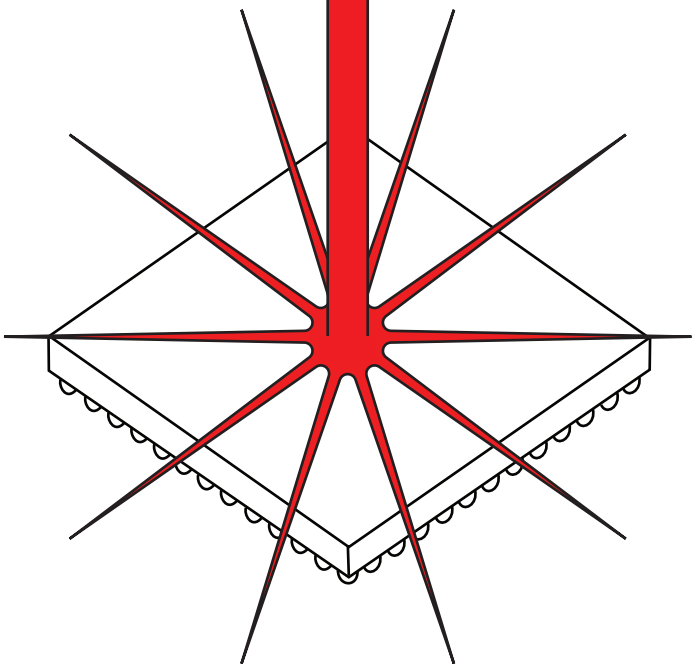
Bachelor's Thesis

Optimized Sample Preparation for effective Laser Fault Injection and Emission Microscopy

Security testing of a WLCSP significantly improved



B.A.P. Swinkels

Bachelor's Thesis

Optimized Sample Preparation for effective Laser Fault Injection and Emission Microscopy

Security testing of a WLCSP significantly improved

B.A.P. Swinkels

January 18, 2023

Electrical Engineering
The Hague University of Applied Sciences
Rotterdamseweg 137, Delft, The Netherlands
First supervisor: Fidelis Theinert
Second supervisor: Stephen O'Loughlin

Riscure B.V.
Delftechpark 49, Delft, The Netherlands
Company Mentor: Santiago Córdoba Pellicer
Internship period: 1 Sep. 2022 - 31 Jan. 2023

Disclaimer
This document describes work undertaken at Riscure as part of a programme of the study Electrical Engineering of the Hague University of Applied Sciences. All views and opinions expressed therein remain the sole responsibility of the author and do not necessarily represent those of the Faculty or Riscure.

Colophon
This document was typeset with the help of KOMA-Script and LaTeX using the kaobook class. The design of the layout is heavily influenced by the attractive typesetting of the theses by Aaron Turon and Théo Winterhalter. The bibliography was processed by biblatex.

Optimized Sample Preparation for effective Laser Fault Injection and Emission Microscopy

Abstract

Laser Fault Injection (LFI) is often used for security testing of Integrated Circuits (IC). The method is based on the fact that a laser can inject a fault into the circuit. For LFI to be effective, the light of the laser must reach the internal circuity of the IC. Unfortunately, this is not always the case, as silicon reflects and absorbs a large amount of light. The same problem occurs with Emission Microscopy (EMMI), where an extremely sensitive camera must capture the tiny amount of photons produced by the switching behavior of a transistor.

This thesis presents two possible ways to improve the effectiveness of LFI and EMMI on an IC. The LFI effectiveness increases if the number of effective faults at certain laser power increases. The EMMI effectiveness increases if the number of acquisitions needed to find a statistically valid result is reduced. The first presented method is to create a thick-film, index-matching coating using glass and immersion oil on the silicon surface. The second method is thinning the silicon through polishing.

The results of LFI and EMMI on unpolished samples, samples with an index-matching coating, and polished samples are compared to see if there is an improvement.

The results of the experiments show that thinning the silicon positively impacts both LFI and EMMI. However, the LFI and EMMI experiments showed no significant difference between the samples with and without an index-matching coating using glass and immersion oil. Future research might investigate the effect of thin-film anti-reflective coatings on light transmission through silicon.

Samenvatting

Laser-foutinjectie (LFI) is een methode die vaak wordt gebruikt voor het testen van de beveiliging van geïntegreerde schakelingen (IC). De methode is gebaseerd op het feit dat een laser een fout in het circuit kan induceren. Om LFI te laten werken, moet het laserlicht het circuit binnenin een IC bereiken. Dit is niet altijd succesvol, omdat silicium een grote hoeveelheid van het licht reflecteert en absorbeert. Hetzelfde probleem doet zich voor bij emissie-microscopie (EMMI), waarbij een uiterst gevoelige camera de kleine hoeveelheid fotonen moet vastleggen die wordt geproduceerd door het schakelgedrag van een transistor.

Deze scriptie presenteert twee mogelijke manieren om de effectiviteit van LFI en EMMI op een IC te verbeteren. De LFI-effectiviteit verbetert wanneer het aantal effectieve fouten bij een bepaalde laser vermogen toeneemt. De EMMI-effectiviteit verbetert als het aantal acquisities af neemt wat nodig is om een statistisch valide resultaat te vinden. De eerste gepresenteerde methode is het creëren van een thick-film, index-matching coating op het siliciumoppervlak door gebruik te maken van glas en immersie olie. De tweede manier is het verdunnen van de siliciumlaag door middel van polijsten.

De resultaten van LFI en EMMI op ongepolijste samples, samples met een index-matching coating en gepolijste samples zijn vergeleken om te zien of er een verbetering plaatsvindt.

De resultaten laten zien dat verdunnen van silicium een positief effect heeft op zowel de effectiviteit van LFI als EMMI. De thick-film, index-matching coating door gebruik te maken van glas en immersie-olie levert echter geen verbetering op. Toekomstig onderzoek zou het effect van thin-film antireflectiecoatings op de lichttransmissie door silicium kunnen onderzoeken.

When a photon comes down, it interacts with electrons *throughout* the glass, not just on the surface. The photon and electrons do some kind of dance, the net result of which is the same as if the photon hit only on the surface.

– Richard Feynman
QED: The Strange Theory of Light and Matter

Preface

Thank you for reading my thesis. I've had a lot of fun researching and writing it, and I hope you can experience that fun while reading it.

I am writing this thesis for my graduation in Electrical Engineering at the Hague University of Applied Sciences in Delft, where I have spent the past four years with great pleasure. Before that, I followed a training in precision engineering. Although it is something completely different, it taught me to work in a structured and precise way and to document my work well. Moreover, it made me discover what I like: creating new things. Fortunately, these are all skills that are immensely useful for Electrical Engineering.

For this thesis, I interned for five months at Riscure, an independent security lab in Delft. Where to my delight, I will soon start working as a security analyst. Security analysis is something that is not offered in an electrical engineering course, but it is an important part of the development of embedded and smart devices. In addition, the skillset of a security analyst has many similarities with that of an electrical engineer. These skills include everything from reverse engineering to low-level, bare metal programming to high-level programming in, for example, Python to control a test setup.

During this internship, I have been given the opportunity to put my accumulated knowledge and skills of recent years into practice and got the chance to learn many new things. I look forward to sharing that knowledge. I wish you a good read!

Bob Swinkels
Delft, January 18, 2023

Acknowledgements

(There is no real order in which the acknowledgments are listed)

You are about to read my thesis, which I wrote during my internship at Riscure.

First and foremost, I would like to thank my company mentor Santiago Córdoba Pellicer for his warm presence and availability during my thesis internship. Santi has the ability to make you feel at ease and to make you feel like you are part of the team. Often he suddenly appears, just when you need it, to give you a nudge in the right direction. He has been a great help in my internship, and I am very grateful for his guidance and support.

I want to thank all my future colleagues at Riscure for their warm welcome and support during my internship. I am very excited to start working with you all. I would especially like to thank Chris, Dennis, Rafa, and Barış for helping me with my research and setups. Not to forget Tin and Wim from lab support, who are always there when you need something.

My first coach from the Hague University of Applied Sciences, Fidelis Theinert, was very helpful during my internship. He was always available for questions, and he was very supportive. I want to thank him for that as well as for his guidance during my internship.

I would like to thank my parents, Johan and Nicolette, for proofreading and catching a few writing mistakes.

Last but not least, I would like to thank my wife, Paula, for her support and patience. She was there for me when I needed her and always there to listen while I just went rambling on about very technical topics. I am very grateful for her support, and I love her very much.

Contents

List of Figures

List of Tables

List of Listings

Prologue

1

Introduction

1.1 MOTIVATION

Riscure is an independent security lab in Delft that evaluates the security of software, chip technology, and embedded/connected devices. Riscure performs security assessments and often uses Laser Fault Injection (LFI) and Emission Microscopy (EMMI) for this:

- LFI uses a laser to transmit light through the silicon of a chip to disturb the behavior of a device while a secure operation occurs. LFI can be used, for example, to flip a single bit in a static memory cell of a microcontroller. [1, 2].
- EMMI is used when performing side channel analysis to detect photons emitted by the logic inside the Integrated Circuit (IC). Therefore targeting single transistors becomes possible. For this, an InGaAs detector is used because of its high spectral sensitivity in the infrared and near-infrared spectrum. [3]

[1]: Dutertre et al. (2012), *Fault Round Modification Analysis of the Advanced Encryption Standard*
[2]: Vasselle et al. (2017), *Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot*
[3]: Orlic et al. (2012), *Simple Photonic Emission Analysis of AES - Photonic Side Channel for the Rest of Us*

A device is usually approached from the silicon side when performing LFI and EMMI. Therefore light has to travel through the silicon of the IC. Silicon is more "transparent" for light with longer wavelengths. Therefore infrared light in the 1064 nm range is used. Even though the silicon is more transparent to infrared light than to visible light, the silicon reflects and absorbs a large portion of the infrared light.

Riscure has multiple laser sources available, some of which can supply up to 30W of optical power [4]. However, the laser source is sometimes not powerful enough to induce a fault in a specific target, and LFI is unsuccessful. Therefore samples are thinned by an external company. This is done by using a mechanical process that removes a layer of silicon from the sample. As a result, the thickness of the sample is reduced by 50% on average. After thinning, fault injection is usually successful. However, it is unknown if further thinning of the sample would result in increased effectiveness of LFI.

[4]: Riscure (n.d.), *Diode Laser 1064nm NIR (30W, 50MHz, Multimode)*

1.2 RESEARCH GOALS

This study aims to determine if sample preparation can improve the effectiveness of LFI and EMMI on an IC. The effectiveness of LFI increases if the number of effective faults at certain laser power increases. The effectiveness of EMMI increases if the number of acquisitions needed to find a statistically valid result is reduced. This thesis validates two possible methods to improve the effectiveness of LFI and EMMI:

1. By creating a thick-film, index-matching coating using glass and immersion oil on the silicon surface.
2. By thinning the silicon through polishing.

The results of LFI and EMMI on modified and unmodified samples will be compared to see if there is an improvement.

1.3 HYPOTHESIS

The amount of light transmitted through the silicon of an IC can be expressed as the transmission coefficient T, the fraction of light that is not reflected or absorbed by the silicon.

- An anti-reflective coating on top of the silicon will transmit part of the light previously reflected through the silicon, resulting in a lower reflection coefficient and a higher transmission coefficient.
- The amount of light absorbed by the silicon depends on the absorption coefficient and thickness. As the absorption coefficient for a specific wavelength of light is constant, the only variable is the thickness of the sample. Because of that, by thinning the sample, the absorption coefficient is reduced, and the transmission coefficient is increased.

Earlier studies have shown that the transmission coefficient of the silicon of an IC can be improved by thinning the silicon [5] or by using an anti-reflective coating [6, 7]. This research indicates that the transmission coefficient can be improved. However, it still needs to be researched if the effectiveness of LFI and EMMI can be improved by using an anti-reflective coating or thinning the silicon. It is hypothesized that this is indeed the case and that the effectiveness of LFI and EMMI can be improved by using an anti-reflective coating or by thinning the silicon.

[5]: He et al. (2016), *Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection*

[6]: Davis et al. (2000), *Antireflection Coatings for Semiconductor Failure Analysis*

[7]: Wang et al. (2001), *Effect of Ga Staining Due to FIB Editing on IR Imaging of Flip Chips*

1.4 THESIS OVERVIEW

This thesis is organized as follows:

Chapter 2, Chapter 3, and Chapter 4 provide an overview of the background knowledge required to understand the rest of the thesis. Chapter 5 describes the equipment used for the setups and experiments in this thesis.

Part 'Sample preparation' describes the preparation of the samples. Chapter 6 describes the coating used for the experiments, and Chapter 7 describes the thinning process used to thin the samples.

Part 'Laser Fault Injection' describes the LFI background (Chapter 8), the setup and method (Chapter 9), and the results (Chapter 10) of the experiments.

Part 'Emission Microscopy' describes the EMMI background (Chapter 11), the setup and method (Chapter 12), and the results (Chapter 13) of the experiments.

Lastly, Chapter 14 summarizes the results, and the discussion is given in Chapter 15, which discusses future work and explains the results.

2

Structure of an Integrated Circuit

2.1 Semiconductor Packaging

Semiconductor packaging is the process of enclosing and protecting the active components of an IC, such as transistors and other electronic components, in a package that can be easily connected to the external circuitry of a device. There are several different types of semiconductor packaging methods, including:

- *Dual In-line Package (DIP)*: A DIP is an IC package with two parallel rows of external pins. DIPs are typically used for through-hole mounting, in which the pins are inserted into holes in a printed circuit board (PCB) and soldered in place, or they are inserted into a socket.
- *Pin Grid Array (PGA)*: A PGA is an IC package with a grid of external pins arranged in rows and columns. PGAs are typically inserted into a socket or mounted on a PCB using a through-hole method, in which the package is soldered directly to the PCB.
- *Ball Grid Array (BGA)*: A BGA is an IC package with a grid of external balls, rather than pins, that connect the package to the external circuitry. BGAs are typically used for surface mount technologies (SMT) and offer a higher density of connections than PGAs.
- *Package On Package (POP)*: A POP is a type of IC package in which one package is stacked on top of another package, allowing for more compact packaging. POPs are typically used in portable electronic devices where space is limited.
- *Wafer Level Chip Scale Packaging (WLCSP)*: A WLCSP is one of the smallest package types currently available on the market. WLCSPs are commonly used in modern smartphones because of their small size [8].

