**BRNO UNIVERSITY OF TECHNOLOGY**
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

**FACULTY OF INFORMATION TECHNOLOGY**
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

**DEPARTMENT OF INTELLIGENT SYSTEMS**
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

# ANALYSIS OF ATTACKS ON (MICRO)CHIPS AND DEVELOPMENT OF ENHANCEMENT OF THEIR ROBUSTNESS/SECURITY

ANALÝZA ÚTOKŮ NA (MIKRO)ČIPY A NÁVRH ZVÝŠENÍ JEJICH ODOLNOSTI/BEZPEČNOSTI

**EXTENDED ABSTRACT OF DOCTORAL THESIS**
ROZŠÍŘENÝ ABSTRAKT DISERTAČNÍ PRÁCE

**AUTHOR** **Ing. DOMINIK MALČÍK**
AUTOR PRÁCE

**SUPERVISOR** **prof. Ing., Dipl.-Ing. MARTIN DRAHANSKÝ, Ph.D.**
ŠKOLITEL

**BRNO 2019**

## Abstract

Nowadays, microchips are used virtually everywhere, from simple home devices to confidential military equipment. In many scenarios, sensitive data is being processed by these devices. For example, in the case of electronic personal documents, fingerprints, facial images, and personal data are processed by the chip; and in some cases also iris images. Auditing proclaimed functions and a level of security of such microchips is becoming a valued service. In this doctoral thesis, we present an experimentally proven process for the microscopic analysis of chips, feasible in a low-cost setup. The described process was demonstrated on a chip acquired from the Czech biometric passport—from extracting the chip out of the plastic card up to analysis of the acquired microscopic images. We investigated and evaluated various potentially viable methods for logic element recognition; without the employment of machine-learning. Additionally, hardware-oriented attacks are discussed and followed by proposals for countermeasures leading to the hindering of microscopic analysis.



## Abstrakt

S využitím mikročipů se dnes setkáváme prakticky na denní bázi, od jednoduchých zařízení pro domácí použití až po utajované vojenské vybavení. V mnoha případech navíc svěřujeme těmto zařízením velmi citlivá data, jako i v případě elektronických dokladů – otisky prstů, fotografie obličeje, osobní data; a v některých případech například i obraz oční duhovky. Ověření deklarované funkčnosti a míry zabezpečení takových mikročipů se tak stává žádanou službou. V rámci této disertační práce prezentujeme experimentálně ověřený proces mikroskopické analýzy mikročipů proveditelný v nízkonákladovém režimu. Popsaný proces jsme poté demonstrovali na čipu z českého biometrického pasu – od získání čipu z plastové karty až po jeho analýzu na základě získaných mikroskopických snímků. V rámci analýzy jsme prozkoumali a porovnali různé metody bez strojového učení potenciálně využitelné k rozpoznávání logických elementů. Dále jsme provedli zhodnocení aktuálních hardwarově orientovaných útoků na mikročipy. V návaznosti na toto zhodnocení jsme navrhli možná protiopatření zaměřená primárně na ztížení procesu mikroskopické analýzy.



## Keywords

Microchip, chip, chip package, deprocessing, dry etching, wet etching, security analysis of chips, microscopic analysis, SmartMX, MIFARE Classic.

## Klíčová slova

Mikročip, čip, pouzdro čipu, deprocesing, plasmatické leptání, chemické leptání, bezpečnostní analýza čipů, mikroskopická analýza, SmartMX, MIFARE Classic.

## Reference

MALČÍK, Dominik. *Analysis of attacks on (micro)chips and development of enhancement of their robustness/security.* Brno, 2019. Extended abstract of doctoral thesis. Brno University of Technology, Faculty of Information Technology. Supervisor prof. Ing., Dipl.-Ing. Martin Drahanský, Ph.D.

# Contents


**1 Introduction** **3**
1.1 Motivation . . . 3
1.2 Thesis Contribution . . . 3
1.3 Thesis Organization . . . 4

**2 Research Goals** **5**

**3 Microscopic Analysis** **6**
3.1 Obtaining Chips from Plastic Cards . . . 6
3.2 Chip Decapsulation . . . 6
3.2.1 Chemical Approach for Removal of Plastic Packages . . . 7
3.2.2 Grinding and Polishing of Plastic Packages . . . 9
3.3 Chip Deprocessing . . . 9
3.3.1 Cross-Section Analysis . . . 9
3.3.2 Chemical Deprocessing . . . 10
3.4 Layers Scanning . . . 11
3.4.1 Processed Chips . . . 11
3.5 Analysis of The Images . . . 12

