COMPANY MENTORS
Barış Ege
Santiago Córdoba Pellicer

COMPANY
Riscure
Delftechpark 49, 2628 XJ Delft

STUDY ADVISER
C. de Joode

INTERNSHIP COORDINATOR
D. Djairam

STUDENT
Bob Swinkels
18057519

COURSE
HBO Elektrotechniek voltijd
The Hague University of Applied Sciences
Rotterdamseweg 137
2628 AL Delft

DATE
31 January 2022

PHYSICAL ATTACK ON A WLCSP

FINAL REPORT

Version 1.0

ABSTRACT

This internship has evaluated the feasibility of performing a physical attack by removing the RDL and probing the inner signals on the metal side of a STM32L082CZY6TR.

By approaching the sample from the metal-side, it was possible to capture EM signals (relating to the implemented software AES encryption) that were not visible on the silicon side of the sample.

TABLE OF CONTENTS

FIGURES AND TABLES

1 Introduction

1.1 Context & Background

Bob Swinkels is a third-year student at The Hague University of Applied Sciences. He has completed his third-year internship at Riscure from 15 November 2021 until 04 February 2021. During this period, the student has independently demonstrated the competencies in which he is considered proficient according to the Electrical Engineering degree (see Appendix D).

Bob Swinkels has worked as a security analysis intern in Riscure's innovation hub. The company mentors, Barış Ege and Santiago Córdoba Pellicer, are security analysts at Riscure and have coached the student during this internship.

1.2 About Riscure

Marc Witteman, who started Riscure in 2001, has worked in the semiconductor security industry since 1993. Founded in Delft, Netherlands, Riscure has now expanded its services to include clients from around the globe. Customers in the financial sector were primarily served by the company's first offerings, which mainly consisted of security evaluation services. Later on, evaluation services expanded into the pay-television market. At some point in 2005, Riscure's first product was sold to a customer, and the development of security test equipment became a vital part of the company's business. For its customers in North America, Riscure launched an office in San Francisco in 2011. For a similar reason, in 2017, they built a third office in Shanghai, China, to better collaborate with their customers in major markets.

To ensure the safety of all connected devices, Riscure tests the security of software, chip technology, and embedded/connected devices. Riscure is an international industry leader in offering test equipment for side-channel and fault injection robustness for chip technology. Manufacturers, government agencies, and security testing facilities worldwide rely on Riscure's equipment. [1]

1.3 Problem Description

Riscure needs to perform security analysis on Wafer Level Chip Scale Packages (WLCSP) with increasing regularity.

Before a physical attack can be executed on a WLCSP, the sample must first be prepared. Therefore, Riscure wants to investigate the possibility of preparing the samples in-house to perform physical attacks on this type of package.

1.4 Goal

This internship will evaluate the feasibility of performing a physical attack by removing the RDL and probing the inner signals on a WLCSP-49.

Specifically, the focus was on performing a physical attack on the STM32L082CZY6TR; this is an ARM Cortex-M0, STM32L0 Series Microcontroller in a WLCSP49 package.

2 The WLCSP

The Wafer Level Chip Scale Package (WLCPS) is one of the smallest package types currently available on the market, and because of their small size, WLCSPs are commonly used in modern smartphones. [2]

2.1 General

A WLCSP is usually 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 (Figure 1).

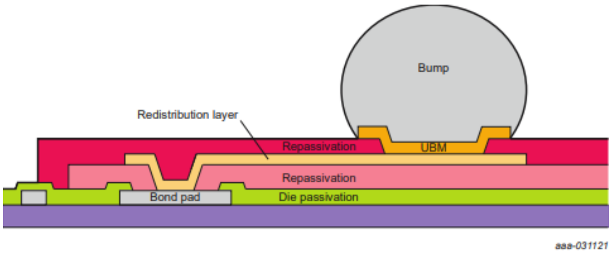
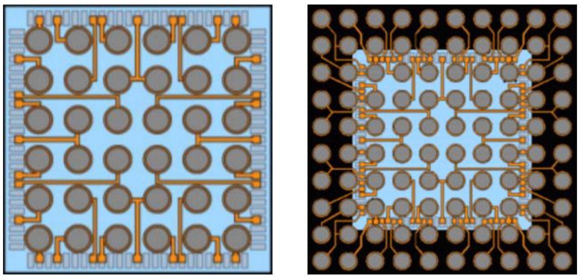


Figure 1 WLCSP layers [3]

There are two types of WLCSPs; Fan-Out and Fan-In. With Fan-In Wafer Level Packaging

(WLP), all traces on the RDL are routed towards the center of the die, whereas Fan-Out WLP allows for traces to be routed both inwards and outwards of the die area, thus allowing for more I/Os (see Figure 2). [4]



Fan-In WLP

Fan-Out WLP

Figure 2 Fan-In WLP vs. Fan-Out WLP [4]

2.2 STM32L082CZY6TR

The STM32L082CZY6TR is an ultra-low-power microcontroller with a high-performance Arm Cortex-M0+ 32-bit RISC core operating at a 32 MHz frequency, incorporated USB 2.0, hardware AES, a true random number generator, and is available in a WLCSP-49 format.

The WLCSP-49 package is very small, about 3.3 by 3.3mm in size (see Figure 3).

This microcontroller is chosen specifically for this feasibility study as it's widely available.

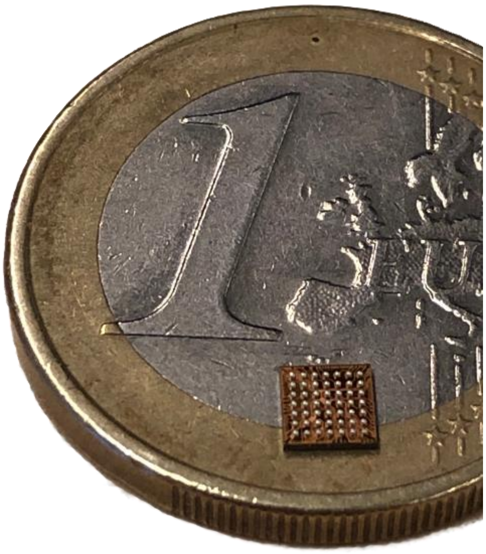
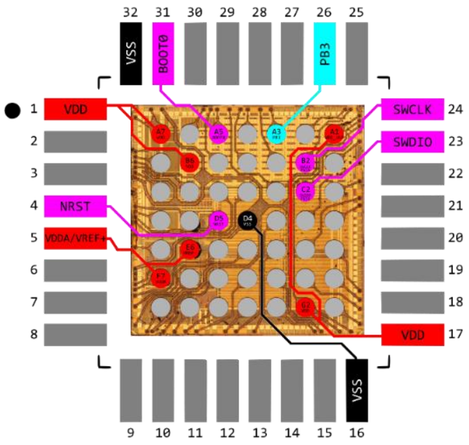


Figure 3 The STM32L082CZY6TR on top of a euro coin, metal side up

3 Dead-Bugged Prototype

The minimum pin configuration is determined by studying the datasheet [5] and relevant application notes [6, 7, 8, 9, 10].

A NUCLEO-L031K6 was used for verifying the minimum pin configuration of the STM32L082CZY6TR. The pads on the Nucleo board matching the pins of the minimum configuration are determined using the corresponding schematic [11] and Gerber files [12] (see Figure 4).