[8]: LaPedus (2015), *Fan-Out Packaging Gains Steam*

2.2 Wafer Level Chip Scale Packaging

A WLCSP consists of a bare die with a redistribution layer (RDL) on top. The purpose of the RDL is to relocate the I/Os on the die to their corresponding bump locations of the ball grid array (BGA). The redistribution layer is surrounded by two repassivation layers [9] (shown in Figure 2.1).

[9]: NXP Semiconductors (2016), *AN10439 Wafer Level Chip Scale Package*

A WLCSP with a BGA can be soldered just like any other BGA package, but the orientation internally is flipped in regards to a standard BGA package. This is called a flip-chip, as the silicon side points away from the PCB. Because the silicon side is on top and exposed, a WLCSP requires significantly less sample preparation to access the silicon side. [10].

[10]: Swinkels (2021), *PHYSICAL ATTACK ON A WLCSP*

2.3 The STM32G061F8Y6TR

For this thesis, the samples used are the STM32G061F8Y6TR microcontroller. This microcontroller is chosen as it is widely available, actively produced by ST Microelectronics, and is available in a WLCSP-20 form factor. The STM32G061F8Y6TR is an ultra-low-power microcontroller with a high-performance Arm Cortex-M0+ 32-bit RISC core operating at a 64 MHz frequency, hardware AES, and a true random number generator [11].

[11]: ST Microelectronics (n.d.), *STM32G061F8Y6TR*

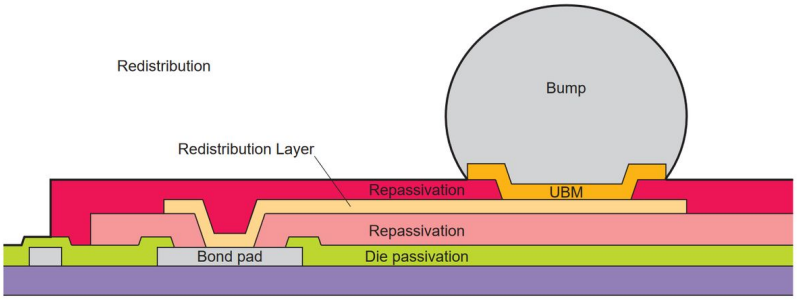


Figure 2.1: Layers of a WLCSP [9].

The WLCSP-20 package is very small, about 1.94mm by 2.40mm in size, shown in Figure 2.2.

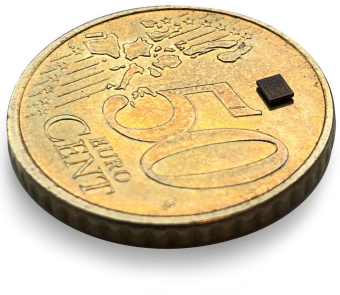


Figure 2.2: WLCSP-20 package on top of a 50-cent coin for scale.

A breakout board is ordered from Proto Advantage on which the STM32G061F8Y6TR can be soldered, making the device easier to work with. The breakout board is shown in Figure 2.3.

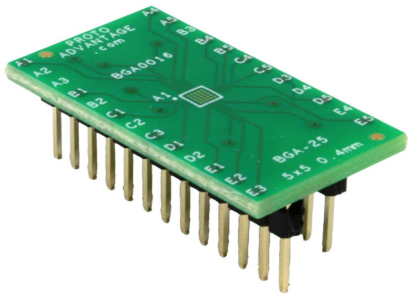


Figure 2.3: Breakout board for the STM32G061F8Y6TR.
Source: [12]

3

Fault Injection

Fault Injection is the art of finding out how a system behaves while being perturbed and therefore operates outside its rated operating conditions. For some conditions, the system resets or stops responding, while unexpected behavior is observed for others. Often this "misbehavior" can be exploited to to defeat security features, or compromise system assets.

3.1 Fault Injection Methods

There are different ways to induce faults in (the hardware of) a system:

3.1.1 *Voltage glitching*

Adjusting the supply voltage outside the normal operating range for a brief period may cause the processor to skip instructions or misinterpret them [13]. To maximize the effectiveness of voltage glitching, external capacity, like decoupling capacitors, needs to be removed, and power lines need to be as short as possible.

[13]: Bar-El et al. (n.d.), *The Sorcerer's Apprentice Guide to Fault Attacks*

3.1.2 *Clock glitching*

By inserting an additional, shorter clock cycle between two other clock edges, it is possible to cause an instruction miss or a data misread. In case of the instruction miss, the program counter increments, and the processor executes the next instruction before the execution of the current instruction is completed. In case of a data misread, the processor tries to read the value from the bus before the memory has time to latch the requested value. [14]

[14]: Barenghi et al. (2012), *Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures*

Clock glitching is usually the most effective on older devices that do not have an internal clock. Newer devices often have an internal clock for the actual processing. They only use the external clock signal to synchronize the communications with external devices or as a reference for the internal clock (PLL). [15]

[15]: Aarts (2013), *Electromagnetic Fault Injection Using Transient Pulse Injections*

3.1.3 *Electromagnetic glitching*

Electromagnetic fault injection (EMFI) induces high-power electromagnetic pulses in a specific part of a circuit. Due to the highly localized effect of EMFI, the same results as voltage glitching can be achieved while circumventing countermeasures specifically implemented to prevent voltage glitching. [16]

[16]: Thessalonikefs (2014), *ElectroMagnetic Fault Injection Characterization*

3.1.4 *Temperature*

When RAM cells are heated above the upper-temperature threshold specified by the manufacturer, they may be randomly modified. When cooling the RAM cells, the temperature can be tuned such that the cells reach a point where write operations work but read operations do not or the other way around. [13]

3.1.5 *Optical Fault Injection*

An electron is emitted when a photon with a high enough energy level interacts with a semiconductor. This is called the photoelectric effect, and almost all circuits are sensitive to it. This is one of the reasons integrated circuits are usually packaged inside opaque black epoxy. [14]

[14]: Barenghi et al. (2012), *Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures*

Through this means, light can be used to induce a current in specific parts of a circuit. A specific circuit area can be targeted using a laser, such as a single bit in a register. The feasibility of being able to target a single bit depends on the feature size of the sample and the laser spot size. [17]

[17]: Agoyan et al. (2010), *Single-Bit DFA Using Multiple-Byte Laser Fault Injection*

3.2 DIFFERENT TYPES OF FAULTS

Electronic circuits can be subject to various types of faults, which can be classified into two categories: transient and permanent. Transient faults, also known as provisional faults, are temporary disruptions in the normal behavior of an electronic circuit. These faults are usually caused by the ionization of silicon, which can induce a current falsely interpreted by the circuit as an internal signal. However, once the device is reset and the ionization ceases, the induced current and the resulting faulty signal also disappear, and the chip returns to its normal behavior. On the other hand, permanent faults, also known as destructive faults, are caused by purposely inflicted defects to the structure of the chip. These defects permanently affect the behavior of the chip, which means that the chip will not return to its normal functioning once inflicted. [13, 18]

[13]: Bar-El et al. (n.d.), *The Sorcerer's Apprentice Guide to Fault Attacks*
[18]: Clark et al. (1995), *Fault Injection: A Method for Validating Computer-System Dependability*

When using fault injection to attack an IC, transient faults are preferred because they allow faults to be tested under different experimental conditions until the desired effect is achieved. Moreover, the system remains functional after the completion of the attack, which is not the case with destructive faults. Destructive faults usually render the target unusable and require the manufacturing of a clone, which is not an efficient or cost-effective approach. [13]

[13]: Bar-El et al. (n.d.), *The Sorcerer's Apprentice Guide to Fault Attacks*

3.3 COUNTERMEASURES

Chip manufacturers can implement a variety of hardware protections to protect against fault injection attacks. These protections include light detectors, supply voltage detectors, frequency detectors, active shields, and hardware redundancy measures [13]:

- *Light detectors* detect changes in the light gradient and can be used to protect against fault injection attacks involving light.
- *Supply voltage detectors* react to abrupt variations in the applied potential and can be used to detect and protect against fault injection attacks that involve supply voltage.
- *Frequency detectors* impose an interval of operation outside which the electronic circuit will reset itself and can be used to protect against fault injection attacks that involve frequency.
- *Active shields* are metal meshes that cover the entire chip and have data passing continuously through them. If there is a disconnection or modification of the mesh, the chip will not operate, protecting against fault injection attacks that involve probing. An active shield also mitigates EMFI as the shield usually prevents the EM energy from penetrating to lower metal layers where the sensitive circuitry is located.

- *Hardware redundancy measures* consist of duplicating certain logical operations in hardware and comparing their output before processing the output. If the outputs do not match, the chip will reset itself, protecting against fault injection attacks that involve logic.

Software countermeasures can be implemented when hardware countermeasures are insufficient or when there is a need to protect against future attack techniques that defeat present-generation hardware countermeasures. There are a variety of software countermeasures that can be used to protect against fault injection attacks, some of which can also be implemented in hardware [13]:

[13]: Bar-El et al. (n.d.), *The Sorcerer's Apprentice Guide to Fault Attacks*

- *Checksums*: Checksums can be implemented in software to detect and correct errors in data. This is often complementary to hardware checksums, as software checksums can be applied to buffer data (sometimes fragmented over various physical addresses) rather than machine words.
- *Execution randomization*: If the order is randomized in which operations in an algorithm are executed, it becomes difficult for an attacker to predict what the machine is doing at any given cycle. This can slow down a determined adversary but may not be effective against attacks requiring faults in specific places or orders.
- *Variable redundancy*: Variable redundancy is a software implementation of Simple Duplication with Comparison (SDC), in which hardware blocks are duplicated, and the results are compared to detect and correct errors.
- *Execution redundancy*: Execution redundancy involves repeating algorithms and comparing the results to verify that the correct result is generated. This can be more secure if the second calculation is different than the first (for example, its inverse) so that two identical faults cannot be used at different times.
- *Ratification counters and baits*: Baits are small code fragments that perform an operation and test its result. When a bait detects an error, it increments a non-volatile memory (NVM) counter. The system ceases to function when this counter exceeds a tolerance limit (usually three).

4

Optical properties of materials

4.1 Reflection and absorption of an optical medium

The refractive index of a material, given by definition 4.1.1, is a scalar quantity representing the ability of a medium to "slow down" light that is passing through it.

Definition 4.1.1 *The absolute refractive index n of an optical medium is equal to the ratio of the speed of light in a vacuum, $c = 299792458m/s$, and the phase velocity v of light in the medium.*

$$n = \frac{c}{v}$$

When given two materials with known refractive indices, Fresnel's equations, given by definition 4.1.2, can be used to determine the reflection and transmission at the interface between these materials.

Definition 4.1.2 *Fresnel's equations determine that reflectance for s-polarized light on the interface between a material with refractive index n_1 and material with refractive index n_2, where the angle of the incident ray and the refracted ray with the normal of the interface are given as respectively θ_i and θ_t, is equal to:*

$$R_s = \left| \frac{n_1 \cos\theta_i - n_2 \cos\theta_t}{n_1 \cos\theta_i + n_2 \cos\theta_t} \right|^2$$

Similarly, the reflectance for p-polarized light on the interface is equal to:

$$R_p = \left| \frac{n_1 \cos\theta_t - n_2 \cos\theta_i}{n_1 \cos\theta_t + n_2 \cos\theta_i} \right|^2$$

If the angle of the incident ray and the refracted ray with the normal of the interface is equal to 0, $\theta_i = \theta_t = 0$, which is called "normal incidence," the reflectance on the interface can be simplified to:

$$R = \left| \frac{n_1 - n_2}{n_1 + n_2} \right|^2$$

Because of the law of conservation of energy, the transmission T is equal to the portion of the incident power that is not reflected.

Respectively, transmission for s-polarized light through the interface is equal to:

$$T_s = 1 - R_s$$

Respectively, transmission for p-polarized light through the interface is equal to:

$$T_p = 1 - R_p$$

Respectively the transmission of light with normal incidence through the interface is equal to:

$$T = 1 - R$$

Transmission through an interface is inversely proportional to the reflection, but the transmission through a material gets further reduced if the material has an absorption coefficient κ larger than 0. This absorption coefficient often gets expressed as the complex refractive index given in definition 4.1.3.

Definition 4.1.3 *The complex refractive index $\underline{n}$ of an optical medium is equal to the absolute refractive index n, plus the absorption coefficient κ.*

$$\underline{n} = \frac{c}{v} + i\kappa$$

4.2 OPTICAL PROPERTIES OF CRYSTALLINE SILICON

In 2015 Schinke et al. [19] published a paper about their measurements of the optical properties of crystalline silicon and the uncertainty of those measurements.

[19]: Schinke et al. (2015), *Uncertainty Analysis for the Coefficient of Band-to-Band Absorption of Crystalline Silicon*

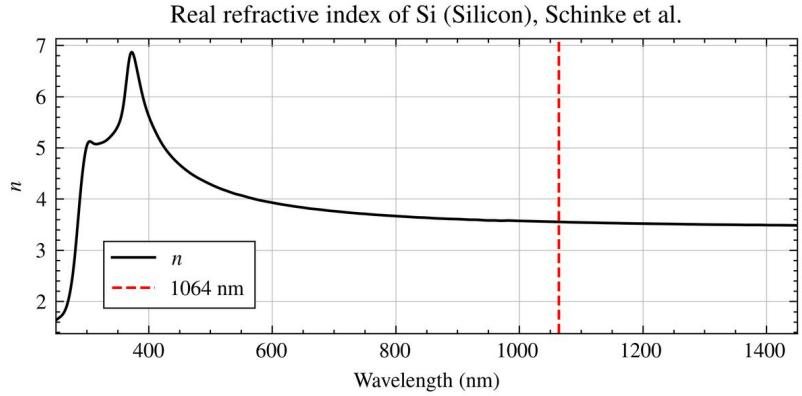


Figure 4.1: The real part of the refractive index of crystalline silicon according to Schinke et al.

