Infrared Imaging for Integrated Circuit Trust and Hardware Security

Maxime Cozzi

THÈSE POUR OBTENIR LE GRADE DE DOCTEUR DE L'UNIVERSITÉ DE MONTPELLIER

En microélectronique

École doctorale I2S

Unité de recherche LIRMM

Imagerie Infrarouge, Intégrité des Circuits Intégrés et Sécurité Matérielle

Présentée par Maxime COZZI
Le 18 novembre 2019

Sous la direction de Philippe MAURINE et Jean-Marc GALLIERE

Devant le jury composé de

Jean Michel PORTAL	Professeur	Université de Aix – Marseille	Rapporteur
Vincent BEROULLE	Professeur	Université Grenoble – Alpes	Rapporteur
Séverine GOMES	Directrice de Recherche	CETHIL – Université de Lyon	Examinatrice
Pascal NOUET	Professeur	LIRMM – Université de Montpellier	Président du jury
Laurent SAUVAGE	MCF	Télécom Paris	Invité
Philippe MAURINE	MCF	LIRMM – Université de Montpellier	Directeur de Thèse
Jean Marc GALLIERE	MCF	LIRMM – Université de Montpellier	Co-encadrant de Thèse

UNIVERSITÉ DE MONTPELLIER

Acknowledgements

Mes premiers remerciements s'adressent à mes encadrants de thèse, Philippe MAURINE et Jean-Marc GALLIERE pour leur confiance, leur soutien ainsi que pour m'avoir challengé tout au long de ces trois années de doctorat. Je les remercie également fortement pour la bonne humeur qu'ils ont su instaurer au sein de l'équipe et pour leur encadrement de qualité qui m'a permis de mener ce projet à bien. J'ajoute une mention spéciale pour les barbecues chez Philippe qui m'ont permis de découvrir le HB, boisson aux moult propriétés bénéfiques et inspirantes. Je remercie aussi Marc LACRUCHE pour son aide, nos montages bricolos et pour sa passion (grandement partagée) pour les boissons houblonnées.

J'aimerais également remercier fortement mes parents, Laura CAZAUX, et plus généralement toute ma famille pour leur soutien et leurs conseils durant cette thèse. J'adresse une pensée toute particulière à mes parents qui ont su me transmettre leur esprit curieux ainsi que leur intérêt pour la science. Je souhaite également mentionner mon grand-père Ennio COZZI pour l'intérêt ainsi que le soutien apporté durant mes études, et en particulier pendant mon doctorat.

Je suis particulièrement reconnaissant envers Victor LOMNE et Thomas ROCHE de la société NinjaLab pour leur soutien ainsi que pour m'avoir guidé et conseillé pendant mon doctorat. Je les remercie également pour toutes les pauses café et les échanges que nous avons eus et qui m'ont permis d'enrichir mes connaissances sur le milieu de la sécurité matérielle.

Je remercie très sincèrement Caroline LEBRUN pour sa bonne humeur, son aide et sa franche camaraderie qui ont été essentiels au maintien de ma santé mentale. En particulier, je tiens à mentionner ses actions héroïques au cours de la défense des doctorants contre les forces du mal. Je la remercie également d'avoir assuré mon index glycémique grâce aux "Napolitain" et autres pâtisseries.

Finalement, j'aimerais remercier toutes les personnes avec qui j'ai tissé de forts liens d'amitié pendant ce doctorat. En particulier, je remercie Nicolas JEANNIOT pour ses nombreux traquenards et son soutien, Guillaume AICHE co-fondateur des apéros MICROB, pour son assistance à l'impression 3D ainsi que pour les plans du V2, Mégane MIQUEL pour son "popolopopopo" et ses talents d'organisatrice, João SANTOS pour son amour des canapés, Vinayak KALAS pour sa passion lunaire, JR REALPE pour ses pintes de tequila, Julien TOULEMONT pour nos séances de râlerie et nos délires vidéo-ludiques, Gwenaël CHAILLOU alias "Msieur CHAILLOU" pour les pauses café et ses folles anecdotes de soirées, Geoffrey ENJOLRAS pour son humour poilant et pour m'avoir permis d'économiser sur tout les produits iodés.

Contents

List of Figures

List of Tables

List of Abbreviations

AES	**A**dvanced **E**ncryption **S**tandard
CCD	**C**harge **C**oupled **D**evice
CDF	**C**umulative **D**istribution **F**unction
DSO	**D**igital **S**amplig **O**scilloscope
DUT	**D**evice **U**nder **T**est
EM	**E**lectro**M**agnetic
EMFI	**E**lectro**M**agnetic **F**ault **I**njection
FA	**F**ailure **A**nalysis
FIA	**F**ault **I**njection **A**ttack
FOV	**F**ield **O**f **V**iew
FPGA	**F**ield **P**rogrammable **G**ate **A**rray
HTH	**H**ardware **T**rojan **H**orse
IC	**I**ntegrated **C**ircuit
IR	**I**nfra**R**ed
IP	**I**ntellectual **P**roperty
KS	**K**olmogorov **S**mirnov
LFI	**L**aser **F**ault **I**njection
MOS	**M**etal **O**xyde **S**emiconductor
NEP	**N**oise **E**quivalent **P**ower
PUF	**P**hysical **U**nclonable **F**unction
PVT	**P**rocess **V**oltage **T**emperature
RO	**R**ing **O**scillator
SCA	**S**ide **C**hannel **A**ttack
SoC	**S**ystem **o**n **C**hip
SNR	**S**ignal (to) **N**oise **R**atio
TRNG	**T**rue **R**andom **N**umber **G**enerator
VLSI	**V**ery **L**arge **S**cale **I**ntegration

List of Publications

Conference and Workshop Papers

- M. Cozzi, J. Galliere and P. Maurine, "Thermal Scans for Detecting Hardware Trojans"," 2018 Constructive Side-Channel Analysis and Secure Design (COSADE), Singapore, 2018, pp. 117-132.
  doi: 10.1007/978-3-319-89641-0_7

- M. Cozzi, J. Galliere and P. Maurine, "Exploiting Phase Information in Thermal Scans for Stealthy Trojan Detection," 2018 21st Euromicro Conference on Digital System Design (DSD), Prague, 2018, pp. 573-576.
  doi: 10.1109/DSD.2018.00100

- M. Cozzi, J. Galliere and P. Maurine, "Statistical Lock-In Thermography to Improve Contrast and Detectivity of ICs Thermal Maps", 2019 Thermal Investigation of IC and Systems (Therminic), 2019, Lecco - Soon to be published.

- A. Vasselle, P. Maurine and M. Cozzi, Breaking Mobile Firmware Encryption through Near-Field Side-Channel Analysis, 2019 Attacks and Solutions in Hardware Security (ASHES), 2019, London - Soon to be published.

Journal Papers

- M. Cozzi, J. Galliere and P. Maurine, "An IC Investigation Technique Based on Robust PVT Properties of Lock-in Thermography Measurements", 2019 IEEE Transactions on Instrumentation and Measurement - Under reviewing process.

French Summary

1 Introduction

Aujourd'hui, la majorité des secteurs d'activités (financier, militaire, énergétique, divertissement) repose sur des outils électroniques, conçus à partir de circuits intégrés (CI). Certains de ces secteurs sont dit "sensibles" lorsqu'un dysfonctionnement peut avoir de lourdes conséquences humaines et/ou financières. Dans ce contexte, la sécurité des systèmes électroniques est donc un enjeu capital.

Un système est dit sécurisé lorsque son intégrité, son authenticité ainsi que sa confidentialité peuvent être garanties. Dans cette optique, la cryptographie est souvent l'outil privilégié. Actuellement, les algorithmes de chiffrement sont considérés comme mathématiquement "inviolable" (AES par example). En revanche, l'état de l'art montre que de nombreuses attaques au niveau matériel peuvent compromettre la sécurité des circuits électroniques.

Parmi ces attaques, on distingue notamment les attaques par canaux cachés ainsi que l'injection de faute. Les attaques par canaux cachés exploitent les conséquences de fonctionnement d'un circuit intégré (émission de chaleur, rayonnement électromagnétique (EM), etc.), pour retrouver des secrets tel qu'une clé de chiffrement. Sans contre-mesure, ou lors d'une implémentation naïve, une information sensible manipulée électroniquement est susceptible de fuir sur ces "canaux cachés". Typiquement, l'analyse par canal caché s'effectue par l'analyse EM ou photonique [dBWGS11, SNK+12].

L'injection de faute consiste à briser l'aspect aléatoire nécessaire à un chiffrement robuste. Il est ainsi possible de remonter au secret en utilisant des procédés mathématiques et statistiques. L'injection de faute utilise le plus souvent des impulsions EM ou laser pour modifier l'état d'un ou plusieurs bits [DDRT12, VWWM11].

Cependant, ces attaques nécessitent, la plupart du temps, de connaitre l'emplacement du composant sécurisé (typiquement l'accélérateur cryptographique). Malgré l'augmentation exponentielle de la densité de transistors, l'accroissement de la complexité des architectures requiert des circuits occupant une surface de silicium de plus en plus élevée. Ainsi, si la surface d'une carte à puce mesure en moyenne $1\,mm^2$, celle des circuits plus complexes tel que les systèmes sur puce

(SoCs) ou les circuits programmables (FPGA) mesure souvent plus de $100\,mm^2$. Le positionnement d'un laser de quelques micromètres de diamètre ou d'une sonde EM au dessus de la cible devient donc difficile. Pour cette raison, une étape de rétro-ingénierie est souvent opérée pour localiser le périphérique au sein du circuit. Par conséquence, l'imagerie de circuit peut grandement influencer la qualité d'une attaque.

Les chevaux de Troie matériels représentent également une menace sérieuse pour les CI. Une modification malveillante d'un circuit intégré pendant sa phase de conception ou lors de sa fabrication peut être réalisée pour faciliter la fuite d'information, le déni de service ou l'obsolescence programmée. Les méthodes employées pour leur détection reposent essentiellement sur le test et l'imagerie.

La sécurité des systèmes électroniques s'appuie essentiellement sur un ensemble d'attaques connues pour lesquels des contre-mesures spécifiques ont été développées en fonction du niveau de sécurisation requis pour le composant. Le développement de techniques d'imagerie efficaces se révèle donc être un élément important pour l'amélioration de la sécurité des systèmes intégrés.

Ce document présente les résultats obtenus en utilisant l'imagerie thermique infrarouge (IR). En particulier, une plateforme faible coût d'analyse IR est présentée ainsi qu'une technique statistique d'identification des zones d'activités thermiques au sein du circuit. Enfin, une méthode de comparaison d'images IR est aussi proposée. Les méthodologies mises en œuvre sont par la suite appliquées à la rétro-ingénierie sur des circuits commercialisés ainsi qu'à la recherche de chevaux de Troie et à l'analyse de défaillance.

2 Imagerie Thermique Infrarouge pour la Cartographie de Circuits Intégrés

2.1 Rayonnement des Matériaux

Tout matériau ayant une température supérieure au zéro absolu ($-273,15\,^{\circ}C$) émet spontanément de la lumière. Bien que le comportement des matériaux réels varient énormément en fonction de leur composition, ce dernier peut-être modélisé par le comportement du corps noir.

Rayonnement du Corps Noir

Le corps noir est une entité idéale et non existante. Sa principale caractéristique est d'émettre l'intégralité du rayonnement absorbé sans aucune perte. La loi d'émission de Planck lie l'amplitude du rayonnement lumineux émis à sa longueur d'onde en suivant la relation ci-dessous :

$$I_b(\lambda, T) = \frac{2.h.c_0^2.\lambda^{-5}}{e^{\frac{h.c_0}{k.\lambda.T}} - 1} \tag{1}$$

où λ represente la longueur d'onde émise, c_0 est la vitesse de la lumière dans le vide, T définit la température du materiau, h et k sont respectivement les constantes de Planck et de Boltzmann [ID02a]. Le graphe présenté en fig. 1 donne la puissance des émissions spectrales d'un corps noir en fonction de la longueur d'onde pour différentes températures.

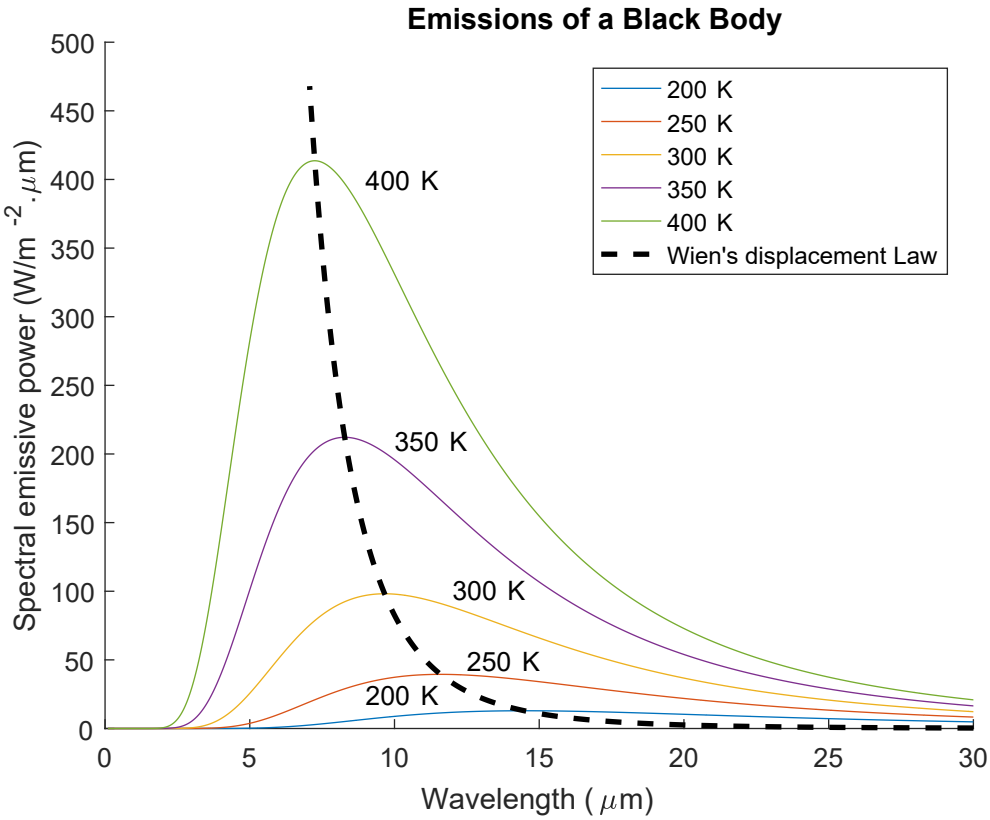


FIGURE 1: Graphe représentant les émissions spectrales d'un corps noir en fonction de la longueur d'onde pour plusieurs températures.

Entre $300° K$ et $400° K$, ce qui représente l'intervalle des températures de fonctionnement de la majorité des CI, on peut noter que le pic d'émission se situe dans les longueurs d'ondes IR. Pour cette raison, la gamme de rayonnement IR constitue un choix de prédilection pour l'analyse et l'imagerie des CI.

Rayonnement des Matériaux Réels

Le rayonnement des matériaux réels diffère de celui d'un corps noir à l'émissivité près. En effet, ceux-ci peuvent émettre de la lumière, en absorber, la transmettre ou la réfléchir.

La loi de Kirchhoff stipule qu'un matériau est en équilibre thermodynamique si le rayonnement absorbé est égal au rayonnement émis. Dans ces conditions, l'émissivité s'obtient en calculant le ratio entre la lumière émise par le corps et le total de lumière émis par le corps noir. De façon similaire, la transmissivité et la réflectivité s'obtiennent par le ratio de lumière transmise (respectivement réfléchie) par la quantité de lumière incidente. Chaque paramètre a ainsi une valeur comprise entre 0 et 1. Dans des conditions d'équilibre thermodynamique, les propriétés thermiques d'un matériau réel s'expriment comme suit :

$$\alpha + \rho + \tau = 1 \tag{2}$$

où α est l'émissivité, ρ est la transmissivité et τ la réflectivité.

2.2 Les Types de Capteurs

La réalisation d'une cartographie IR d'un circuit électronique requiert un capteur capable de transformer le signal lumineux en un signal électrique, interprétable par des instruments de mesure classiques. Les capteurs infrarouges se classent selon quatre catégories, en fonction de leur procédé de transduction. Ces catégories, accompagnées de leurs caractéristiques, sont présentées dans le tableau ci-dessous.

Detecteur		**Réponse spectrale** (μm)	**Température de Fonctionnement** (K)	$\mathbf{D^*}(cm.Hz^{\frac{1}{2}}.W^{-1})$
Bolomètre		Dépend de la vitre du boitier	300	1×10^8
Pyroélectrique			300	2×10^8
Photo-conducteur	**PbS**	1 à 3.6	300	1×10^9
	PbSe	1.5 à 5.8	300	1×10^8
	InSb	2 à 6	213	2×10^9
	HgCdTe	2 à 16	77	2×10^{10}
Photovoltaïque	**Ge**	0.8 à 1.8	300	1×10^{11}
	InGaAs	0.7 à 1.7	300	5×10^{12}
	InAs	1 à 3.1	77	1×10^{10}
	InSb	1 à 5.5	77	2×10^{10}
	HgCdTe	2 à 16	77	1×10^{10}

TABLE 1: Caractéristiques générales des différents types de capteurs, issues de la documentation technique de l'entreprise Hamamatsu [HP11a].

Les bolomètres et les capteurs pyroélectriques sont des capteurs souvent préférés pour leur capacité d'intégration plutôt que pour leurs performances. Leur détectivité $D^*(\sim 10^8 cm.Hz^{\frac{1}{2}}.W^{-1})$ et leur bande passante fréquentielle $(\sim Hz)$ sont ainsi souvent inférieures à celles des autres types de capteurs. Ceux-ci sont donc, en général,

utilisés lors de l'implémentation de matrices de détection pour les caméras thermiques. Malgré leur capacité à pouvoir acquérir une image complète en une seule acquisition, ces capteurs restent inadaptés pour l'imagerie de circuit basse consommation.

Au final, ce sont les capteurs photovoltaïques qui possèdent les performances les plus adéquates pour l'objectif visé. Le fonctionnement de ces capteurs correspond essentiellement à celui d'une diode dont la caractéristique est translatée verticalement en fonction du flux IR reçu.

Pour avoir lieu, l'effet photovoltaïque nécessite la présence d'une zone de charge d'espace, telle que les jonctions p-n ou les barrières Schottky peuvent créer. Lorsqu'un photon d'énergie suffisante (correspondant à la gamme de longueurs d'ondes détectées par le capteur) est absorbé par la zone active du capteur, des porteurs de charges (trous ou électrons) dans un état excité sont générés. Ces porteurs de charges entrent ensuite dans la zone de charge d'espace où ils sont triés suivant leur charge, créant le courant photovoltaïque. Ce courant est ainsi proportionnel à la quantité de rayonnement IR reçu et peut être mesuré par des outils classiques tel qu'un oscilloscope. La large bande spectrale en longueur d'onde du capteur photovoltaïque ainsi que sa résolution temporelle ($\sim\mu s$) en font un capteur privilégié pour l'étude des circuits intégrés.

2.3 Les Techniques d'Acquisitions

Pour cartographier les CI, deux grandes techniques peuvent être employées. La première acquiert l'intégralité du rayonnement lumineux provenant du circuit, tandis que la seconde mesure la quantité de rayonnement infrarouge présent à une fréquence préalablement déterminée. Les avantages et inconvénients de ces deux techniques sont discutés ci-dessous.

Acquisition Continue (DC)

Cette technique correspond à la façon la plus intuitive et simple de mesurer le rayonnement IR d'un circuit. Les résultats présentés dans [RCN11] et reportés fig. 2 montrent une application directe de cette technique pour analyser la répartition spatiale de la chaleur au sein d'un processeur AMD Athlon II 240. Dans ces travaux, l'auteur démontre la possibilité de suivre en temps réel la charge thermique du composant en lui appliquant plusieurs charges de calculs de référence. Les zones chaudes apparaissent ainsi au-dessus des périphériques actifs (générant de la consommation électrique).

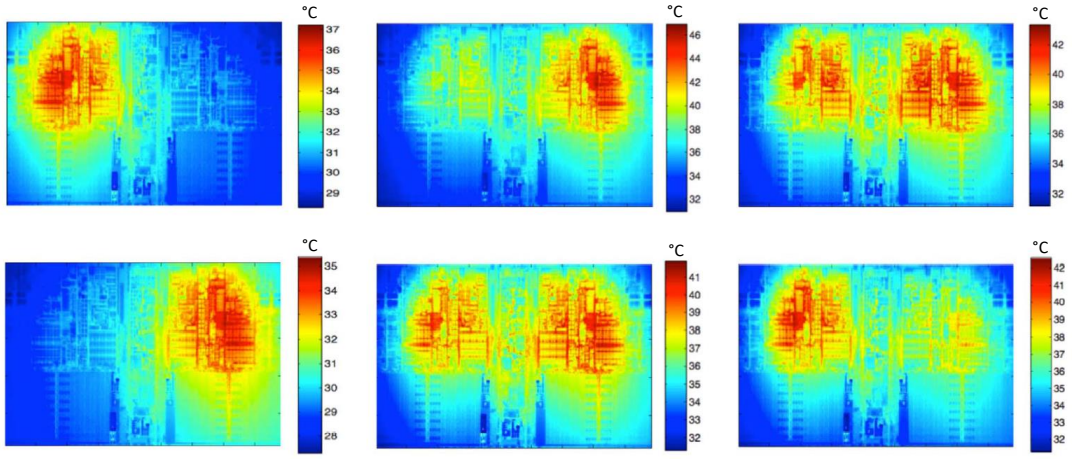


FIGURE 2: Visualisation de l'activité thermique d'un AMD Athlon II 240. Chaque image correspond à une charge logicielle différente, mettant en avant la consommation électrique de plusieurs périphériques [RCN11].

Cependant l'utilisation de cette méthode est restreinte à des mesures temporellement courtes. En effet, la mesure de l'intégralité du rayonnement issu du circuit la rend sensible aux conditions externes telles que les variations de luminosité et de température ambiante. De plus, cette méthode reste sensible à la variation d'émissivité des matériaux.

Les résultats présentés fig. 2 montrent des gradients de température allant jusqu'à 14°C. De tels gradients ne peuvent être mesurés que sur des circuits possédant une forte consommation électrique (de l'ordre de l'ampère) comme les processeurs. Les circuits basse consommation comme les SoCs embarqués ou les microcontrolleurs possèdent des consommations inférieures (de l'ordre de la centaine de milliampères) et génèrent donc des flux IR bien moins puissants. De longues mesures nécessitant de nombreuses acquisitions moyennées sont donc nécessaires et incompatibles avec cette technique de mesure.

Pour parer ce problème, [BWL10b, BWL10c] introduisent une technique basée sur la modulation de la consommation électrique du circuit et donc du signal IR associé. Cette technique est détaillée dans la section suivante.

Détection Synchrone (AC)

La détection synchrone (*lock-in*) permet d'isoler une composante fréquentielle particulière d'un signal. Ainsi dans le cas où la fréquence à mesurer est préalablement connue, cette technique permet d'extraire l'information recherchée même si celle-ci est noyée dans le bruit de mesure. Cette fréquence est désignée par f_{lockin} dans le reste du document. Il devient ainsi possible d'analyser des consommations électriques beaucoup plus faibles.

La détection thermique synchrone est réservée aux signaux alternatifs. Cela signifie qu'il doit exister une alternance entre période de chauffe et période de refroidissement. La fréquence f_{lockin} permet donc de jouer sur la résolution spatiale. Plus la fréquence de modulation de l'activité est élevée, moins la chaleur a de temps pour se diffuser au sein du substrat. Les zones d'activités apparaissent donc moins étendues. En revanche, une fréquence trop élevée peut empêcher la chaleur d'atteindre la surface du circuit. Cela génère donc une perte d'information importante puisque l'activité thermique n'est plus détectée.

Généralement, la modulation thermique est souvent artificielle. La modulation de la tension d'alimentation est la technique la plus courante mais devient impossible sur les circuits modernes qui possèdent des régulateurs de tension interne. Par la suite, il est donc proposé de recourir au "clock gating" (activation/désactivation de l'arbre d'horloge), une méthode permettant d'aiguiller l'arbre d'horloge d'un circuit dans le but d'économiser de l'énergie. L'horloge d'un circuit peut donc être consécutivement activée et désactivée pour créer la modulation thermique.

Dans [BWL10b], O. Breitenstein montre que l'étude d'un échauffement non harmonique peut-être ramenée à un problème harmonique à condition que le taux d'échantillonnage soit grand devant f_{lockin}. Ceci est généralement le cas avec les équipements modernes, donc cette condition n'est que peu contraignante. Le signal recherché peut être exprimé sous la forme suivante :

$$S(t) = A \cdot sin(2 \cdot \pi \cdot f_{lockin} \cdot t + \Phi) \tag{3}$$

où A est l'amplitude du signal, Φ sa phase et f_{lockin} sa fréquence.

La mesure synchrone consiste à réaliser l'intégration discrète du signal mesuré $F(t)$ possédant n échantillons, multiplié par le signal de corrélation $K(t)$ sur un nombre de mesures N:

$$S_\Phi = \frac{1}{n \cdot N} \sum_{i=1}^{N} \sum_{j=1}^{n} K_j F_{i,j} \tag{4}$$

L'analyse bi-canal utilise deux signaux de corrélation, un en phase, le second déphasé de 90° afin de construire les images en phase S_0 et en quadrature de phase S_{90}. $K(t)$ est ensuite remplacé par un sinus pour obtenir S_0 et par un cosinus pour obtenir S_{90}.

En utilisant les équations (5) et (6) il est possible d'obtenir l'amplitude A et la phase Φ du signal en ne connaissant que la fréquence de modulation.

$$S_0 = A \cdot cos(\Phi) \tag{5}$$

$$S_{90} = A \cdot sin(\Phi) \tag{6}$$

Celles-ci s'expriment alors comme suit :

$$A = \sqrt{S_0^2 + S_{90}^2} \tag{7}$$

$$\Phi = arctan(\frac{S_{90}}{S_0}) \tag{8}$$

Par la suite, une version "quatre quadrants" de la fonction *arctan* est utilisée. Le rétablissement du retard de phase dû à la diffusion du signal thermique est réalisé en utilisant l'équation (9)

$$\Phi = arctan(\frac{-S_{90}}{S_0}) \tag{9}$$

Les valeurs de cette fonction *arctan* étant comprises dans l'intervalle $[-180°, 180°]$, celles-ci sont ramenées sur $[0°, 360°]$ en utilisant l'équation (10).

$$\Phi_{th} = -180 - \Phi \quad (if\ \Phi > 0) \tag{10}$$

En plus d'être capable de mesurer des signaux fortement bruités, l'analyse synchrone permet de s'affranchir des émissions IR continues. Ainsi, les sources de consommations comme les courants de fuite ne sont plus pris en compte dans la mesure ce qui permet d'améliorer la lisibilité des cartes d'émissions IR. En outre, l'image de phase présente l'avantage d'être indépendante de l'émissivité des matériaux constituant le CI. Enfin, ce procédé de mesure présente une robustesse accrue aux variations des conditions de mesure telles que la température et/ou l'éclairage ambiant.

3 Identification de Zones Actives dans les Circuits Intégrés

Les systèmes d'imagerie connus reposent, le plus souvent, sur l'interprétation humaine pour la localisation des zones d'activités. Par exemple, cela est souvent réalisé par un contraste de couleurs différentiant les zones actives des zones inactives. Cependant, lorsqu'un circuit comporte de gros contrastes de densité spatiale de puissance, la différence de couleur entre une activité nulle et une activité faible peut être insuffisante pour une visualisation distincte des deux activités. De plus, il est possible que certains résultats soient sujets à une interprétation subjective lorsque l'image est peu lisible (faible résolution ou faible contraste).

Pour répondre à ce problème, cette section propose une méthode permettant de

différentier automatiquement les zones présentant de l'activité thermique du reste du circuit. Cette méthode repose sur l'analyse de paramètres statistiques variant en fonction de la présence ou non de signal IR. En particulier, il est démontré que la variance de la phase est un puissant indicateur de présence d'information thermique.

3.1 Critère de Différentiation

Les résultats présentés fig. 3 tracent les distributions théoriques de 1000 échantillons d'amplitude et de phase calculés en présence et en absence de signal IR. Pour simuler l'absence de signal IR, des distributions de $n = 10^8$ éléments possédant une moyenne de $\mu_t = 0$ et un écart type de $\sigma_t = 20$ sont générées. Afin d'être représentative des résultats expérimentaux présentés par la suite, la détection synchrone est menée à une fréquence de $10\,Hz$. Ainsi, chaque période est constituée de 10^5 échantillons.

La phase Φ est le décalage mesuré entre le signal d'activation de la source thermique et le signal IR reçu par le capteur. Lorsqu'aucune source n'est active, le signal n'est composé que de bruit. Le processus de détection synchrone fournissant forcément un résultat, une distribution de phase aléatoire (donc uniformément répartie) est attendue sur l'intervalle des valeurs possibles, à savoir $[-360^\circ\ 0]$. À l'inverse, une distribution normale devrait être obtenue lors de la présence d'information thermique à la fréquence f_{lockin}. Ce comportement est bien celui observé en fig. 3 lors de l'étude des distributions théoriques.

L'amplitude, elle, semble être répartie de façon normale dans chacun des cas. Cependant, en raison de son caractère quadratique, celle-ci ne peut être négative. Par conséquent, en l'absence de signal IR, la distribution de valeurs d'amplitude ne peut être centrée en zéro. Pour cette raison, il est probable que la distribution modélisant le mieux le comportement statistique de l'amplitude soit la distribution log-normale.

L'hypothèse d'uniformité de la distribution de phase en absence de signal IR est par la suite confirmée expérimentalement en réalisant 1000 mesures au dessus d'un FPGA. Lors de cette expérience, une source thermique reste inactive pendant la première phase de mesure et est ensuite activée pour réaliser une seconde acquisition de 1000 mesures. Les résultats sont présentés fig. 4. Conformément aux attentes, la phase est bien uniformément répartie en l'absence de signal thermique.

La variance statistique d'un groupe d'échantillons de mesure de phase est donc un indicateur important de la présence de signal IR. La section suivante propose ainsi un test statistique permettant d'extraire automatiquement les pixels possédant une activité thermique.

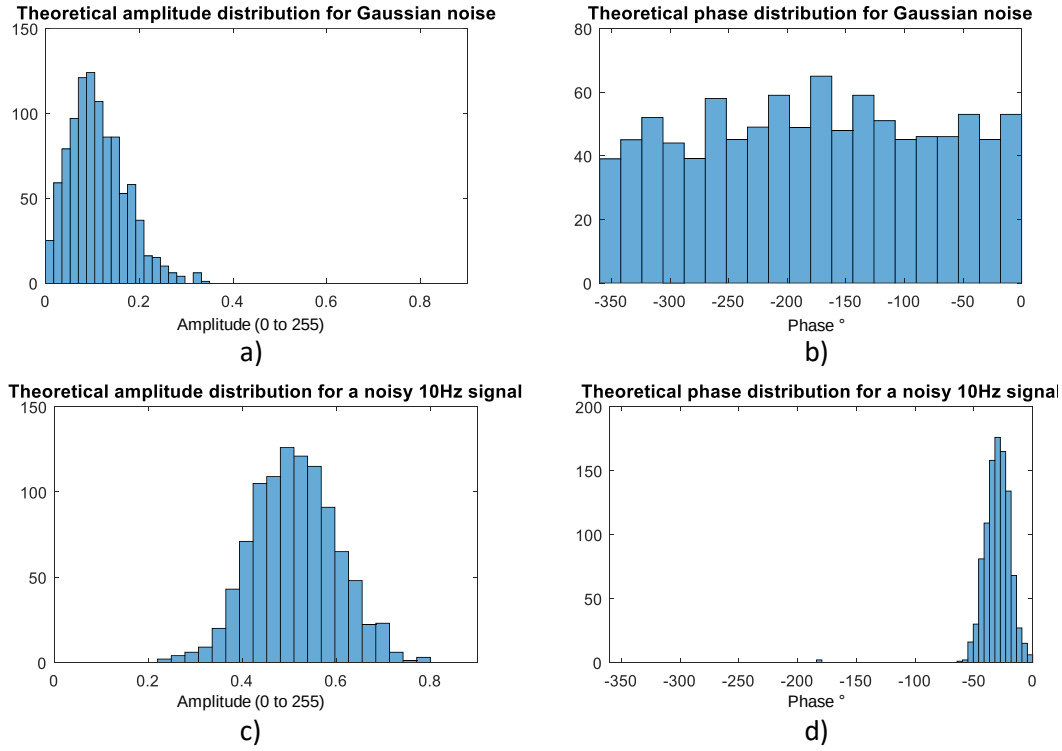


FIGURE 3: Comparaison des distributions **théoriques** statistiques de l'amplitude et de la phase lorsque la source thermique est désactivée (images du dessus) et activée (images du dessous).

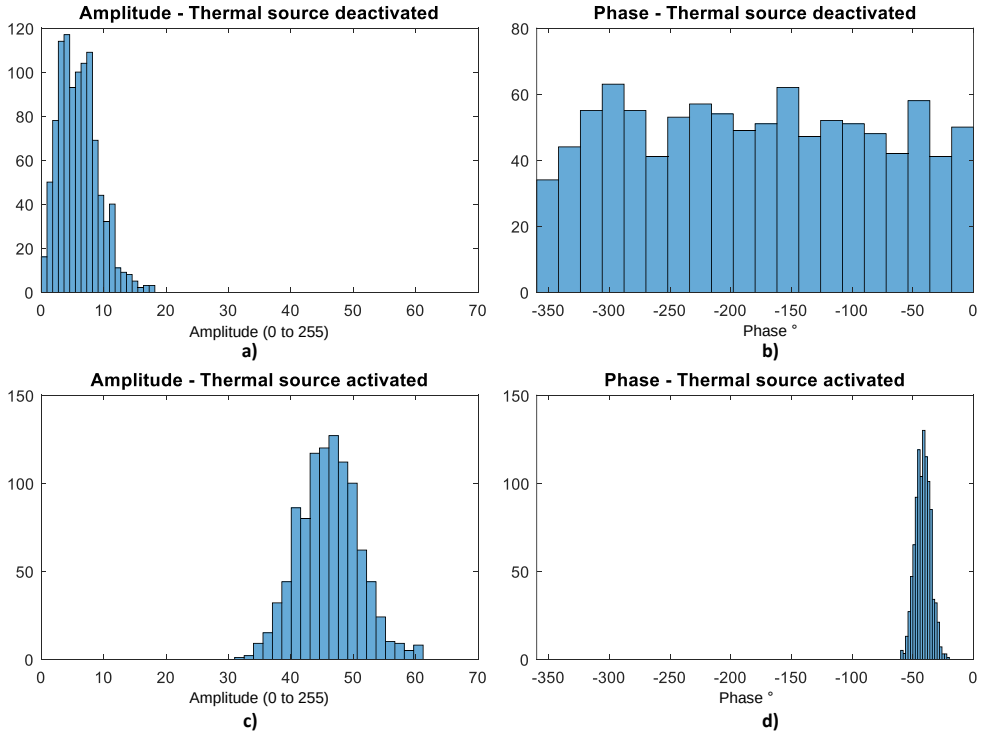


FIGURE 4: Comparaison des distributions **expérimentales** statistiques de l'amplitude et de la phase lorsque la source thermique est désactivée (images du dessus) et activée (images du dessous).

3.2 Optimisation des Images Thermiques

Les tests statistiques permettent de comparer un paramètre statistique (moyenne, variance, etc.) de deux jeux de données sous l'hypothèse H_0 que le paramètre étudié est égal pour chaque groupe d'échantillons. A l'issu de chaque test, un score est obtenu et fait parti d'une distribution théorique préalablement connue. Il est donc possible de calculer la probabilité P d'obtenir un score différent (plus grand ou plus petit que celui obtenu) sous l'hypothèse H_0. L'intervalle de confiance défini par $\alpha = 1 - P_{crit}$ est ensuite choisi pour définir la probabilité critique à partir de laquelle H_0 est acceptée ou rejetée. Typiquement, cet intervalle est fixé à 1% ou 5%.

Même si la variance et la moyenne sont des paramètres variant énormément en fonction de la présence d'un signal thermique, les différents tests associés (Welch t-test et Fischer) ont montré qu'ils étaient incapables de détecter les très faibles sources de chaleur. Pour cette raison, le test de Kolmogorov Smirnov (KS) est choisi. Le test de KS est un test d'ajustement permettant de déterminer si deux jeux de données sont issus de la même distribution. Plus précisément, il compare les fonctions de répartition suivant l'équation suivante :

$$ks = \sup_x |F_1(x) - F_2(x)| \tag{11}$$

où ks représente le score du test et F_1 et F_2 sont les fonctions de répartition associées aux deux jeux d'échantillons. Ainsi, en appliquant ce test entre une distribution de référence et celles correspondants aux pixels de la carte, il est possible de déterminer statistiquement tous les pixels dont l'activité thermique diffère de celle de la référence.

Les tailles d'échantillons comparés pouvant être différentes, la distribution de référence peut être construite théoriquement ou expérimentalement. Le choix d'une distribution dénuée de signal IR permettra d'identifier tout pixel représentant un point du circuit où la consommation électrique est suffisante pour être détectée par le capteur. A l'inverse, une distribution de référence normale centrée sur une valeur de phase particulière permettra d'identifier les équipotentielles au sein de la carte.

Pour une mise en pratique expérimentale, un circuit de test est conçu sur un FPGA Virtex 5 de chez Xilinx. L'activité nominale du circuit est celle d'un AES réalisant des chiffrements en continue. Sa signature thermique est ensuite modulée à 20 Hz en utilisant le "clock gating".

Les résultats de l'analyse thermique et statistique sont présentés fig. 5. L'image a) montre la cartographie thermique classique issue de la détection synchrone. Sur cette image, en plus de l'AES au centre, il peut être noté que trois légères activités thermiques sont également présentes dans le coin inférieur gauche. Ces sources

additionnelles sont en opposition de phase ce qui indique qu'elles sont indépendantes du design de l'AES. Sans information supplémentaire il n'est possible que de spéculer sur leur origine. Il est cependant suspecté que cette activité est liée au "clock gating" utilisé pour réaliser la modulation thermique et, de ce fait, possède une très faible consommation électrique.

L'image b) présente une cartographie du score fourni par le test de KS pour chaque pixel. Les mêmes activités que sur l'image a) sont retrouvées, avec un contraste amélioré, dû au changement d'échelle.

Enfin, les images c) et d) représentent les résultats binaires du test pour deux niveaux de confiance différents. Chaque pixel de couleur rouge représente ainsi les points rejetés par le KS test, et indiquent donc la présence de signal IR. Inversement, la couleur bleu représente les points dénués de toute activité thermique. On notera que l'augmentation du niveau de confiance permet de diminuer le bruit et le nombre de faux positifs. En retour, les faibles sources de chaleurs sont moins clairement détectés.

En comparaison, aucun des tests statistiques effectués sur la moyenne (t-test) ou la variance (f-test) n'a réussi à détecter les sources présentes dans le coin inférieur gauche. Le KS test est donc l'outil statistique le plus adapté pour la recherche de sources thermiques faibles consommations.

L'utilisation de ce procédé d'identification statistique permet d'améliorer la lisibilité des cartographies thermiques par deux méthodes : le masquage et l'amplification. La première solution s'appuie sur les résultats binaires du test pour ne garder que les zones d'intérêt thermique. Les images d'amplitude et de phase sont ainsi multipliées point à point suivant l'équation 12.

$$\begin{aligned} A_{masked}(x,y) &= \overline{A}(x,y) \cdot KS_{BinMask}(x,y) \\ \Phi_{masked}(x,y) &= \overline{\Phi}(x,y) \cdot KS_{BinMask}(x,y) \end{aligned} \tag{12}$$

Par ailleurs, dans le cas où les valeurs d'origines ne sont pas requises (localisation de sources de chaleur par example), le contraste des images thermiques peut être amplifié en pondérant chaque pixel par le score du test qui lui est associé. La normalisation permet d'obtenir un résultat cohérent par rapport à l'échelle de couleur :

$$\begin{aligned} A_{weight}(x,y) &= \frac{1}{\underset{(x,y)}{max}\left(\frac{\overline{A}(x,y)}{KS_{stat}(x,y)}\right)} \cdot \frac{\overline{A}(x,y)}{KS_{stat}(x,y)} \\ \Phi_{weight}(x,y) &= \frac{1}{\underset{(x,y)}{min}\left(\frac{\overline{\Phi}(x,y)}{KS_{stat}(x,y)}\right)} \cdot \frac{\overline{\Phi}(x,y)}{KS_{stat}(x,y)} \end{aligned} \tag{13}$$

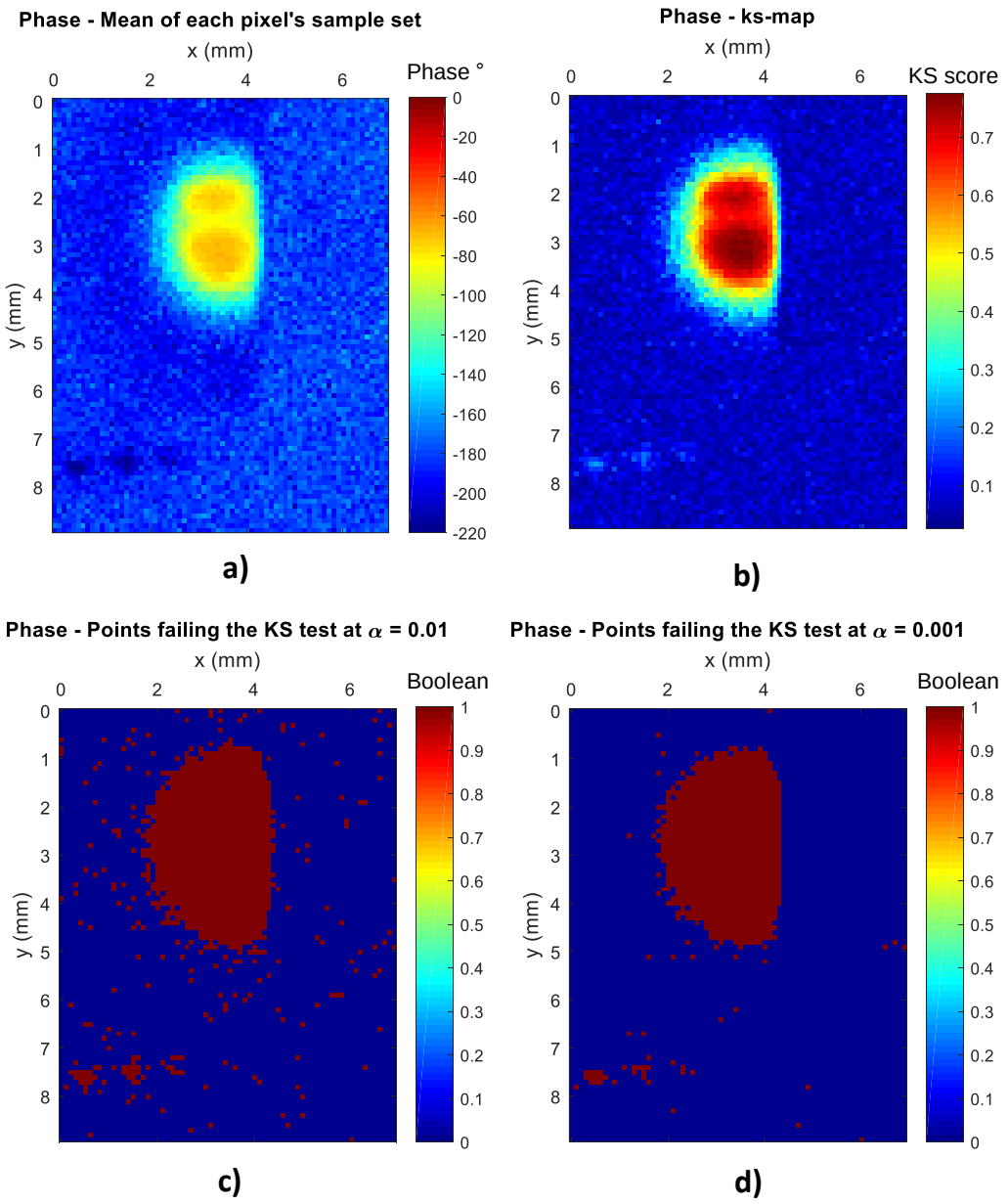


FIGURE 5: Détection de la signature thermique d'un circuit de chiffrement AES à l'aide du test de KS.

4 Banc de Mesure

Dans cette section, la configuration et les composants utilisés pour construire le banc de mesure IR sont détaillés. Le banc est ensuite caractérisé pour fournir ses performances en termes de résolution spatiale et détectivité.

4.1 Description de la Plateforme

La plateforme utilisée pour acquérir les cartographies thermiques présentées dans ce document utilise la photodiode IR J12E3 de chez Judson-Technologies. Ce capteur, fonctionnant à une température nominale de $-65^\circ C$, est thermorégulé grâce à un régulateur externe. La détectivité maximale de ce capteur monte à $D^* = 1,2 \times 10^{11}\, cm.Hz^{\frac{1}{2}}.W^{-1}$ pour $\lambda_{peak} = 3,2\,\mu m$. Sa bande passante spectrale s'étend sur l'intervalle $[1,8,\ 3,4]\,\mu m$.

Le courant généré par la photodiode étant de l'ordre du nA, ce dernier est amplifié par un amplificateur transimpédance. Le modèle d'amplificateur utilisé est un FEMTO LCA-20K-200M possédant un gain $G = 2 \times 10^8\, V/A$, une entrée ultra faible bruit de $14\, fA/Hz^{\frac{1}{2}}$ et une bande passante de $20\, kHz$. Un second étage d'amplification est ajouté avec l'amplificateur FEMTO DLPVA-100-F-S. Cet amplificateur programmable est capable de fournir un gain additionnel allant jusqu'à $100\, dB$ pour une bande passante de $100\, kHz$. Un filtre passe-bas amovible dont la fréquence de coupure est de $1\, kHz$ est également intégré à l'amplificateur. Afin de diminuer le bruit de mesure, ce filtre est activé sur l'ensemble des résultats expérimentaux présentés dans ce document. En pratique, pour éviter toute saturation liée au bruit dont l'amplitude est généralement supérieure à celui du signal IR, le gain du second étage d'amplification est limité à $40\, dB$.

