work as good as a CPA.

Moreover the CPA with the highlighted POI at 25 cm did not succeed. This figure 3.11 shows that the sosd and sost metric is not always an efficient metric for revealing the points of interest, and have to be used when the level of noise is low and the conditions of measurement are optimal. Moreover we have tried to execute CPAs on the samples highlighted, but they all fail. Regarding the sost on the measurement at 25 cm, several POIs are revealed among samples that are not related to the secret data. Thus sost is neither a trustworthy tool to identify POIs. One reason that decreases the efficiency of these tools might be the poor PDFs estimation in presence of large amounts of noise.

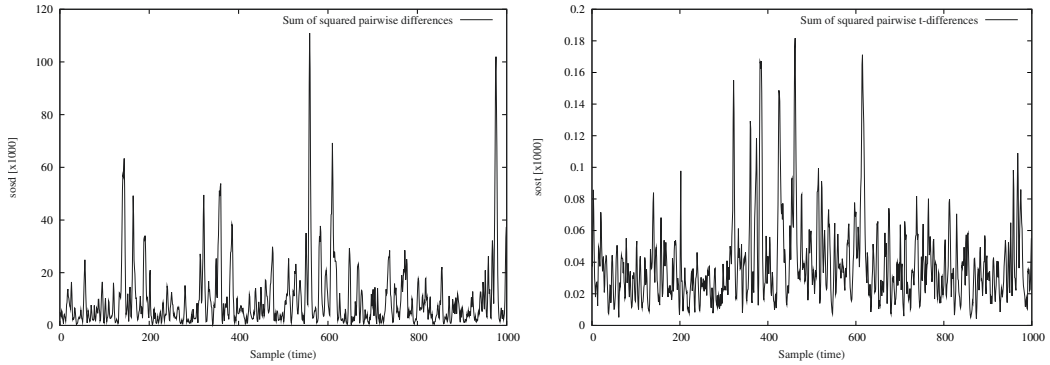


Figure 3.11: Sosd and Sost at 25 cm,right key hypothesis

3.2.2 Information Theoretic Metric

Regarding the Mutual Information, also plotted in figure 3.12 it matches well the sost at short distances, but features peaks with no information (notably the samples 441 and 975). It is thus not a reliable tool. The principal reason is that the PDFs are poorly estimated in the presence of large amounts of noise.

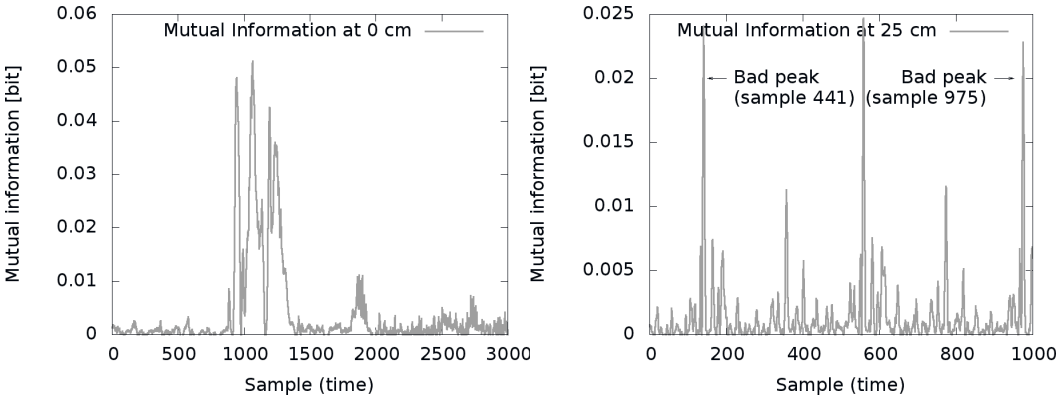


Figure 3.12: I(O;l) for campaign at 0 cm and at 25 cm,right key hypothesis

3.2.3 The PCA

One of the main contributions of the template attack is that an adversary may use all the information given by any trace. However, he is confronted with enormous data quantity he has on hand, especially for the covariance matrices computation. This method poses some issues for computations, since, because of algorithmic noise, large covariance matrices are poorly conditioned.

For this purpose, the principal component analysis (PCA) is used to get round those drawbacks. It allows to analyze the structure of the covariance matrix (variability, dispersion of data).

The aim of PCA is to reduce the data to $q \ll N$ new descriptors, that summarize a large part of (if not all) the variability. Also, it allows to better visualize the data in 2 or 3 dimensions (if $q = 2$ or 3). These new descriptors are given by the data projection on the most significant eigenvectors given by PCA.

Let EV be the matrix containing the eigenvectors classified according to the decreasing eigenvalues. The mean traces and covariance matrices are then expressed in this basis by:

$$p\mu_o = (EV)^\mathsf{T}\mu_o \qquad \text{and} \qquad P\Sigma_o = (EV)^\mathsf{T}\Sigma_o(EV)\,.$$

The PCA aims at providing a new description of the measurements by projection on the most significant eigenvector(s) of the empirical covariance matrix of (μ_j).

We propose to use the PCA with our measurement at distance. The measurements are sorted by using the following selection function $\mathcal{L} = HW(\text{state}_9[sbox] \oplus \text{ciphertext}[sbox])$. We obtain a matrice with 9 vectors.

If we compare the success rate of the CPA, applied after a PCA, we can notice, that in the case of the campaign at distance, featuring a high level of noise, the eigenvector corresponding to the greatest eigenvalue is not necessarily suitable. The success rate of the CPA after a projection onto each of the nine eigenvectors is given in figure 3.13.

At 25 cm, we notice that the projection onto the first eigenvector is not necessarily the most suitable, since it does not yield the best attack success rate. The projection onto the third eigenvector turns out, quite surprisingly, to be more efficient. At the opposite, when the noise level is low and the electromagnetic probe set at short distance, the projection onto the first vector is indeed more efficient.

This phenomena can be explained by the fact that the number of curves in the sub-set corresponding to the Hamming distances 0 and 8 are in same proportion, nevertheless the level of noise is higher, since they contain the fewest number of traces. Indeed, the proportion of traces available for the training is equal to $\frac{1}{2^8} \cdot \binom{8}{l}$, which is lowest for $l = 0$ or 8. The estimation of those classes is thus less accurate.

In order to improve the PCA, we have reduced the number of partitions from 9 to 7 sub-sets depending on the Hamming distance $HD \in [1, 7] = [0, 8]\backslash\{0, 8\}$. We observe that, under this restriction, the best success rate is obtained for the projection on the first eigenvector. In the meantime, the condition number of the empirical covariance matrix decreases, which confirms that the weakly populated

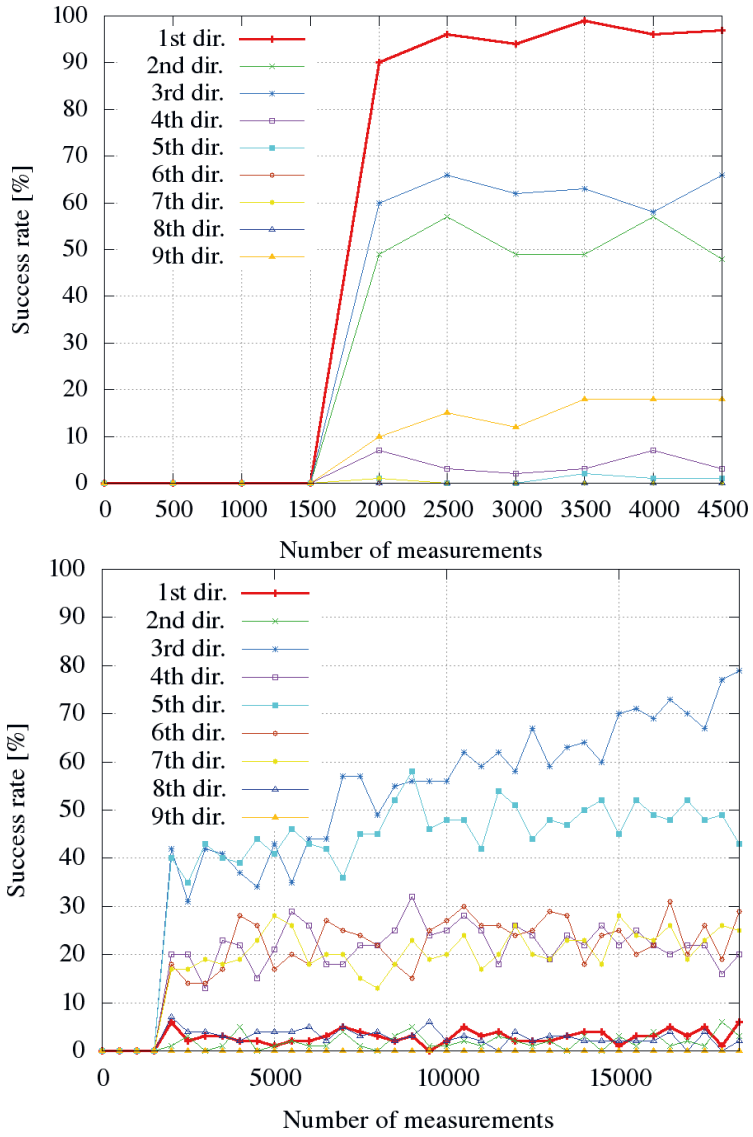


Figure 3.13: Success rate of the CPA after PCA pre-processing at 0cm (*on the left*) at 25cm (*on the right*).

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

Table 3.1: Information and probability of the Hamming weight of an 8-bit uniformly distributed random variable.

classes $l \in \{0, 8\}$ added more noise than signal to the PCA. Amazingly enough, this approach is antinomic with the multi-bit DPA of Messerges [MDS99]. If we

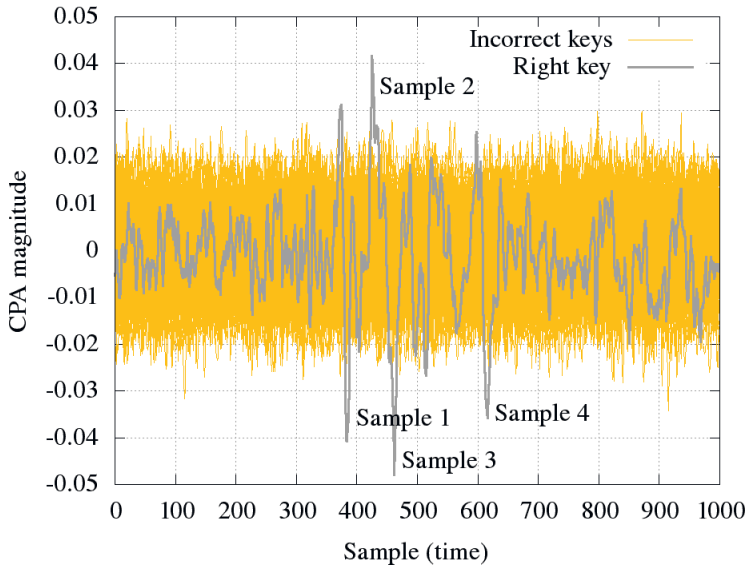


Figure 3.14: Correlation traces obtained for the right key hypotheses and for incorrect key hypotheses at 25 cm.

transpose from DES to AES, Messerges suggests at the opposite to get rid of the classes $l = [1, 7]$ and to retain only $l = \{0, 8\}$. Those extremal samples have two ambivalent properties. They convey the most information, as shown in Tab. 3.1, but also are the rarest samples, and thus are the most noisy coefficient in the covariance matrix.

3.3 Combining Time Samples

3.3.1 Observations

The correlation trace obtained for the right key with measurements at distance is given in figure 3.14. We observe that the correlation traces are extremely noisy. Moreover for some time samples, identified in as Sample{1,2,3,4} in figure 3.14, the magnitude of the correlation trace obtained for the right key is clearly higher than the magnitude of the correlation traces for bad key hypotheses. These samples are all located within the same clock period that corresponds to the last round of the AES. At the four identified time splots, the samples are undoubtedly carrying secret information.

3.3.2 Sample Combination Principle and Results.

We aim at showing that there is a gain in combining the leaks from the four identified dates. First of all, we confirm that the four samples of peak CPA are actually POIs. To do so, we perform successful CPAs at these time samples. The result is shown in figure 3.16 ; all four attacks pass over a success rate of 50 % using at least

12,000 traces. Second, we devise a method to attack that exploits at once all those samples. Similar methods have already been introduced in the context of combining samples in order to defeat masking countermeasures [PRB09]. In [CJRR99], Chari *et al.* suggest to use the product of two leakage models. In [JPS05], Joye *et al.* recommend to combine two samples with the absolute value of the difference. As in our case we intend to combine more than two samples, we resort to the product for the combination function. We apply it to Pearson empirical correlation coefficients $\hat{\rho}_t$, where t are the four identified dates. The new distinguisher we promote is thus:

$$\hat{\rho}_{\text{combined}} \doteq \prod_{t \in \text{Sample}\{1,2,3,4\}} |\hat{\rho}_t| \ . \tag{3.1}$$

As shown in figure 3.16(a), the success rate of this new attack is greater than that for mono-samples attacks. Additionally, we confirm in figure 3.16(b) that our combination defined in Eqn. (3.1), although simple in its setup, clearly outperforms a CPA after performing PCA.

In figure 3.15(a), we build all possible combinations of 3 samples among 4 samples and in (b) the combination of 2 samples out of 4. We notice, that for every product when the sample number 3 is present we obtained a better success rate.

This observation confirms those obtained by observing the success rate for the time sample on figure 3.16(a), where the best success rate for mono sample is obtained for the sample 3. We notice consequently that the leakage is not equally spread among the samples.

However, we have only shown that when knowing some POIs in the curve, a powerful combining multi-sample attack can be devised. Now, the only method to exhibit those POIs has been to apply a successful attack (a CPA in our case). Therefore, an open question is to locate those POIs without knowing the key beforehand or without conducting another less powerful attack. We suggest two solutions to spot the POIs: either online or by pre characterization on an open sample assuming the position of the POIs do not depend on the secret key.

3.3.3 POIs Independence with the Key

To check the assumption that the Points Of Interest do not depend on the particular value of the secret key, we propose to evaluate our attack of eq (3.1) on the measurements of the DPA contest v2 public data base. The traces for the DPA Contest were acquired from a SASEBO-GII board, which contains a Xilinx Virtex-5 cryptographic FPGA implementing a 128-bit hardware version of AES. We target the last round of the AES on these power measurements, and we select three time samples by considering the differential traces obtained by computing a CPA, as shown on figure 3.17. The three time samples must be chosen distinct, to avoid an important coupling between them: the attack will consequently be more powerful than without combination.

After having chosen these samples, during the characterization step, we keep the same time samples position for every S-boxes and every key. The traces of public

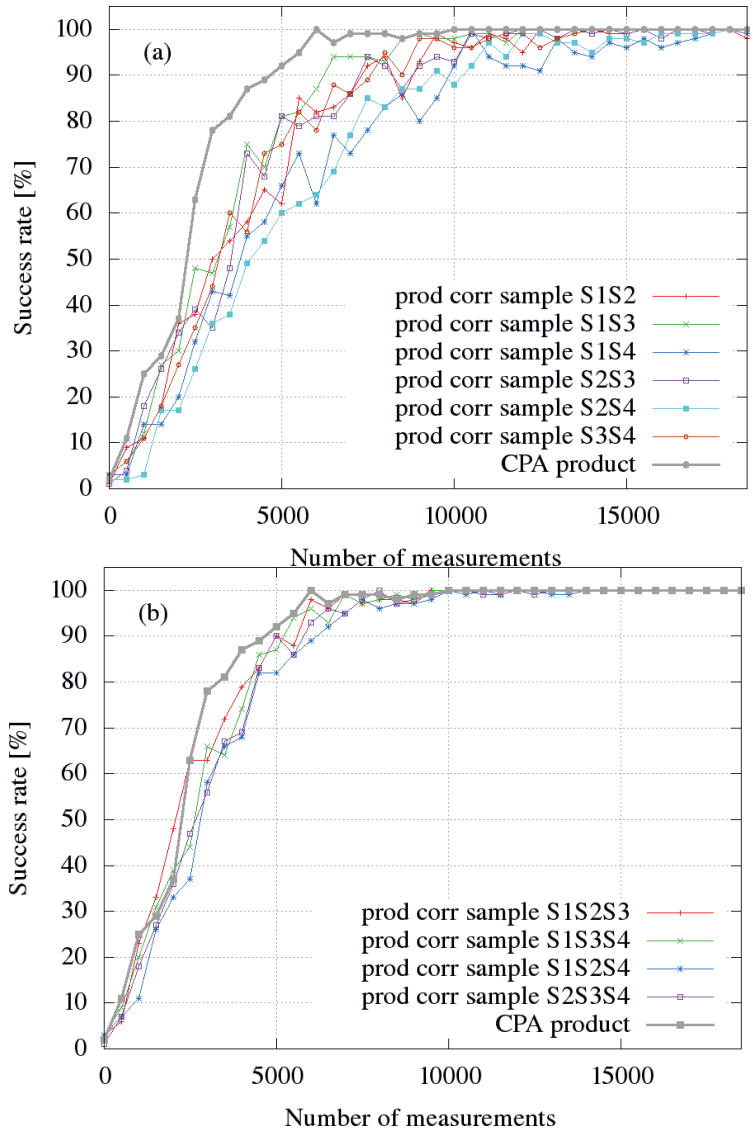


Figure 3.15: (a): Success rate of product of 2-samples correlation attack, and product of 4-samples of correlations attack; (b): Success rate of product of 3-samples correlation attack, and product of 4-samples of correlations attack.

database consist of 32 different cipher keys, each one containing 20,000 random plain texts. With these data, we are able to compute a success rate for this attack, as shown on figure 3.18.

By keeping the same time sample index, we show that we can break all the sboxes, even if we change the secret key. The figure 3.18 indeed proves that the Points Of Interest can be choose independently of the key and of the Sbox: the global success rate is definitely greater than 80% after 15,421 traces, whereas a regular CPA does not reach this score with 20,000 traces.

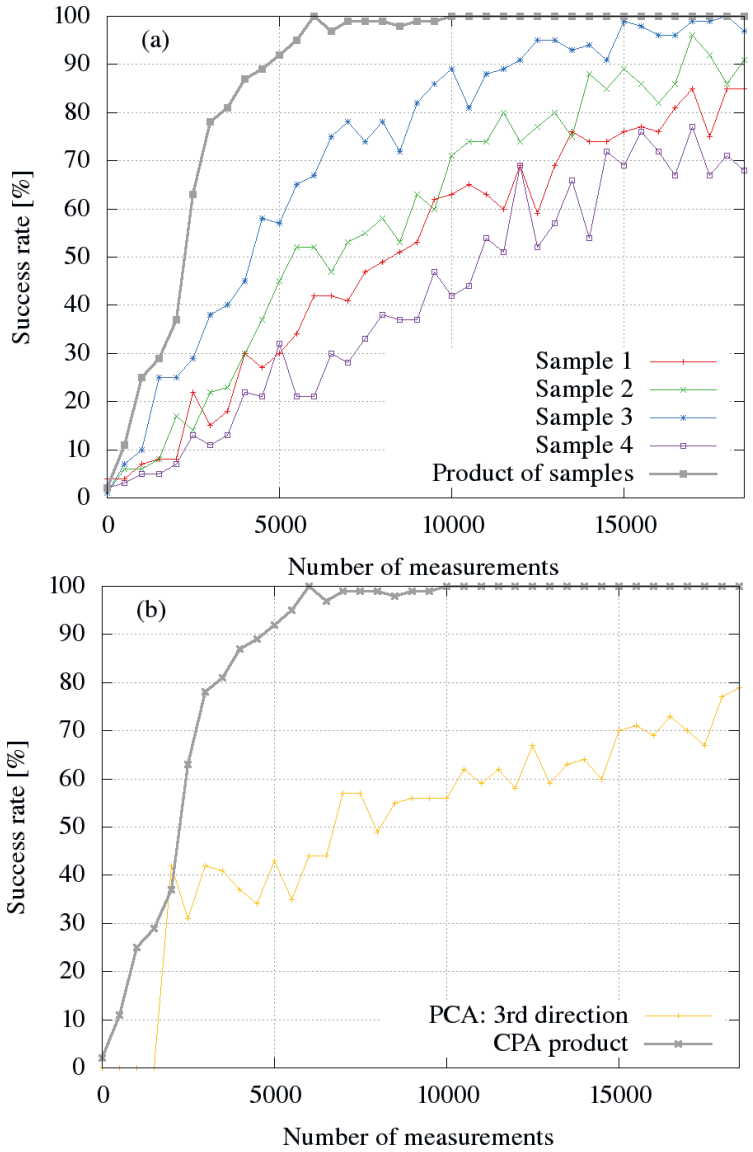


Figure 3.16: Comparison of success rates between Eqn. (3.1) with (a) mono-sample attacks and (b) pre-treatment by PCA.

3.4 Conclusion

We provide the first systematic study of CEMA as a function of the distance. Our investigations have revealed that two steps in the attacks are critical: the adequate signal amplification and the relevance of the leakage model. First of all, with a simple indicator we are able to trace the SNR curve decreasing slowly with the distance. Hence an attack at 50 cm is possible provided the signal is amplified sufficiently.

Second, we demonstrate that the leakage model distorts more and more with the distance. Therefore, we show that the leakage models change according to

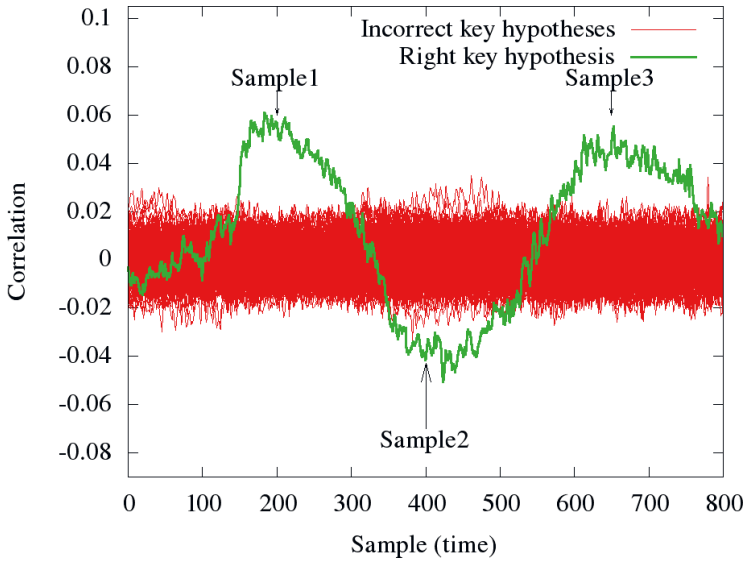


Figure 3.17: Differential traces obtained for the Sbox#2 using measurements from the DPA Contest v2 public database.

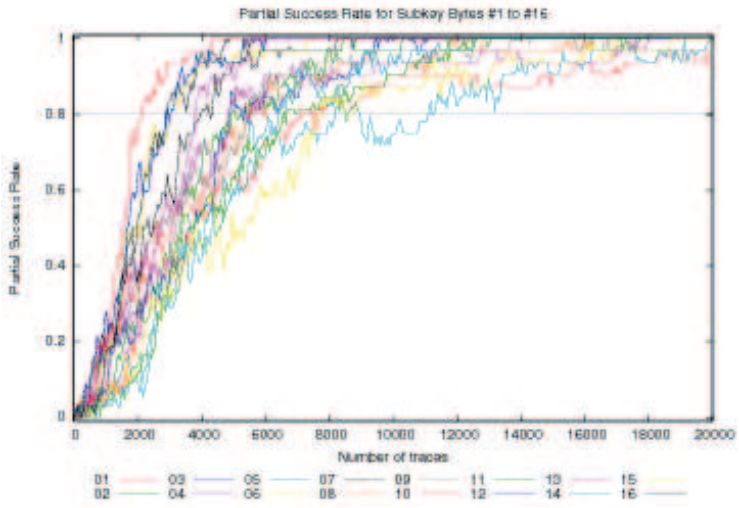


Figure 3.18: Success rate of Eqn. (3.1).

thresholds. We identify three regions: in near-field, the switching distance is the most suited, as initially observed in the article [PSQ07b]; in medium-distance ($d \in [0, 5]$ cm), the Hamming model is adequate; in long-distance ($d > 5$ cm), the model becomes less relevant. We highlight the existence of the leakage model in far field EM signals. We show how the leakage of each sample can be combined better than usual leakage reduction methods (*e.g.* the sosd, the sost or the PCA). This improvement comes from the fact that each sample features a leakage of different nature that can be exploited individually, which is out of the reach of global

techniques that consist in identifying points with large variation. Our improved combining distinguisher consists in multiplying the Pearson correlation coefficients for several POIs. Although this attack leads to better success rates than other attacks using different state-of-the-art pre-processing, we do think it can still be enhanced by another method to identify the points of interest accurately even when the side-channel observations are extremely noisy. We analyse the efficiency of a set of tools used to select POI. After, we propose a new attack by combining several timing samples in such a way a sample-adaptive model attack yields better key recovery success rates than a mono-model attack using only a combination of samples.