NOT to scale
PIN1-dot on sample is located behind pin A1
PIN1-dot of footprint is located on Nucleo board

Figure 4 Dead-bug connections for Nucleo Prototype

With this information available, the microcontroller present on the Nucleo board can be removed, and the STM32L082CZY6TR can be glued "upside-down" on the Nucleo board. Then the connections are made using a micro soldering iron and very fine insulated copper wire. The result is shown in Figure 5.

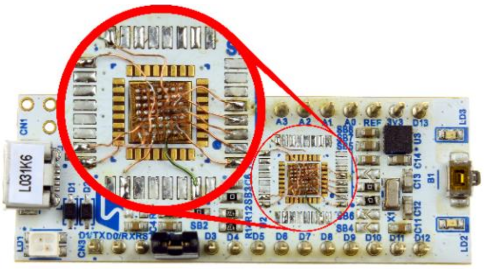


Figure 5 STM32L082CZY6TR dead-bugged on top of NUCLEO-L031K6 board

It was verified that this minimum configuration worked by flashing the microcontroller with minimal firmware to blink the onboard led with a fixed interval.

4 REMOVING THE RDL

To be able to probe the die itself using EM probing, first, the solder bumps and then the following layers on the metal side of the sample must be removed:

- Top-Repassivation layer
- Redistribution layer

For voltage probing, the following layers need to be removed in addition to the layers mentioned above:

- Bottom-Repassivation layer
- Die Passivation layer

4.1 POLISHING

The solder bumps, redistribution-, passivation- and repassivation layers can be removed using careful polishing. The problem with this is that, according to AN10439 [3], the bond pads are at the same level as the die passivation layer, so it is not possible to remove one without the other. Therefore this is a feasible method to prepare the sample for EM probing or preprocess the sample for chemical etching (see section 4.2).

For polishing, the MetPrep 3™ grinding/polishing machine is used (shown in Figure 6).

Figure 6 MetPrep 3™ grinding/polishing machine [13]

On this machine, polishing papers and grinding papers with various coarseness's/grids can be placed. You can accomplish amazing results by moving gradually to a finer grid during polishing.

4.1.1 By hand (or finger)

First, polishing was attempted by holding the sample directly with a finger which gave amazing results on the first try, and the sample was polished perfectly (see Figure 7). However, there was no success reproducing this result with successive samples after the first attempt.

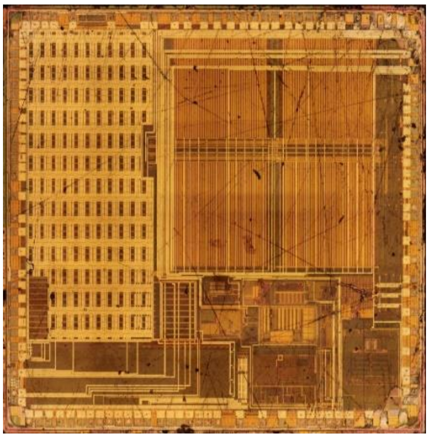


Figure 7 First attempt polishing sample

4.1.2 Machined sample holders

Sample holders (Figure 9) were machined on a Lathe (Figure 8) from extruded PMMA rod to make the polishing process more controllable

Figure 8 Lathe with PMMA rod inserted

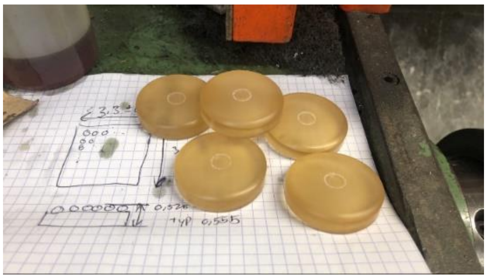


Figure 9 Finished sample holders

While machining the sample holders, extra attention was paid to ensuring the plane contacting the sample was parallel with the plane that contacts the polishing surface.

The chip can be fixed in the circular pocket in the center of the face of the sample holder using CA-glue[1]. Next, the holder is placed on the polishing machine with the face containing the sample touching the polishing disk.

The upside of this method is much more control over the polishing process. This is because the polished surface is much bigger, resulting in greater overall flatness of the polishing surface and a slower polishing process, thus more time to make corrections.

The downside is that the polishing-/grinding paper is clogged by the removed material of the sample holder, and when it's "full" with material, the polishing has almost no effect. This means you have to change polishing papers a lot which is time-consuming and wasteful. Furthermore, when you replace the polishing-/grinding paper, the polishing goes much faster again, leading to an inconsistent polishing process.

4.1.3 3D-Printed Sample Holders

Simultaneous with the machined sample holder, a few 3D-printed sample holders were designed and made (see Figure 10) to verify if this is a good alternative for the machined sample holders. However, these sample holders yielded significantly worse results than the machined sample holders.

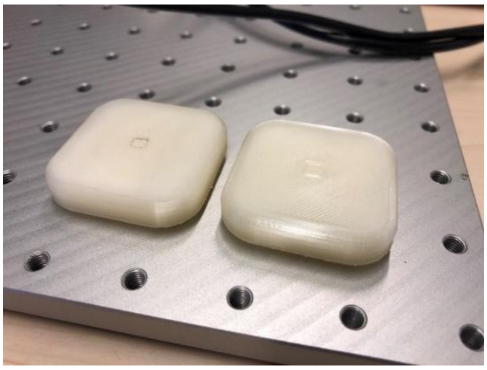


Figure 10 3D-Printed Sample Holders

The suspected reason for this is that the used material, polylactide (PLA), is too soft compared to the sample. Thus, the material is not removed by the abrasive but instead constantly deformed. Also, the material's melting temperature is much lower (because this is necessary for 3D printing); thus, if there is not enough cooling, the material softens, loses its mechanical stability, and is quickly ground away by the abrasive.

Therefore we decided not to continue with the 3D-Printed sample holders. However, possible future research can be done in holders printed on a 3d printer using Stereolithography (SLA) as these epoxies can be harder and have a higher melting temperature [14].

4.1.4 Tripod Polisher

The solution to the problems mentioned in sections 4.1.1, 4.1.2, and 4.1.3 is to use a device called a "tripod polisher."

To prepare the samples for TEM and SEM, researchers at the IBM East Fishkill Laboratory designed the Tripod Polisher (see Figure 11).

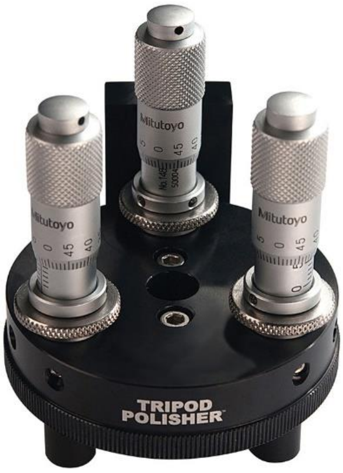


Figure 11 The PELCO® Tripod Polisher™ 590 [15]

The sample is attached to a Pyrex rod and the rod using a mounting wax, like Mounting Wax 70 (or 52) or Crystal Bond. Then the rod is attached to the center of the Tripod polisher, and the tripod polisher is placed on the polishing surface of the polishing machine. The micrometers each have a Delrin foot that rests

[1] Cyanoacrylate-glue, commonly referred to as superglue.

on the polishing surface. The micrometers can be used to tune the orientation while polishing. [16]

During this internship, a proposal was written to order a tripod polisher. This proposal can be found in Appendix A. Paul Verhaar, the Resource Manager at Riscure, approved this proposal, and the Tripod Polisher is ordered. However, the Tripod Polisher will arrive after the internship is finished because of the long lead times.