En fin de chaîne de mesure, un filtre passe bas programmable à capacités commutées est ajouté. Sa fréquence de coupure est réglée au plus proche de la fréquence de *lock-in* afin de minimiser le bruit de mesure. Dans l'idéal, un filtre passe bande possédant une bande passante très étroite serait préféré. Chaque mesure est finalement numérisée et transmise à l'ordinateur de contrôle par le biais d'un oscilloscope commandé à distance. Le capteur étant mono-pixel, une table à trois axes motorisés est nécessaire afin de scanner la totalité de la surface du circuit. Ces axes sont également piloté par l'ordinateur de contrôle.

Initialement, le capteur possède un champ de vision de 60° et se trouve à une distance de $1,524\, mm$ de la vitre du boitier. Le rayonnement infrarouge reçu par le capteur provient donc d'une surface beaucoup plus grande que la zone active du capteur. Cet effet nuit gravement à la résolution spatiale du système. Pour cette raison, une optique permettant la réduction du champ de vision a été ajoutée sur le boitier.

Cette optique comprend un capuchon qui se place devant la vitre du boitier. Ce capuchon est percé en son centre pour laisser la lumière IR atteindre le capteur. Le diamètre du trou de perçage est toutefois très inférieur au diamètre de la vitre. Enfin, une lentille bille permet de focaliser le rayonnement issu du trou sur la zone active du capteur. Avec un perçage à $500\, \mu m$, le diamètre du disque focalisé par le capteur

est ainsi réduit de $1759,8\,\mu m$ à $500\,\mu m$.

4.2 Performances

Résolution en Phase

Cette plateforme présente un avantage considérable comparée aux caméras classiques en terme de fréquence d'échantillonnage. Dans le cas d'une fréquence f_{lockin} de $1\,Hz$ une caméra possédant une fréquence d'échantillonnage de $500\,Hz$ pourra fournir 500 échantillons (images) par période seulement. Par conséquence la résolution de phase obtenue est de 0.72° ($\frac{360}{500}$).

Les taux d'échantillonnage élevés des oscilloscopes modernes (~GEch/s) permettent d'obtenir des résolutions beaucoup plus élevées. Cependant, il est rare de pouvoir atteindre des taux d'échantillonnages aussi haut. En effet, les fréquences de *lock-in* faibles nécessaires à l'observation de basses consommations ainsi que la profondeur mémoire limitée des appareils de mesure sont souvent des facteurs limitant. Néanmoins, avec la même fréquence $f_{lockin} = 1\,Hz$ et un taux d'échantillonnage de $1\,MEch/s$ la résolution de phase obtenue pour la plateforme développée est de $3,6 \cdot 10^{-4}\,^\circ$. En conséquence, la résolution est améliorée d'un facteur 2000.

Capacité de Détection

La détermination de la plus petite consommation électrique détectable est difficile à estimer car elle dépend de la densité de puissance. Cette dernière varie en fonction de chaque circuit et suivant sa technologie silicium. En effet, lorsque la densité de transistors actifs est plus élevée, la détection de sources de chaleur par IR est facilitée. Il devient donc possible de localiser des sources dont la consommation est plus faible.

Les FPGA sont des circuits programmables dont la densité de transistors est des plus élevées. Cependant tous les transistors ne participent pas au fonctionnement du circuit conçu. Une partie de ces transistors ne sert qu'à l'élaboration de l'architecture du circuit et reste inactif par la suite. En conséquence, les densités de puissance de ces circuits sont bien inférieures à celles des SoCs ou des ASICs. Néanmoins, l'aspect programmable de ces circuits reste un avantage majeur, en particulier pour la caractérisation de bancs de mesures. Pour cette raison, les résultats obtenus dans cette section représentent un scénario pessimiste en terme de capacité de détection. Cela représente cependant une bonne approximation de l'ordre de grandeur de la consommation électrique détectable par notre banc de mesure.

Les images présentées ci-dessous sont acquises sur une puce Xilinx Virtex 5, gravée en technologie silicium 65 nm et dont la tension de cœur nominale est de 1 V. Le circuit de test se compose de cinq groupes de micro-chauffage. Ces micro-chauffages sont réalisés à l'aide d'oscillateurs en anneau possédant trois portes logiques et ayant une consommation de 200 μA environ. Chaque groupe est ainsi composé de 1, 2, 4, 8 et 16 micro-chauffages afin de générer des consommations électriques différentes.

Sur chaque oscillateur, une entrée logique d'activation est implémentée afin de réaliser la modulation thermique. Cette dernière est réalisée par un compteur placé à l'extérieur de la zone cartographiée pour ne pas influencer les consommations des groupes de micro-chauffage. La modulation thermique est réalisée à une fréquence de 10 Hz.

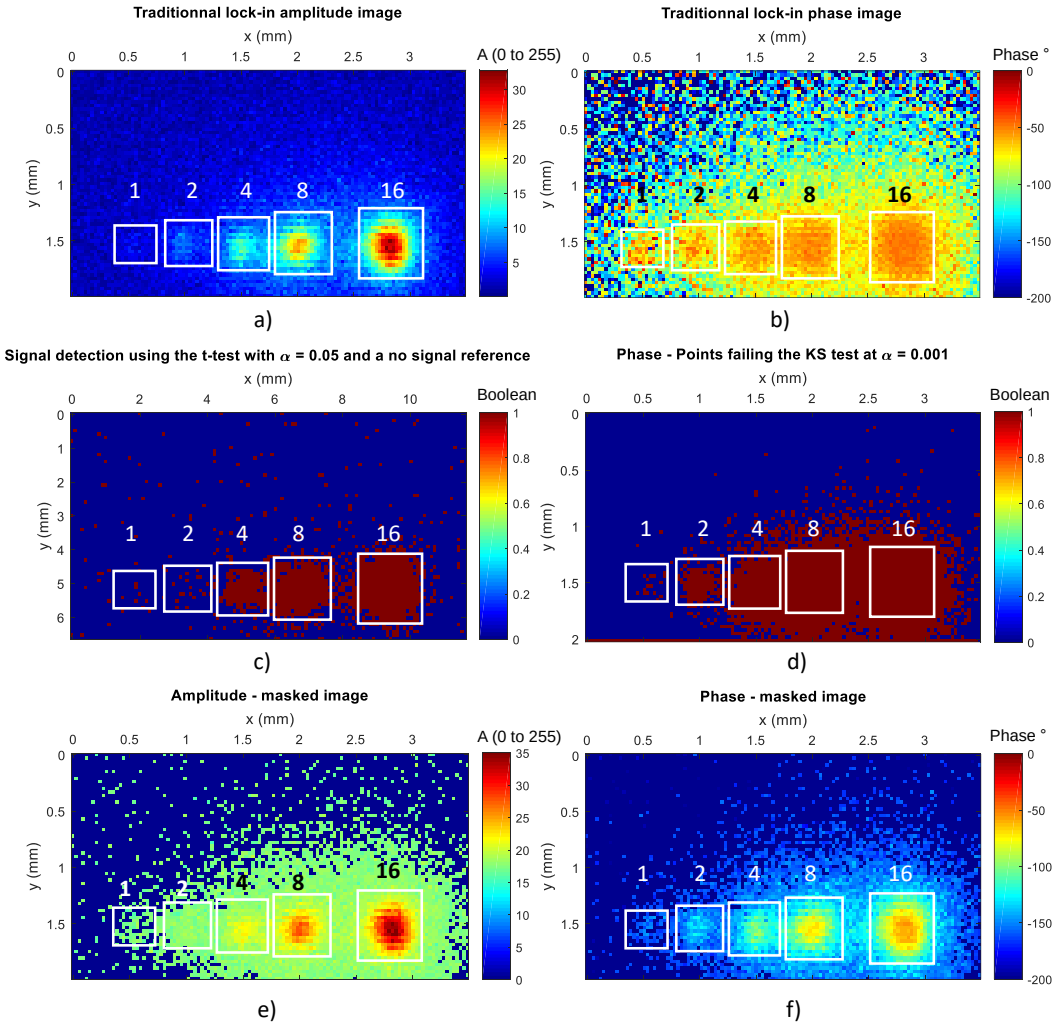


FIGURE 6: Détection de sources consommant différentes puissances électriques. Le nombre de micro-chauffages au sein de chaque source est indiqué par le chiffre juxtaposé au carré signalant son emplacement.

Les résultats expérimentaux sont présentés fig. 6. Chaque image est basée sur les

mêmes données expérimentales. Seul le traitement de données varie d'une cartographie à l'autre. Les images a) et b) correspondent à l'implémentation classique de la détection synchrone. Ces résultats montrent qu'il est possible de détecter une puissance de 400 μW en utilisant l'image d'amplitude et de 200 μW en utilisant l'image de phase.

Les images c) et d) cartographient les points rejetant l'hypothèse H_0 du t-test de Welch sur l'amplitude (test sur la moyenne) et du test KS sur la phase. La détectivité de l'image d'amplitude est conforme aux résultats présentés en a) et montre que la consommation minimale détectée est de $400\mu W$. Le test de KS sur la phase est en revanche capable de repérer chacune des sources de chaleur implémentées. Il devient donc possible de repérer l'activité d'un unique oscillateur en anneau possédant une consommation de 200 μW. Les images d'amplitude et de phase sont ensuite masquées en utilisant l'image d) et correspondent aux résultats e) et f).

Résolution Spatiale

La résolution spatiale définit la capacité d'un système d'imagerie à distinguer deux éléments spatialement rapprochés. Lors d'une analyse thermique, ce paramètre est complexifié par la présence de diffusion susceptible de masquer des sources moins puissantes.

Pour déterminer la résolution spatiale de la plateforme d'analyse, deux sources thermiques distantes sont implémentées sur un FPGA puis sont progressivement rapprochées. Une image thermique est acquise pour chaque distance séparant les deux sources. La dernière image où les deux sources sont distinguables représente ainsi la résolution spatiale limite de la plateforme.

La fig. 7 illustre les résultats de ce procédé. À cause de la diffusion thermique la position recherchée peut apparaitre subjective. Pour cette raison, la moyenne verticale des pixels de l'image est tracée en b) et d). Ces graphes permettent de confirmer que la distance séparant les deux sources est bien la limite avant que celles-ci ne soient confondues.

Ainsi, l'image d'amplitude fournit une résolution spatiale de 300 μm relative à l'échantillon test. L'image de phase est en revanche moins précise avec une résolution spatiale de 600 μm.

4.3 Rétro-conception de CI

Dans cette section, les méthodes détaillées précédemment sont appliquées à la rétro-ingénierie sur deux SoC disponibles commercialement. Pour ces circuits,

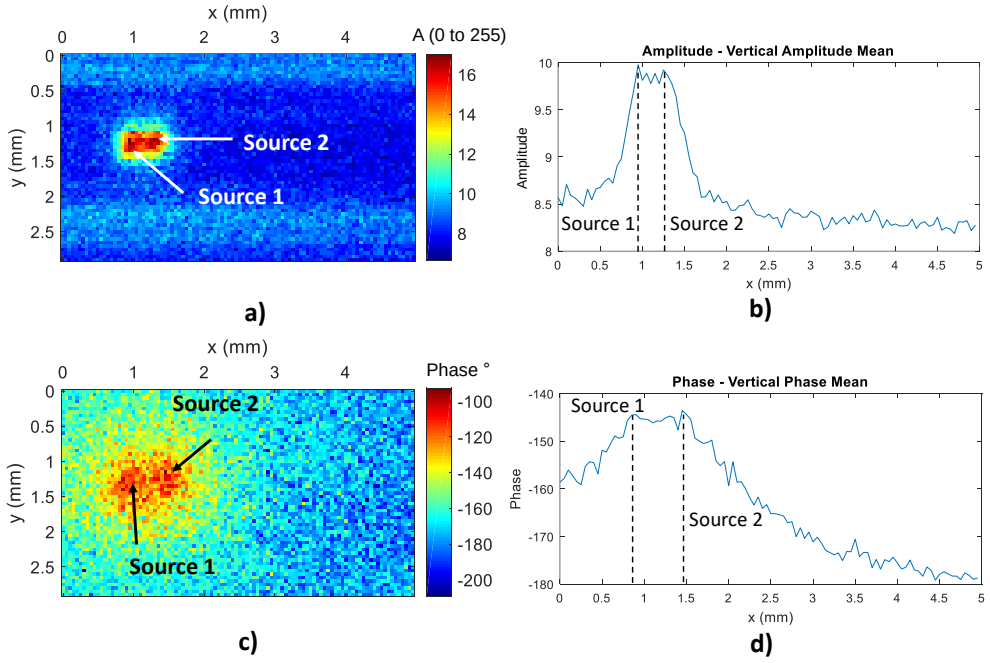


FIGURE 7: Mesure de la résolution spatiale du banc de mesure IR. a) et c) sont les images d'amplitude et phase respectivement. b) et d) représentent la moyenne verticale des pixels de l'image correspondante.

l'objectif est de trouver l'emplacement de l'accélérateur cryptographique AES. Afin de le localiser par détection synchrone, son activité est modulée en alternant des phases de chiffrement répétées et des phases d'inactivité. Les deux analyses sont menées à la fréquence $f_{lockin} = 1\,Hz$.

Le premier circuit est le SoC Exynos 4412, fabriqué en technologie 32 nm et monté sur une carte mère de *smartphone*. Le CPU principal du circuit fonctionne à $1,4\,GHz$ et son accélérateur cryptographique à $200\,MHz$. De manière à faciliter la cartographie du circuit, ce dernier a été décapsulé. L'acquisition thermique se fait donc directement au contact du silicium en face arrière.

Une fois la manipulation terminée, les images d'amplitude et de phase obtenues sont masquées grâce au test de KS et sont superposées au *layout* du circuit. Ces résultats sont présentés fig. 8. On peut notamment constater l'apparition de deux sources de chaleur. L'image de phase permet de déterminer que seule la source thermique de gauche est issue du coprocesseur cryptographique puisqu'il s'agit de l'unique activité en phase avec la modulation ($\Phi < 180°$). La seconde activité thermique observée correspond à un des cœurs du CPU principal. Ce dernier réalise des lectures répétées sur un registre de *timer* permettant de gérer l'ordonnancement de la modulation thermique.

Le second circuit cartographié est le Kirin 620, lui aussi un processeur de *smartphone* fabriqué en technologie 28 nm. L'échantillon étudié est cependant monté sur

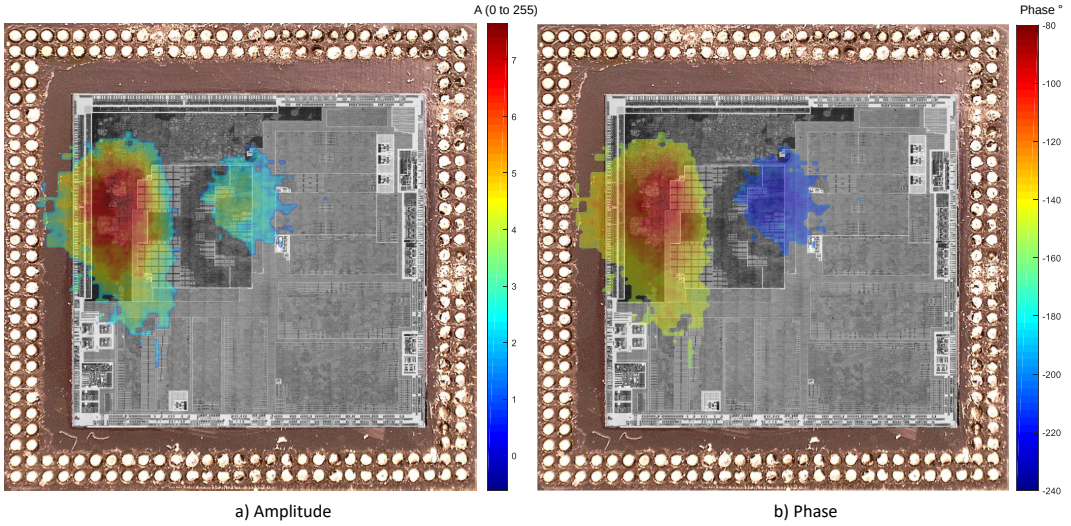


FIGURE 8: Analyse thermique synchrone de l'accélérateur cryptographique de l'Exynos 4412 à 1 Hz. Le résultat obtenue est masqué puis superposé au "layout" du circuit.

un circuit imprimé (PCB) d'étude, facilitant l'utilisation des ports de sortie (GPIO). Pour cette analyse, le circuit n'est pas décapsulé et l'image thermique du composant est acquise directement au dessus du boîtier époxy.

Les cartographies thermiques du Kirin 620 sont présentées fig. 9. Cette fois, les images thermiques ne laissent apparaître que l'emplacement du périphérique de chiffrement. La traversée des multiples couches constituant le boitier du circuit permet à la chaleur de se diffuser davantage latéralement. La consommation du bloc AES étant largement supérieure à celle du cœur dans ce cas précis, seule cette première apparaît sur l'image finale.

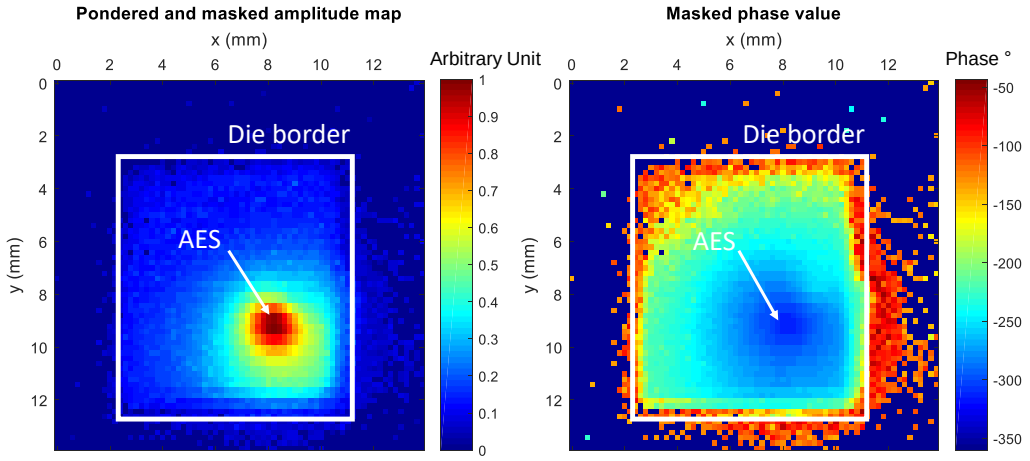


FIGURE 9: Analyse thermique synchrone de l'accélérateur cryptographique du Kirin 620 à 1 Hz.

Le fait d'avoir utilisé une fréquence de *lock-in* si faible permet, en outre, de repérer les dimensions exactes de la puce silicium au sein du boîtier époxy. La chaleur se diffusant plus rapidement dans le silicium que dans l'époxy, la puce apparaît par transparence sur les cartographies de phase et d'amplitude.

Une fréquence d'analyse plus élevée (10 Hz) permet de visualiser l'activité du cœur de calcul, déphasée de celle de l'AES, similairement aux résultats présentés en fig. 8. La position du circuit silicium dans le boîtier n'est en revanche plus visible.

5 Méthode de Comparaison de carte Thermiques

La comparaison de deux cartes est un outil efficace pour localiser de petites variations dans le comportement du circuit. Cela peut être appliqué à l'analyse de défaillances ou à la recherche de chevaux de Troie par exemple. Cependant, afin que les variations identifiées soient significatives, plusieurs critères de mesures doivent être validés. En particulier, l'invariance du procédé de fabrication (*process*), de la tension d'alimentation (*voltage*) et de la température (PVT) sont des propriétés cruciales pour la comparaison d'images thermiques. Elle permet notamment de certifier qu'une même valeur d'amplitude (ou de phase), mesurée sur différents circuits, correspond à la même activité thermique.

5.1 Sensibilité des Mesures Infrarouges aux Variations PVT

La mesure d'amplitude peut être tout de suite écartée de la notion d'insensibilité PVT. En effet, celle-ci dépend de l'émissivité des matériaux et est liée à la température à la puissance quatre par la loi de Stefan-Boltzman:

$$E_b(T) = \sigma \cdot T^4 \tag{14}$$

La valeur d'amplitude est donc susceptible de varier fortement en fonction du procédé, de la tension et de la température.

À condition d'utiliser le *clock gating* comme technique de modulation, il est prouvé que les mesures de phase sont théoriquement indépendantes des variations PVT. En pratique, une dépendance à la température peut-être remarquée. Cependant, sans la possibilité de pouvoir réguler la température du laboratoire précisément, il est impossible de déterminer si cette dépendance provient d'un lien physique entre la température et la phase ou des équipements de mesure. Néanmoins, ce résultat permet de comparer des cartographies thermiques tout en minimisant l'apparition de faux positifs.

5.2 Méthode de Comparaison des Images Thermiques

La méthode de comparaison proposée ici comprend quatre étapes.

- **Acquisition** : il s'agit ici d'acquérir les données expérimentales. Les deux circuits à comparer sont donc cartographiés par analyse thermique synchrone.
- **Alignement** : les variations et dérives de procédés durant l'étape de mise en boîtier du circuit rendent cette étape obligatoire de manière à ce que les pixels comparés correspondent au même positionnement sur le circuit. De plus, si les cartographies sont acquises de façon séquentielle, il est nécessaire de retirer le premier circuit pour cartographier le second. Ce déplacement génère lui aussi des erreurs d'alignement.

  Pour compenser cela, il est proposé de réaliser un alignement automatique en utilisant le t-test de Welch comme métrique. Concrètement, le test s'applique pixel à pixel entre les deux images. Les scores obtenus sont alors sommés pour obtenir le score d'alignement. Une des images est ensuite décalée d'un pixel horizontalement ou verticalement. La position fournissant le score d'alignement le plus faible correspond à la position où les deux images sont alignées.

  Une fois cette étape réalisée, une erreur résiduelle peut être constatée. Celle-ci est due à la correction d'alignement, appliquée au pixel près. Un décalage inférieur à la taille d'un pixel ne saurait être compensé par cette méthode. De plus, le défaut d'alignement en rotation n'est pas corrigé.
- **Comparaison - cas général** : la comparaison pixel à pixel engendre l'apparition de nombreux faux positifs, rendant l'interprétation du résultat difficile. Pour cette raison, il est proposé de comparer des groupes de pixels.

  Ainsi, la densité de pixel rejetant l'hypothèse H_0 du t-test effectué pour l'alignement fournit la probabilité d'avoir mesuré un comportement thermique déviant. Cette probabilité suit une loi binomiale dont la distribution peut être calculée théoriquement. Un test de KS permet ensuite de déterminer si les deux distributions sont similaires. Lorsque la distribution expérimentale est déclarée différente de la distribution théorique au sens du test KS, une anomalie est détectée.
- **Comparaison - cas du capteur mono pixel** : dans le cas d'un capteur mono pixel, l'erreur de déplacement du banc motorisé vient s'ajouter à celle de l'étape d'alignement. Pour cette raison une méthode dite de *fingerprinting* est appliquée.

  Celle-ci consiste à remplacer la distribution théorique par une distribution empirique de référence contenant elle aussi l'erreur de déplacement. Cette distribution est construite en cartographiant N circuits différents ou N fois le même

circuit de référence. Dans le cas où le même circuit est utilisé, ce dernier doit être enlevé puis replacé pour que l'erreur d'alignement soit significative. En utilisant le niveau de confiance du test KS, des limites haute et basse (B_{ref}^{low} et B_{ref}^{high}) permettent de définir une zone de fonctionnement nominale. Tout dépassement de cette zone par la fonction de répartition expérimentale du circuit étudié indique une déviance significative de son comportement thermique.

5.3 Application à la Recherche de Variation de Signature Thermique

Dans cette section, la méthode présentée précédemment est appliquée à la recherche de défaillance ainsi qu'à la localisation de chevaux de Troie matériels. En particulier, il est montré que l'addition ou la soustraction d'une source de chaleur non visible par l'analyse classique peut être détectée par la méthode de comparaison proposée. Le capteur utilisé est mono-pixel (cf. section 4 Banc de Mesure). La comparaison utilisant le *fingerprinting* est donc mise en œuvre.

Analyse de Défaillance

Une défaillance électrique au sein d'un circuit ou l'un de ses périphériques engendre automatiquement une modification de son comportement thermique, que ce soit par l'ajout (court-circuit) ou la soustraction (périphérique inactif, sortie logique "collée") d'une source. Même si le *clock gating* permet de sélectionner le périphérique à moduler thermiquement, la localisation du problème au sein de ce dernier reste difficile à cause de la diffusion de la chaleur.

Pour émuler ce problème, plusieurs oscillateurs en anneau ont été juxtaposés au circuit AES présenté précédemment. Deux cas sont étudiés avec des consommations de $800\,\mu W$ et $3,2\,mW$ alors que le circuit de chiffrement consomme environ $80\,mW$.

Les résultats de comparaison sont présentés fig. 10. On voit ici que si l'impact thermique des oscillateurs n'est pas détecté sur une cartographie classique, elle est en revanche parfaitement localisée par comparaison des images thermiques.

Ces résultats montrent un cas particulier de la détection en comparant le circuit défectueux à un circuit de référence donné. La fig. 11 donne le graphe des fonctions de répartition des mesures obtenues en réalisant la méthode du *fingerprinting*. La référence est construite en utilisant les mesures acquises sur six circuits. On voit ainsi que les fonctions de répartition correspondant aux CI où les oscillateurs ont été ajoutés sortent de la zone de fonctionnement nominale définies par $B_{ref}^{low}(u)$ et $B_{ref}^{high}(u)$.

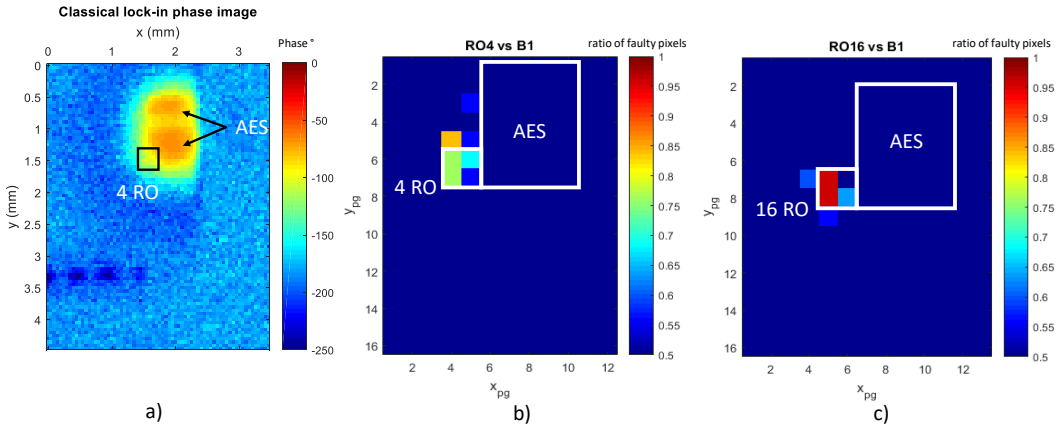


FIGURE 10: Émulation d'un périphérique défectueux générant une source de chaleur additionnelle (oscillateurs en anneau) **a)** Image "lock-in" classique **b)** Détection de la consommation additionnelle de 4 oscillateurs **c)** Détection de la consommation additionnelle de 16 oscillateurs.

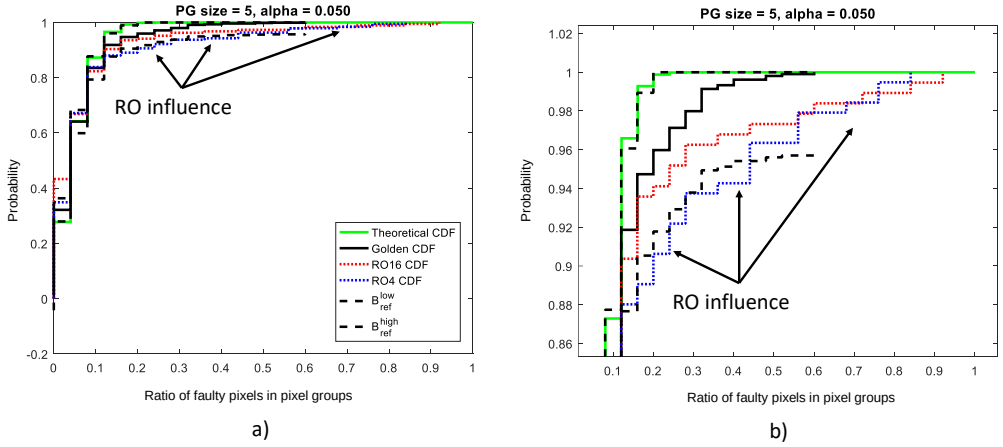


FIGURE 11: **a)** Application du *fingerprinting* pour l'analyse de défaillance **b)** Zoom sur la partie supérieure du graphe a).

Recherche de Chevaux de Troie

L'insertion d'un cheval de Troie matériel se caractérise par la modification d'un ou plusieurs éléments sur le circuit dans un objectif malveillant. Ainsi, la consommation électrique et donc sa signature thermique sont modifiées. L'exemple suivant montre la détection d'un cheval de Troie matériel servant à faire fuir certains octets d'une clé secrète utilisée au sein d'un circuit AES. Les résultats de localisation de l'infection sont présentés fig. 12.

Similairement à l'étude de défaillance précédente, le *fingerprinting* est aussi appliqué dans ce scénario. Ici aussi, on note que les fonctions de répartition correspondant aux circuits infectés traversent les limites du comportement thermique nominal du circuit. Cela indique ainsi la présence d'une fonction malveillante au sein de ce dernier.

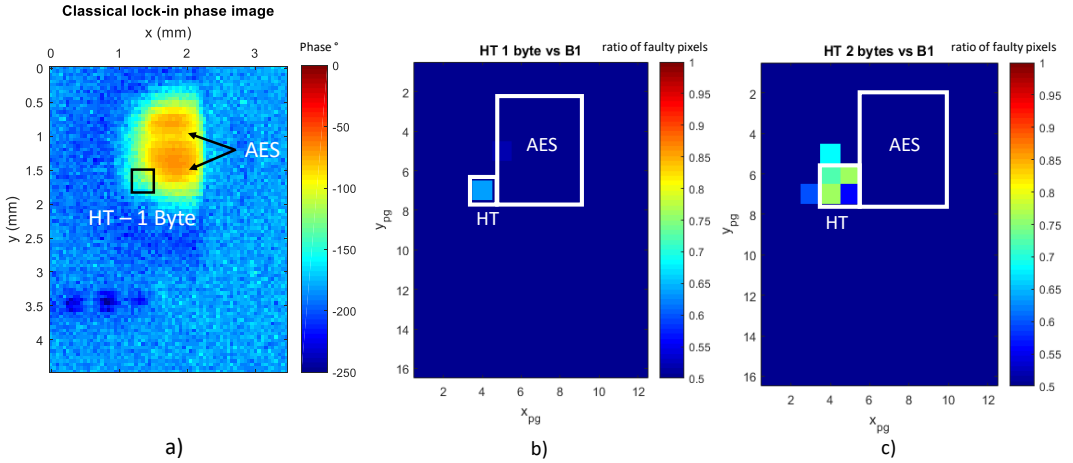


FIGURE 12: Émulation d'un cheval de Troie matériel sur un FPGA Virtex 5 **a)** Image *lock-in* classique **b)** Cheval de Troie laissant fuir un octet de clé **c)** Cheval de Troie laissant fuir deux octets de clé.

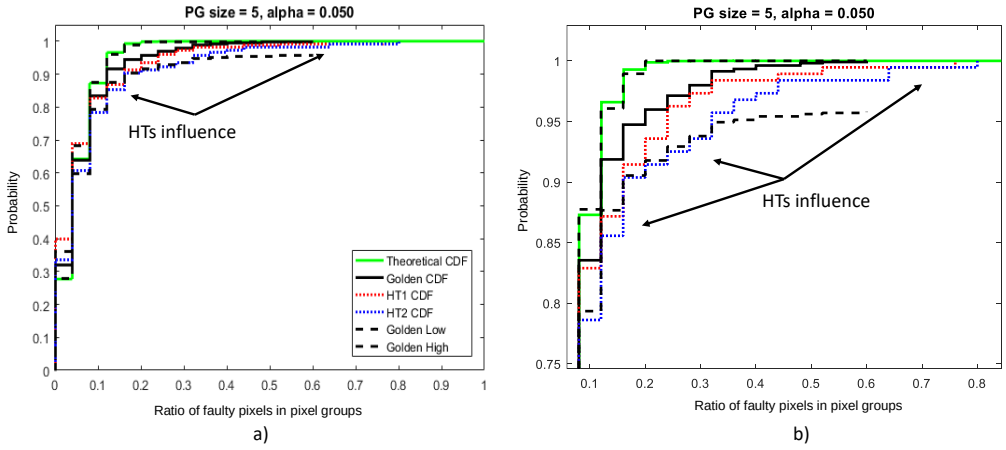


FIGURE 13: **a)** Application du *fingerprinting* pour la détection de chevaux de Troie **b)** Zoom sur la partie supérieure du graphe a).

6 Conclusion

L'imagerie thermique représente un moyen efficace pour cartographier un circuit thermiquement. En particulier, la détection synchrone (*lock-in*) permet de mesurer des signaux extrêmement faibles. L'étude thermique de circuits basse consommation comme les SoC embarqués peut ainsi être envisagée.

L'étude de la répartition statistique des valeurs de phase en présence et en absence de signal a permis de mettre en place un critère de mise en évidence des zones actives du circuit. En effet, il a été démontré que la distribution statistique de la phase est uniforme lorsque qu'aucun signal IR n'est détecté à f_{lockin}. En revanche, cette dernière devient normale lorsque le capteur est placé au dessus d'une source

thermique modulée. Ce procédé d'identification permet ainsi d'affranchir les cartographies thermiques de l'interprétation subjective de l'opérateur. Une application sur des SoCs Exynos et Kirin est finalement proposée avec la localisation de leur accélérateur cryptographique.

Par ailleurs, l'invariance en PVT des valeurs de phase permet la comparaison des images thermiques entre elles. Ainsi, de très faibles variations dans la consommation des circuits peuvent être identifiées pour la localisation de défauts dans les circuits ou la détection de chevaux de Troie.

Le banc de mesure présenté restant une preuve de concept, les performances sont loin d'être optimales. Il est cependant démontré que ce banc possède la capacité de pouvoir détecter des consommations de l'ordre de $200\,\mu A$. En particulier, le remplacement des optiques "artisanales" pourrait grandement améliorer la qualité du signal IR mesuré et donc des performances de la plateforme. Enfin, il serait intéressant de poursuivre l'analyse sur les longueurs d'ondes du proche infrarouge, où le silicium possède une meilleure émissivité. En outre, les capteurs photovoltaïques InGaAs possèdent une détectivité environ cent fois plus élevée sans être refroidis. L'imagerie thermique faible coût peut ainsi devenir un outil puissant pour guider des attaques par canaux cachés ou par injection de fautes.

Chapter 1

General Introduction

1.1 Security and Trust for IC

Today, integrated circuits are key components to every day objects and infrastructures. They can be found in most sectors of human activity such as economy, entertainment, medical, or military. Among these domains, many of them represent critical systems (military, finance, etc.). There is thus a high need to ensure the security of these electronic devices and their data against malicious attackers.

To be considered secured, a set of data (or an electronic chip) must fulfil at least three criteria:

- **authenticity and non repudiation**: data (or ICs) are what they should be and cannot be replaced nor denied;
- **integrity**: the data (or ICs) have not been modified and are genuine;
- **confidentiality**: data are not readable nor exploitable by attackers;

Encryption is a methodology that scrambles the information according to a secret key in order to render it unreadable to attackers. It is well known that the majority of secured systems rely on encryption whether it is symmetric (both communicating ends know the secret key) or asymmetric (encryption and decryption are done with two different keys).

Current ciphering algorithms (AES for example) remain mathematically unbroken. However, numerous researches demonstrate that if the algorithm is theoretically secured, the electronic devices implementing the encryption functions constitute easy targets if naively implemented. In the absence of countermeasures, a

large panel of hardware attacks are susceptible to compromise the authenticity, the integrity, or the confidentiality of the data.

These attacks are generally sorted into two main categories: non invasive attacks and invasive attacks. The first one regroups attacks that leave the circuit unmodified and functional once the attack has been performed. Semi-invasive methodologies also exist, where the die requires to be modified (decapsulation, substrate thinning, etc), but remains operational post analysis.

Side-channel (SCA) and fault injection (FIA) attacks are a good example of non invasive or semi invasive attacks. SCA consist in exploiting physical consequences of the nominal operation of the die that are linked to the handled data. Therefore, the development of countermeasures is difficult as the analyzed parameter (the side channel) cannot be suppressed. For example, one can analyze the electromagnetic (EM) radiations of an electronic circuit which is an image of its power consumption. By correlating these measurements to a power consumption model, it is possible to retrieve the secret key and compromise the data or the circuit [dBWGS11]. Photonic measurements also proved to be efficient by allowing the read of a memory content bit by bit [SNK+12].

FIA are disruptive actions that lead to the modification of the handled data. The aim of this operation is to break the pure randomness that is critical for efficient and secured encryption. Thereafter, mathematical processes and statistics allow to retrieve the secret key. Classical means for fault injection are EM pulses, laser pulses or power supply disruptions [DDRT12, VWWM11]. However, these methodologies present a higher risk of damaging the circuit than SC attacks.

Hardware security is often considered for sensitive data but can also be applied to electronic devices. Intellectual property (IP) is an example that illustrates this issue. Reverse engineering methodologies can reveal the internal composition or the layout of a circuit, allowing an attacker to improve an existing attack or simply profit from counterfeited dies. These attacks usually rely on techniques such as EM or thermal imaging. Because this thematic is central to the work presented in this document, further details on classical imaging techniques are provided in chapter 2.

In comparison, invasive attacks require to modify or break the circuit to extract the secret whether it is a secret key or an IP. The most common example is the scanning electron microscopy of each layer of an IC that provides a detailed image of the internal structure of the circuit. An example of such attack is presented in [TJ09], where a pixel array is imaged at the polysilicon level. In this work, transistors, their dimensions, and the layout of the circuit appear clearly.

Another type of invasive attack consists in modifying the circuit during its design or its manufacture. This type of attack is known as the hardware Trojan horse

(HTH) insertion. The objectives of such attack can be various (denial of service, data leakage, performances degradation, etc) and can happen at almost every stage of the circuit manufacture. The speculative nature of such attack makes the development of efficient countermeasures very difficult. Therefore, the detection of infected circuit relies more on complementary methodologies and design strategies rather than on a single detection technique.

It is thus clear that the security of electronic devices can be breached in many ways. In the next section, the perspective of the achieved work is presented. Current problematics of hardware attacks are exposed as well as the proposed solutions.

1.2 Perspective of the Thesis

1.2.1 IC imaging

Nowadays, hardware security relies on countermeasures established from a panel of known attacks of the state of the Art. These attacks are then ranked in function of their complexity, their cost, and their implementation time which helps defining the level of security of an IC. Therefore, new attacks are continuously designed to improve the security of the latest IC.

Originally, most of these attacks targeted smartcard devices as they are widely commercialized, involved in sensitive domains (e.g. finance), and have relatively simple architectures. Typically, the die surface of these devices is of 1 or 2 mm^2. This makes the placement of laser beams or EM probes relatively easy, as the surface to explore to find the secured elements is limited. However, modern SoCs and FPGAs can have die areas over 100 mm^2 which severely increases the positioning difficulty, considering the size of a laser beam ($\sim \mu m$) or a EM probe ($\sim 100 \mu m$). A first step of reverse engineering is therefore necessary to locate the targeted peripheral (e.g. AES crypto accelerator).

As later presented in chapter 2, many imaging techniques already exist. From the state of the art it is found that thermal analysis, and in particular infrared (IR) thermography, provides very interesting results as it is capable of sweeping large areas in a reasonable period of time. Additionally, contrarily to EM imaging, thermal activity is always found on top of the active part of the circuit.

IR lock-in thermography is a selective imaging technique that allows to select thermal emissions at a given frequency. Using clock gating, a specific peripheral of the circuit can then be thermally modulated. It is then possible to mathematically retrieve the amplitude and the phase of the measured signal, knowing only the modulation frequency. Originally applied to thermal camera measurements, this

technique is adapted to a mono-pixel sensor that scans the surface of the die using motorized axes. This way, measurements benefit from high sampling speed of modern digital sampling oscilloscopes (DSO) and provide very high phase resolution.

Despite the variety of existing imaging techniques, they rely, most of the time, on human interpretation to localize electronic activity. Therefore, information and small nuances are susceptible to be lost due to poor resolution or poor contrast. Here, based on the lock-in thermography technique, it is proposed to apply statistical treatments to thermal images to automatically identify areas of interest. In particular, it is demonstrated that the phase variance of thermal signals is a massive indicator of the presence of thermal activity. Statistical tests on thermal measurement distributions can therefore be applied and extract locations of electrical activities.

1.2.2 Comparison of IC Thermal Images

The main limitation of thermal imaging is often attributed to its limited spatial resolution. Due to the lateral thermal propagation within the die, the temperature distribution appears quite different than the power density one. While the power density can be represented by sharp geometric figures, the temperature distribution evolves smoothly. This is problematic as two close power sources may appear as a single one due to the diffusion effect.

The comparison of thermal maps can bring forward several differences that would remain concealed otherwise. In particular, in the case of an HT insertion, the modification of the layout of the circuit is expected to modify its nominal thermal behavior. Using a trusted thermal reference image (golden reference), it is possible to highlight small differences in thermal activity between the golden circuit and the device under test (DUT).

Lock-in amplitude measurements proved to be unadapted to such comparison because of its sensitivity to process, voltage and temperature (PVT) variations. However, under the condition of specific lock-in modulation, it is found that phase measurements provide a much more viable alternative. Thereby, the robustness of phase measurements to PVT variations is demonstrated theoretically and experimentally.

From the latter result, the work presented here then proposes a methodology to efficiently compare thermal maps. This methodology relies on an automated realignment procedure and on statistical analysis of the density of pixel failing the Welch's t-test. Because pixel to pixel comparison between the golden reference and the DUT would generate to many false positive, it is found that the study of pixel groups is far more efficient. The probability of detecting an anomaly is thus governed by a binomial law that can be theoretically modeled to determined if there is a deviance in the thermal behavior of the DUT.

The proposed methodology is generic and is compatible with other measurement strategies (e.g. cameras) as long as they follow the lock-in modulation requirement leading to PVT robustness. Such methodology can therefore be applied in various applications such as HT insertion identification or failure analysis (FA).

1.2.3 Contribution of the Thesis

The contribution of this work are the following:

- design of a fully characterized cost effective IR scanning platform based on single pixel sensors;
- identification of a statistical criterion to sort non thermally active areas from active ones;
- implementation of an automated thermal localization feature based on statistical analysis of thermal images;
- application to reverse engineering on SoCs and FPGAs;
- demonstration of the PVT robustness of lock-in phase measurements theoretically and experimentally;
- definition of a generic thermal map comparison;
- application of the comparison methodology to FA and HT identification.

1.3 Structure of the Thesis

The structure of the document is as follows:

Chapter 2

Chapter 2 starts by providing the state of the art in IC imaging techniques. In this state of the art, pros and cons of each technique are related and the choice of pursuing research on thermal imaging is justified.

Following, the theoretical aspect of IR emission from materials is detailed. This section thus justifies that IR light analysis is an adapted medium for thermal imaging of ICs. A concise state of the art on IR acquisition technologies is then provided. In particular, it shows that cooled InAs sensors represent the most reasonable compromise between size, bulk and price.

Finally, different existing strategies allowing thermal imaging are presented and compared. For the need of reverse engineering and low power thermal imaging, it is shown that IR lock-in thermography is by far better suited than steady state thermography. The choice to rely on this technique is therefore justified.

Chapter 3

Chapter 3 first describes the experimental set-up used to acquire the thermal images presented along this document. This IR measurement platform is composed of off-the-shelf components only and remains at a reasonable price compared to current IR cameras. The platform is then characterized to obtain measurements of its spatial resolution and its detection limits in terms of power consumption.

In a second part, examples of reverse engineering applications are proposed. For that, two different SoCs are analyzed, each time performing thermal analysis to locate the AES crypto-accelerator. While the first SoC is decapsulated (i.e. the package has been removed), the second SoC is analyzed through the package.

Chapter 4

Chapter 4 demonstrates theoretically and experimentally the weaknesses of lock-in amplitude and the robustness of lock-in phase toward PVT variations. Then, the comparison methodology is precisely detailed, step by step. Thereafter, two application examples are proposed. The first one focuses on detecting the insertion of a benchmarked HTH while the second one aims at detecting a faulty peripheral. In both cases it is shown that the abnormal activity could not be identified using classical thermal analysis. Experimental results however show that the comparison methodology is capable of detecting these small differences.

Chapter 5

Finally, chapter 5 concludes by recalling main contributions of the presented work and performances of the developed set-up.

Chapter 2

Thermal Investigation Of Integrated Circuits

In this chapter, basics of infrared thermography are presented. Following a brief state of the Art on integrated circuit imaging, the thermal emission mechanisms of ideal and real materials are presented. Then, the operation of several infrared sensors are explained. Their advantages and inconvenients are compared in order to choose the best suited detector for the application at hand. Finally, two methodologies regarding infrared measurements are detailed. The latter opposites DC measurements versus AC measurements with their pros and cons. It is hence explained how AC lock-in measurements allow to solve numerous issues related to DC infrared thermography.

2.1 Chapter Introduction

This chapter is an introduction to integrated circuits (IC) imaging. In particular, IR imaging techniques and methodologies are discussed. As shown along the chapter, integrated circuit imaging can rely on very various parameters. Indeed, each physical quantity influenced by the IC operation can theoretically be exploited to reveal information about its internal composition or its activity.

Due to the Joule effect, heat generation is one of the most intrinsic consequence of the operation of an electronic circuit. Spontaneous photon emissions from materials is closely linked to their temperature. Thus, IC thermal mapping appears as a straightforward research axis.