Part III

Characterization of the electromagnetic Side channel and demodulation techniques

Chapter 4

TEMPEST

Electronic devices such as computers or communication equipment emit energy during their operation. Various forms of energy might be produced such as electrical currents, light, conducted and radiated electromagnetic waves etc. Most of the time an important part of this energy is correlated to processed data and form unintended information leaks. These emanations allow an attacker to get unauthorized access to processed confidential data.

Therefore compromising electric and electromagnetic emanations become a serious computer security threat when the information can be remotely separated from background noise and decoded with equipment such as Radio Frequency (RF) receiver. Known as compromising emanation or TEMPEST radiation, this threat has been a significant research topic in sensitive military and diplomatic computer applications. Historically the US military code word TEMPEST (a random dictionary word) was used to call a classified US government program aimed at studying such emission security problems and at developing evaluation methods and protection standard. Then it became a synonym for compromising emanations and is used broadly in the entire field of Emission Security or Emanation security (EMSEC). This codename stands for the operation of the NSA to secure electronic communications equipment from potential eavesdroppers, and the ability to intercept and interpret those signals from different sources. In this chapter, we introduce the problematic of compromising emanation and TEMPEST radiation. After a brief history about the TEMPEST program, we present the state of art of tempest evaluation, and the different techniques of evaluation.

Contents

4.1 Historic Background 56

4.1.1 Military Issues 56

4.1.2 TEMPEST Standard 56

4.1.3 Academic Research 57

4.1.4 Protections and Countermeasures 58

4.2 TEMPEST Evaluation and Signal Acquisition 59

4.2.1 Correlated Emanation 59

4.2.2 State of the Art Methods for TEMPEST Evaluation 59

4.1 Historic Background

4.1.1 Military Issues

At the end of the 19^{th} century appeared compromising electromagnetic problem with the development of the use of the telephones. Due to extremely dense wire networks, people could hear other conversations. This phenomena named cross-talk can be easily canceled by using twisted pair cables. Many historical examples of TEMPEST attack can be recounted such as during World War I when single-wire transmission lines were used to connect telephones, and the ground acts as the return path. Therefore ground spikes were used to create ground loop that allows to quickly establish from the both sides eavesdropping posts. Another example of TEMPEST attack is described by Peter Wright against the French Embassy in London. The MI5 and the GCHQ (Government Communications HeadQuaters) a British intelligence agency tried to break the French diplomatic cipher by analyzing the compromising emanations over the telegraph cable. To this end, they used a broad band radio-frequency receiver connected to the telex cable and noticed that the ciphered traffic carried a faint secondary signal. The plaintext can be recovered from the parasitic emanations. To counter this threat different recommendations have been suggested, for instance some protections well-known in the EMC community such as shielding the equipment or the logic bus. Another required recommendation consists in taking care of the power supply lines and the ground lines in order to isolate the circuit and avoid unintentional coupling. Even with these recommendations, the *Red/Black* separation principle must be followed. It means that a distance must be maintained or a shielding installed between circuits and equipment used to handle classified plaintext (*Red*) and the rest of the normal equipment (*Black*). This kind of TEMPEST equipment must be built under careful quality control and TEMPEST test evaluation, knowing that changing even a single wire can invalidate TEMPEST Evaluation. Therefore US and NATO have defined standards, and tests for certified equipments.

4.1.2 TEMPEST Standard

The first Compromising-emanations test standard were defined by the US government in the 1950s and 1960s with the name "NAG1A" and "FS222". Now the standards define three levels of protection requirements, depending of the potential distance between the eavesdropper and the sensitive equipment:

- **NATO SDIP-27 Level A** and **USA NSTISSAM Level 1** this is the highest level of security for devices that are operated in NATO zone 0, where an attacker could have an immediate access for instance 1 m distance.
- **NATO SDIP-27 Level B** and **USA NSTISSAM Level 2** for device operated in NATO zone 1, the attacker can not get closer than 20 m distance,
- **NATO SDIP-27 Level C** and **USA NSTISSAM Level 3** for device in

NATO zone 2, the attacker is at 100 m in line of Sight or equivalent attenuation through building.

Additional standards have been published such as **NATO SDIP-29** that define the electrical installation requirements for devices handling classified information (grounding and cable distance). The **AMSG-799B** defines the "NATO zoning procedure", where individual area in a security perimeter can be classified into zone 0, zone 1, zone 2. All these standards remain classified and no information concerning the measurement procedures and the actual emission limits are publicly available. Moreover a list of the tempest compliant equipments is published by NATO agencies. It is important to know that these tests are provided by accredited testing labs and the TEMPEST certification must consider the entire system and not just an individual component, since a simple connection of an unshielded component could dramatically change the RF characteristic.

4.1.3 Academic Research

Since the 1960's, information about the TEMPEST and the risks of compromising electromagnetic emanations on computer and more largely electronic device have been published. However we can cite the work of Van Eck in 1985, where he showed that a picture displayed on cathode ray tubes (CRT) computer monitor can be reconstructed at several meters by using a basic equipment. Consequently he published in [Eck85] the first unclassified technical analysis of the security risks of compromising electromagnetic emanations. With the declassification in the 90's of a portion of the US TEMPEST standards, some others works from academic researchers came to the public. Smulders, in 1990 showed in [Smu90] that a RS-232 communication link emits unattended radiations at a distance and can be eavesdropped with low-cost material. Later Kuhn brought new elements into this area in [KA98], by eavesdropping experiments on CRT screens and LCD (Liquid Crystal Display) flat panel. In 2001, Gandolfi, Mourtel and Olivier extended the works and method on Differential Power Analysis previously published in 1999 by Kocher, Jaffe and Jun to the electromagnetic radiation in [GMO01]. With those publications they showed that it is feasible to recover secret elements from a cryptographic device without any reverse engineering of the low-level design. Just by looking for correlations with words of some bits in intermediate results of the executed algorithms, they are in position to retrieve the right key hypothesis. Quisquater and Samyde proposed in [QS05] the Simple Electromagnetic Analysis, that aims to retrieve a secret key bit sequence just by considering the electromagnetic radiation and a method of pattern matching. Agrawal, Archambeault, Rao and Rohatgi in [AARR03] established a classification between the direct and indirect emanations and showed how a secret sequence from an SSL accelerator can be recovered. In [Kuh05], in 2005 Kuhn listed the radiation risks and established the security limits for compromising Emanations. He formalized different considerations about the signal noise ratio, bandwidth of the signal, attenuations , the required material and their characteristics antenna... Moreover in [Kuh05], Kuhn showed how to create a covert channel conveyed by a crafted TV

Figure 4.1: Level A Screen Monitor, Level A Power Supply (EMI suppression filter) *source www.sst.ws*

program. In [Tan07] Tanaka showed how to estimate the amount of information that is leaked as electromagnetic emanation, and proposed to use the channel capacity to quantify the amount of information leakage via electromagnetic emanations. More recently an academic research have applied demodulation techniques to intercept keystroke signal [VP09] at distance. The attack relies on collecting Electromagnetic radiation through a bi-conical antenna from the keyboard and then decodes them to reproduce the keystrokes from the keyboard. Concretely they find out the password that has been entered on a PS/2 keyboard with a bi-conical antenna, by tunning the receiver at the frequency carrying the most information.

4.1.4 Protections and Countermeasures

Aware of these threats some research studies have been carried, for instance on protection and countermeasures. The first used protections were issued from the EMC community and aim at reducing the electromagnetic radiation by basic suppression measures:

- shielding for radiations
- filtering signal lines
- masking for spaced radiated and conducted signals.

Therefore the device was most of the time encapsulated which caused some problems of heat dissipation and made maintenance operations extremely difficult. Some progresses have been made in the protection against this threat, consisting in isolating and taking care of power supplying lines and ground lines. The devices are also better isolated and the outputs filtered. Some of these protections are shown in the figure 4.1.

Figure 4.2: Bi-conical Antenna(20 MHz to 200 MHz), Double Ridge Horn Antenna (200 MHz to 2 GHz)(*source www.dynamicsciences.com*)

4.2 TEMPEST Evaluation and Signal Acquisition

During the evaluation, the eavesdropper or evaluator has to records and analyze some accessible *Black* emanation, to evaluate the correlation with the *Red* signal or to gain information about a supposedly inaccessible signal.

4.2.1 Correlated Emanation

EM radiations arise as a consequence of current flowing through diverse parts of the device. Each component affects the other component's emanations due to coupling. This coupling highly depends on the device geometry. Therefore it is sometimes easier to extract information from signals unintentionally modulated at high frequencies. These black emanations are not necessarily related to the clock frequency, than baseband signals also referred to as direct emanations. A TEMPEST evaluation aims at distinguishing the correlation between spurious emissions of radiated energy or detectable emissions and any plaintext data that are being processed. To process this evaluation, most of the time an evaluator uses some techniques and signal detection methods similar to the ones used in Electro-Magnetic Compatibility (EMC). During this evaluation, the correlation between direct or indirect emanation and the sensitive signal have to be evaluate.

4.2.2 State of the Art Methods for TEMPEST Evaluation

4.2.2.1 A Set of Antenna

Different types of antenna exist to manage a TEMPEST evaluation. The main characteristics of the antenna are the Dipole LC oscillator and the bandwidth. The frequency selectivity depends on the $\frac{L}{C}$ ratio, a low ratio (with a large capacitance and a low inductance) makes the dipole less frequency selective. In figure 4.2 the biconical antenna that we will use in the next chapter is depicted. The choice of the antenna might be done according to the characteristics of the signal that we want to observe. For instance the energy transfered by this bi-conical antenna is optimal between 20 and 200 MHz.

4.2.2.2 Spectral Analyser

Firstly, to perform a coarse electro-magnetic analysis of the piece of equipment a spectral analyser might be used to detect the signal carriers related to the operating device. But one main drawback of this method is that the signal might be detected only if its duration is significant. Consequently compromising emanation composed from tiny and short compromising spurious peaks become difficult to detect with a spectral analyser. Another suitable but nonetheless expensive material is the wide band receiver and more specially the TEMPEST receiver.

4.2.2.3 Wide-band TEMPEST Receiver

Another method based on a wide-band receiver tuned on a specific frequency with a relative bandwidth is a suitable tool. With this equipment, the evaluator has to scan the whole frequency range of the receiver and demodulate the raw signal. With this technique we consider the Amplitude Modulation (AM) or the Frequency Modulation (FM). When an interesting frequency is detected some equipment might be added like filters and narrow band antenna. This technique of demodulation allows to consider a specific band of frequencies and improve the Signal Noise Ratio. In practice wide-band receivers such as R-1250 from Dynamic Sciences International are used in [Kuh03]. These receivers are commonly named TEMPEST receivers, and superheterodyne. It means that the signal from the antenna is filtered by a wide band pre-selector multiplied with a sine wave generated by a Local Oscillator (LO). The signal obtained after multiplication contains consequently the received frequencies shifted to two intermediate frequency ranges that depends of the LO. Another intermediate frequency filter selects one of these two terms and reduce the bandwidth of the signal. This type of receiver can be tuned on the whole range of frequencies, with different bandwidths. The gain and attenuators can be manually adjusted.

With this kind of apparatus we can detect the compromising electromagnetic emanations. But the detection of these emanation depends on the acuity of the evaluator and is time consuming and irksome. That is why we propose in the next chapter methods to automatically detect the compromising emanation. According to Kuhn [Kuh03] the measurement techniques include not only spectrum analysers, TEMPEST Receivers and oscilloscopes but devices to evaluate correlations between the *red* signal and *black* emanation.

Chapter 5

Keyboard Emanation Methods to Detect Compromising Frequencies

Characterization of the frequencies that modulate the leakage is a scientific challenge, since as of today no relevant tool allows to distinguish which frequency actually contains sensitive information. For this reason, we propose a methodology based on an empirical approach, that we contrast with another based on information theory, to characterize the electro-magnetic emanation of a keyboard. Our methodology enables attacks that can be conducted without an expensive TEMPEST receiver. Moreover electronic device manufacturors are legally required to conduct genuine TEMPEST evaluations. For them, our evaluation can give a first idea of the robustness of their devices. Also it can be seen as a preliminary test instead of a complete TEMPEST evaluation, which is time consuming and expensive.

Contents

5.1 Experimental Setup 61
5.1.1 Measurement Setup 62
5.1.2 PS/2 Protocol 62
5.2 Frequency Distinguishers 63
5.2.1 An Empirical Approach based on CPA 65
5.2.2 Approach based on Mutual Information Analysis 66
5.2.3 Frequency Distinguisher in Principal Subspaces 69
5.3 Exploiting Compromising Emanation 70
5.3.1 Confirmations of the Results with a Hardware Receiver . . . 70
5.3.2 Software Filtering 73
5.4 Conclusion 74

5.1 Experimental Setup

In this chapiter we consider the indirect emanations. These emanations are produced by non linear coupling, crosstalk... Actually, there is no method to discover how these radiations are provoked and the different reasons proposed to theoritically explain these compromising emanations are only probable causes. Proposing methods to detect unintentional and modulated radiations has become an interesting research topic. Therefore we propose different methods to find out unintentional

radiation. To perform this we reproduce the initial setup by using a keyboard which is connected to a PC with a PS/2 connection.

5.1.1 Measurement Setup

As shown in figure 5.1 we place a bi-conical antenna at 10 meters from a keyboard connected to a laptop by a PS/2 cable. In our case, we name the data signal the red signal and the signal intercepted from the antenna, the black emanation. To be sure that the radiated emissions are produced only by the keyboard, the experimental test bench is placed in Faraday cage.

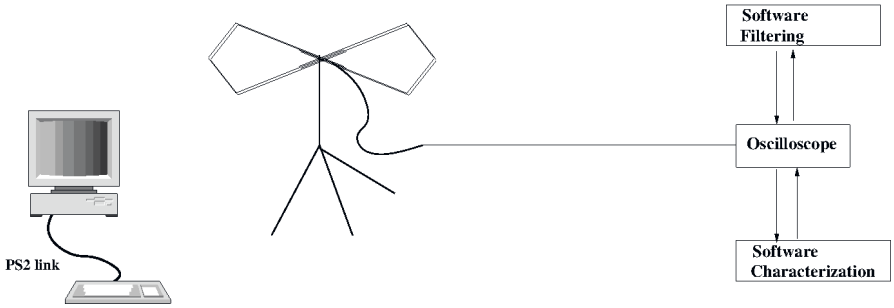


Figure 5.1: Setup used for the keyboard eavesdropping.

The attack consists in recovering the red signal from one interception of the black emanation. Ideally an efficient attack can be conducted if the eavesdropper is able to use an antenna adapted to the frequency of the signal on which the receiver is set.

5.1.2 PS/2 Protocol

The PS/2 protocol is a bidirectional serial communication based on four wires (data, clock, ground, power supply). The data and clock lines are open-collectors and have two possible states: low and high states. If no data is transmitted the data and clock lines are in the high state. The bus is "Idle" and the keyboard is allowed to begin transmitting data. The PS/2 protocol transmits data in a frame, consisting of 11 bits. These bits are

- 1 start bit, always at 0,
- 8 data bits, least significant bit first, (d_i, $i \in [0, 7]$),
- 1 optional parity bit (odd parity, equal to $\bigoplus_{i=0}^{7} d_i$),
- 1 stop bit, always at 1.

Data sent from the keyboard to the computer is read on the falling edge of the clock signal as shown in figure 5.2. When a frame is sent, the clock is activated at a frequency specific to each keyboard, typically between 10 kHz and 16.7 kHz.

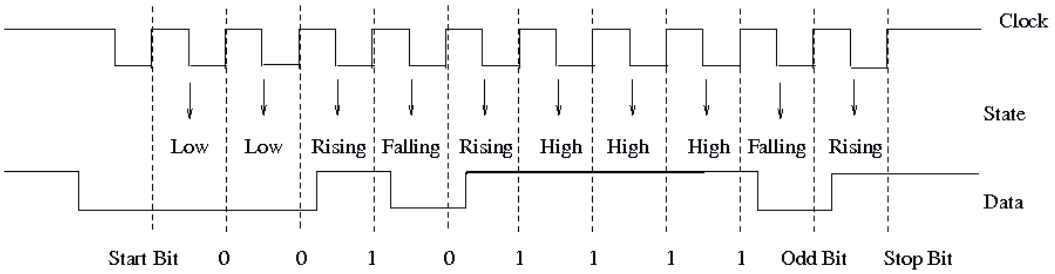


Figure 5.2: PS/2 protocol, involved in the keyboard to computer communication.

The state of sensitive data can be reconstructed thanks to the falling edge of both clock and data. Indeed because these signals are open-collectors, their low state consumes much more power than their high state. This property has already been noticed by Kuhn in [Kuh03]. The combination of the falling edge of the clock and the falling edge of the data helps the attacker in guessing the data. In fact a falling edge of the clock is always synchronized with the data start bit, contrarily to the data's falling edges whose positions depend of the keystroke. The eavesdropper can first of all build a dictionary with the positions of data's falling edges as a function of the key stroked.

5.2 Frequency Distinguishers

The phenomena of compromising signal has different origins such as radiation emitted by the clock, crosstalk or coupling. Traditionally, we differentiate the direct emanations and the indirect or unintentional emanations. The first ones can be considered at a very short distance and requires the use of special filters to minimize interference with baseband noise. The direct emanations come from short bursts of current and are observable over a wide frequency band. On contrary, indirect emanations are present in high frequencies. According to Agrawal [AARR03] these emanations are caused by electromagnetic and electrical coupling between components in close proximity. Often ignored by circuits designers, these emanations are produced by a modulation. The source of the modulation carrier can be the clock signal or other sources, including communication related signals. Li *et al* provide in [LMM05] a model to explain such kind of modulation.

In [VP09], Vuagnoux and Pasini use standard techniques, such as Short Time Fourier Transform (STFT) and compute spectrum to detect compromising emanations and more precisely direct emanations. The STFT provides a 3D signal with time, frequency and amplitude. Another approach is traditionally done by using a spectral analyser to detect signal carriers. Thus the whole frequency range of the receiver is scanned and at each potential frequency of interest the signal is demodulated by the evaluator and manually checked for a presence of red signal.

We lack a lot of information about the TEMPEST tests, which remain classified.

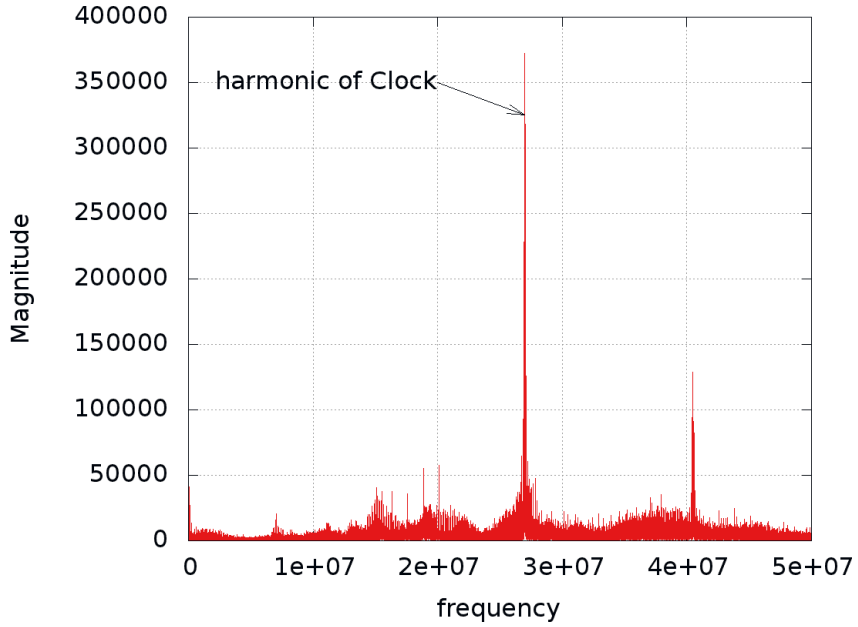


Figure 5.3: Spectrum of the black emanation.

Nevertheless, figure 5.3 lets us think that the tools employed for this kind of evaluation are not only based on the spectrum analysers commonly used in standard Electro-Magnetic Compatibility (EMC) and Radio Frequency Interference (RFI) testing. As shown in figure 5.3, the signal in the frequency domain becomes exploitable beyond 15.0 MHz, which is coherent with our equipements specifications. The bi-conical antenna is amplified with low-noise amplifier of 60.0 dB gain and has an approximative bandwidth of 20.0 MHz to 200.0 MHz. Consequently we cannot observe the low frequencies of the data signal, but we observe a high peak at 28.0 MHz. This peak could correspond to some odd harmonic of the internal keyboard microcontroller, for instance the seventh (7.0×4.0 MHz) for a microcontroller inside the keyboard running at a frequency of 4.0 MHz, depending on the device constructor, as described in [tes, tod].

Hence the indirect emanations are also caused in our case by the cross-talk and the coupling between the internal frequency clock of the keyboard's microcontroller, the data and the clock frequency signal of the PS/2 line. Besides the FFT applied on the whole black emanation does not provide us every leaking frequency.

Therefore we propose in the sequel an approach based on the correlation between the red signal measured directly from the target system and the black emanation, noisy and distorted, received from antenna. We can distinguish the keystroke by the position of the falling edges of the data signal. We propose to gather a large number of measurements with the same keystroke. Each pair is composed of a red signal related to the data and a black emanation from the antenna as shown in figure 5.4. After acquisition the black emanation is cut according to the data, represented by the red signal.

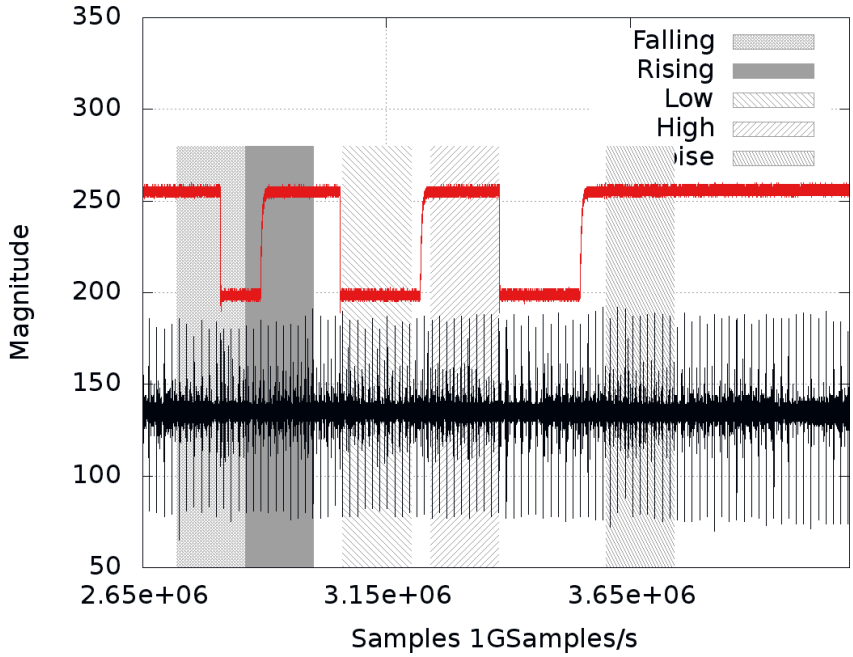


Figure 5.4: Red signal/Black emanation.

The parts of the black emanation correspond respectively to the low state, high state, falling edge and rising edge of the red signal, and an additional part corresponds to the ambient noise. When no data is transmitted by the PS/2 link, the bus line is in the "Idle" state (*see Section 5.1.2*). After this windowing phase we perform a FFT for each part of the measurement. Using a FFT and frequency domain is one technique also used by Shimmel *et al* in [SDB+10]. Each section of the signal is equal in term of number of samples. Then we calculate an average spectrum and the variance for each part of the signal. It is noticeable that the results do not change with the size of the window. We introduce a technique inspired from the Correlation Power Analysis.