4.2 Chemical Etching

The redistribution-, passivation- and repassivation layers can be removed using chemical etching.

It was decided not to use chemical etching because it generates chemical waste, which must be deposited appropriately. In addition, the containers for the waste are single-use and expensive, and working with these chemicals requires special training.

4.2.1 Removing the (Re)Passivation Layer

The passivation- and repassivation layers are made of silicon oxide and can therefore be considered a glass layer that can be etched using Hydrofluoric Acid.

Because working with pure Hydrofluoric Acid can be dangerous, products can be used that contain a lower percentage of Hydrofluoric Acid or that contain similar acids. Examples of this are *Armour Etch glass etching cream* or *Pulpdent porcelain etch gel*. The porcelain etch gel has the benefit that it is less concentrated. It is a gel and coloured, thus easier to work with and see. [17, 18]

NOTE: Hydrofluoric acid and the products mentioned above are really dangerous chemicals and should only be used in a chemical lab with the necessary precautions and proper training. These chemicals are mentioned only for educational purposes, and the author nor Riscure recommends using these chemicals.

4.2.2 Removing the Redistribution Layer

The redistribution layer is made of metal and can be removed using Hydrochloric acid mixed with hydrogen peroxide or boiling Nitric acid. [18, 19]

NOTE: Hydrochloric acid and Nitric acid *are really dangerous chemicals and should only be used in a chemical lab with the necessary precautions and proper training. These chemicals are mentioned only for educational purposes, and the author nor Riscure recommends using these chemicals.*

4.3 Localized Passivation Layer Removal

During this internship, a new way of removing the passivation- or repassivation layers had been discovered. This method used the wire bonding machine to remove the (re)passivation layers using ultrasonic energy applied through the wire bonding machines wedge. This ultrasonic energy breaks the (re)passivation layer, after which it can be scraped away with the wedge. Using Localized Passivation Layer Removal, copper on the Redistribution layer can be exposed, after which a connection to it can be made using wire bonding (see Figure 12).

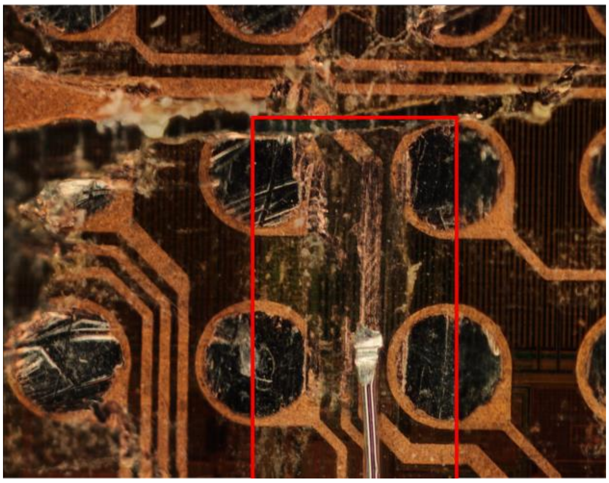


Figure 12 A wire, bonded to RDL trace that is exposed using Localized Passivation Layer Removal

For this, use the following procedure:

1. Set the machine to long bonding time.
2. Set the machine to high ultrasonic power.
3. For the 1st bond, set the TIME, POWER, and FORCE dials to their minimum value.

4. For the 2nd bond, the TIME and POWER dials are set to their maximum value, and the FORCE dial is set to its minimum value.
5. Remove the wire from the wedge.
6. Make a first bond during which the wedge touches the surface shortly and does nothing.
7. Now press and hold the STICH button.
8. While holding the STICH button, continue making bonds. Then, every time the wedge touches the surface, move the manipulator slowly away from you, dragging the wedge over the surface while it applies ultrasonic energy to the device.
9. You should see the material being removed very clearly through the microscope.

5 WIRE BONDING

At Riscure, there is a Kulicke & Soffa Model 4321 Wedge Bonder.

Wedge bonding is a kind of wire bonding used to fuse a wire to a pad of a device. This device can be a semiconductor IC, a chip carrier, or a PCB.

Wire diameters range from 15 µm to several hundred micrometers for high-power applications and are usually made from aluminium or gold. Aluminium wires can be bonded at room temperature, while gold wires need to be bonded at elevated temperatures of about 150°C. For this, a heated Workholder is needed.

Wedge bonding uses three types of energies:

- The heat from the Workholder - if the wire is gold wire (aluminium wire is bonded at room temperature).
- The ultrasonic vibration of the Wedge tip. This vibration is generated by the Ultrasonic Transducer that receives electrical energy from the Logic Board and translates into mechanical vibrations.
- The pressure (or Bonding Force) exerted by the wedge on the wire. An electromagnetic Force Actuator applies the Bonding Force on the rear of the Bonding Head armature, which is translated into a downward force at the front of the armature.

The K&S 4123 at Riscure has a wedge that supports a bonding wire thickness of 30µm.

The connector of the heated Workholder is not compatible with the connector present on the machine. Because of this, it is only possible to wire bond at room temperature, which makes it only possible to use aluminium or gold-coated aluminium bonding wire. The recommended elongation is 1-3%.

The machine only supports 0.5" spools.

5.1 WIRE BONDING MANUAL

During this internship, all procedures for setting up, calibrating, and working with the wire bonding machine have been documented in a 30-page Riscure procedure. They were reviewed by Carlo Maragno and tested by Barış Ege. The procedure has been placed on Treehouse (Riscure's Intranet).

6 CUSTOM PCB

A custom PCB had to be designed to break out the connections from the sample and connect the chip using Chip-On-Board (COB). COB is a method where the chip is placed directly on top of the PCB, and the connections are made using wire bonding.

During the design of the PCB, the design guidelines from the PCB, Würth Elektronik for COB [20], and the Else Kooi Laboratory for COB [21] were taken into account.

The final PCB (see Figure 13) has two layers and uses EuroCircuit's Class 6 tolerances to ensure minimal production times and optimal cost.

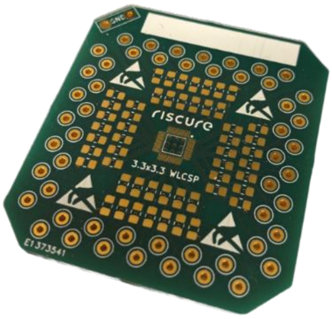


Figure 13 Custom PCB for attaching the sample using COB

There is a trace connecting every bond pad to a 0805 footprint and a trough-hole footprint where a test point can be inserted in the PCB. The other side of every 0805 footprint connects to ground, so it can be bridged to connect to ground directly, or a 100nF ceramic capacitor can be placed when the trace needs decoupling.

The bottom layer consists of a ground plane connected to the ground loop in the top left corner and the thermal plane under the chip using thermal via's.