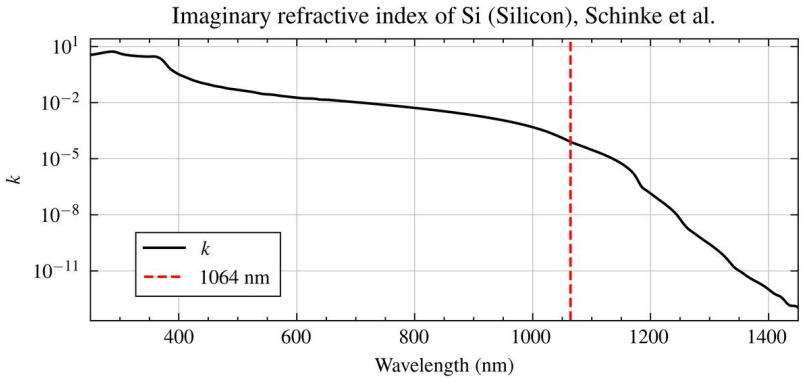


Figure 4.2: The imaginary part of the refractive index of crystalline silicon according to Schinke et al.

Figure 4.1 shows the real part of the refractive index of crystalline silicon, and Figure 4.2 shows the imaginary part of the refractive index of crystalline silicon. From the results of Schinke et al., it becomes clear that the real and imaginary parts of the complex refractive index of crystalline silicon depend on the wavelength.

Using the real ($n_{1064\text{nm}} = 3.5549$) and imaginary ($\kappa_{1064\text{nm}} = 81.110 \cdot 10^{-6}$) components, the formula the complex refractive index of crystalline silicon for a wavelength $\lambda = 1064\text{nm}$ can be determined and is given in equation (4.1).

$$\underline{n}_{1064\text{nm}} = 3.5549 + 81.110i \cdot 10^{-6} \tag{4.1}$$

Using definition 4.1.2 and equation (4.1), the reflectance of an air-silicon interface for light at normal incidence with a wavelength of 1064nm can be determined, see equations (4.2, 4.3).

$$R = \left|\frac{n_1 - n_2}{n_1 + n_2}\right|^2 = \left|\frac{1 - 3.5549}{1 + 3.5549}\right|^2 = 0.3146 = 31.46\% \tag{4.2}$$

$$T = 1 - R = 1 - 0.3146 = 0.6854 = 68.54\% \tag{4.3}$$

The absorption coefficient formula can be derived from Maxwell's equations. The absorption coefficient describes the fractional decrease in light intensity with distance. The absorption coefficient is given in definition 4.2.1.

Definition 4.2.1 *The absorption coefficient α of an optical medium equals the fractional decrease in light intensity with distance. The absorption coefficient α depends on the wavelength λ and the absorption coefficient κ.*

$$\alpha = \frac{4\pi\kappa}{\lambda}$$

Using definition 4.2.1 and equation (4.1), the absorption coefficient of crystalline silicon for a wavelength of 1064nm can be determined, see equation (4.4).

$$\alpha = \frac{4\pi\kappa}{\lambda} = \frac{4\pi \cdot 81.110 \cdot 10^{-6}}{1064 \cdot 10^{-9}} = 957.950\text{m}^{-1} = 9.5795\text{cm}^{-1} \tag{4.4}$$

The fraction of light absorbed is proportional to the thickness of the material. Therefore almost all light is absorbed when the thickness of the silicon is larger than 1mm. This is shown in Figure 4.3.

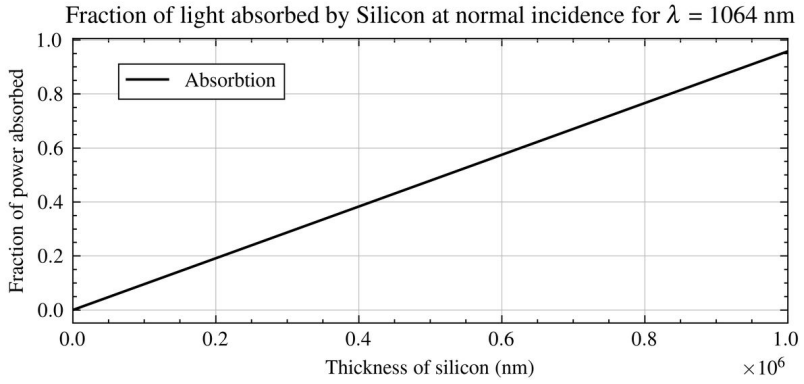


Figure 4.3: Thickness vs. the fraction of power absorbed by crystalline silicon.

5

Riscure Equipment

5.1 Riscure's Inspector FIPy

Inspector FIPy is a powerful Python-based framework for performing scripted fault injection setups. This tool is fully customizable and adaptable to specific targets, making it a versatile tool for performing FI testing on various devices and systems. In addition, Riscure's FIPy also includes a visual analysis tool called FI Spotlight, which allows for fast and accurate analysis of results, providing valuable insights into the vulnerabilities of a system. Inspector FIPy can be used to control the Riscure Laser Station (see Section 5.2), the Riscure Spider (see Section 5.4), the InGaAs camera (see Section 5.5), and VISA devices like the Keysight B2902B (see Section 5.6).

5.2 Riscure Laser Station

The Laser Station 2 (shown in Figure 5.1) is a device used to perform advanced laser fault attacks on smart cards to assess their security against such attacks. It offers a range of new features and advanced capabilities, such as the ability to support front and back-side attacks, a heavy stable base for high magnifications, and integration with software and fault analysis modules. Various laser sources are available, including blue, green, red, and NIR, and a zoomable camera for easy navigation. Additionally, it has an automated Z-axis, spot sizes down to 1um, and fast multi-time glitching. Lastly, it has a motorized XYZ stage for automatically scanning the surface of a chip with high repetition accuracy. An SDK is available for integration into custom setups and has an FDA/CE-approved safety enclosure. [20]

[20]: Riscure (2018), *Laser Station 2*

Figure 5.1: Riscure Laser Station
Source: [20]

5.3 Riscure Diode Laser 1064nm NIR

The Diode Laser 1064nm NIR (shown in Figure 5.2) is a high-power diode laser that is multi-mode and selected for its high power rating. This allows for coarse chip surface scanning with a large spot size and sufficient intensity within the spot. It has a configurable pulse length, high pulse frequency, short delay, and minimal jitter. The pulse length can be as small as 2ns, and the high

pulse frequency allows for multi-pulse fault injection attacks. The laser diode has minimal aging and can be integrated with Riscure products such as Laser Station (see Section 5.2). The Riscure Spider controls the optical power and laser timing (see Section 5.4). [21]

[21]: Riscure (2022), *Diode Laser 1064nm NIR (30W, 50MHz, Multimode)*

Figure 5.2: Riscure Diode Laser 1064nm
Source: [21]

5.4 RISCURE SPIDER

The Spider (shown in Figure 5.3) is a workbench tool for interacting with embedded devices during side channel analysis and fault injection testing. It simplifies the setup process by providing a single point of control for I/O and reset lines and can be controlled from the Inspector software or as a standalone device. It can read and respond to signals associated with protocols such as JTAG, I2C, and SPI, providing an information channel to the internal processing state of the targeted hardware. Additionally, it can generate arbitrary glitch waves with a high time resolution and custom wave shapes, allowing for specific testing of embedded chipsets and stretching their robustness. [22]

[22]: Riscure (2022), *Spider*

Figure 5.3: Riscure Spider
Source: [22]

5.5 INGAAS CAMERA

The AV Goldeye G-008 from Allied Vision (shown in Figure 5.4) is a camera that uses an InGaAs sensor to capture images in short wave infrared (SWIR) range. The SWIR technology lets the camera capture light in the electromagnetic spectrum between the visible and mid-infrared ranges. This camera is used for EMMI purposes, which allows for an overview of the interesting parts of a chip to pinpoint fault injection attempts precisely. The camera has 320 (H) x 256 (V) pixels, an active sensor size of 9.6 mm x 7.7 mm, and a frame rate of 344 frames/s. Its spectral sensitivity range is between 900 - 1700 nm, and it uses a 14-bit A/D converter for digitalization. [23]

[23]: Riscure (2022), *AV GoldEye G-008 InGaAS Camera (EMMI)*

5.6 SOURCE MEASURE UNIT

The Keysight B2902B (shown in Figure 5.5) is a precision source/measure unit that is a 2-channel, compact and cost-effective benchtop device that can source and measure both voltage and current. It includes application software that facilitates PC-based instrument control and has high throughput and

Figure 5.4: AV GoldEye G-008 InGaAS Camera from Allied Vision
Source: [23]

SCPI command support. It is controllable using VISA drivers to automate measurement setup. [24]

[24]: Keysight (2022), *B2902B Precision Source / Measure Unit (2 Ch, 100 fA)*

Figure 5.5: B2902B Precision Source / Measure Unit
Source: [24]

Sample preparation

6

Anti-reflective coatings

Anti-reflective coatings are films applied to surfaces to reduce the amount of light that is reflected. These coatings are used in various applications, such as optical lenses, solar cells, and electronic displays. This chapter documents the steps to find a suitable coating for this study.

6.1 Types of anti-reflective coatings

Two effects make an anti-reflective coating work. These are *thick-film* and *thin-film* effects. The thick-film effect is caused by the refractive index of the coating and is described in Subsection 6.1.1. The thin-film effect is caused by the thickness of the coating and is described in Subsection 6.1.2.

6.1.1 *Index matching coating*

When a material, for example, glass, is coated with a material with a different refractive index, the top of the coating will reflect light as well as the interface between the two materials. The amount of reflected light depends on the angle of incidence and the refractive indices of the two materials. As given by definition 4.1.2, the reflection coefficient R at normal incidence between a material with refractive index n_1 and a material with refractive index n_2 is given by $R = \left|\left(n_2 - n_1\right)/\left(n_2 + n_1\right)\right|^2$ and its transmission is given by $T = 1 - R$.

The reflection on an interface between glass ($n \approx 1.5$) and air ($n \approx 1$) is given by equation (6.1). If the glass now is coated with a material with a refractive index that is the geometric mean of the refractive indices of the surrounding materials $n = \sqrt{1 \cdot 1.5} = 1.225$, the reflection coefficient is given by equations (6.2, 6.3). The reflection coefficient is now only half of what it was before applying the coating.

$$R = \left|\frac{1.5 - 1}{1.5 + 1}\right|^2 = 0.04 \tag{6.1}$$

$$R = R_{\text{air-coating}} + \left(1 - R_{\text{air-coating}}\right) \cdot R_{\text{coating-glass}} \tag{6.2}$$

$$R = \left|\frac{1.225 - 1}{1.225 + 1}\right|^2 + \left(1 - \left|\frac{1.225 - 1}{1.225 + 1}\right|^2\right) \cdot \left|\frac{1.5 - 1.225}{1.5 + 1.225}\right|^2 = 0.02 \tag{6.3}$$

The same can be applied to crystalline silicon, which has a refractive index of $n \approx 3.6$. The reflection coefficient of crystalline silicon is given by equation (6.4). An optimal coating with a refractive index of $n = \sqrt{1 \cdot 3.6} = 1.90$ would reduce the reflection coefficient according to equation (6.5) to 18%.

$$R = \left|\frac{3.6-1}{3.6+1}\right|^2 = 0.319 \tag{6.4}$$

$$R = \left|\frac{1.9-1}{1.9+1}\right|^2 + \left(1 - \left|\frac{1.9-1}{1.9+1}\right|^2\right) \cdot \left|\frac{3.6-1.9}{3.6+1.9}\right|^2 = 0.18 \tag{6.5}$$

6.1.2 *Interference coating*

An interference coating is a coating that is designed to reduce the reflection of light at a specific wavelength. In theory, this is an index-matching coating of which the thickness is precisely tuned to cancel the reflection by destructive interference. Therefore the coating needs to have a thickness of $d = \lambda/4$, where λ is the wavelength of the light on which the coating needs to be tuned, and refractive index $n = \sqrt{n_1 \cdot n_2}$, see Figure 6.1. [25]

[25]: Edmund Optics (n.d.), *Anti-Reflection (AR) Coatings*

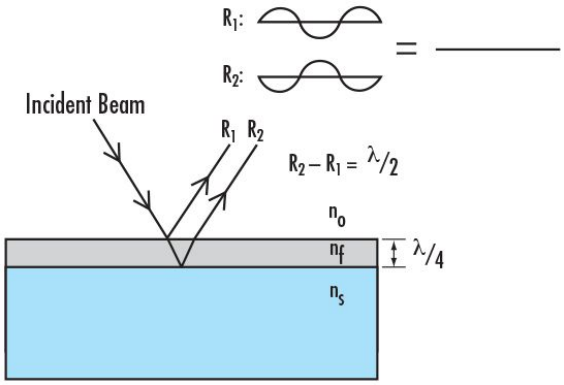


Figure 6.1: Interference coating
Source: [25]
Note: the incident beam is only drawn at an angle for illustrative purposes, its real orientation is at normal incidence.

6.2 APPLYING THE COATING

Thin-film coatings will typically be applied through a vapor deposition process or a sputtering process. In vapor deposition, the coating is applied by evaporating the material from a heated source and depositing it on the substrate. In a sputtering process, the coating is applied by bombarding the substrate with ions of the material. The ions will then deposit on the substrate. As both these methods are very expensive and require a clean room, they are typically only used for large-scale production, and the cost is high. [26]

[26]: Vandendriessche (2016), *No One-Size-Fits-All Approach to Selecting Optical Coatings*

Thick-film coatings can be applied through means of spin or dip coating. In spin coating, the coating is applied by spinning the substrate at high speed and applying the coating on the substrate. The coating will then spread out over the substrate. This method is relatively cheap and can be done in a regular laboratory. In dip coating, the coating is applied by dipping the substrate in the coating. Both methods are relatively cheap and can be done in a regular laboratory. [27]

[27]: Thomas (1994), *Optical Coating Fabrication*

Because of the high cost and specific equipment needed for applying thin-film coatings, they are considered out of scope for this thesis. Therefore the focus will be on thick-film coatings.

6.3 COATING MATERIAL

The coating needed for this study needs to be transparent in the visible spectrum and have a refractive index of $n \approx 1.9$. The coating also needs to be able to be applied through the means of spin coating. The coating needs to

withstand a temperature of at least 200°C as the sample needs to be soldered after coating.