An approach based on the correlation between the red signal measured directly from the target system and the electro-magnetic emanation, is appropriate. As we will see in the next section, we can attribute to each part of the signal a specific spectral signature. We propose in Section 5.2.1 an empirical approach.

5.2.1 An Empirical Approach based on CPA

We use an approach derived from CPA, introduced in [BCO04]. However we process the signal in frequency domain, as already shown in [GHT05, SDB+10] by Gebotys and Schimmel where they introduced the DFA, *i.e.* the Differential Fourier Analysis. In this technique, the FFT (*Fast Fourier Transform*) is used to avoid synchronization problems. In [PHF08], the FFT is used to mitigate randomization countermeasures like shuffling. Here the FFT is used in order to select the frequencies which are carrying sensitive information and their bandwidth for characterizing the EM side

channel. It is a profiling stage in the frequency domain that allows to learn details about the frequencies that depend on the red signal. Therefore we compute the difference between

- the mean of the spectrum related to a specific state and
- the mean of the noise spectrum (*i.e.* when nothing occurs on the PS/2 link).

Then we divide this difference by the variance of the noise. It is suggested by Le *et al* in [LCC+06] that in some cases the normalization factor induces a high noise level in CPA signal. To avoid this artifact, it is recommended to add a small positive constant ε to the denominator. Thus we obtained four vectors in the frequency domain by computing:

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

where $E(f, State)$ and $E(f, N)$ represent the averaged spectrum curve obtained respectively for one state and for the noise and $\sigma(f, N)$ stands for the variance of the noise for every frequency f. State is a state from the *StateSet* set, defined as the set containing all the possible configurations of the red signal: $StateSet = \{High, Low, Falling, Rising\}$. The four frequency vectors corresponding to each state are plotted in figure 5.5. From these curves, we can deduce the range of frequencies that characterize each state.

The "correlation" level in $\rho(f, Falling)$ is higher and contains a lot of frequency peaks compared to the other frequency domains traces. We notice three ranges of relevant frequencies:

- between 14.0 and 20.0 MHz,
- between 24.0 and 32.0 MHz,
- between 40.0 and 49.0 MHz.

5.2.2 Approach based on Mutual Information Analysis

In section 5.2.1, we highlighted a range of frequencies that can possibly carry information about the red signal. Now we adopt an information theory viewpoint. In previous work [Tan07], Tanaka used the calculation of the channel capacity (using information theory) for evaluating the success rate of spied images reconstruction. The author calculates the amount of information per pixel in the reconstructed image and estimates a threshold from which it is effective. In our case, it is also interesting to adopt a method based on the information theory, in order to retrieve the relevant frequencies and to bring evidence that the information is not necessarily carried by the clock frequency and its harmonics such as specified by Carlier *et al.* in [CCDP04, CCDP05].

In 2008, Gierlichs introduced in [GBTP08] the Mutual Information Analysis. This tool is traditionally used to predict the dependence between a leakage model

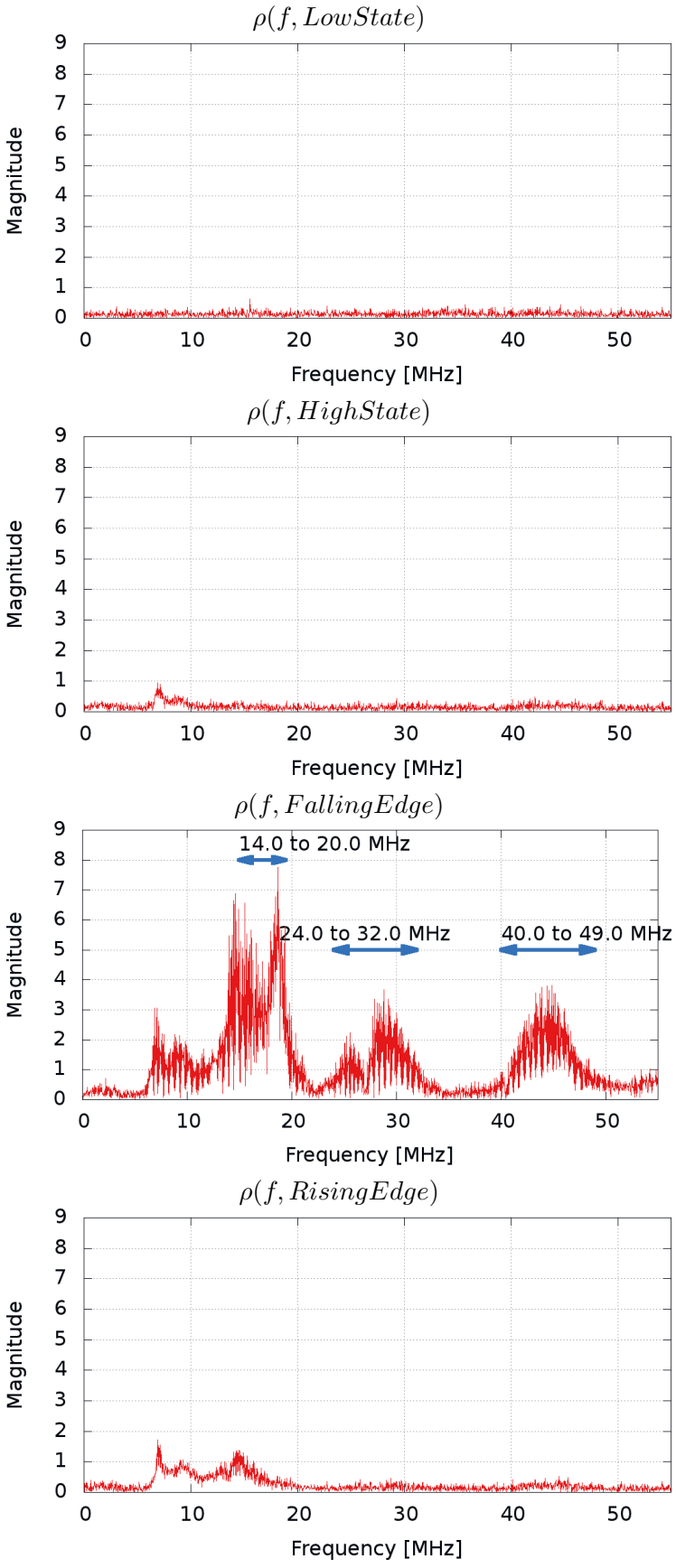


Figure 5.5: Results of the Correlation for every state.

and observations (*or Measurements*). Therefore we can use it as a metric that gives an indicator on carriers frequencies. To do so, we compute for each frequency the Mutual Information (MI) $\mathrm{I}(O_f; State)$ between Observations O_f and $State$ that corresponds to the state of the red signal. Thereby, if $\mathrm{I}(O_f; State)$ is close to zero for one frequency, we can say that this frequency does not carry significant information. On the contrary, if $\mathrm{I}(O_f; State)$ is high, the sensitive data and the frequency are linked. If we filter the black emanation around this frequency, we can retrieve a significant part of the red signal. The MI is computed as:

$$\mathrm{I}(O_f; State) = \mathrm{H}(O_f) - \mathrm{H}(O_f|State) \ , \tag{5.1}$$

where $\mathrm{H}(O_f)$ and $\mathrm{H}(O_f|State)$ are the entropies respectively of all the observations and of the observations in frequency domain knowing the $State$. Both of these entropies can be computed using:

$$\begin{aligned} \mathrm{H}(O_f) &= -\int_{-\infty}^{+\infty} \Pr(O_f)(x) \log_2 \Pr(O_f)(x)\, \mathrm{d}x \ , \\ \mathrm{H}(O_f|State) &= \sum_{s \in State} \Pr(s) \mathrm{H}(O_f|s) \ . \end{aligned}$$

with

$$\mathrm{H}(O_f|s) = -\int_{-\infty}^{+\infty} \Pr((O_f)(x)|s) \log_2 \Pr((O_f)(x)|s)\, \mathrm{d}x \ ,$$

where $\Pr(O_f)$ denotes the probability law of observations at frequency f. The random variable O_f takes its values x on $\mathbb{R}$, and $\Pr(O_f)(x)\,\mathrm{d}x$ is the probability that O_f belongs to $[x, x + \mathrm{d}x]$. Besides we consider that the states configuration are equi-probable events therefore $\forall s \in State$, $\Pr(s) = \frac{1}{4}$. And the distribution of $\Pr(O_f)$ is assumed to be a normal law $\sim N(\mu, \sigma^2)$ of mean μ and variance σ^2, given by:

$$\Pr(O_f)(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \ ,$$

we call a parametric model. We approximate this model by a parametric estimation, and we use the differential entropy defined for a 1-dimensional normal random variable O_f of mean μ and standard deviation σ as the analytical expression: $H(O_f) = \log_2(\sigma\sqrt{2\pi e})$. From this value, the Mutual Information defined in Eqn. (5.1) can be derived, by combining for each state the differential entropy:

$$\mathrm{I}(O_f; State) = \mathrm{H}(O_f) - \frac{1}{4}(\mathrm{H}(f|High) + \mathrm{H}(f|Low) + \mathrm{H}(f|Rising) + \mathrm{H}(f|Falling)) \ ,$$

that can be simplified as:

$$\mathrm{I}(O_f; State) = \frac{1}{4} \log_2 \frac{\sigma_{O_f}^4}{\sigma_{O_f,High} \times \sigma_{O_f,Low} \times \sigma_{O_f,Rising} \times \sigma_{O_f,Falling}} \ . \tag{5.2}$$

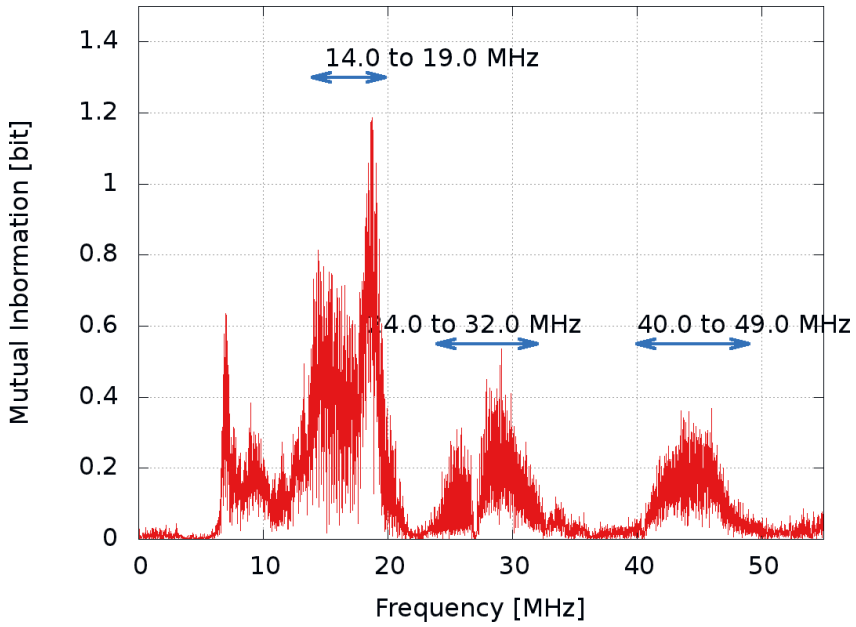


Figure 5.6: Result of Mutual Information Metric I(f; $State$).

The figure 6.13 represents the result of Eqn. (5.2).

The result of the MIA are similar to that of $\rho(f, FallingEdge)$: we obtain the same ranges of relevant frequencies. In this respect, we confirm that some frequencies radiate more information than the others. As this method provides a result with a quantity expressed in bit, the leakage frequencies are easy to interpret. Consequently we are now able to fairly compare the level of compromising signal emanated by different keyboards or electronic devices. Such a MI metric also allows to quantify the level of protection against TEMPEST attacks. In addition to the CPA approach, it is worthwhile to underline that MI considers the non linear dependencies; this metric is able to capture any coupling, such as cross-talk, that occurs when keys are pressed on a PS/2 keyboard.

5.2.3 Frequency Distinguisher in Principal Subspaces

The identification of relevant frequencies can also benefit from the PCA (Principal Component Analysis). The PCA has been applied to side-channel analysis by Archambeau *et al.* in [APSQ06] and Standaert *et al.* in [SA08b] in the case of template attacks.

In order to investigate the benefit of PCA, we have adapted it to our topic. In this approach, we use the same partitioning as defined previously in section 5.2. The observations of black emanation in frequency domain are classified according to the state of the data signal, in order to build the covariance matrix. We denote by $\mu_j(f)$ the average of the observations corresponding to a state j, and by $\mu(f)$

the average of all the observations:

$$\mu(f) = \sum_{j \in StateSet} \mu_j(f).$$

The attacker also computes the covariance matrix Σ_o, as:

$$\Sigma = \frac{1}{4} \sum_{j \in StateSet} (\mu_j(f) - \mu(f))(\mu_j(f) - \mu(f))^{\mathsf{T}}. \tag{5.3}$$

The PCA gives us four main components, which are linear combinations of the averaged measurement in the frequency domain of the emanations for every state. These components form a basis, which characterizes four modalities of compromise. The main leakage modality is given by PCA as the eigenvector corresponding to the largest eigenvalue. The four eigenvectors are plotted in figure 5.7.

On the first eigenvector, the three frequencies ranges identified by CPA and MI are visible. Nonetheless, the ranges [24.0, 32.0] MHz and [40.0, 49.0] MHz have a small amplitude and are noisy. Additionally, one narrow peak appears at $f = 27$ MHz, that can be bound to the frequency of the keyboards' microcontroller.

The second eigenvector is very similar to the first one. Anyway the ratio between the largest eigenvalue and the second one is greater than five orders of magnitude. This means that the first direction contains an overwhelming quantity of information.

The fourth eigenvalue is theoritically null, but because the covariance matrix is badly conditioned the numerical computation yields value 2×10^7 this indicates that the eigenvector corresponding to small eigenvalue are very approximative, thus untrustworthy. Therefore the two last ones carry mostly noise information. However the PCA does not consider the non-linear dependencies.

To summarize, in Tab. 5.1 we establish a comparison between the different methods.

To verify the results obtained with the three previous methods, we have set up the following two experiments. The first one consists in using a hardware receiver, as described by Agrawal in [AARR03] and Kuhn in [Kuh03]. The second one consists in software demodulation thanks to an appropriate filtering.

5.3 Exploiting Compromising Emanation

5.3.1 Confirmations of the Results with a Hardware Receiver

As described in chapter 4, we propose to use a receiver similar to the one presented by Kuhn and depicted in figure 5.8. Those receivers are super-heterodyne and wideband. They offer a large panel of configurations. For example, they can be tuned continuously between 100 Hz and 1 GHz and they offer the selection of 21 intermediate frequency bandwidths from 50 Hz to 200 MHz. They switch automatically

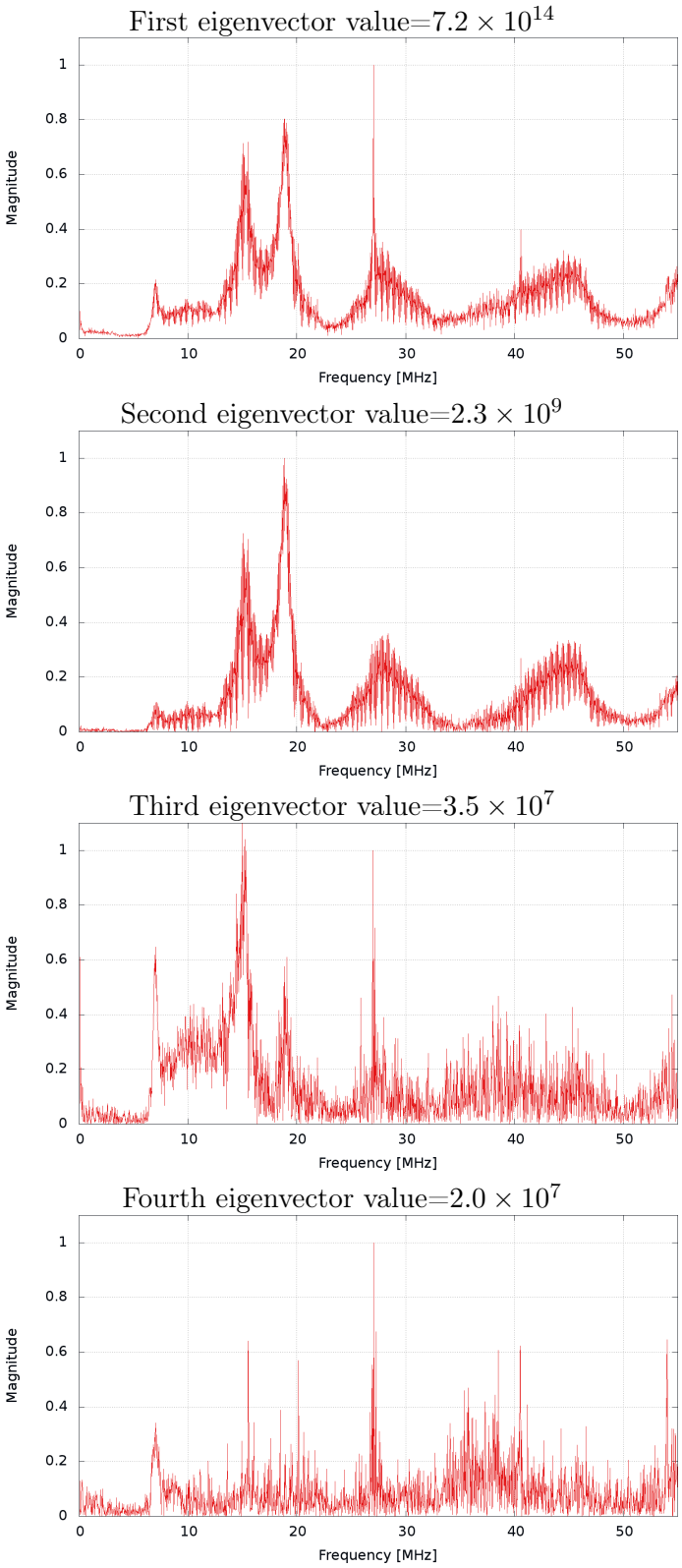


Figure 5.7: The four eigenvectors obtained by PCA.

Distinguisher	Advantages	Drawbacks
CPA	⋆ Easiest method.	⋆ Four results curves. ⋆ Hard to compare two implementations. ⋆ Only linear dependencies considered.
MIA	⋆ Based on information theory. ⋆ Single curve result. ⋆ Commensurable results (Mutual Information values are expressed in bits). ⋆ Non-linear dependencies considered.	
PCA		⋆ Hard to compare two implementations. ⋆ Results are not only on first eigenvector. ⋆ Spurious peaks appear. ⋆ Only linear dependencies considered.

Table 5.1: Drawbacks and advantages of the three analyzed distinguishers.

between different pre-selection filters and mixers depending on the selected tuning frequency. Therefore those devices are quite expensive and uncommon. These devices are usually used to receive an Amplitude Modulated narrow-band signal:

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

where f_c is the carrier frequency, $v(t)$ is the broadcast signal, A is the carrier's amplitude and m is the modulator's amplitude. Concerning the setup measurement represented in figure 5.1, we use the receiver instead of the oscilloscope. With such a device, we successfully demodulate the black radiation at various frequencies, as shown in figure 5.10. We focus on a range of frequencies between 0.0 and 50.0 MHz, and demodulate at the frequencies exhibited by the previous methods (PCA, MIA and PCA), at 17.0 MHz, 27.0 MHz and 41.0 MHz with a bandwidth of 1 MHz. Each time, the demodulated signal shows a peculiarity that allows to distinguish clearly the state of the red signal. More precisely, the falling edge of the red signal is indicated by a clear peak. This concurs with the observation about the "falling edge transition technique" explained by Vuagnoux in [VP09]. Also, it is consistent with observations from section 5.1.2.

Moreover the data are read on the falling edge of the clock. Consequently the falling edge of the clock occurs just after the falling edge of the data, as already

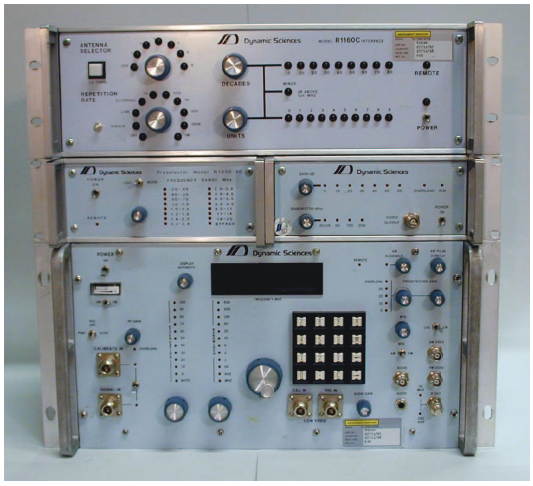


Figure 5.8: R-1250 wide-range receiver and its preselector and wide-band AM detector, *source M Kuhn Thesis*

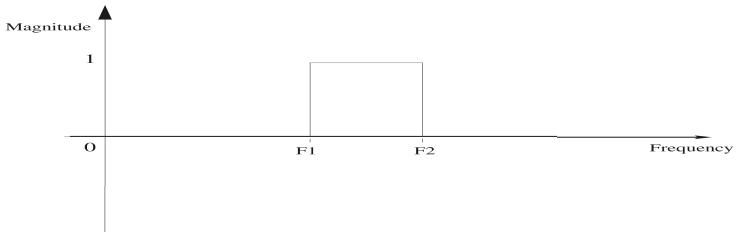


Figure 5.9: Design of bandpass filter.

shown in figure 5.2. We see on the demodulated signal that the energy at dates corresponding to the clock falling edges is not constant. Empirically, clock peaks have more energy when the state of data signal is high, and are doubled by falling transitions of the signal data. This is another leakage that can be used to recover the red signal.

During these experiments we noticed another kind of compromising signal not based on the "Falling edge Transition Technique". As shown in figure 5.11, at the frequency 36.0 MHz, only the signal related to data (falling edge) appears, whereas the peaks bound to the clock completely disappear. This compromising signal is not very obvious to characterize, and requires some care to find this particular frequency of demodulation. In this case, the TEMPEST receiver definitely provides us the setup to pinpoint this compromising frequency.

5.3.2 Software Filtering

To estimate the part of the sensitive signal contained in our measurements, and also to find the compromising signal, we devise a software band-pass filter using

MATLAB. We perform bandpass filtering within the range frequencies identified during the leaking frequencies characterization stage.

We propose to realize a filter based on the zero padding technique in frequency domain: its frequency response is sketched in figure 5.9. The complete software demodulation consists of:

- converting the black signal from the time to the frequency domain thanks to an FFT,
- multiplying this signal with our pass-band filter,
- converting back the signal from the frequency to the time domain thanks to an IFFT.

This process allows to obtain the approximative shape of the demodulated signal, from which we are hopefully able to extract the key that was pressed.

The figure 5.12 and 5.13 show the result of a single black curve demodulated by this software approach. We can distinguish the compromising signal, *i.e.* the falling edge of the data line. Furthermore, the levels of the compromising signal related to PS/2 clock do not have the same amplitude: it is directly linked to that of the red signal's state. Those observations do match those obtained with the hardware demodulator. Thus the software filtering process offers the possibility to have a coarse idea of the compromising signal shape.

Nevertheless with this tool we do not have the advantage of hardware demodulation:

- the bandwidth of the software filter is larger: it cannot be set that narrow as the 1 MHz of the hardware receivers;
- the gain and attenuation cannot be tunned and adjusted regarding the range of frequency;
- the compromising signal at 36 MHz spotted by the hardware receiver is not visible with the software filtering: no compromising signal is visible.

5.4 Conclusion

We introduce a new set of techniques to extract the leakage frequencies from the black radiation providing information about the red signal. They have successfully been tested on the electromagnetic emissions of a PS/2 keyboard intercepted at a distance of 5 meters. By the help of side channel analysis methods applied in frequency domain, we are able to distinguish the frequencies that are more leaking sensitive information and their bandwidth. Thanks to these tools (inspired from CPA, MIA and PCA), we demonstrate that we are in position to give quick diagnostics about EM leakage.