At the top and the back of the PCB, there is an area where a small note can be written using a permanent fineliner.

The schematic for the PCB can be found in Appendix B, and the top and bottom renders in Appendix C.

The source and production files can be found on the internal Riscure GitLab (https://gitlab.com/riscure/interns/3.3x3.3-wlcsp-wire-bonding-pcb). When you push a commit, the DRC and ERC are run automatically by the implemented CI pipeline. Likewise, when you tag a commit with a version number, a release is automatically created, and the production files are compiled and added to the release.

While compiling the files, the date of the commit and version number of the tag are added to the documents and PCB, replacing the `%%date%%` and `%%version%%` placeholders.

7 Bonding the Sample

The decision was made to only prepare a sample for EM probing and not for voltage probing. This has the advantage that there is a minimal chance of damaging the bond pads on the die during sample preparation.

First, the sample is fixed, metal-side up, in the center of the custom PCB (section 6) using CA-glue.

The decision was made only to remove the repassivation layer where the wire bonds need to be made. Therefore, the Localized Passivation Layer Removal method (section 4.3) is used.

After this, bonds are made to the pads corresponding to the pins determined during the minimum pin configuration (section 3) (Figure 14).

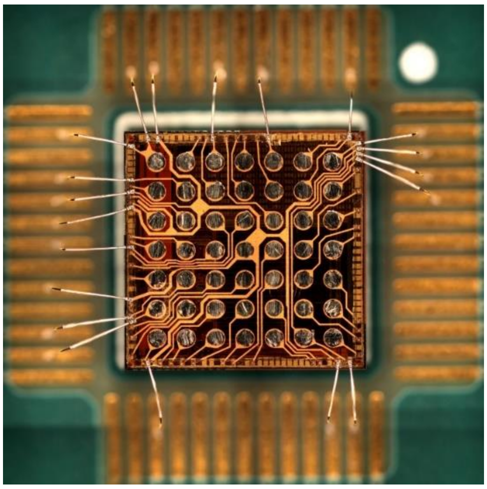


Figure 14 Sample COB connected to custom PCB (using wire bonding)

Then an ST-LINK V2 programmer is connected to the custom PCB using jumper wires (see Figure 15 and Figure 16).

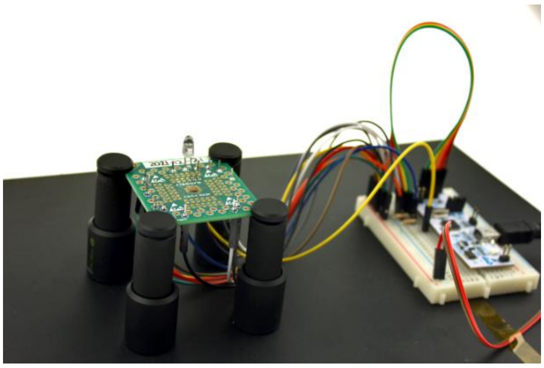


Figure 15 Custom PCB with wire-bonded sample and ST-LINK V2 programmer

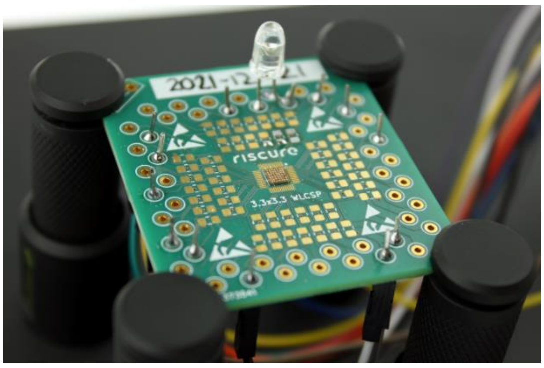


Figure 16 Custom PCB with wire-bonded sample

It was verified that the wire-bonded sample works by flashing the microcontroller with minimal firmware to blink the connected led with a fixed interval.

8 TVLA T-TEST

Next, it was determined if there is a benefit to doing all this work and approaching the device from the metal side when doing Side-Channel Analysis (SCA). EM traces were captured from both sides of the device and analyzed.

A software AES algorithm was implemented on the microprocessor using *Tiny AES in C* [22] that encrypts at random (determined by the onboard true random number generator) one of two predetermined inputs using a known key. The inputs are determined in such a way that one input returns a high Hamming weight on the 8th round, and the other input returns a low Hamming weight on the 8th round.

```
KEY:     0x5f440895d6d92d881f1e011084975684
INPUT1:  0x4286744AD46E1B83A61583BC4F632F9F
INPUT2:  0xC582E39FAA8ECB5850BA43B2821C32C6
```

8.1 TEST SETUP

The data acquisition takes place using Inspector FIPy, Riscure's platform for controlling the test equipment using Python. A script was written to control the XYZ stage, the BUS-Pirate, and the LeCroy oscilloscope from FIPy.

While the AES encryption is taking place, the led is illuminated. We use the led as a trigger for the oscilloscope, followed by a short pulse if the second input is encrypted and no pulse if the first input is encrypted. The pulse count can be retrieved from the oscilloscope using FIPy and used later to separate the traces into two groups when doing the TVLA analysis.

A block diagram of the test setup is shown in **Error! Reference source not found.**.

8.2 SILICON SIDE

To access the device from the silicon side, a sample was dead bugged to a PCB with a square hole in it (see Figure 18).

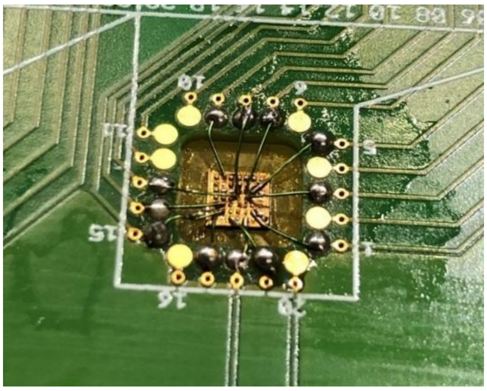


Figure 18 Sample dead-bugged in hole breakout PCB

It was verified that the dead-bugged sample works by flashing the microcontroller with minimal firmware to blink the connected led with a fixed interval.

Then the sample was covered with hot glue to fix it in place and protect the bonding wires. Finally, the PCB was flipped over, and the protective film on top of the sample was carefully removed using a scalpel with a chisel blade similar to blade SM62 (see Figure 19).