Such a coating is not readily available. The closest coating found is the *Norland Optical Adhesive 170* [28], which has a refractive index of 1.70 and can only withstand temperatures up to 100°C as it is polymer-based. This coating is UV curable, but this has to be done under a nitrogen atmosphere to prevent oxygen inhibition. Therefore the spin coating setup must have a built-in UV light source and a nitrogen purging system.

[28]: Norland Products (2022), *NOA170*

As such a setup is not readily available, it was decided to search for an alternative method to verify the effectiveness of an anti-reflective coating because building a custom spin coating setup is not the main focus of this thesis.

6.4 ALTERNATIVE METHOD

While an ideal index-matching coating would have a refractive index equal to the geometric mean of the refractive indices of the surrounding materials, it is not necessary to have a coating with a refractive index of exactly 1.9. The reflection coefficient should theoretically be reduced if the coating has a refractive index between refractive indices of the surrounding materials.

For the alternative method, inspiration is taken from another field of science, namely biology and material science. When small structures need to be imaged, immersion microscopy is used, shown in Figure 6.2. In this method, the sample is placed in a liquid with a refractive index equal to the refractive index of glass, and the objective lens is placed in direct contact with the liquid, thus eliminating the air-glass interface. Because of this, a lot more light enters the objective.

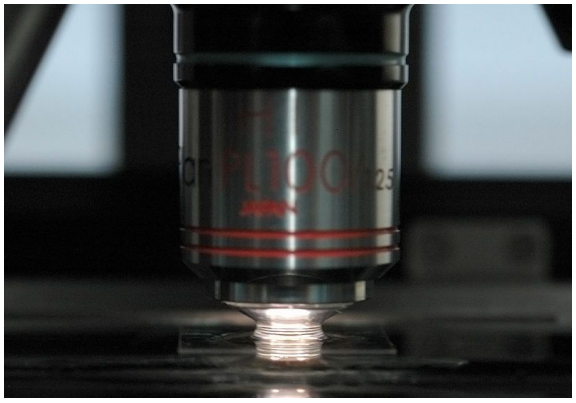


Figure 6.2: Immersion microscopy
Source: [29]

While immersion microscopy would be a solution to improve the transmission through the silicon, special objective lenses are needed. In addition, laser stations need to be modified as the objective lenses used in the existing setups are unsuitable for immersion microscopy. However, the liquid used for immersion microscopy is affordable and commonly available. Therefore it was decided not to go down this path but instead apply the principle of immersion microscopy to emulate an index-matching coating.

6.5 EXPERIMENTAL SETUP

The emulated coating used in this study is shown in Figure 6.3. The black layer on top of the silicon layer of the IC, in which the part number is laser-engraved, is scraped off using a scalpel with a Swann Morton ACM No 17 Blade. The Swann Morton ACM No 17 Blade is a chisel-like blade with a straight edge. On top of the now exposed silicon, a drop of immersion oil [30] is placed using a

[30]: Boomlab (n.d.), *Immersie-Olie Voor Microscopie*

Pasteur pipette. An optical flat is a piece of glass that is polished so that the top and bottom are almost perfectly parallel (in this case, they are parallel within $< 00'05"$). The optical flat used (OPB-10C01-10-5) is produced by OptoSigma! and will be placed on top of the immersion oil drop [31]. The optical flat has the same refractive index as the immersion oil, so that it will form a single interface. This interface will act as an index-matching coating.

[31]: OptoSigma! (2021), *Optical Parallel / OPB-10C01-10-5*

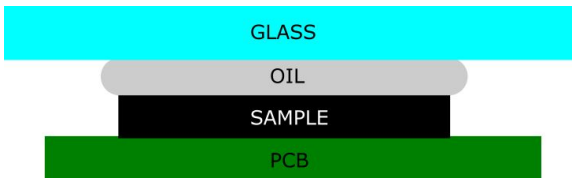


Figure 6.3: Emulated coating

Silicon without a coating would have a theoretical reflection coefficient of $R = 0.319$ and therefore reflect 31,9% of the incoming light, see equation (6.6). On the other hand, the reflection coefficient of silicon with the emulated coating is $R = 0.203$, and therefore, only 20.3% of the light would be reflected, see equation (6.7).

$$R = \left|\frac{3.6-1}{3.6+1}\right|^2 = 0.319 \tag{6.6}$$

$$R = \left|\frac{1.5-1}{1.5+1}\right|^2 + \left(1 - \left|\frac{1.5-1}{1.5+1}\right|^2\right) \cdot \left|\frac{3.6-1.5}{3.6+1.5}\right|^2 = 0.203 \tag{6.7}$$

The final result is shown in Figure 6.4.

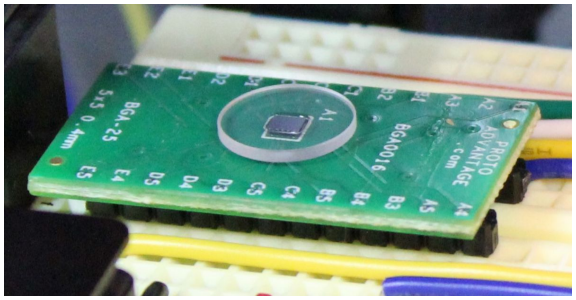


Figure 6.4: Sample with refraction oil and glass on top.

The only thing that cannot be accurately controlled is the thickness of the oil and glass layer. Therefore three different optical flats will be used, numbered "glass1", "glass", and "glass3". If the tickness is of influence on the results, the expected results should be different for all three samples.

7

Polishing

Polishing a semiconductor has to happen carefully as it can easily damage the device, and the goal is for the device to still be fully functional after polishing.

7.1 POLISHING EQUIPMENT

The MetPrep 3 grinding/polishing machine is used, shown in Figure 7.1. The MetPrep 3 is a grinding and polishing machine that allows for the use of various polishing papers and polishing suspensions to achieve a polished surface. The process involves gradually moving to a finer grid during polishing for optimal results.

Figure 7.1: MetPrep 3 grinding/polishing machine
Source: [32]

7.2 TRIPOD POLISHER

A tripod polisher is a valuable tool for sample thinning. It provides a stable base for holding the specimen while allowing easy movement and control. The tripod polisher is set up for wedge polishing. Then the sample is mounted to the pyrex rod using Crystalbond 509, a transparent adhesive that provides excellent adhesion. Crystalbond 509 is preferred over waxes as it is transparent in thin cross-sections, minimizes clogging of diamond tools compared to waxes, and can be easily removed by dissolving it in acetone [33]. After this, the polishing process can begin.

[33]: Ted Pella, Inc. (n.d.), *Crystalbond™ Adhesives*

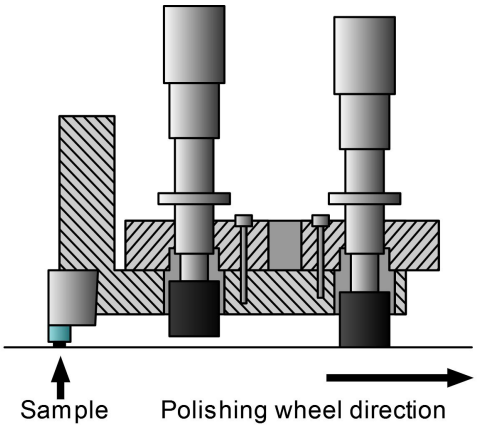


Figure 7.2: Tripod polisher

7.3 POLISHING PROCESS

In addition to the research documented in this thesis, a polishing process was developed for thinning samples based on [34–38] using the MetPrep 3 machine, a tripod polisher, and disposables from Bueler. The polishing process will be made available internally at Riscure. A summary of the procedure is given in Table 7.1.

After each polishing step, the sample is inspected under the microscopy setup with an infrared camera to check if the surface is smooth enough and if the polished surface is planar to the internal features of the sample. If the sample is not planar, the micrometers on the tripod polisher are compensated for this before continuing to the next step. The compensation is calculated using basic geometry. An example of the calculations is given by equations (7.1-7.5) with accompanying Figure 7.3.

[34]: Buehler (2004), *Buehler Sum-Met: The Science behind Materials Preparation*
[35]: Benedict et al. (1991/ed), *Recent Developments in the Use of the Tripod Polisher for TEM Specimen Preparation*
[36]: Ted Pella, Inc. (2018), *PELCO® Tripod Polisher™ 590TEM, 590SEM, 590TS*
[37]: Allied High Tech Products, inc. (2011), *TEM Wedge Polishing Tool*
[38]: Allied High Tech Products, inc. (2011), *MetPrep 3™ Grinder/Polisher*

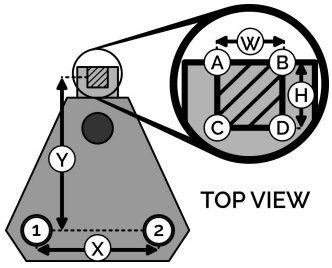


Figure 7.3: Top view of the tripod polisher

$$\text{x\_corr\_stat} = \frac{|A - B + C - D|}{2} \tag{7.1}$$

$$\text{x\_corr\_dyn} = \frac{X \cdot (A - B + C - D)}{4W} \tag{7.2}$$

$$\text{y\_corr} = \frac{|A + B - C - D|}{4} - \frac{Y \cdot (A + B - C - D)}{2H} \tag{7.3}$$

$$\Delta\text{micrometer}_1 = \text{y\_corr} + \text{x\_corr\_stat} + \text{x\_corr\_dyn} \tag{7.4}$$

$$\Delta\text{micrometer}_2 = \text{y\_corr} + \text{x\_corr\_stat} - \text{x\_corr\_dyn} \tag{7.5}$$

All lapping films and the ChemoMet polishing mat must be rinsed with plenty of water after polishing to remove any particles that may have been left behind. The lapping papers are best stored in a photographic blotter book. The ChemoMet polishing mat is best stored in a resealable plastic bag.

Step	Disposable used	Material removed
1	UltraPrep Lapping Film, Plain Backed, 6µm, 8in	≈100µm
2	UltraPrep Lapping Film, Plain Backed, 3µm, 8in	≈30µm
3	UltraPrep Lapping Film, Plain Backed, 1µm, 8in	≈10µm
4	UltraPrep Lapping Film, Plain Backed, 0.5µm, 8in	≈5µm
5	ChemoMet, PSA, 8 in 0.06µm MasterMet suspension (colloidal silica)	until mirror smooth ≈2µm

Table 7.1: Summary of polishing procedure.

Laser Fault Injection

8

About Laser Fault Injection

LFI is a method of intentionally introducing perturbations into a system by using a laser to physically manipulate the electrical properties of a system. This technique is often used to test the robustness and security of electronic devices, such as microprocessors and memory chips, by simulating the effects of naturally occurring faults or external tampering. The laser is precisely aimed at a specific location on the device, and the energy from the laser pulse can cause a temporary or permanent change in the electrical characteristics of the targeted component. This allows researchers and engineers to evaluate the response of the system to faults and identify potential vulnerabilities. This chapter explains the general LFI process. The following chapters will explain the LFI method and results applied in this study.

8.1 Laser fault injection setup

A general LFI setup consists of a laser, a microscope, a movable stage, and a device under test (DUT). The laser is used to generate a laser pulse that is focused onto the DUT. The microscope is used to focus the laser on the DUT. Usually, there is an optical splitter present in the system so that an infrared camera can be used to observe the DUT and the laser beam. The microscope stage moves the DUT and the laser beam into the correct position.

At Riscure, a laser station is used to perform LFI. The laser station consists of a microscope, a motorized microscope stage, a beam splitter, and an infrared camera; the laser station is shown in Section 5.2. Multiple laser sources can be used with the laser station.

8.2 Parameter space

The main challenge when performing LFI is that the parameter space that can be searched is very large. Mainly because multiple parameters can be varied, such as:

- Pulse power
- Pulse duration
- Pulse delay
- Laser focus
- X-position
- Y-position

The situation is further complicated because the parameters are not independent. This means that the parameter space is a complex multi-dimensional space, making it very difficult to find the optimal parameters for a specific device. Therefore a systematic approach is required.

9

Laser Fault Injection method

9.1 SETUP

The LFI setup used in this study is shown in Figure 9.1 and Figure 9.2. A PC is running Riscure's Inspector FIPy and controls several things:

- A Riscure Spider - Section 5.4 - which in turn:
  - Controls a Riscure Diode Laser (1064nm) - Section 5.3
  - Reads the trigger signal from the device under test.
  - Controls a solid state relay for cold resetting the device under test.
- The XYZ stage of the laser station, which is used to position the laser beam on the sample - Section 5.2
- An STM32G061F8Y6TR mounted on top of a breakout board referred to as the device under test (DUT) - Section 2.3
- An FTDI USB to Serial adapter to communicate with the DUT
- An STM Nucleo board of which the onboard ST-LINK/V2-1 is used to program the DUT, and the onboard 3.3V regulator is used to power the DUT.

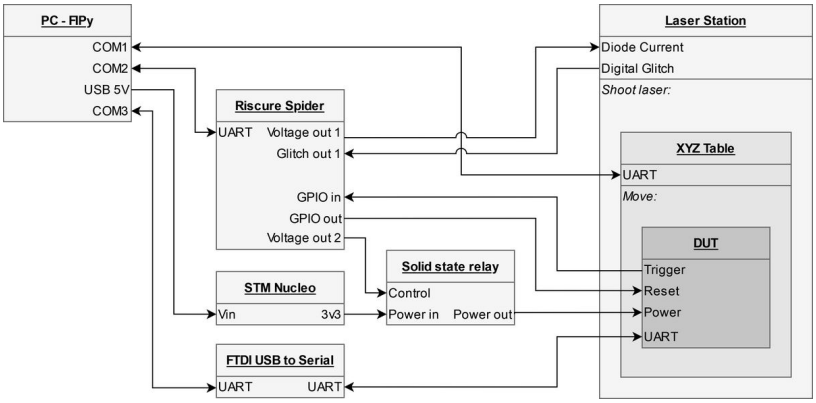


Figure 9.1: Block diagram of the LFI test setup.

9.2 FIRMWARE

The firmware running on the device under test is a proprietary firmware developed by Riscure called Fault Injection Resistance Measure or, in short, FIRM. The firmware was ported to run on an ARM cortex-M0+ microcontroller. Therefore some Assembler code needed to be modified to comply with the ARMv6-M Thumb instruction set.

FIRM implemented different tests to test the fault injection resistance of a device, but only the memory test, documented in Subsection 9.2.1, was used in this thesis.