Our experiments show that the leakage is carried by some frequencies that are not necessarily the harmonics of the clock frequency. This confirms the observations

previously done in the work of M. Hutter *et al.* [HMF07]. We also notice that our three methods retrieve the same compromising spectrum shape, and consequently the same leakage frequencies. CPA and MIA yield clearly the most accurate results. Some frequencies that leak more sensitive information than others might result from non-linear phenomena. We show that the red signal can be recovered from the demodulation of the electromagnetic emanation, either with a hardware receiver or by a software band-pass filtering technique, which consists merely in selecting frequencies of interest from the FFT of the black emanation. Despite its simplicity, this filter enables an identification of the leakage in time domain. We could successfully characterize the leaking frequencies from our raw radiation using our methods. This allows us to recover the secret information which is the red signal in this case. However, these generic methods could also be applied in different contexts, for instance RSA recovering key problematics. Indeed in asymmetric cryptography, in some implementations, the sequence of operations are secret dependant. Someone able to find out square and multiply operation sequences occurring during an RSA encryption is able to recover the private exponent. A possible extension to this work could consist in applying our methodology to a confidential sequence of operations.

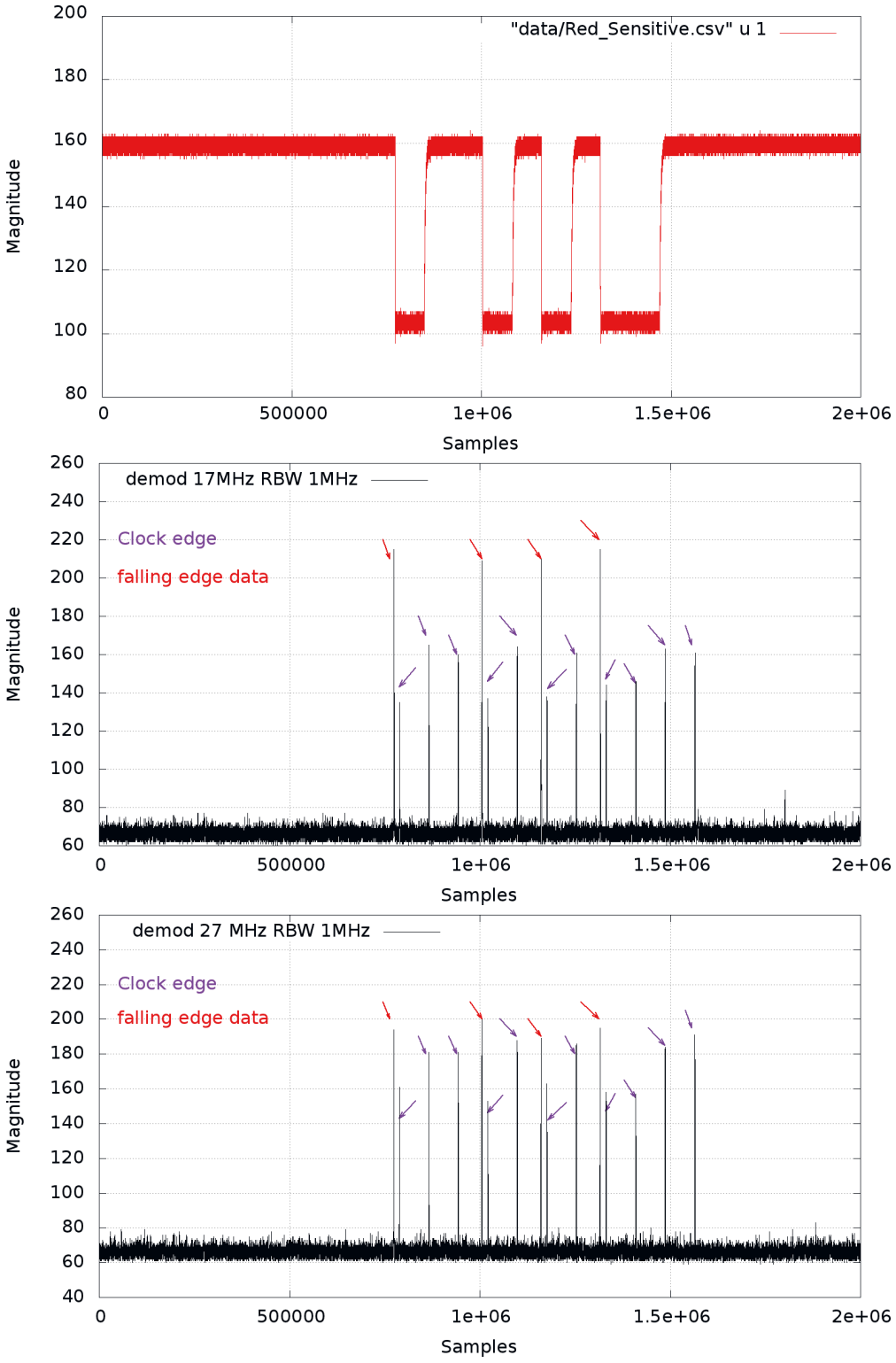


Figure 5.10: Results of demodulation (red signal, and black signal demodulated at 17.0 MHz, 27.0 MHz.

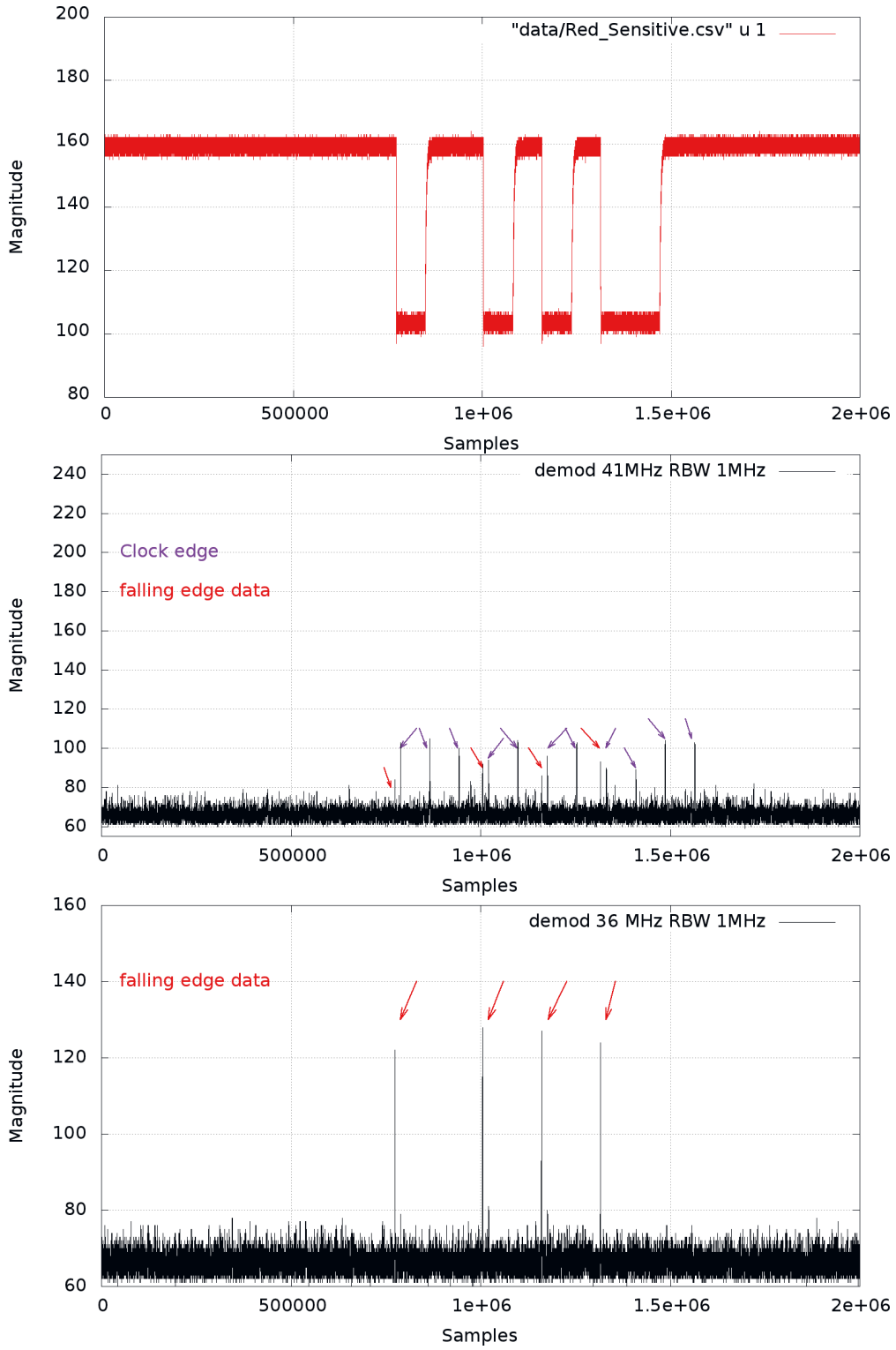


Figure 5.11: Results of demodulation (red signal, and black signal demodulated 41.0 MHz and 36.0 MHz).

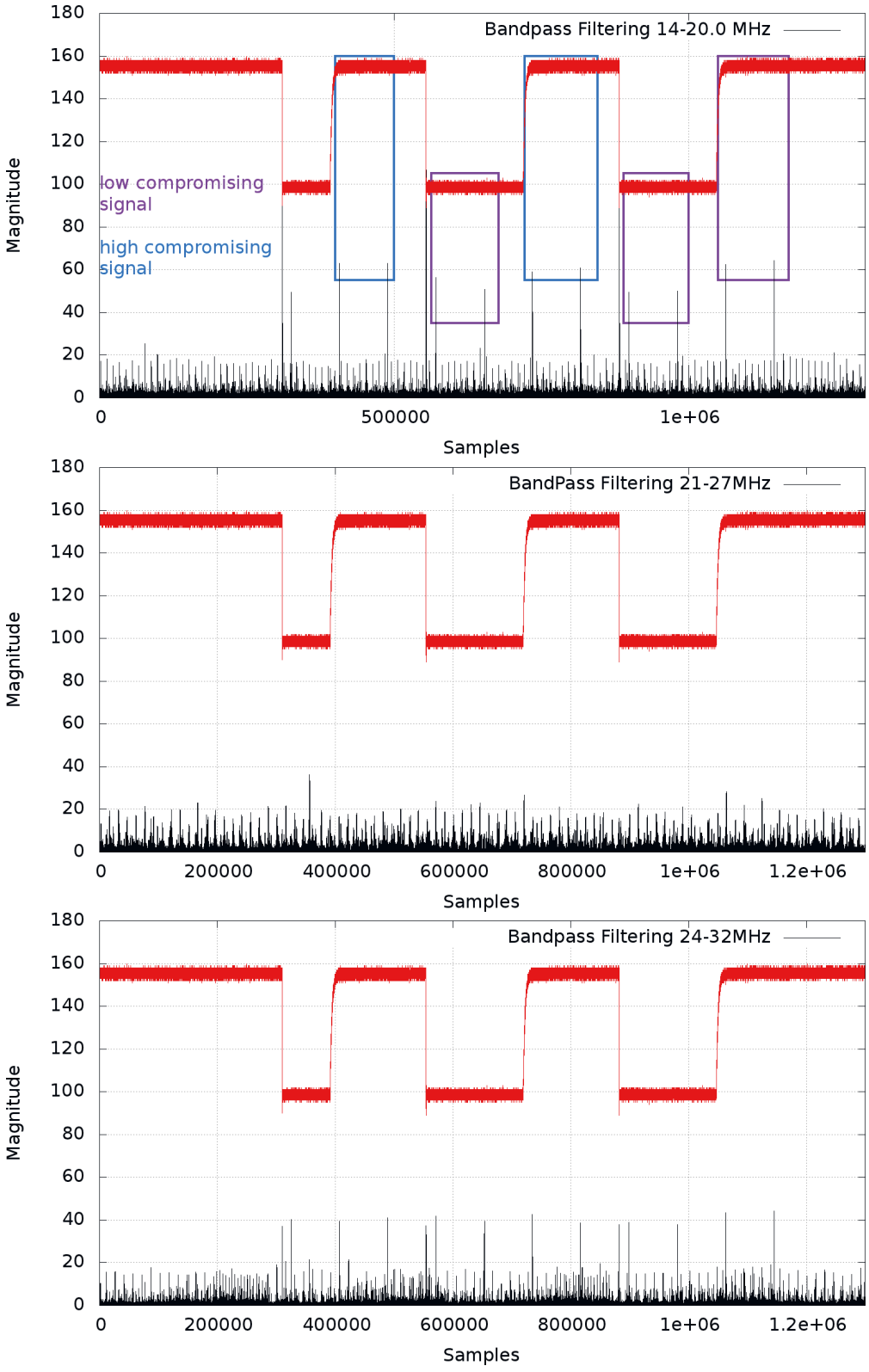


Figure 5.12: Results of software demodulation between 14-20 MHz,21-27 MHz(No Signal) and 24-32 Mhz.

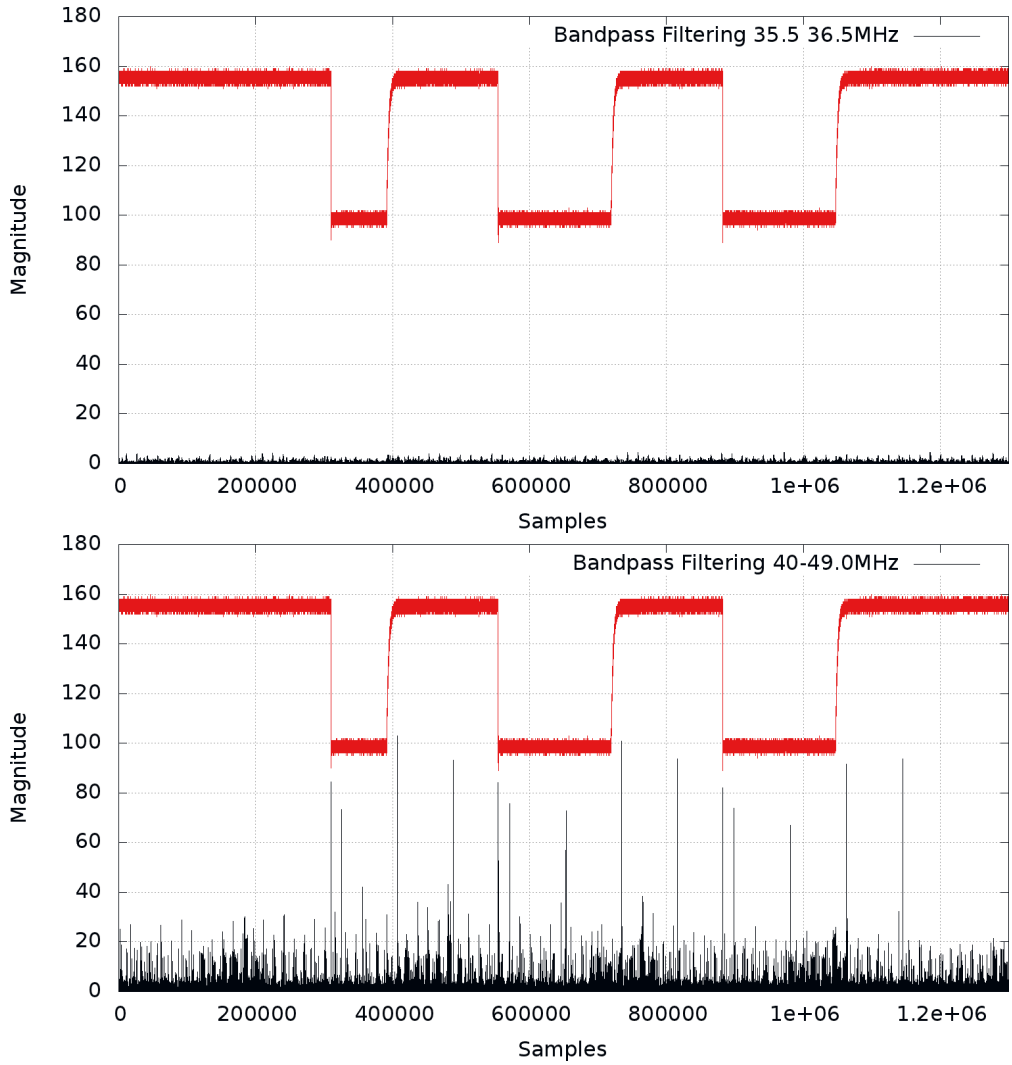


Figure 5.13: Results of software demodulation between 35.5-36.5 MHz(No Signal) and 40-49 MHz.

Chapter 6

Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization and Demodulation Techniques

SPA/SEMA (Simple Power/Electro-magnetic Analysis) attacks performed on public-key cryptographic modules implemented on FPGA platforms are well-known from the theoretical point of view. However, the practical aspect is not often developed in the literature. Indeed, SEMA on RSA needs to make a difference between square and multiply which use the same logic; this contrast with SEMA on ECC, which is easier since doubling and add that are two different operations from the hardware point of view. In this chapter, we wonder what to do if a SEMA fails to succeed on a device. Does it mean that no attack is possible? We show that hardware demodulation techniques allow the recording of a signal with more information on the leakage than a raw recording. Then, we propose a generic and fast method enabling to find out demodulation frequencies. The effectiveness of our methods is demonstrated through actual experiments using an RSA processor on the SASEBO FPGA board. We show cases where only demodulated signals permit to defeat RSA.

Contents

6.1 SEMA and Target Device Implementation 82
6.1.1 SEMA on a RSA Implementation 82
6.1.2 SASEBO-G and VirtexII 83
6.1.3 Identification of the Information Leakage Spots 84
6.2 Characterization of the EM Channel in Frequency Domain 88
6.2.1 Windowing and Sample Preparation 89
6.2.2 An Information Theory Viewpoint 91
6.3 Demodulation Technique 93
6.3.1 Confirmation of the Results with a Hardware Receiver 93
6.3.2 Unintentional emanations 93
6.4 Conclusions 96

6.1 SEMA and Target Device Implementation

6.1.1 SEMA on a RSA Implementation

The RSA cryptosystem is a *de facto* standard public-key cryptosystem PKCS #1, which is based on encryption and decryption, as shown below:

$$\text{Encryption} \quad C = P^E \bmod N, \tag{6.1}$$

$$\text{Decryption} \quad P = C^D \bmod N, \tag{6.2}$$

where P is the plaintext, C is the ciphertext and (E, N) is the public key. Usually, the size of P, C, D and N is greater than $1,024$ bits for security reasons. ALGORITHM 1 shows a classical way for computing a modular exponentiation called the left-to-right binary method.

ALGORITHM 1
MODULAR EXPONENTIATION (L-TO-R BINARY METHOD)