The study of thermal analysis state of the Art and more broadly of IC investigation, reveals that imaging techniques can be incredibly precise, allowing to map circuits down to the transistor level but at the price of very local measurements or

extremely time-consuming acquisitions (laser based methods, photonics, etc). Inversely, methods allowing fast investigation of the whole die, e.g. IR cameras, usually lack precision or detectivity.

To better understand the limitation of the existing systems, this chapter details available technologies allowing IR thermal analysis as well as the associated measurement strategies. Therefore, the chapter is structured as follows. First, the state of the Art concerning IC microscopy is presented. In particular, section 2.2 details imaging systems based on electromagnetic (EM) measurements, photon emission, laser, and thermal measurements . Then, section 2.3 describes the physical spontaneous photon emission of materials. From there, it is demonstrated that IR radiations are a particularly adapted medium for thermal IC investigation. Section 2.4 presents the state of the art concerning IR detectors. Performances, pros and cons of IR detection technologies are addressed. Then, two acquisition strategies for IR circuit imaging are presented. Finally, section 2.5 concludes on the established existing research concerning thermal and other IC investigation techniques.

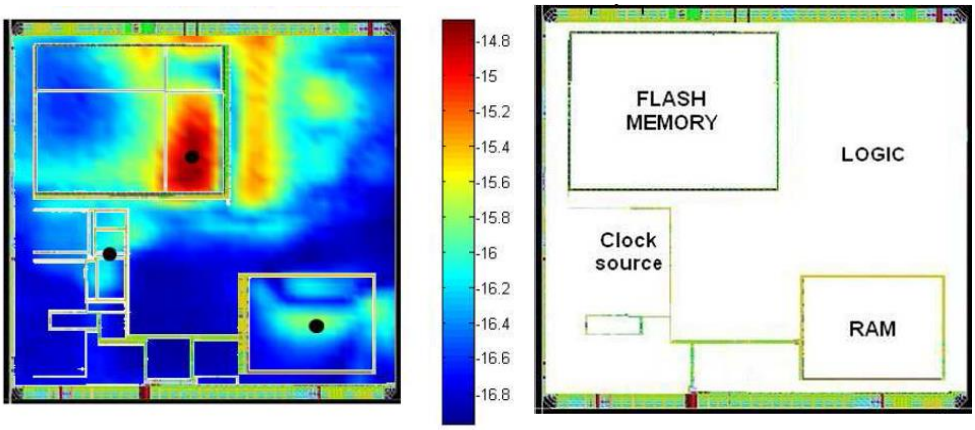
2.2 Investigation of Integrated Circuits

2.2.1 Electromagnetic Emission Imaging

Switching currents in electronic circuits produces electromagnetic emissions that can be measured and reveal the positioning of macro-blocks such as RAM, CPU or analog functions. In [OLS+09], authors establish that using low cost off the shelf components and with very few post treatment, one can retrieve quite easily the location of these macro-blocks. For that, the targeted circuit is scanned by a close field EM probe, acquiring one or multiple traces for each location. The integration of those traces then provides an image over time of the local switching current at a specific location. By representing spatially this switching activity on a color map, it is then possible to reconstruct activity areas of the circuit, each sample corresponding to a specific moment in time.

Fig 2.1 presents an activity map example where it is possible to identify active macro blocks on the die. On this figure, activity in the flash memory, the clock generator and the RAM are observed.

The work related in [PTL+11] shows that the coupling between an EM probe and the die is done through the power rails. To demonstrate this assertion, the authors map the circuit's response to EM fault injection (EMFI). The coupling of EM probes being bidirectional, this statement remains valid for EM analysis. The latter



a) Spectral density energy b) Floorplan of the circuit

FIGURE 2.1: EM cartography of a microcontroller by analysis of the spectral density for $f \in [1\ 1000]\ MHz$ [OLS+09].

phenomenon is however the source of one the main inconvenient of EM IC investigation as it shows that the EM emissions are global. Therefore, the locality of the measurements is not guaranteed and the acquired measurements are not necessarily an image of the activity under the probe. This problem was adressed in [LM19] and resolved at the price of heavy computation and longer acquisition times.

A second inconvenient inherent to the physics of EM emissions lies in the incapacity of EM analysis to detect sources having a constant power supply such as ring oscillators (RO) without disrupting its nominal operation. This issue is mentioned in [BBA+12] when authors aim at detecting ROs of true random number generators (TRNG) circuits to guide EMFI attacks on crypto-processors.

2.2.2 Body Bias Injection Imaging

Body biasing is a common technique for controlling process variations and static power dissipation in ICs. In [MTOL12] body bias injection is used as an alternative solution to laser fault injection (LFI) and EMFI for cryptographic circuit attacks. The aim of this attack is to shut down the power voltage and generate errors on the circuit. For that, a pulse is applied on the substrate of the circuit, generating parasitic currents that can be measured on the power supply rails. The total current generated by the pulse is susceptible to vary regarding the internal architecture, and especially regarding the integration density.

As a matter of fact, RAM memories, processing cores, and flash memories posses very different internal transistor structures and thus different integration densities of

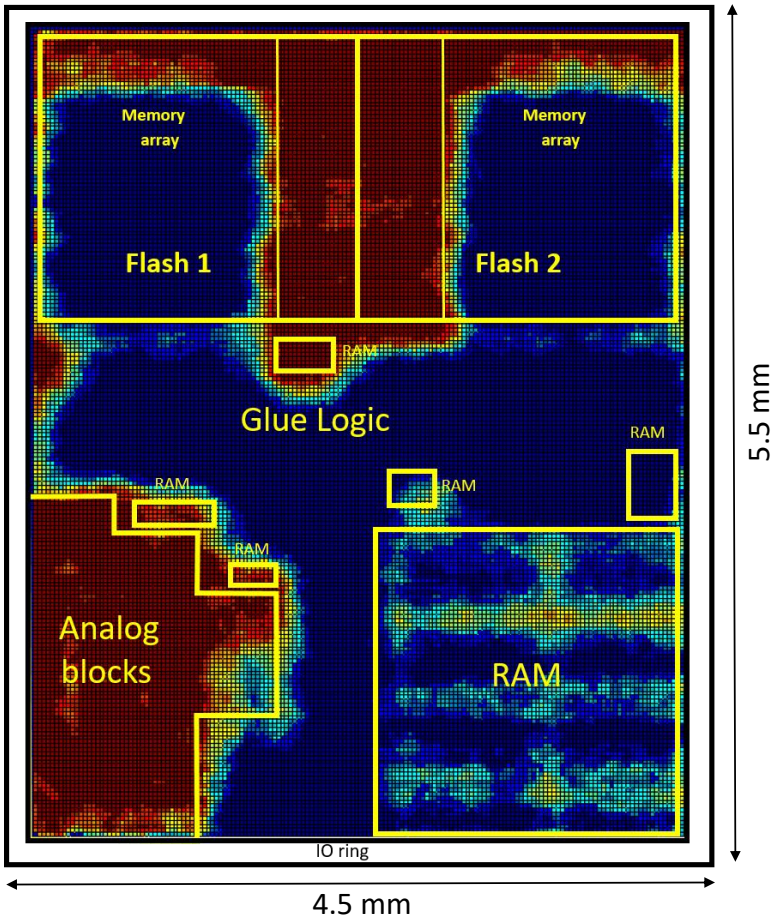


FIGURE 2.2: Analysis of VDD and GND currents when performing body bias injection at different locations of a micro-controller [MTOL12].

P^+ and N^+ contacts between the substrate and GND (respectively VDD). By pulse-mapping the device under test (DUT) while monitoring the power rails currents and voltages, it is then possible to identify macro blocks of a complex architecture such as a micro-controller. Figure 2.2 presents an example of such analysis. To facilitates the reading, the simplified floorplan of the chip is overlayed on the acquired measurement. On this image, blue locations represent low contact density areas such as memories. Inversely, red locations reveal areas where the density of contact is higher which is expected from memory controllers or analog blocks.

2.2.3 Photo-Emission Imaging

Photo-emission imaging consists in acquiring rare emissions of photons during transistors operations. Although several phenomenons can lead to photon emission, the most commonly exploited one is called hot carrier luminescence. In CMOS technology, when a carrier is transmitted through the transistor channel, it is accelerated due to the drain-source voltage. When reaching the pinch-off region, there

is a probability that the carrier's kinetic energy is released by a radiative transition, generating photons around the 1.1 μm wavelength [TFW07, SNK+12].

Originally, this technique was used for failure and defect analysis and thus relied on extremely expensive equipment. As an example, the starting price for an integrated Picosecond Imaging Circuit Analysis (PICA) system is around one million Euro. In 2012, [SNK+12] proved that photonic analysis was possible for the equivalent price of a mid range oscilloscope. Using a $-70°$K cooled CCD sensor, they show their ability to read the content of the S-box memory from an Advanced Encryption Standard (AES) algorithm. This result is presented fig. 2.3 where a memory word is decoded directly from the photonic measurements.

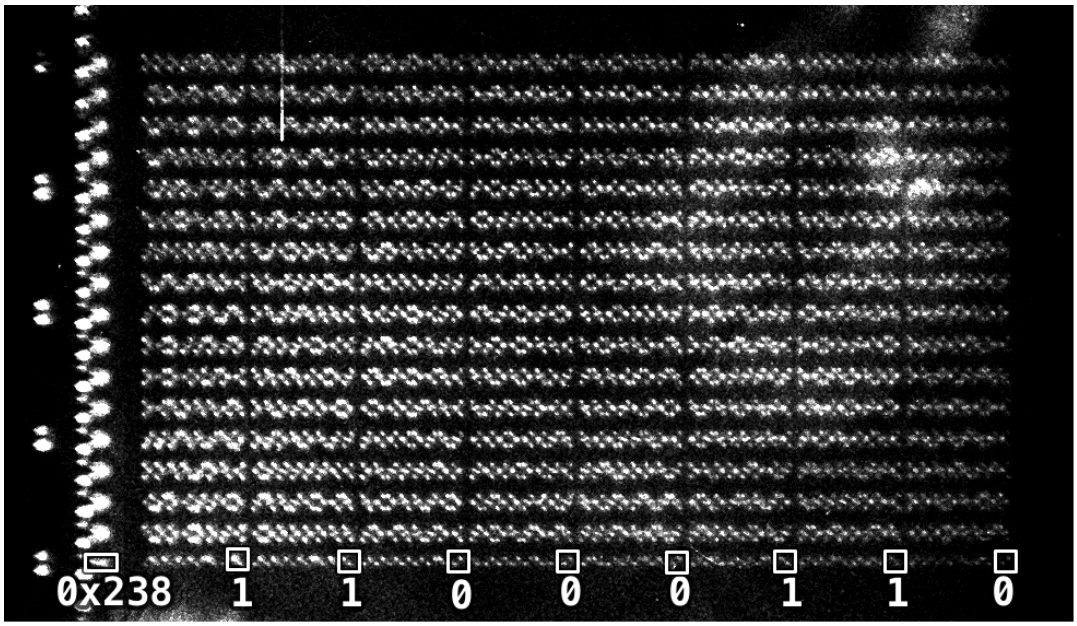


FIGURE 2.3: SRAM content from an AES S-box of an ATmega328p using photonic microscopy [SNK+12].

However, front side analysis of dies is limited by the density of metal layers of modern circuit, preventing the photons from reaching the sensor. Thus backside analysis is mandatory but suffers from photon absorption for wavelengths shorter than the energy bandgap of silicon. The substrate must therefore be mechanically thinned. In order to be investigated, a die must go through meticulous preparation in order to remove the packaging (decapsulate) and thin its substrate. This process constitutes the main weakness of the technique as it is costly, time consuming and presents a significant probability of damaging the die.

2.2.4 Laser Voltage Imaging and Probing

Laser voltage imaging (LVI) is an extension of the laser voltage probing (LVP) technique, developed for debug and characterization of ICs by allowing the extraction of a signal from the backside of a DUT. The LVI technique relies on the interaction of a laser beam and a transistor operating at a known frequency. When the laser beam reaches the toggling transistor, it is reflected, modulating both amplitude and phase at the transistor switching frequency [SNL+10]. The reflected light is then acquired using a photo detector and fed to a spectrum analyzer to compute the frequency modulation of the reflected light. Using this technique, it is therefore possible to map areas of identical frequency switching transistors. This technique is particularly appreciated in fault analysis as the measurement precision only depends on the spectrum analyzer performances and not on the measurement probe in itself. In comparison, LVP acquisitions require a triggered loop to average the output signal and achieve sufficient signal to noise ratio (SNR).

One strong advantage of this technique is that the precision of modern lasers makes it viable for transistor level investigations. In addition, LVI is a selective imaging technique which means that some operations of the DUT may be targeted specifically as long as the measured frequency difference is higher than the resolution of the spectrum analyzer. Fig. 2.4 illustrates this principle by comparing a layout transistor representation obtained by classical laser microscopy (on the left) and the image acquired using LVI (on the right). In this experiment, some of the transistors are clocked at a different frequency than the one of interest. Both images show similar results for transistors toggled at the investigated frequency. Classical laser imaging shows every transistors without any distinctions while LVI allows the targeting of transistors operating at the frequency of interest only.

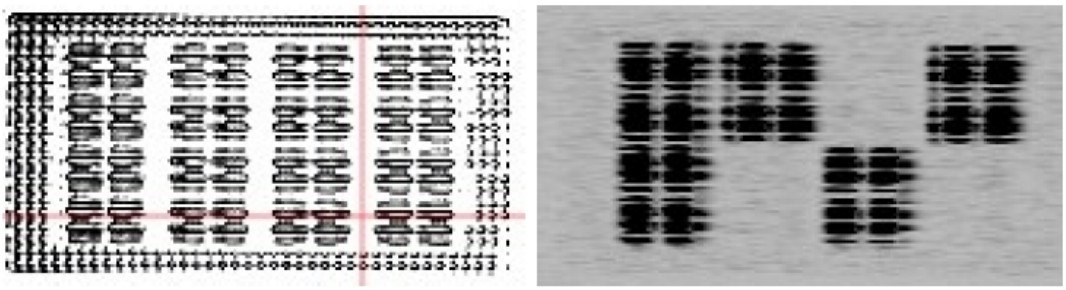


FIGURE 2.4: Detection of active transistors using LVI technique [SNL+10].

While being mostly employed for the identification of defective transistors in RAM or gluelogic, the work in [TLSB16] shows that LVI is also an incredible tool for secret extraction and reverse engineering purposes. Here, the authors aim at attacking the key generation mechanism of a secured circuit. In this case, the final key (red key in fig 2.5) is computed from an encrypted "black key" which is useless

as is for an attacker. The red key is then obtained by xor operation of the black key and a physical unclonable function (PUF) generated key.

To implement LVI, the operation frequency is artificially set by forcing hardware resets at 50 MHz to the DUT. Registers being initialized at a zero value, many bits are then switched to one when the chip reboots, thus ensuring a constant toggle at the hardware reset frequency. LVI is then applied to the registers containing data used for the key generation.

Fig. 2.5 shows that performing LVI on the registers containing the black key and the PUF key allows to read directly their content on the obtained image and thus to disclose the red key. For the demonstration purposes the red key register is also imaged in order to verify the final value obtained by the attacker. First an overview is presented by mapping the region containing the three critical registers (fig. 2.5. a). To be able to read easily their content, detailed images are later realized (fig. 2.5. b). Experimental results show that in each case, measured register values are equal to the configuration value. Therefore the red key can be retrieved by the attacker.

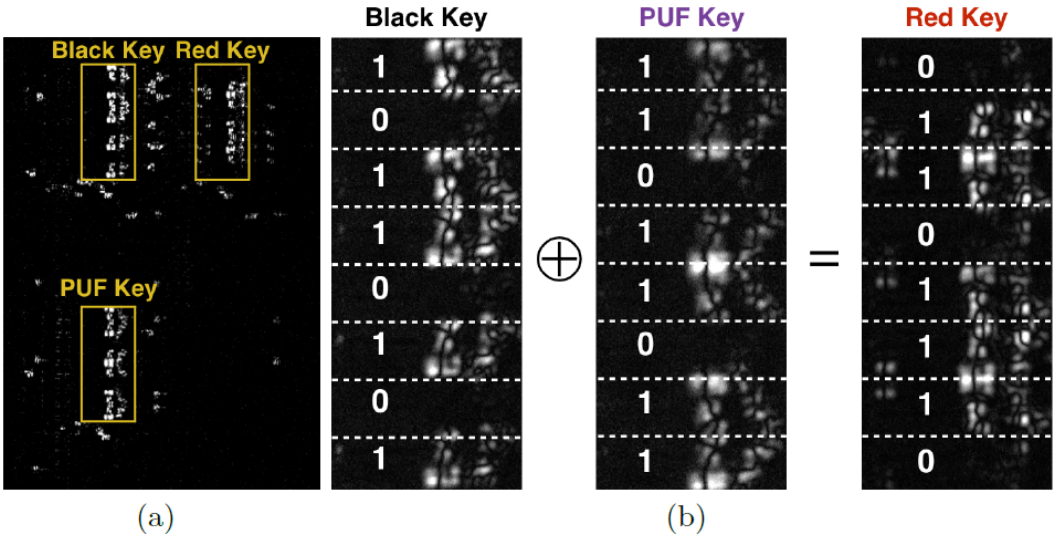


FIGURE 2.5: **a)** Critical register overview using LVI **b)** Detailed image of the critical registers and their values [TLSB16].

However, this technique is efficient in case the area of interest, which is of the $10\mu m^2$ order of magnitude, is known beforehand. Otherwise, the die size of modern SoCs and FPGA may become problematic as the experimental time acquisition becomes quite long. In addition, the price of the necessary equipment may also limit the application of the LVI technique.

2.2.5 Thermal Imaging

Thermal imaging of ICs is based on identifying areas of activity from local temperature gradients. Because of the Joule effect, a local temperature difference is synonym of a higher power consumption in the investigated area and thus of an electrical activity. By establishing a map of local temperature and correlating it to the known behavior of the circuit it is then possible to identify active parts.

Temperature measurements can be performed through a very wide panel of tools. One of the oldest technique regarding temperature measurement is contact thermometry. This technique uses a probe where the tip is applied to the surface of the DUT [LY07]. A very localized heat transfer then happens, between the circuit and the probe. When a local equilibrium is reached, the thermal measurement is saved and the probe moves to the next location to be measured. By scanning the whole die, a thermal map can then be built. According to [Maj99, MLC+95] lateral resolution down to 100 nm can be achieved depending on the contact area of the probe, the heat transfer mechanism and the design of the probe. The lateral resolution of this technique largely exceeds optical measurements ones but suffers from numerous drawbacks making the latter more suitable for IC investigation. First, measurement values highly depend on the force applied by the tip of the probe on the sample. For coherent measurements, this force must remain constant and thus must be precisely controlled. Also, this technique is temporally inaccurate as thermal equilibrium between the probe and the sample must be reached before each measurement. Finally, repetitive measurements may damage the sample and the probe due to the repeated contact of a sharp probe tip on the die's substrate. This is rather inconvenient, especially for hardware security, where imaging is often performed on a very restrained sample size.

Alternatively contactless methods relying on optical detection are reviewed in [LY07]. In particular, infrared imaging (IR) has been of great interest since the silicon is transparent to wavelength above 1.1 μm. However this property tends to vary with the doping concentration and often requires silicon substrates to be thinned when using these techniques.

Optical imaging techniques can be active or passive. Thermoreflectance, which is an active technique, uses the temperature dependent reflective property of materials. When applying an incident IR light to the DUT, the reflected light's intensity is modulated by the heat generated in the circuit. The reflected light is captured using an IR camera or a photodiode and allows the localization of heat sources on the die.

In [TBB+07], authors use this method to investigate temperature and power dissipation of metal layers in ICs. While a submicron spatial resolution is reached, there is no mention of the temporal resolution. Fig. 2.6 presents a thermal image of a gold

resistor investigated in [TBB+07]. The resistor dissipates 609 mW, a quite high value

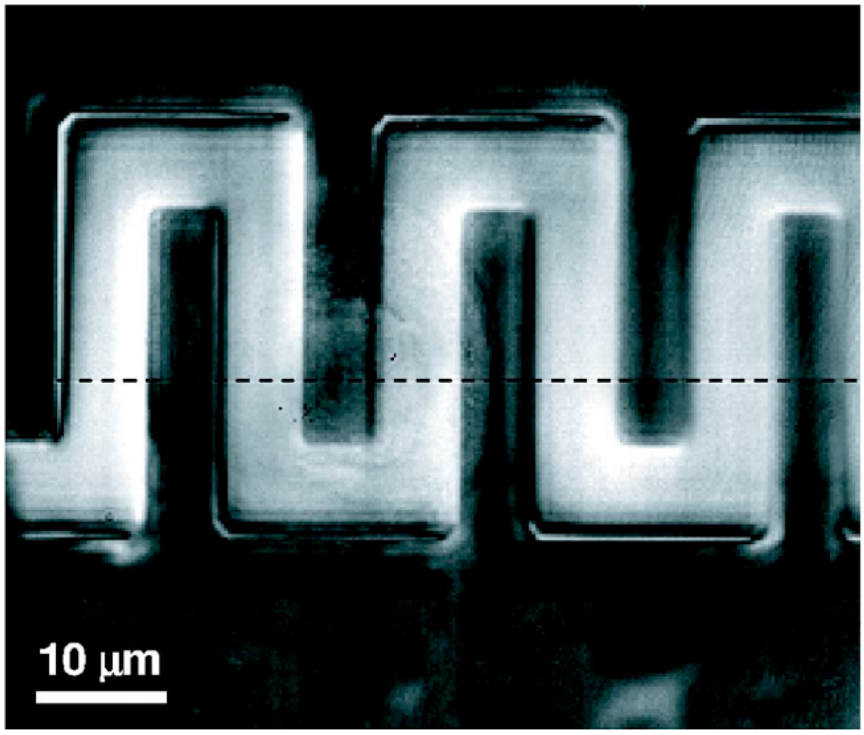


FIGURE 2.6: Thermoreflectance image of a gold resistor through a 500 μm silicon substrate [TBB+07].

and is imaged through 500 μm of silicon substrate.

The work presented in [KBR06a] combines thermoreflectance with pulsed probing light and pulsed bias of the circuit. The analysis is performed from the decapsulated front side of the DUT and can therefore rely on a light source of smaller wavelength than 1.1 μm to improve the spatial resolution. By progressively desynchronizing those two pulses, this technique allows visualizing the heat flow paths and identifying areas of high power consumption. The technique is then applied for the detection of latchup areas in ICs.

Due to the very small variation of the reflection coefficient regarding temperature, thermoreflectance is limited to high power investigations with heat sources consuming several hundreds of milliamperes. In addition, active thermography usually envolves costly equipment such as lasers and synchronization equipment [KBR06a, KBR06b].

For these reasons, the research presented in this thesis is orientated toward passive IR thermography. This imaging technique relies on spontaneous light emission properties of materials. The rest of this chapter describes physical mechanisms of light emissions in materials, the state of the Art infrared detectors and different strategies for the acquisition of thermal IR emissions.

2.3 Thermal Infrared Emissions of Materials

2.3.1 Black Bodies

Planck's Law

A black body (BB) is an entity considered as a perfect radiator and absorber of energy at all wavelengths. This means that the absorbed energy is fully re-emitted without any losses. Such entity is of course theoretical and is used to model property of real bodies when studying light radiations of materials. Planck's law, presented in eq. (2.1), gives the spectral distribution $I_b(\lambda, T)$ in $W.m^{-2}.sr^{-1}.Hz^{-1}$ of BB emissions where λ is the wavelength, c_0 is the speed of light in a vacuum, T is the temperature in Kelvin, h is the Planck constant, and k the Boltzmann constant [ID02a].

$$I_b(\lambda, T) = \frac{2.h.c_0^2.\lambda^{-5}}{e^{\frac{h.c_0}{k.\lambda.T}} - 1} \tag{2.1}$$

BBs are diffuse emitters. This term is used for any surface whose radiation intensity is independent of direction. In this case, the spectral, hemispherical emissive power, in $W.m^{-2}$, is:

$$E_b(\lambda, T) = \pi \cdot I_b(\lambda, T) \tag{2.2}$$

Figure 2.7 illustrates the emission process of BBs by plotting the evolution of the spectral emissive power $E_{\lambda,b}$ for different temperatures in function of the wavelength. From the latter figure, it appears that for each temperature, the spectral emissions of the BB possess a maximum for a specific wavelength λ_{max}. This phenomenon is described by Wien's diplacement law which states:

$$\lambda_{max} \cdot T = 2897.8\,\mu m.K \tag{2.3}$$

Those maxima are represented by the dash curve in fig. 2.7. The classical temperature operation of commercial silicon circuits ranges from $0°\,C$ to $+70°\,C$ (i.e. $273\,K$ to $343\,K$). Comparing these temperatures to the emissions of BBs in fig 2.7, shows that the wavelengths located in the $[2\,,15]\,\mu m$ interval are of particular interest for IC analysis. This interval corresponds to the mid/far IR spectrum and is one of the reasons that explain the success of IR investigation of ICs.

Performing the integration of eq. (2.2) over λ results in the Stefan-Boltzman law (eq. (2.4)). It states that the total emissive power $E_b(T)$ in W/m^2 is linearly linked to the fourth power of temperature T by the Stefan-Boltzmann constant $\sigma = 5.670.10^{-8}\,W.K^4.m^{-2}$. This constitutes an important result as it enables the calculation of the emitted hemispherical power over all wavelengths only knowing the

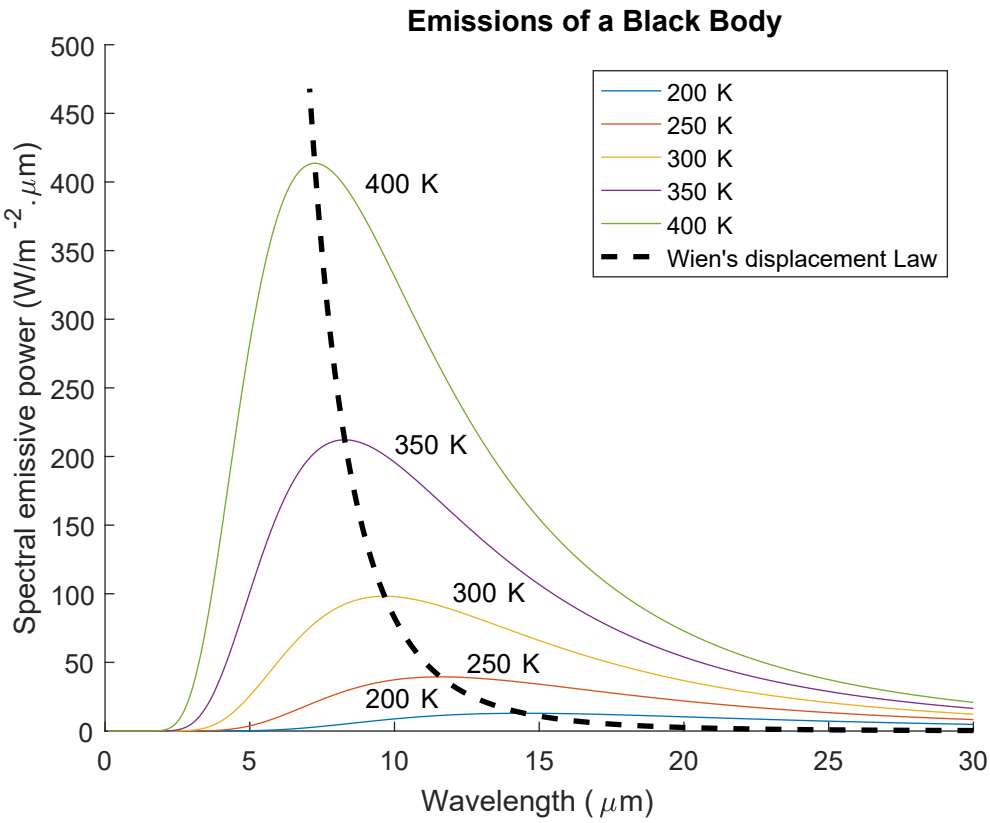


FIGURE 2.7: Relation of the spectral emission of a BB to temperature and wavelength.

temperature. Inversely, by measuring the radiated power of a body it is then possible to compute its temperature. The Stefan-Boltzman law is the core principle of IC thermal investigation.

$$E_b(T) = \sigma \cdot T^4 \tag{2.4}$$

The concept of total emissive power $E_b(T)$ from a surface can be extended to include radiations generated by emissions and reflections of other surfaces and is called irradiation [ID02a]. It is computed similarly to emissive power and in the case of a diffuse incident radiation I_i the irradiation $G(W/m^2)$ is defined by:

$$G = \pi \cdot I_i \tag{2.5}$$

2.3.2 Real Bodies

The spectral emissive power described in eq. (2.2) is the theoretical maximum of what a real body can emit. It can therefore be seen as a reference to characterize emissions of real bodies [ID02a]. In reality, the radiation behavior of a body is modulated by four optical parameters called emission, absorption, reflection and transmission.

Emissivity vs Absorptivity

The absorptivity, α, characterizes the ability of a material in absorbing incident radiations. It is defined by the ratio between the absorbed incident spectral intensity over the total incident spectral intensity. Like emissivity ϵ, this property is dependent on the directional distribution of the radiation and its wavelength. Considering a closed volume in thermal equilibrium with homogeneous optical properties, the energy absorbed must be equal to the radiated energy in order to respect the thermodynamic equilibrium. This is known as Kirchhoff's identity and states $\alpha = \epsilon$, α being the absorption and ϵ the emissivity.

To characterize real body emissions, emissivity is defined as the ratio between the emissive power $E(T)$ of the body itself and the emissive radiation of a BB. Thus emissivity can be seen as a weighting coefficient, which value is between 0 and 1, applied to the emitted power of the black body to obtain the power emitted by a real body. Equation (2.6) provides the expression of the total hemispherical emissivity:

$$\epsilon = \frac{E(T)}{E_b(T)} \tag{2.6}$$

It is important to note that the spectral radiation of a real body can differ quite largely from the Planck distribution and is often non continuous. In addition, the studied surface may not be considered as a diffuse emitter. Hence, the total hemispherical emissity presented in eq.(2.6) can be seen as an average over all directions and wavelengths. When investigating ICs, measurements can be realized in close field. If this is the case, the IR measurements over a diffuse surface and a non diffuse one should show very little difference. In other words, because the IR sensor is very close to the substrate, most of the power emitted from the surface is collected by the measurement platform, regardless of the direction it is emitted in.

Reflection ρ

This property describes the proportion of the incident radiation power that is reflected by the body. Similarly to the previous properties, the reflectivity, ρ, is defined by the ratio of reflected incident spectral irradiation, G_r, over the total incident spectral irradiation, G:

$$\rho = \frac{G_r}{G} \tag{2.7}$$

The reflective property can be quite constraining for bodies constituted of different layers of materials. In this case, one of the layer might possess a reflective layer at the wavelength of interest, preventing the acquisition of the sought out signal. For example, this is typically the case when performing IR thermography on ICs. The

latter are constituted of metal conductors layered on a silicon substrate. Metals being of a rather reflective nature, the acquisition of IR light from the front side of dies is therefore severely impaired.

Transmission τ

The transmissivity property translates the ability of light to pass through the studied material. Although this problem is often complicated by the treatment of the response of a semitransparent material [ID02a], an approximated value of the transmissivity can be obtained as follow:

$$\tau = \frac{G_t}{G} \tag{2.8}$$

G_t being the transmitted irradiation and G the total irradiation.

Radiation Balance

From the precedent optical properties, an incident radiation can be absorbed, reflected or transmitted. The sum of the reflected, absorbed and transmitted power are therefore equal to the power of the incident radiation :

$$\alpha + \rho + \tau = 1 \tag{2.9}$$

Consequently, for a black body, $\epsilon = \alpha = 1$ and $\rho = \tau = 0$. While other bodies have $\epsilon < 1$, a "grey body" is defined as a material having a wavelength independent emissivity. Likewise, if the emissivity is strongly linked to wavelength, e.g. silicon, it is called "selective emitter" [BWL10b, ID02a].

Infrared and silicon investigation

The Planck law given in eq. (2.1) and its graphical representation fig. 2.7, show that for ambient temperatures the emission maximum of a black body is around $\lambda = 10\,\mu m$ and thus in the mid-IR spectrum. Therefore IR seems to be well adapted to investigate dynamic consumption of ICs. However, real optical properties of silicon are such that it is transparent to IR light for wavelengths greater than $1.1\,\mu m$. Theoretically, this renders the investigation of silicon substrates impossible using IR light as very few photons would be emitted from the DUT.

Nonetheless bare silicon is rarely used in IC manufacturing. To be usable for such application it is primarily doped with specific atoms in order to increase the

concentration of carriers (electrons and holes). This process has considerable effects on the optical properties of silicon.

The work related in [SCMR99] shows that, at 300°K and for $\lambda > 1.1\,\mu m$, low-doped silicon with a carrier concentration of $1.10^{16} atoms/cm^3$ is indeed highly transparent to IR radiations, with approximately $\epsilon = 0$, $\tau = 0.55$ and $\rho = 0.45$. However, when tuning up the doping levels of the same silicon substrate up to $1.10^{19} atoms/cm^3$, results are considerably different. For $1.1\,\mu m < \lambda < 2.5\,\mu m$ the silicon substrate possesses a peak in transparency. At this λ value, optical properties are as follows: $\epsilon = 0.39$, $\tau = 0.22$ and $\rho = 0.39$. On the other hand, for wavelengths superior to $2.5\,\mu m$, most of the IR flux is emitted from the wafer which is what is needed for passive thermal investigation. In this case, $\epsilon = 0.65$, $\tau = 0$ and $\rho = 0.35$.

According to [SCMR99], the latter results correspond to theoretical calculations but have been verified and validated experimentally. In addition, the presence of texture seems to worsen the transmission abilities of the silicon wafer at the benefit of the emissivity coefficient. This observation remains true for low-doped silicon. Consequently IR wavelengths seem to be well suited for optical thermal investigation of ICs. While the preferred spectrum range would locate around the $10\,\mu m$ wavelength to maximize IR emissions, constraints imposed by the measurement equipment also have to be taken into account. For this reason, the next section presents the available technologies enabling IR detection and measurement.

2.4 Heat Source Detection in Integrated Circuits

Now that the light emission mechanisms of ideal and real materials have been presented, the focus is brought on how to acquire and analyze those emissions for IC investigation. In this section, types of IR sensors are discussed and different technologies are presented, along with their pros and cons. Finally the two main techniques regarding passive IR acquisition are detailed.

2.4.1 Thermal Measurement Acquisition

Terminology

The ability of an IR sensor to transduce incident light into an electrical quantity (voltage or current) is called photo sensitivity or responsivity. It is expressed in voltage (or current) per watt of incident energy ($\frac{V or A}{W}$), whitout taking noise into

account and is obatined by the following formula [HP11a]:

$$R = \frac{S}{I \cdot A} \tag{2.10}$$

S being the signal output (V or A), I the incident surface energy $(W.cm^{-3})$ and A the detector's active area (cm^3).

To take the noise into account, the noise equivalent power (NEP) is defined as the quantity of incident light required to obtain a SNR of 1. As shown in eq. (2.11), the NEP is bandwith dependent, the larger the bandwidth the more noise there is in the measurement [HP11a].

$$NEP = \frac{I.A}{\frac{S}{N} \cdot \sqrt{\Delta f}} \tag{2.11}$$

Here, Δf represents the bandwidth (Hz) and N the output noise of the sensor (V or A).

Depending on their technology, IR detectors do not necessarily have the same active surface. To ease sensors comparison, the photo sensitivity per unit of active area of a detector $D^*(cm.Hz^{\frac{1}{2}}.W^{-1})$ is defined and is computed as in eq. (2.12):

$$D^* = \frac{\frac{S}{N} \cdot \sqrt{\Delta f}}{I.\sqrt{A}} = \frac{\sqrt{A}}{NEP} \tag{2.12}$$

The higher the D^*, the more the detector is able to detect small amounts of light.

Types of IR sensors

This section gives a brief state of the art of existing thermal sensors. It has been established in section 2.2.5 that contact measurements are not suitable for small sample sizes and repetitive measurements due to the risk of damaging the circuit. Therefore, the focus is put on optical IR detectors. While not exhaustive, the aim is to give an overview on available technologies for IR investigation along with their advantages and inconveniences.

Microbolometers: This detector is higly integrable and is often used in IR cameras such as in the Variocam HD Head 800 [HP11b]. They consist of an absorbent membrane stacked onto a thermometer [BSJL09]. When lighted with incident IR light, photons are absorbed in the membrane causing it to heat up. The generated heat is then measured by a variable resistor which value is modulated in regard of its temperature coefficient. A read out circuitry performs the measurement of the resistance's value in order to provide an image of the incident IR power. To minimize

noise and for integration purposes the read out circuitry is implemented directly on the substrate.

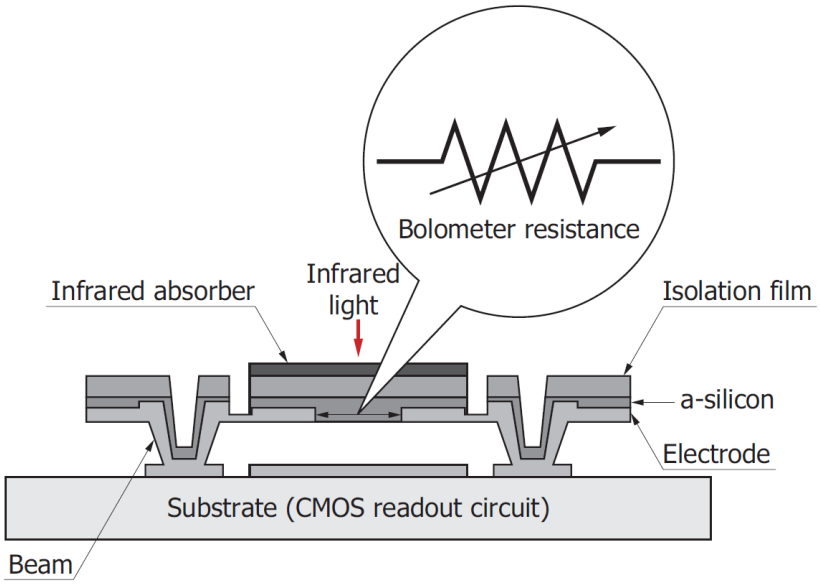


FIGURE 2.8: Cross-sectional view of a bolometer's pixel [HP11b].

The three main contributors to noise generation in microbolometers are thermal (Johnson) noise, 1/f (Flicker) noise, and thermal fluctuation (phonon) noise. While the thermal noise can easily be minimized by rising the bias voltage of the read out circuit, thermal fluctuation noise represent the fundamental limit in microbolometers performances and is limited by placing the detector in a vacuum package [KB04, HP11b]. 1/f noise is the largest noise contributor in current uncooled microbolometers and remains the factor limiting the detectivity of these sensors. Figures in [HP11b] show that microbolometers are part of detectors possessing the lowest detectivity with $D^* = 1.10^8 cm.Hz^{\frac{1}{2}}.W^{-1}$

The temporal resolution of these detectors is, in addition, very low as they provide short bandwidths. Microbolometers are characterized by their slowness with cutt-off frequencies remaining under 100 Hz [KB04]. This type of sensor is therefore preferred for their integrability in matrices rather than for a standalone mono-pixel detection use.

Pyroelectric detector: They rely on a particular characteristic of lead zirconate titanate (PZT) materials whose polarization is affected by temperature. The charge variation induced by the absorption of IR photons by the PZT layer can therefore be outputted as a voltage or a current to the read out circuitry [HP11a]. The voltage configuration is often used in human body detection as it offers a sensitivity peak at low frequencies, simple circuit configuration and low noise characteristics. The current mode is preferred for laser detection, benefiting from high gain.

However, similarly to microbolometers, this type of detector possesses relatively low detectivities ($D^* = 2.10^8\, cm.Hz^{\frac{1}{2}}.W^{-1}$) and reduced bandwidths ($< 500\, Hz$). Here again, pyroelectric detectors present high integrability but mediocre performances in terms of IR detection. In consequence, no further description on this detector is given in this state of the Art.

Photoconductive detector: These detectors rely on a very simple principle which is the electrical resistance decrease when subjected to IR radiations. If of sufficient energy, incident photons can be absorbed by the detector's material to excite an electron from the non conducting band to the conducting band [Key77]. The energy level of a photon is dependent on its wavelength under the classical equation:

$$E = \frac{h \cdot c}{\lambda} \tag{2.13}$$

where h is the Planck constant, c the speed of light in a vacuum and λ the photon wavelength. Thus, this process defines the light spectrum in which the detector operates. The photoconductive effect is then obtained by applying a bias voltage to the detector. This way, the generated current is proportional to the excited electron concentration and is equal to:

$$I_p = A.q.\eta.\Phi.G \tag{2.14}$$

Here, A is the active surface of the detector, $q = 1.60217662 \cdot 10^{-19}\, c$ is the electronic charge, η is the quantum efficiency, Φ is the incident photon flux, and G is the photogain (number of excited electrons flowing per absorbed photon).

As for every detector, the detectivity is limited by noise mechanisms. For photoconductive detectors, the predominant noise sources are generation-recombination noise and thermal noise [Key77]. Thermal noise arises from the random thermal motion of carriers and generation-recombination noise is generated by the random charge fluctuation created by hole/electron interactions within a semiconductor. These are fundamental noises and are intrinsic to the design and the materials of the sensor. Apart from decreasing the temperature, very little can be done from a circuit design point of view to minimize generated noise in these sensors.

Performances of such devices can greatly vary regarding the materials composing the sensitive area of the detector and the temperature [HP11a]. However, the most common association are PbS and PbSe. These photoconductive detectors provide high detectivity but mediocre bandwidths making them quite suitable for continuous or low frequency IR source detection. They usually perform in the close and/or mid IR spectrum, i.e. detecting wavelengths from $1\, \mu m$ to $6\, \mu m$. For higher wavelengths, mercury cadmium telluride (MCT) detectors are required and can measure wavelength up to $22\, \mu m$.

PbS and PbSe detectors can perform at room temperature or be cooled for higher performances. However, dark resistance, photo sensitivity and response characteristics are temperature sensitive. Therefore, incoherences in measurements are highly probable in environments where the temperature is not precisely controlled. In this matter, thermo-regulation can be applied at the price of a more complex design.

Figures 2.9 a), b) and c) describe classical performances of PbS and PbSe photoconductive detectors from Hamamatsu. As expected, decreasing the operating temperature of such sensors rises their detectivity. Most semiconductor have a positive band gap coefficient, which means that the minimal required energy to absorb a photon increases with temperature. Inversely, the negative band gap coefficient of PbS and PbSe widens their detection spectrum as temperature decreases [HP11a]. This phenomenon is showed in fig. 2.9 a) and b) and highlights a powerful advantage of these detectors.

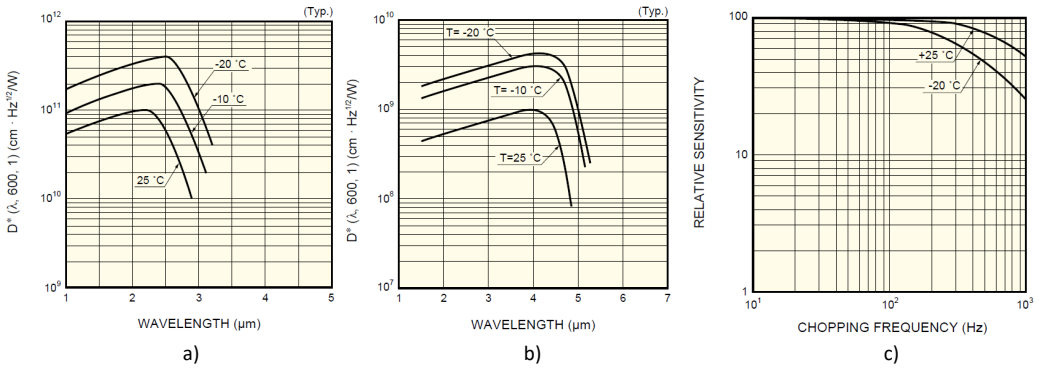


FIGURE 2.9: Example of characteristics of Hamamatsu PbS and PbSe photoconductive detectors. **a)** Spectral detectivity of PbS sensors for three different temperatures **b)** Spectral detectivity of PbSe sensors for three different temperatures **c)** Bandwidth of PbS and PbSe detectors [HP11a].

Photovoltaic detectors: The physical principle of photovoltaic detectors is similar to photoconductive ones. Incident photons of sufficient energy are absorbed and generate excited electrons. However, the photovoltaic effect takes place in materials where there is a space-charge layer, typically p-n junctions and Schottky barriers [Key77]. The excited carrier enters the space-charge layer, where electrons and holes are separated, generating an output current called photocurrent. Most photovoltaic sensors are p-n junctions that can be integrated into matrices for camera applications or used in standalone packages for single pixel acquisitions.

As shown in fig. 2.10, a photovoltaic detector can be modeled by a current source Iph in parallel with a diode D, a capacity C, and a resistor R_D. A serial resistance R_S can be serially added to model the output impedance of the sensor. These detectors are usually used at zero bias. This means that the thermal noise can be considered

predominent even if additionnal sources as shot noise or 1/f noise are also present [Key77, HP11a]. The output current I_S is expressed as:

$$I_S = I_{Iph} \cdot \frac{R_D}{R_D + R_S + R_{load}} \tag{2.15}$$

To maximize the output current, the load must be carefully chosen to have the smallest input impedance possible.

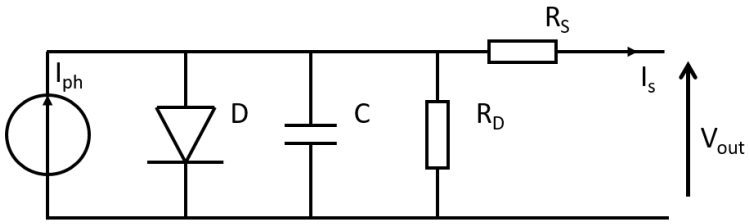


FIGURE 2.10: Equivalent electronic circuit of an InAs photovoltaic detector.