9.2.1 *Memory test*

Eleven memory words containing a 32-bit random number are written to the memory as shown in Listing 9.1.

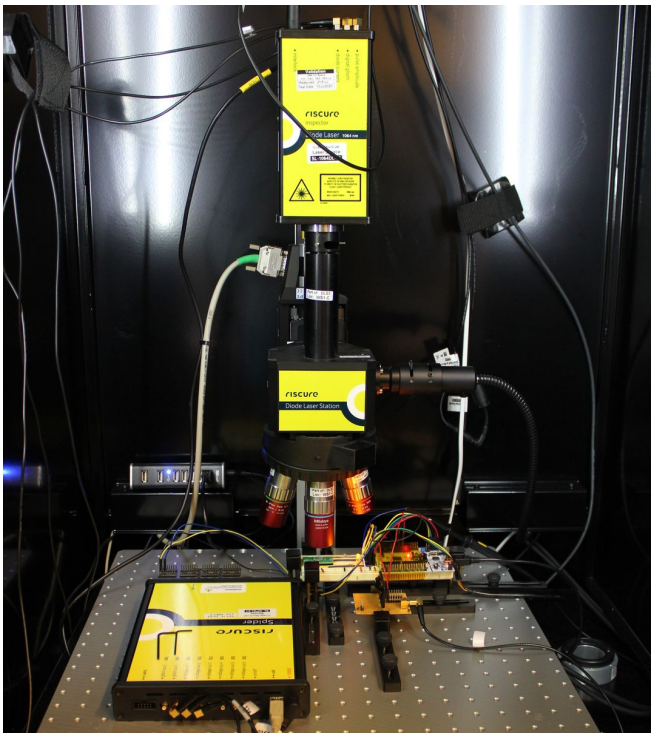


Figure 9.2: LFI setup.

```
volatile unsigned int memory_fill [MEM_SIZE] = {0x1B9E7B3D,
    0xA7F8D9E2, 0xC6B5F1A9, 0x8E2A43D6, 0x5F7B981C, 0x3D6E5A7F,
    0x9E2C1B9B, 0xF1A8A7F8, 0x43D6C6B5, 0x981C8E2A, 0x5A7F5F7B};
```

Listing 9.1: C code for memory initialization.

The starting address of the block of random numbers is stored in register `R1`. Then the 32-bit data words are moved from adjacent memory locations to the register `R0` and back. For this, the LDR (load) and STR (store) instructions are used as shown in Listing 9.2.

```
// Move the memory pointer to register R1
unsigned int *memory_pointer = memory_fill;
__asm__("mov r1, %0" : : "r" (memory_pointer));
// Write the data from memory to register R0 and back
__asm__("ldr r0, [r1]");
__asm__("str r0, [r1]");
__asm__("ldr r0, [r1, #4]");
__asm__("str r0, [r1, #4]");
__asm__("ldr r0, [r1, #8]");
__asm__("str r0, [r1, #8]");
...
__asm__("ldr r0, [r1, #36]");
__asm__("str r0, [r1, #36]");
```

Listing 9.2: Inline Assembler code for memory test.

The 11 memory words, along with their original values, are returned by the device under test over its UART interface. The values are then compared to the original ones, and if they are not identical, it is classified as a fault. There are two possible situations:

- One memory location contains the value of another memory location. In this case, the address was most likely changed by the fault. This can

be called an *address fault*.

- The value of a memory location is different from the original value. In this case, the contents were most likely changed by the fault. This can be called a *data fault*.

9.3 MEASURING PROCEDURE

In Riscure's Inspector FIPy, a generator object can return coordinates for the XYZ stage to move according to a preconfigured scan grid and random parameters within a preconfigured range. The parameter space is searched randomly to ensure the whole parameter space is covered.

First, the XYZ stage is moved to the first position of the scan grid, the laser power is set, and the device under test is turned on. Then the command to start the memory test is sent to the device under test. The device under test will pull the trigger GPIO pin high as soon as the operation start, and as soon as the rising edge on the trigger line is detected, the timer is started for `pulse_delay`. Once `pulse_delay` has elapsed, the laser is turned on for the duration of `pulse_length`, after which the laser is turned off again. The device under test returns its information over its UART interface, and we save this data to the database in Fipy. This is repeated for the configured number of attempts, then the XYZ stage is moved to the next position, and the process is repeated until the whole scan grid has been scanned. A flowchart of the FIPy script is shown in Figure 9.3.

After this, the results are analyzed, and the parameter search space is narrowed down to the most promising parameters. Then the process is repeated using the new parameter space. The experiment is executed for an unpolished sample, a polished sample, and three samples with different glass and immersion oil coatings.

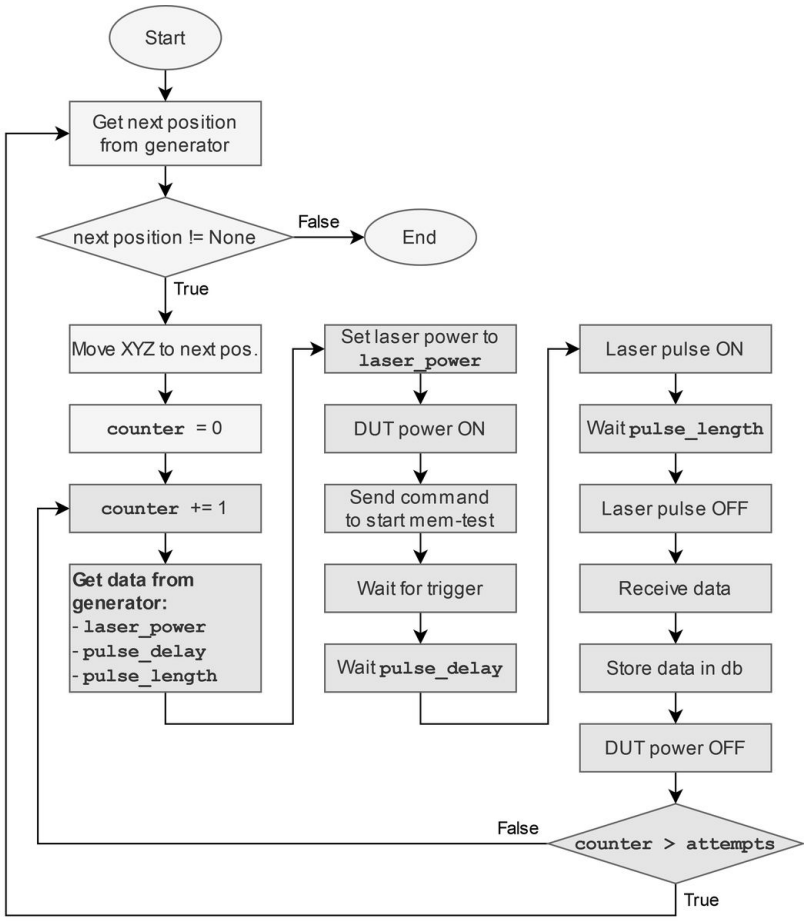


Figure 9.3: Flowchart of LFI FIPy script.

10

Laser Fault Injection Results

The results of the LFI experiments are shown in this chapter. The first section Section 10.1 describes the results while narrowing the parameter space. The second section Section 10.2 describes the results of the experiments on the polished and unpolished samples. Finally, the third section Section 10.3 describes the results of the experiments on the coated samples.

10.1 NARROWING THE PARAMETER SPACE

First, a full scan of the device is executed with a wide parameter space, of which the result is shown in Figure 10.1.

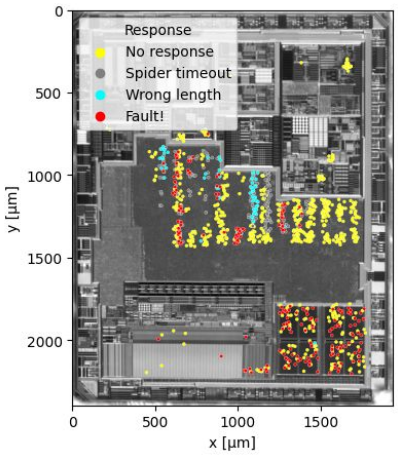
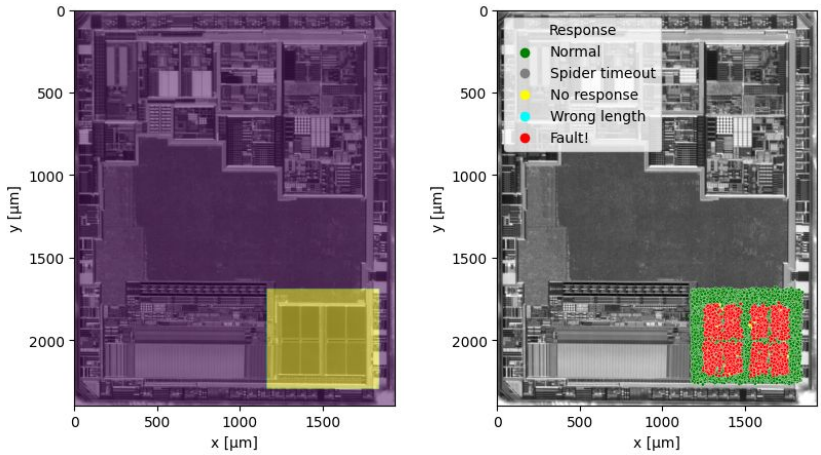


Figure 10.1: LFI First scan.

The scan is then narrowed down by masking only the SRAM (in the lower right corner), see Figure 10.2a, as this is where consistent faults seem to occur. The result of this second scan is shown in Figure 10.2b. Note the faults only occur within the SRAM cells themselves.



(a) Mask

(b) Second scan

Figure 10.2: LFI mask and second scan.

10.2 LASER FAULT INJECTION RESULTS ON POLISHED SAMPLES

In Figure 10.3, the results of the experiments on the polished and unpolished samples are shown. The X-axis shows the laser power in micro-Joules, and the Y-axis shows the number of effective faults. The results show that laser power greatly affects the number of faults. The results also show that the polished sample is about twice as susceptible to faults at low laser power than the polished sample.

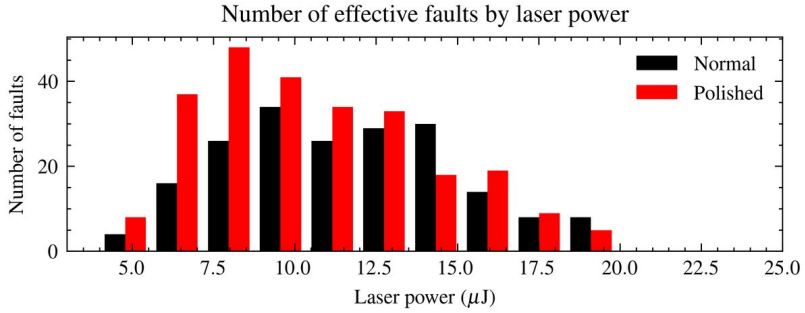


Figure 10.3: LFI results polished vs. unpolished samples.

10.3 LASER FAULT INJECTION RESULTS ON COATED SAMPLES

In Figure 10.4, the results of the experiments on the coated samples are shown. The X-axis shows the laser power in micro-Joules, and the Y-axis shows the number of effective faults. The results show no significant difference between the number of faults on a coated and an uncoated sample for a certain laser power.

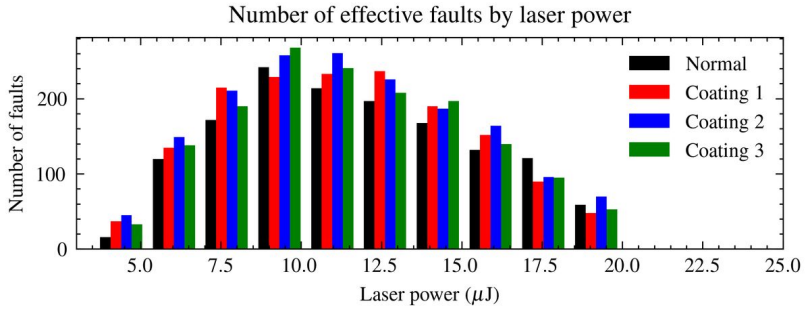


Figure 10.4: LFI results glass.

Emission Microscopy

11

About Emission Microscopy

When an IC operates, photons are emitted by the internal circuitry. EMMI, sometimes referred to as Photon Emission Microscopy (PEM)[1], is an often-used technique or microelectronic failure analysis [39, 40] but has limitations when used for failure analysis. For example, it can usually only be used to indicate the place of the failure, not the type of failure that has occurred [40].

Definition 11.0.1 *"Side-channel analysis (SCA) is an alternative attack that exploits information leaking from physical implementations of e.g. cryptographic devices to discover cryptographic keys or other secrets." [41]*

When used for security analysis, EMMI can be seen as a side-channel attack (see definition 11.0.1). For example, when using EMMI, the unknown location of a register or a hardware crypto engine can be derived based on optical leakage.

EMMI can be subdivided into two categories, static EMMI and dynamic EMMI. With static EMMI, the device is studied while it is halted in a known static state. For side-channel analysis, dynamic EMMI is used. Dynamic EMMI is used to study the device while it operates and the transistors are switching. [42]

1: In this thesis, the broader term EMMI will be used to refer to PEM, as this is the term Riscure has chosen to use.

[39]: Phang et al. (2005), *A Review of near Infrared Photon Emission Microscopy and Spectroscopy*

[40]: De Wolf et al. (2001), *Spectroscopic Photon Emission Microscopy: A Unique Tool for Failure Analysis of Microelectronics Devices*

[41]: Hospodar et al. (2011), *Machine Learning in Side-Channel Analysis: A First Study*

[42]: Bruce et al. (2003), *ABCs of Photon Emission Microscopy*

11.1 Rules of thumb

According to ABCs of Photon Emission Microscopy from ASM International [42], there are a few rules of thumb to remember when using EMMI:

1. Photon emission cannot occur without current, so if there is photon emission, there is always current.
2. The intensity of the emission is related to the amount of current.
3. Transistors emit photons when switching because there flows current as they charge or discharge capacitive loads, which include various capacitances such as the junction and gate capacitance and the capacitance of any connected gates or interconnects.