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 mod N;          – squaring
4:     if (e_i = 1) then
5:         Z := Z * X mod N;      – multiplication
6:     end if
7: end for
```

Multiplications and squaring operations are done sequentially according to the bit pattern of the exponent D. This algorithm always performs a squaring at line 3 regardless of the scanned bit value, but the multiply operation at line 5 is only executed if the scanned bit is 1. Let us note that multiplication and squaring are done using the same module of the SASEBO. This module employs the high-radix Montgomery's modular multiplication. However, a multiplication loads two operands while the square only loads one. Furthermore, a conditional branch in the algorithm (between square or multiply) may introduce a bias in energy consumption or a delay. Therefore, if an attacker is able to make a difference between a multiplication and squaring operation, he can recover the whole secret with only one trace. This is the original idea of the Simple Power Analysis (*SPA*)/ Simple electro magnetic Analysis (*SEMA*) against the RSA cryptosystem. Figure 6.1 illustrates the dependency.

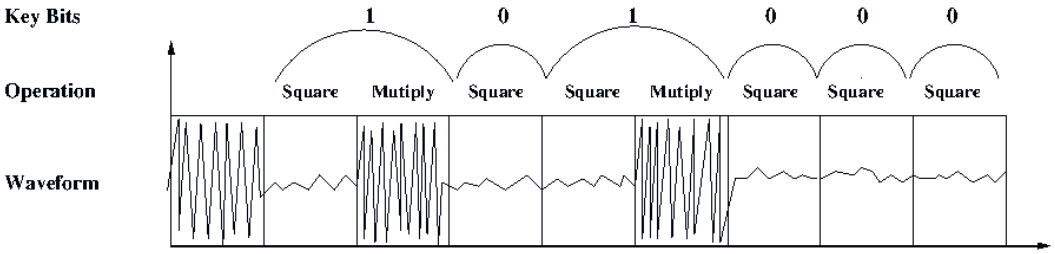


Figure 6.1: SEMA principle on RSA.

6.1.2 SASEBO-G and VirtexII

We employ a Side-channel Standard Evaluation Board (SASEBO-G) which is widely used as a uniform testing environment for evaluating the performance and security of cryptographic modules. Until now, various experiments associated with side-channel attacks are being conducted on the SASEBO boards, and many useful results are being expected to support the international standards work [Sat]. Figure 6.2 shows the SASEBO-G used in this experiment, which employs two Xilinx FPGAs; one FPGA is used to implement a cryptographic module in hardware or software and the other FPGA is used to communicate with a host computer through RS-232 or USB cables.

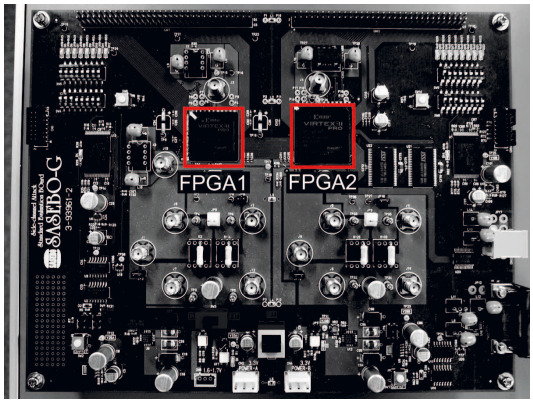


Figure 6.2: Overview of SASEBO-G.

We implemented an RSA processor based on a conventional left-to-right binary method and Montgomery Multiplication [HMA+10] in FPGA2 shown in figure 6.2. The processor handles key of length 1,024-bit key length based on 32-bit word length for radix, and is predominantly-comprised of one 32-bit multiplier. On the other hand, we did not use FPGA1 in order to simplify the intensity emanation from the SASEBO. The RSA operation was performed at a clock frequency of 24 MHz. The input value is R^{-1} ($=2^{-k} \mod N$ in order to produce large differences between the multiplication and squaring operations. An RSA processor based on ALGORITHM 1 was implemented in an FPGA (Xilinx Virtex II) on the SASEBO-G board.

6.1.3 Identification of the Information Leakage Spots

Firstly we propose as a preliminary to investigate the dependencies between the intensity of EM radiation and that of EM information leakage. For this purpose, we propose to use some methods from EMC community to highlight the area of the board where the EM radiation have the highest intensity. Then to evaluate the EM information leakage at a board level we perform Simple Electro-Magnetic Analysis (SEMA) experiments. We can consequently evaluate which points of the board and which frequencies are effective for EM information leakage.

Table 6.1: Measurement conditions

Cryptographic device (SASEBO-G)	
Target FPGA	Xilinx Virtex-II Pro
Clock frequency (crystal oscillator)	24 MHz
Power supply voltage	3.3 V
EMC scanner (WM7400) setting	
EM probe	MT-545
Distance from SASEBO surface	20 mm
Distance from FPGA surface	5 mm
Pitch for SASEBO surface	5 mm
Pitch for FPGA surface	1 mm

Our first experiment was to test the SEMA on the SASEBO-RSA with near-field EM techniques. We first generate an EM-field map on the entire surface of the device, and then pinpoint the points with high EM-field intensity, and then perform a SEMA without any additive apparatus. It means that the antenna is directly connected to the oscilloscope.

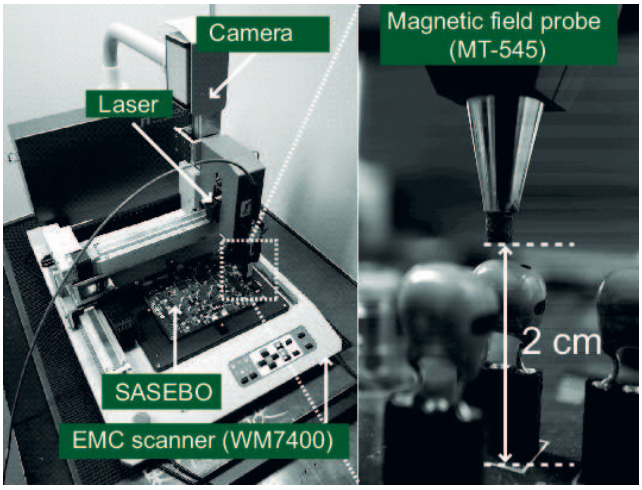


Figure 6.3: EM measurement system.

Figure 6.3 shows an overview of the EM measurement system in this experiment.

The above SASEBO was set on the scanning table. The experimental scanner (WM7400) employs a micro EM probe whose bandwidth ranges from 1 MHz to 3 GHz, and scans the surface of the SASEBO. The probe head is arranged precisely at 2-cm distance from a target device within a tolerance of one micrometer. The system can measure the distance by the equipped laser geodesy, figure 6.3 also shows an image of the EM probing. The measurement condition are summarised in Table 6.1.

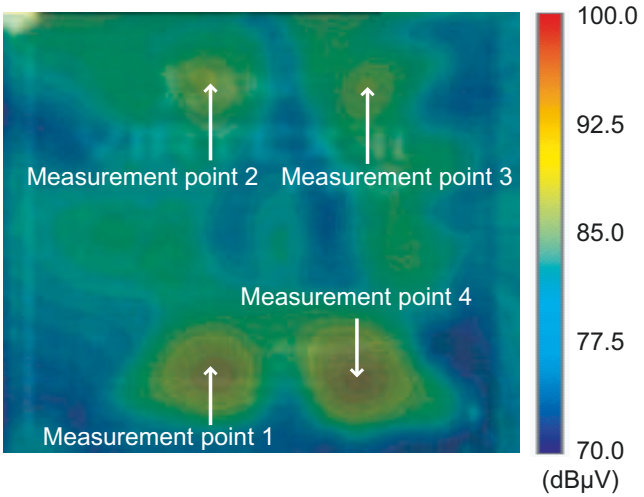


Figure 6.4: EM-field map over FPGA2.

In order to identify the source of EM radiation, we first examine the surface of FPGA2 while performing an RSA operation. Figure 6.4 shows an EM-field map over FPGA2, whose frequency band ranges from 10 to 500 MHz. The map indicates that there are four effective spots which have higher intensities.

Therefore, we selected the four points as representatives in the next experiment. Figure 6.5 shows the frequency characteristics of EM radiation for the four points over the FPGA2. We can confirm here that EM radiation at the clock frequency (24 MHz) and its harmonic frequencies are much higher than other frequencies. In particular, the EM radiation at the clock frequency has the highest intensity among them.

Figure 6.6 shows EM field maps on the entire surface of the SASEBO corresponding to the frequency bands ranging between (a) 10-100 MHz, (b) 100-200 MHz, (c) 200-300 MHz, and (d)300-400 MHz, where the red and blue areas indicate higher and lower intensities, respectively. The result shows that specific areas around FPGA2 and a crystal oscillator, which is located at the upper side of FPGA2 in figure 6.2, have higher EM-field intensities than other areas. This is because only the two components are active components on the board. We confirmed from the result that the EM-field intensity at the clock frequency is relatively higher than those of other frequencies.

In order to evaluate EM information leakage, we performed simple electromag-

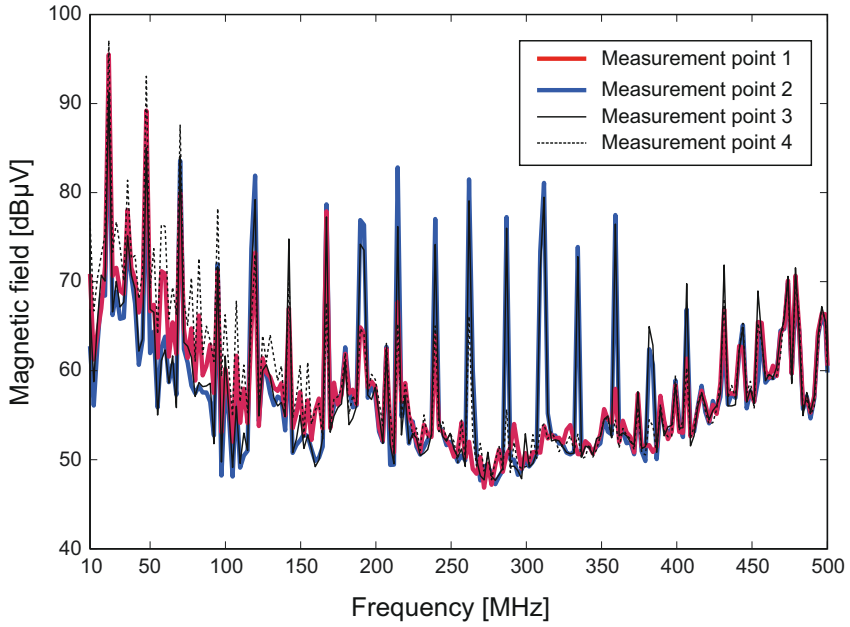


Figure 6.5: Frequency characteristics of EM radiation over four points over FPGA2.

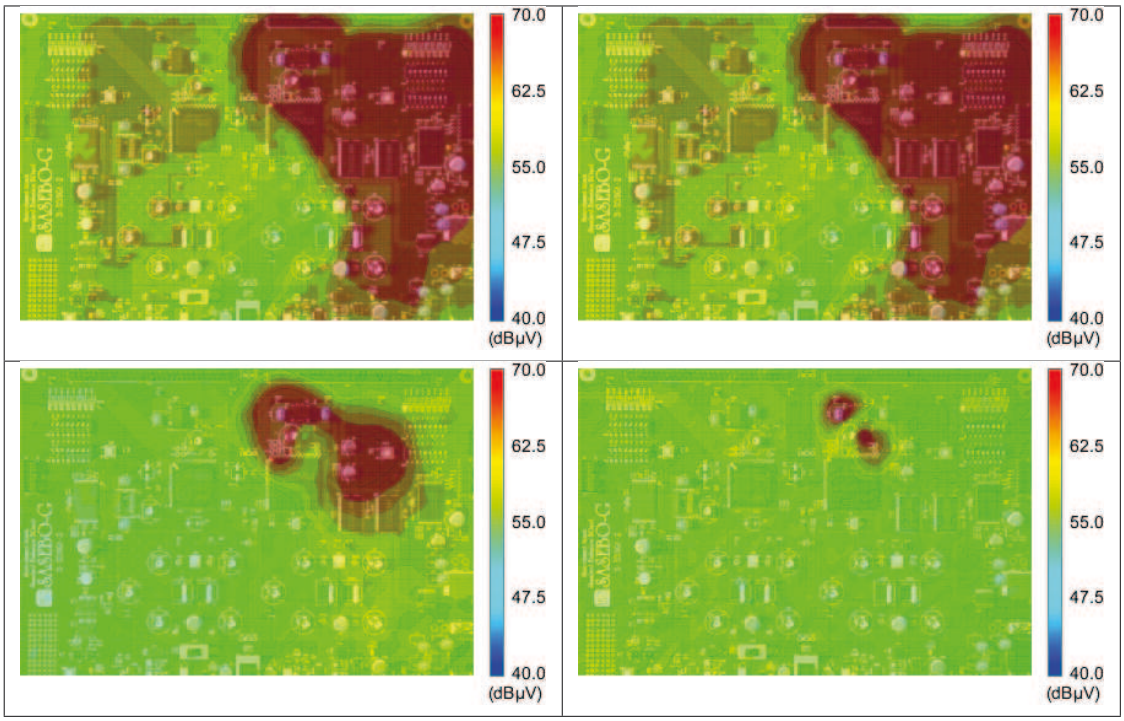


Figure 6.6: EM-field maps: (a) 10-100 MHz, (b) 100-200 MHz, (c) 200-300 MHz, and (d) 300-400 MHz.

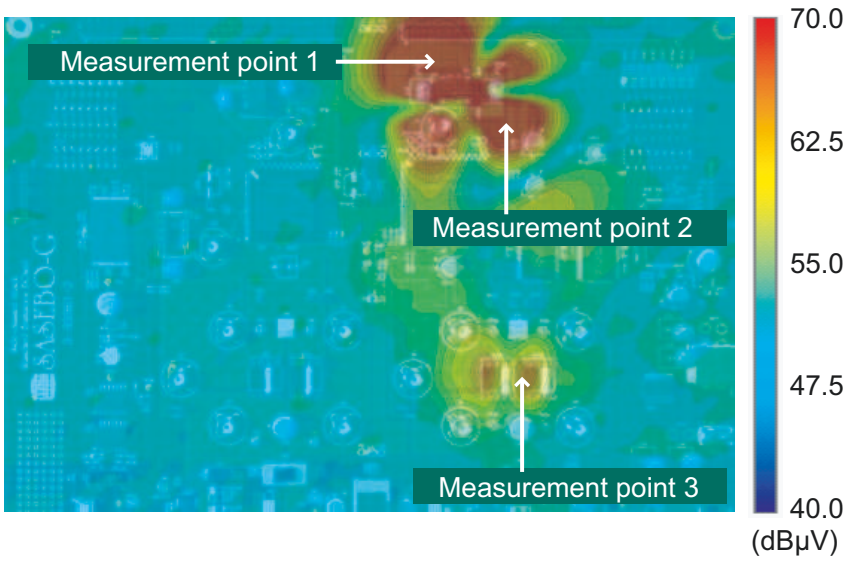


Figure 6.7: EM-field map at 24 MHz.

netic analysis (SEMA) experiments on the above SASEBO-G. In this experiment, we focus on the EM radiation at 24 MHz as a primary frequency. Figure 6.7 shows an EM-field map on the entire surface of the SASEBO at 24 MHz. We selected three specific points as regions of interest according to the result, where Point 1 is on the crystal oscillator, Point 2 is on the cryptographic module, and Point 3 is on the resistor between the FPGA ground pin and the ground plane.

Highest EM radiations were observed at Points 1 and 2, and a relatively-high EM radiation was observed at Point 3 even though it is not close to the cryptographic module. Figure 6.8 shows the EM traces of the three points, where the horizontal and vertical axes indicate time and voltage, respectively. The conventional SEMA is performed using the waveforms, but no relationship between the waveform patterns and the operations was observed. In this experiment, therefore, a demodulation technique is applied for the waveforms in order to emphasize the differences, and the waveforms as shown in figure 6.9 are obtained using a demodulation at 24 MHz. The multiplication and squaring can easily be distinguished as shown in figure 6.9 (c).

We tune the receiver to the clock frequency (*i.e.*, 24MHz) with a resolution bandwidth of 1MHz. In figure 6.9 (a), we get one measurement by demodulation at 24 MHz, over the crystal oscillator at position 1, but this measurement is not carrying information. This part of the PCB supplies the clock frequency to the RSA module on the FPGA. Its radiation is therefore constant and doesn't carry any information. In figure 6.9 (b), the measurement is done at 2 cm from the FPGA. The radiation from the FPGA are weak at this distance. Finally we observe only at Position 3 in figure 6.9 (c), over the resistor between the FPGA ground pin and the ground plane, a difference between the square and multiply operation.

It is important to notice that this position is a bit far away from the cryp-

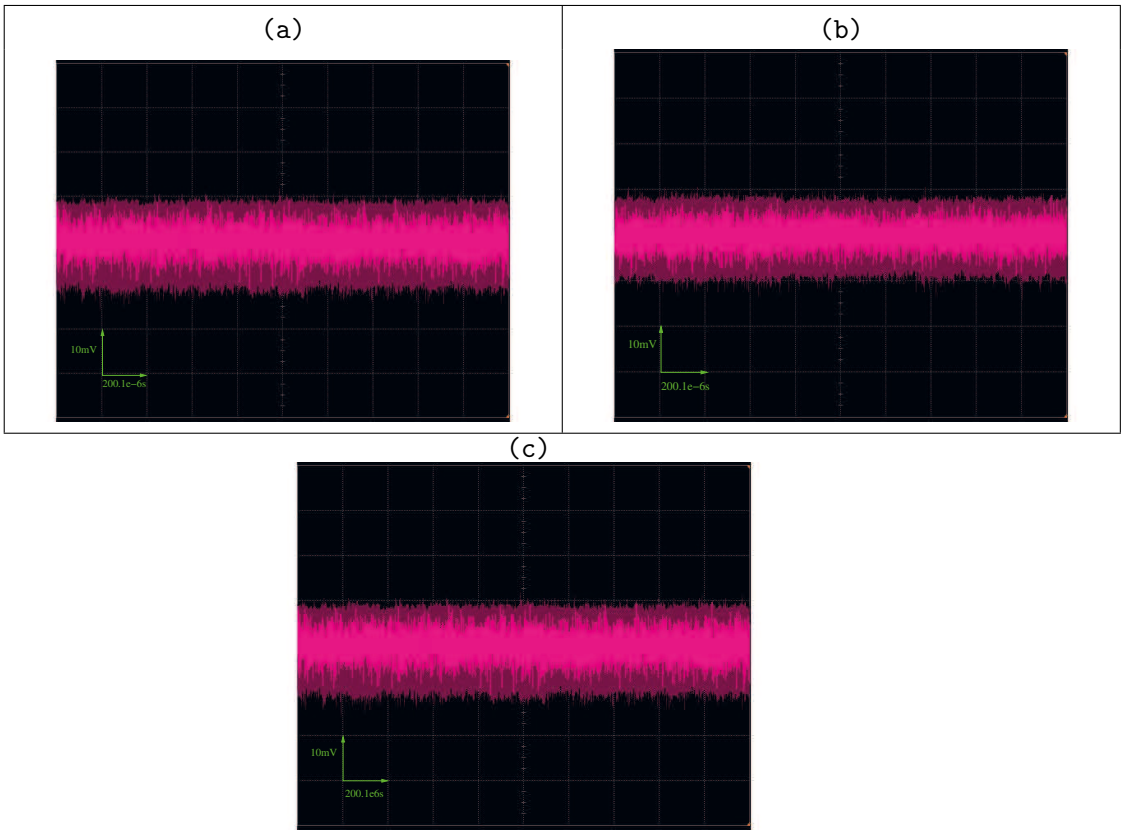


Figure 6.8: EM waveforms of: (a) point 1, (b) point 2, and (c) point 3.

tographic module but his radiations are carrying information. This observation confirms the assumption of Agrawal. The unintentional emanation such as the ubiquitous clock signal can be one of the most important sources of signal and the information can be carried far from the cryptographic module. These first results suggest that the signal (information)to noise ratio should be improved by using a receiver that reduce the range of frequencies.

6.2 Characterization of the EM Channel in Frequency Domain

In this section, we propose to consider the global emanation from the SASEBO Board, and to apply a method to characterize the leakage in the frequency domain. Indeed the use of the receiver tunned on a compromising frequency can help the attacker or the evaluator. For this experiment we have used a loop-type EM probe as shown in figure 6.10 and the EM signals have been amplified by 60 dB.

For the same bit sequence shown in figure 6.1, we obtained the EM trace illustrated on figure 6.11.

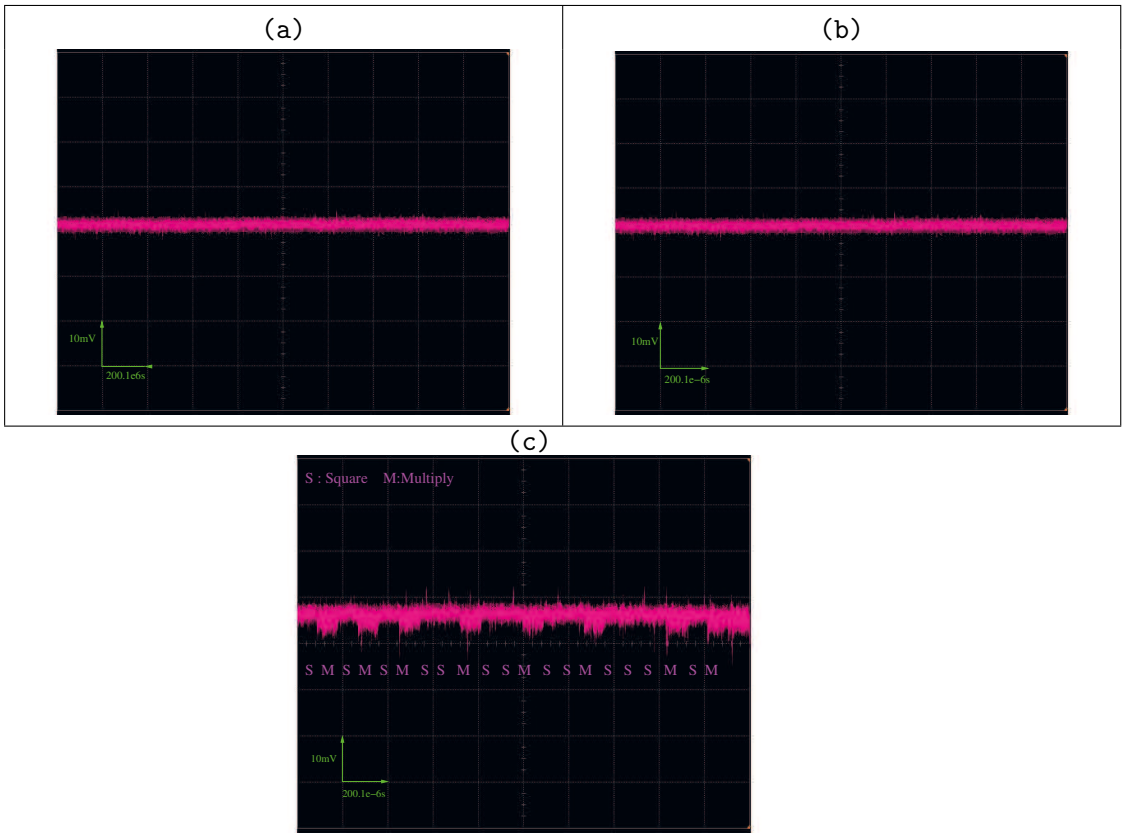


Figure 6.9: Demodulated EM waveforms of: (a) point 1, (b) point 2, and (c) point 3.

No difference appears between a square and multiply, even when messages are chosen to improve the result. We have even tried to improve the analysis using pattern matching techniques but without any satisfactory results in terms of contrast.

We propose to adapt the method presented in previous chapter to characterize the leakage coming from a cryptographic component. With this characterization we are able to select the frequencies and their associated optimal bandwidth. The useful information is contained in these ranges of frequencies. Therefore, with a receiver tuned on the right frequency, we can retrieve the compromising signal.

6.2.1 Windowing and Sample Preparation

To provide this characterization, we propose an approach based on information theory. This method can be managed as follows:

First we gather a large number of measurements, by knowing the key *i.e.* the operations that are computed by the chip. These EM measurements from the antenna are noisy, distorted and the operations are not distinguishable. For this step, we choose a time window where only one operation of square and one operation of

Figure 6.10: EM loop on the SASEBO Board during an RSA computation.

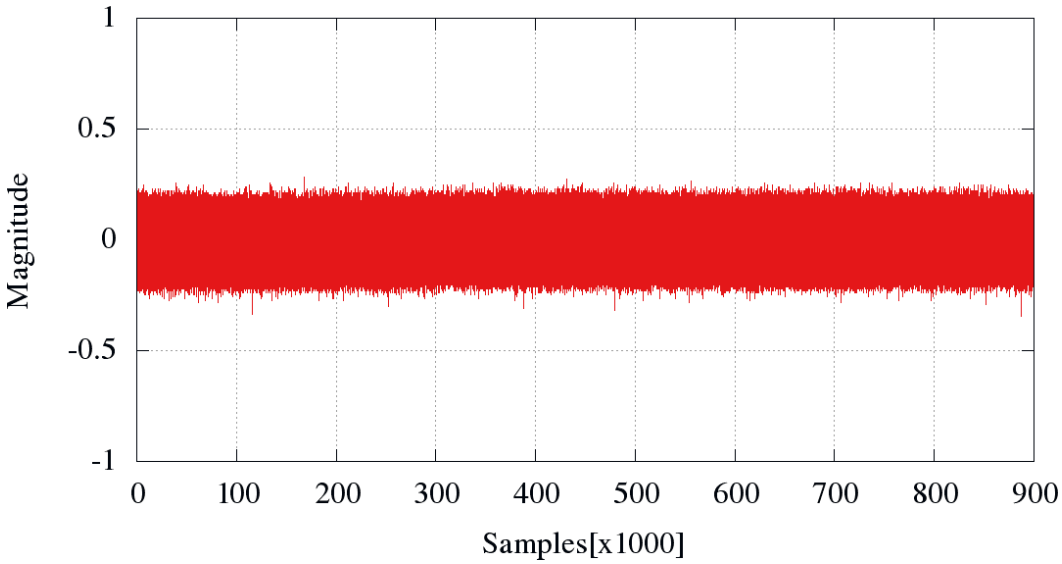


Figure 6.11: Direct EM radiations emitted during an RSA computation.

multiply are performed as shown on figure 6.12. After the measurements are segmented according to the performed operation. The number of samples is equal in each segment of the signal. Each section of the signal is equal in term of number of samples. Consequently, we get as much parts of EM signal for the multiplication as for the squaring, and we obtain two sets of measurements.

Then, for each set, we compute: the FFT (*Fast Fourier Transform*) of every observation O_f; the mean spectrum related to each operation; and the mean of

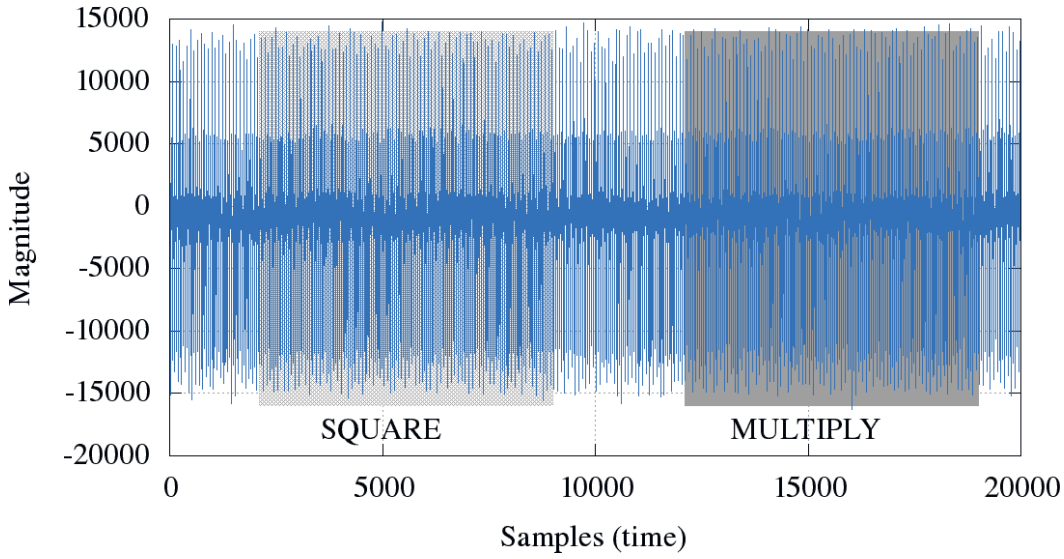


Figure 6.12: EM measurement split into Square and Multiply parts.

all the observations. Therefore we obtain a specific spectral signature for each operation of the modular exponentiation algorithm. Finally we compute the Mutual Information value for each frequency. Thus we attribute a specific spectral signature to each operation of the modular exponentiation algorithm. see ALGORITHM 2.

ALGORITHM 2

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 $(\sigma_{Square}, \sigma_{Multiply})$
6 : Compute the Mutual Information in frequency domain.

We will introduce some details about the information theory in section 6.2.2.

6.2.2 An Information Theory Viewpoint

It is interesting to adopt an information theory viewpoint to retrieve the relevant frequencies and to bring a mathematical proof that the information is not necessarily

carried by the clock frequency. We compute the Mutual Information as:

$$\mathrm{I}(O_f; Operation) = \mathrm{H}(O_f) - \mathrm{H}(O_f|Operation), \tag{6.3}$$

where $\mathrm{H}(O_f)$ and $\mathrm{H}(O_f|Operation)$ are the entropies of all the observations in the frequency domain and of the observations knowing the operations. Both these entropies can be obtained according to:

$$\begin{aligned} \mathrm{H}(O_f) &= -\int_{-\infty}^{+\infty} \Pr(O_f) \log_2 \Pr(O_f), \\ \mathrm{H}(O_f|Operation) &= \sum_{j \in \{Multiply, Square\}} \Pr(j)\mathrm{H}((O_f|j)). \end{aligned}$$

$\Pr(O_f)$ denotes the probability law of observations at a frequency f. Moreover we consider that the computed operations are equi-probable events, therefore $\forall j \in Operation$, $\Pr(j) = \frac{1}{2}$. And the distribution is assumed to be normal $\sim N(\mu, \sigma^2)$ of mean μ and variance σ^2. The same approximation as in the previous chapter is used: $H(O_f) = \log_2(\sigma\sqrt{2\pi e})$. From this value, the Mutual Information defined in Eqn. (6.3) can be rexpressed, by computing for each operation the differential entropy:

$$\begin{aligned} \mathrm{I}(O_f; Operation) &= \mathrm{H}(O_f) \\ &- \frac{1}{2}(\mathrm{H}(f|Multiply) + \mathrm{H}(f|Square)), \end{aligned}$$

that can be simplified as:

$$\mathrm{I}(O_f; Operation) = \frac{1}{2} \log_2 \frac{\sigma_{O_f}^2}{\sigma_{O_f, Multiply} \sigma_{O_f, Square}}. \tag{6.4}$$

The figure 6.13 represents the result of the MIA computation on the traces as defined in Eqn. (6.4). We notice that the desired information might be contained in a range of frequency between 5.0 and 60.0 MHz with the presence of a large spikes spread over these frequencies.

This method provides a result expressed in bit, that allows us to interpret easily the leakage frequencies regarding the level of compromising signal. The maximum Magnitude is obtained for the frequencies around 24.0 MHz, that corresponds to the clock frequency of the component. We decide to pick up three ranges of frequencies corresponding to the three peaks highlighted in figure 6.13:

- around 24.0 MHz,
- around 34.0 MHz,
- around 54.0 MHz.

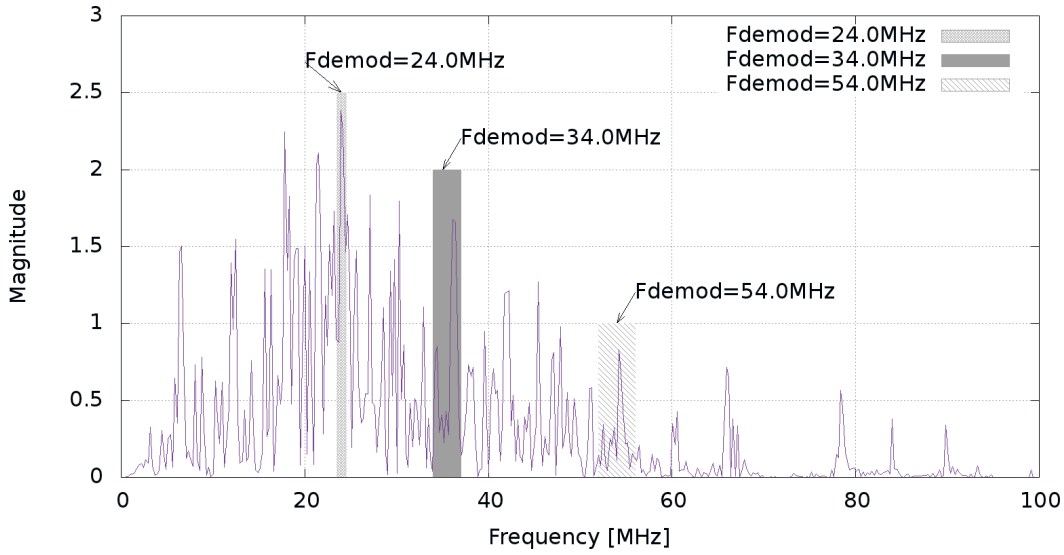


Figure 6.13: Result of MIA in frequency domain.

6.3 Demodulation Technique

In section 6.3, we study the results of the demodulation at these frequencies. Then we show the efficiency of our approach. We use the results obtained previously. We need a dedicated apparatus for the frequency analysis: a spectrum analyser that can be used in demodulator/ Receiver mode.

6.3.1 Confirmation of the Results with a Hardware Receiver

For this experiment, we propose to use the TEMPEST receiver depicted in previous chapter we use the same setup (RSA implementation on a SASEBO-G and loop antenna) as in the previous section, but the output of the probe is connected to a receiver/demodulator and we perform the measurements directly on the FPGA. In [AARR03] Agrawal *et al* used a demodulator to measure EM emanation from an SSL accelerator. We apply a similar technique to the FPGA implementation which consumes far less power than the SSL accelerator. The EM radiation is expected to be weaker than the previous one. We focus on a range of frequencies between 0.0 and 100.0 MHz and demodulate at the frequencies exhibited by the previous analysis at 24.0 MHz, 34.0 MHz and 54.0 MHz. Each time, the demodulated signal shows a peculiarity that allows to distinguish clearly the two distinct operations. In this experiment, we employ the demodulation technique to investigate unintentional (or indirect) emanation.

6.3.2 Unintentional emanations

The unintentional emanation described by Agrawal *et al* is the result of modulation or intermodulation between a carrier signal and the sensitive signal. In particular,

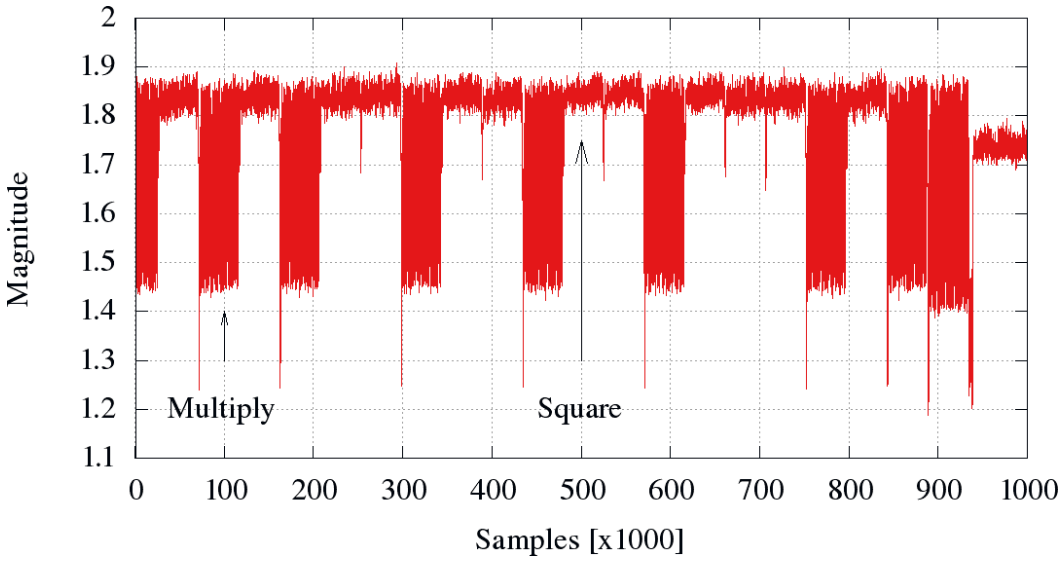


Figure 6.14: One Single Demodulated EM waveform at 24 MHz.

the ubiquitous clock signal can be one of the most important sources of carrier signals. This assumption is confirmed by our results on figure 6.13. We tune the receiver to the clock frequency (*i.e.*, 24MHz) with a resolution bandwidth of 1MHz. Figure 6.14 shows one single demodulated EM waveform at 24 MHz. Indeed, the receiver improves the differences between the two operations dramatically as shown in figure 6.14. We can obtain similar results by tuning the frequency of the receiver to the harmonics of the clock frequency. Moreover we can enlarge the distance between the FPGA and the probe despite a significant lose of S/N ratio. In order to obtain more powerful signals, we used an increased resolution bandwidth and then performed the same SEMA attacks successfully for ranges over 5 cm. With the method developed previously we can also focus on different frequencies that are not necessarily clock harmonics. To measure such emanation, the probe must be placed close to the FPGA. Then an eavesdropper has to tune the receiver at every frequency of the spectrum.