Shot noise is typical of p-n junction and is associated to the statistical process of carriers passing the potential barrier of the space-charge layer. The process is random and depends on the velocity and energy of the carriers. Therefore, the current flowing through the junction is actually a succession of random and independent pulses. However because of the very large number of the latter pulses, the photocurrent is considered constant [PRG93]. The actual non flatness of the junction current is called shot noise. Due to the absence of current bias, the noise figure of photovoltaic detectors is generally flat and both shot and 1/f noises can be neglected [TEL00].

As explained in [HP11a], the fluctuation of background light at a temperature of 300°K cannot be neglected and is also a considerable noise source. To answer this issue, a cold shield reducing the field of view (FOV) of the detector can be used.

Like photoconductive detectors, photovoltaic sensor performances greatly varies in function of their composition. In this case, the most current material combinations are InAs, InGaAs and InSb. While InGaAs provides detectivity in the short IR spectrum, ranging from 0.9 μm to 2 μm, InAs and InSb technologies provide wider mid-IR spectral range, going from 2 μm to 5.5 μm. These devices are known for their very high detectivity with D^* up to $5.10^{12}\, cm.Hz^{\frac{1}{2}}.W^{-1}$ for InGaAs sensors [HP11a] and around $1.10^{11}\, cm.Hz^{\frac{1}{2}}.W^{-1}$ for InAs and InSb detectors [HP11a, TEL00]. Therefore using such detectors, the SNR is greatly improved. Figure 2.11 a) and b) give typical characteristics for InAs, InGaAs and InSb detectors from the Hamamatsu catalog [HP11a].

Again, it is noted that decreasing the temperature significantly improves performances of such detectors. The first explanation for this is the fast increase of the shunt resistance R_D when temperature decreases. According to eq. (2.15) the output

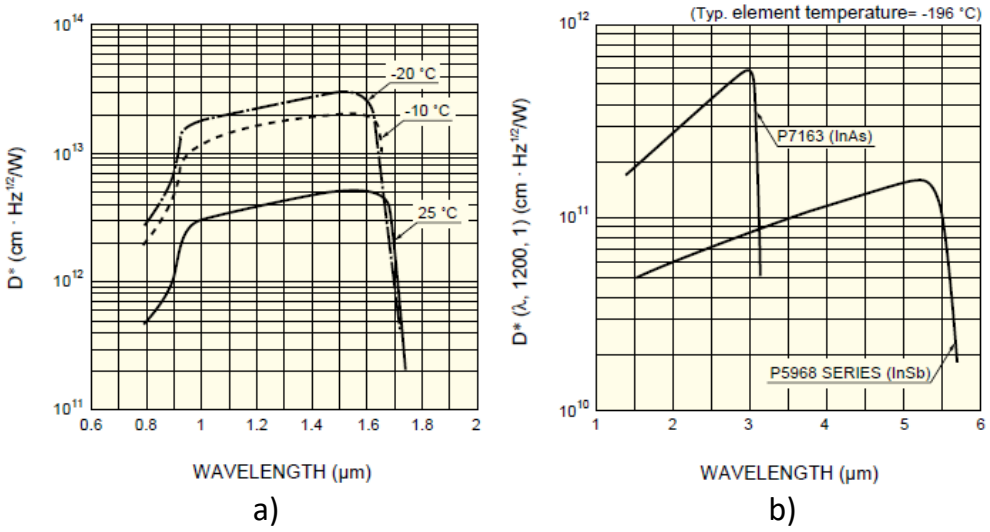


FIGURE 2.11: Example of characteristics of Hamamatsu InGaAs, InAs and InSb photovoltaic detectors. **a)** Spectral detectivity of InGaAs sensors for three different temperatures **b)** Spectral detectivity of InAs and InSb sensors at $-196°C$ [HP11a].

current and thus the responsivity of the sensor is improved. Secondly, thermal noise mainly depends on temperature and thus becomes insignificant when the temperature drops.

More importantly, and unlike the previous presented technologies, photovoltaic sensors naturally provide faster response speed [HP11a, TEL00]. The bandwidth of these detectors can reach hundreds of megahertz in order of magnitude due to the low value of the p-n junction capacity C. As an example, the J12 photodiode from Teledyne Judson Technologies has a response time of only 2.5 ns to a 1 ns laser pulse [TEL00]. In addition, for very high speed applications, the p-n junction of the photovoltaic detector can be reverse biased. This allows to decrease the junction capacity and thus to widen the bandwidth.

Table 2.1 briefly summarizes the described IR detectors and their associated performances from Hamamatsu technical datasheet [HP11a].

Detector		**Spectral response** (μm)	**Operating temperature** (K)	$\mathbf{D^*}(cm.Hz^{\frac{1}{2}}.W^{-1})$
Bolometer		Depends on window material	300	1×10^8
Pyroelectric			300	2×10^8
Photo-conductive	**PbS**	1 to 3.6	300	1×10^9
	PbSe	1.5 to 5.8	300	1×10^8
	InSb	2 to 6	213	2×10^9
	HgCdTe	2 to 16	77	2×10^{10}
Photo-voltaic	**Ge**	0.8 to 1.8	300	1×10^{11}
	InGaAs	0.7 to 1.7	300	5×10^{12}
	InAs	1 to 3.1	77	1×10^{10}
	InSb	1 to 5.5	77	2×10^{10}
	HgCdTe	2 to 16	77	1×10^{10}

TABLE 2.1: Detectors characteristics from Hamamatsu technical datasheet [HP11a]. The underlined values correspond to the type of sensor later used in this document.

The next section presents two different strategies for passive IR acquisition and thermal mapping of ICs. The latter strategies are based on whether IR emission are to be acquired dynamically (AC mode) or statically (DC mode). Therefore the next section lists advantages and weaknesses for both techniques.

2.4.2 Passive thermal acquisition strategies

Steady State Thermography

Steady state thermography consists in the acquisition of all IR emissions from the analyzed circuit. This means that no difference is made between the useful signal and background IR noise sources. The production of useful thermal maps therefore relies on the contrast and the noise performance of the IR sensor.

In [RCN11], authors study hot spot locations in high power consumption circuits such as modern processors. This work takes place in the context of improving reliability, performances and power consumption of ICs. In this objective, local hot spots and temperature are tracked to "provide new experimental techniques for thermal characterization". Concretely, from hot spots located on IR images, the authors propose a new thermal sensor allocation technique to monitor heat sources more accurately.

In the paper, the DUT is a dual core AMD Athlon II 240, working at 2.1 GHz in flip-chip configuration. It was previously mentioned that low doped silicon as die substrates benefit from silicon transparency in the mid-IR spectrum. The flip chip packaging thus greatly facilitates the IR analysis as the chip becomes back-side accessible. The thermal imaging is realized using a FLIR SC5600 IR camera. This device is able to acquire IR radiation in the $2.5 - 5.1\,\mu m$ spectrum using a 640×512 InSb sensor array and a framerate of 100 Hz. To reduce noise and thus improve detectivity, the camera is cooled at $-196°C$.

The authors demonstrate how different workloads can lead to variations in hot spot location. Several configurations, assigning the workload only to one core or both of them, are used. Thereby, the possibility of thermal hot spot tracking using IR thermography is demonstrated as heat sources are found on top of active areas while sectors of lower activity remain cooler. This is illustrated in fig 2.12 issued from [RCN11], which shows thermal images of the AMD processor under various workloads. Red areas correspond to high temperature on the die and thus high electronic activity, while blue areas indicates colder locations and thus lower power consumption. It is then possible to identify toggling activity between one core and the other depending on the applied benchmark.

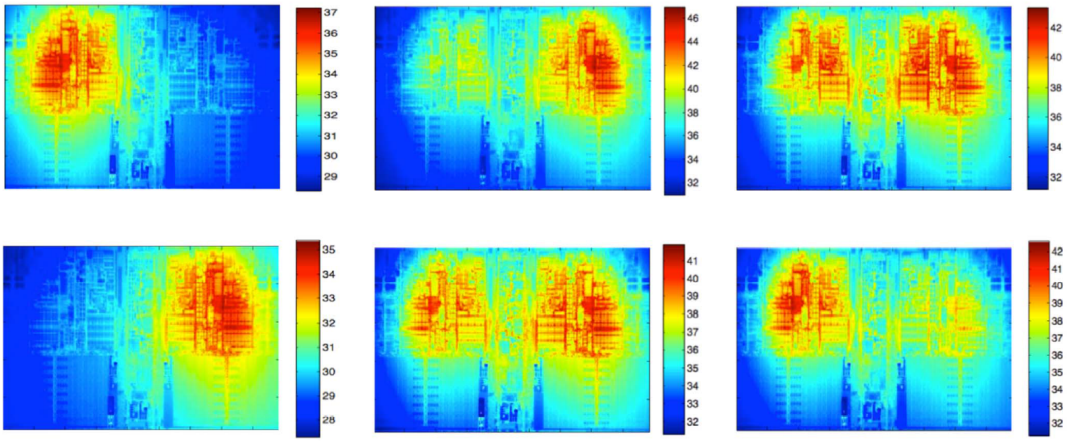


FIGURE 2.12: Tracking electronic activity using steady state thermography on an AMD Athlon II 240. Each image corresponds to a different workload, therefore highlighting different power consumption locations on the die [RCN11].

In an extension of the previous work, Sherief Reda elaborated a methodology to invert temperature maps toward power map. The method is then applied to identify true power consumption of active blocks in a processor for post-silicon characterization [Red11]. This brings forward the low pass filtering effect of silicon dies that is a consequence of heat diffusion. The power maps are usually sharp and geometric, following the layout of the DUT. The local power consumption is therefore subject to abrupt variation in space [Red11]. However, because of lateral heat spreading, the temperature and thus the IR emissions vary smoothly in the circuit. As a consequence, transposing temperature maps to power maps is usually an ill-posed problem as the spatial filtering breaks the uniqueness condition required for the inversion [Red11].

It is stated in [BWL10b] that a hot spot is detected under the condition that the temperature contrast at the surface of the die exceeds the detection capability of the sensor. Let us consider an area of the DUT that possesses a high power consumption which is divided through a high frequency spatial pattern. In such situation, the IR emissions of each separated hotspot could fall under the threshold detection of the sensor. Spatial filtering of silicon substrates can thus lead to critical losses of information. This process is illustrated in fig 2.13 from [Red11] where a continuous emission block is subsequently divided at different frequencies using a checkboard pattern.

If steady state thermography seems adapted to high power devices, it is common knowledge that the methodology suffers from various flaws making the investigation of lower power consumption devices nearly impossible [BWL10b]. In fig. 2.12, the color scale shows measured temperature gradients going up to 14°C. That kind of huge temperature variation can only be measured on high power ICs such as processors whose current consumption can largely exceed fifty amperes.

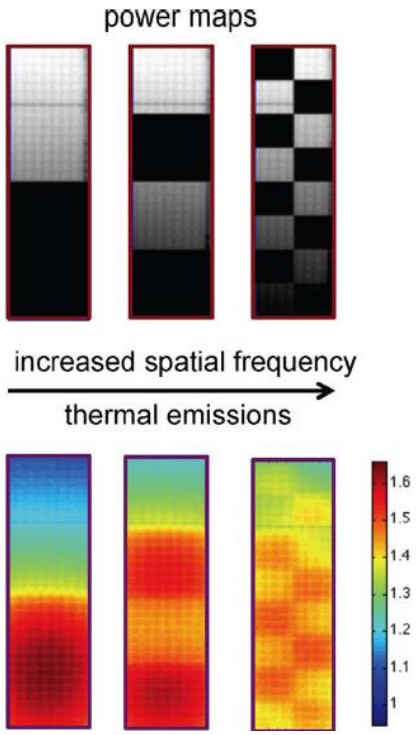


FIGURE 2.13: Illustration of the spatial low pass filter effect affecting thermal signals [Red11].

The high power consumption of such circuits ensures strong IR emission and thus a high SNR. Unfortunately, this is not the case for other complex architectures as microcontrollers or FPGAs whose current consumption is of the hundreds of milliampere order of magnitude at most. The camera used in [Red11, RCN11] provides a temperature resolution of 20° mK which is clearly insufficient as is for low power devices investigation [BWL10b].

As the SNR decreases, longer acquisition times are required to average out the noise making the IR acquisitions vulnerable to slow drifts of external parameters as temperature or ambient light. In section 2.3.1, it was showed that IR emissions are intimately linked to the fourth power of temperature by the Stefan-Boltzman law (eq. (2.4)). Despite being the very reason making IR thermography possible, it is the source of many incoherences if the experience is subjected to a temperature drift. This drift can also affect the IR detector if the latter is not thermo-regulated.

In addition, steady state thermography is based on the acquisition of every IR radiations emitted from the DUT. As a consequence, a DC offset is generated by the static power consumption of the chip such as the clock tree or the cumulative leakage of CMOS transistors. The low heat resistance of silicon makes it prone to lateral heat conduction which affects the spatial resolution and the contrast of thermal maps [BWL10b]. The heat diffusion generated by undesired power consumption can therefore lead to weak hot spot concealing and thus information losses.

Another limitation, is the emissivity contrast problem. Metals layers are a perfect examples illustrating this issue. Contrarily to silicon, metals are highly reflective and poor emitters and transmitters. Thus, the emissivity contrast between materials make the thermal imaging of heterogeneous designs such as ICs quite complex. Two materials at the same temperature but with different emissivities would appear to have different thermal activities and thus different power consumption. To compensate the emissivity contrast, [RCN11] applies a calibration process, forcing the off-powered DUT into various isothermal status to build an emissivity model for each pixel in function of the temperature. A correction is then latter applied to the real measurements. However this correction is only applicable to camera based thermal images. Alternately, [BWL10c], proposes to cover the surface of the die with a thin layer material of high emissivity like graphite or special varnishes.

To summarize, steady state thermography is a powerful tool for the investigation of high power chips such as modern processors. However, the sensitivity of this methodology to external parameters (light, temperature) and material emissivities added to its lack of detectivity makes it an unreliable tool for low power investigation. In the next section, a particular methodology named lock-in correlation is introduced and solves most of the issues previously mentioned at the cost of being frequency selective. It is demonstrated that this method improves significantly the detectivity of IR detectors, nullifies the influence of emissivity contrast while remaining robust to temperature and light drifts.

Lock-in Thermography

Thermal lock-in correlation is a technique proposed by O. Breitenstein in [BWL10b, BWL10c] in order to identify small defects in the manufacturing of ICs. Due to the investigation of low power heat sources, it is expected that the IR power emitted is of extremely weak amplitude. Therefore extracting the targeted signal from noise is a key challenge for low power IC investigation. Instead of acquiring all IR emissions from the circuit, the lock-in correlation proposes to target radiations generated by a specific operation in the circuit based on its frequency. The frequency at which the method is applied is thus named the lock-in frequency.

This method is based on the principle that an alternative power consumption generates alternative IR emissions at the same frequency. Tools from synchronous detection and signal processing are therefore applicable. Mathematically, the lock-in thermography technique is equivalent to a Fourier transform performed at a single frequency. From there, the method provides the amplitude and phase values of the fundamental harmonic from the measured signal.

Computing amplitude and phase values at a single frequency drastically reduces the noise of the measurement, the latter being spread along the bandwidth of the measurement equipment. The ultra narrowed bandwidth of lock-in correlation therefore allows to extract useful information from signals where the SNR is greatly inferior to one. In addition, the DC signal component is suppressed from acquired signal. This means that clarity of thermal images are greatly improved as it is spared from any background thermal lateral conduction. Both contrast and spatial resolution are thus increased.

In [BWL10c], it is demonstrated that non harmonic heatings can be reduced to an harmonic problem as long as the lock-in frequency is small in regard of the sampling rate of the measurement system. Therefore only the harmonic case can be considered, meaning that thermal signals would be reduced to eq. (2.16):

$$S(t) = A \cdot sin(2 \cdot \pi \cdot f_{lockin} \cdot t + \Phi) \tag{2.16}$$

The amplitude of $S(t)$ is noted A, its phase Φ, and its frequency f_{lockin}. From there, the lock-in correlation technique consists in computing the discrete integration of the multiplication of the acquired signal $F(t)$ of length n by a correlation signal $K(t)$ over the number N of acquisitions:

$$S_\Phi = \frac{1}{n \cdot N} \sum_{i=1}^{N} \sum_{j=1}^{n} K_j F_{i,j} \tag{2.17}$$

In case of a two-channel correlation, S_0 is obtained by replacing $K(t)$ by the sine function (a.k.a the in-phase correlation signal). Similarly, S_{90} is obtained by replacing $K(t)$ by the cosine function (a.k.a the 90° shifted correlation signal) [BWL10c]. By decomposing eq. (2.16) using the addition theorem and combining it with eq. (2.17), the following equations are established:

$$S_0 = A \cdot cos(\Phi) \tag{2.18}$$

$$S_{90} = A \cdot sin(\Phi) \tag{2.19}$$

It is then easy to infer eq. (2.20) and (2.21), expressing the amplitude and phase of $F(t)$ respectively.

$$A = \sqrt{S_0^2 + S_{90}^2} \tag{2.20}$$

$$\Phi = Arctan(\frac{S_{90}}{S_0}) \tag{2.21}$$

The range of the arctan function is $[-90°,\ 90°]$. This means that the arctan repeats itself twice on the $[0°,\ 360°]$ domain. For this matter, a four quadrant version of the arctan function can be used. As a result, phase values are computed as:

$$\Phi = Arctan(\frac{-S_{90}}{S_0}) \tag{2.22}$$

The obtained phase values are comprised in the $[-180°, 180°]$ range. The delay due to thermal propagation is then restored using:

$$\Phi_{th} = -180 - \Phi \quad (if\ \Phi > 0) \tag{2.23}$$

To simplify notations, the corrected phase is referred as Φ in the rest of the document. The whole lock-in correlation methodology is summarized fig 2.14.

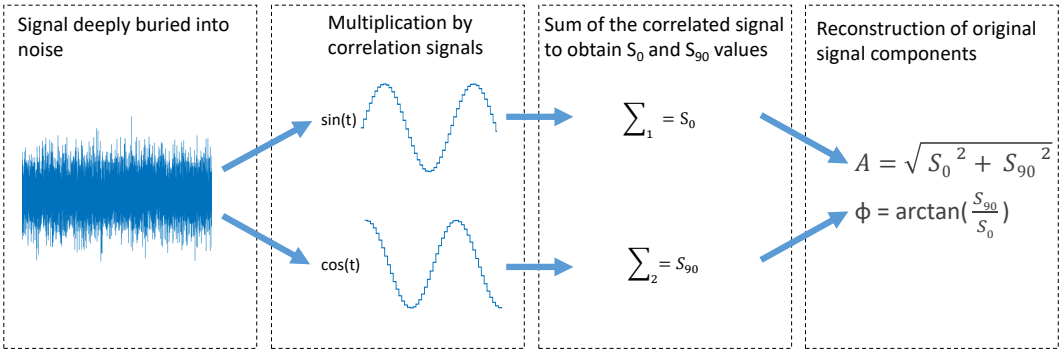


FIGURE 2.14: Discrete lock-in process.

If DC measurements are not suitable for low power hot spot mapping, they are of great utility to learn about the thermal behavior of the DUT. Thereby, they can guide dynamic measurement, i.e. the application of the lock-in thermography approach, by defining acceptable range for certain experimental parameters such as the lock-in frequency. Plain curves of fig. 2.15 show the thermal IR response of a Xilinx Virtex 5 FPGA to power consumption steps of different magnitudes. The thermal stimulation is created by activating micro heaters composed of ROs. Each plotted curve corresponds to a different amount of active ROs and thus to a different magnitude.

The first order modeling of the presented measurements are plotted with dashed lines on the same figure. From this model, the IC thermal behavior of the DUT is characterized by a cutting frequency of $5\,mHz$. The first order model states that an attenuation of twenty decibels per decade appears once the cutting frequency is passed. As a consequence, by performing the lock-in thermography methodology at

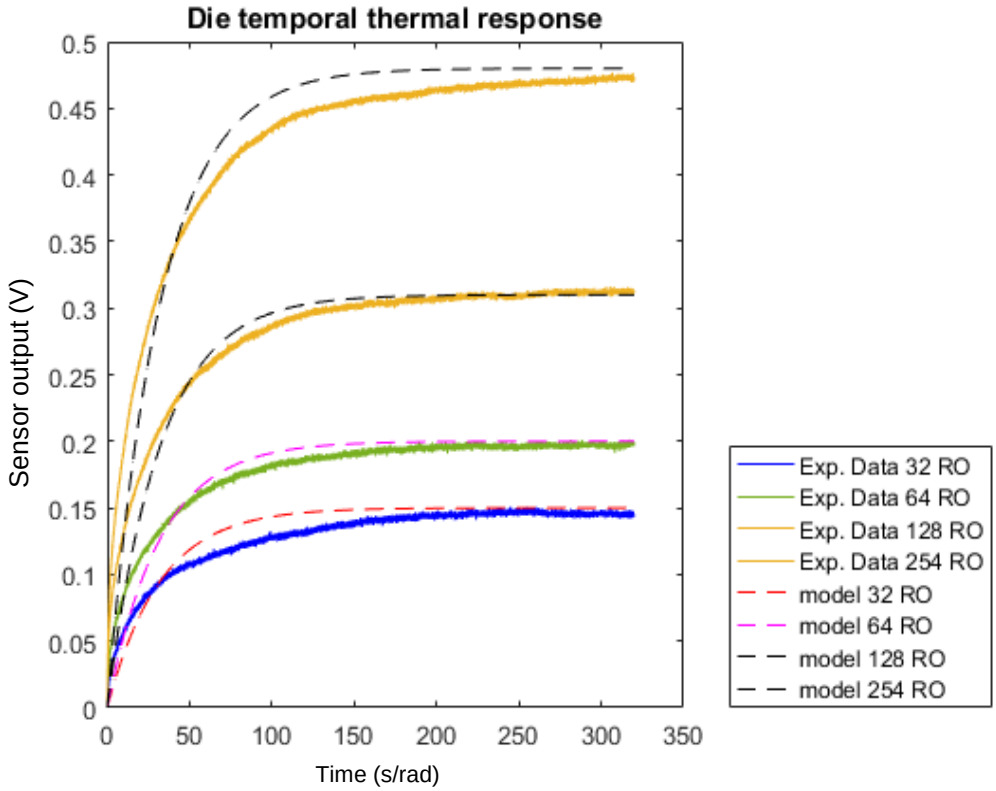


FIGURE 2.15: Experimental and calculated first order thermal responses of the DUT to several thermal step inputs.

$10Hz$, at least $60dB$ gain is required from the measurement chain only to compensate the attenuation engendered by the slowness of heat diffusion.

These results demonstrate that lock-in thermography is a rather low frequency methodology. The choice of the lock-in frequency remains tricky and must be chosen with great attention. As explained in [NWR11], it is a delicate balance between spatial resolution and signal to noise ratio (SNR). This frequency determines the heating and the cooling timings of the circuit. Because heat is a slow phenomenon compared to internal clock speed of ICs, choosing a high frequency prevents the heat from reaching the surface of the die thus leading to information loss as low power sources remains under the detection threshold of the measurement system. On the contrary, a low frequency results in a blurry image because of the lateral heat diffusion, therefore impairing the spatial resolution. Generally, the lock-in frequency is quite low and is comprised between 1 Hz and 100 Hz [BWL10c, NWR11].

Because of this low value the lock-in heat modulation must generally be artificially created. This is actually an advantage as it allows the user to precisely target any part of the circuit depending on the chosen modulation. A common modulation, presented in [BWL10c], consists in superimposing a low frequency AC signal

to the power supply of the die. This point is further detailed in chapter 3.

Most thermography methods rely on the analysis of amplitude values as it is a straightforward value to interpret. Phase values are a measure of the delay existing between the activation of a thermal source and the moment the IR radiations are detected by the acquisition chain. Applied to IC investigation, they present many advantages over amplitude values. In particular, they are independent of amplitude and therefore immune to the emissivity contrast of materials composing an IC [BWL10c]. An interesting use of these measurements is made in [SASD10] as phase is exploited to investigate depth of defects in silicon dies. This approach allows to locate more precisely the problematic area by using 3D maps instead of classical 2D analysis. Additional interesting properties of phase regarding its statistical distribution are also later developed in chapter 3 section 3.3.3 of this document. However, the spatial resolution of phase images is usually inferior to the amplitude ones. Other images can also be exploited as the $\frac{S_0}{S_{-90}}$ map. This image provides good spatial resolution while benefiting from the emissivity contrast immunity of phase images. Examples of such thermal maps are presented fig. 2.16.

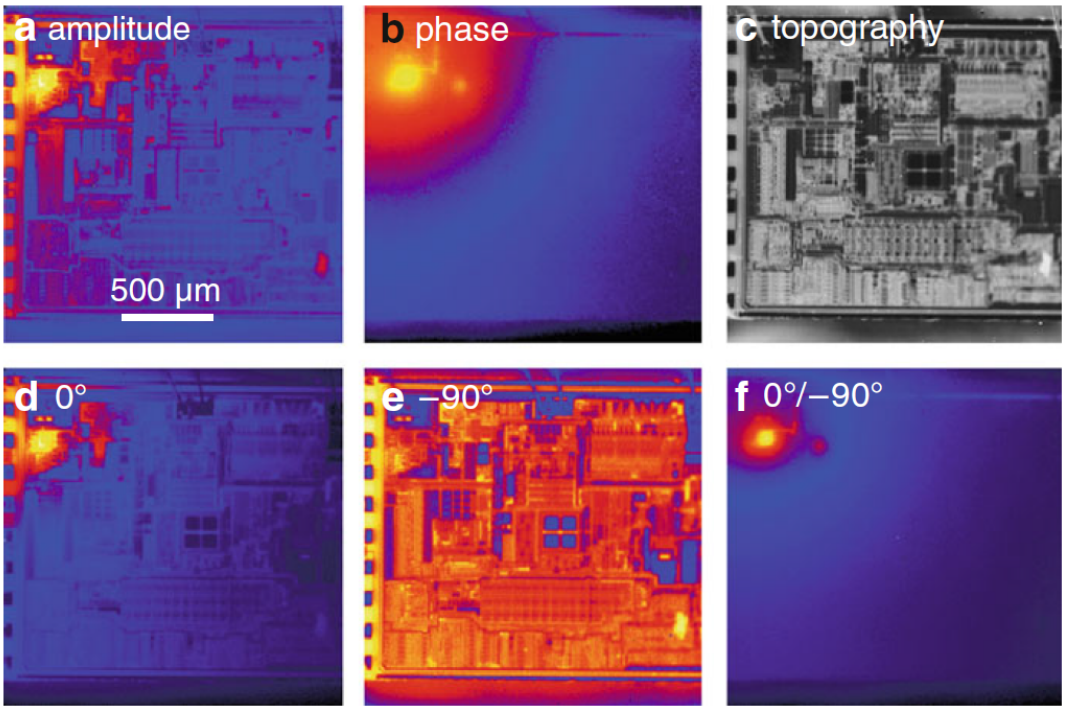


FIGURE 2.16: Example of lock-in thermal maps [BWL10a]. **a)** Amplitude image **b)** Phase image **c)** Topography image **d)** S_0 image **e)** S_{-90} image **f)** $\frac{S_0}{S_{-90}}$ image.

In the end, lock-in thermography is a promising tool allowing the identification of very weak AC signals buried in noise. In addition, this methodology solves the previous mentioned issues tied to steady state thermography, namely the emissivity contrast, the information loss due to DC lateral heat conduction and the sensitivity toward the experimental environment. Due to the low bandwidth imposed by the

first order thermal model of heat diffusion, the lock-in correlation relies mostly on artificial modulation (e.g a pulsed power supply) in order to identify thermal sources in ICs. This modulation also allows the investigation of hot spots that could have a natural DC behavior. Lock-in thermography is therefore a well adapted tool for IC imaging and investigation.

2.5 Chapter conclusion

This chapter has presented a broad state of the Art regarding IC microscopy and imaging. While being non exhaustive, its aim was to list pros and cons of existing methodologies in order to identify vectors of possible improvements.

The state of the Art reveals that existing imaging techniques are either inaccurate (EM activity coupling issue) or extremely expensive (photonic, laser imaging, thermal camera, etc). Their application spectrum can vary largely, some allowing the identification of macro blocks (thermal imaging, EM imaging, etc) while others being able to get details down to the transistor level. In addition, precise methodologies are usually impaired by huge acquisition times when the location of the targeted source is not known beforehand. IR imaging is quite successful due to its advantageous properties, mainly, the transparency property of silicon allowing easy back side investigation. However, most of the existing work relies on costly cameras that possess very poor sampling speed. The review on IR detector showed that alternative sensor types, as photovoltaic detectors, could provide both very high detectivity and very short temporal responses.

It was demonstrated that, high SNR requirement, lateral DC heat conduction, and emissivity contrast, make steady state thermography unsuitable for investigation of low power hot spots. Lock-in thermography on the other hand, seems to provide much better performances, mostly due to its ability to extract signals from noisy measurements. In addition, the ability to draw timing images of thermal signals seems quite powerful as it is intrinsically immune to emissivity contrast issues. Very few researches were axed on this subject in IC investigation apart from depth defect location.

Finally the lock-in correlation allows imaging thermal sources of very weak amplitude without being impaired by emissivity contrast, lateral heat diffusion nor experimental conditions. Therefore this methodology is used and adapted to the IR microscopy platform presented in chapter 3 where the detailed design of the measurement set-up is presented. New ways in applying the lock-in correlation are also described. In particular, the statistical distributions of lock-in measurements are studied. From that, an automated thermal extraction feature is designed. To the best of our knowledge, such work remains nonexistent in the actual state of the art.

In order to demonstrate the achieved performances, a full characterization of the platform, including detectivity limits, spatial resolution and application to real test cases, is then presented.

Chapter 3

IR Measurement Platform and Thermal Scan Methodology

This chapter presents the designed IR measurement platform. After detailing and justifying each piece of hardware composing the acquisition chain, obtained thermal measurements are studied from a statistical point of view. From there, it is demonstrated that lock-in distributions possess several properties that allow us to have efficient identification of pixels containing thermal information. These properties are therefore exploited to characterize the performance of the IR platform and perform reverse engineering on commercialized SoCs. The work presented in this chapter have lead to the publication of a conference paper at Therminic 2019.

3.1 Chapter Introduction

In the context of hardware security, identifying the location of secured elements in an IC can be critical to maximize the success probability of an attack. The targeted circuits range from SoC and FPGAs to microcontrollers, thus, the topology and the power consumption of investigated circuits is susceptible to vary greatly. As an example, FPGAs are usually large chips that consume several hundreds of milliwatts. Due to their programmable nature and their homogeneous layout, non selective imaging techniques are unable to identify active macro blocks of a design. Yet, their relatively high power consumption facilitates thermal investigations. Inversely, microcontrollers, much smaller size wise, are often designed for low power applications. Therefore, a very high detectivity is required to establish thermal maps of these circuits.

The packages of the mentioned devices are also to be taken into account. Modern devices with many IOs (FPGAs, SoCs) are frequently found in flip-chip configuration which offers direct access to the DUT backside once decapsulated. Classical wire bonded packages are in contrast harder to investigate. In the case where

they are chemically etched, they only provide access to the front side which present poor IR emission characteristics due to the high reflectivity of metal layers. Custom boards are therefore required if backside analysis is to be performed on this type of die. Alternatively, through package analysis can be performed but at the cost of a degraded spatial resolution due to the lateral heat diffusion within the package layers. These facts highlight the need for a measurement platform capable of being adapted to the configuration of the DUT and its PCB.

The state of the art reveals that cameras are far from ideal for such investigations as they lack detectivity and are temporally limited by their read out circuitry. Chapter 2 shows that mono-pixel detectors provide both the high detectivity and the fast response time required for low power heat source investigation. Following on this ascertainment, this chapter proposes a customizable acquisition chain build with off the shelf components. Combined with the high sampling rate of modern digital sampling oscilloscopes (DSO), it is shown thermal lock-in imaging can be a powerful tool for low power source identification. What is more, based on statistical analysis of lock-in measurement distributions, this chapter proposes an automated thermal information extraction feature. Thereby, the analysis of thermal maps does not rely on human interpretation but on statistical tests, in the aim of providing more objective conclusions. The work presented in [AM11] and [MLdS13] uses statistical tests to improve the contrast of thermal map but no detection criterion is mentioned. While sub mW power consumption can be identified by the methodology proposed in this chapter, the ability to localize several crypto-processors on modern architectures is also demonstrated. In the following sections, the focus is first put on describing and characterizing the designed IR platform. Then, practical cases of SoC investigation are presented.

This chapter is organized as follows. In section 3.2, a detailed description of the measurement system is given. The type of sensor, optics and signal conditioning are justified and the mapping methodology explained. As the thermal lock-in correlation is applied, section 3.3 provides additional information on the thermal measurements. In particular, thermal modulation techniques are presented, as well as the statistical behavior of amplitude and phase values. Subsequently, in section 3.4, the platform is characterized by showing spatial resolution and power consumption detection limits. Different commercial SoCs investigation are then presented as practical cases. Finally, section 3.5 concludes on the performances of the platform.

3.2 Acquisition chain

3.2.1 Sensor

Photodiodes are advantageous devices as they are low cost and, above all, have a far better detectivity than IR cameras at equivalent temperature. The IR detector used on this platform is issued from the J12 photovoltaic InAs detector serie, manufactured by Teledyne - Judson Technologies [TEL00]. Its active area is a disk of 250 μm and detects IR light in the $[1,\ 3.8]\,\mu m$ spectrum range. As shown in chapter 2, the response of this type of detector is very sensitive to temperature variations. For that reason, the manufacturer proposes several versions of the sensor, some being equipped with cooling modules. Cooling is optionnal and usually reserved for low light applications, the absence of thermo-regulation requires a stable room temperature to prevent any variation in the detector's response. Initially equipped with the room temperature version of the J12 photodiode, the platform's detector was replaced with the J12TE3 version in order to maximize the detectivity and minimize temperature drift errors.

The J12TE3 configuration places the detector in an hermetically sealed package which embeds three stacked thermoelectric modules for heat extraction. Using a build-in thermistor and an external current regulator, the detector can be cooled down to $-65\,°C$. Both the detector and its thermal regulator are presented in fig. 3.1. On the bottom right image, the sensor is equipped with a homemade optical system that allows to greatly improve the spatial resolution of the thermal images. Further details on the optics are provided in section 3.2.4

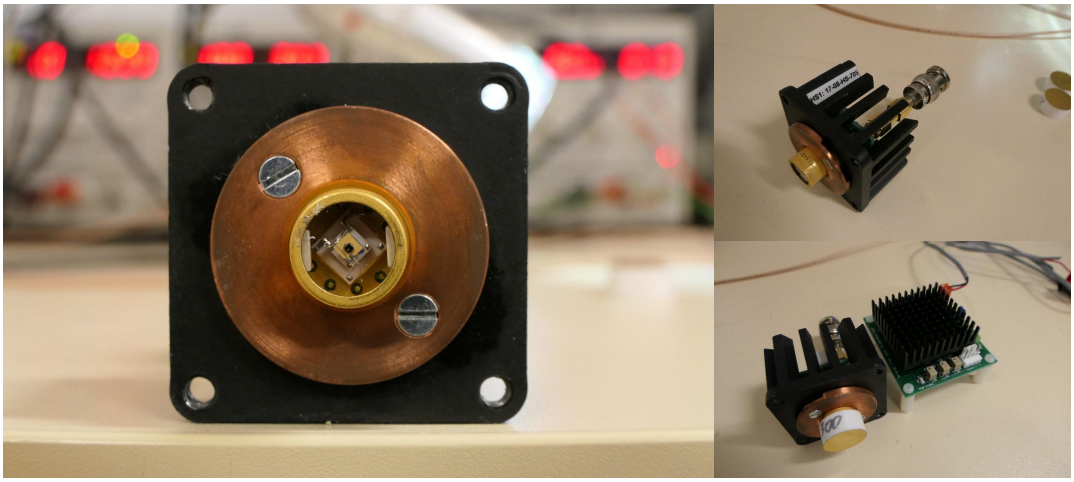


FIGURE 3.1: J12TE3 detector and its thermo-regulation module.

Graphs in fig. 3.2 present the main characteristics of the J12TE3 sensor and compare it to other versions of the photodiode, operating at different temperatures. As shown in fig. 3.2 a) the J12 photodiode detectivity is greatly improved when its

operating temperature decreases. Comparing the room temperature version (22 °C) to the J12TE3 (−65 °C) reveals that the sensor's detectivity is improved by a factor 100. This is explained by the temperature dependence of the shunt resistor of the device in fig. 3.2 b) and the reduction of internal thermal noise. When cooled down to −65 °C, the detectivity peaks at $D^* = 1.2 \times 10^{11}\, cm.Hz^{\frac{1}{2}}.W^{-1}$ for $\lambda_{peak} = 3.2\,\mu m$. However, it must be noted that due to the positive band gap coefficient of the materials composing the detector, the spectrum detection range is slightly reduced from 3.8 μm to 3.4 μm. This phenomenon is illustrated in fig. 3.2 c).

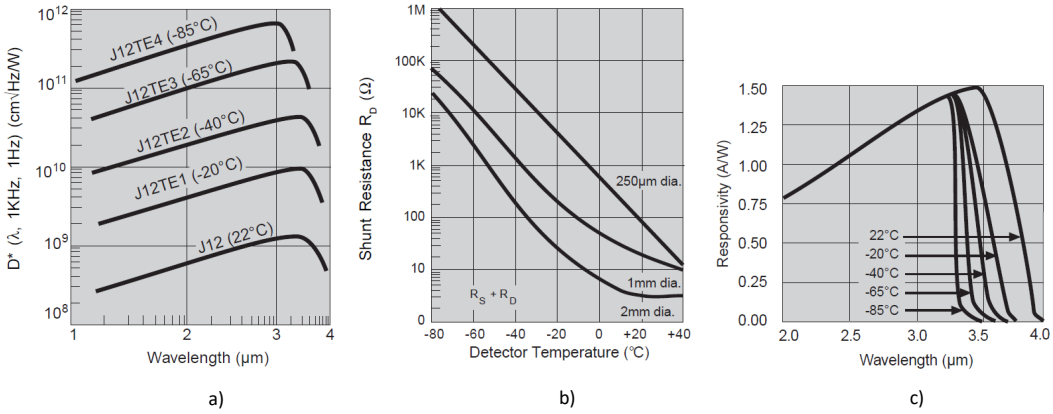


FIGURE 3.2: Teledyne J12 photodiode characterization **a)** Detectivity over wavelength for different cooling temperatures **b)** Shunt resistor value over temperature for different sensor sizes **c)** Responsivity of the detector over light spectrum for different cooling temperatures [TEL00].

3.2.2 Signal Conditioning

This section discusses the amplification and filtering of the signal provided by the output of the photodiode. It is common knowledge that when performing acquisition on signals of low SNR, the first amplification stage is critical as it defines the noise quantity to be amplified by the following stages. In addition, a very high gain is required to compensate the weak nature of IR thermal emissions and the low pass filtering effect of heat diffusion.

The output current of the photovoltaic detector imposes the first stage to have a transimpedance amplification to convert the photocurrent into a voltage. The FEMTO LCA-20K-200M is particularly adapted as it is designed to minimize the detector's dark current by applying a quasi-perfect zero bias on the photodiode. In addition it provides a high gain of $G = 2 \times 10^8\, V/A$, an ultra low input current noise of 14 $fA/Hz^{\frac{1}{2}}$ and a bandwidth of 20 kHz. To minimize the input noise and conduction losses, the first stage amplifier is placed as close a possible to the detector.

The FEMTO DLPVA-100-F-S is a programmable gain voltage amplifier that is added serially to the first stage amplifier and can provide up to $100\,dB$ additional gain. However, the maximum applicable gain is often limited by the noise level from the first stage that saturates the second stage amplifier. For this reason, voltage gain is limited to $40\,dB$ in practice. While capable of providing a bandwidth of $100\,kHz$, this amplifier is equipped with a low pass filter allowing to reduce the bandwidth down to $1\,kHz$. This allows to limit the bandwidth of the total measurement chain and thus the acquired noise. Fig. 3.3 presents the two amplifiers operating on the platform.

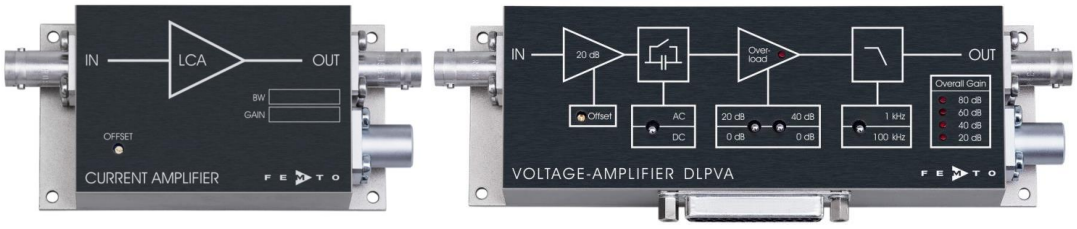


FIGURE 3.3: Femto current amplifier (left) and voltage amplifier (right) used on the platform.

Finally, in order to push even further down the noise level, a fifth order switched capacitor filter is placed at the output of the second stage amplifier. This filter is programmable as the output bandwidth is proportional to the input clock frequency used to toggle the internal capacities. If performing lock-in measurements on very small signals, a selective band pass filter can be inserted between the two amplification stages to decrease the noise level and thus allow the use of a higher gain on the programmable amplifier.

3.2.3 Acquisition and post-treatment

Once the thermal signal is acquired, amplified, and filtered by the measurement chain, it is digitized using a DSO communicating with a control computer that stores the experimental data. In the rest of the document, a digitized signal from the DSO is called a trace.

On this platform, the DSO is a Lecroy Wave Runner 800 series. It has a vertical resolution of 8 bits and a programmable sampling rate up to $20\,GS/s$ combined to a memory depth of 16 million points. Software lock-in correlation can therefore be applied either during the cartography once the traces have been transmitted to the control computer or as post-treatment on the stored traces. The case where the lock-in correlation is applied directly during the acquisition is called "online lock-in correlation".

One downside of single-pixel detectors is the necessity to sequentially acquire each pixel of the image which leads to long acquisition times. Each experimental results presented further in this document requires around 24 hours to be acquired. The sensor is mounted on xyz motorized axes controlled by the remote computer in order to scan a defined area. Even if proceeding this way is time consuming, it provides 100% customization possibilities. The image acquisition time can be tuned by adjusting parameters such as pixel step, lock-in frequency or the number of acquired traces.

Different acquisitions and computation strategies can be applied. eq. (3.1) recalls the lock-in mathematical process presented in 2.4.2.

$$S_{lockin} = \frac{1}{n \cdot N} \sum_{i=1}^{N} \sum_{j=1}^{n} K_j F_{i,j} \tag{3.1}$$

In this equation, because the sums are finite, they can mathematically be swapped. This means that the acquisition of a small number of traces can be compensated with a high sampling rate. Inversely, a low sampling rate can be compensated by the acquisition of many traces for better averaging. For optimization purposes, it is advantageous to acquire only one trace of many lock-in periods using a high sampling rate. In this way, communication delays between the control PC and the DSO are reduced. Similarly, performing online lock-in correlation, spares the necessity to perform repetitive and time consuming write operations on hard drives. Finally, it is found that binary is the most efficient data format to transmit (and store) as each sample is coded on a single byte. Consequently, the amplitude's unit is also expressed in binary. Amplitude values therefore range from 0 to 255, corresponding to the 256 sampling levels of the 8 bits DSO. The time saved can then be used to increase the thermal map size or its resolution. Once acquired, the lock-in data can be exploited as images in which each pixel is the averaged amplitude or phase value or as 3D matrices containing statistical distributions of thermal measurements (amplitude or phase) for each position.

Finally, this set-up provides a tremendous advantage over cameras in terms of sampling rate. Even with lock-in frequencies as low as 1 Hz, a camera with a nominal frame rate of 500 Hz only provides 500 samples (images) by period. Eventually, this number can be slightly raised if a smaller image resolution is set. As a consequence a resolution of 0.72° is obtained on phase measurements. In comparison, using a photodiode and setting the sampling rate of the DSO to 1 MS/s yields a 1 Hz lock-in frame containing $1 \cdot 10^6$ samples. With such settings, the obtained phase resolution is $3.6 \cdot 10^{-4}\,^\circ$. Obviously, the phase resolution of the measurements obtained with our platform are higher than the ones obtained with an IR camera. For the same reason, sampling rate is generally prioritized over the number of acquisitions.

It was previously mentioned that lock-in correlation results are immune to external parameters such as light or temperature. While this is mostly true, precision of the data can still be affected by the variation of these parameters. For example, fluorescent light, which is used in most offices and laboratories, is in reality pulsed at 100 Hz. This frequency is quite close to usual lock-in frequencies and while it will certainly be filtered out by the narrowed bandwidth of the lock-in correlation, it still appears on the trace acquired by the DSO. The amplitude of this light is usually much bigger than the targeted light emission from the IC and thus imposes a larger calibre on the DSO to avoid signal clipping. The use of such large sensitivity may conceal tiny variations of the targeted light as they are susceptible to remain under the minimum sampling quantile of the DSO (limited vertical resolution). Similarly, measurements performed in DC coupling on the DSO are subjected to variable offsets due to temperature drifts. To avoid these inconveniences, the set-up is placed in a closed environment. This allows to perform measurements in the dark and minimizes abrupt temperature drifts. By means of illustration, fig. 3.4 shows the platform inside its container.

FIGURE 3.4: IR acquisition platform in its isolation container.

Overall, the measurement instruments (sensor, optics, filter and amplifiers) presented in this thesis were acquired for less than 5 k\$. In comparison, an IR camera costs around 70 k\$.

3.2.4 Optics

The package of the photodiode is derived from the TO-66 one [TEL00]. Its front window is a 9 mm diameter round sapphire IR transparent glass, placed at d_1 =

1.524 mm from the sensor (see fig. 3.5). Using this type of sensor, measurements are realized in close field to maximize the amount of received IR light and minimize the solid angle integration. Because of the distance between the detector plane and the package window, the surface focused by the sensor on the DUT is much wider than the surface of the IR sensitive area and depends on the sensor's field of view (FOV). In this condition, the active part of the sensor is considered punctual. The diameter of the focused circle on the DUT without optics is then computed as follows:

$$D = 2 \cdot (d_1 + d_2) \cdot tan(\frac{FOV}{2}) \tag{3.2}$$

where d_1 is the distance between the window and the detector plane and d_2 is the distance between the DUT and the window. Fig. 3.5 summarizes the latter descriptions into a schematic view of the package.