11.2 Performing emission microscopy

When performing EMMI, we use the rules of thumb mentioned in Section 11.1. When localizing, for example, a crypto engine through the silicon side of a device, we create two situations, one in which our device operates normally, and the crypto engine is not used, and a second in which the crypto engine is heavily used. If the crypto engine is heavily used, it will emit more photons than when it is not used, as more transistor switching and more current flows in the crypto engine.

First, we take a long exposure acquisition of the situation where the crypto engine is not used and add it to image set 1. Then we take a long exposure acquisition of the situation where the crypto engine is heavily used and add it to image set 2.

Because there will be very little emission and the long exposure acquisition also captures a lot of sensor noise, we need a bigger dataset to filter out the noise. Therefore this process is repeated a couple of hundred times until we have two image sets of adequate sizes.

11.3 ELIMINATING THE NOISE

The example data shown in Figure 11.1 is used. The data consists of two sets of 10000 gaussian noise images of 10 by 10 pixels. To the first set, an offset is added to represent, for example, the emission of a register.

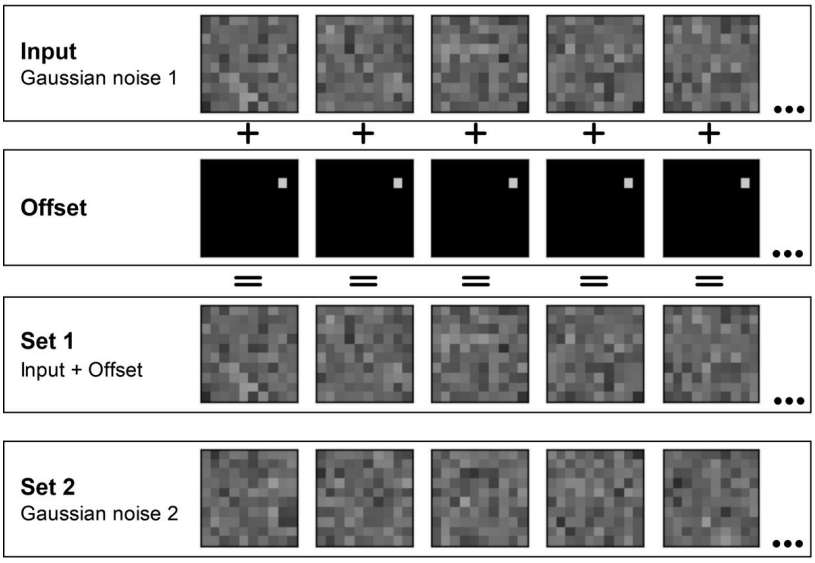


Figure 11.1: Example data for filtering with T-test.

The offset is no longer visible when looking at a single image in set 1; therefore, the noise must be eliminated first. For that, a Welch's unequal variances t-test [43] can be used on the image sets. The formula for the t-statistic is given by equation (11.1), where $\bar{X}_1$, s_1 and N_1, respectively, the sample mean, corrected sample deviation, and sample size of set 1. $\bar{X}_2$, s_2, and N_2 are the respective sample mean, corrected sample deviation, and sample size of set 2. Then, the degrees of freedom can be approximated using the Welch-Satterthwaite equation [44] given by equation (11.2). After that, the p-value can be determined using the previously determined t-value and degrees of freedom from a lookup table [45].

[43]: Welch (1947), *The Generalization of 'Student's' Problem When Several Different Population Variances Are Involved*

[44]: Loveland (2011), *Mathematical Justification of Introductory Hypothesis Tests and Development of Reference Materials*

[45]: Piegorsch (2002), *Tables of P-values for t-and Chi-Square Reference Distributions*

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{\sqrt{N_1}} + \frac{s_2^2}{\sqrt{N_2}}}} \tag{11.1}$$

$$\nu \approx \frac{\left(\frac{s_1^2}{N_1} + \frac{s_2^2}{N_2}\right)^2}{\frac{s_1^4}{N_1^2(N_1-1)} + \frac{s_2^4}{N_2^2(N_2-1)}} \tag{11.2}$$

A two-tailed test will be used, If the p-value is smaller than the chosen significance level, the null hypothesis is rejected, and the alternative hypothesis is accepted.

- The null hypothesis H_0 is that the means of the two sets are equal ($\bar{X}_1 = \bar{X}_2$).

- The alternative hypothesis H_a is that the means of the two sets are different ($\bar{X}_1 \neq \bar{X}_2$).

Fortunately, the t-value, degrees of freedom, and p-value rarely have to be calculated by hand. Python, Julia, R, Matlab, and various other mathematically oriented programming languages have functions to calculate the t-statistic and the p-value for a given array. In Listing 11.1 example code is given to calculate the t-statistic and the p-value in Python.

```python
import numpy as np
from scipy import stats

print(imageset1.shape)   # (10000, 10, 10)
print(imageset2.shape)   # (10000, 10, 10)

# Calculate the t-statistic and p-value
t_statistic, p_values = stats.ttest_ind(imageset1, imageset2,
    equal_var=False)

print(t_statistic.shape) # (10, 10)
print(p_values.shape)    # (10, 10)
```

Listing 11.1: Python example code to calculate the t-statistic and p-value.

The resulting `t_statistic` array still contains a lot of noise. But the location of the offset already becomes visible as the pixels with the most extreme values (Figure 11.2.a). The `p_values` can filter the noise and keep the statistically significant data as the p-value represents the probability of obtaining a test result by random chance at least as extreme as the actual observed result.

At first thought, a simple threshold of 0.001 may seem sufficient, but this is not the case as the family-wise error rate (FWER)—the probability of making one or more false discoveries—increases with the number of tests performed. The family-wise error rate for significance level α and m independent tests is given by FWER $= m \cdot \alpha$. Therefore if we have a significance level of 0.001 and 100 tests (10x10 pixels), the family-wise error rate is 1%. This means that there is a 1% chance a false discovery is made, see Figure 11.2.b. To remedy this, a Bonferroni correction is applied to the threshold value. The Bonferroni correction rejects the null hypothesis if the p-value is smaller than α/m. Therefore the threshold becomes $0.001/(10 \cdot 10)$. The data with Bonferroni correction is shown in Figure 11.2.c; only the offset pixel remains.

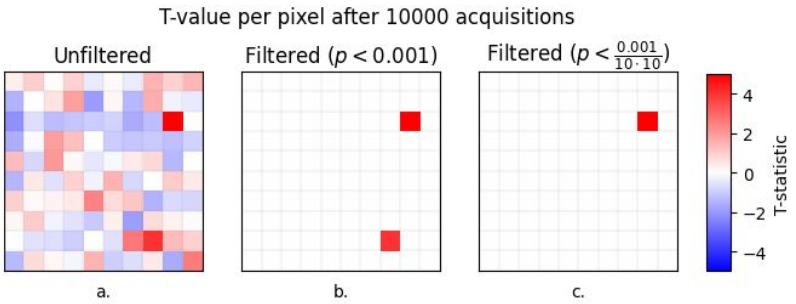


Figure 11.2: (a) T-values unfiltered, (b) T-values filtered, (c) T-values filtered with Bonferroni correction.

12

Emission Microscopy Method

12.1 SETUP

The EMMI test setup is shown in Figure 12.1. A PC is running Riscure's Inspector FIPy and controls several things:

- An STM32G061F8Y6TR mounted on top of a breakout board referred to as the device under test (DUT) - Section 2.3
- The InGaAs camera - Section 5.5
- A Riscure Laser Station where on the XYZ stage the sample is mounted - Section 5.2
- A Riscure Spider to programmatically toggle a GPIO and control the infrared (IR) ringlight. - Section 5.4
- A Source Measure Unit (SMU) to power the device, and cut the power to perform a hard reset - Section 5.6

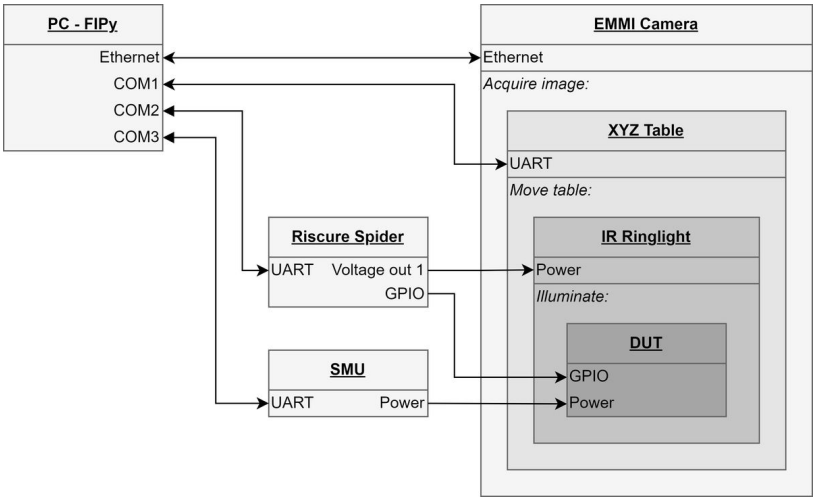


Figure 12.1: Block diagram of the EMMI test setup.

12.2 FIRMWARE

On the device under test, the firmware is running. The firmware is created using the STM32CubeIDE [46] and consists of two functions `ASM_Function_toggle1` and `ASM_Function_toggle2`. These functions target register `R3` and `R0` respectively and are implemented in Assembler, shown in Listing 12.1. These functions flip all the bits in a specific register 10000 times. This is done through an unrolled loop containing a *move not* instruction to itself, resulting in a binary inversion.

[46]: (n.d.), *STM32CubeIDE - Integrated Development Environment for STM32 - STMicroelectronics*

An `Assembler.h` file is created containing the function prototypes for the Assembler functions. Using the `#include` directive, the `assembler.h` file is included in the `main.c` file, shown in Listing 12.2. The C code uses the Hardware Abstraction Layer (HAL) provided STM32Cube [47]. The C code is responsible for reading the GPIO pin `MYIN_Pin`, and based on the value, it will call either `ASM_Function_toggle1` or `ASM_Function_toggle2`. The C code also contains the initialization code for the GPIO pins and the System Clock.

[47]: STMicroelectronics (2020), *UM2319 Description of STM32Go HAL and Low-Layer Drivers*

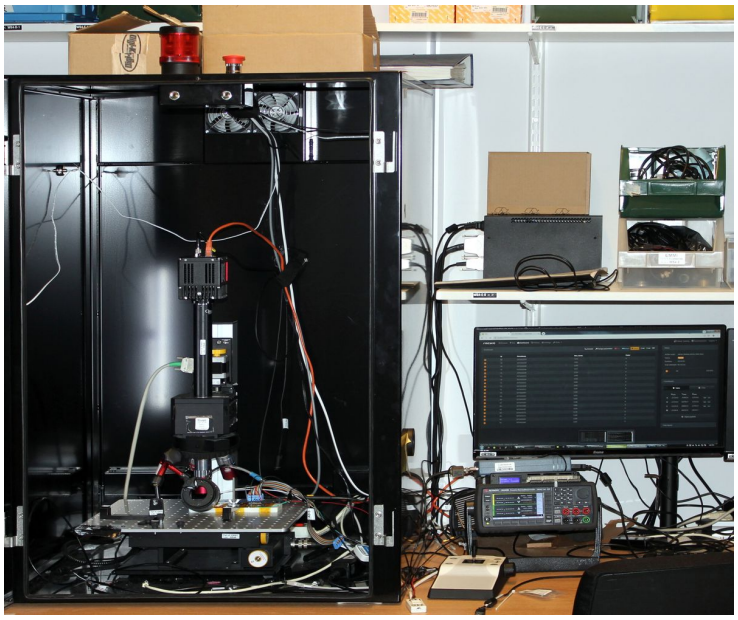


Figure 12.2: Emission Microscopy setup.

Listing 12.1: Assembler code for EMMI.

```
//Assembler.s
.syntax unified

.text
.global ASM_Function_toggle1
.global ASM_Function_toggle2
.thumb_func

#define A1 mvns R3, R3;
#define A10 A1 A1 A1 A1 A1 A1 A1 A1 A1 A1;
#define A100 A10 A10 A10 A10 A10 A10 A10 A10 A10 A10;
#define A1000 A100 A100 A100 A100 A100 A100 A100 A100 A100 A100;
#define A10000 A1000 A1000 A1000 A1000 A1000 A1000 A1000 A1000
    A1000 A1000;

#define B1 mvns R0, R0;
#define B10 B1 B1 B1 B1 B1 B1 B1 B1 B1 B1;
#define B100 B10 B10 B10 B10 B10 B10 B10 B10 B10 B10;
#define B1000 B100 B100 B100 B100 B100 B100 B100 B100 B100 B100;
#define B10000 B1000 B1000 B1000 B1000 B1000 B1000 B1000 B1000
    B1000 B1000;

ASM_Function_toggle1:
A10000
bx lr

ASM_Function_toggle2:
B10000
bx lr
```

12.3 MEASURING PROCEDURE

In Riscure's Inspector FIPy, a generator object is available that can return coordinates for the XYZ stage to move to according to a preconfigured scan grid. The scan grid is configured to cover the whole die in a 9 by 9 grid. This way, there is approximately 30% overlap between the images.

```c
// main.c
#include "main.h"
#include "assembler.h"

void SystemClock_Config(void);
static void MX_GPIO_Init(void);

int main(void) {
    HAL_Init();
    MX_GPIO_Init();
    if (HAL_GPIO_ReadPin(MYIN_GPIO_Port, MYIN_Pin)) {
        HAL_GPIO_WritePin(MYOUT_GPIO_Port, MYOUT_Pin, 1);
        while (1) { ASM_Function_toggle1(); }
    } else {
        HAL_GPIO_WritePin(MYOUT_GPIO_Port, MYOUT_Pin, 0);
        while (1) { ASM_Function_toggle2(); }
    }
}
```

Listing 12.2: C code for EMMI.

The XYZ stage is moved to the position returned by the generator. Then a reference picture is taken with the ring light on. This picture can be used for stitching later. Then the ring light is turned off, and the EMMI images are taken. First, the GPIO is set low, the sample is powered, and a long exposure image is taken and added to *image set 1*. Then the power of the sample is cut again. After that, the GPIO is set high, the sample is powered again, and a long exposure image is taken and added to *image set 2*. This is repeated for the number of configured attempts. Finally, the reference images and image sets are saved to a folder with the name of the current position. This is done for every position returned by the generator. This process is shown in the flowchart in Figure 12.3.