Figures 6.15 and 6.16 show the single demodulated EM waveform at 34 and 54 MHz, which have been identified by the peaks obtained on our MI analysis on figure 6.13. The same sequence is replayed by changing only the demodulation frequency.

If we compare the figures 6.14 and 6.15 we notice that sharp peaks appear at the beginning of every square operation. These peaks are not present before a multiply operation and thus we can easily distinguish the square from the multiply operations. We obtained the same phenomena for the demodulation at 54 MHz shown in figure 6.16. Moreover it is important to notice that the magnitude of the compromising signal decreases when the frequency of demodulation increases. The magnitude of the compromising signal follows the trend obtained in the previous section. These results confirm the results obtained during the characterization as

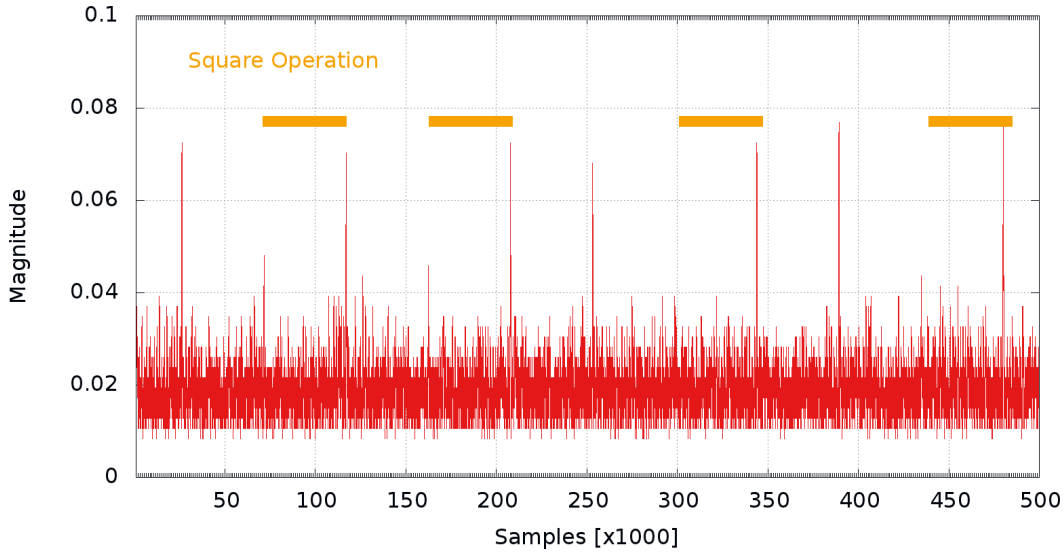


Figure 6.15: One single Demodulated EM waveform at 34 MHz.

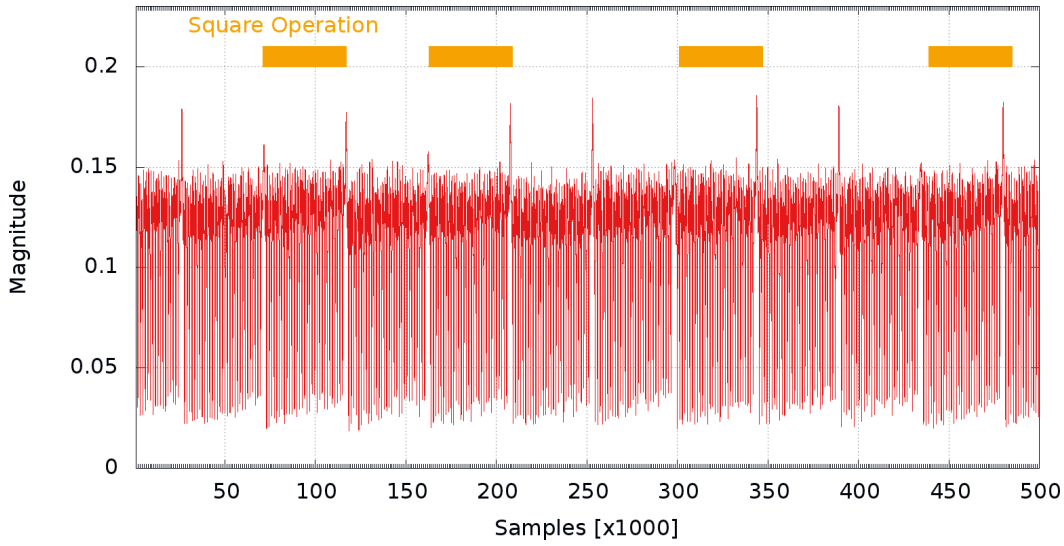


Figure 6.16: One Single Demodulated EM waveform at 54 MHz.

shown on the table 6.2, and the shape of the curve of the figure 6.13.

Frequency	**MI [bit]**	**Magnitude**
24.0 MHz	2.5	0.5
34.0 MHz	1.7	0.03
54.0 MHz	1.0	0.02

Table 6.2: Comparison between the results.

6.4 Conclusions

This chapter presents possible SEMA attacks performed with a contactless probe on an FPGA implementation of RSA. On the studied implementation the raw EM measurements show no obvious leakage. In order to distinguish square and multiply operations in the SEMAs, we introduce a method to detect and characterize a cryptosystem in frequency domain, *i.e* a distinguisher of frequencies that are carrying information. In addition we show that our method provides exploitable results and allows us to retrieve the leakages frequencies for unintentional emanations. The method proposed based on the mutual information analysis in frequency domain allows to extract the leakage frequencies of the signal related to the square and multiply operations. By following this method we are able to pinpoint the frequencies that are leaking more information and their bandwidth. Thanks to this tool we demonstrate that we are in position to give a quick diagnostic about the EM leakage of a device. As a comparison the TEMPEST methodology requires to scan exhaustively all the frequencies to discover those that leak. The demodulation allows to detect some biases that can be exploitable, for instance:

- conditional branch and control command,
- difference of operands,
- difference in computation of the High Radix Multiplier.

Therefore an attacker is able to perform SEMAs. These emanations allow to highlight control instructions performed before each square/multiply operation. The method of choosing a suited demodulation frequency is crucial; and thanks to our characterization based on the MI, information leaked through direct and indirect EM emanations can be detected and observed with one single demodulated EM waveform. Indeed our method allows a thorough characterization of leaking frequencies. This powerful tool enhances dramatically the SEMA approach.

Part IV

Intentional Electro-Magnetic Interference

Chapter 7

Non Invasive Intentional Electro-Magnetic Interference Attacks

In this chapter we introduce some methods to attack a cryptographic device by generating Electro-Magnetic Interferences. This kind of method can be used for both Side Channel Analysis or Fault Attack. The presented techniques are done at distance from the electronic device, and thus non intrusive. Firstly we introduce some experiments done in radiative condition, where we use a stripline to expose the component to a sine wave emitted by a signal generator.We use a technique initially introduced by University of Tohoku, based on radiative techniques on the power supply to conduct fault injection. By these experiments we show that the leakage can be modified and transposed on high frequency.

Contents

7.1 Radiative Intentional Electro-Magnetic Interference Attacks 100
7.1.1 Particular Experimental Setup 100
7.1.2 Results and Observations 101
7.2 Conductive/Radiative Intentional Electro-Magnetic Interference Attacks 102
7.2.1 Experimental setup 103
7.2.2 Fault Injection on Sasebo-G with AES 104
7.2.3 Fault Injection onto the DES SecMat-V1 105
7.3 Power Analysis in Frequency Domain 109
7.4 Conclusion 110

The Electromagnetic Compatibility studies the unintentional generation and propagation of electromagnetic waves, that produce Interference. As shown in chapters 3, 5 and in 6, EMC studies the emission issues related to unwanted radiation, that can be used by an attacker to recover the secret key. In this chapter we focus more on Susceptibility or Immunity issues of the cryptographic device. In this context, we consider that the component is referred as a *victim* of unplanned electromagnetic disturbances named IEMI (*Intentionnal Electro-Magnetic Interference*). As mentioned by Hayashi *et al.* in [HHS+11] and in [RBW04], IEMI is defined as "intentional malicious generation of electromagnetic energy introducing noise or

signals into electric and electronic systems thus disrupting, confusing or damaging these systems for different purposes". Different ways to introduce the signal might be considered. For all these experiments we consider continuous interferences. A source, for instance an Analog signal Generator, emits regularly Continuous Waves (CW) at a given frequency. Different coupling are consequently produced, for example: radiative, conductive, capacitive and magnetic or inductive. In this chapter, we firstly introduce different experiments realised by considering radiative coupling. Then we describe improved experiment with the conductive coupling.

7.1 Radiative Intentional Electro-Magnetic Interference Attacks

7.1.1 Particular Experimental Setup

To manage experiments in radiative IEMI, we first use a dispersive device like an antenna then a non dispersive device such as a stripline. We have used the SASEBO-G as in the previous chapter. To perform these experiments some cautions have been adopted, for instance experiments have been realised in Faraday cage knowing the value of the generated electromagnetic field (around 100V/m), as illustrated in the figure 7.1.

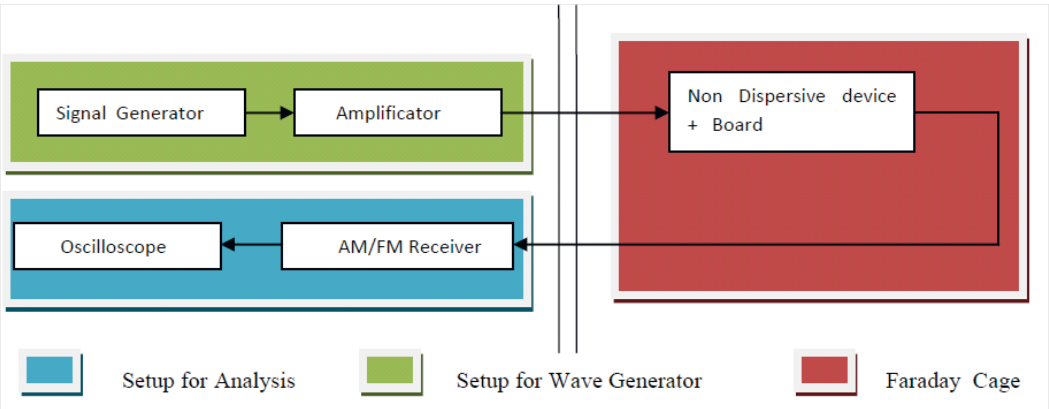


Figure 7.1: Schema of general experimental setup.

An antenna is considered as a source of dispersive radiations. Experiments realized with antenna are inconclusive, and do not have any effect onto the board and the computation, whatever the frequency and the magnitude of the generated wave. Then we propose to use a non dispersive device like a stripline. A stripline is composed of two metal plates that lead the electromagnetic wave between them. The SASEBO board was placed between the both plates, and the stripline acts somewhat like a coaxial cable as shown on figure 7.2.

Consequently the board is subject to strong electromagnetic fields. To study the

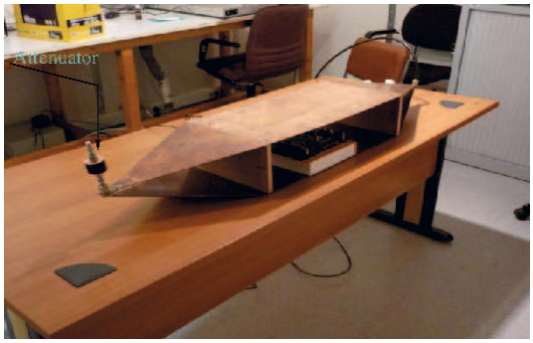


Figure 7.2: Real experiment with a stripline and attenuator configuration.

wave, or the electro-magnetic field that interacts with the board two possibilities may be considered:

- use of a coupler,
- connect the output of the stripline to analysis setup.

In the first case, the incident wave enters and exits the stripline from the same point. The use of an attenuator at the opposite of the stripline allows this behaviour. A coupler is then used to separate the incident wave from the back wave. An attenuator acts as a ground which should be placed at the other end. Thus the dissipation is decreased and the wave must go back by the same path.

In the other configuration, the point of entry and exit of the wave are distinct.

7.1.2 Results and Observations

With the coupler the incident wave is split from the wave that has travelled on the board. An attenuator has to be placed on the stripline as shown in the figure 7.2. We obtained interesting results by using the configuration with a coupler. In order to observe the modifications generated by the magnetic fields, we set an electromagnetic probe on the FPGA. We can therefore study the behavior of the component placed in high Electro-magnetic field.

As illustrated in figure 7.3 we can observe the spectrum of the working FPGA2, without any wave injection. We notice that some peaks are present between 0 and 300 MHz. These peaks correspond to the clock frequency of the FPGA at 24 MHz and to its harmonics at 48 MHz, 72 MHz...

When the wave is injected, the spectrum is largely modified. For instance in figure 7.4 a wave of 900 MHz is injected. By comparison with the figure 7.3, we can observe three ranges of frequencies, where the activity of the cryptographic device is modified. As shown in figure 7.4 around:

- 900 MHz
- 1800 MHz

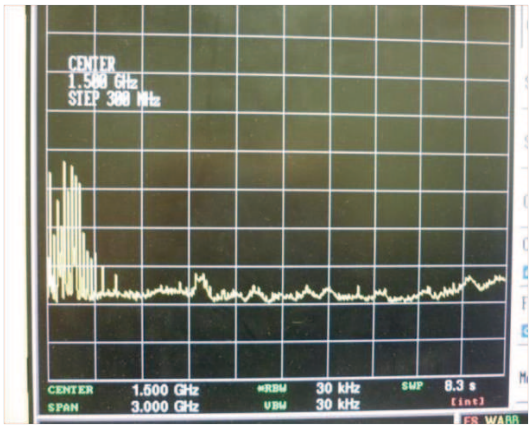


Figure 7.3: Spectrum of the working component without injecting wave.

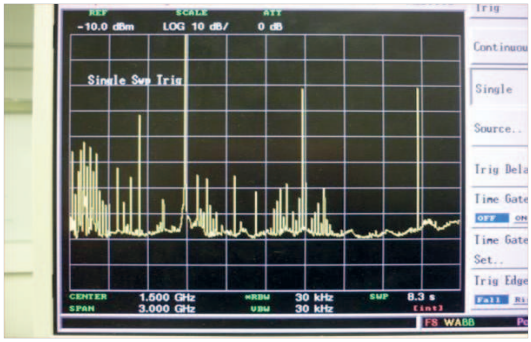


Figure 7.4: Spectrum of the working component with injected wave.

- 2400 MHz

that corresponds to the harmonics of the injected wave at 900 MHz. To obtain this phenomena, the magnitude of the wave have to be set at the minimum at 12 dBm to generate an electromagnetic field at 140 V/m.

This experiment shows that the signal is modulated around the carrier, and also that we can highlight non linear phenomena. More precisely, we can increase this phenomena by injecting a carrier. However in these frequency areas, we have noticed that the magnitude of the modulated signal is much lower than the magnitude of the carrier. This did not allow an easy demodulation of the signal even with a TEMPEST receiver. A very narrow filter has to be used to eliminate the carrier and its harmonics.

7.2 Conductive/Radiative Intentional Electro-Magnetic Interference Attacks

To avoid the issue of demodulation, another solution is to use conductive injection with a current probe as shown in the figure 7.5. Consequently the magnitude of the

injected carrier is lower than in radiative condition, and the use of a Faraday cage is not required. Recent works done by the university of Tohoku and more precisely by Hayashi *et al* concerning the fault injection by Intentional Electro-magnetic emanation have been introduced in NIAT and EMC conference in [HHS+11]. In this paper they introduce a new technique based on the conductive emission. In the next part we describe the experiment done by Hayashi and prove that this technique is also suitable for an ASIC. We are able to produce some exploitable faults. We provide more details about this experiment and show that different phenomena like glitch on clock and glitch on power are produced by these two experiments.

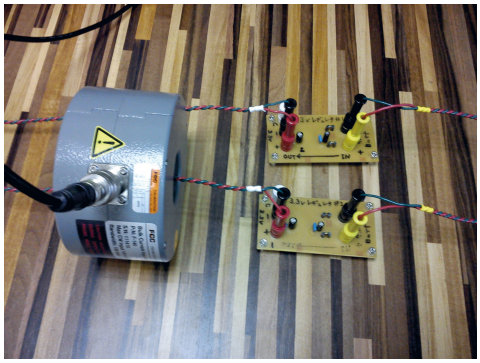


Figure 7.5: Coil, FCC probe.

7.2.1 Experimental setup

Table 7.1 summarizes the main equipment for the experiment. A coil FCC Fischer Current Probe is used to inject the current wave without any synchronisation. An analog signal generator with an amplifier are used to generate the current wave at different frequencies.

Apparatus	**Model**	**Characteristic**
Injection apparati		
Analog signal generator	Agilent N5181A	100 kHz – 3 GHz
Power amplifier	TESEQ CBA 1G-018	18 W, 100 kHz – 1 GHz
Current probe	Fischer FCC-2000	100 KHz – 1 GHz
Cryptographic apparati		
Sasebo-G board	AIST Tohoku University	Board supplied at 3.3 V
SecMatV1 board	TELECOM-ParisTech	DES is supplied nominally at 1.2 V

Table 7.1: Characteristics of the different setups used.

We present the experiments of fault injection on the AES running on a SASEBO-G Board.

7.2.2 Fault Injection on Sasebo-G with AES

In this experiment, both FPGA of the SASEBO board are separately powered. We focus on the power supply of the FPGA dedicated to the cryptography. The Vdd and Gnd power wires of the crypto FPGA are inserted into the coil FCC probe, to inject the generated wave.

We used the frequency characterization and the transfer function provided by Hayashi *et al* in [HHS+11] to select a range of frequencies and a magnitude to inject the current wave. We select the range of frequencies between 170 MHz and 230 MHz to generate a sinusoidal wave of these frequencies by using sweep functionality of the signal generator. This range of frequencies is obtained by comparing the transfer function near the clock generator and close to the FPGA that implements AES. In this experiment we modify the behavior of the clock, by injecting a carrier of variable frequency. That confirms that circuits are sensible to noise injected on their power lines and proves that the fault injection comes from a clock glitch. In other words, one specific component of the board can be targeted to disrupt its behavior and to generate faults. The generated wave has a frequency between 170 and 230 MHZ and a magnitude between 130 and 135 dBμV. In this context we obtain the faults shown in table 7.2.

Round	**Faulty Sbox**	**Faulty Hamming Weight**
R1	S9	H1
R3	S11	H2
R3	S14	H1
R5	S15	H1
R6	S3	H1
R8	S3	H1
R9	S9	H1
R9	S3	H7
R9	S9	H1
R9	S5	H4

Table 7.2: First results of fault injection onto the AES.

We notice that some faults can occur on the different rounds of the AES, and different Sboxes. The number of bits changed per Sbox is in the third column. One to 7 bits per sbox can be faulted. Moreover experimentally we observe that some faults are redundant depending on the injected frequency and of the magnitude. For the next experiment it might be interesting to developp a study of fault sensibility on this target. By considering these faults an attacker can easily retrieve the secret key by using Piret Quisquater Fault analysis or the state of the art attack for the middle round of the AES presented by Leresteux *et al.* in [DFL11] at CHES 2011. Indeed an attacker by comparing the faulty ciphertext with the correct computation can predict the right key. This technique is called DFA for Differential Fault Analysis.

To succeed a DFA the main purpose of the attacker is to realize a fault onto the last rounds of the block cipher. Therefore she decreases the number of possible key candidates, as the faulty computation depends on a subset of the key.

In this part we describe a successful oscillator frequency injection that inserts spurious latching of the registers in the logic. Then we propose to extend this technique to an ASIC device SECMAT V1 [SG] that implements a DES.

For this experiment it is interesting to observe successful fault injection, despite the presence of regulators. One explanation is that the regulator acts as low pass filter, and the injected frequency is so high for them, that they can not have any effect on the injected carrier. Indeed the injection current mode is common-mode current consequently some fluctuation are caused between the VDD and GND. A part of the common mode-current is converted into differential mode current due to the presence of parasitic elements for instance inductance capacitance... And these currents are passed to the board.

7.2.3 Fault Injection onto the DES SecMat-V1

We intend to focus on the impact of the IEMI onto the power supply. SecMatV1 due to its separated power supply for each part the board appears as a convenient device to realize these experiments.

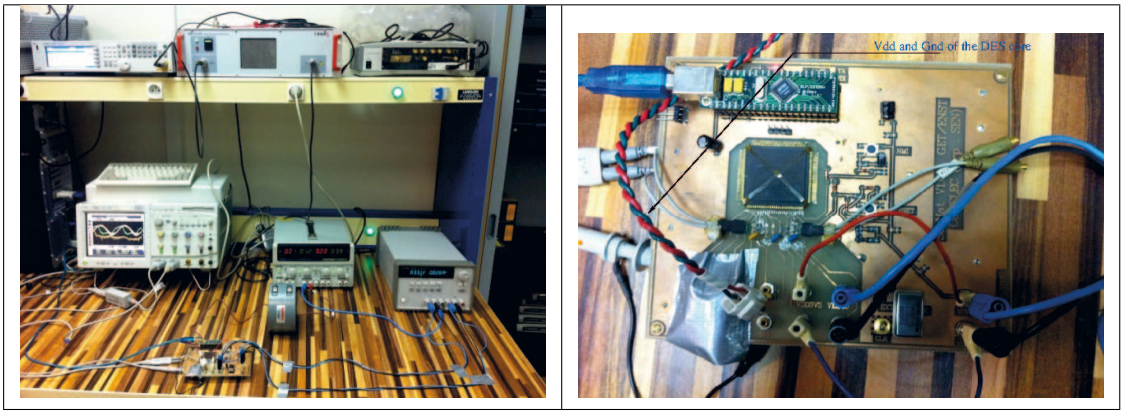


Figure 7.6: Fault injection experiment onto SecMatV1 DES, with separated power supply.

The attacker can choose to alter only the power supply of the DES core as shown on the figure 7.6. For this model there is no voltage regulator on the power supply of the DES core. During these experiments we adopt a different strategy than the one presented in the previous part. From a practical point of view, an attacker starts the fault injection attack by testing with low frequency and voltage. It means that we do not try to characterize the board as a preliminary. We prefer to observe the faults generated by changing the Voltage and the frequency till we find an efficient range of frequencies. The transfer function showing the field amplitude where the first faults appear is plotted in figure 7.8.

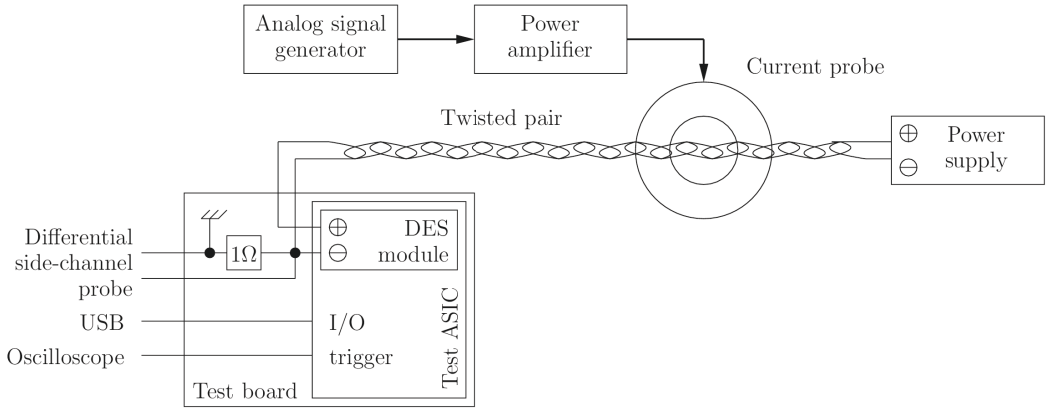


Figure 7.7: Schematic of the fault injection setup.

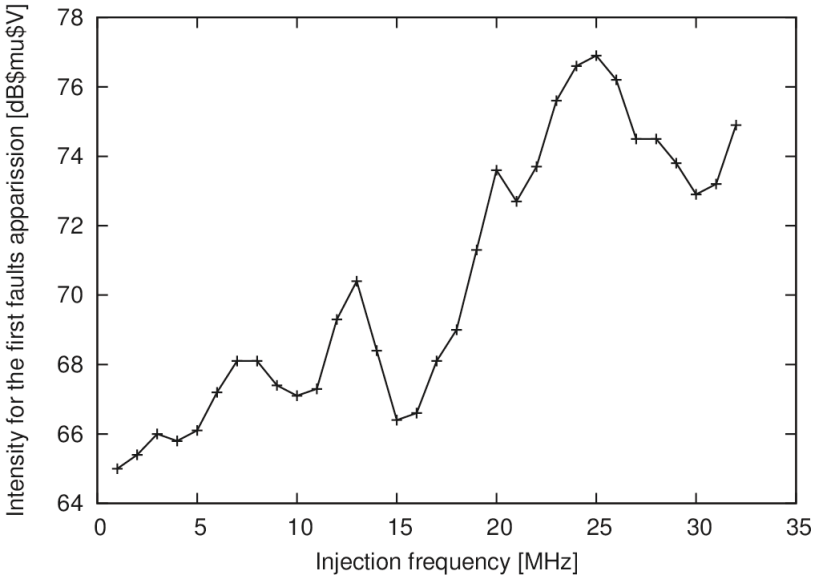


Figure 7.8: Transfer function.

We notice that for frequencies close to 1 MHz some faults are produced. Given the structure of DES, bitflips in the last round cause one difference in the ciphertext. Bitflips in the last but one round affect one or two substitution boxes. Bitflips upper in the rounds affect strictly more than two substitution boxes. It is thus clear that the sole observation of the number of bits changed in the ciphertext allows to pinpoint faults occurring in the last but one round.