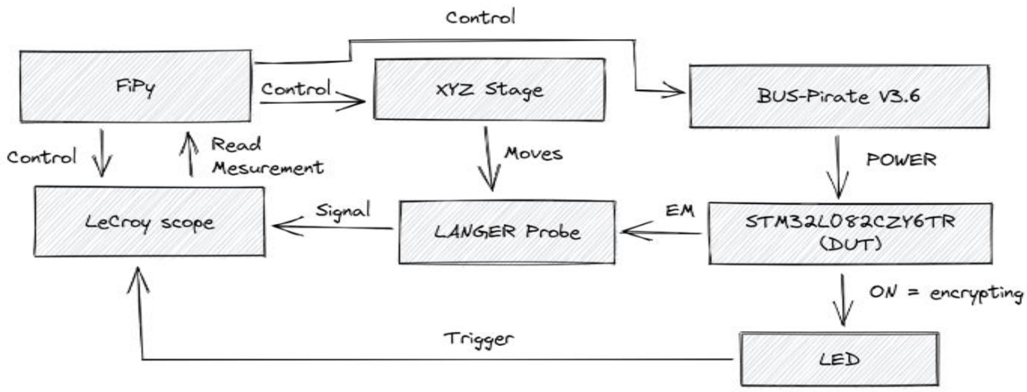


Figure 17 Block diagram test setup

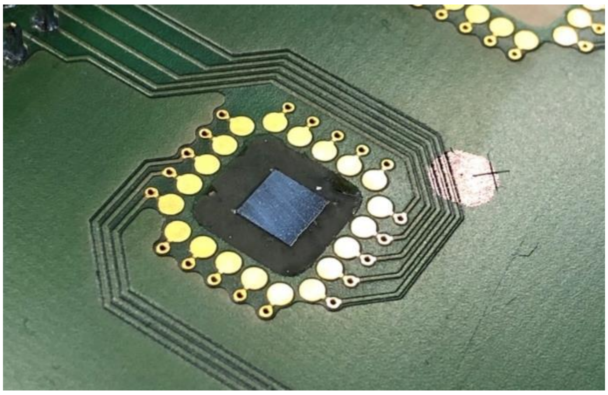


Figure 19 Silicon-side dead-bugged sample

The Langer EM probe was moved systematically over the device's silicon side using a scan grid of 20x20 points, and at each position, a trace was captured during the AES encryption. The AES encryption was not visible on the captured traces. It was also impossible to align the traces, which indicates no repeating pattern present. A few traces and a multispectral intensity plot are given in Figure 20 and Figure 21.

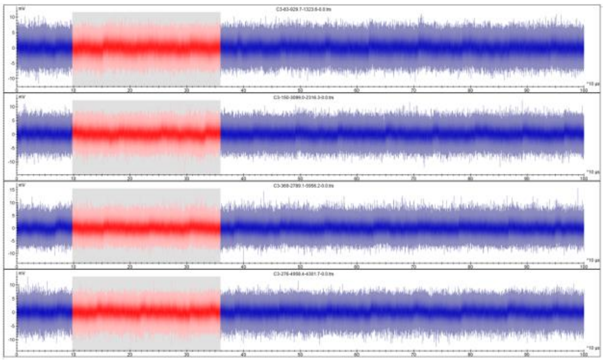


Figure 20 Traces silicon side during software AES encryption

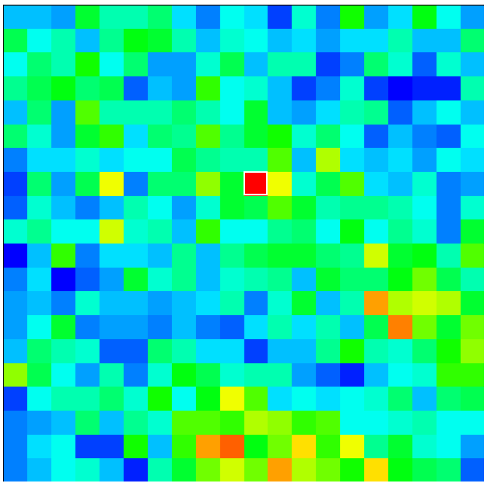


Figure 21 Multispectral intensity plot traces silicon side

8.3 Metal Side

The metal-side measurements were taken at every spot in-between the solder bumps resulting in 36 measurements. These locations are marked in Figure 22 with white stars.

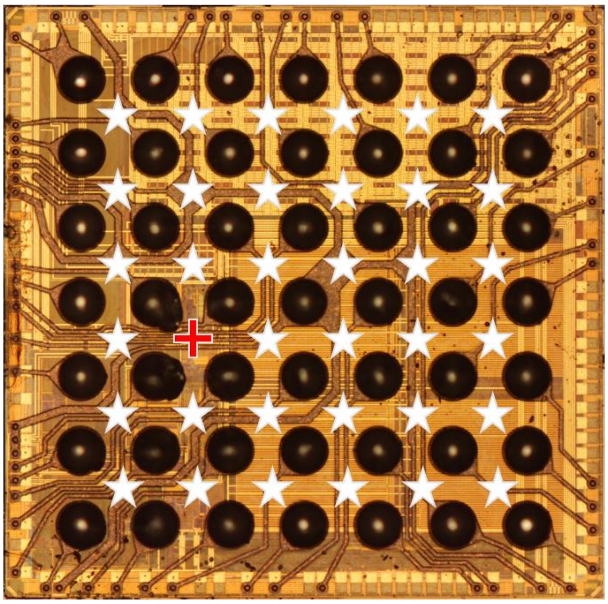


Figure 22 Measurement locations on the sample

When moving the probe between locations, the BUS-Pirate was used to cut the power to reduce the chance of the probe creating a short by touching two solder bumps simultaneously.

The traces were viewed in Inspector, and the spot with the best signal (see Figure 23), marked with a red cross in Figure 22, was chosen for the final acquisition. In this trace, all ten encryption rounds can be clearly seen.

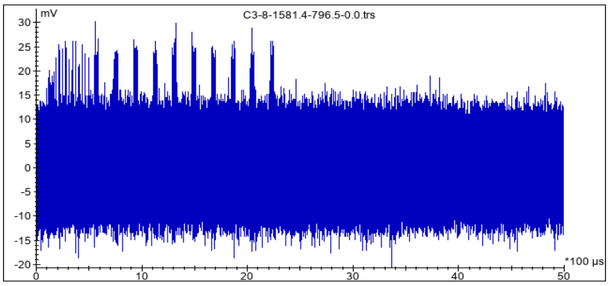


Figure 23 Trace from the location with the best signal, window = 200% of AES encryption

The Langer EM probe is placed on the spot with the best signal, and the scope capture window is set such that the last three rounds of the encryption are in view (see Figure 24 and Figure 25). Then 10.000 traces are captured using FIPy.

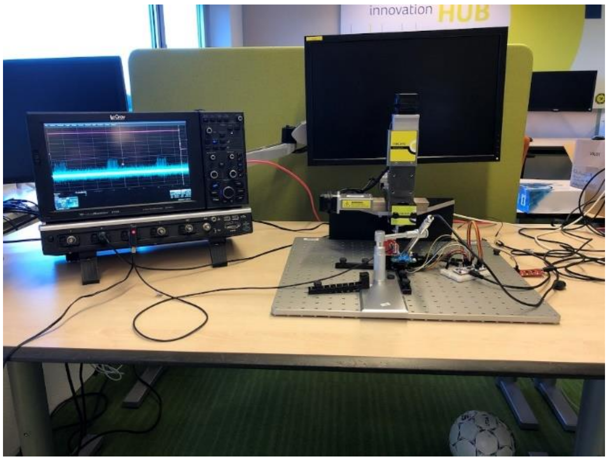


Figure 24 Test setup SCA

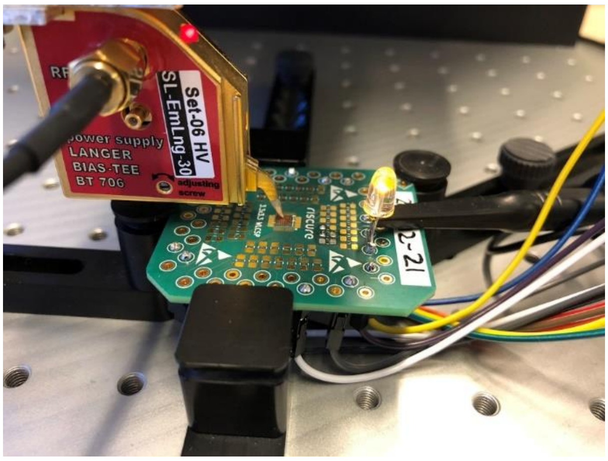


Figure 25 Langer probe positioned on the spot with the best signal

These traces are loaded into Inspector, and they are statically aligned, and then a Fixed vs. Fixed TVLA T-Test is executed (see Figure 26). As expected, we see the T-value clearly crossing the Threshold line at the 8th encryption round (where the Hamming weights are the highest).