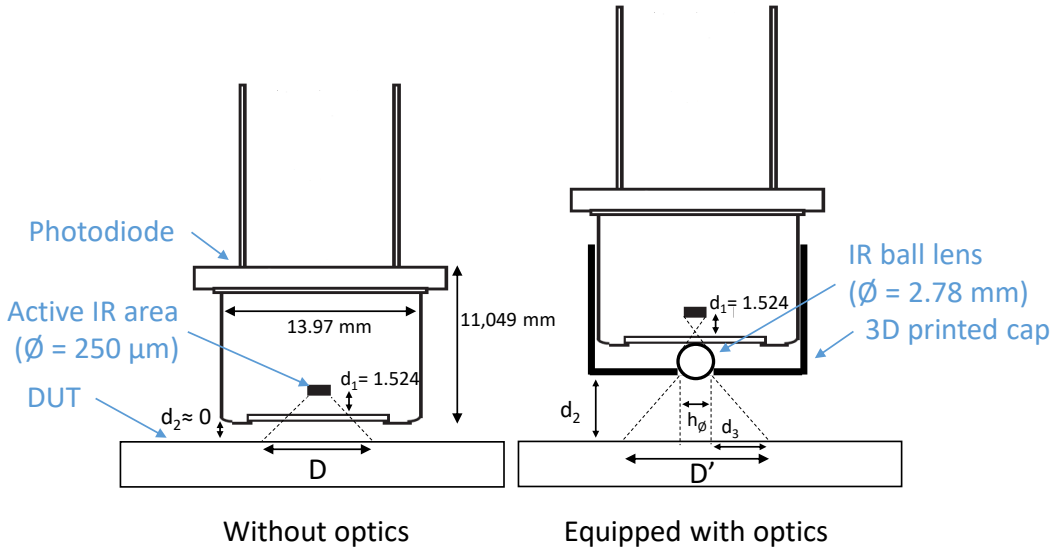


FIGURE 3.5: Optical system designed to improve spatial resolution.

The FOV of the Judson Technologies J12 detector is 60° and $d_1 = 1.524\,mm$, therefore placing the sensor in contact with the DUT means that the focused area has a diameter of 1759.8μm. The acquired IR signal is then a combination of the emissions of all hot spots present in this area. As a consequence the spatial resolution is severely degraded.

In the objective of improving the spatial resolution of the platform, several optics have been designed. Their principle is based on drastic reduction of the FOV while using a lens to focus incident IR radiations. To reduce the FOV of the sensor, a polylactide (PLA) 3D printed cap is inserted in front of the sapphire window. At the center of the cap, a hole allows the IR rays to reach the detector. Because the 3D printer has a limited resolution, the minimal achieved clean hole diameter was 1 mm. A sapphire ball lens of $E = 2.78\,mm$ in diameter is also inserted in the cap to

focus the IR radiations on the active area of the detector.

Much smaller hole size were however achieved by printing vias on flexible PCB substrates (not presented in fig 3.5). Those vias were designed with sub millimeter diameters and a pad size corresponding to the diameter of the cap. While the via lets the IR light pass, the metal of the pad reflects all the emissions from the surroundings, therefore ensuring the IR proofness of the cap. The flexible PCB substrates were then glued to the 3D printed piece, making sure holes from the cap and the via were perfectly aligned with the sensitive area of the detector. This process allowed to design holes as small as 160 μm in diameter. In the absence of the flexible PCB pads, the printed cap must be coated with an absorbent material in order to prevent any IR radiation from getting through the PLA (polylactic acid).

Once the optic is installed the focused area on the circuit has to be computed differently. The tip of the optic, that is equipped with the hole and the lens, can no longer be considered punctual due to its proximity with the circuit. In addition, the numerical aperture of the optic, that defines its field of view FOV', must also be calculated. The diameter of the focused area D' is the sum of the hole diameter, $h_{\varnothing}$, and twice the lateral distance seen by the numerical aperture of the lens: $2 \times d_3$ (see fig. 3.5). Eq. (3.3) and (3.4) provide the formulas to compute the FOV of the optic. Then eq. (3.5) computes the diameter of the focused area using the designed optical system.

$$NA = \frac{2 \cdot h_{\varnothing} \cdot (n_{lens} - 1)}{n_{lens} \cdot E} \tag{3.3}$$

$$\frac{FOV'}{2} = n_{air} \cdot NA \tag{3.4}$$

$$D' = h_{\varnothing} + 2 \cdot d_3 = h_{\varnothing} + 2 \cdot d_2 \cdot tan(\frac{FOV''}{2}) \tag{3.5}$$

In these equations, n_{lens} and n_{air} are respectively the refractive index of the lens and air, NA is the numerical aperture of the lens and FOV' its field of view. All remaining distances are defined fig. 3.5. Note that in this figure, d_2 is voluntarily exaggerated for readability reasons.

Table 3.1 presents values of D (no optic) and D' for various distances d_2 and different cap hole size. As expected, the smallest focused area is obtained with the minimum hole size and $d_2 = 0$.

Obviously, a trade-off exists between the spatial resolution which is linked to the cap opening size and the quantity of IR received by the sensor. A too small aperture decreases the SNR as the detector receives smaller quantities of light. To find the

d_2 \ ⌀ hole	no optic	160 μm	300 μm	500 μm
$d_2 = 0\mu m$	1759.8μm	160 μm	300 μm	500 μm
$d_2 = 250\mu m$	2048.4μm	185 μm	347.2 μm	579.2 μm
$d_2 = 500\mu m$	2337.1μm	210.2 μm	394.4 μm	658.4 μm

TABLE 3.1: Values of D and D′ for different values of the parameter d_2 and aperture sizes.

aperture that produces optimum detectivity and spatial resolution, several cap designs are assembled with different opening sizes. A test circuit is then implemented on a Xilinx Virtex 5 FPGA in order to compare results from the different optics. To save time only a small portion of the circuit is mapped. Five heat sources of different power consumptions are implemented on the circuit and are mapped using the presented platform. Each thermal source is composed of 3-gate ring oscillators (RO). To allow the use of lock-in thermography, each source is gated with an enable input. Various numbers of ROs are then used to generate the different power consumptions. Table 3.2 gives the power consumption and the number ROs for each heat source.

Source	1	2	3	4	5
Number of ROs	1	2	4	8	16
Power consumption	200μW	400μW	800μW	1600μW	3200μW

TABLE 3.2: Power consumption of each thermal source mapped in fig. 3.6.

The acquired thermal maps are presented in fig. 3.6. Original location of the heat sources are represented by black or white rectangles on the thermal maps. Thermal maps a) and b) show that when no optics are used, the spatial resolution is quite poor as none of the epicenter of any heat source is visible. Instead, a global area of several millimeter square shows the approximate position of the five sources. Thermal maps c) through j) show, as expected, that the spacial resolution is improved when the size of the cap opening decreases. However images i) and j) reveal that in the event of very small apertures, some low power thermal sources can be missed. This is the case for the weakest source located on the left of the circuit that is barely detected using the smallest aperture. Therefore, for this platform, the optimum aperture size is found to be 300 μm. For this reason, images g) and h) provide median filtered maps to reduce the salt and pepper effect. This way, the readability of the thermal maps is improved.

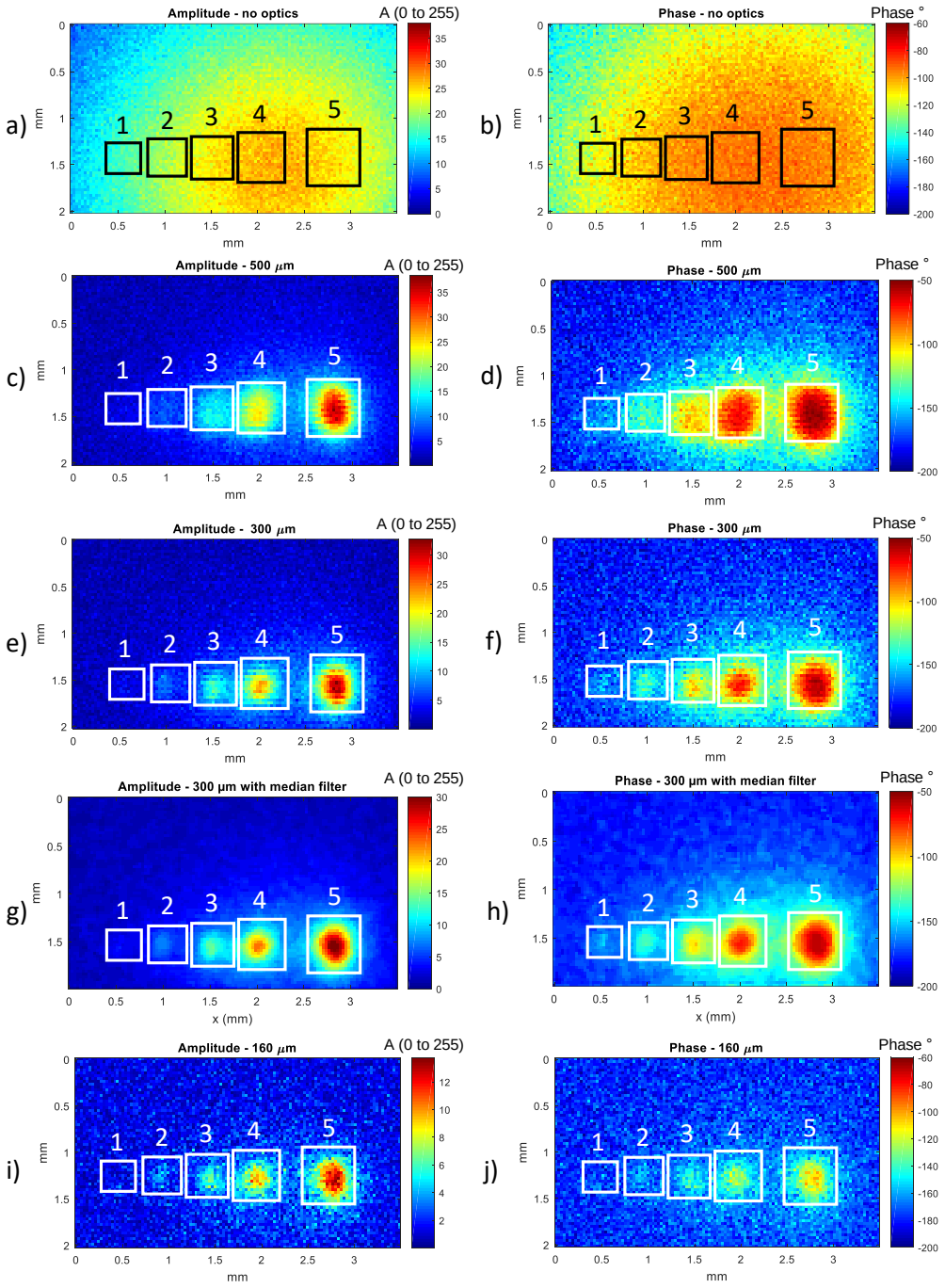


FIGURE 3.6: Thermal maps for different cap opening sizes of five heat source of different power consumptions.

3.3 Thermal Measurements

3.3.1 Thermal Modulation Techniques

This section aims at providing more details on the thermal modulation required to apply lock-in correlation on the measurements. The lock-in modulation aims at

transforming a DC power consumption into a low frequency AC one. This remains valid if the original instantaneous power consumption is fast enough to be assimilated to an averaged DC one. During the thermal modulation two phases can be distinguished. First, an increase in thermal activity (power consumption) is generated and corresponds to the heating phase. Then, the previous thermal activity is stopped. The generated heat dissipates, mostly by lateral conduction, and creates the cooling phase. In order to maximize the amplitude located at the lock-in frequency, a 50% duty cycle is preferred.

The original and most common modulation method is the one used in [BWL10c] where the DC supply voltage is superimposed with a low frequency AC signal. In this case the power consumption is modulated over the whole circuit. It is efficient for failure identification and in particular for resistive paths identification [SAB12]. Yet, the lack of selectiveness remains a problem as strong hot spot are likely to conceal the activity of weaker ones. In addition, this methodology is efficient on architectures where no power regulation is implemented on the die. Other architectures such as SoCs or FPGAs are often equipped with voltage regulators to prevent any fault due to unstable power supply. These regulators can be either directly implemented on the silicon die or be external like on most FPGA boards. The latter can however be removed but at the price of intervening physically on the DUT's board.

Digital complex circuits rely on a digital system clock to operate. To reduce power consumption, peripherals and/or macro blocks are generally clock gated [SS11]. Therefore, another global modulation technique consists in gating the system clock in order to enable periodical transistor activity. On FPGAs this solution proved to be quite efficient as it is possible to target a specific group of slices by building separated clock branches. Alternativelly, it is generally possible to control the clock speed through PLLs circuits. One can hence generate two phases of different power consumptions, depending on the clock speed. As a consequence, this enables specific operation targeting on the DUT and leads to more precise thermal maps.

SoCs and micro-controllers are software programmable circuits. This means that the power consumption can also be modulated using code implementation. In this case, a peripheral is repeatedly activated to generate thermal activity and then left idle during the same amount of time. This is a powerful method as it allows to pinpoint the location of any peripheral on the die, even if they are very low power. Both clock gating and instruction based modulation implies that it is synchronized to the system clock. This property can be exploited in the context of process, voltage and temperature robustness and is further investigated in chapter 4 section 4.2.2.

The ability to localize any peripheral or active block on the die is a major feature proposed by lock-in thermography. However, the contrast and SNR of low power

thermal maps can be limited, thus, the automated extraction of areas of interest from thermal map could become a powerful feature of such analysis. The next section proposes several methods to do so, relying on particular properties of lock-in phase statistical distributions.

3.3.2 Phase Values

Phase values represent the delay existing between the activation of the thermal source and the moment it is detected by the sensor. It is thus linked to the temporal aspect of heat propagation within the circuit. Let us consider a unique punctual thermal source in a die. Chronologically, the first detected IR radiations are emitted from the area located on the surface at the vertical of the hot spot. Then, secondary areas, due to thermal diffusion, appear as concentric circles around the surface epicenter. This phenomenon manifests itself on amplitude maps by progressive decrease of the thermal IR magnitude from the thermal origin. On phase values, the link to power consumption is lost and areas are differentiated by timing variations in regard of the lock-in trigger.

Traditionally, the lock-in correlation uses S_0 and S_{90} images to obtain amplitude and phase values. From these measurements, it is possible to compute all the intermediary thermal wave components $S_0, S_1, ..., S_{360}$ at any phase position. In [BWL10c], the author proposes to do so using eq. (3.6):

$$S_{\Phi'} = A \cdot cos(\Phi' - \Phi) \tag{3.6}$$

where Φ' is the component at the desired phase and Φ is the measured lock-in phase. This allows to build a time laps of heat propagation in the circuit.

Alternatively, it is possible to temporally filter thermal events using only the phase values of a thermal map. The particularity of phase analysis is that it provides only temporal data on the acquired signal. Displaying phase maps on a small sliding phase interval reveals each thermal event separately in chronological order.

Both methods allow to sort lateral diffusion from original thermal information which is a significant improvement for spatial resolution and heat detection. First, these methods provide the ability to confirm that observed sets of measurements are issued from thermal IR emissions and not from ambient noise (light, 50 Hz power grid, temperature drift, etc). Thermally modulated locations are expected to primarily appear as punctual and then spread to the surroundings on the heating sequence of the lock-in cycle. On the cooling sequence, these same locations are to progressively vanish from the epicenter to the outskirts of the diffusion area. Secondly, diffusion areas impairing readability and spatial resolution of the displayed results can

be filtered out. Thus, final thermal images are much more precise as only relevant information are presented.

Illustration of the mentioned "thermal propagation time laps" is given in fig. 3.7. Thermal images are obtained using the filtering method on phase values. In this experiment, the observed thermal activity is the one of an AES design, at $f_{lockin} = 10\,Hz$. On top of each figure, the phase window corresponding to the displayed measurement is given.

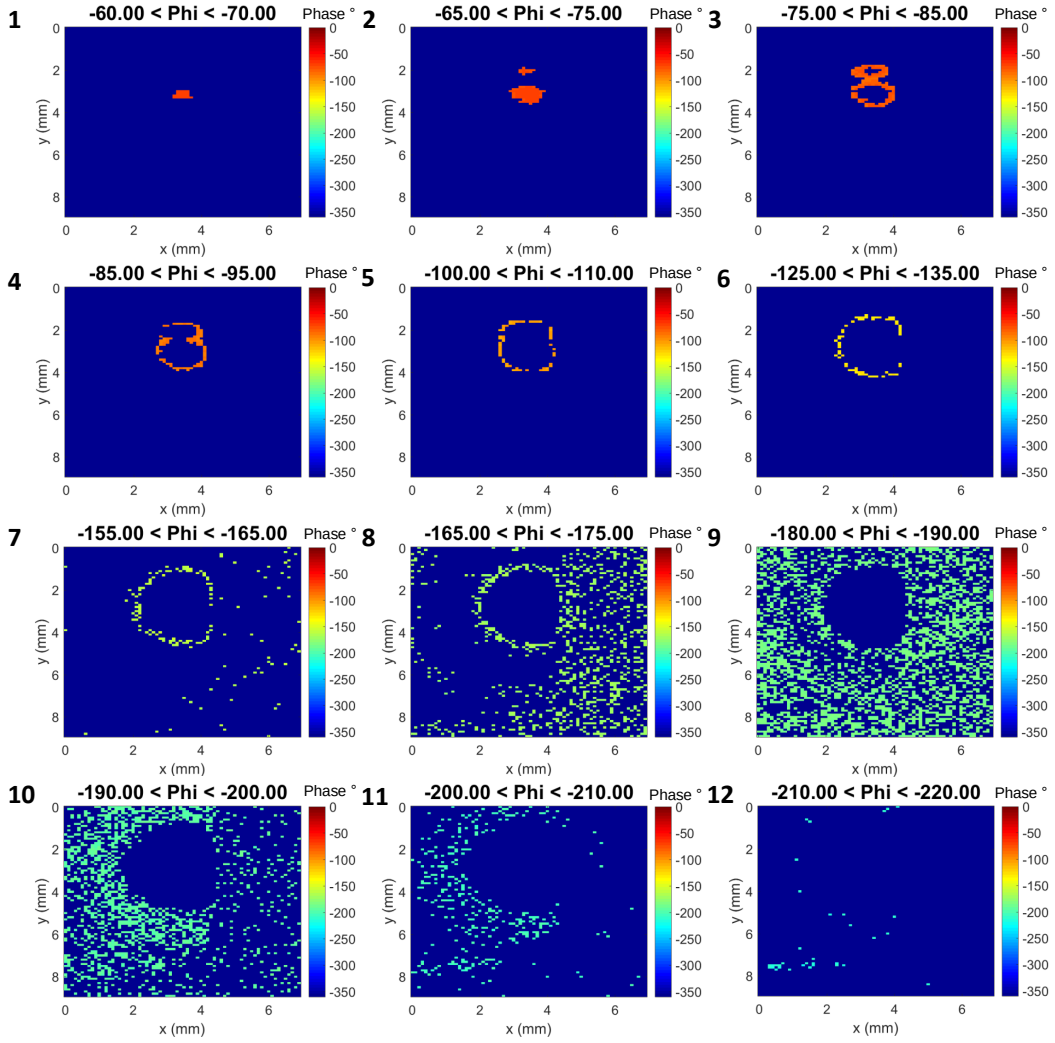


FIGURE 3.7: Reconstructed time laps of thermal propagation in the die. Results are obtained by displaying phase values on a 10° sliding window over the $[0°, -360°]$ domain.

3.3.3 Signal Detection Criteria

When applying lock-in correlation, amplitude and phase values are computed from S_0 and S_{90} images. As shown in eq. (3.1) the in-phase and quadrature images are traditionally computed over several lock-in periods to reduce noise (averaging

process). In this section, it is chosen to repeatedly compute lock-in values over single periods in order to construct statistical sample sets for each pixel. Instead of computing one lock-in output over N measurements, N lock-in values are obtained for each acquired trace of N lock-in period. It is then demonstrated that phase measurements are of particular interest over amplitude ones due to the finite range of their values.

Statistical Distributions of Lock-in Values

Phase values are computed modulo 360°. In the presence of a thermal signal, the computed phase depends on the delay between the trigger of the thermal source and its detection by the IR sensor. However, in the absence of any thermal source, the acquired signal is constituted of noise only. Because the lock-in computation systematically provides a result, one can expect its value to be uniformly distributed over the $[-360°,\ 0°]$ interval. Inversely, the stronger the heat source under the sensor, the closer to a Gaussian distribution are phase measurements.

To verify this assumption, the lock-in correlation is applied to a trace constituted of Gaussian noise only. For that, $n = 10^8$ samples are generated randomly from a Gaussian distribution of mean $\mu_t = 0$ and of standard deviation $\sigma_t = 20$. To be representative of the results further presented in this chapter, the lock-in frequency is chosen at $f_{lockin} = 10\,Hz$. This way, 1000 lock-in values are computed over periods of 10^5 samples. The same computation is then reiterated with a $10\,Hz$ sinusoidal signal added to the noise. The sinus possesses an amplitude of $A_e = 0.5$ and a phase of $\Phi_e = -30°$. Resulting distributions of amplitude and phase values are given in fig. 3.8.

As hypothesized, when the signal is constituted of noise only, phase values are uniformly distributed on the $[-360°,\ 0°]$ interval (fig. 3.8.b). Looking at the amplitude distribution fig. 3.8.a, one can notice that it is not exactly Gaussian. Amplitude is of quadratic nature (eq. 3.1), and so, necessarily positive. Thus, when no signal is present at the lock-in frequency the amplitude distributions cannot be centered on zero. For that reason, the log-normal distribution is generally more suitable for this kind of data.

In the case where the $10\,Hz$ sinus is added, fig. 3.8.c and 3.8.d show normally distributed results. Their means correspond respectively to the predefined amplitude $A_t = 0.5$ and phase $\Phi_t = -30°$ of the sinus, confirming the ability of lock-in correlation to extract signals buried into noise.

To experimentally confirm these results, a data set of 1000 lock-in values (amplitude and phase) is acquired using a fixed position over the DUT. In the first case, the

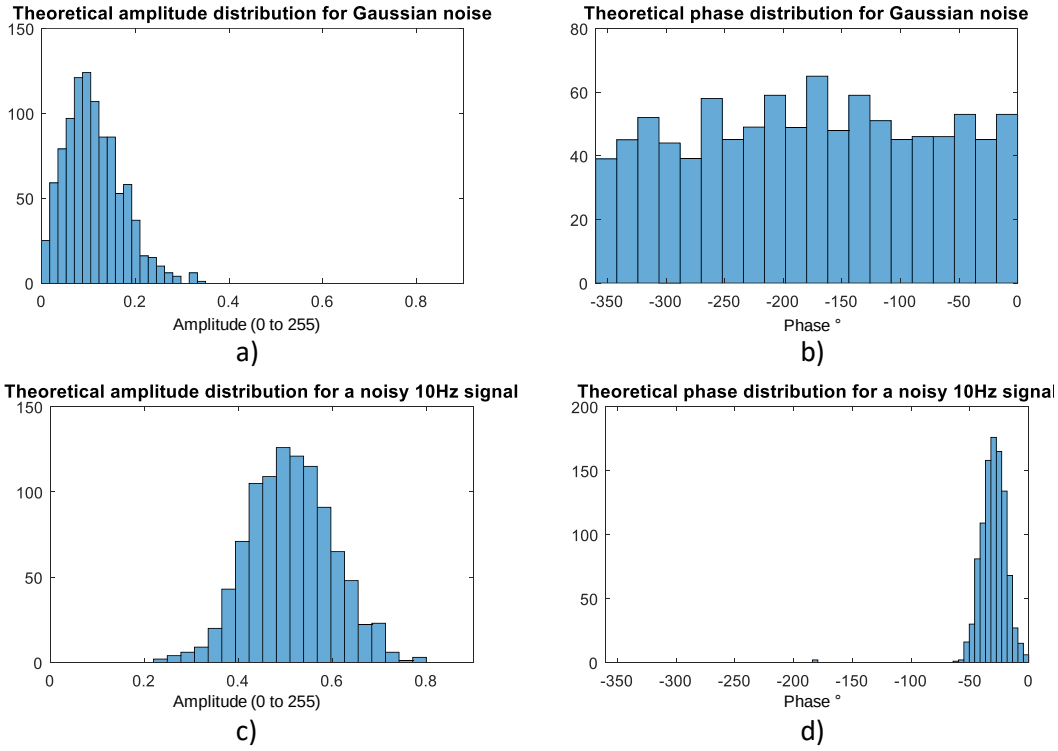


FIGURE 3.8: Theoretical distribution of lock-in values for a "no signal" trace constituted of Gaussian noise.

thermal source under the detector remains inactive, the acquired signals are therefore only constituted of noise. In the second case, the thermal source is activated and thus emits IR signals. The obtained statistical distributions are given fig. 3.9. Here again, when no thermal emissions is detected at the lock-in frequency, phase measurements are uniformly distributed over $[-360°,\ 0°]$. If thermal activity is detected, both amplitude and phase values are normally distributed.

Fig. 3.9.a shows that the corresponding amplitude distribution is centered on a much higher value than during the theoretical study. As both the theoretical and the experimental trace are computed using the same script, this offset is most likely generated by a non Gaussian noise present during the experiment. This noise is canceled when classical lock-in correlation is applied and appears when lock-in values are computed on single periods to build statistical distributions of amplitude and phase. Instead of obtaining two averaged images S_0 and S_{90}, N images are obtained respectively for the in phase data (S_0) and the shifted phase (S_{90}) data. Because amplitude is of quadratic nature, computed amplitudes are spread on a larger interval, resulting in an offset when computing its mean.

In the case where the thermal source is deactivated (fig. 3.9.a), the averaged amplitude gives $\overline{A} = 6.04$. Hence, this offset is susceptible to impair weak sources detection, as any lower thermal amplitude would be mistaken for noise. Best result are therefore obtained on phase values which possess much more interesting

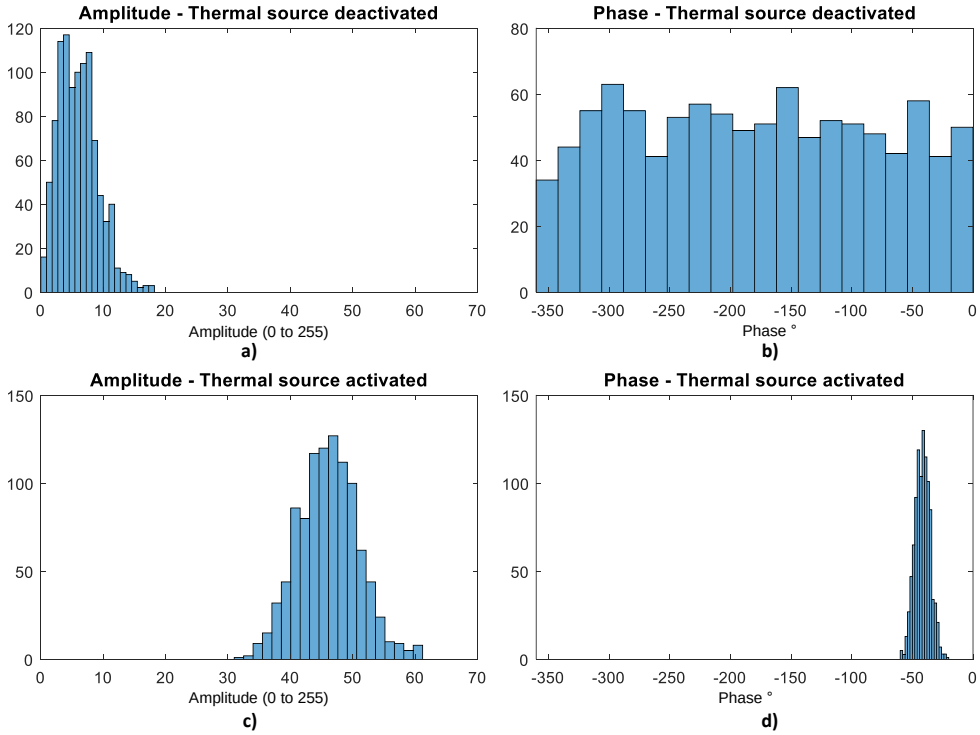


FIGURE 3.9: Comparison of amplitude and phase statistical distributions when the thermal source is deactivated (top) versus when it is activated (bottom).

features.

Fig. 3.8.b and fig. 3.9. b show that in the absence of thermal information, the phase distribution is homogeneously spread on the $[-360°,\ 0°]$ interval and thus follows an uniform distribution. This means that enormous differences in variance can be observed between measurements over a thermal source and measurements over an inactive part of the circuit. That difference can then be exploited in order to highlight locations with thermal activity modulated at the lock-in frequency. The closer the variance of the measured distribution is to $\frac{-360^2}{12}$, the less thermal information there is in the acquired sample set. The previous dataset illustrates this phenomenon by having a variance $V_{\Phi_{Sig}} = 39.34$ when the source is active versus $V_{\Phi_{NoSig}} = \frac{-360^2}{12} = 10800$ when the thermal source is inactive.

Displaying raw images of the mean phase might also be problematic. Due to its uniformity and in the absence of signal, corresponding measurements are located around $\overline{\Phi}_{NoSig} = -180°$. In contrast, if the activity of the investigated thermal source is synchronized to the lock-in frequency, the phase is necessarily in $[-180°,\ 0°]$. However, several cases may generate phases around $-180°$ thus leading to misinterpretation of the experimental data. If a low power source or a thick circuit is investigated, the generated heat can take longer than usual to reach the detector thus implying a longer delay. Also, it happens that the investigated source is in

phase opposition with the lock-in modulation. The associated phase is then comprised in $[-360°, -180°]$. Under those circumstances, the mean of the lock-in phase is likely to be close to $\overline{\Phi}_{NoSig} = -180°$. The resulting image should thus suffer from very poor contrast due to the algebraic proximity between $\overline{\Phi_{Sig}}$ and $\overline{\Phi_{NoSig}}$. Criteria to separate pixels containing thermal information from inactive pixels are therefore required.

It is demonstrated that statistical parameters such as mean and variance are affected by the quantity of detected signal. Classical methodologies rely on human interpretation of color contrast to localize thermal activity area. Hence, obtained results are often subjective. It is found that statistics are an effective tool to dig out small variations in distributions as they rely on mathematical processes to identify variations. In the next paragraphs, several methods relying on statistical analysis are presented to automatically extract locations containing thermal lock-in information.

Variance Criterion

This first criterion is a naive computation of the variance of each pixel's sample set. To test the signal extraction criterion, an AES running on a Xilinx Virtex 5 FPGA has been implemented. The design performs continuous ciphering operations. Its thermal emissions were then modulated by gating the clock of the AES circuit at 20 Hz. In order to have a consequent amount of points containing thermal information and reasonable experiment durations, only the region containing the design has been mapped. In this experiment, the optical system possesses a 1 mm aperture.

Fig. 3.10 compares maps obtained when computing the mean, the variance, and the standard deviation of the phase measurements. The strongest thermal source is

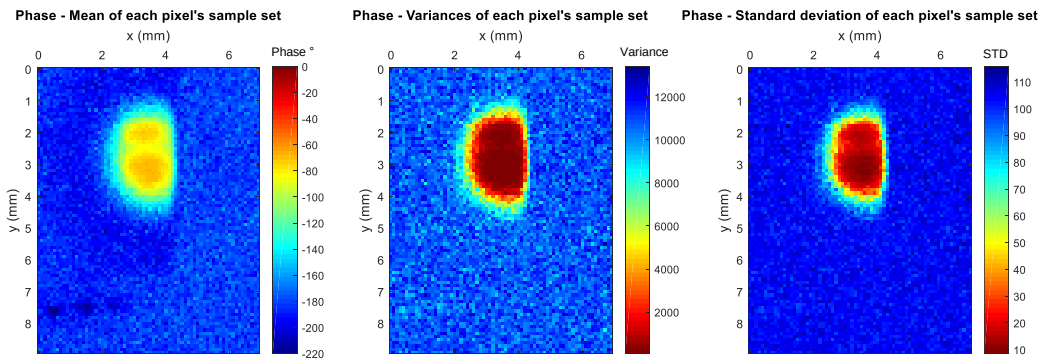


FIGURE 3.10: Comparing mean, variance, and standard deviation heat maps for phase measurements.

the AES and is located at the center of the thermal map. Small additional sources are slightly visible on the bottom left corner and are related to the clock gating circuitry.

Without additional details on the layout of the die, it is not possible to determine their origin. Nonetheless, it is known from the amplitude map that they are of very weak amplitude. Even without knowing their origin, these weak and very local heat sources are useful to test the performances of the signal identification criteria. Note that according to fig. 3.9 the variance and the standard deviation of phase measurements are inversely proportional to the presence of thermal information. Consequently, the color bars have been inverted on the concerned thermal maps to respect the color code of the other displayed images.

Results show that variance and standard deviation maps provide efficient detection on strong heat sources. Because the standard deviation is the square root of variance, applying it on thermal maps provides better contrast due to the smaller scale of its output values and is thus easier to display on a colored map.

Interestingly, the link to power consumption, absent from raw phase measurements, is restored by this criterion. As the SNR decreases, weaker thermal sources tend being a mixture of the uniform and the normal distributions. The variance of this mixture is therefore higher than the one of strong thermal sources but smaller than the zero signal uniform distribution.

Yet, hot spots of very small power consumption tend to not be detected by this criterion. This is the case for the previously mentioned bottom left sources. Accordingly, this method is better suited to detect relatively strong power consumptions ($> 2\,mW$). In addition, even if contrast is globally improved, it is still up to the observer to decide if a pixel contains thermal information.

Reference Point Comparison

Two-sample statistical tests allow the comparison of two set of samples (e.g. X_1 and X_2) for a statistical parameter (mean, variance, goodness of fit, etc) under the hypothesis H_0 that the parameter is equal for both data samples. Each test produces a score that falls into a known distribution. It is therefore possible to compute, for each score, the probability P, under the H_0 hypothesis, to have a higher or lower value than the obtained score. A confidence level $\alpha = 1 - P_{crit}$ is then chosen to decide under which probability, P_{crit}, H_0 is accepted or rejected. Typically, α is set to 5% or 1%. For a given confidence level and data set length, a critical statistic is obtained above which H_0 is rejected and H_1 (the parameter is not equal) accepted.

The analysis of amplitude distributions shows that the mean is the parameter affected by thermal activity. For that reason, the two-sample Welch t-test is applied. Using a reference point, the objective is to discover slight changes of the mean of experimental distributions to assert if thermal information is present at the investigated location. As sample sets can be of different sizes, the reference point can be

built by drawing samples from a theoretical distribution or from an experimental one. Choosing a zero signal reference and looking at points failing the test enables to find all locations where the power consumption is modulated at f_{lockin}. Alternatively, setting the reference on a location with thermal information and observing locations passing the test provides equipotential areas (same thermal activity). For amplitude values it is equivalent to revealing areas of equal IR emissions.

Welch's t-test compares the mean of two samples by computing the following statistic:

$$t = \frac{\overline{X}_1 - \overline{X}_2}{\sqrt{\frac{V_1^2}{n_1} + \frac{V_2^2}{n_2}}} \tag{3.7}$$

where $\overline{X}_1$ and $\overline{X}_2$ are the sample sets' means, V_1 and V_2 the associated estimated variances, n_1 and n_2 are the compared data sample sizes [Wel47]. The statistic t is the output of the test and images the difference between the mean of the two data sets. Here, Welch's t-test is bilateral which means that t-values are signed. Positive values correspond to locations with more thermal activity than the reference while negative values correspond to locations of inferior thermal activity.

Using the confidence level α, it is then possible to influence the strictness of the test. Fig. 3.11 presents results when the t-test is applied to the amplitude map, taking the top left pixel as a no signal reference. Image 3.11.a and 3.11.b provide respectively the classical amplitude map as a reference and the t-value map. Fig. 3.11.c and 3.11.d show the binary map of the pixels passing or failing the t-test for $\alpha = 0.01$ and $\alpha = 0.0001$. Here again, the methodology is quite efficient for strong thermal sources but smaller ones as those located in the bottom left corner remain undetected. Nonetheless, contrarily to the variance criterion, thermal sources are statistically identified by the test.

The two-sample Fisher test allows comparing the variance of two distributions and is thus quite adapted to analyze phase distributions. Its statistic is computed as follows [SC67]:

$$f = \frac{V_1^2}{V_2^2} \tag{3.8}$$

where V_1 and V_2 are the estimated variances of each population and f is the output Fisher statistic. This test is however reserved for Gaussian type sample sets and can only be applied to positions where thermal signal is detected. The Fisher test is thus adapted to display the earlier mentioned equipotentials. Results displayed in fig. 3.12 show all pixels where the phase is equal to $\Phi = -192°$, $\Phi = -169°$ and $\Phi = -75°$ respectively. In particular, this result brings forward the heat propagation phenomenon and its temporal evolution on the die. Similarly to results presented in section 3.3.2, it is thus possible to recover the precise location of the epicenter of a heat source and all the simultaneous events on the circuit. This principle is demonstrated in image 3.11.c where the top group of points correspond to the origin

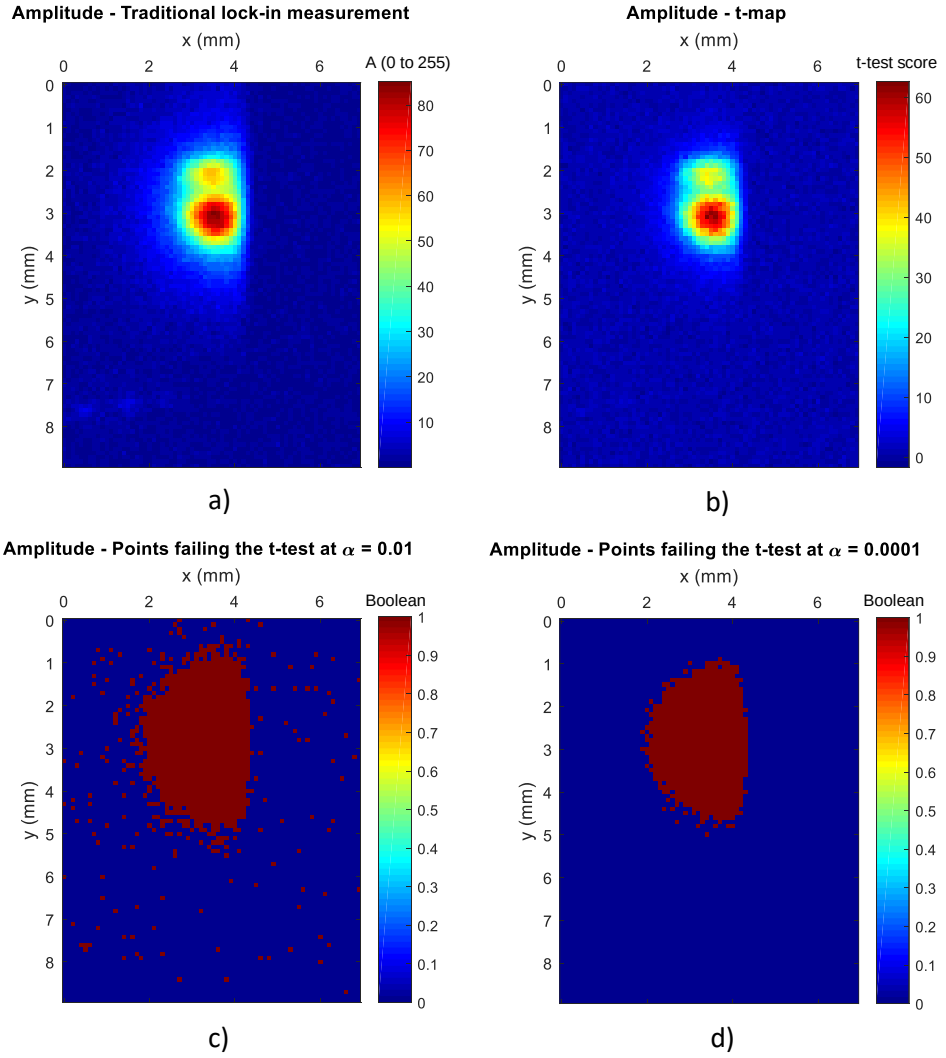


FIGURE 3.11: Application of the t-test between the distributions at each pixel and a no signal reference point. **a)** Classical lock-in measurements **b)** t-value map **c)** Failing points at $\alpha = 0.01$ **d)** Failing points at $\alpha = 0.0001$.

of the upper thermal signature of the AES.

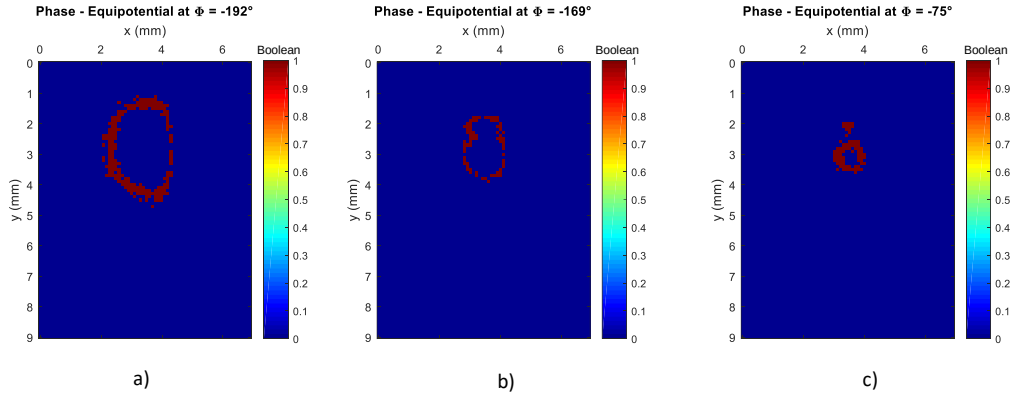


FIGURE 3.12: Displaying phase equipotentials using Fisher's variance test.

In the end, mean and variance tests provide interesting results but globally lack the ability to detect weak heat sources. For this reason, the next section introduces a third test that estimates how good a statistical model fits a set of observation.

Goodness of Fit Tests

Another approach to differentiate active areas from inactive ones is to compare whole distributions instead of associated parameters such as mean or variance. It has been previously demonstrated that phase measurements have different population types depending on the amount of thermal information they embed. This means that their cumulative distribution function (CDF) also differ. Using a no signal reference population measurement, it is then possible to compare each acquired sample-set to verify the distribution matching. In this objective, the two samples Kolmogorov – Smirnov (KS) goodness of fit test is applied. The statistic of this test is:

$$ks = \sup_x |F_1(x) - F_2(x)| \tag{3.9}$$

where F_1 and F_2 are the empirical cumulative distribution functions of the two data sets to compare. Applying this test, any distribution different than the reference empirical uniform one is identified as containing thermal lock-in information.

As presented in fig. 3.13, this test is able to retrieve all locations where the AES is active similarly to its predecessors. In addition, very weak heat sources as the one on the bottom left corner of the thermal maps are also identified as carrying useful information. It must also be noted that for a given confidence level α, the salt and pepper effect due to false positive identification is reduce by using the KS test. This methodology is therefore well adapted to the investigation of low power thermal emissions. Here again, because thermal information is retrieved using statistical tests, the final results are independent of the observer and provide objective results depending only on the initial chosen confidence level.

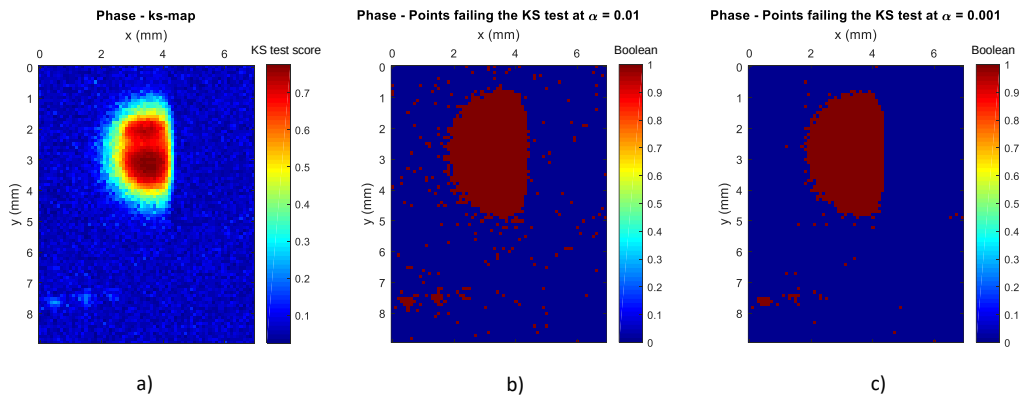


FIGURE 3.13: Precise identification of thermal activity using the KS test. **a)** ks-value map **b)** Failing points at $\alpha = 0.05$ **c)** Failing points at $\alpha = 0.01$.

Enhanced lock-in images

Even if they present different aspects of the thermal signal, amplitude and phase values are spatially coherent. This means that the results of the previous goodness of fit test can also be applied to amplitude in order to enhance the quality of the thermal maps or only display relevant thermal information.

In the case where genuine lock-in values are required, the binary output of the KS test can be applied as a mask to the thermal image. Mathematically, the mask and the mean lock-in map are considered as 2D matrices of same dimensions. This means that they can be multiplied element wise. In the following, $\overline{A}(x,y)$ is the mean amplitude and $KS_{BinMask}(x,y)$ is the binary output of the KS test displayed in fig. 3.13 c). Similarly, $\overline{\Phi}(x,y)$ is the mean phase for a given pixel. (x,y) represents the coordinates of the considered pixel on the thermal map. The enhanced images $A_{masked}(x,y)$ and $\Phi_{masked}(x,y)$ are computed as:

$$\begin{aligned} A_{masked}(x,y) &= \overline{A}(x,y) \cdot KS_{BinMask}(x,y) \\ \Phi_{masked}(x,y) &= \overline{\Phi}(x,y) \cdot KS_{BinMask}(x,y) \end{aligned} \tag{3.10}$$

Following on eq. (3.10), all locations deprived of thermal activity are reduced to zero while areas of interest are kept to the original measured lock-in value. This has for main effect to eliminate the background noise an thus improve the readability of the thermal map. As phase maps do not exactly posses a zero signal value, it can be chosen to set them either to 0° or 360°.