Therefore, we restrict to faults affecting only one bit. This means that we consider that relevant fault models are bit-flips in the registers. The analysis of faults is guided in this respect. We search exhaustively for all the possible bit-flips in R register (32 bits) for each round (16 of them), hence a $32 \times 16 = 2^9$ exploration

size for each fault.

For the rest of the analysis, we focus on 2 remarkable frequencies: 9 and 32 MHz. The experimental setups and the results obtained for these two frequency carriers are shown on the Table. 7.3.

	First Experiment	Second Experiment
Carrier	9 MHz	32 MHz
Power, range sweep	66.5 – 68.00 dBuV	74.1 – 76.9 dBuV
Encryptions	34626	54138
Correct encryptions	24929	34871
Single bit-flip	946	87
Probability of single bit-flip	2.7 %	0.2 %

Table 7.3: Experimental conditions and statistics.

At 9 MHz the magnitude required to generate fault is lower than the magnitude at 32 MHz frequency, which is close to the maximal magnitude. The cryptographic component is clocked at 32 MHz, the energy necessary to disrupt one computation is therefore higher for this frequency.

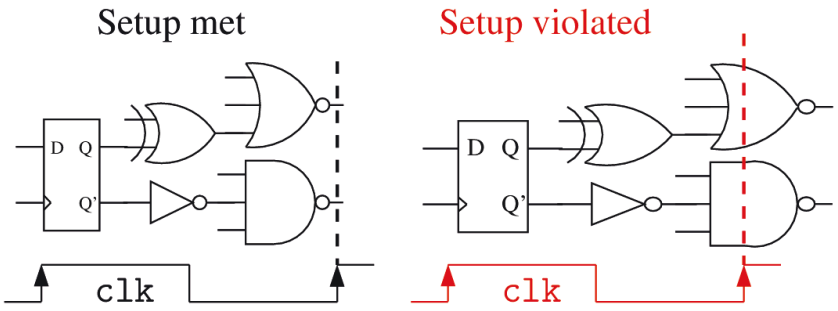


Figure 7.9: Setup time violation.

In this case, we can consider that the phenomena produced by this technique is setup time violation as shown on the figure 7.9. This phenomenon is due to transient under-power line that slows down the gates and the signals.

In the following we show more accurate statistical results obtained for these frequency carriers. The results concern the number of single bit errors obtained per round and sbox These results are listed in Tab. 7.4 and 7.5.

With this technique we can perform different types of faults. We consider the faults as uninteresting when they are key independent. In this case, they consist in a difference of one single bit in the ciphertext. An other possibility is when several bits are flipped and are not concerned with input/output of the same sboxes. The exploitable faults occur in the last but one (*i.e 15th*) round: as in the Feistel scheme

9 MHz	Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	Proba [%]	3	7	0	1	0	31	1	2	9	1	19	9	1	1	7	9
32 MHz	Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	Proba [%]	31	1	2	2	5	5	21	2	6	2	9	7	3	0	1	2

Table 7.4: Round statistics for the 9 MHz and clock-frequency injection.

9 MHz	Sbox	1	2	3	4	5	6	7	8
	Proba [%]	3	58	3	19	14	3	1	0
32 MHz	Sbox	1	2	3	4	5	6	7	8
	Proba [%]	8	41	11	13	1	3	8	14

Table 7.5: Sbox statistics for the 9 MHz and clock-frequency injection.

of DES the difference propagates directly and through the key addition followed by the sbox. They are identified by looking for single bit-flips in the right half and at least one bit flip in the sbox that they also address. Faults upper in the rounds are much more easier to detect because they cause more change in the ciphertext. Another advantage of this fault is that they make possible to attack simultaneously different sboxes. In literature, exploitation of fault in round 14 and 13 is described in paper about DFA in [BDL97]. For the inner rounds for instance 12, 10 11, 9 Rivain proposes a method in [Riv09].

We can claim that this technique to inject fault is relevant and useful. With these first results we highlight that we can reach the different rounds of the DES. This attack can be performed on a FPGA equipped with regulators and obviously on an ASIC. We notice that with this technique single bit-flip faults *i.e DES* can also be performed as single byte-flip fault with the first experiment on the AES. Moreover this technique has some advantages regarding the state of the art faults injection analysis as it does not require a synchronisation or a direct access to the component. Power cables and communication cable can be used to disrupt a crypto-system. The attack can also be performed at distance and considered as:

- radiated, since the perturbing field is created by a coil that can drive high currents, or

- conducted, as the perturbation, after conversion from the field, is conducted by the targeted wire (clock, power, etc.).

Finally it is important to notice that the component does not need to be modified or a specific preparation for example depackaging of the module is not required. In the next section, we propose some experiments to analyse the behaviour of the flowing current on the SASEBO Board.

7.3 Power Analysis in Frequency Domain

Now it is interesting to observe the phenomena by analysing power consumption measurement before having faults. We use the SASEBO-G Board, as previously described. First of all, we catch a power measurement of the Sasebo board without injecting a carrier. We perform an analysis in frequency domain and we notice two ranges of frequencies between 0 and 100 MHz and between 170 MHz and 250 MHz that differ from the rest of the spectrum as depicted on the figure 7.10.

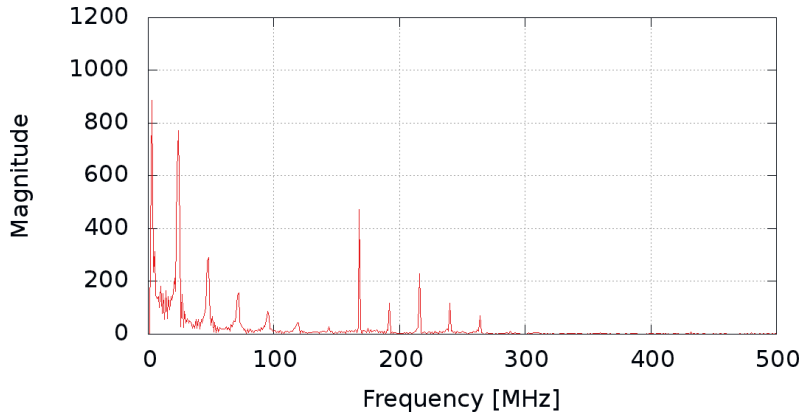


Figure 7.10: Spectrum of one power measurement without injecting a carrier.

We used the same setup as described in previous section 7.2.2. But we choose different frequencies between 170 MHz and 250 MHz and decrease the magnitude of the injected carrier in order to avoid faults. We used a Tempest receiver and scan the range of the frequency around the injected carrier and at the double frequency of the injected carrier. We used the same setup as described in the depicted schema 7.7

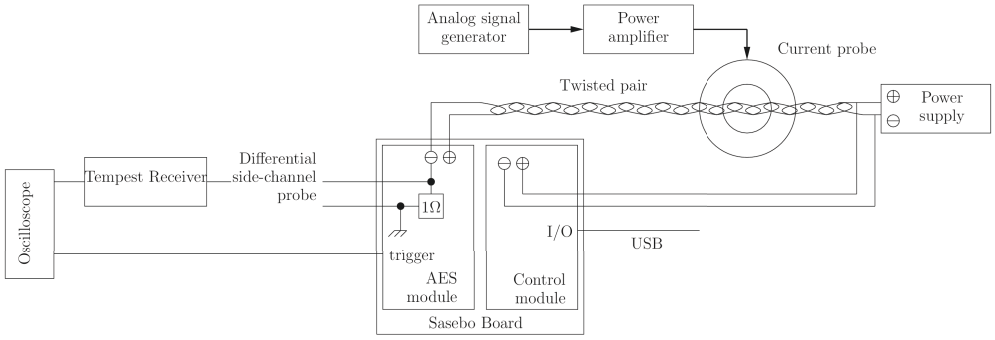


Figure 7.11: Setup of the power analysis with injected carrier and demodulation technique.

Experimentally we remark that for an injected frequency at $190MHz$ and a demodulated signal at $380MHz$, we observe the ten rounds of the AES as shown in figure 7.12. We gather 50 000 traces in this configuration. By considering demod-

ulated signal at $380MHz$, carrier injected at $190MHz$ we perform CPA which is successful on few sboxes.

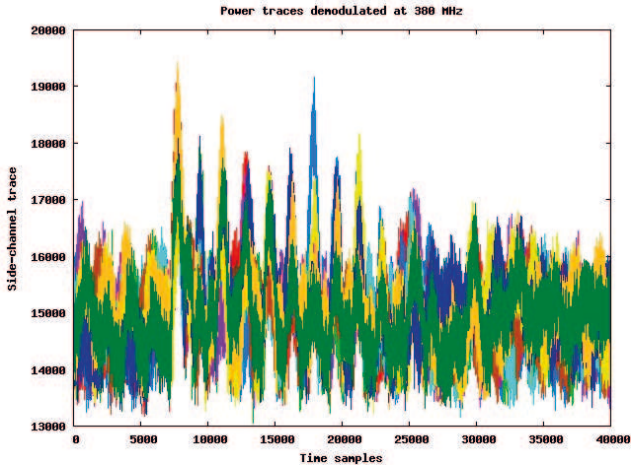


Figure 7.12: Power Measurement by injecting a carrier at 190 MHz and demodulating at 380 MHz.

The CPA has succeeded only on 4 sboxes as illustrated in figure 7.13. To success, this CPA we need a larger number of traces than for a classical CPA. This can be explained, by the fact that by injecting a carrier we add more noise and such kind of attack is not relevant in this case. Thanks to this experiment, we have proved that leakage is present at different frequencies but lost in the noise. By demodulation we reduce the range of frequencies and the power of the leakage signal. Injecting a carrier becomes therefore necessary to increase the level of the signal.

7.4 Conclusion

In this chapter, we have presented a feasibility study of active attacks based on electromagnetic theory. Experiments have shown that by using a radiative setup as described in the first section, the information is modulated by the carrier and its harmonics. Non-linear phenomena are generated but are difficult to exploit. The magnitude of the injected carrier is huge and generates a strong electromagnetic field that can damage the board. A relevant method to attack a cryptographic device is to consider conductive coupling. Experiments have been presented in the second part of this chapter. We show that a common mode current is produced by the large coil and at lower magnitude than in radiative experimentation. We performed fault attacks on two cryptographic devices (an implementation of the AES onto SASEBO Board and an implementation of the DES on an ASIC). Two types of faults can be considered single byte flip and single bit-flip. This technique appears as a new threat against cryptographic devices. Therefore new countermeasure have to be devised. From an electromagnetic compatibility point of view, first countermeasure might be to connect the board to the ground just after the input of the power supply,

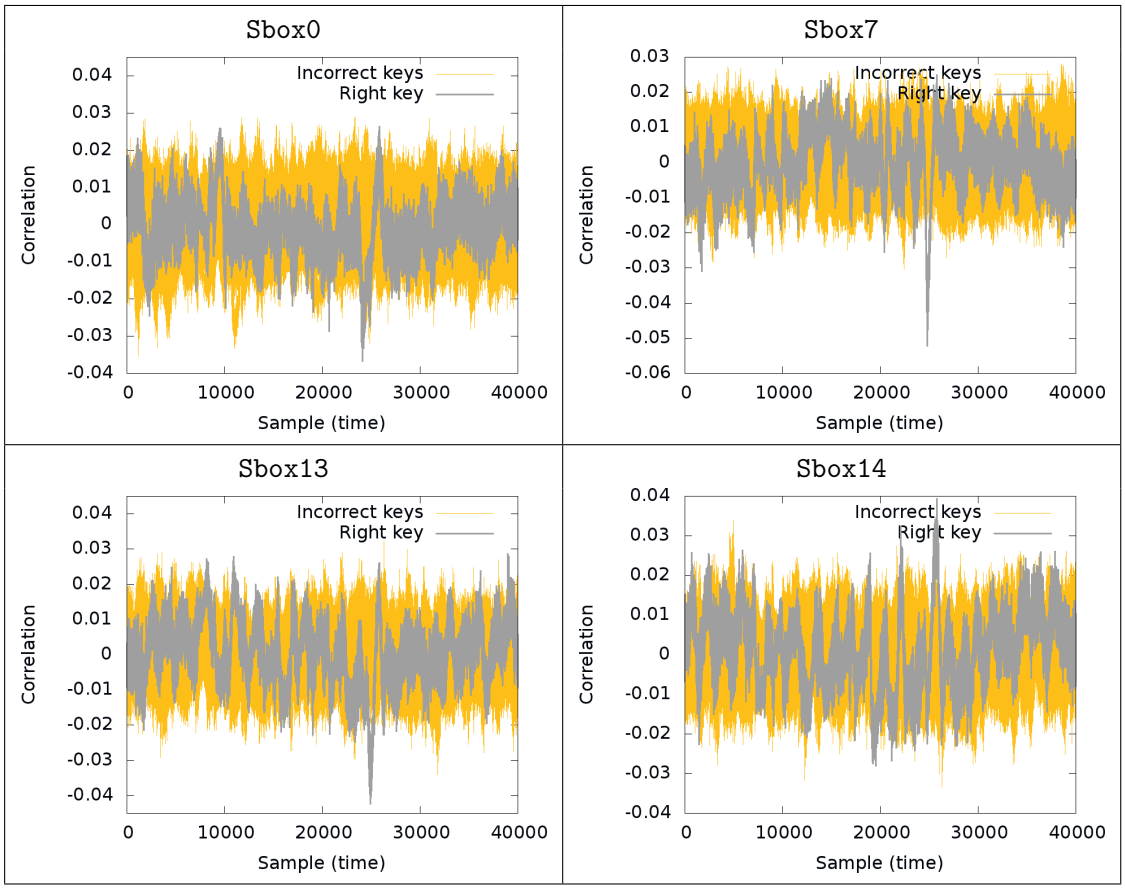


Figure 7.13: Differential traces obtained for the right key hypothesis, by injecting a carrier at 190 MHz and demodulating at 380 MHz.

and thus cancel the common mode current. Still this method has some advantages like the fact that it is not necessary to have a correct trigger to inject the carrier. The depackaging of the chip is not necessary required in comparison of the state of the art fault attack methods. In this way, this technique can be considered as an efficient technique. Finally we show that the leakage of a cryptographic device can be highlighted at different frequencies by using tempest demodulation on the same fault injection platform. However we injected a wave just under the level to provoke faults.

Chapter 8

Conclusion

In this thesis we conduct a more precise study of electromagnetic radiation and their characterization in the frequency domain to improve the EMA attacks at distance. Firstly, we present the state of the art of these attacks. We show that a cryptographic device leaks at distance some information. At 50 cm from the component an attacker can retrieve the secret data computed by an AES component. By using different leakage model an attacker can enhance the process to retrieve the secret. In DATE 2010 [MGDS10], we published several results concerning the attacks at distance and a systematic study of the behavior of leakage signal with the distance. Then in WISA 2010 [AMGD10], COSADE 2011 [**?**] and EMC 2010 [SMGD08] we propose a method by combining time samples to improve these attacks, in order to limit the degradation of the leakage model due to low signal to noise ratio. Next we show the limits of the attack before proposing methods of frequency analysis, to focus the analysis on a wide band of frequencies. In some cases an analysis and a characterization in frequency domain might improve the quality of the signal carrying information.

Indeed we present different methods of frequency analysis allowing us to extract information from a raw signal. We illustrate these methods with two cases of studies. The first study published in [MGF+10], shows how to deal with radiation from a PS/2 keyboard to calibrate TEMPEST receiver and thus retrieve a password typed on the keyboard, at a distance.

These methods are based on cryptanalysis distinguisher applied in frequency domain. After this characterization, the attacker, or evaluator can take advantage of using TEMPEST receiver. The gain and the attenuator of this apparatus can be carefully tuned to enhance the signal noise ratio for a given range of frequency. By demodulating at a given frequency the EM radiations, the attacker obtains a compromising signal, with some peculiarities that help him to retrieve the secret or right logic sequence for the emanations of a Keyboard. We demonstrate that these techniques can be applied to the asymmetric cryptographic algorithms and allow to perform SEMA (Simple Electromagnetic Analysis) with a pre-demodulation processing on a cryptographic component in DATE 2011 [MRG+11] and EMC 2011 [MHH+11]. We conclude that the TEMPEST receiver presents a real advantage to enhance the electromagnetic side channel attack. Indeed an attacker with a suitable method of detecting the compromising frequencies and with TEMPEST Receiver, could tackle the strongest counter measures by detecting bit commands, cancelling algorithmic noise ...

After we experiment electromagnetic compatibility techniques traditionally used

to evaluate the Immunity or susceptibility of electronic device, to perform fault and modify the leakage at different frequencies. We explore the richness of the common mode current that appears as a real threat against cryptographic device. With the presented experiment, the fault model can be single-bit flip or single-byte flip. These faults are produced by setup time violation due to glitch on power and on clock. Moreover this technique is very convenient, because it does not need depackaging or chip preparation, and no trigger is required. Then by injecting a carrier on the power of the board we can carry out fault injection attack in order to recover secret elements but we demonstrate that we can also modify the leakage of a crypto-system in frequency domain.

Publications

[A] Olivier Meynard and Sylvain Guilley and Jean-Luc Danger and Laurent Sauvage, **Far Correlation-based EMA with a precharacterized leakage model**, 2010, March 8-12, DATE'10, 977–980, IEEE Computer Society, Dresden, Germany.

[B] Laurent Sauvage and Olivier Meynard and Sylvain Guilley and Jean-Luc Danger, **ElectroMagnetic Attacks Case Studies on Non-Protected and Protected Cryptographic Hardware Accelerators**, 2010, July 25-28, IEEE EMC, Special session #4 on Modeling/Simulation Validation and use of FSV,Fort Lauderdale, Florida, USA.

[C] Sylvain Guilley and Olivier Meynard and Laurent Sauvage and Jean-Luc Danger, **An Empirical Study of the EIS Assumption in Side Channel Attacks against Hardware Implementations**, COSADE, 2010, February 4-5, 10-14, Darmstadt, Germany. http://cosade2010.cased.de/files/proceedings/cosade2010_paper_3.pdf.

[D] Olivier Meynard and Sylvain Guilley and Florent Flament and Jean-Luc Danger and Denis Réal and Frédéric Valette, **Characterization of the Electro-Magnetic Side Channel in Frequency Domain**, InsCrypt, 2010, October 20-23, pages 175-190, Springer, LNCS, Shanghai, China.

[E] Olivier Meynard and Sylvain Guilley and Denis Réal and Jean-Luc Danger, **Time Samples Correlation Attack**, COSADE 2011, February 24-25,p 67-72, Darmstadt, Germany. http://cosade2011.cased.de/files/2011/cosade2011_talk7_paper.pdf.

[F] Olivier Meynard and Denis Réal and Sylvain Guilley and Jean-Luc Danger and Naofummi Homma, **Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques**, DATE, 2011, March 14-18, IEEE Computer Society, Grenoble, France.

[G] Olivier Meynard, Yu-Ichi Hayashi, Naofumi Homma, Sylvain Guilley, Jean-Luc Danger, **Identification of information leakage spots on a cryptographic device with an RSA processor**, 2011, aug., pages 773 -778, 2011 IEEE International Symposium on Electromagnetic Compatibility (EMC),

Bibliography

[14001] Federal Information Processing Standards (FIPS) Publication 140-2, *Security requirements for cryptographic modules*, May 25 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. (Cited on page 8.)

[AARR03] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi, *The EM Side–Channel(s)*, Cryptographic Hardware and Embedded Systems - CHES 2002 (Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, eds.), LNCS, vol. 2523, Springer, 2003, pp. 29–45. (Cited on pages 57, 63, 70 and 93.)

[AMGD10] Moulay Abdelaziz El Aabid, Oliver Meynard, Sylvain Guilley, and Jean-Luc Danger, *Combined Side-Channel Attacks*, WISA, LNCS, vol. 6513, Springer, August 24-26 2010, Jeju Island, Korea. DOI: 10.1007/978-3-642-17955-6_13, pp. 175–190. (Cited on page 113.)

[APSQ06] Cédric Archambeau, Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater, *Template Attacks in Principal Subspaces*, CHES, LNCS, vol. 4249, Springer, October 10-13 2006, Yokohama, Japan, pp. 1–14. (Cited on pages 42 and 69.)

[BCO04] Éric Brier, Christophe Clavier, and Francis Olivier, *Correlation Power Analysis with a Leakage Model*, CHES, LNCS, vol. 3156, Springer, August 11–13 2004, Cambridge, MA, USA, pp. 16–29. (Cited on pages 26, 29, 31, 35 and 65.)

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, *On the Importance of Checking Cryptographic Protocols for Faults*, Proceedings of Eurocrypt'97, LNCS, vol. 1233, Springer, May 11-15 1997, Konstanz, Germany, pp. 37–51. (Cited on pages 14 and 108.)

[Ber05] Daniel J. Bernstein, *The Poly1305-AES Message-Authentication Code*, FSE, 2005, pp. 32–49. (Cited on page 12.)

[CCD00] Christophe Clavier, Jean-Sébastien Coron, and Nora Dabbous, *Differential Power Analysis in the Presence of Hardware Countermeasures*, CHES (London, UK), LNCS, Springer-Verlag, August 2000, pp. 252–263. (Cited on page 37.)

[CCDP04] Vincent Carlier, Hervé Chabanne, Emmanuelle Dottax, and Hervé Pelletier, *Electromagnetic Side Channels of an FPGA Implementation of AES*, Cryptology ePrint Archive, Report 2004/145, 2004, http://eprint.iacr.org/. (Cited on page 66.)

[CCDP05] ———, *Generalizing Square Attack using Side-Channels of an AES Implementation on an FPGA*, FPL (Tero Rissa, Steven J. E. Wilton, and Philip Heng Wai Leong, eds.), IEEE, 2005, pp. 433–437. (Cited on page 66.)

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi, *Towards Sound Approaches to Counteract Power-Analysis Attacks*, CRYPTO, LNCS, vol. 1666, Springer, August 15-19 1999, Santa Barbara, CA, USA. (Cited on page 48.)

[CKN00] Jean-Sébastien Coron, Paul C. Kocher, and David Naccache, *Statistics and Secret Leakage*, Financial Cryptography, Lecture Notes in Computer Science, vol. 1962, Springer, February 20-24 2000, Anguilla, British West Indies, pp. 157–173. (Cited on page 29.)

[CRR02] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi, *Template Attacks*, CHES, LNCS, vol. 2523, Springer, August 2002, San Francisco Bay (Redwood City), USA, pp. 13–28. (Cited on page 26.)