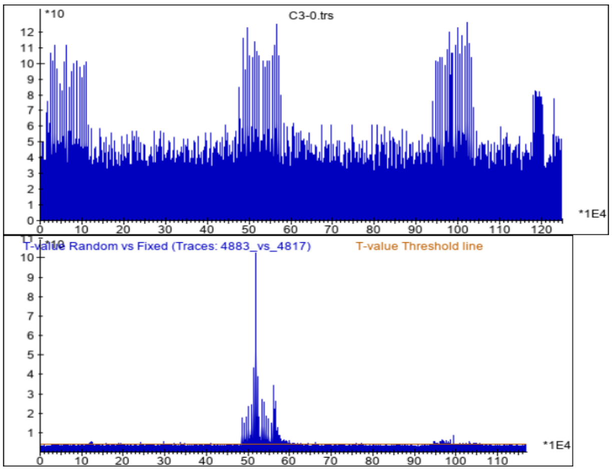


Figure 26 Result from Fixed vs. Fixed TVLA T-Test

Conclusion

The methods described in this report offer a feasible way to perform a physical attack, by removing de passivation layer and probing the inner signals, on a STM32L082CZY6TR in a WLCSP-49 package. As there is a low chance of destroying the device and there is information visible that is inaccessible when probing from the silicon side.

In addition to the benefits mentioned above, another benefit is that sample preparation can be done in house and can be relatively fast, as it takes around 5 hours of work.

The outputs of this internship are this progress report, the K&S Model 4123 Wedge Bonder procedure (available on Treehouse, Riscure's intranet), the proposal for ordering a tripod polisher, and a design for a custom PCB for attaching 3.3x3.3mm samples using a Chip-on-Board method.

References

[1] Riscure, "About Riscure," [Online]. Available: https://www.riscure.com/about-riscure. [Accessed 15 November 2021].

[2] M. Lapedus, "Fan-Out Packaging Gains Steam," 23 November 2015. [Online]. Available: https://semiengineering.com/fan-out-packaging-gains-steam/. [Accessed 2021 November 15].

[3] NXP Semiconductors, "Appl. Note AN10439," 10 July 2018.

[4] ASE Group, "Fan-Out Packaging," [Online]. Available: https://ase.aseglobal.com/en/technology/fan_out. [Accessed 15 November 2021].

[5] STMicroelectronics, "STM32L082CZ," 14 November 2019. [Online]. Available: https://www.st.com/resource/en/data

sheet/stm32l082cz.pdf. [Accessed 20 January 2022].

[6] STMicroelectronics, "ST-LINK/V2," 25 November 2020. [Online]. Available: https://www.st.com/resource/en/data_brief/st-link-slsh-v2.pdf. [Accessed 20 January 2022].

[7] STMicroelectronics, "AN5543," 29 June 2021. [Online]. Available: https://www.st.com/resource/en/application_note/an5543-enhanced-methods-to-handle-spi-communication-on-stm32-devices-stmicroelectronics.pdf. [Accessed 20 January 2022].

[8] STMicroelectronics, "AN4879," 18 December 2018. [Online]. Available: https://www.st.com/resource/en/application_note/an4879-usb-hardware-and-pcb-guidelines-using-stm32-mcus-stmicroelectronics.pdf. [Accessed 20 January 2022].

[9] STMicroelectronics, "PM0223," 10 October 2019. [Online]. Available: https://www.st.com/resource/en/programming_manual/pm0223-cortexm0-programming-manual-for-stm32l0-stm32g0-stm32wl-and-stm32wb-series-stmicroelectronics.pdf. [Accessed 20 January 2022].

[10] STMicroelectronics, "UM1075," 18 October 2018. [Online]. Available: https://www.st.com/resource/en/user_manual/dm00026748-st-link-v2-in-circuit-debugger-programmer-for-stm8-and-stm32-stmicroelectronics.pdf. [Accessed 20 January 2022].

[11] STMicroelectronics, "STM32 Nucleo (32 pins) schematics," 9 October 2018. [Online]. Available: https://www.st.com/resource/en/schematic_pack/nucleo-32pins_sch.zip. [Accessed 20 January 2022].

[12] STMicroelectronics, "STM32 Nucleo (32 pins) gerber files," 09 October 2018. [Online]. Available: https://www.st.com/resource/en/board_manufacturing_specification/nucleo-32pins_gerber.zip. [Accessed 20 January 2022].

[13] Direct Industry, "Sample preparation grinding polishing machine 5 - 350 rpm | MetPrep 3™," [Online]. Available: https://www.directindustry.com/prod/allied-high-tech-products/product-34997-1510091.html. [Accessed 28 January 2022].

[14] Formlabs , "3D Printing For High Thermal Stability: Get to Know High Temp Resin," 6 December 2018. [Online]. Available: https://formlabs.com/blog/high-temp-resin-high-thermal-stability-3d-printing/. [Accessed 20 January 2022].

[15] Agar Scientific Ltd., "59100-tripod-polisher-590-900px_1.jpg," 16 June 2021. [Online]. Available: https://www.agarscientific.com/media/catalog/product/cache/9c154f880acfcfd48a442571bde42c42/5/9/59100-tripod-polisher-590-900px_1.jpg. [Accessed 20 January 2022].

[16] H. w. Cha, M.-C. Kang, K. Shin and C.-W. Yang, "Transmission Electron Microscopy Specimen Preparation of Delicate Materials Using Tripod Polisher," *Applied Microscopy,* vol. 46, no. 2, pp. 110-115, 2016.

[17] Hackaday, "Hackaday Supercon - Ken Shirriff : Studying Silicon: Reverse Engineering Integrated Circuits," 04 November 2018. [Online]. Available: https://www.youtube.com/watch?v=TKi1xX7KKOI. [Accessed 20 January 2022].

[18] HackersOnBoard, "Defcon 21 - Decapping Chips The Strike Easy Hard Way," 16 November 2013. [Online]. Available:

https://www.youtube.com/watch?v=0Z4aF-qiziM. [Accessed 20 January 2022].

[19] Robert Baruch, "How I reverse engineer a chip," 24 April 2017. [Online]. Available: https://www.youtube.com/watch?v=r8Vq5NV4Ens. [Accessed 20 January 2022].