Alternatively, if the experiment aims only at retrieving the location of thermal sources, the KS statistical map given in fig. 3.13.a, can be used to ponder individually each pixel of the amplitude map:

$$\begin{aligned} A_{weight}(x,y) &= \frac{1}{\underset{(x,y)}{max}\left(\frac{\overline{A}(x,y)}{KS_{stat}(x,y)}\right)} \cdot \frac{\overline{A}(x,y)}{KS_{stat}(x,y)} \\ \Phi_{weight}(x,y) &= \frac{1}{\underset{(x,y)}{min}\left(\frac{\overline{\Phi}(x,y)}{KS_{stat}(x,y)}\right)} \cdot \frac{\overline{\Phi}(x,y)}{KS_{stat}(x,y)} \end{aligned} \tag{3.11}$$

In eq. (3.11), KS_{stat} is the map of the output statistical score of the KS test. High values of the KS statistical output reveals thermal signal locations. Consequently, in A_{weight} pixels containing thermal information are represented by the lower values of the scale. Inversely, on phase maps, the pondered values of interest are the higher ones as computed values are negative. The normalization of the data allows the reduction of the value scale and thus provides a better contrast. The readability of the final heat map is therefore significantly enhanced compared to the one of fig. 3.10. Results of those two enhancing techniques are presented in fig. 3.14.

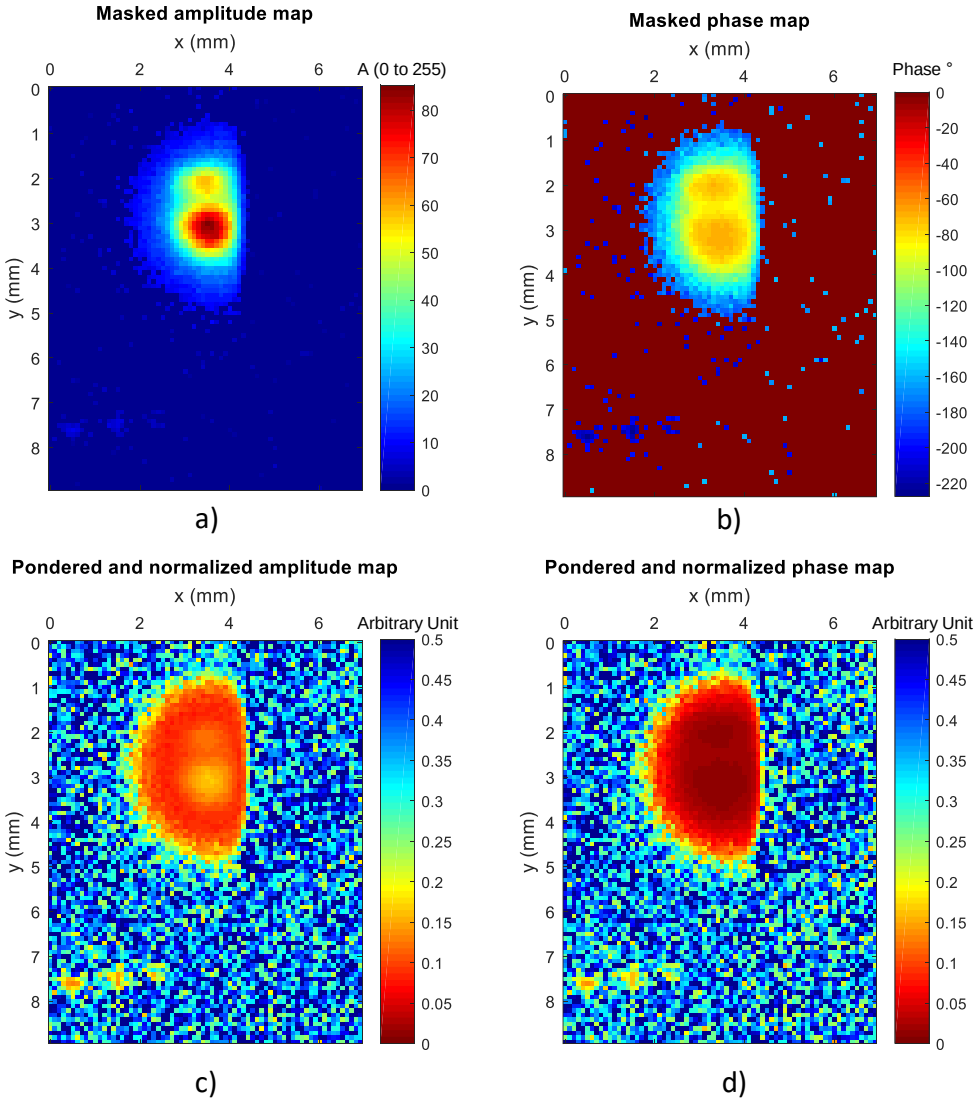


FIGURE 3.14: Results of the enhancement techniques. Top images represent amplitude and phase masked by the KS test's binary output while bottom images are the pondered-normalized ones.

As expected, the masking computation efficiently removes the background noise. Here again, the finite modulo range of phase values allows to choose on which side of the interval lies the "no signal" color. This explains why the phase image is easier to interpret. It can be noted that both amplitude and phase masked maps presents several statistical errors. These are due to the high number of performed test and can be suppressed by choosing a higher confidence level (smaller α) or by applying a 3×3 2D median filter.

Pondering the lock-in values by the KS test's statistic also proves to be efficient. The obtained images provide high contrast as all heat sources appear with approximately the same magnitude.

3.4 Platform Characterization and Test Cases

This section first presents limit capabilities of the developed IR platform applying the previously established KS test criterion. Detectivity and spatial resolution are presented along with the associated methodology. In a second part, real SoCs investigations are presented. The ability of the platform to locate thermal activity on commercialized circuits is thus demonstrated.

3.4.1 FPGA

Circuit Preparation

Before applying the developed IR scan methodology, the targeted circuit must go through several preparation steps to ensure maximum IR transmission. These include decapsulating the chip. The sensor is then placed as close as possible to the thermal sources in order to avoid lateral heat conduction in the packaging layers. Fig. 3.15 illustrates the main steps to access the silicon substrate of a Xilinx Virtex 5 FPGA. After removing both the heat sink and the metal lid, the chip must be cleaned from any residual thermal paste using acetone. These steps must be completed delicately in order to leave the silicon substrate undamaged. The diffraction created by scratches on the circuit can greatly disrupt the thermal IR analysis.

The studied die presents a standard thickness of 750 μm and is manufactured in 65 nm silicon technology. In some cases, it is possible to mechanically thin the substrate to reduce IR absorption and lateral heat spreading. However, this technique is quite expensive as it requires specialized equipment and presents high risks of damaging the chip. It is thus not applied in any of the experiments presented in this document.

Thermal Detection Limits

FPGAs are suitable targets to characterize imaging platforms. Modern tools provide several options allowing custom routing to emulate real SoC configurations. As the DUT usually requires decapsulation, being able to implement several designs in a single re-configurable chip is quite advantageous. Despite these assets, the density of FPGAs, event recent ones, remains problematic for thermal analysis. Transistor wise, FPGAs may be the most dense chip commercially available. However, many of these transistors implement the programmable functions of the chip and remain inactive from a dynamic power consumption point of view. The slices, which are the elementary blocks allowing the implementation of a design in a FPGA, present

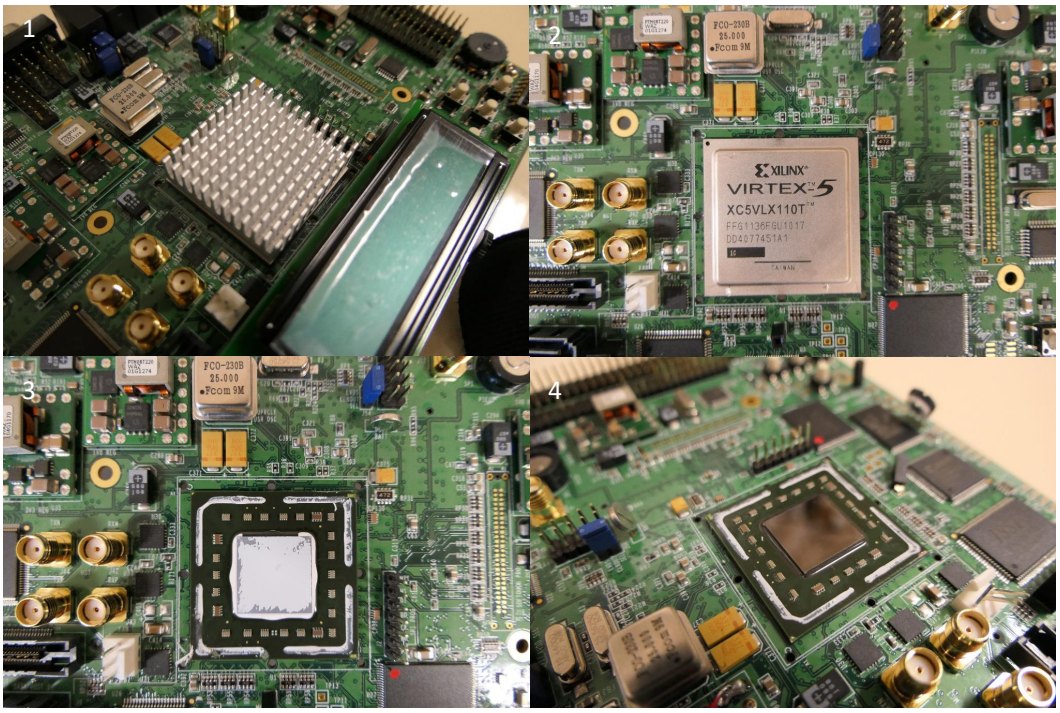


FIGURE 3.15: Decapsulation process of a flip-chip FPGA: **1.** heat sink removal **2.** uncaping the metal lid package **3.** Cleaning the thermal paste of the silicon substrate **4.** Final cleaned silicon die.

a much lower density. The thermal source is thus spread in series of high frequency small emissive patterns. From chapter 2 it is known that this kind of configuration is submitted to heavy attenuation as the total power consumption is divided on a wider surface. Due to the heat extraction problematic present in advanced silicon technologies, the performances of this platform are susceptible to improve as the transistors size diminishes. Consequently, the smallest detected power consumption provided in this paragraph is given as general indication of the performance of the platform.

The test circuit consists of groups of ROs routed together to implement micro-heaters of different power consumptions. Each RO is composed of three gates, two NOT gates and a NAND gate and consumes approximately 200 μA under the nominal core voltage 1 V. The power consumption of a single RO has been deduced from the one of 255 ROs measured both in activated and disabled states. This way, the DC power consumption of the die is not taken into account. The measured power consumption is hence divided by 255 to find the rough power consumption of a single RO.

The NAND gate allows us to implement an "enable" input which is controlled by a counter for lock-in thermal modulation. During this experiment, the activation signal of the micro-heaters is toggled at 10 Hz with a duty cycle of 50%. This means that the ROs are periodically active (respectively idle) for 50 ms. Five micro-heater

groups of various power consumptions are routed close to each other. The groups are formed of respectively, 1, 2, 4, 8, and 16 ROs. The $2\,mm \times 3.5\,mm$ area containing the targeted heat sources is then mapped using a step of $30\,\mu m$. For this experiment, a $300\,\mu m$ aperture optic is used.

Experimental results are presented in fig. 3.16. In a) and b), it displays images of traditional lock-in computation, confronted to the previously described statistical

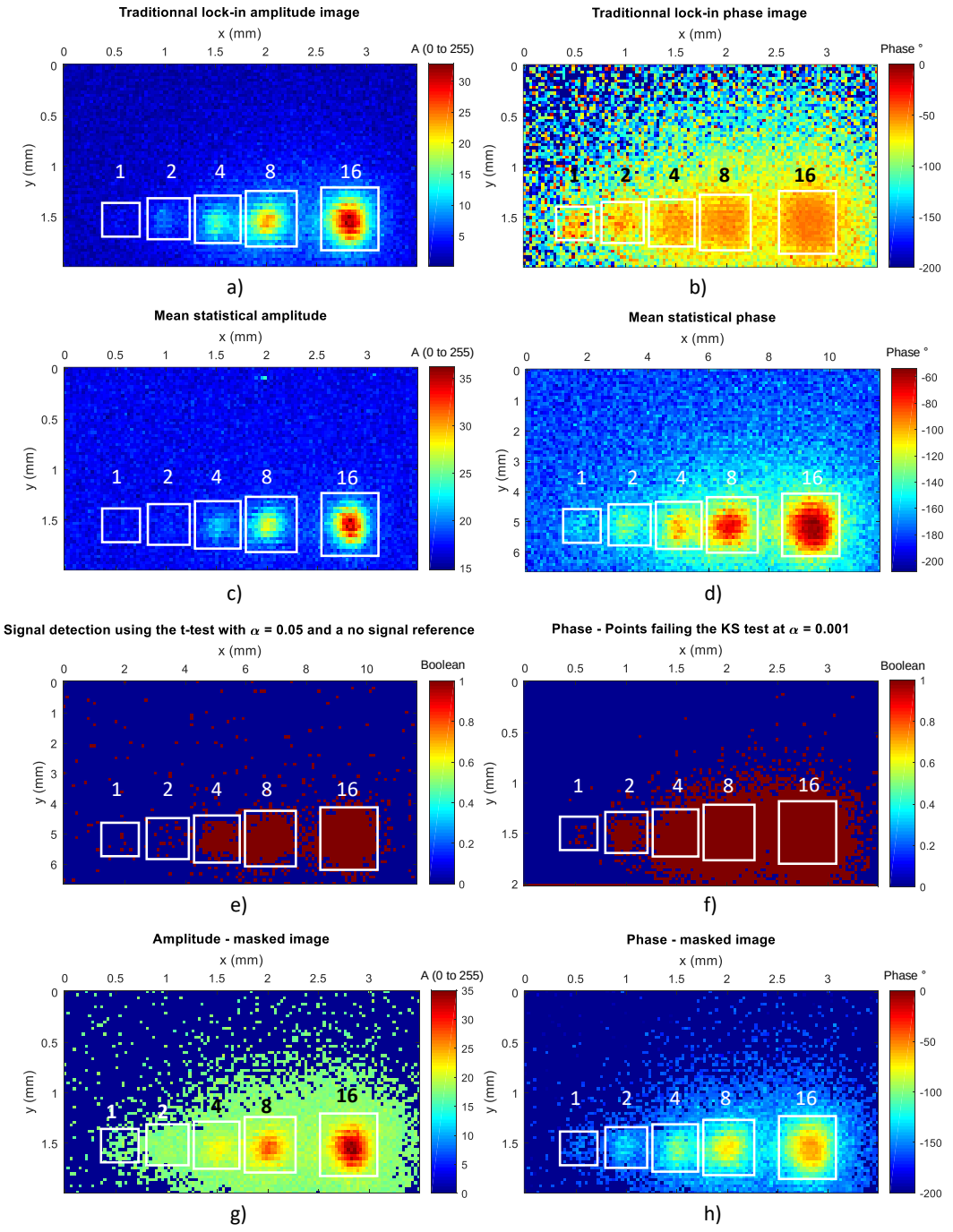


FIGURE 3.16: Comparison of the smallest detected power consumption using traditional lock-in, mean of each pixel's distribution and statistical tests.

lock-in methodology. Middle images c) and d) present thermal maps of the mean value of each pixel's distribution while bottom images e) and f) show the result of the signal detection criteria. Amplitude signal locations are determined using Welch t-test while the KS test is applied to phase value. In either case, the top left corner pixel is used as a no signal reference point.

As expected, the statistical thermal detection on amplitude values is bottlenecked by their distribution type, preventing the mean of a no signal location from being located near zero (see fig. 3.9). All measured values being under the offset value created by this phenomenon is therefore concealed. The minimal power consumption detectable by amplitude analysis is thus 800 μW (4 ROs). In comparison, phase analysis is much more powerful as it identifies power consumptions down to 200 μW, one quarter of what was achieved using amplitude measurements. Yet, this represents the very minimum power consumption detectable by this platform on this FPGA as even if sources are spatially separated, only a few points reveal the position of the one RO micro-heater thermal source.

Images g) and h) present enhanced lock-in thermal maps obtained using the previously described methodology. Thanks to the phase results and using the masking technique, all five sources are localized. The thermal sources composed of one and two ROs are however still considered as undetected because their identification rely on phase measurements detection capabilities.

It must be reminded that measurements are acquired using $f_{lockin} = 10\,Hz$. Many results presented in the state of the Art were acquired using lock-in frequencies inferior to 5 Hz [TBB+07, SASD10, BWL10a]. Reducing the lock-in frequency allows time for more heat to reach the surface of the die and thus maximize IR emissions. Smaller power consumptions can then be detected. In this case, it is however hard to generate a characterizable constant power consumption bellow 200 μW using a FPGA.

Spatial Resolution

Spatial resolution defines the ability to distinguish two separated sources in a thermal map. For IR images it is theoretically limited by the acquired wavelength because of diffraction effects. However, in practice the spatial resolution is often affected by other parameters which are, for this platform, the lock-in frequency, the aperture of the optic, and the thickness of the die. It is thus susceptible to vary, depending on the circuit that is investigated.

It is expected that amplitude and phase images possess different spatial resolutions. [BWL10a] and [BR] show that all signal components S_Φ do not decay equally

over the increasing distance from the source origin. By tracing radial profiles of thermal propagation in a homogeneous substrate, these works show that the S_{-90} signal drops linearly, hence slowly, while the S_0 component seems to drop exponentially. Thereby, the amplitude decays much faster than the phase with increasing distance from the source. This results in amplitude maps having a better spatial resolution than phase maps.

To measure the spatial resolution, two thermal sources constituted of 2 ROs are implemented on a Xilinx Virtex 5 FPGA. They are initially separated by a relatively great distance insuring that both thermal signatures are distinguishable. For each acquired thermal map, the distance separating the sources is progressively reduced, until no difference can be made between the thermal signatures. The last heat map where both hot spots are distinguishable is then representative of the spatial resolution of the platform. In this experiment, the lock-in frequency is set at $10\,Hz$, the aperture of the optic at $1\,mm$ and the measurement step at $50\,\mu m$. The lock-in thermal modulation is the one used in section 3.4.1. Because Xilinx does not provide any information of the layout of their circuits, the theoretical distance separating two slices is unknown prior to the experiment. Hence, for practical reasons, this value is called d_{slice} for the rest of the experiment.

Fig. 3.17 and fig. 3.18 present thermal maps where two sources are separated by different distances. Fig. 3.17.a and fig. 3.18.c represent the spatial resolution limit of the platform as both source thermal activity are on the verge of being merged. Graphs of the x axis signal topology is plotted for each thermal map. Each column of pixel of the image is hence averaged to form a vector representing the evolution of the signal along the axis formed by the two hot spots. Those graphs are presented fig. 3.17 b), d) and fig. 3.18 b), d).

One can notice that amplitude possesses a better resolution than phase. Fig. 3.17 a) shows that this platform is capable of distinguishing thermal sources separated by only $300\,\mu m$, representing $2 \times d_{slice}$ using amplitude maps. On this figure two additional lines of very weak thermal activity are also present on the thermal maps. According to the floorplan schematic provided in Xilinx ISE 14.7, it seems that these activities correspond to the location of RAM blocks. It is suspected that the emissivity contrast is responsible for theses thermal artifacts as memories possess dense metal layers susceptible to reflect IR emissions. This hypothesis is supported by the fact that nothing of the sort is identified on the phase map, which is free from any emissivity contrast. In the same configuration, the phase map (fig. 3.18.a) presents a unique hot spot where the thermal signature of both sources are merged.

Fig. 3.18.c shows that phase analysis allows to distinguish hot spots separated by at least $4 \times d_{slice}$. Nonetheless, it must be reminded that in this case both thermal sources are activated simultaneously. In the case where the source's activity is not

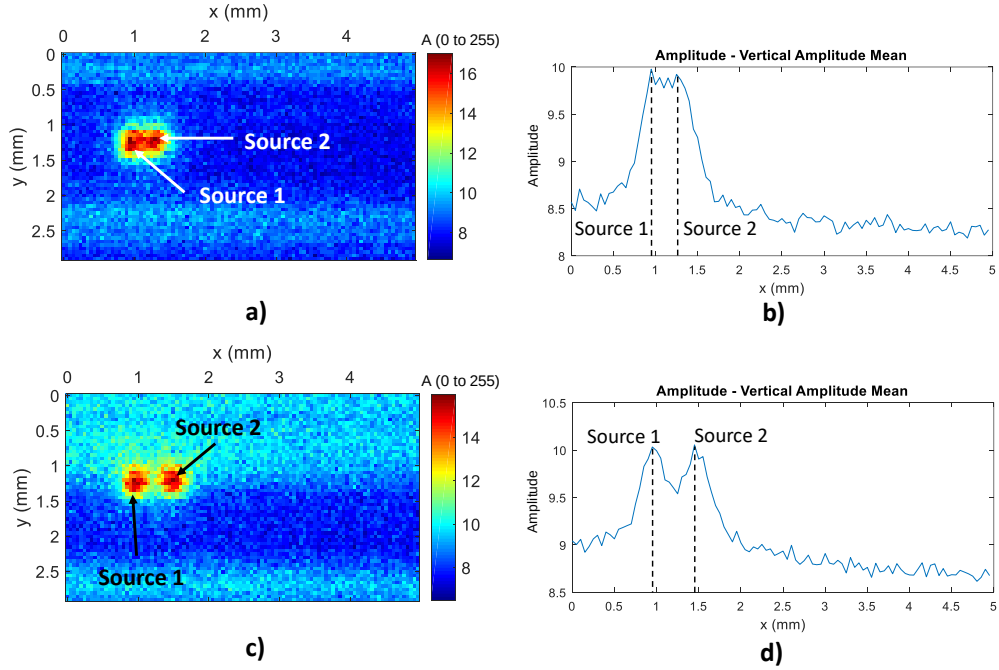


FIGURE 3.17: Measure of the spatial resolution for amplitude maps. **a)** Amplitude map showing thermal sources separated by two slices **b)** Vertical average of each pixel column of the amplitude map a) **c)** Amplitude map showing thermal sources separated by four slices **d)** Vertical average of each pixel column of the amplitude map c).

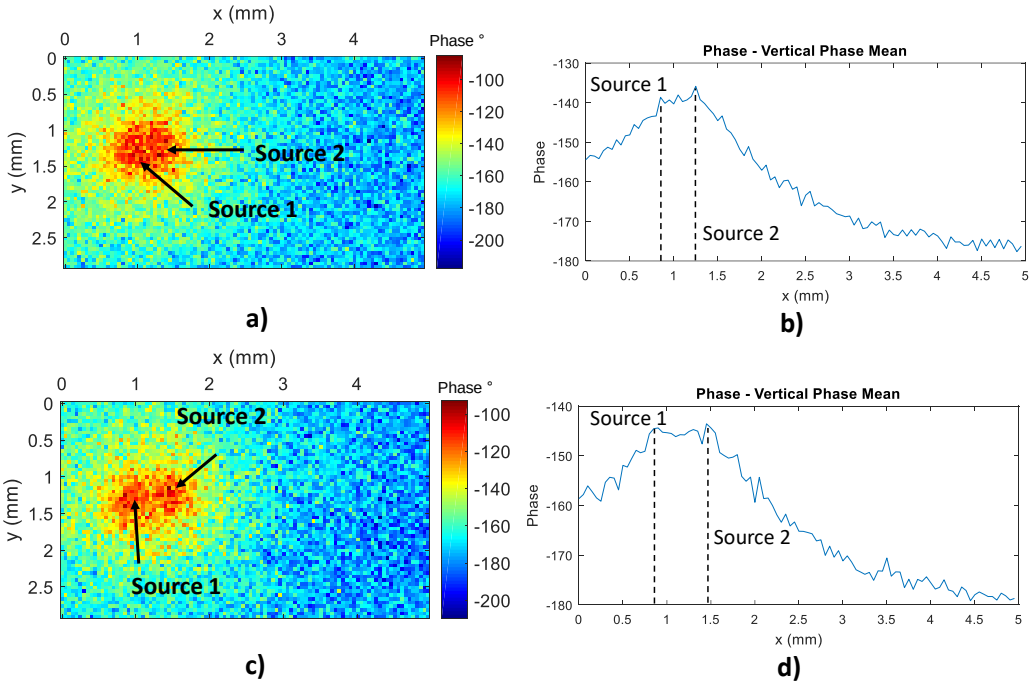


FIGURE 3.18: Measure of the spatial resolution for phase maps. **a)** Phase map showing thermal sources separated by two slices **b)** Vertical average of each pixel column of the phase map a) **c)** Phase map showing thermal sources separated by four slices **d)** Vertical average of each pixel column of the phase map c).

synchronized, a phase gap appears providing a higher contrast and thus a much better spatial resolution. However, every circuit does not allow this configuration, depending on the chosen thermal modulation. Overall, thinning the substrate also improves the spatial resolution as it reduces the lateral conduction within the die.

Of course, to improve spatial resolution, the lock-in frequency can also be raised to reduce the lateral conduction around the source. Yet, an increase of the lock-in frequency generally results in a decrease of the SNR as the thermal wave have less time to spread within the circuit. Consequently, this technique is more adapted to investigate high power sources. For low power sources, statistical errors introduced by ultra low SNR measurements are often problematic, especially for the clarity and contrast of thermal maps.

3.4.2 Modern SoC Analysis

Until now, presented results were obtained on custom designs implemented on FPGAs where it is easy to control the experiment set-up. As commercial products offer less freedom degrees, parameters like the acquisition trigger or the lock-in thermal modulation are more challenging to set-up. The most efficient way to proceed highly depends on the characteristics of each device. In this section, the analysis of two different commercialized SoCs is presented. Each device is thermally investigated to locate the AES crypto-core, the difference lying in the packaging of the circuits. While the first SoC is decapsulated, the second one is analysed through the package.

Decapsulated SoC

In this paragraph, the objective is to locate the AES crypto-processor implemented within the ARM Exynos 4412 SoC. The chip can be commercially acquired in embedded electronic devices such as smartphones and is manufactured in 32 nm semiconductor technology. This is illustrated in fig. 3.19.a, where the chip is soldered onto the smartphone's motherboard. As previously mentioned, commercial products are usually more difficult to investigate due to the limited degrees of liberty available to set up the experiment. In particular, because the circuit of interest is embedded in an ultra portable device, the access to IOs is very limited. This turns out to be quite constraining as the DSO used for signal acquisition requires to be triggered for each new trace acquisition. Also, the package on package configuration stacking the RAM and the SoC in the same device complicates the access to the SoC's silicon substrate. Some adjustments are thus required before being able to map the circuit. This special packaging technique places the RAM module on top of the SoC. As shown in fig. 3.19.b, the RAM IOs are connected to the SoC by a small

ring of solder balls on the border of the package. This configuration allows to save space and improves performances as timing constraints due to long PCB wires are reduced. However, this layout is problematic for thermal analysis as the RAM module blocks IR emissions from the SoC toward the sensor. It is therefore required to remove the top RAM package in order to access the targeted silicon chip. Following this operation, custom programs have to be executed from an external SD card.

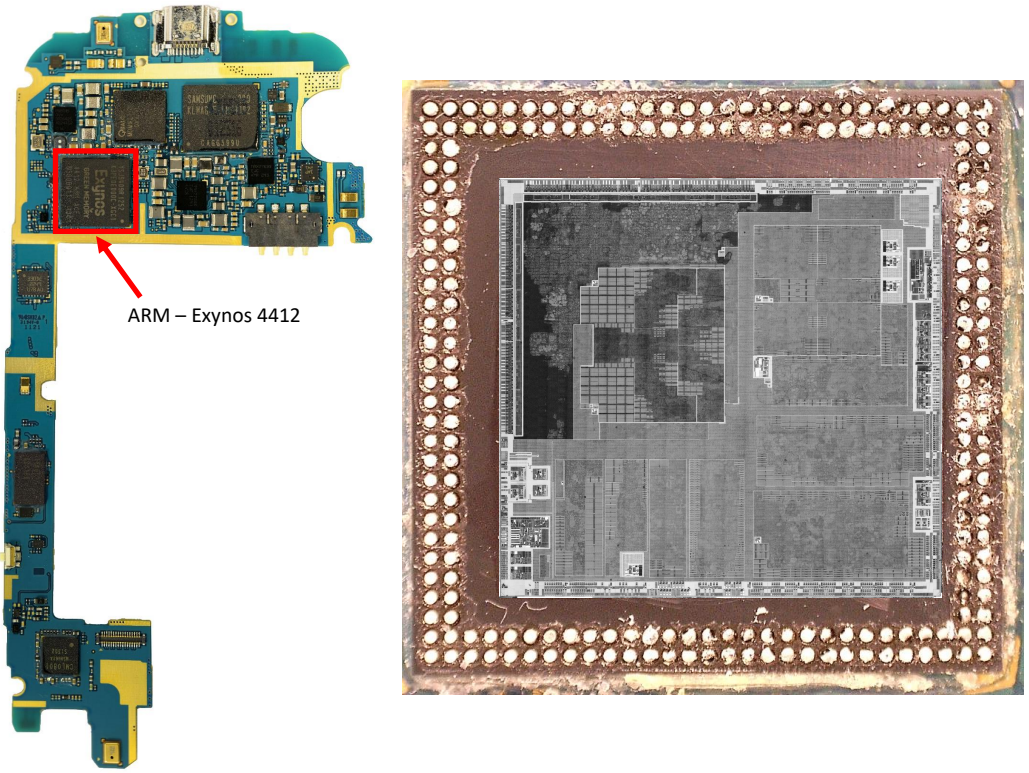


FIGURE 3.19: **a)** Motherboard of the smartphone **b)** Optical photography of the decapsulated die overlayed with an InGaAs thermal camera image showing the internal layout of the SoC (RAM removed).

Yet, this package still presents some advantageous features for thermal analysis. The limited available vertical space forces the manufacturer to reduce the thickness of the die's substrate. Instead of the standard 750 μm, the thickness is thus reduced to 250 μm. The sensor is therefore closer to the heat source and the lateral heat conduction is minimized.

In order to analyse the thermal emissions of this chip, a custom program is implemented. After booting and configuring the device, the program enters a loop modulating the thermal activity of the crypto-processor at 1 Hz. One loop execution corresponds to a lock-in period and is constituted of chained AES executions followed by an idle time of the same duration. The idle period is implemented using one of the hardware counters on the SoC. During this experiment only one core is

active and periodically checks if the counter has reached its final value. Once the idle period is over, a flag is raised asking the main program to resume the ciphering operation and start a new lock-in sequence. Nominally, the core is clocked at 1.4 GHz and the AES cipher core at 200 MHz.

Each period is identified by sending a character on the USB serial communication of the phone toward the control computer. Because the memory depth of the DSO is limited, the sampling rate was kept at 100 kHz. Thus, sending a byte over the serial channel clocked at a significantly higher frequency would appear as a single pulse with such low sampling rate. This signal is therefore usable as a trigger to synchronize the DSO to the lock-in period.

Results of the thermal analysis are presented fig. 3.20. First, location showing lock-in thermal activity are extracted using the KS test. Thermal maps are then enhanced using the making technique of section 3.3.3. Amplitude and phase results are median filtered to eliminate the salt and pepper effect of sequential measurements. Finally, each image is overlayed on top of the floorplan optical image obtained using an InGaAs camera.

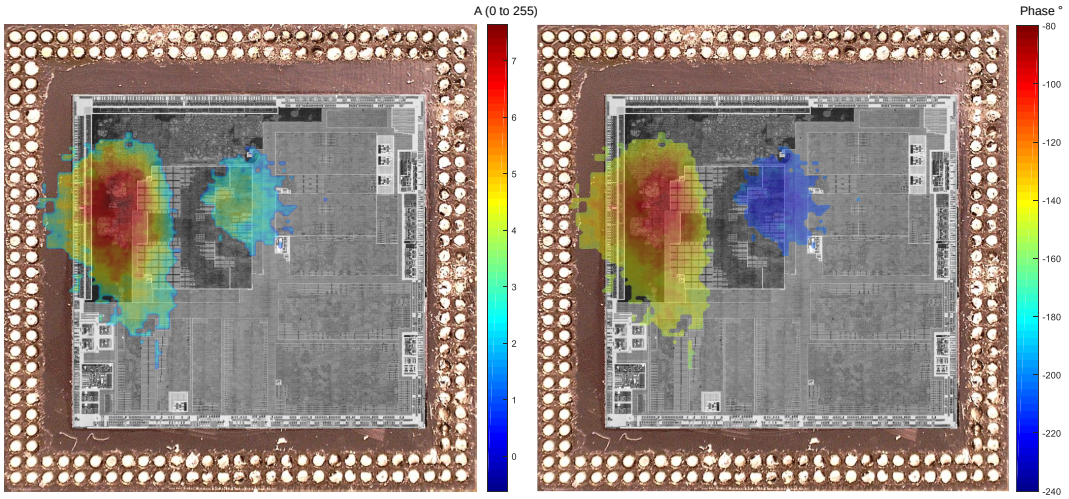


FIGURE 3.20: Superimposition of optical images and acquired thermal maps for the Exynos 4412 modulating the crypto-processor's thermal activity at 1 Hz.

Amplitude image shows two different areas of power consumption. Based on the layout image, area of smaller thermal magnitude is assumed to be the location of the active core of the SoC, performing read operations on the counter's register at high frequency. Inversely the high magnitude thermal source indicates the location of the AES hardware. Logically, the phase map displays two areas in phase opposition. Knowing that the SoC first executes the AES loop sequence, the left thermal activity can be attributed to the AES crypto-processor. The right hot spot therefore corresponds to the main core executing the lock-in program which confirms the previous hypothesis.

These results were acquired with an early version of this platform. In particular, no optics were used, explaining the poor spatial resolution of the thermal maps. Displayed images demonstrate the ability of the platform to target low power secured peripherals on a modern SoC. As demonstrated in [VMC19] the location of the AES core can then be exploited to apply EM side channel (SC) attacks to retrieve cryptographic keys.

Packaged Circuit

In this section the thermal investigation is done on the Kirin 620 SoC which is implemented in 28 nm technology. Contrarily to the Exynos 4412, this circuit is commercialized on standalone boards. In particular, this board is routed with a deported RAM. This significantly facilitates the acquisition of IR radiations as the analysis can be performed directly through the package. Because the thermal wave has to propagate through additional layers of material before reaching the sensors, thermal measurements are expected to have, algebraically speaking, smaller values. Here, the objective remains the same: localize the AES crypto-processor on the circuit.

Similarly to the previous experiment, the lock-in modulation is realized by alternating ciphering and idle phase. On the reception of a character through the UART, a lock-in period is initiated. The custom code implemented on the SoC repetitively ciphers the input text during half the lock-in period. Like for the Exynos 4412, duration of the idle phase is then enforced using a hardware counter. In this case, it is no longer necessary to trig the DSO on the serial communication as the board is equipped with a GPIO connector. For this experiment, the sensor is equipped with a 300 μm aperture optic.

The first thermal analysis is conducted with a lock-in frequency of 1 Hz. Fig. 3.21 presents the obtained thermal maps once the thermal data has been processed. In this case, the mapped area correspond to the epoxy package of the circuit. Interestingly, because of the low lock-in frequency, heat has time to propagate on the whole die. It is thus possible to visualize the position of the silicon substrate through the package.

A very high contrast between the crypto-processor and the rest of the die was observed with traditional amplitude values. To improve readability, amplitude values are pondering and masked, following the method presented in section 3.3.3. For this experiment, a confidence level of $\alpha = 0.05$ is used. The masking procedure was however enough to highlight the thermal information contained by phase values. As expected, phase values are algebraically smaller than usual due to the many layer to run through.

In a second experiment, the same thermal investigation is conducted but with a

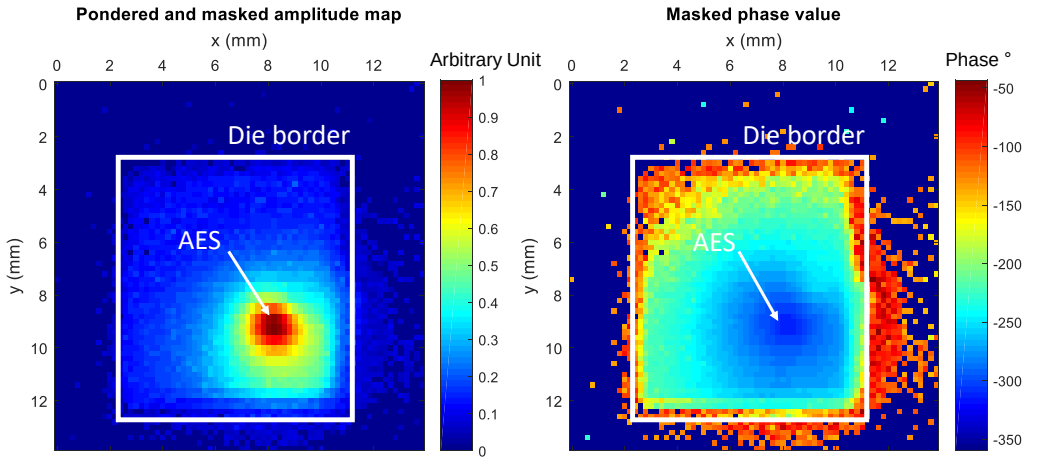


FIGURE 3.21: Thermal lock-in investigation of the Kirin 620 AES processor activity at 1 Hz.

lock-in frequency of 10 Hz. A higher frequency modulation reduces the time allowed for lateral diffusion and thus improves the spatial resolution. Results are presented in fig. 3.22.

In addition of the AES thermal activity, an additional heat source is now appearing on the right of the circuit. Because it is of weak amplitude, this thermal source was previously concealed by the activity of the crypto-processor when performing the analysis at 1 Hz. Similarly to the experiment on the Exynos 4412, it is believed that this additional source is generated by one of the SoC's main core when performing repetitive reads on the counter registers. As before, this hypothesis is supported by the phase opposition between the AES activity and the new hot spot. However, without additional information it is difficult to provide any conclusion on the matter.

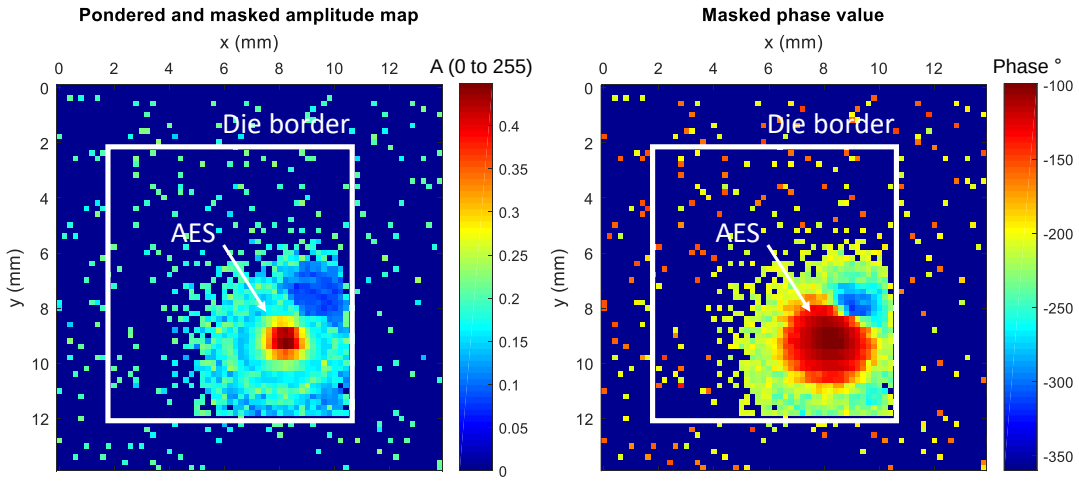


FIGURE 3.22: Through package thermal lock-in investigation of the Kirin 620 AES processor activity at 10 Hz.

Results presented along this chapter demonstrated the efficiency of both the established methodology and the presented platform in acquiring low power IR thermal images. In particular, the ability to locate peripheral and macro blocks is showed in section 3.4.2. This feature can be a critical advantage when performing SCA against secured ciphering accelerators.

Historically, many hardware attacks, including EM SCA and EM FIA, were designed to be performed against smart card devices. Such attacks require to place an EM probe over the circuit to analyze or inject an EM field. EM analysis aims at rebuilding an image of the power consumption of the circuit by acquiring the EM emissions from the DUT. Correlated to a power consumption model, the secret cryptographic key can then be extracted from the investigated circuit. Alternatively, EM fault injection disrupts the nominal activity of the circuit using strong local EM emissions. The mathematical analysis of these faults (one or several bit flips) can then lead, here again, to the extraction of the secret key. Obviously, optimum probe placement is critical as maximizing the SNR of the acquired signal improves the success rate of these attacks.

Because they are ultra low power and have limited peripheral requirements (communication and encryption) smartcard ICs are implemented on tiny die sizes. Typically, the required silicon area to implement such IC in $60\,nm$ technology is of the mm^2 magnitude (usually $1.5 \times 1.5\,mm^2$). Considering that the tip of an EM probe ranges from $20\,\mu m$ to $500\,\mu m$ [OLS+09, PTL+11, BBA+12, CP12], their placement is facilitated by the small dimensions of smart card ICs.

In the last twenty years, research in hardware security highlighted the fact that many other circuits could be compromised by SCA. This includes micro-controllers [LBC17], SoCs [LDMPT15, VMC19], and FPGAs [CCDP04]. A microcontroller is approximately two to three times larger in silicon surface than a smartcard and embeds several macro blocks (power module, clock generation, large memories, etc) that are susceptible of decreasing the targeted signal's SNR. These problematics are increasingly critical with the size and complexity of the DUT. Therefore, positioning an EM probe on large devices such as SoC and FPGAs remains a fastidious and time consuming process [VMC19]. This issue is illustrated in fig. 3.23, where typical sizes of different ICs types are presented.

The proposed IR platform and methodology solves this issues by being capable of localizing precisely peripherals of interest (e.g. the AES accelerator) within the IC. The research area to obtain an acceptable SNR is therefore significantly reduced.

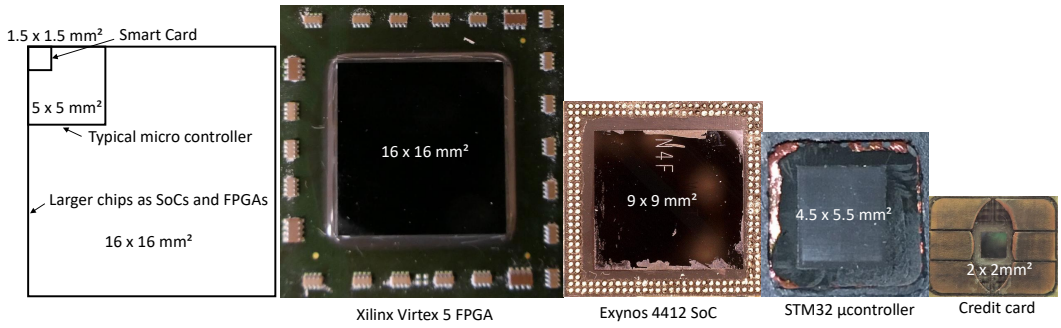


FIGURE 3.23: Comparison of four types of ICs in terms of silicon area

3.5 Chapter Conclusion

This chapter aims at presenting new methodologies for IC thermal investigation. In the first part, an alternative to costly camera is proposed. Based of a single pixel photodiode, the objective is to capitalize on high sampling rate provided by modern DSOs to provide high resolution lock-in phase measurements. Combining lock-in thermography techniques and statistical analysis, the presented platform achieves high detectivity by identifying thermal sources possessing a power consumption as low as 200 μW. Fair performances in spatial resolution are also demonstrated with the detection of two hot spot separated by 300 μm.

In a second part, statistical distributions of lock-in values are analyzed. In particular, the focus is put on distribution variations depending on the quantity of thermal information in the measurement. This revealed that lock-in phase measurements possess a singular behavior and can be modeled by two distinct distributions, depending on the presence of measured lock-in IR radiations. The absence of thermal information provides uniform distributed measurements while measurements over a hot spot tend to be closer to a Gaussian type distribution. Following on this result, different criteria based on statistical analysis are proposed to implement an automated extraction feature for the analysis of thermal maps. In the end, the best results were obtained by construction of a "no signal" distribution reference and performing goodness of fit tests for each pixel of the lock-in phase map. The output statistics of the test are then used to enhance original lock-in measurements by masking and/or pondering areas of interest.

Finally, using the previous mentioned tools, the platform is fully characterized. Several designs are implemented on a Xilinx Virtex 5 FPGA to determine detectivity limits and spatial resolution. Thereafter, two thermal investigation of commercialized SoC are proposed as test-cases. In both case the aim is to retrieve the location of the AES crypto-processor for reverse engineering and hardware security purposes. The first case proposes the analysis of the Exynos 4412 SoC powering used in embedded systems as smartphones. This case offers several challenges as the package on

package configuration of the chip or the need to trigger the DSO without any GPIO access. The second investigation is realized on a Kirin 620 standalone board without any circuit preparation. Thermal radiations are thus acquired directly on top of the epoxy package. In both case, the thermal signature of the target is precisely localized.

Obtained results demonstrate that the combination of lock-in measurements and statistics is a powerful tool for circuit imaging. In the next chapter, it is demonstrated theoretically and experimentally that phase measurement provide good PVT robustness. Hence, this property is exploited to perform thermal map comparison. The proposed comparison methodology is then applied to circuit reliability and hardware Trojan detection.