Next, for every folder (representing a scan grid location), a Welch two-samples t-test is executed for every pixel. The pixel values in *image set 1* are used for the first group, and for the second group, the pixel values in *image set 2* are used. The t-values are saved as a new image.

The reference images are used to stitch a complete image using MIST [48]. Then the position file produced when stitching the reference images is used to stitch the images of the t-values.

[48]: Chalfoun et al. (2017), *MIST: Accurate and Scalable Microscopy Image Stitching Tool with Stage Modeling and Error Minimization*

The minima and maxima of the resulting image are studied to find the most probable location of the registers. Then the XYZ stage is positioned at this location, and a reference image is taken with the ring light on. Next, the ring light is turned off, and the EMMI images are taken. First, the GPIO is set low, the sample is powered, and a long exposure image is taken and added to *image set 1*. Then the power of the sample is cut again. After that, the GPIO is set high, the sample is powered again, and a long exposure image is taken and added to *image set 2*. This is repeated for the number of configured attempts.

For every pixel, a Welch two-samples t-test is executed. The pixel values in *image set 1* are used for the first group, and for the second group, the pixel values in *image set 2* are used. The t-values are saved as a new image. The resulting t-value image is filtered using the p-values with a Bonferroni correction. Therefore only the pixel values with a p-value $< 0.001/(320 \cdot 256)$ are preserved.

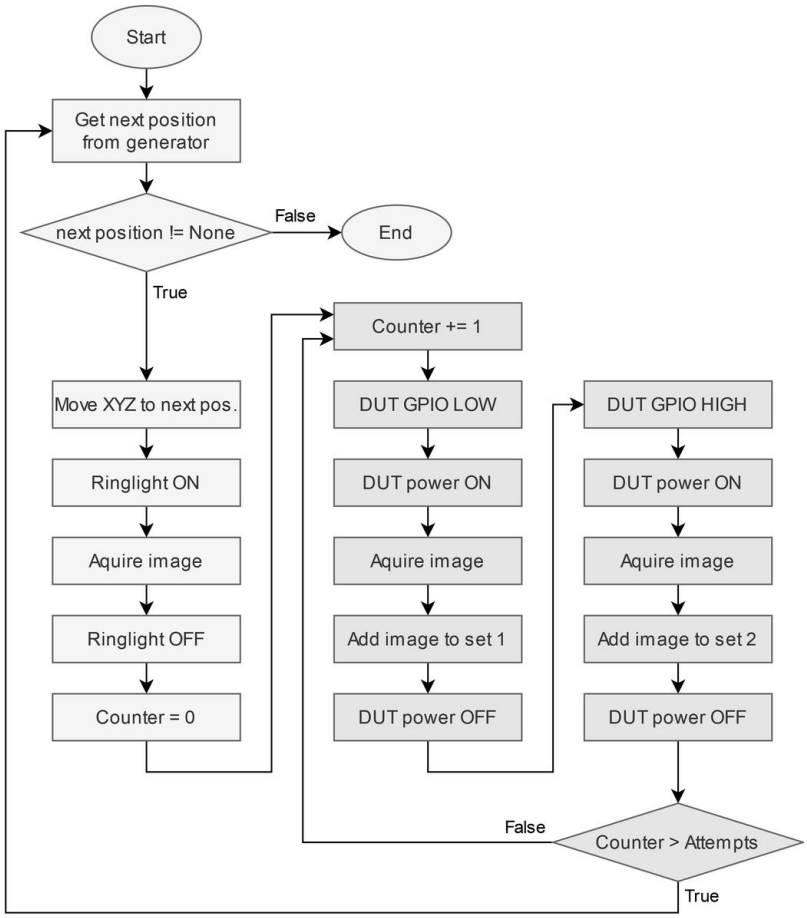


Figure 12.3: Flowchart of the FIPY script.

The experiment is executed for an unpolished sample, a polished sample, and three samples with different glass and immersion oil coatings.

13

Emission Microscopy Results

The results of the EMMI experiments are presented in this chapter. The first section presents the results of the EMMI experiments on the polished sample. The second section presents the results of the EMMI experiments on the coated sample.

13.1 NARROWING THE PARAMETER SPACE

A full scan of the device is executed to find the location of the registers in the glue logic. The found location is shown in Figure 13.1.

Figure 13.1: Location of the registers in the glue logic.

13.2 EMISSION MICROSCOPY RESULTS ON POLISHED SAMPLE

In Figure 13.2, the T-statistic for the polished sample and the unpolished are shown for the pixel at the location of register `R0` and register `R3`. Only the values that have a corresponding p-value lower than our threshold of ($p < 0.001/(320 \cdot 256)$) are shown. The X-axis shows the number of acquisitions over which the T-statistic is calculated. The Y-axis shows the T-statistic value.

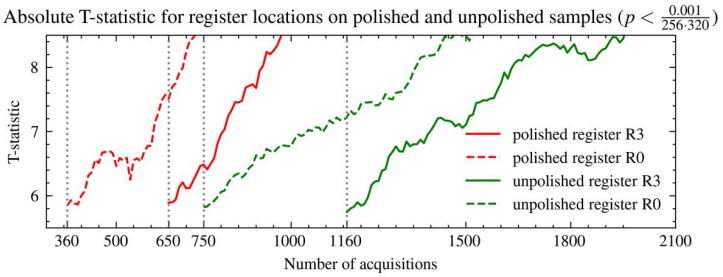


Figure 13.2: EMMI T-statistic for both polished and unpolished samples.

As becomes clear in Figure 13.2, only after 650 acquisitions was a statistically valid position for the registers on the polished sample found. For the unpolished sample, 1160 acquisitions are needed before the position of the register becomes known.

In Figure 13.3.a and Figure 13.3.b, the location of the registers are shown for respectively the polished and unpolished sample. Also, note that the light on the unpolished sample is more scattered than on the polished sample, which can be seen because two "blue" pixels are visible in the image. This is because the unpolished sample is not as smooth as the polished sample.

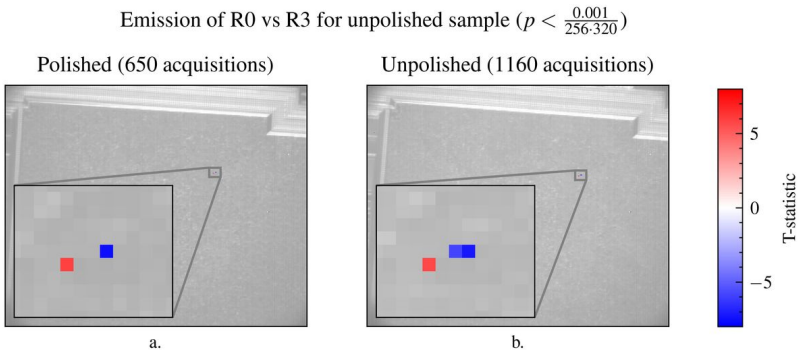


Figure 13.3: (a) Register location for polished sample after 650 acquisitions, (b) Register location for unpolished sample after 1160 acquisitions.

13.3 EMISSION MICROSCOPY RESULTS ON COATED SAMPLES

In Figure 13.4, the T-statistic for the unpolished sample and the coated samples is shown for the pixel at the location of register `R0` and register `R3`. The X-axis shows the number of acquisitions over which the T-statistic is calculated. The Y-axis shows the T-statistic value. It becomes clear that the T-threshold values of the coated samples are equal to or lower than the threshold values of the unpolished sample. This indicates a smaller difference of means; thus, the register location is less visible.

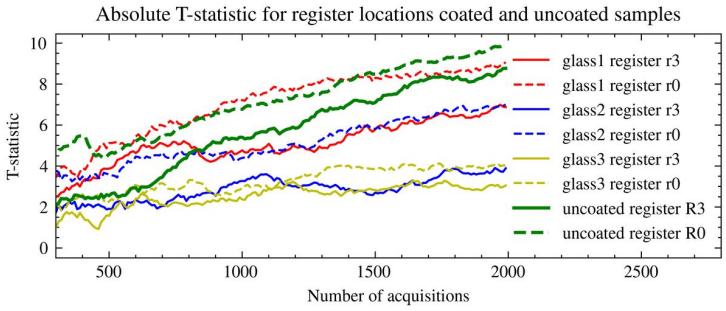


Figure 13.4: EMMI T-statistic for both coated and uncoated samples.

In Figure 13.5, only the values that have a corresponding p-value lower than our threshold of ($p < 0.001/(320 \cdot 256)$) are shown. Therefore only the statistically valid register positions are shown. As can be seen, only for the uncoated sample and the sample with coating *glass1* both register positions are found within 2000 acquisitions. For the sample with coating *glass2*, only register position `R0` is found within 2000 acquisitions. For the register `R3` of the sample with coating *glass2* as well as register `R0` and register `R3` of the sample with coating *glass3*, no statistically significant register position is found within 2000 acquisitions.

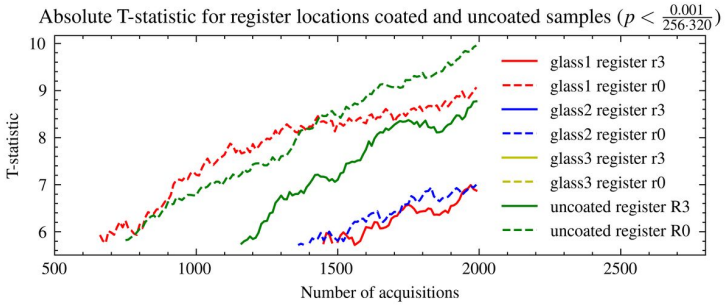


Figure 13.5: EMMI T-statistic for both coated and uncoated samples filtered with P-threshold value.

Epilogue

14

Conclusion

This thesis aims to determine if an index-matching coating and/or thinning of the silicon can increase the effectiveness of LFI or EMMI by respectively increasing the number of effective faults at certain laser power and reducing the number of acquisitions needed to find a statistically valid result.

14.1 POLISHED SAMPLES

The results of the experiments show that thinning the silicon positively impacts both LFI and EMMI. In the case of LFI, thinning the silicon increases the number of effective faults for a certain laser power. In the case of EMMI, thinning the silicon reduces the number of acquisitions needed to find a statistically valid result.

14.2 ANTI-REFLECTIVE COATED SAMPLES

The LFI and EMMI experiments showed no significant difference between the samples with and without an index-matching coating using glass and immersion oil. Therefore, it can be concluded that an index-matching coating using glass and immersion oil does not improve the effectiveness of LFI or EMMI.

15

Discussion

As hypothesized, there is an improvement in the effectiveness of LFI when the sample is polished. The most likely cause is that the faction of light absorbed by the silicon is proportional to the thickness of the material, as shown in Section 4.2. Therefore less light is absorbed by the silicon when the sample is polished, resulting in a higher transmission coefficient. This is also supported by the results of the EMMI, where there is a larger T-value for the polished samples than for the unpolished samples, indicating a greater difference in means. This confirms the assumptions made in [5]. These findings can be incorporated into the used security testing methodology and processes of Riscure.

[5]: He et al. (2016), *Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection*

The results of the coated samples are different from what was hypothesized, as there is no significant difference between the number of faults on a coated and an uncoated sample for a certain laser power. This is also supported by the results of the EMMI, where there is no significant difference between the T-values of the coated and uncoated samples. Therefore the results significantly differ from the results of [6, 7]. This is most likely caused by using a thick-film coating where [6, 7] make use of a thin-film coating. The difference in the type of coating might explain the difference in results.

[6]: Davis et al. (2000), *Antireflection Coatings for Semiconductor Failure Analysis*
[7]: Wang et al. (2001), *Effect of Ga Staining Due to FIB Editing on IR Imaging of Flip Chips*

15.1 LIMITATIONS

The reader should bear in mind that because thin-film coatings are very expensive and require a clean room, they are typically only used for large-scale production (see Section 6.2). Therefore, another type of anti-reflective coating was chosen during this study, and only this coating was researched. The chosen coating is a thick-film index matching coating. Therefore the results of this study are not generalizable to all types of anti-reflective coatings.

15.2 FUTURE RESEARCH

As this study did not research thin-film coatings, future research could explore other anti-reflective coatings, specifically thin-film coatings. While the coating used in this study is a thick film coating, and there was no significant improvement in the effectiveness of LFI or EMMI, a thin-film coating might improve the effectiveness.

Also, it might be interesting to explore other multiple testing corrections than the Bonferroni correction for filtering the EMMI results. This might yield better results as the Bonferroni correction might be conservative if the test statistics are positively correlated or there are a large number of tests [49].

[49]: Moran (2003), *Arguments for Rejecting the Sequential Bonferroni in Ecological Studies*

Lastly, a study can be conducted to see if the theoretical thickness vs. transmission coefficient curve can be observed in practice by progressively thinning the silicon and repeating the experiments conducted in this thesis for each thickness.

Appendix

A

Demonstration of Competencies

In this appendix, I will show how I have demonstrated the competencies of the National Competency Profile Electrical Engineering during my internship at Riscure [50].

[50]: Landelijk Competentieprofiel et al. (2014), *Landelijk Competentieprofiel Elektrotechniek Opleidingscode 34267*

A.1 TO ANALYZE

First and foremost, a project plan had to be written. During a verbal briefing with general details of the problem and the desired outcome, I recorded the desired requirements for the project. At first, it was unclear what the right strategy would be to tackle the problem, so I asked the right questions to find out the motivation behind the research question and came up with a possible solution strategy through literature research. Then, I independently selected relevant aspects related to the research question. Lastly, I formulated a clear problem statement, objective, and assignment based on the client's wishes. The first draft of the project plan was accepted, indicating the project plan was a good representation of the customer's wishes.

Also, I drafted a polishing procedure for in-house sample preparation at Riscure. For that, I independently had to model a procedure based on multiple existing procedures. Riscure will use this process to prepare samples in the future.

A.2 TO RESEARCH

For the project plan, I formulated the objectives of a desired research based on the research question, which I further specified during the initial research phase after the project plan was approved. I independently selected scientific literature and collected other sources of information while correctly assessing their reliability. I managed all my sources using the open-source reference management software Zotero to keep all my sources organized and findable in the future.