[20] Würth Elektronik Group, "Würth Elektronik Webinar: Wire bonding on PCBs, the perfect connection for unpackaged semiconductors," 3 June 2015. [Online]. Available: https://www.youtube.com/watch?v=qzOpemvJG20. [Accessed 20 January 2022].

[21] Else Kooi Laboratory, "General Rules for Bonding and Packaging at the Else Kooi Laboratory," 31 May 2017. [Online]. Available: https://d1rkab7tlqy5f1.cloudfront.net/EWI/Onderzoek/Else%20Kooi%20Lab/AssemblyDesignRulesv4%20%281%29.pdf. [Accessed 20 January 2022].

[22] Kokke, "Tiny AES in C v1.0," 1 February 2019. [Online]. Available: https://github.com/kokke/tiny-AES-c. [Accessed 20 January 2022].

APPENDIX A. PROPOSAL TRIPOD POLISHER

Proposal Tripod Polisher

Drafted by: Bob Swinkels

Background

During the internship of Bob Swinkels, various attempts were made at removing the redistribution and passivation layers from a sample in a WLCSP-49 package. The goal was to remove these layers while keeping the sample functional to attach and wire bond the sample, metal side up, to a custom PCB.

The polishing machine at Riscure can be considered a rotating disk with no other method of controlling the sample than by hand during the polishing process. Because of this, at the moment, polishing a sample is more of an art than a science, and thus results are not very repeatable.

Another field requiring very precise polishing of samples is Transmission Electron Microscopy (TEM) and Scanning Electron Microscopy (SEM). To prepare the samples for TEM and SEM, researchers at the IBM East Fishkill Laboratory designed the Tripod Polisher [1] (see Figure 1).

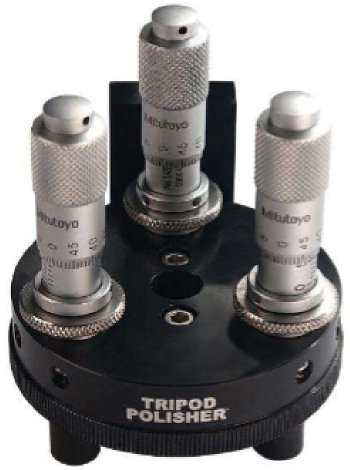


Figure 1 The PELCO® Tripod Polisher™ 590

The sample is attached to a Pyrex rod and the rod using a mounting wax, like Mounting Wax 70 (or 52) or Crystal Bond. Then the rod is attached to the center of the Tripod polisher, and the tripod polisher is placed on the polishing surface of the polishing machine. The micrometers each have a Delrin foot that rests on the polishing surface. The micrometers can be used to can tune the orientation while polishing. [2]

Proposal

We propose to order a tripod polisher capable of parallel polishing from Agar Scientific. The polisher and the accessories needed for parallel polishing can be ordered from their distributor, Van Loenen Instruments [3,4]. We need the following parts [5,6]:

AG59100 Tripod Polisher™ 590TEM precision sample thinning for TEM

AG59301 Parallel Polishing Mount with Pyrex

AG59302 Parallel Polishing Mount, 1.25-inch dia., Stainless Steel

AG59303 Planarizing Tool

AGB7311 Crystalbond 555 Adhesive Stick (68g)

AGB7312 Crystalbond 509-3 Adhesive Stick (90g)

References

[1] J. Benedict, R. Anderson, S. Klepeis, M. Chaker, in Specimen Preparation for Transmission Electron Microscopy of Materials-II, ed. Anderson, R., Mater. Res. Soc. Proc. 199, Pittsburgh, PA USA p. 189 (1990).

[2] H.-W. Cha, M.-C. Kang, K. Shin, en C.-W. Yang, "Transmission electron microscopy specimen preparation of delicate materials using Tripod polisher," Applied Microscopy, vol 46, no 2, bll 110–115, 2016.

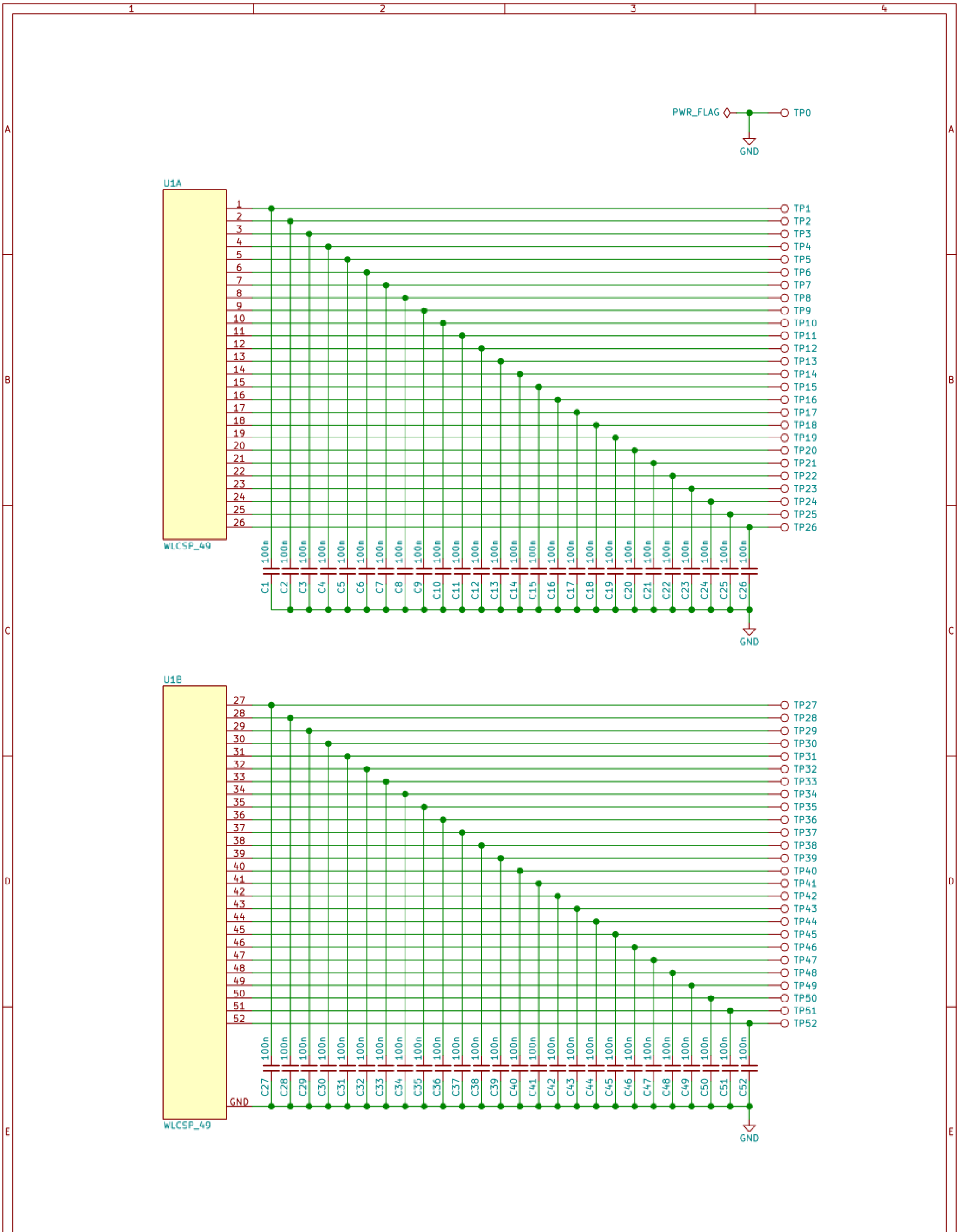
[3] https://www.agarscientific.com/fr/agents-distributors#N