Chapter 4

New Statistical Methodology for Thermal Map Comparison

This chapter aims at providing a new method allowing the statistical comparison of IR thermal images. To allow such comparison, the robustness of lock-in phase measurements to process, voltage and temperature variation is first demonstrated. This remains valid only under the condition of using clock-gating as a thermal modulation mechanism. Then, each step of the proposed methodology is detailed and justified. Finally, two scenarios of application are proposed with the study of failure analysis and hardware Trojan detection. Intermediary methodologies have lead to the publication of two conference papers respectively at COSADE 2018 and DSD 2018. The final methodology presented in this chapter have been submitted to the journal IEEE transaction on instrumentation and measurement.

4.1 Introduction

Practically, the comparison of thermal maps can reveal small differences in the thermal activity between identical circuits. However, from one circuit to another, differences in measurements are susceptible to affect the correctness of the comparison by generating numerous false positives. These differences are due to the susceptibility of the measured physical variable to process, voltage and temperature (PVT) variations but also to measurement noise.

While being theoretically the same, circuits from a same batch suffer from small differences resulting of inaccuracies during IC manufacturing. These variations can alter power consumption, speed and dimensions of transistors within an IC. In this chapter it is shown that lock-in phase measurements are quasi PVT-independent. Therefore, the comparison of phase thermal maps becomes possible.

In order to compare thermal images, a new methodology is proposed. Similarly

to the work presented in chapter 3, this methodology relies on statistical tests. However, instead of trying to assess the presence of thermal information, the aim is to use the output of the test to investigate a potential thermal anomaly. In addition of an automated realignment process, this comparison methodology uses the density of pixels failing Welch's t-test to identify small variations in the thermal activity of two circuits. It is then demonstrated experimentally that this method can be used to identify weak thermal sources that are not distinguishable from the surrounding thermal activity.

Failure analysis (FA) and hardware Trojan (HT) investigation have many aspects in common. Both rely on the identification of very a weak thermal activity that is susceptible to be concealed (purposely in the case of an HT or randomly in the case of a defect) by other thermal sources. In addition, because the variation in thermal activity is often compared to a reference, the PVT robustness of the measurement must be insured. For this reason two applicative scenarios are considered in this chapter. The first one introduces small additional thermal sources emulating post silicon IC failure while the second one introduces a benchmarked sequential HT. In both cases the performances of the proposed methodology is given.

The chapter is structured as follows. Section 4.2 presents why amplitude measurement are ill-suited for thermal map comparison. Then, phase's PVT robustness is demonstrated theoretically and experimentally. In section 4.3, the precise steps to implement the comparison methodology are explained. Section 4.4 presents the two previously mentioned scenarios. Basics of FA and HT investigation are recalled before introducing experimental results. Finally, section 4.5 concludes the chapter.

4.2 PVT influence on Lock-in Measurements

4.2.1 PVT sensitivness of Amplitude

From chapter 2 it is known that the spectral power emitted by a black body at the temperature T is defined by Planck's law:

$$I_b(\lambda, T) = \frac{2.h.c_0^2.\lambda^{-5}}{e^{\frac{h.c_0}{k.\lambda.T}} - 1} \tag{4.1}$$

where λ is the wavelength, c_0 represents the speed of light in a vacuum, T is the temperature of the black body, h is the Planck constant, and k the Boltzmann constant [ID02a].

By integrating eq. (4.1) over all wavelengths, the Stefan-Boltzmann law (4.2) is obtained. This equation states that the IR power emitted by a black body ($W.m^2$) is

proportional to its temperature at the fourth power:

$$E_b(T) = \sigma \times T^4 \tag{4.2}$$

In this equation, $\sigma = 5.670 \times 10^{-8} W.K^{-4}.m^{-2}$ and is known as the Stefan-Boltzmann constant.

Black bodies are ideal entities and do not represent the thermal behavior of most real bodies. The magnitude of light emitted by real bodies, although based on Planck's law, is highly modulated by emissivity. This parameter, comprised between 0 and 1, is usually extremely non linear and often non continuous. To obtain the real emission of a body, the spectral density in eq. (4.1) must be multiplied by the emissivity at the corresponding wavelength.

Although being the root of thermal investigation of ICs, applying the Stefan-Boltzmann law (eq. 4.2) can be the origin of many errors when comparing thermal maps. Any drift in the temperature generates critical differences in the thermal amplitude measurements while the two samples location present exactly the same electrical activity. This is highly problematic as it is the source of many false positives when comparing thermal maps.

By affecting the performances of a die, process variations also impacts its power consumption. Therefore, the thermal amplitude can be different even if both circuits have theoretically the same activity. In addition, emissivity has proven to be a problematic parameter when relying on process variation robustness. Modern chips present a broad variety of materials that are each characterized by their own emissivity. This emissivity can vary significantly depending on the type of material. As an example, metals are known for their very weak emissions as they are highly reflective while silicon is a quite good emitter. In consequence, cumulative variations on element composing the circuit can alter the emissions of the investigated circuit and thus once again generate false positives.

To illustrate those issues, thermal amplitude maps have been acquired on 6 different boards (B_1 to B_6). Additional details about experimental procedures are given in section 4.4. The cumulative distribution function (CDF) of the measurements over the whole mapped area are given in fig. 4.1 a). Similarly, two CDFs corresponding to acquisitions over board B1 with different core voltages are also given in dashed line on the same figure. It features lock-in thermography amplitude analysis under core voltages of $1.05\,V$ and $0.95\,V$ in regard of other boards with the nominal core voltage of $1\,V$.

The most critical deviance in amplitude CDFs is observed when the core voltage is altered. These variations impact directly the power consumption of the circuit, thus, it is only logical that this variation is passed onto the amplitude values when

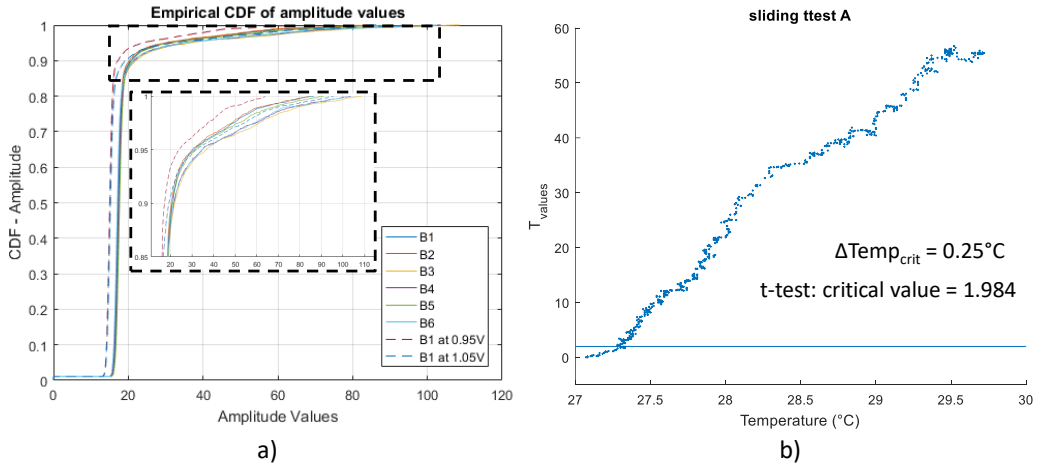


FIGURE 4.1: Impact of **a)** process and voltage variations and **b)** temperature variation on amplitude

performing IR thermal lock-in correlation. This deviance can change the CDF up to a probability of 0.12. While process variations impact lock-in amplitude measurements to a lesser extent, the measured variation is still enough to generate a large amount of false positives when comparing measurements acquired over different circuits.

Because of our inability to control precisely the ambient temperature of our laboratory during the measurements acquisition, the temperature impact is studied differently. The IR sensor is placed on a fixed position over the circuit while the room temperature is progressively raised. To find the critical temperature variation that raises a false positive in our analysis, Welch's t-test [Wel47] is performed between the 100 first measurements and a sliding window of the same number of measurements. Because the measurement acquisition rate is high in regard of the temperature variation, this is comparable to performing multiple t-tests between a sample set acquired at a reference temperature and different sample sets acquired at various temperatures. Fig. 4.1 b) shows that lock-in amplitude measurements vary almost instantly with the temperature raise with $\Delta Temp_{crit} = 0.25^{\circ}\,C$.

From those experiments, it is clear that the study of lock-in amplitude is not adapted for thermal map comparison due to its high dependence on PVT parameters.

In the rest of the chapter, the focus is put on the analysis of the phase of IR emission. This choice is explained and justified in the next section.

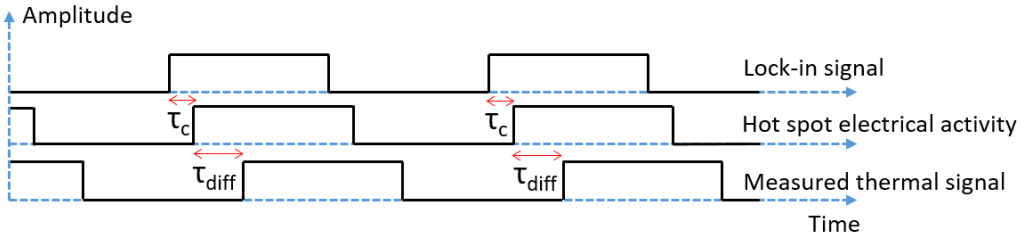


FIGURE 4.2: Signal timing of lock-in clock, hot spot electrical activity, and measured thermal activity

4.2.2 Process voltage and temperature robustness of phase

In order to understand the impact PVT variations have on phase measurements, it is necessary to understand its origin. Let us consider three signals:

- the lock-in clock, which is the actuation signal for the circuit block/peripheral to be investigated
- the actual hot spot activity which represents the precise working schedule of the hot spot
- the IR acquired signal corresponding to the output of the sensor.

The relative timing of those signals are given fig. 4.2.

The phase-shift existing between the lock-in signal and the actual electrical activity of the hot spot is named Φ_c. Similarly, the phase-shift between the electrical activity of the targeted heat source and the ability of the IR sensor to detect the activity due to thermal diffusion is called Φ_{diff}. The total phase measured by the lock-in correlation technique is called Φ and is equal to:

$$\Phi = \Phi_c + \Phi_{diff} \tag{4.3}$$

The delay τ_{diff}, also called diffusion time and related to Φ_{diff} appears because of the slowness of heat conduction. According to O. Breitenstein in [BWL10d], this delay depends on the die's thickness. A chip is considered thermally thin if its thickness is small in regards of the thermal diffusion length. In this case the chip can be seen as a 2D surface emitter and the phase between the lock-in signal and the measured signal should be close to $0°$. If the die is thermally thick, a larger phase-shift should appear, corresponding to the delay caused by heat conduction within the substrate. The thermal diffusion length is the distance over which the amplitude of

the thermal wave decays by $\frac{1}{e} = 0.37$ and is computed as in (4.4):

$$\mu = \sqrt{\frac{\alpha}{\pi \cdot f_{lockin}}} \tag{4.4}$$

α being the thermal diffusivity (in $m^2 \cdot s^{-1}$) and f_{lockin} the lock-in frequency.

The τ_{diff} value depends on the material of the die's substrate and on its thickness. According to the work presented in [SASD10], the phase-shift, given in degrees, generated by heat diffusion can be expressed as follows:

$$\Phi_{diff} = \frac{\sum_{i=1}^{l} z_i}{\sum_{i=1}^{l} \mu_i} \cdot \frac{180}{\pi} \tag{4.5}$$

z_i and μ_i being respectively the thickness and the thermal diffusion length of the i^{th} layer of material between the circuit's hot spot and the sensor. In eq. (4.5), it is shown that the phase-shift generated by thermal diffusivity only relies on intrinsic material parameters and are therefore immune to voltage variations. Nevertheless, variations on the core voltage of a die can influence the detected distance run by the heat as the total power consumption is affected. On the other hand, the thermal diffusivity α is the ratio of thermal conductivity k to the product of density ρ and heat capacity c_p [ID02b]:

$$\alpha = \frac{k}{\rho \cdot c_p} \tag{4.6}$$

In [ZBS19], it is shown that the thermal conductivity varies less than 3% on the $[289, 297]\,K$ temperature range, a quite large span when considering temperature drifts in a test room. Similarly, in [GP01], the specific heat variation does not excess 2% on the same temperature range. Considering that the ambient temperature drift of our test room has been measured around 2 K, the thermal diffusion length μ is considered quasi insensitive to temperature. Finally, the layer thickness z can be considered independent of PVT variations based on the results and figures presented in [FB91] and [SRF+11]. In consequence, Φ_{diff} is declared quasi PVT independent.

For non software lock-in (e.g. asynchronous thermal modulations), the delay between the lock-in clock and the actual electrical activity of the circuit is prone to PVT variations as the lock-in clock may vary independently from the DUT clock tree. Conversely, in the case of a synchronous modulation (e.g. software lock-in) both the delay τ_c and the lock-in period can be expressed as multiples of the circuit's clock period T_{clk}:

$$\tau_c = p \cdot T_{clk} \qquad p \in \mathbb{N} \tag{4.7}$$

$$T_{lockin} = q \cdot T_{clk} \qquad q \in \mathbb{N} \tag{4.8}$$

Therefore, Φ_c can be expressed as:

$$\Phi_c = \frac{\tau_c}{T_{lockin}} \cdot 360 = \frac{p \cdot T_{clk}}{q \cdot T_{clk}} \cdot 360 = \frac{p}{q} \cdot 360 \tag{4.9}$$

From chapter 3, it is known that lock-in modulations are realized at low frequencies ($< 100\,Hz$), which means that q is a very large integer. Inversely, the order of magnitude of τ_c, is about a few clock cycles T_{clk}, and thus is extremely short in comparison. Therefore, the $\frac{p}{q}$ ratio has an extremely small value ($\approx 10^{-7}$ for a 200 MHz clock and a 20 Hz thermal modulation). Hence, the delay τ_c has very little impact on the total phase Φ.

The very low frequency ($< 100\,Hz$) of the modulation forces the acquisition of signals over long time periods. Thus, the sampling rate must be kept low ($\leq 10\,MS/s$) to comply with the limited memory depth ($16\,MS$ in our case) of DSO, even with up to date equipment. For PVT variations to have a significant impact on Φ, they must induce a $\tau_c + \tau_{diff}$ variation greater than the time sample of the DSO. This situation is very unlikely to occur in modern ICs in which timings are generated with a sub-nanosecond accuracy. Finally, under the condition of using software lock-in and sampling rates values significantly greater than the lock-in frequency, phase measurements can be considered quasi PVT independent.

To experimentally demonstrate this property, PVT variation experiences done on amplitude in section 4.2.1 are reiterated, this time using phase analysis. Process and voltage results are acquired on the same 6 boards and presented in fig. 4.3 a). Obtained results are in line with the theoretical aspect of lock-in phase presented previously and show that phase measurements are quasi independent of process and voltage variations. Indeed, the observed variation on the CDF is inferior to 0.01.

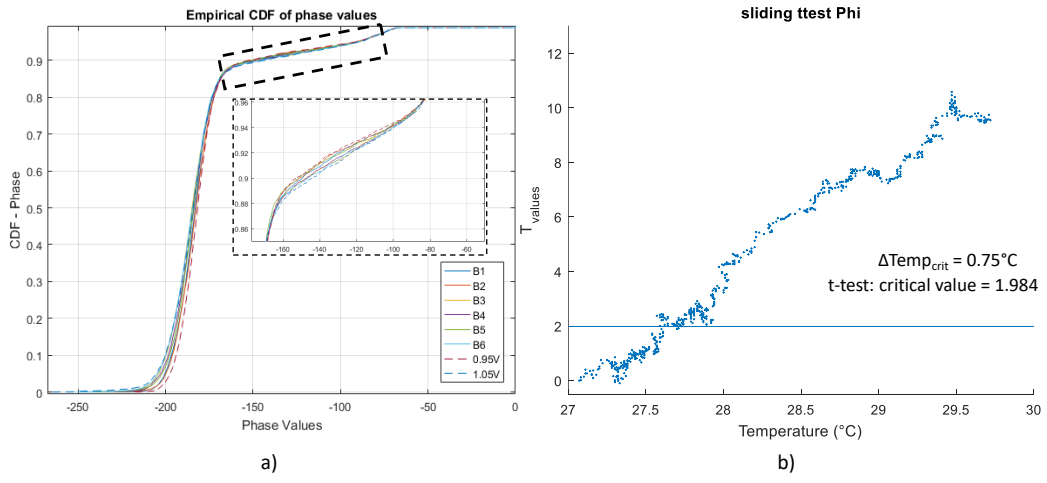


FIGURE 4.3: Impact of **a)** process and voltage variation on phase **b)** temperature variation on phase

While it is admitted that 6 boards is a small quantity for process variations study, the cost and the availability of virtex 5 FPGAs have been limiting factors. However these boards are most likely from different manufacturing batches as they were purchased separately over several years and some of them have been used in accelerated aging studies. Therefore, these six boards should present significant PVT variation as it is shown during the amplitude analysis.

Temperature wise, phase measurements are capable of enduring a temperature drift of approximately $0.75°C$ before showing any significant deviance as shown in fig. 4.3 b). In addition, it is believed that the observed deviance in phase measurements is linked to the sensor's thermoregulation. To minimize noise, the sensor used in this experiment (see chapter 3) operates at $-65\,°C$. If the room temperature is too high, the thermal exchange between the sensor's radiator and the ambient air becomes sub-optimal, leading to drifts in measurements. Thus, with the appropriate equipment, phase measurement should be able to endure larger temperature spans. In this way and considering our experimental conditions, lock-in phase measurement are declared robust to temperature variations.

To summarize the process and voltage variation effects, Kolmogorov-Smirnov tests have been performed between the measurements of the board B1 and the measurements of the other boards. This test's score provides an image of the existing differences between the cumulative distributions of the analysed circuits. As presented fig. 4.4, phase maps present fewer differences between each others and, more importantly, the remaining errors are quite constant between boards. In comparison, variations from one amplitude map to another is, in addition of being of greater magnitude, a lot more fluctuating, making it difficult to compensate.

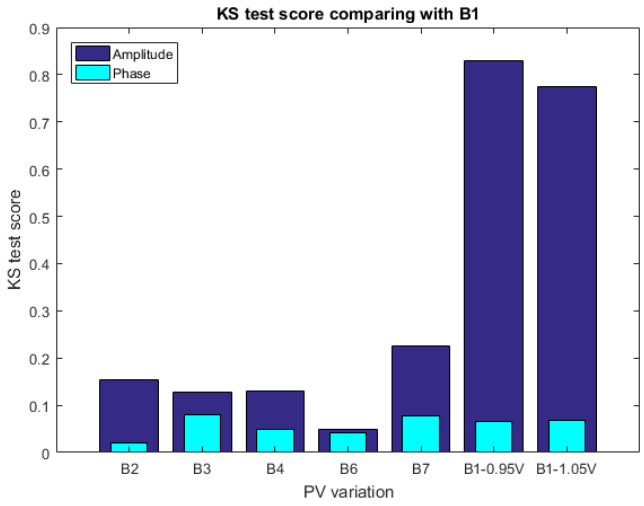


FIGURE 4.4: Quantification of the differences between thermal maps distributions using the Kolmogorov-Smirnov test.

In the end, it seems that phase measurements are, by far, better suited for comparing two thermal maps acquired either on the same device (e.g. B1 vs B1) or on different devices (e.g. B_1 vs B_i). In the rest of the paper, the focus is put on the worst case situation which is when two maps acquired on different devices are compared.

4.3 Methodology

This section discusses the experimental protocol suggested for identifying small differences between thermal maps.

Acquisition

Two thermal maps of $m \times n$ coordinates are acquired and denoted r and d, respectively representing the thermal maps of the reference and the DUT. Each of them is acquired with k measurements at each coordinate. In the end, each phase measurement is noted as follows:

$$\begin{aligned} \Phi^r(x_i, y_j) &= \{\phi_1^r, ..., \phi_k^r\} \\ \Phi^d(x_i, y_j) &= \left\{\phi_1^d, ..., \phi_k^d\right\} \end{aligned} \tag{4.10}$$

with $i = 1, ..., n$ and $j = 1, ..., m$. To ensure the accuracy of the following statistical tests, $k > 50$ is preferred.

Note that $\Phi^r(x_i, y_j)$ is resumed to $\Phi_{i,j}^r$ (respectively $\Phi_{i,j}^d$) in the rest of the paper for ease of reading.

Maps alignment

On our platform, performing thermal analysis on different dies requires to physically remove the board. This process creates significant errors in the die positioning. In addition, PCB and packaging process variations can also shift the absolute location of hot spots from one map to another. Consequently, with our equipment, misalignment up to 600 μm was observed between thermal maps during our numerous experiments. This misalignment is expected to be lower when using an IR camera.

In order to compare relevant data, thermal scans must be realigned. Our solution is software based and is applied as a post treatment. Let us define $P_{i,j}$ as the P_{value} of the Welch t-test at the significance level α between $\Phi_{i,j}^r$ and $\Phi_{i,j}^d$. Similarly, $T_{i,j}$ represents the T_{value} of the Welch t-test between $\Phi_{i,j}^r$ and $\Phi_{i,j}^d$ at the same significance

level α. The realignment process consists in finding the couple $(\Delta x_{al}, \Delta y_{al})$ such that eq. (4.11) is satisfied.

$$(\Delta x_{al}, \Delta y_{al}) = \underset{(\Delta x, \Delta y)}{\arg\min} \left(\sum_{i,j} T(x_i^d + \Delta x, y_j^d + \Delta y) \right) \tag{4.11}$$

$\Phi^r(x_i^{r\prime}, y_j^{r\prime})$ and $\Phi^d(x_i^{d\prime}, y_j^{d\prime})$ are aligned thermal maps with:

$$\begin{aligned} x_i^{d\prime} &= x_i^d + \Delta x_{al} \\ y_j^{d\prime} &= y_j^d + \Delta y_{al} \\ x_i^{r\prime} &= x_i^r \\ y_j^{r\prime} &= y_j^r \end{aligned} \tag{4.12}$$

This way, the DUT's thermal map is shifted, pixel by pixel vertically and horizontally, over the reference one until hot spots are aligned. The t-test score is used as a metric to determine if pixels have the same thermal activity. It is considered that the best alignment is reached when the sum of T_{values} is minimal. Once this process is achieved, pixel coordinates are expressed in function of (x, y) in the rest of the chapter to simplify the notation.

Of course, as the shift between two thermal maps is usually an uneven number of pixels, residual misalignment errors remain. In addition, errors on the z-axis positioning may occur and can not be compensated by the proposed alignment process as it affects the solid angle with which the measurements are done (see chapter 3 table 2.1). This imprecision in the solid angle is aggravated by the size of the Virtex 5 board ($210 \times 150\, mm^2$) and thus it susceptibility to bend over time. Also, rotational errors are not taken into account by this alignment process.

Maps comparison

Because of the aforementioned residual errors and the large number of pixels, comparing two thermal maps by applying point to point Welch's test is not efficient. Indeed, this approach leads to a large number of false positives.

An effective alternative approach consists in analyzing the spatial density of pixels failing Welch's test. Indeed several neighboring positions failing the test are more likely to indicate a true anomaly between the two scans than an isolated one.

In this objective, the thermal maps are divided into pixel groups of size $(2a + 1) \times (2a + 1)$ with $a \in \mathbb{N}$. Each pixel group is assigned with a score, using the

following function:

$$pg(x_{pg}, y_{pg}) = \sum_{i=x_{pg}-a}^{i=x_{pg}+a} \sum_{j=y_{pg}-a}^{j=y_{pg}+a} \varphi(P_{i,j}) \tag{4.13}$$

with

$$\begin{array}{rccl} \varphi: & [0,1] & \longrightarrow & \{0,1\} \\ & p & \longmapsto & \left| \begin{array}{l} 0 \; if \; P(x,y) < 1-\alpha \\ 1 \; if \; P(x,y) \geq 1-\alpha \end{array} \right. \end{array} \tag{4.14}$$

Using such definition, pg is the number of pixels failing Welch's test in the pixel group and α is the confidence level of the test. As a result, if maps are perfectly aligned, pg is a trial in the binomial distribution:

$$PG = \mathrm{B}\left((2a+1)^2, \alpha\right) \tag{4.15}$$

Anomalies in the thermal behavior are detected if the experimental distribution $\mathrm{B}_{exp}\left((2a+1)^2, \alpha\right)$ corresponding to the DUT deviates from the theoretical one. The KS goodness of fit test is used to measure the difference between the theoretical distribution and the experimental one. In the case where the DUT's thermal distribution fails to pass the KS test, the compared thermal signatures are declared different.

Compensation of Positioning Error for Monopixel Sensors

As explained in chapter 3, thermal images can be acquired using a photodetector mounted on motorized axes for automated displacement. This acquisition technique introduces positioning errors between each pixel measurement and can be problematic when comparing the thermal maps. In this case, fingerprinting comparison must be applied. If thermal maps are acquired using IR camera, this step is most likely unnecessary.

Fingerprinting consists in replacing the theoretical binomial distribution by an experimental estimation containing the residual positioning errors. This is done by mapping one circuit n times or mapping n different circuits. If using a single circuit, each time, the latter must be removed then placed back on the platform to generate new positioning errors.

The n scans are compared to get $(n-1)$ pixel groups distributions: pg_1 to $pg_{(n-1)}$. The empirical reference CDF is then computed as:

$$\mathrm{B}_{ref}(u) = P(\bigcup_{i=1}^{i=n-1} pg_i < u) \tag{4.16}$$

where u is the density of pixels failing Welch's t-test.

From there upper and lower bounds are defined using the critical statistic of the KS test for the corresponding α:

$$\mathrm{B}_{ref}^{low}(u) = \mathrm{B}_{ref}(u) - KS_{crit}(\alpha) \tag{4.17}$$

and

$$\mathrm{B}_{ref}^{high}(u) = \mathrm{B}_{ref}(u)) + KS_{crit}(\alpha) \tag{4.18}$$

Therefore, when the thermal map of a DUT is obtained, it is compared to one of the available references to get the $\mathrm{B}_{exp}^{DUT}(u)$ distribution. The DUT is considered suspect (infected or having a defect) if:

$$\exists u, \mathrm{B}_{exp}^{DUT}(u) < \mathrm{B}_{ref}^{low}(u) \mid \mathrm{B}_{exp}^{DUT}(u) > \mathrm{B}_{ref}^{high}(u) \tag{4.19}$$

In other words, $\mathrm{B}_{ref}^{high}(u)$ and $\mathrm{B}_{ref}^{low}(u)$ form a region of nominal operation. If the empirical CDF $\mathrm{B}_{exp}^{DUT}(u)$ crosses the borders of this region, this means that a statistical significant anomaly is present in the thermal activity of the DUT.

The graph in fig. 4.5 illustrates the described methodology. The black curves represent the data issued from the fingerprinting methodology. While the plain line is the averaged reference CDF, the dashed line delimitates the area of acceptable error due to remaining alignment and positioning errors. The dotted red curve represent a device under test whose thermal behaviour is significantly deviant. This can be seen as it crosses the lower bound $\mathrm{B}_{ref}^{low}(u)$. Finally, the theoretical binomial distribution is given in green. Note that curves are not displayed once the averaged reference CDF reaches the probability '1' to ease the visualisation of pixel groups with high density of faulty pixels.

Using this type of graph, it is possible to deduct clues on the topology of the element causing the thermal deviance. For example, a very local, thus dense, thermal source will probably impact very few pixel groups. Therefore, it is likely that the comparison highlight one or two pixel group with a high ratio of pixel failing the t-test. In this scenario, the difference will be observed on high values of the faulty pixel ratio. On the contrary a spread and less dense (or less powerful) thermal variation is more likely to be observed on lower values of faulty pixel ratios.

4.4 Applications

This section presents the results obtained by applying the thermal map comparison methodology. For that, two scenarios are considered. The first application is

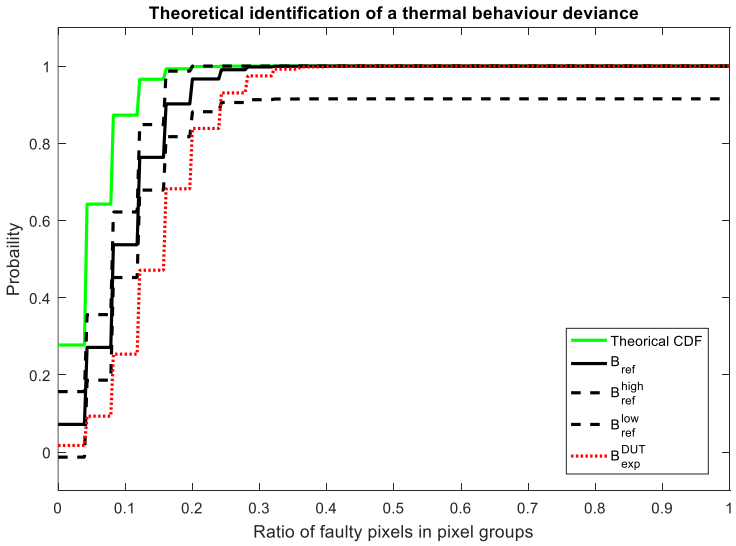


FIGURE 4.5: Quantification of the differences between thermal maps distributions using the Kolmogorov-Smirnov test.

the one where a faulty peripheral is being investigated. In the second, the study is focused on a recent and emerging threat concerning ICs: hardware Trojan insertion.

The IR platform used to acquire thermal maps is mounted with a monopixel sensor. Therefore, all results presented in the next paragraphs are obtained by applying the previously mentioned fingerprinting methodology. In this context, fingerprinting allows to compensate for the alignment error when each pixel is acquired sequentially.

4.4.1 Failure Analysis

Context

In ICs, failure can happen at any stage of its operating life, from manufacturing, till it is inserted in a commercialized product. The associated failure rate is best modeled by the bath-tub curve [Lak01] and is presented fig. 4.6.

This graph shows that a failure can happen during three major periods during the life cycle of a circuit. First, the infant mortality period corresponds to failure happening during manufacture or shortly after [Lak01]. This can be caused by design flaws, unreliable manufacturing processes, or punctual rare events affecting the quality of the manufacturing flow (faulty equipment, particle contamination, temperature drift, etc). The extremely small dimensions, of the *nm* order, forced by the aggressive scaling of the semiconductor industry, inevitably induces failures in the implementation of these circuits. For example, it is well known that the smallest particle contamination can lead to shorts and be fatal to the circuit operation. By means

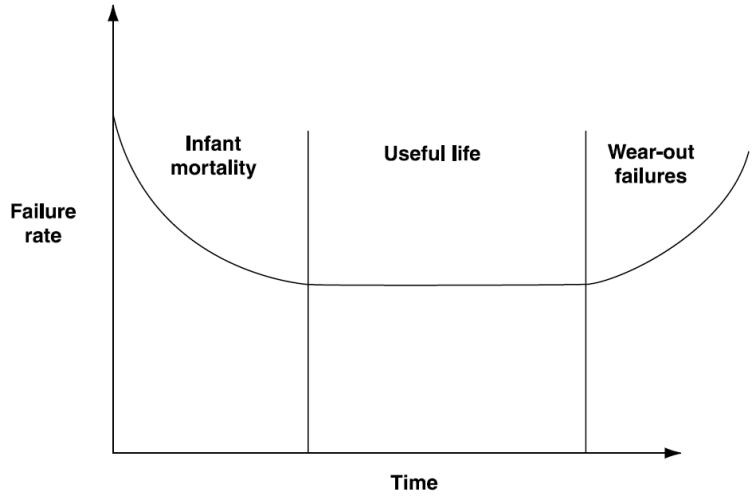


FIGURE 4.6: Model of failure rate within ICs operating life [Lak01]

of illustration, fig. 4.7 presents a faulty micro-controller due to a $0.2\,\mu m \times 0.4\,\mu m$ nickel particle contamination. In comparison the circuit possesses an area of $196\,mm^2$ [SA95]. Also, the chemical processes used to implement an IC are limited in precision. Put together, inaccuracies of each step can create several failures. Among them, excessive leakage, short circuits, junction breakdowns, latch ups or high resistive opens are the most found [SAB12]. Both designs and process are then revised so that the failure rate is minimal during the useful life period of the product.

Most of the time, failure happening during the normal operation region are due to stresses exceeding the specified conditions (high temperature, electrical surge, humidity, mechanical stress, etc) [Lak01]. During this phase, failure is supposedly

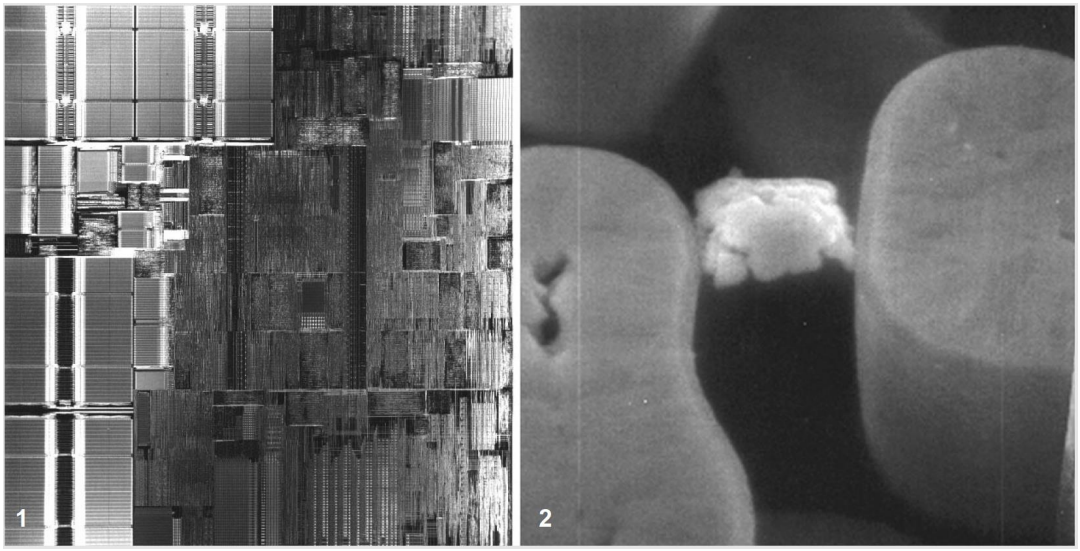


FIGURE 4.7: Investigation of a faulty micro-controller. **1.** topological image of the IC measuring $196\,mm^2$. **2.** $0.2\,\mu m \times 0.4\,\mu m$ nickel particle contamination causing a short between two electrical nodes [SA95]

minimal as it corresponds to the nominal operating period.

Finally, wear-out failures regroup all failures that happen once the expected lifetime of the IC is past. They are generally due to normal aging of materials composing the die. This aging is generally caused by several parameters such as moisture, corrosion, insulation breakdown, etc [Lak01].

To be profitable, ICs must usually be produced in significant amounts (hundred of thousand or millions). In such scenario, the yield becomes an important parameter [Val97]. Failure analysis (FA) regroups methodologies and tools used to understand IC failure causes and how to overcome them. The necessity of FA is thus crucial to the semiconductor industry as collected data provide crucial indication of designs and manufacture weaknesses. FA is hence applied during every step of the IC's manufacture [SA95] and during each period the IC life cycle (see fig. 4.6). This way, reliability, yield and performances of components can be improved.

Existing FA Methodologies

Similarly to reverse engineering, FA techniques can be sorted between destructive and non destructive methods [CYX+14]. Non destructive analysis are usually performed prior to destructive methods as the number of available sample is often limited. Depending on the step FA is applied to, the DUT can be packaged or not. Semi-invasive techniques are a gray area that regroups analyses that require special preparation prior application but leaves the circuit operational once completed (e.g. circuit decapsulation). Because some methods can perform in both case, it is considered in this document, that any method leaving the die operational post-analysis is non destructive. This is the case for IR thermography.

In the beginning, most FAs methodologies consisted in destructive reverse engineering of the DUT [SA95]. Each layer was observed through optical microscopy to localize and identify the origin of the defect. Obviously, this method rapidly became inefficient due to the exponential growth of transistor numbers within a single die. Techniques with performances matching the complexity of very large scale integration (VLSI) dies were then required [SA95]. In particular, the aim is generally to locate precisely the fault on the circuit using non destructive methods before attempting mechanical or chemical reverse engineering. The defect in itself is, most of the time punctual (e.g. a short or open path between two nodes) in regards of the circuit dimensions. However, the symptoms of the defect are often observable on a larger scale (increased power consumption, large abnormal heat spread, etc). Precise and selective circuit imaging has thus been widely investigated [SA95, CYX+14, SAB12, Ira12, Lak01].

FA review shows that many techniques already exists and rely on various principles such as x-ray, electron beam induced current, photon, or thermal emissions [CYX+14, SA95]. Because it is not the aim of this document to realize another review on the subject, only results issued from lock-in thermography analysis are recalled. These results are presented in order to serve as references for the experimental data presented in section 4.4.1.

Originally, IR lock-in thermography has been designed for failure identification within ICs. A major contribution to this field has been realized by O. Breitenstein in [BWL10c, BR, SAB12, BBW09]. Fig. 4.8 presents an example of such investigation superimposing a topography and a lock-in thermography image. In this work, the investigation relies on a thermal modulation realized by pulsing the power supply. IR radiations are acquired using a Thermosensorik TDL 640XL system, which possesses a pixel resolution of 640×512. While the type of investigated IC is not mentioned in [SAB12], it shows an IC with a resistive short caused by lack of etching of a TiN barrier. The position of the actual fault is localized by the white arrow.

As it can be noticed, due to the nominal operation of the circuit several other locations present thermal activity and the defect can not be identified directly from fig. 4.8. Because of the very weak nature of the failure, authors had to reiterate the experiment using a solid immersion lens in order to magnify the fault's location.

In [SASD10], the lock-in phase measurement is exploited to extract the depth of the defect. According to the authors, this technique aims at facilitating the investigation of complex 3D packaging as system in package or package on package. This method is based on the fact that the deeper is the defect, the more time the heat

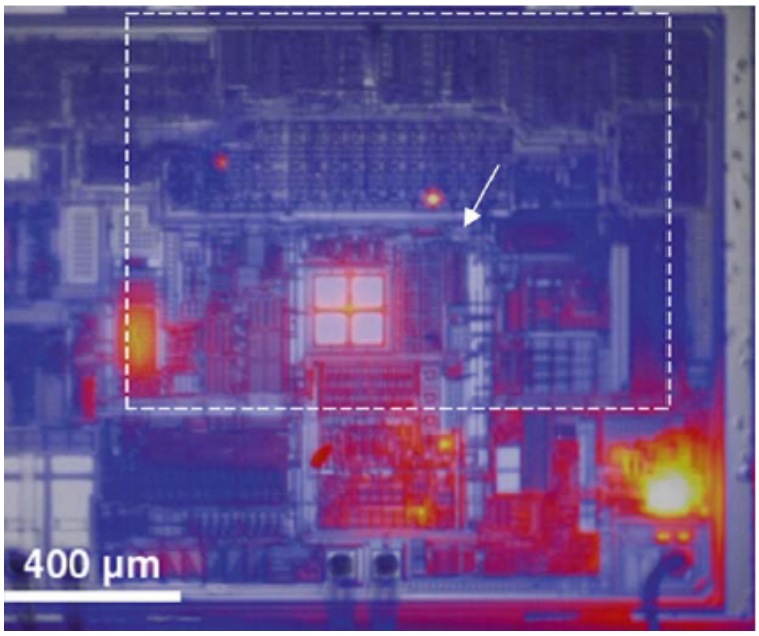


FIGURE 4.8: Default localization using lock-in thermography [SAB12]

wave needs to reach the IC surface. From there, it is demonstrated theoretically and experimentally that the lock-in phase is proportional to the depth of the defect. One advantage of this method is the introduction of the z-axis in the defect location. In particular, this allows through package imaging.

Each presented work seems quite efficient in detecting thermal anomalies when they are isolated from every other thermal sources. However, these results highlight a recurring problem in thermal imaging. Closer to one of the strong thermal source, (e.g. the one on the bottom right corner in fig. 4.8), the short would have certainly remained undetected. The identification of unexpected weak thermal behavior becomes almost impossible using these methods if the defect is localized close to a strong source. In the following section, an example of defect location is proposed using the thermal map comparison method proposed earlier.

FA Using Statistical Lock-in Thermography

When investigating VLSI circuits, it is probable that the thermal signature of a peripheral changes if a failure occurs. A path defect (open/short circuit or resisitive path) is likely to add or subtract a source within the peripheral. Theoretically, this type of defect is easily detectable by classical lock-in thermography using a pulsed power supply as modulation [BBW09]. However many circuits are equipped with internal regulators preventing the application of this technique. Using clock gating as thermal modulation solves the previous problem but only allows to activate the whole peripheral. Hence, discrete modification of the IR thermal signature can be difficult to identify visually. To remedy this issue, we propose to apply the previous thermal map comparison methodology to identify small modifications in the thermal behaviors between functional dies (golden references) and the DUT.

In this scenario, the aim is to emulate the simultaneous activation of different hot spots (e.g. sub circuits and a failure resistive path) within the peripheral of a complex digital architecture (SoC, FPGA, etc). For that, a custom design is implemented on a Xilinx Virtex 5 FPGA. Four micro-heaters, consuming 200 μA each, are placed next to a bigger activity source. The micro-heaters are implemented using 3 gates RO who each fit into a single FPGA slice. To be thermally modulated by the same clock gating mechanism, the micro-heaters are designed with an enable input. The high power consumption source is implemented using an AES performing continuous encryptions and consumes 85 mA. Thermal maps are acquired with an optical aperture of 1 mm. To provide additional details, fig. 4.9 presents the layout of the design. For this experiment, the thermal modulation is set at 20 Hz.

Fig. 4.10 a) presents the traditional thermal lock-in phase image where both the

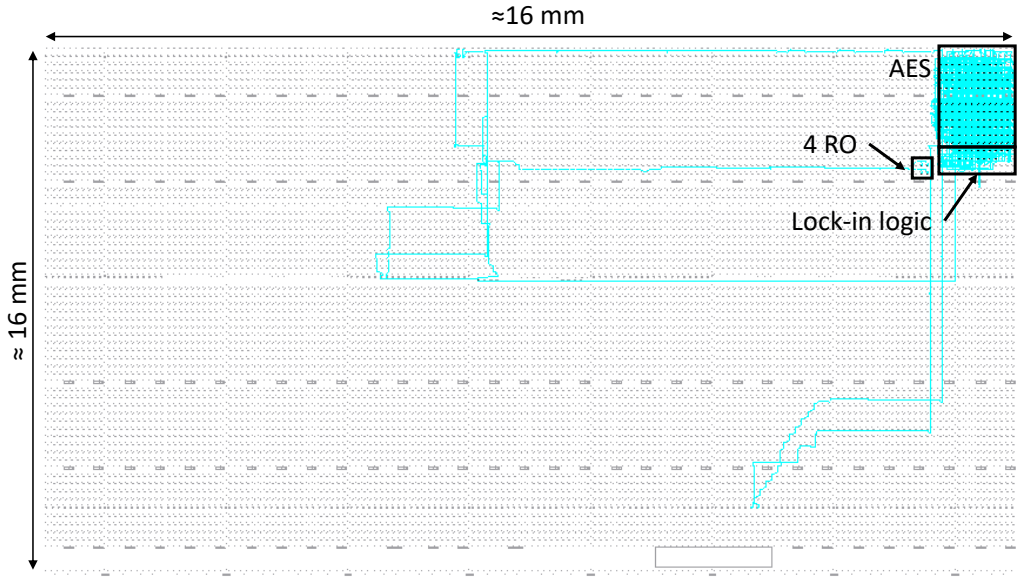


FIGURE 4.9: Floorplan of the RO location test design. Here, the RO are used to emulated an additional thermal activity caused by a defect in the IC.

AES and the micro-heaters are activated. For readability reasons, only the ROs' positions have been indicated, the thermal activity of the AES being indicated by the black arrows. As illustrated, the thermal signature of the micro-heaters is completely concealed by the lateral diffusion of the strong power source (AES). It is thus impossible to visually locate or identify the weak thermal signature of the ROs. Four punctual thermal sources can also be spotted on the bottom right of the image. Because the measurements reveal a phase opposition activity, it can be affirmed that those source are unrelated to our design. However without additional information of the layout of the chip, it is not possible to confirm their origin.

Fig. 4.10 b) and c), show the result of the binomial trial mentioned in equation

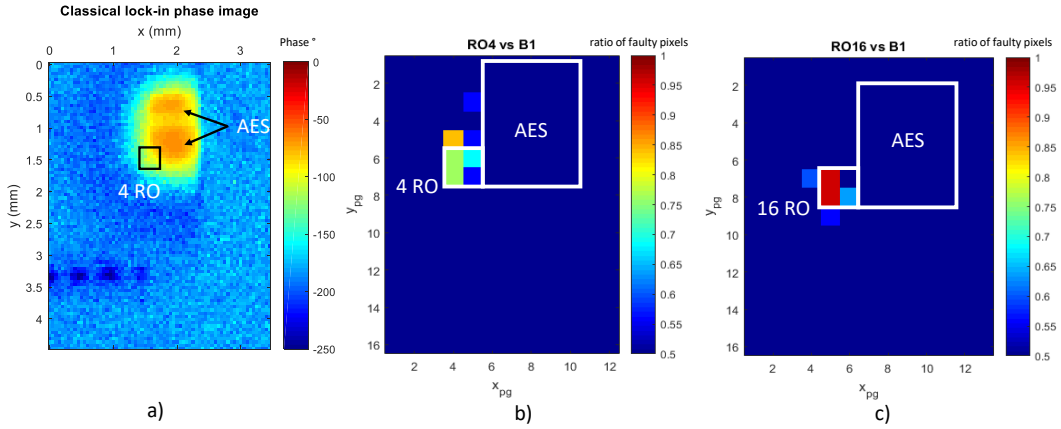


FIGURE 4.10: Emulation of a faulty peripheral creating an additional hot spot using ROs **a)** Classical lock-in phase image **b)** pg map for 4 ROs **c)**pg map for 16 ROs

(4.15). Thereby, the comparison of the DUT to the reference board B1 reveals the emulated defect location. For this application, $a = 2$, so that the pixel groups contain 25 pixels and a confidence level of $\alpha = 0.05$ is chosen. As expected, only the location where the ROs have been implemented corresponds to areas with high density ($\geq$ 70%) of pixel failing Welch's test. The relative placement of the ROs is given by the white rectangles in fig. 4.10. Note that the exact location of sources in fig. 4.10 b) and c) can vary from a) as the alignment process requires to shift the image vertically and horizontally to find the best match.