For this thesis, I also independently selected various sources of information, assessed their relevance and reliability, and used this research to summarize, structure, and interpret the results and draw conclusions related to the research question. Furthermore, I reported the results according to the common IEEE standard. Finally, in my conclusion, I made recommendations for follow-up research based on the results obtained.

A.3 TO DESIGN

During the initial research, I developed a strategy to research the topic while considering the manufacturability and testability of the sample preparation methods. First, I researched the different coating methods and concluded that using a thin-film anti-reflective coating is not feasible for this study. The main reason for this was the cost and complexity. Therefore I came up with a thick-film index-matching coating. In the end, I documented my research in the form of this thesis and a presentation.

A test setup had to be designed for both the LFI and the EMMI experiments. For this, I considered the manufacturability and testability of the setup, as well as the reliability. As the setup needs to run for a long time, it is of the essence that there is no wear on the test equipment and no errors occur that will block the test from continuing during the night or the weekends.

A.4 TO REALIZE

I had to use the correct materials, processes, and methods for the sample preparation. For this, first, a lot of research has to be conducted. During the realization process, the processes regarding the thick-film index-matching glass and immersion oil coating and the sample thinning were both documented in this thesis, and the sample thinning is additionally documented in the drafted polishing procedure. Also, the very small samples had to be polished and coated using the before-drafted procedures. For this, appropriate use of materials, processes, and methods was of the essence.

The polished and unpolished samples were soldered on a micro-BGA breakout board. For this, appropriate use had to be made of materials, soldering procedures, and EMC guidelines to minimize the risk of samples being destroyed.

I assembled components into an integral product to create the test setups for the experiments. First, I had to assess what was the right tool for the job, then I compared alternative tools to be aware of any downsides to my choice, and lastly, I checked the availability of the chosen tools/components. Finally, after building the setup, I validated the functioning and verified if all the requirements were met. Then I documented the realization process in this thesis.

A.5 TO MANAGE

During the internship, I communicated and collaborated with others in a multicultural, international, and multidisciplinary environment. At Riscure, the main language is English, and we have people from many nationalities and cultural backgrounds. This diversity is one of the reasons I like working at Riscure so much. In addition, I had to communicate task and process-oriented, and the research project had to be monitored in terms of time, money, and quality.

I drafted a project plan to manage the timeline and the project scope. Also, I set up a sub-project for the polishing procedure developed and drafted during this internship. The polishing procedure can be seen as the resulting project documentation. I had to quantify the time invested in trying different polishing methods and money for ordering polishing supplies and disposables. Lastly, I delegated work to my company mentor or the lab support team for booking equipment or ordering supplies.

Bibliography

Here are the references in citation order.

[1] Jean-Max Dutertre et al. "Fault Round Modification Analysis of the Advanced Encryption Standard." In: *2012 IEEE International Symposium on Hardware-Oriented Security and Trust*. June 2012, pp. 140–145. DOI: 10.1109/HST.2012.6224334 (cited on page 3).

[2] Aurélien Vasselle et al. "Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot." In: *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Sept. 2017, pp. 41–48. DOI: 10.1109/FDTC.2017.18 (cited on page 3).

[3] Susanna Orlic et al. "Simple Photonic Emission Analysis of AES - Photonic Side Channel for the Rest of Us." In: Jan. 2012. DOI: 10.1007/978-3-642-33027-8_3 (cited on page 3).

[4] Riscure. *Diode Laser 1064nm NIR (30W, 50MHz, Multimode)*. URL: https://getquote.riscure.com/en/quote/2101051/diode-laser-1064nm-nir-30w-50mhz-multimode.htm (visited on 01/04/2023) (cited on page 3).

[5] Wei He et al. "Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection." In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Aug. 2016, pp. 102–113. DOI: 10.1109/FDTC.2016.13 (cited on pages 4, 53).

[6] Brennan Davis and Wilson Chi. "Antireflection Coatings for Semiconductor Failure Analysis." In: *ISTFA 2000*. ASM International, Oct. 2000, pp. 155–160. DOI: 10.31399/asm.cp.istfa2000p0155 (cited on pages 4, 53).

[7] Q. S. Wang et al. "Effect of Ga Staining Due to FIB Editing on IR Imaging of Flip Chips." In: *ISTFA 2001*. ASM International, Oct. 2001, pp. 275–280. DOI: 10.31399/asm.cp.istfa2001p0275 (cited on pages 4, 53).

[8] Mark LaPedus. *Fan-Out Packaging Gains Steam*. Nov. 2015. URL: https://semiengineering.com/fan-out-packaging-gains-steam/ (visited on 01/03/2023) (cited on page 5).

[9] NXP Semiconductors. "AN10439 Wafer Level Chip Scale Package." In: 2016 (2016), p. 16 (cited on pages 5, 6).

[10] Bob Arnoud Pieter Swinkels. *PHYSICAL ATTACK ON A WLCSP*. Student Project Plan v1.0. Delft, Nov. 2021, pp. 2–3 (cited on page 5).

[11] ST Microelectronics. *STM32G061F8Y6TR*. URL: https://estore.st.com/en/stm32g061f8y6tr-cpn.html (visited on 09/06/2022) (cited on page 5).

[12] Proto Advantage et al. *BGA-25 to DIP-25 SMT Adapter (0.4 Mm Pitch, 5 x 5 Grid)*. URL: http://www.proto-advantage.com/store/product_info.php?products_id=4000016 (visited on 01/15/2023) (cited on page 6).

[13] Hagai Bar-El et al. *The Sorcerer's Apprentice Guide to Fault Attacks*. URL: https://eprint.iacr.org/2004/100.pdf (visited on 01/04/2023) (cited on pages 7–9).

[14] Alessandro Barenghi et al. "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures." In: *Proceedings of the IEEE* 100.11 (Nov. 2012), pp. 3056–3076. DOI: 10.1109/JPROC.2012.2188769 (cited on pages 7, 8).

[15] Maurice Aarts. "Electromagnetic Fault Injection Using Transient Pulse Injections." PhD thesis. Dec. 2013 (cited on page 7).

[16] George Thessalonikefs. "ElectroMagnetic Fault Injection Characterization." In: 2014. (Visited on 01/04/2023) (cited on page 7).

[17] Michel Agoyan et al. "Single-Bit DFA Using Multiple-Byte Laser Fault Injection." In: *2010 IEEE International Conference on Technologies for Homeland Security (HST)*. Nov. 2010, pp. 113–119. DOI: 10.1109/THS.2010.5655079 (cited on page 8).

[18] J.A. Clark and D.K. Pradhan. "Fault Injection: A Method for Validating Computer-System Dependability." In: *Computer* 28.6 (June 1995), pp. 47–56. DOI: 10.1109/2.386985 (cited on page 8).

[19] Carsten Schinke et al. "Uncertainty Analysis for the Coefficient of Band-to-Band Absorption of Crystalline Silicon." In: *AIP Advances* 5.6 (June 2015), p. 067168. DOI: 10.1063/1.4923379 (cited on page 12).

[20] Riscure. *Laser Station 2*. Nov. 2018. URL: https://getquote.riscure.com/en/quote/2101106/laser-station-2.htm (visited on 01/14/2023) (cited on page 15).

[21] Riscure. *Diode Laser 1064nm NIR (30W, 50MHz, Multimode)*. Jan. 2022. URL: https://getquote.riscure.com/en/quote/2101051/diode-laser-1064nm-nir-30w-50mhz-multimode.htm (visited on 01/14/2023) (cited on page 16).

[22] Riscure. *Spider*. Nov. 2022. URL: https://getquote.riscure.com/en/quote/2492015/spider.htm (visited on 01/14/2023) (cited on page 16).

[23] Riscure. *AV GoldEye G-008 InGaAS Camera (EMMI)*. June 2022. URL: https://getquote.riscure.com/en/quote/2346776/av-goldeye-g-008-ingaas-camera-emmi.htm (visited on 01/14/2023) (cited on pages 16, 17).

[24] Keysight. *B2902B Precision Source / Measure Unit (2 Ch, 100 fA)*. Nov. 2022. URL: https://www.keysight.com/us/en/product/B2902B/precision-smu-2ch-100fa-resolution-210v-3a-dc-10-5a-pulse.html (visited on 01/14/2023) (cited on page 17).

[25] Edmund Optics. *Anti-Reflection (AR) Coatings*. URL: https://www.edmundoptics.eu/knowledge-center/application-notes/lasers/anti-reflection-coatings/ (visited on 01/14/2023) (cited on page 22).

[26] Stefaan Vandendriessche. *No One-Size-Fits-All Approach to Selecting Optical Coatings*. Dec. 2016. URL: https://www.photonics.com/Articles/No_One-Size-Fits-All_Approach_to_Selecting/a61285 (visited on 01/14/2023) (cited on page 22).

[27] Ian M. Thomas. "Optical Coating Fabrication." In: *Sol-Gel Optics: Processing and Applications*. Ed. by Lisa C. Klein. The Springer International Series in Engineering and Computer Science. Boston, MA: Springer US, 1994, pp. 141–158. DOI: 10.1007/978-1-4615-2750-3_6 (cited on page 22).

[28] Norland Products. *NOA170*. Jan. 2022. URL: https://www.norlandprod.com/adhesives/NOA170.html (visited on 01/14/2023) (cited on page 23).

[29] ja:user:GcG. *Immersion_microscopy by Olympus Plan PLL X100 Lens*. Feb. 2009. URL: https://commons.wikimedia.org/wiki/File:Immersion_microscopy.jpg (visited on 01/15/2023) (cited on page 23).

[30] Boomlab. *Immersie-Olie Voor Microscopie*. URL: https://www.boomlab.nl/product/55004699-0100+sigma-aldrich-immersie-olie-voor-mikroskopie-55004699-0100 (visited on 01/15/2023) (cited on page 23).

[31] OptoSigma! *Optical Parallel / OPB-10C01-10-5*. Mar. 2021. URL: https://jp.optosigma.com/en_jp/opb-10c01-10-5.html (visited on 01/15/2023) (cited on page 24).

[32] DirectIndustry. *MetPrep 3™ - Sample Preparation Grinding Polishing Machine by Allied High Tech Products*. URL: https://www.directindustry.com/prod/allied-high-tech-products/product-34997-1510091.html (visited on 01/15/2023) (cited on page 25).

[33] Ted Pella, Inc. *Crystalbond™ Adhesives*. Technical Note (cited on page 25).

[34] Buehler. *Buehler Sum-Met: The Science behind Materials Preparation*. Lake Bluff, Il: Buehler, 2004 (cited on page 26).

[35] John Benedict, Ron Anderson, and Stanley J. Klepeis. "Recent Developments in the Use of the Tripod Polisher for TEM Specimen Preparation." In: *MRS Online Proceedings Library (OPL)* 254 (1991/ed), p. 121. DOI: 10.1557/PROC-254-121 (cited on page 26).

[36] Ted Pella, Inc. *PELCO® Tripod Polisher™ 590TEM, 590SEM, 590TS*. Operation Manual. May 2018 (cited on page 26).

[37] Allied High Tech Products, inc. *TEM Wedge Polishing Tool*. Operation Manual Version 2.4. Jan. 2011 (cited on page 26).

[38] Allied High Tech Products, inc. *MetPrep 3™ Grinder/Polisher*. Operation Manual Version 1.2. Feb. 2011 (cited on page 26).

[39] J.C.H. Phang et al. "A Review of near Infrared Photon Emission Microscopy and Spectroscopy." In: *Proceedings of the 12th International Symposium on the Physical and Failure Analysis of Integrated Circuits, 2005. IPFA 2005.* June 2005, pp. 275–281. DOI: 10.1109/IPFA.2005.1469178 (cited on page 39).

[40] Ingrid De Wolf and Mahmoud Rasras. "Spectroscopic Photon Emission Microscopy: A Unique Tool for Failure Analysis of Microelectronics Devices." In: *Microelectronics Reliability* 41.8 (Aug. 2001), pp. 1161–1169. DOI: 10.1016/S0026-2714(01)00104-4 (cited on page 39).

[41] Gabriel Hospodar et al. "Machine Learning in Side-Channel Analysis: A First Study." In: *Journal of Cryptographic Engineering* 1.4 (Oct. 2011), p. 293. DOI: 10.1007/s13389-011-0023-x (cited on page 39).

[42] Michael Bruce and Victoria Bruce. "ABCs of Photon Emission Microscopy." In: *Electronic Device Failure Analysis* 5 (Aug. 2003), pp. 13–20. DOI: 10.31399/asm.edfa.2003-3.p013 (cited on page 39).

[43] B. L. Welch. "The Generalization of 'Student's' Problem When Several Different Population Variances Are Involved." In: *Biometrika* 34.1-2 (Jan. 1947), pp. 28–35. DOI: 10.1093/biomet/34.1-2.28 (cited on page 40).

[44] Jennifer Loveland. "Mathematical Justification of Introductory Hypothesis Tests and Development of Reference Materials." In: *All Graduate Plan B and other Reports* (May 2011), p. 47. DOI: 10.26076/40c5-3546 (cited on page 40).

[45] Walter W Piegorsch. "Tables of P-values for t-and Chi-Square Reference Distributions." In: *University of South Carolina Statistics Technical Report* (2002) (cited on page 40).

[46] *STM32CubeIDE - Integrated Development Environment for STM32 - STMicroelectronics*. URL: https://www.st.com/en/development-tools/stm32cubeide.html (visited on 01/11/2023) (cited on page 43).

[47] STMicroelectronics. *UM2319 Description of STM32Go HAL and Low-Layer Drivers*. Tech. rep. Oct. 2020, p. 2202 (cited on page 43).

[48] Joe Chalfoun et al. "MIST: Accurate and Scalable Microscopy Image Stitching Tool with Stage Modeling and Error Minimization." In: *Scientific Reports* 7.1 (July 2017), p. 4988. DOI: 10.1038/s41598-017-04567-y (cited on page 45).

[49] M.d. Moran. "Arguments for Rejecting the Sequential Bonferroni in Ecological Studies." In: *Oikos* 100.2 (2003), pp. 403–405. DOI: 10.1034/j.1600-0706.2003.12010.x (cited on page 53).

[50] Landelijk Competentieprofiel et al. *Landelijk Competentieprofiel Elektrotechniek Opleidingscode 34267*. Tech. rep. Jan. 2014 (cited on page 57).