[DFL11] Patrick Derbez, Pierre-Alain Fouque, and Delphine Leresteux, *Meet-in-the-middle and impossible differential fault analysis on aes*, CHES, 2011, pp. 274–291. (Cited on page 104.)

[Eck85] Wim Van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, Computers Secutity, 1985. (Cited on page 57.)

[EG10] Moulay Abdelaziz Elaabid and Sylvain Guilley, *Practical Improvements of Profiled Side-Channel Attacks on a Hardware Crypto-Accelerator*, AFRICACRYPT, LNCS, vol. 6055, Springer, May 03-06 2010, Stellenbosch, South Africa. DOI: 10.1007/978-3-642-12678-9_15, pp. 243–260. (Cited on page 27.)

[FZY+06] Yibo Fan, Xiaoyang Zeng, Yu Yu, Gang Wang, and Qianling Zhang, *A modified high-radix scalable Montgomery multiplier*, ISCAS, IEEE, May 21-24 2006, Island of Kos, Greece. (Cited on page 12.)

[GBTP08] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel, *Mutual Information Analysis*, Cryptographic Hardware and Embedded Systems – CHES 2008 (Elisabeth Oswald and Pankaj Rohatgi, eds.), LNCS, vol. 5154, Springer, 2008, pp. 426–442. (Cited on pages 26, 42 and 66.)

[GDMPV09] Benedikt Gierlichs, Elke De Mulder, Bart Preneel, and Ingrid Verbauwhede, *Empirical comparison of side channel analysis distinguishers on DES in hardware*, ECCTD. European Conference on Circuit Theory and Design (IEEE, ed.), August 23-27 2009, Antalya, Turkey, pp. 391–394. (Cited on page 29.)

[GHT05] Catherine H. Gebotys, Simon Ho, and C.C. Tiu, *EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA*, Cryptographic Hardware and Embedded Systems – CHES 2005 (Josyula R. Rao and Berk Sunar, eds.), LNCS, vol. 3659, Springer, 2005, pp. 250–264. (Cited on page 65.)

[GLRP06] Benedikt Gierlichs, Kerstin Lemke-Rust, and Christof Paar, *Templates vs. stochastic methods*, Cryptographic Hardware and Embedded Systems - CHES 2006 (Louis Goubin and Mitsuru Matsui, eds.), LNCS, vol. 4249, Springer, 2006, pp. 15–29. (Cited on page 42.)

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier, *Electromagnetic analysis: Concrete results*, Cryptographic Hardware and Embedded Systems - CHES 2001 (Çetin Kaya Koç, David Naccache, and Christof Paar, eds.), LNCS, vol. 2162, Springer, 2001, pp. 251–261. (Cited on pages 21 and 57.)

[HHS+11] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, *Non-invasive emi-based fault injection attack against cryptographic modules*, Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on, aug. 2011, pp. 763 –767. (Cited on pages 99, 103 and 104.)

[HMA+10] Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir, *Comparative Power Analysis of Modular Exponentiation Algorithms*, IEEE Trans. Computers **59** (2010), no. 6, 795–807. (Cited on page 83.)

[HMF07] Michael Hutter, Stefan Mangard, and Martin Feldhofer, *Power and em attacks on passive $13.56 MHz$ rfid devices*, CHES '07: Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems (Berlin, Heidelberg), Springer-Verlag, 2007, pp. 320–333. (Cited on page 75.)

[HNI+06] Naofumi Homma, Sei Nagashima, Yuichi Imai, Takafumi Aoki, and Akashi Satoh, *High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching*, CHES, LNCS, vol. 4249, Springer, October 10-13 2006, Yokohama, Japan, pp. 187–200. (Cited on page 36.)

[JPS05] Marc Joye, Pascal Paillier, and Berry Schoenmakers, *On Second-Order Differential Power Analysis*, CHES, LNCS, vol. 3659, Springer, August 29 – September 1st 2005, Edinburgh, UK, pp. 293–308. (Cited on page 48.)

[JY03] Marc Joye and Sung-Ming Yen, *The montgomery powering ladder*, Cryptographic Hardware and Embedded Systems - CHES 2002 (Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, eds.), LNCS, vol. 2523, Springer, 2003, pp. 291–302. (Cited on page 16.)

[KA98] Markus G. Kuhn and Ross J. Anderson, *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, Information Hiding, 1998, pp. 124–142. (Cited on page 57.)

[Ker83a] Auguste Kerckhoffs, *La cryptographie militaire (1)*, Journal des sciences militaires **9** (1883), 5–38, http://en.wikipedia.org/wiki/Kerckhoffs_law. (Cited on page 4.)

[Ker83b] ———, *La cryptographie militaire (2)*, Journal des sciences militaires **9** (1883), 161–191, http://en.wikipedia.org/wiki/Kerckhoffs_law. (Cited on page 4.)

[KJJ96] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, CRYPTO'96, LNCS, vol. 1109, Springer-Verlag, 1996, (PDF), pp. 104–113. (Cited on page 12.)

[KJJ99] ———, *Differential Power Analysis*, Proceedings of CRYPTO'99, LNCS, vol. 1666, Springer-Verlag, 1999, pp. 388–397. (Cited on pages 14, 26 and 31.)

[Kuh03] Markus G. Kuhn, *Compromising Emanations: Eavesdropping risks of computer Displays*, Technical Report UCAM-CL-TR-577, December 2003. (Cited on pages 60, 63 and 70.)

[Kuh05] ———, *Security Limits for Compromising Emanations*, Cryptographic Hardware and Embedded Systems – CHES 2005 (Josyula R. Rao and Berk Sunar, eds.), LNCS, vol. 3659, Springer, 2005, pp. 265–279. (Cited on page 57.)

[LCC+06] Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume, *A Proposition for Correlation Power Analysis Enhancement*, CHES, LNCS, vol. 4249, Springer, 2006, Yokohama, Japan, pp. 174–186. (Cited on pages 31 and 66.)

[LCC08] Thanh-Ha Le, Cécile Canovas, and Jessy Clédière, *An overview of side channel analysis attacks*, ASIACCS, ASIAN ACM Symposium on Information, Computer and Communications Security, 2008, DOI: 10.1145/1368310.1368319. Tōkyō, Japan, pp. 33–43. (Cited on page 29.)

[LMM05] Huiyun Li, A. Theodore Markettos, and Simon Moore, *Security Evaluation Against Electromagnetic Analysis at Design Time*, Cryptographic Hardware and Embedded Systems – CHES 2005 (Josyula R. Rao and Berk Sunar, eds.), LNCS, vol. 3659, Springer, 2005, pp. 280–292. (Cited on page 63.)

[Man04] Stefan Mangard, *Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness*, CT-RSA, LNCS, vol. 2964, Springer, 2004, San Francisco, CA, USA, pp. 222–235. (Cited on pages 37 and 38.)

[MDS99] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan, *Investigations of Power Analysis Attacks on Smartcards*, USENIX — Smartcard'99, May 10–11 1999, Chicago, Illinois, USA (Online PDF), pp. 151–162. (Cited on page 46.)

[Mes00] Thomas S. Messerges, *Using Second-Order Power Analysis to Attack DPA Resistant Software*, CHES, LNCS, vol. 1965, Springer-Verlag, August 17-18 2000, Worcester, MA, USA, pp. 238–251. (Cited on page 32.)

[MGDS10] Olivier Meynard, Sylvain Guilley, Jean-Luc Danger, and Laurent Sauvage, *Far Correlation-based EMA with a precharacterized leakage model*, DATE'10, IEEE Computer Society, March 8-12 2010, Dresden, Germany, pp. 977–980. (Cited on page 113.)

[MGF+10] Olivier Meynard, Sylvain Guilley, Florent Flament, Jean-Luc Danger, Denis Réal, and Frédéric Valette, *Characterization of the Electro-Magnetic Side Channel in Frequency Domain*, InsCrypt, LNCS, Springer, October 20-23 2010, Shanghai, China, pp. 175–190. (Cited on page 113.)

[MHH+11] O. Meynard, Y. Hayashi, N. Homma, S. Guilley, and J. Danger, *Identification of information leakage spots on a cryptographic device with an rsa processor*, Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on, aug. 2011, pp. 773 –778. (Cited on page 113.)

[MOP06] Stefan Mangard, Elisabeth Oswald, and Thomas Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, December 2006, ISBN 0-387-30857-1, `http://www.dpabook.org/`. (Cited on pages 29 and 38.)

[MRG+11] Olivier Meynard, Denis Réal, Sylvain Guilley, Jean-Luc Danger, and Naofummi Homma, *Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques*, DATE, IEEE Computer Society, March 14-18 2011, Grenoble, France. (Cited on page 113.)

[Pee06] Éric Peeters, *Towards Security Limits of Embedded Hardware Devices: from Practice to Theory*, Ph.D. thesis, Université catholique de Louvain, November 2006. (Cited on page 38.)

[PHF08] Thomas Plos, Michael Hutter, and Martin Feldhofer, *Evaluation of side-channel preprocessing techniques on cryptographic-enabled hf and uhf rfid-tag prototypes*, Workshop on RFID Security 2008, Budapest, Hungary, July 9-11, 2008 (Sandra Dominikus, ed.), 2008, pp. 114 – 127. (Cited on page 65.)

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan, *Statistical Analysis of Second Order Differential Power Analysis*, IEEE Transactions on Computers **58** (2009), no. 6, 799–811. (Cited on page 48.)

[PSQ07a] Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater, *Power and electromagnetic analysis: improved model, consequences and comparisons*, Integr. VLSI J. **40** (2007), 52–60. (Cited on page 31.)

[PSQ07b] Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater, *Power and electromagnetic analysis: Improved model, consequences and comparisons*, Integration, The VLSI Journal, special issue on "*Embedded Cryptographic Hardware*" **40** (2007), 52–60, DOI: 10.1016/j.vlsi.2005.12.013. (Cited on pages 31, 39, 41 and 51.)

[QS01] Jean-Jacques Quisquater and David Samyde, *ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smard Cards*, Smart Card Programming and Security (E-smart 2001) (I. Attali and T. P. Jensen, eds.), LNCS, vol. 2140, Springer-Verlag, September 2001, Nice, France. ISSN 0302-9743, pp. 200–210. (Cited on pages 13 and 21.)

[QS05] ———, *Radio frequency attacks*, Encyclopedia of Cryptography and Security (Henk C. A. van Tilborg, ed.), Springer, 2005. (Cited on page 57.)

[QS07] Jean-Jacques Quisquater and François-Xavier Standaert, *Physically Secure Cryptographic Computations: From Micro to Nano Electronic Devices*, DSN, Workshop on Dependable and Secure Nanocomputing (WDSN), IEEE Computer Society, June 28 2007, Invited Talk, 2 pages, Edinburgh, UK. (Cited on page 31.)

[RBW04] W.A. Radasky, C.E. Baum, and M.W. Wik, *Introduction to the special issue on high-power electromagnetics (hpem) and intentional electromagnetic interference (iemi)*, Electromagnetic Compatibility, IEEE Transactions on **46** (2004), no. 3, 314 – 321. (Cited on page 99.)

[Riv09] Matthieu Rivain, *Differential Fault Analysis on DES Middle Rounds*, CHES, Lecture Notes in Computer Science, vol. 5747, Springer, September 6-9 2009, Lausanne, Switzerland, pp. 457–469. (Cited on page 108.)

[SA03] Sergei P. Skorobogatov and Ross J. Anderson, *Optical fault induction attacks*, Cryptographic Hardware and Embedded Systems - CHES 2002 (Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, eds.), LNCS, vol. 2523, Springer, 2003, pp. 2–12. (Cited on page 15.)

[SA08a] François-Xavier Standaert and Cédric Archambeau, *Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages*, CHES, Lecture Notes in Computer Science, vol. 5154, Springer, August 10–13 2008, Washington, D.C., USA, pp. 411–425. (Cited on page 34.)

[SA08b] François-Xavier Standaert and Cédric Archambeau, *Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages*, Cryptographic Hardware and Embedded Systems – CHES 2008 (Elisabeth Oswald and Pankaj Rohatgi, eds.), LNCS, vol. 5154, Springer, 2008, pp. 411–425. (Cited on page 69.)

[Sat] Akashi Satoh, *Side-channel Attack Standard Evaluation Board, SASEBO*, Project of the AIST – RCIS (Research Center for Information Security), http://www.rcis.aist.go.jp/special/SASEBO/. (Cited on page 83.)

[SBG+09] Nidhal Selmane, Shivam Bhasin, Sylvain Guilley, Tarik Graba, and Jean-Luc Danger, *WDDL is Protected Against Setup Time Violation Attacks*, FDTC, IEEE Computer Society, September 6th 2009, In conjunction with CHES'09, Lausanne, Switzerland. DOI: 10.1109/FDTC.2009.40; Online version: http://hal.archives-ouvertes.fr/hal-00410135/en/, pp. 73–83. (Cited on page 17.)

[SBM+05] François-Xavier Standaert, Lejla Batina, Elke De Mulder, Kerstin Lemke, Nele Mentens, Elisabeth Oswald, and Eric Peeters, *Report on DPA and EMA attacks on FPGAs*, July 31 2005, ECRYPT (IST-2002-507932, "European Network of Excellence in Cryptography". Deliverable D.VAM.5, http://www.ecrypt.eu.org/ecrypt1/documents/D.VAM.5-1.pdf). (Cited on page 21.)

[SDB+10] Oliver Schimmel, Paul Duplys, Eberhard Boehl, Jan Hayek, and Wolfgang Rosenstiel, *Correlation power analysis in frequency domain*, COSADE, February 4-5 2010, pp. 1–3. (Cited on page 65.)

[SG] Jean-Luc Danger-Florent Flament Sylvain Guilley, Renaud Pacalet. (Cited on page 105.)

[SGV08] François-Xavier Standaert, Benedikt Gierlichs, and Ingrid Verbauwhede, *Partition vs. Comparison Side-Channel Distinguishers: An*

Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices, ICISC, LNCS, vol. 5461, Springer, December 3-5 2008, Seoul, Korea, pp. 253–267. (Cited on page 26.)

[SMGD08] Laurent Sauvage, Olivier Meynard, Sylvain Guilley, and Jean-Luc Danger, *ElectroMagnetic Attacks Case Studies on Non-Protected and Protected Cryptographic Hardware Accelerators*, IEEE EMC, Special session #4 on Modeling/Simulation Validation and use of FSV, July 25-28 2008, Fort Lauderdale, Florida, USA. (Cited on page 113.)

[Smu90] Peter Smulders, *The threat of information theft by reception of electromagnetic radiation from rs-232 cables*, Computers & Security **9** (1990), no. 1, 53–58. (Cited on page 57.)

[SMY09] François-Xavier Standaert, Tal Malkin, and Moti Yung, *A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks*, EUROCRYPT, LNCS, vol. 5479, Springer, April 26-30 2009, Cologne, Germany, pp. 443–461. (Cited on page 27.)

[SPRQ06] François-Xavier Standaert, Éric Peeters, Gaël Rouvroy, and Jean-Jacques Quisquater, *An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays*, Proceedings of the IEEE **94** (2006), no. 2, 383–394, (Invited Paper). (Cited on page 37.)

[Tan07] Hidema Tanaka, *Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures*, ICISS, 2007, pp. 167–179. (Cited on pages 58 and 66.)

[tes] test, `http://www.beyondlogic.org/keyboard/keybrd.htm`. (Cited on page 64.)

[tod] todo2, `http://www.computer-engineering.org/ps2keyboard/`. (Cited on page 64.)

[VCS09] Nicolas Veyrat-Charvillon and François-Xavier Standaert, *Mutual Information Analysis: How, When and Why?*, CHES, LNCS, vol. 5747, Springer, September 6-9 2009, Lausanne, Switzerland, pp. 429–443. (Cited on page 29.)

[VP09] Martin Vuagnoux and Sylvain Pasini, *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards*, Proceedings of the 18th USENIX Security Symposium, USENIX Association, 2009. (Cited on pages 58, 63 and 72.)

Caractérisation et Utilisation du Rayonnement Electromagnétique pour l'attaque de composants cryptographiques

Résumé : Actuellement les algorithmes mathématiques de cryptographie sont de plus en plus sûrs et réputés incassables. Cependant, leurs implémentations sur des composants cryptographiques les rendent vulnérables aux attaques physiques (matérielles ou logicielles) par canaux auxiliaires SCA (Side Channel Analysis). Dans cette thèse nous développons de façon plus précise l'étude des rayonnements électromagnétiques et leur caractérisation dans le domaine fréquentiel afin d'améliorer les attaques EMA à distance. Nous proposons différentes méthodes d'amélioration de ces attaques notamment en combinant des échantillons, afin de limiter la dégradation du modèle de fuite due à un faible rapport signal / bruit. Ensuite nous montrerons les limites des ces attaques avant de proposer des méthodes d'analyse fréquentielle, pour réduire la bande de fréquence d'analyse et améliorer la qualité du signal porteur d'information. Enfin, nous verrons que des méthodes utilisées en compatibilité électromagnétique peuvent être mises en place pour réaliser des attaques en fautes sur des composants cryptographiques.

Mots clés : Cryptographie, Attaques par Canaux Auxiliaires, Système Embarqué, carte à puce, TEMPEST.

Characterization and Use of the EM radiation to enhance Side Channel Attacks

Abstract: Nowadays the mathematical algorithms for cryptography are becoming safer and deemed unbreakable from a mathematical point of view. So the confidence in cryptographic algorithms is increasing and the design of mathematical cryptographic algorithms remains definitively robust. However, the hardware implementation of cryptographic components are still vulnerable to physical attacks. Side Channel Analysis (SCA) is a threat for crypto systems as they can be used to recover secret key. These unintentional physical emanations can be analysed in a view to derive some sensitive information from them. In this thesis we conduct a more precise study of electromagnetic radiation and their characterization in the frequency domain to improve the EMA attacks at distance. We propose a method by combining time samples to improve these attacks, in order to limit the degradation of the leakage model due to low signal to noise ratio. Next we show the limits of the attack before proposing methods of frequency analysis, to focus the analysis on a wide band of frequencies and improve the quality of the signal carrying information. Finally we see that some methods used in electromagnetic compatibility and more precisely to evaluate susceptibility of electronic device. These techniques can be employed to perform fault attack and disrupt cryptographic component.

Keywords: Cryptography, Side Channel Analysis, Embedded System, Smart card, TEMPEST.