Yet, this only represents the results versus one board. False positives are susceptible to occur as the acquisition was realized using a single pixel detector. To validate the presence of an extra source, the graphs presented in fig. 4.11 are used. On this figure, experimental CDF bounds obtained by the fingerprinting methodology are represented using dashed lines. Both the theoretical CDF and the average reference CDF are displayed respectively by the green and the black curves. To improve clarity of the graph, $B_{ref}^{low}(u)$ and $B_{ref}^{high}(u)$ are not extended to the maximum abscissa value and are equal to '1' after their final value.

The data on this graphs show that even with displacement error, golden models have a low density of points failing the Welch's test. In the case where the four ROs are active, the graph shows that the CDFs corresponding to the faulty circuit crosses the limits set by the KS test statistic thus demonstrating the detection of the thermal anomaly.

This scenario showed the ability of the proposed methodology to detect additional sources. However, Welch's t-test is bilateral. This means that it is also possible to detect missing thermal information. In this case the expected T_{values} at the faulty location should be negative.

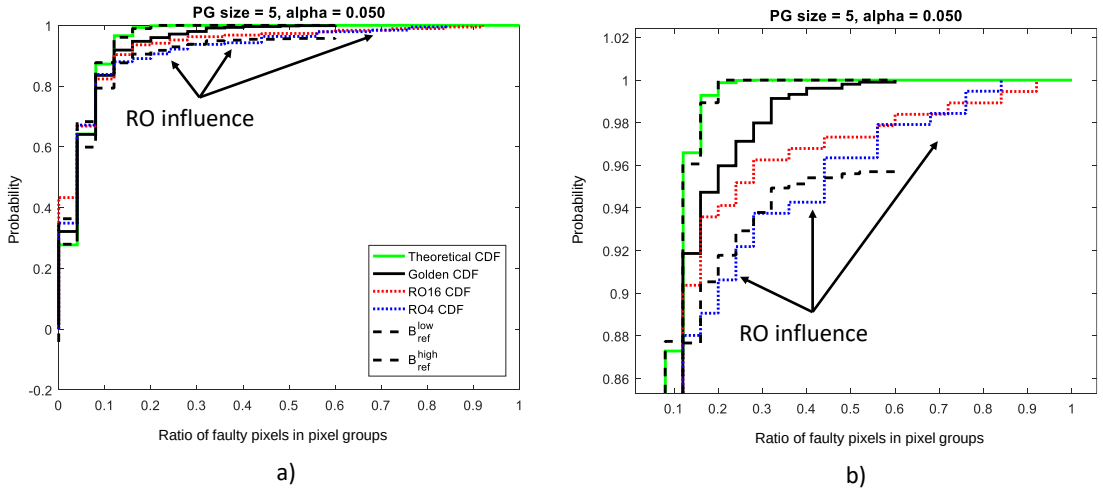


FIGURE 4.11: **a)** Fingerprinting methodology using CDFs for FA analysis **b)** Zoom on the top part of the graph a)

4.4.2 Hardware Trojan Insertion

Context

In the recent years, the proliferation of electronic devices in every day's life systems have raised concerns about security issues in critical systems [TK10]. The security concern is considerably widened because the IC industry has adopted outsourcing as a way to reduce production costs [BR15]. In particular, the ability that one could physically alter a chip in order to generate malicious activity from the latter is commonly known under the hardware Trojan (HT) threat [TK10].

While no physical evidence of HT has yet been made public in commercialized products, the publication of several proofs of concepts demonstrated the disastrous consequences of these malicious devices (data leak, denial of service, etc). This is enough to raise awarness and create the need for efficient countermeasures [BR15]. What is more, several military mishaps have been reported and attributed to the presences of HTs in critical systems [CNB09], [Ade08].

The lack of evidence and the multiple insertion vectors possibilities renders the HT notion quite vague. According to [TK10], HTs can be found under several forms such as hardware modifications on ASICs and SoCs, firmware modifications (e.g. FPGA bistream), or even commercial off the shelf parts. This variety combined to the speculative nature of HTs makes the establishment of common criteria and efficient countermeasures arduous. To address this issue, several research teams have attempted to establish taxonomies and threat vectors. Today, the most used HT taxonomy has been proposed by X. Wang, M. Tehranipoor and J. Plusquellic in [XTP08].

This classification introduces three main categories, sorting HTs following their physical, activation and action characteristics. The physical category is divided into four subsections. First, the "type" of the HT defines if the malicious circuit has been realized by addition/subtraction of transistors (functional HT) or by modification of exiting wires and logic (parametric HT). Second, the "size" of the HT is defined by the number of added/deleted/modified components. Then, the "distribution" subsection describes how the HT is routed within the circuit. Depending on whether the added circuitry is routed compactly in one location or spread in the original design, efficiency of existing identification methodologies is susceptible to vary. Finally, the "structure" of the HT characterizes its physical footprint. Inevitably, the modification of an existing design has consequences on parameters such as power consumption, signal timings, die size, etc. It is therefore critical to be aware of these impacts as they are often key indicators of HT insertion.

The two remaining categories are representative of the malicious circuit's functioning. The action characteristic identifies the disruptive effect, or payload, of the

Trojan. The payload can either transmit (leak) information, modify the original specification of the circuit or modify its function (including disabling and destruction of the circuit). Classical application are denial of service, system destruction, data leakage, programmed obsolescence, etc.

The HT activation characteristic defines the conditions to be met in order to trigger the payload. These can be either internal to the circuit or external. Internal activation is realized through a sensor (e.g. temperature) or a logical combination of signals. External activation requires a device being able to monitor exterior activity. This is implemented through antennas and sensors.

Still according to [XTP08], a given HT can perfectly be hybrids of this classification. One could design a Trojan having multiples payloads or more than one trigger. Fig. 4.12 illustrates the described HT taxonomy.

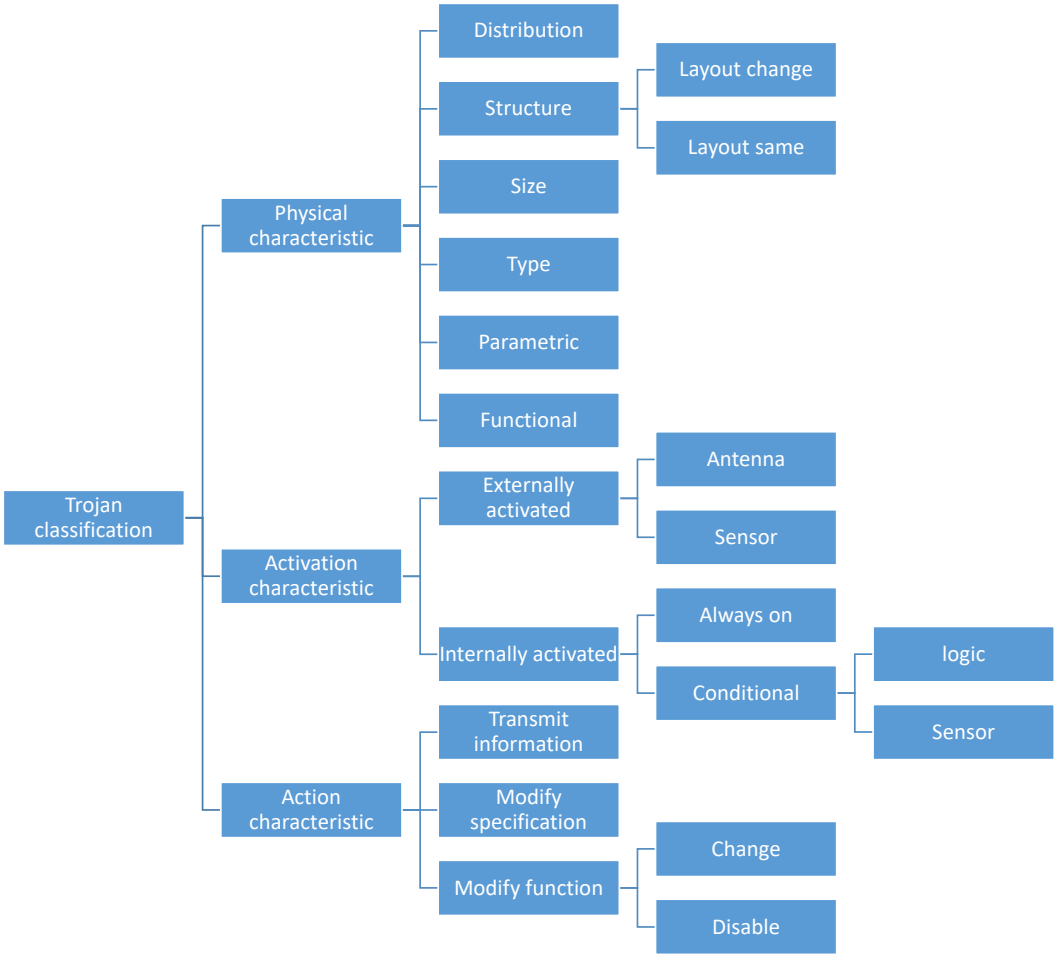


FIGURE 4.12: Taxonomy proposed by X. Wang and al. in [XTP08, TK10]

Threat model

The insertion of malicious hardware can happen in almost every stages of an IC's development cycle. According to [DAR07], the specification phase might be the only one that can be trusted. However, in the case where this stage is out-sourced, specifications are susceptible to be modified without knowledge of the customer. This can, for example, facilitate further insertion attempts [Lec16].

The design phase can be compromised by several factors. Among them, HT insertion by an adversarial member of the design team, the use of third party intellectual property (IP) or compromised development software remain the main threat vectors at this stage [BHN11, Lec16].

Today, one of the most critical phase, regarding IC trust, happens during the manufacturing process of the circuit. Aggressive technology scaling requires massive investments in research and costly equipments. To minimize these costs, the IC industry has massively out-sourced the manufacturing and packaging stages to country where the workforce is cheaper. As a consequence, a vast majority of the circuits are produced by third party companies that are, by definition, untrusted [BHN11].

In the objective of adding/subtracting/modifying the original design, masks used for the manufacturing of the IC can be modified. In addition, equipments such as focused ion beams can also be used to modify the structure of an existing die by addition/subtraction of connections or thinning material layers [Lec16]. Because this document focuses on post-silicon thermal analysis methodologies, only the HT insertion susceptible to happen during the manufacturing process is addressed. It is thus considered possible to access golden models, that are trusted original designs of the DUT.

Post-Silicon HT Detection

The state of the Art shows that many methods aiming at HT detection have been published. To this day, the most accurate method to detect a HT in a die is the complete reverse-engineering of all its layers using chemical etching and scanning electron microscope [BHN11]. However this method has proven to be very time consuming, expensive, destructive and hard to scale.

Non invasive methodologies provide the advantage of leaving the circuit functional once the analysis has been performed. Among them, logic testing proposes to analyze timings and responses to predefined inputs to try to identify abnormal activity [BR15, BHN11]. However, given the complexity of modern digital circuits,

performing analysis over the whole IC logic space would be unreasonable. Different techniques were therefore published trying to achieve the best coverage possible while drastically reducing the test time [BPD+15, JJ08].

Alternatively, the runtime approach consists in monitoring the circuit's activity during its operation to raise a flag if suspicious activity is detected. This monitoring can be achieved, for example, through temperature and power measurements [FBS13, BFS15]. Depending on the design, the concerned area can then be bypassed or the IC can be replaced.

Side Channel analysis is a technique relying on physical parameter variations that are consequence of the die operation to identify unusual behavior. The most common analysis vector are EM analysis [ABK+07, NNB+14] and thermography [NHKR14]. To detect any modification, these techniques usually require a golden model in order to build a reference measurement. However, their efficiency remains limited by their sensitivity to process, voltage and temperature (PVT) variations that strongly reduces their detection capabilities and thus their deployment.

In [NHKR14], authors use thermography to determine whether it is infected or not. The application of 2D principal component analysis, a feature extraction technique used in computer vision, allows the construction of a thermal feature matrix. If trusted data (golden reference for training or trusted simulation models) are accessible, they apply a thresholding method that consists in computing the euclidean distance between the golden and the DUT's thermal feature matrices. Alternatively, the use of a clustering method in the case where no trusted sample can be afforded for training is proposed.

Validation results proposed in the paper are obtained from simulations in which process variations are roughly modeled and voltage and temperature variations ignored. It is also showed that the use of power map instead of thermal map can increase significantly the sensitivity of the method. This way, the detection of a HT with a power density of $0.111\,\mu W/\mu m^2$ and 20% process variation is achieved 85% of the time. In comparison, a HT with a power density of $0.148\,\mu W/\mu m^2$ under the same process variation is only detected 8% of the time using classical thermal maps.

It was previously demonstrated, in this chapter, that lock-in phase measurements are PVT robust. Hence, lock-in IR thermography can be a powerful tool for the localization of HT as the measurement can be performed on different dies without PVT impact. The next section presents results in the attempt of detection the insertion of HT localized in proximity of a strong heat source.

HT Detection Using Statistical Lock-in Thermography

The devices targeted by this platform are digital ICs. To have any impact on the design, the HT is most likely digital as well, meaning it depends on the system clock. Thus, clock gating remains an adapted solution to modulate the trigger's thermal behavior.

For this example, a HT referenced as AES - T100 is implemented. This HT was published in the HT benchmark studies in [tru18, STK13, SHS+17]. The AES T-100 HT is designed to leak the first byte of the secret key from an AES cipher through a covert channel. It uses a technique called code division multiple access used in radio transmission to widen uniformly the bandwidth of the transmitted data for the same emission power [Che98]. A pseudo random number generator implemented with a linear feedback register is used to generate a code sequence. On each clock period, the first byte of the AES secret key is xor-modulated with the generated code sequence. The result of this operation is then propagated through a leakage circuit constituted of 8 identical flip-flops to emulate the effect of a capacitance load.

To demonstrate the capabilities of our methodology, the HT is implemented and located on the side of an AES design similarly to the location of the ROs in the previous experiment. The distance between the HT and the AES is estimated at approximately 600 μm, which is close the spatial resolution limit of phase maps using the actual version of the platform. Two versions of this HT are implemented in order to study different power consumptions. The first version only leaks one key byte, occupies 22 slices and consumes 4 mA. The second HT, leaks two key bytes, occupies 37 slices and consumes 8 mA. By means of illustration, fig. 4.13 presents the layout of the test circuit.

It must be noted that these HTs have relatively high power consumption. However due to the nature of FPGAs, the HT must be routed in a consequent number of slices that are relatively far from each other. On a SoC or an ASIC, the local power density would be much higher which would ease the IR detection. This principle is verified when performing the same analysis on ROs in fig. 4.10, where smaller power consumption are detected in the same conditions.

Detection results are presented fig. 4.14 and use the same parameters $a = 2$ and $\alpha = 0.05$ as for the RO detection. Again, fig. 4.14 a) presents the classical lock-in phase image where the HT thermal signature is concealed by the nominal activity of the DUT. The first HT version leaking 1 key byte is presented in fig. 4.14 b). This HT is at the very threshold of our detection and thus is barely detected as only one pixel group presents a failing density superior to 65%. By contrast, the second version of the HT presented in c) is much more detectable with four pixel groups reaching a failing density between 75% to 80%. Similarly to the RO investigation,

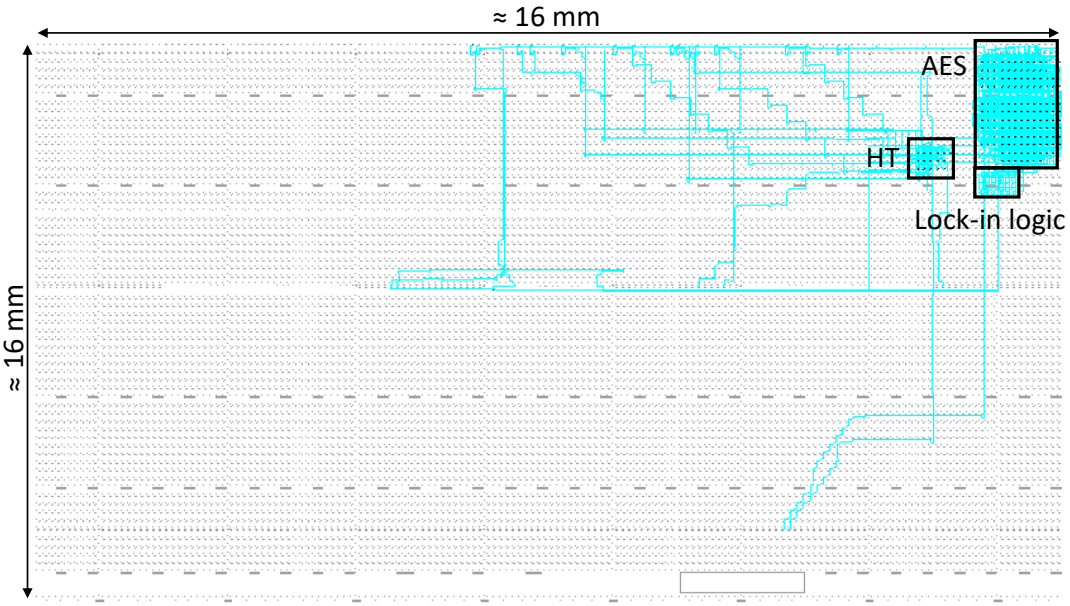


FIGURE 4.13: Floorplan of the HT insertion test design. On this figure, the routed HT is the one leaking 2 bytes of the AES key.

both influences of inserted HT can be spotted on fig. 4.15, comparing the CDFs of the DUTs and the golden references.

It is however possible to increase the probability of detection by acquiring an image with a higher resolution. Consequently, more pixel would fail the test, leading to an easier detection of the additional thermal source. This is however done at the cost of a longer acquisition time.

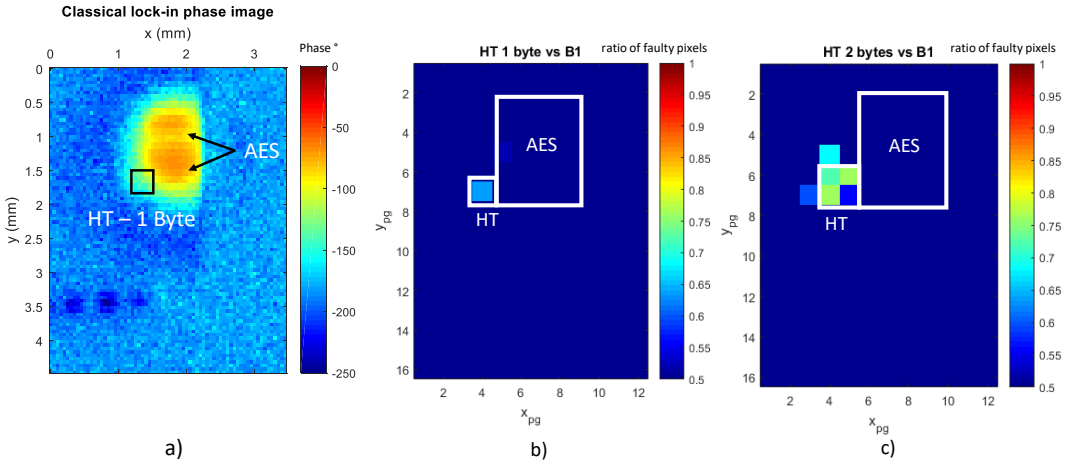


FIGURE 4.14: Emulation of HT insertion in a Virtex 5 FPGA **a)** Classical lock-in phase image **b)** HT leaking one key byte **c)** HT leaking two key bytes

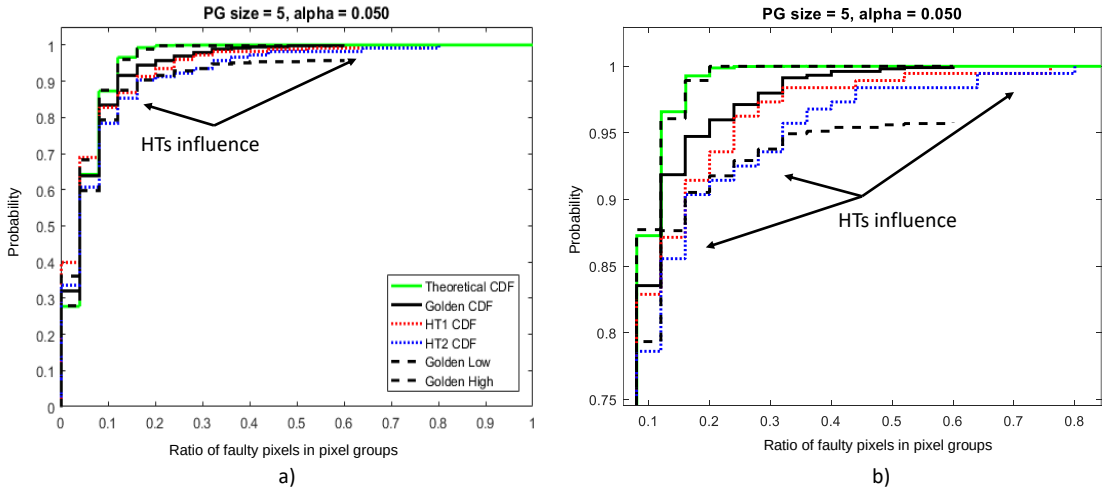


FIGURE 4.15: **a)** Fingerprinting methodology using CDFs for HT investigation **b)** Zoom on the top part of the graph a)

4.4.3 Result Discussion

First, it is worth mentioning that this platform does not aim at being applied "online", during the manufacturing process of ICs. Each thermal map requires 22 hours to be acquired, which is too long for the testing of a single property of a circuit. However, when a circuit is declared faulty (not operational or HT infected) this methodology is of great interest for further investigating the matter. To speed up the process, several parameters as the measurement step and the lock-in frequency can be altered at the price of spatial resolution.

Alternatively, an IR camera can also be used to acquire the thermal maps which solves the pixel displacement error. These devices can acquire many thermal images in minutes but their slow frame rate forces the lock-in frequency to remain quite low in order to build exploitable statistical distributions. However, modern cameras often proposes to decrease the image resolution at the benefit of the frame rate.

Regarding the HT investigation, the example provided in this paper is only a fraction of the designs that can be found in the literature. Given the speculative nature of HTs, it is impossible to assert that any methodology is capable of detecting all types of HT insertions. Yet, it was proven that this methodology is efficient in identifying small thermal sources concealed by the activity of a bigger one, a considerable advantage for HT investigation. Moreover, the proof of concept presented in this chapter is obtained using the J12E3 sensor, that is not the state of the Art in terms of performance. It is strongly believed that results can be significantly improved using sensors with better performances. For example, higher detectivities can be achieved using the J12E4 sensor, cooled at $-85°\,C$ instead of $-65°\,C$. Furthermore, the reduction of the field of view of the IR detector can also greatly improve the spatial resolution. The IR measurement platform demonstrated in this paper is thus quite

advantageous as it is build from off the shelve components making it customizable in function of the application. Consequently, analyses with several options (optics, different sensors, etc) can be performed with the same platform.

4.5 Chapter Conclusion

This chapter is centered around the comparison of thermal maps in order to highlight small variations in thermal signatures. Because the main interest lies in the comparison of thermal maps acquired over different circuits, it must be insured that PVT variations do not have any significant impact to minimize the appearance of false positives.

First, this chapter demonstrated the ill suited character of amplitude values for such comparison as they possess a strong link to temperature and power consumption. In addition, the emissivity of material composing ICs make amplitude value all the way more sensitive to PVT variations.

On the contrary, lock-in phase measurements present much more interesting features because of their temporal nature. Indeed, it was demonstrated theoretically and experimentally that these measurements are at least PVT robust and allow efficient comparison of thermal maps.

From there, a new methodology relying on statistical comparisons of phase measurements is established. This methodology provides a 2D automatic alignment process before comparing the density of pixel failing Welch's t-test to localize anomalies in the thermal activity of the circuit. It is then applied to practical cases for FA and HT identification.

The FA scenario is implemented by inserting ROs close to another functional block. These ROs aim at emulating a defect that would generate a weak additional hot spot next to a more consequent one. For the HT insertion, a benchmarked circuit is used to create the infected test circuit. In both cases, results show that the emulated defect and the inserted HT were detected despite the proximity of another stronger thermal source. Results are then compared to classical lock-in thermography's maps who are unable to identify the thermal signature of the defect nor the HT.

The proposed methodology is also generic and can be applied to measurements using different acquisition methods (e.g. cameras) or even different types of data.

Chapter 5

General Conclusion

Conclusion

In the context of hardware security, reverse engineering can be a decisive tool in the success of an attack. The aggressive scaling of the IC industry rises the transistor density but at the same time more complex circuits require larger silicon areas to be implemented. Classical attacks using laser beams or EM probes are then harder to implement due to the larger surface to explore in order to locate the secured peripheral to analyse.

In this matter, chapter 2 shows that IC imaging can solve this issue by its ability to scan large areas. While several techniques were presented, IR thermal investigation seems to be an especially adapted medium because its ability to scan larger die areas and its ability to detect very low power consumption. In particular, the selective nature of IR lock-in thermography enables to target specific areas of the circuit or specific peripherals. Its ability to extract a unique frequency from a noisy acquisition makes it a powerful tool for low power circuit investigation. Moreover, this technique is robust to external parameters such as environmental lighting variations and provide immunity to material emissivity using phase images.

Originally implemented to work with IR cameras, this technique is adapted to a mono pixel scanning IR platform and presented in chapter 3. The state of the Art shows that thermo-regulated InAs sensor provides the best performances. Combined to off the shelve amplifiers and filters, the platform is able to provide improved lock-in phase resolutions thanks to the high sampling rates of modern DSOs.

The study of IR lock-in measurements shows that statistical distributions of phase values can be exploited to separate thermally active pixels from inactive ones. Indeed, significant variance shifts can be noted as the latter is uniformly distributed in the absence of thermal lock-in signal and normally distributed if a thermal source is active at the lock-in frequency. From there, different statistical criteria are implemented to automatically extract areas of interest within thermal

maps. Experimental results on FPGAs shows that the best detectivity is achieved using the KS test, as power consumptions as low as 200 μA are detected. Using the same criterion, a spatial resolution of 300 μm is obtained for amplitude maps while the spatial resolution of phase maps is slightly inferior with 600 μm.

The ability of the designed measurement system to perform efficient and precise reverse engineering is then tested on two commercialized SoCs. Obtained images show the successful localization of the AES crypto-accelerator. These experiments are realized using non-invasive (through package analysis) and semi-invasive (circuit decapsulation) die preparations.

In chapter 4, it is demonstrated that the statistical comparison of thermal maps is a powerful way to highlight small variations from the thermal activity of one board to another. This comparison relies on the fact that software lock-in phase measurements are PVT robust, which is demonstrated theoretically and experimentally. However, it is also showed that the comparison of amplitude is difficult due to their strong dependence on emissivity and temperature.

The proposed comparison methodology possesses an automated alignment feature and compares pixel groups (as opposed to pixel to pixel comparison) to minimize false positive occurrences. Applications to FA and HT detection are then presented using FPGAs as reconfigurable test-boards to provide golden references and faulty/infected circuits. Experimental results show the identification of an HT occupying 22 slices and consuming 4 mA. In the FA scenario, the fault is emulated using microheaters. Using this methodology, power consumption down to 800 μA are detected.

Perspectives

The designed measurement platform is a proof of concept and is composed of several "homemade" parts (filters, optics, etc). It is believed that performances could be greatly improved using commercial grade components, especially for the optical system. This could, for example, improve the alignment between the cap hole and the active area of the sensor, reducing the signal losses.

The current sensor is capable of acquiring IR radiation in the mi-IR spectrum ($[1,\ 3.8]\mu m$). As explained in chapter 2, silicon suffers from a loss of emissivity at these wavelengths due to increased transparency. It would be interesting to compare results in detectivity using a sensor operating bellow the IR transparency region of silicon ($< 1.1\mu m$), even if the planck law states that this wavelength range possesses inferior emission magnitudes at equivalent temperature.

During the FA and HT analysis, a process variation study is performed over 6 different boards to confirm the robustness of lock-in phase measurements. It is admitted that the sample size is too small to present a final statement on the relation between process variation and phase values. The number of available sample is however limited by the price and the availability of Xilinx Virtex 5 boards. Therefore, a deepen study would be required, using a bigger board pool.

Finally, all experimental results presented in this document are acquired in a "harsh" environment, prone to temperature variation (along the day but also season to season) and noise from human activity and other experiments. It is expected that performances of the platform would greatly benefit from a more adequate environment (real obscurity, temperature stability).

Bibliography

[ABK+07] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. Trojan Detection using IC Fingerprinting. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 296–310, Berkeley, CA, May 2007. IEEE.

[Ade08] Sally Adee. The Hunt For The Kill Switch. *IEEE Spectrum*, 45(5):34–39, May 2008.

[AM11] Francesco Lanza di Scalea Arun Manohar. Wavelet aided multivariate outlier analysis to enhance defect contrast in thermal images. 7981, 2011.

[BBA+12] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In Werner Schindler and Sorin A. Huss, editors, *Constructive Side-Channel Analysis and Secure Design*, pages 151–166, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[BBW09] Jan Bauer, Otwin Breitenstein, and Jan-Martin Wagner. Lock-in thermography: A versatile tool for failure analysis of solar cells. *Electronic Device Failure Analysis*, 11:6, 08 2009.

[BFS15] Chongxi Bao, Domenic Forte, and Ankur Srivastava. Temperature Tracking: Toward Robust Run-Time Detection of Hardware Trojans. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(10):1577–1585, October 2015.

[BHN11] Mark Beaumont, Bradley Hopkins, and Tristan Newby. Hardware Trojans – Prevention, Detection, Countermeasures. page 50, 2011.

[BPD+15] P. Ba, M. Palanichamy, S. Dupuis, M. Flottes, G. Di Natale, and B. Rouzeyre. Hardware trojan prevention using layout-level design approach. In *2015 European Conference on Circuit Theory and Design (ECCTD)*, pages 1–4, Aug 2015.

[BR] Otwin Breitenstein and JP Rakotoniaina. New developments in ir lock-in thermography.

[BR15] Shivam Bhasin and Francesco Regazzoni. A survey on hardware trojan detection techniques. In *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2021–2024, Lisbon, Portugal, May 2015. IEEE.

[BSJL09] R Bhan, Raghvendra Saxena, C.R. Jalwania, and S.K. Lomash. Uncooled infrared microbolometer arrays and their characterisation techniques. *Defence Science Journal*, 59:580, 11 2009.

[BWL10a] Otwin Breitenstein, Wilhelm Warta, and Martin Langenkamp. *Lock-in Thermography*, volume 10 of *Springer Series in Advanced Microelectronics*, chapter 5, pages 149–175. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[BWL10b] Otwin Breitenstein, Wilhelm Warta, and Martin Langenkamp. *Lock-in Thermography*, volume 10 of *Springer Series in Advanced Microelectronics*, chapter 1, pages 1–6. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[BWL10c] Otwin Breitenstein, Wilhelm Warta, and Martin Langenkamp. *Lock-in Thermography*, volume 10 of *Springer Series in Advanced Microelectronics*, chapter 2, pages 7–59. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[BWL10d] Otwin Breitenstein, Wilhelm Warta, and Martin Langenkamp. *Lock-in Thermography*, volume 10 of *Springer Series in Advanced Microelectronics*, chapter 4, pages 107–153. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[CCDP04] Vincent Carlier, Herve Chabanne, Emmanuelle Dottax, and Hervé Pelletier. Electromagnetic side channels of an fpga implementation of aes. *IACR Cryptology ePrint Archive*, 2004:145, 01 2004.

[Che98] A. C. Chen. Overview of code division multiple access technology for wireless communications. In *IECON '98. Proceedings of the 24th Annual Conference of the IEEE Industrial Electronics Society (Cat. No.98CH36200)*, volume 1, pages T15–T24 vol.1, Aug 1998.

[CNB09] Rajat Subhra Chakraborty, Seetharam Narasimhan, and Swarup Bhunia. Hardware Trojan: Threats and emerging solutions. In *2009 IEEE International High Level Design Validation and Test Workshop*, pages 166–171, San Francisco, CA, USA, November 2009. IEEE.

[CP12] J. D. Chisum and Z. Popovic. Performance limitations and measurement analysis of a near-field microwave microscope for nondestructive and subsurface detection. *IEEE Transactions on Microwave Theory and Techniques*, 60(8):2605–2615, Aug 2012.

[CYX+14] X. Chen, G. Yuan, G. Xu, L. Liu, and X. Kuang. Advanced fault localization techniques in microelectronics failure analysis. In *2014 10th International Conference on Reliability, Maintainability and Safety (ICRMS)*, pages 5–9, Aug 2014.

[DAR07] DARPA. Trust in integrated circuits (tic). *Proposer Information Pamphlet*, pages 10–11, 2007.

[dBWGS11] Fred de Beer, Marc Witteman, Bartek Gedrojc, and Yijun Sheng. Practical Electro-Magnetic Analysis. page 18, 2011.

[DDRT12] A. Dehbaoui, J. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 7–15, Sep. 2012.

[FB91] Liu Fengchao and Zheng Bin. The linear coefficient of thermal expansion of silicon at room temperature. *Powder Diffraction*, 6(3):147—152, 1991.

[FBS13] Domenic Forte, Chongxi Bao, and Ankur Srivastava. Temperature tracking: An innovative run-time approach for hardware Trojan detection. In *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 532–539, San Jose, CA, November 2013. IEEE.

[GP01] V. M. Glazov and A. S. Pashinkin. The thermophysical properties (heat capacity and thermal expansion) of single-crystal silicon. *High Temperature*, 39(3):413–419, May 2001.

[HP11a] Solid State Division Hamamatsu Photonics. Application note: Characteristics and use of infrared detectors. 2011.

[HP11b] Solid State Division Hamamatsu Photonics. Application note: Thermal detectors. 2011.

[ID02a] F.P. Incropera and D.P. DeWitt. Fundamentals of heat and mass transfer. 2002.

[ID02b] F.P. Incropera and D.P. DeWitt. Fundamentals of heat and mass transfer. 2002.

[Ira12] Andrea Irace. Infrared thermography application to functional and failure analysis of electron devices and circuits. *Microelectronics Reliability*, 52:2019–2023, 09 2012.

[JJ08] Susmit Jha and Sumit Kumar Jha. Randomization based probabilistic approach to detect trojan circuits. *2008 11th IEEE High Assurance Systems Engineering Symposium*, pages 117–124, 2008.

[KB04] Margaret Kohin and Neal Butler. Performance limits of uncooled vox microbolometer focal plane arrays. *Proceedings of SPIE - The International Society for Optical Engineering*, 08 2004.

[KBR06a] P. L. Komarov, M. G. Burzo, and P. E. Raad. A thermoreflectance thermography system for measuring the transient surface temperature field of activated electronic devices. In *Twenty-Second Annual IEEE Semiconductor Thermal Measurement And Management Symposium*, pages 199–203, March 2006.

[KBR06b] P. L. Komarov, M. G. Burzo, and P. E. Raad. A thermoreflectance thermography system for measuring the transient surface temperature field of activated electronic devices. In *Twenty-Second Annual IEEE Semiconductor Thermal Measurement And Management Symposium*, pages 199–203, March 2006.

[Key77] Robert J. Keyes. *Optical and Infrared Detectors*. 1977.

[Lak01] V Lakshminarayanan. Failure analysis techniques for semiconductors and other devices. *info/card 84, RF semiconductors*, pages 34–46, 2001.

[LBC17] Owen Lo, William J. Buchanan, and Douglas Carson. Power analysis attacks on the aes-128 s-box using differential power analysis (dpa) and correlation power analysis (cpa). *Journal of Cyber Security Technology*, 1(2):88–107, 2017.

[LDMPT15] J. Longo, E. De Mulder, D. Page, and M. Tunstall. Soc it to em: Electromagnetic side-channel attacks on a complex system-on-chip. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems – CHES 2015*, pages 620–640, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[Lec16] Maxime Lecomte. *Système embarque de mesure de la tension pour la détection de contrefaçons et de chevaux de Troie matériels*. PhD thesis, 2016. Thèse de doctorat dirigée par Maurine, Philippe Microélectronique Lyon 2016.

[LM19] Marc Lacruche and Philippe Maurine. Electromagnetic activity vs. logical activity: Near field scans for reverse engineering. In Begül Bilgin and Jean-Bernard Fischer, editors, *Smart Card Research and Advanced Applications*, pages 140–155, Cham, 2019. Springer International Publishing.

[LY07] Wenjun Liu and Bozhi Yang. Thermography techniques for integrated circuits and semiconductor devices. *Sensor Review*, 27(4):298–309, 2007.

[Maj99] A Majumdar. Scanning thermal microscopy. *Annual Review of Materials Science*, 29:505–585, 08 1999.

[MLC+95] A Majumdar, J Lai, M Chandrachood, Osamu Nakabeppu, Y Wu, and Zhenpeng Shi. Thermal imaging by atomic force microscopy using thermocouple cantilever probes. *Review of Scientific Instruments*, 66:3584 – 3592, 07 1995.

[MLdS13] Arun Manohar and Francesco Lanza di Scalea. Detection of defects in wind turbine composite blades using statistically enhanced lock-in thermography. *Structural Health Monitoring*, 12:566–574, 12 2013.

[MTOL12] Philippe Maurine, Karim Tobich, Thomas Ordas, and Pierre Yvan Liardet. Yet Another Fault Injection Technique : by Forward Body Biasing Injection. In *YACC'2012: Yet Another Conference on Cryptography*, Porquerolles Island, France, September 2012.

[NHKR14] Abdullah Nazma Nowroz, Kangqiao Hu, Farinaz Koushanfar, and Sherief Reda. Novel Techniques for High-Sensitivity Hardware Trojan Detection Using Thermal and Power Maps. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(12):1792–1805, December 2014.

[NNB+14] Xuan Thuy Ngo, Zakaria Najm, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger. Method Taking into Account Process Dispersions to Detect Hardware Trojan Horse by Side-Channel. page 17, 2014.

[NWR11] Abdullah Nowroz, Gary Woods, and Sherief Reda. Improved post-silicon power modeling using AC lock-in techniques. In *Design Automation Conference (DAC), 2011 48th ACM/EDAC/IEEE*, pages 101–107. IEEE, 2011.

[OLS+09] Thomas Ordas, Mathieu Lisart, Etienne Sicard, Philippe Maurine, and Lionel Torres. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. In Lars Svensson and José Monteiro, editors, *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, pages 229–236, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[PRG93] Robert G. Meyer Paul R. Gray. *Analysis and Design of Analog Integrated Circuits*. 1993.

[PTL+11] F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx, and P. Maurine. Local and direct em injection of power into cmos integrated circuits. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 100–104, Sep. 2011.

[RCN11] Sherief Reda, Ryan Cochran, and Abdullah Nazma Nowroz. Improved Thermal Tracking for Processors Using Hard and Soft Sensor Allocation Techniques. *IEEE Transactions on Computers*, 60(6):841–851, June 2011.

[Red11] S. Reda. Thermal and power characterization of real computing devices. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 1(2):76–87, June 2011.

[SA95] Jerry M. Soden and Richard E. Anderson. Ic failure analysis: Techniques and tools for quality and reliability improvement. *Microelectronics Reliability*, 35(3):429 – 453, 1995. Reliability Physics of Advanced Electron Devices.

[SAB12] Ch. Schmidt, F. Altmann, and O. Breitenstein. Application of lock-in thermography for failure analysis in integrated circuits using quantitative phase shift analysis. *Materials Science and Engineering: B*, 177(15):1261 – 1267, 2012. MicroTherm2011 – Microtechnology and Thermal Problems in Electronics.

[SASD10] C. Schmidt, F. Altmann, R. Schlangen, and H. Deslandes. Non-destructive defect depth determination at fully packaged and stacked die devices using lock-in thermography. In *2010 17th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits*, pages 1–5, July 2010.

[SC67] George Waddel Snedecor and William G. Cochran. Statistical methods iowa state university press. 1967.

[SCMR99] Bhushan Sopori, Wei Chen, Jamal Madjdpour, and Nuggehalli Ravindra. Calculation of emissivity of si wafers. *Journal of Electronic Materials*, 28:1385–1389, 12 1999.

[SHS+17] Bicky Shakya, Tony He, Hassan Salmani, Domenic Forte, Swarup Bhunia, and Mark Tehranipoor. Benchmarking of hardware trojans and maliciously affected circuits. *Journal of Hardware and Systems Security*, 1(1):85–102, Mar 2017.

[SNK+12] Alexander Schlösser, Dmitry Nedospasov, Juliane Krämer, Susanna Orlic, and Jean-Pierre Seifert. Simple photonic emission analysis of aes. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems – CHES 2012*, pages 41–57, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[SNL+10] Dmitry Skvortsov, Mr Ng, T.R Lundquist, Joy Liao, Steven Kasapi, and Howard Marks. Laser voltage imaging: A new perspective of laser voltage probing. In *ISTFA*, pages 5–13, 11 2010.

[SRF+11] S. K. Selvaraja, E. Rosseel, L. Fernandez, M. Tabat, W. Bogaerts, J. Hautala, and P. Absil. Soi thickness uniformity improvement using corrective etching for silicon nano-photonic device. In *8th IEEE International Conference on Group IV Photonics*, pages 71–73, Sept 2011.

[SS11] Jitesh Shinde and S. S. Salankar. Clock gating: A power optimizing technique for VLSI circuits. In *2011 Annual IEEE India Conference*, pages 1–4, Hyderabad, India, December 2011. IEEE.

[STK13] H. Salmani, M. Tehranipoor, and R. Karri. On design vulnerability analysis and trust benchmarks development. In *2013 IEEE 31st International Conference on Computer Design (ICCD)*, pages 471–474, Oct 2013.

[TBB+07] G. Tessier, M. Bardoux, C. Boué, C. Filloy, and D. Fournier. Back side thermal imaging of integrated circuits at high spatial resolution. *Applied Physics Letters*, 90(17):171112, 2007.

[TEL00] JUDSON TECHNOLOGIES TELEDYNE. Datasheet: J12 series, inas detectors, operating notes. 2000.

[TFW07] J. Tao, P. Fang, and J. Wang. Backside ir photon emission microscopy (ir-pem) observation in failure analysis of the packaged devices. In *2007 8th International Conference on Electronic Packaging Technology*, pages 1–4, Aug 2007.

[TJ09] Randy Torrance and Dick James. *The State-of-the-Art in IC Reverse Engineering*, pages 363–381. 08 2009.

[TK10] M. Tehranipoor and F. Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE Design Test of Computers*, 27(1):10–25, Jan 2010.

[TLSB16] Shahin Tajik, Heiko Lohrke, Jean-Pierre Seifert, and Christian Boit. No place to hide: Contactless probing of secret data on fpgas. volume 9813, 08 2016.

[tru18] trustHUB. http://trust-hub.org/resources/benchmarks/trojan, October 2018.

[Val97] David P. Vallett. Ic failure analysis: The importance of test and diagnostics. *IEEE Des. Test*, 14(3):76–82, July 1997.

[VMC19] A. Vasselle, P. Maurine, and M. Cozzi. Breaking mobile firmware encryption through near-field side-channel analysis, 2019 attacks and solutions in hardware security (ASHES), 2019, london. 2019.

[VWWM11] Jasper GJ Van Woudenberg, Marc F Witteman, and Federico Menarini. Practical optical fault injection on secure microcontrollers. In *2011*

Workshop on Fault Diagnosis and Tolerance in Cryptography, pages 91–99. IEEE, 2011.

[Wel47] B. L. Welch. The Generalization of Student's Problem When Several Different Population Variance Are Involved. *Biometrika*, 34(1-2):28–35, 01 1947.

[XTP08] Xiaoxiao Wang, Mohammad Tehranipoor, and Jim Plusquellic. Detecting malicious inclusions in secure hardware: Challenges and solutions. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 15–19, Anaheim, CA, USA, June 2008. IEEE.

[ZBS19] Amirkoushyar Ziabari, Zhixi Bian, and Ali Shakouri. Adaptive power blurring techniques to calculate ic temperature profile under large temperature variations. 03 2019.

Abstract

The generalization of integrated circuits and more generally electronics to everyday life systems (military, finance, health, etc) rises the question about their security. Today, the integrity of such circuits relies on a large panel of known attacks for which countermeasures have been developed. Hence, the search of new vulnerabilities represents one of the largest contribution to hardware security. The always rising complexity of dies leads to larger silicon surfaces. Circuit imaging is therefore a popular step among the hardware security community in order to identify regions of interest within the die. In this objective, the work presented here proposes new methodologies for infrared circuit imaging. In particular, it is demonstrated that statistical measurement analysis can be performed for automated localization of active areas in an integrated circuit. Also, a new methodology allowing efficient statistical infrared image comparison is proposed. Finally, all results are acquired using a cost efficient infrared measurement platform that allows the investigation of weak electrical sources, detecting power consumption as low as 200 μW.

Résumé

La généralisation des circuits intégrés et plus généralement de l'électronique à tous les secteurs d'activité humaine, nécessite d'assurer la sécurité d'un certain nombre de systèmes critiques (militaire, finance, santé, etc). Aujourd'hui, l'intégrité de ces systèmes repose sur un éventail d'attaques connues, pour lesquelles des contremesures ont été développées. Ainsi, la recherche de nouvelles attaques contribue fortement à la sécurisation des circuits électroniques. La complexité toujours croissante des circuits, permise par les progrès dans les technologies silicium, a pour conséquence l'apparition de circuits occupant de plus en plus de surface. La retro-ingénierie est donc une étape souvent obligatoire menée en amont d'une attaque afin de localiser les périphériques et autres régions d'intérêts au sein du circuit visé. Dans cet objectif, l'étude présenté dans ce document propose de nouvelles méthodes d'imagerie infrarouge. En particulier, il est démontré que l'analyse statistique des mesures infrarouge permet d'automatiser la localisation des régions électriquement actives d'un circuit. Aussi, une nouvelle méthode de comparaison statistique d'image infrarouge est proposée. Enfin, ces résultats sont acquis au moyen d'une plateforme de mesure faible coût, permettant de détecter toute activité électrique possédant une consommation supérieure à 200 μW.