[4] https://www.loeneninstruments.com

[5] https://www.agarscientific.com/fr/pelco-tripod-polisher

[6] https://www.agarscientific.com/fr/accessories-for-pelco-tripod-polisher

APPENDIX B. PCB SCHEMATIC



Logo2 Riscure Logo

Logo3 ESD ESD

Logo5 ESD ESD

Logo1 Riscure Logo

Logo4 ESD ESD

Logo6 ESD ESD

riscure

Riscure

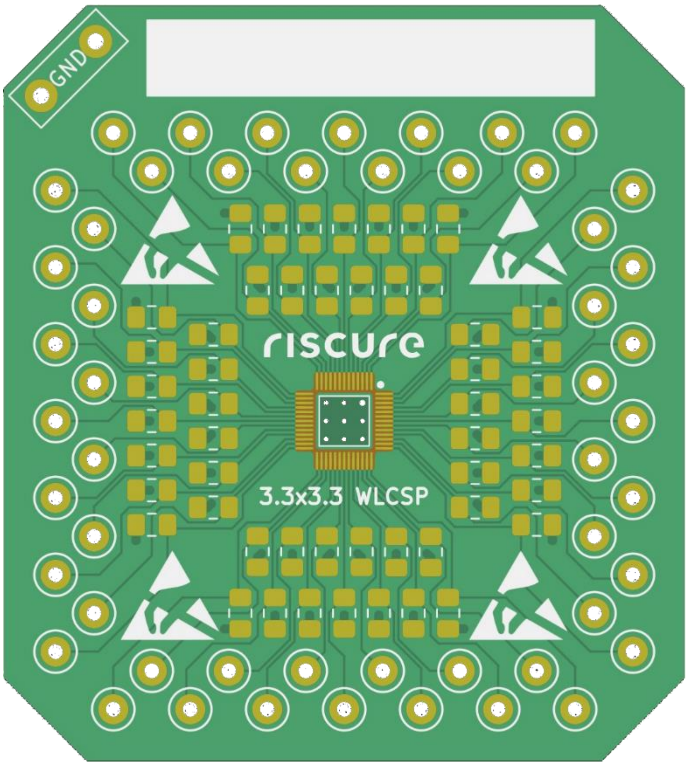
Sheet: /

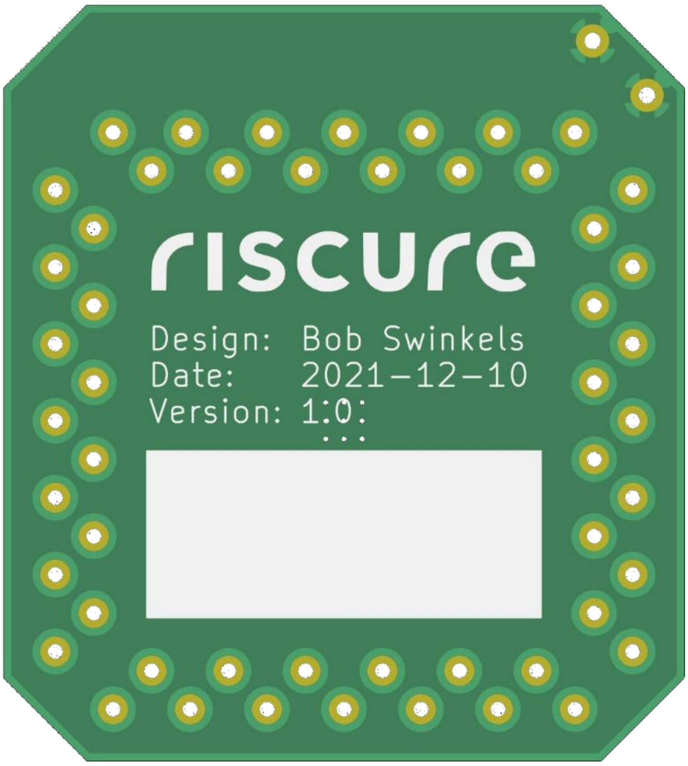
File: wirebonding-pcb.sch

Title: 3.3x3.3 WLCSP Wire Bonding PCB

Size: A4	Date: 2021-12-10	Author: Bob Swinkels	**Rev: 1.0**
KiCad E.D.A. eeschema 5.1.9+dfsg1-1bpo10+1			Id: 1/1

APPENDIX C. PCB TOP & BOTTOM





APPENDIX D. COMPETENCES DURING THE INTERNSHIP

During this internship, a variety of competencies has been shown.

Analyze
This competency was demonstrated during the Project Plan writing process. For example, it was necessary to formulate a clear problem statement based on the client's wishes and select the relevant aspects. This competency was also shown during the research phase when design decisions needed to be made.

Design
A concept solution had to be devised and chosen in response to the requirements. In doing so, the student had to consider the feasibility of the chosen solution and whether or not it meets the established requirements. In addition, this competency was addressed during PCB design because it entails selecting the appropriate design tools and adhering to guidelines. Thus, when making design decisions, this competency when addressed.

Realization
When working with the wire-bonding machine, polishing the samples, creating the sample holders, and making the final prototype for the SCA, the student had to use appropriate materials, processes, methods, norms, and standards. He also had to confirm that this satisfies the requirements. Furthermore, this competency was addressed during the PCB design process.

This competency was also demonstrated by writing the 30-page wire-bonding procedure for Riscure.

Finally, this competency was demonstrated by writing this final internship report, which documents the realization process.

Research
This competency was demonstrated during the Wafer Level Chip Scale Packages (WLCSPs) research because the student must first determine the objective. Then the student had to obtain scientific literature and other information sources independently to delve deeper into the question. The dependability of the information sources must be validated and summarized as part of this process.

This competency was demonstrated during the research into the polishing process and the wire-bonding procedures. Because therefore, "lost" knowledge had to be required.

Lastly, this competency was demonstrated when drafting the proposal for the Tripod Polisher because the student had to obtain scientific literature and other information sources independently to delve deeper into the question. Therefore, the dependability of the information sources must be validated and summarized as part of this process.

Managing
Throughout the internship, the student tad to communicate and collaborate with others in a multicultural, international, and multidisciplinary environment and meet the requirements of being a member of a work organization.

When the student initially had no access to the lab, he had to delegate work to an employee who had access and had received the necessary training. For this, the student's tasks included guiding employees, encouraging cooperation, and delegating.

Throughout the internship, the student was expected to communicate task- and process-oriented.

Professionalize

Throughout the internship, the student had t be flexible to function optimally in the company and various situations, reflect on his actions, determine what could be improved, and check his work.

Furthermore, during this internship, the student had to give an English presentation about his work to the company's other employees.

Finally, the student had to use various forms and modes of communication in Dutch and English to seek information, receive feedback, and request quotations.