**4 Analysis of The Czech Biometric Passport Chip** **13**
4.1 Extraction and Decapsulation . . . 13
4.2 Deprocessing . . . 14
4.2.1 Cross-Section Analysis . . . 14
4.2.2 Removing Layers . . . 14
4.3 Image Scanning . . . 15
4.4 Image Stitching . . . 15
4.5 Analysis . . . 16
4.5.1 Bond Pads Identification . . . 17
4.5.2 Chip Segments Identification . . . 18

**5 Chip Security Improvements** **20**
5.1 Reverse Engineering Countermeasures . . . 20
5.2 Complex Integration and Camouflaging . . . 20
5.2.1 Heterogeneous Integration . . . 21
5.2.2 Cell Camouflaging . . . 21
5.2.3 3D Integration with Dummy Dies . . . 22
5.3 Active Tamper Detection . . . 22
5.3.1 Active Tamper Detection with Active Memory Protection . . . 22

5.3.2 FPGA Employment with Active Bitstream Protection . . . . . . . . 24
5.4 Active Defense Against Microprobing . . . . . . . . . . . . . . . . . . . . . . 24
5.5 Disabling Backside Observations . . . . . . . . . . . . . . . . . . . . . . . 24
5.6 Active Defense Against X-Ray . . . . . . . . . . . . . . . . . . . . . . . . 25
5.7 Passive Defense Against X-Rays . . . . . . . . . . . . . . . . . . . . . . . 25

**6 Software tools for Microscopic Analysis** **26**
6.1 Setup . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
6.2 Template Matching . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
6.2.1 Template Matching Summary . . . . . . . . . . . . . . . . . . . . 28
6.3 Feature Descriptors . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
6.3.1 Feature Descriptors Summary . . . . . . . . . . . . . . . . . . . . 29
6.4 Shape Matching . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30
6.4.1 Shape Matching Summary . . . . . . . . . . . . . . . . . . . . . . 32
6.5 Summary and Future Work . . . . . . . . . . . . . . . . . . . . . . . . . 32

**7 Conclusion** **33**
7.1 Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34

**Bibliography** **36**

**A Relevant Publications** **45**
A.1 Publications . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
A.1.1 Conferences . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
A.1.2 Journals . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
A.1.3 Submitted Publications . . . . . . . . . . . . . . . . . . . . . . . 45

**B Curriculum Vitae** **46**
B.1 Education . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 46
B.2 Conferences, Summer Schools, Presentations . . . . . . . . . . . . . . . . 46
B.3 Projects . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
B.4 Teaching . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
B.5 Work Experience . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 48

# Chapter 1

# Introduction

## 1.1 Motivation

Nowadays, many different types of chips are used virtually everywhere in the real world. There exist various incentives why one would like to see what is under the hood of a chip. Starting with QA departments of the chip producers, continuing over competition scanning, up to security auditing (i.e., auditing a device that was proclaimed secure). Such investigations are available in the market; however, these are mostly available in the commercial sector. The companies providing these services are keeping their know-how concealed. In the academic sphere, we are witnessing rather isolated attempts of such analyses scattered among various departments than a coherent work. We would like to contribute to the knowledge and capabilities maintained in academia with the mapping of the microscopic analysis in detail and, of course, with providing additional value to the status quo.

A few decades back, the chips were rather simple, and actually not that small. Observations, and even understanding of such devices, were possible with not much effort, i.e., we have decapsulated and deprocessed a single chip containing only four NAND cells. Analyses of these uncomplicated devices requires just an optical microscope and a few hours of work in a lab. On the contrary, dealing with contemporary chips used in biometric passports is a completely different challenge (and we have to admit that there are even more advanced chips, e.g., conventional CPUs, GPUs). The growing integration density and increasing die area result in the enormous complexity of the devices. Thus, it is impossible to apply manual only approaches. Moreover, the equipment capable of dealing with such advanced devices is very costly and thus not always available to low-cost attackers, as we are.

## 1.2 Thesis Contribution

Our focus laid mainly in the area of microscopic analysis of the microchips. We had to manage the whole process of chips decapsulation and deprocessing in order to get to the dies we wanted to investigate. Thus, the contributions of this thesis are broader than just a single topic. We truly believe that this thesis will help other institutions that want to tackle microscopic analysis of chips to manage the process based on the very detailed instructions and processes we present in this thesis. We believe that the main contributions are:

- A detailed description of methodologies for obtaining, decapsulation and deprocessing of the chips including improvement of the process of obtaining chips from thermoplastic compounds—plastic cards used for wrapping smartcard chips.

- Proposals for security improvements of the chips, focused primarily on hindering microscopic analysis. Techniques like 3D integration, MEMS, or battery-backed security fuses are presented in this thesis.

- Analysis of a chip belonging to the SmartMX family (used in biometric passports, ID cards, etc.) performed in a low-cost setup. Although not having regular access to needed equipment, we were able to completely analyze the chip construction—described in detail in this thesis, partially deprocess it and analyze the gained specimens.

- The comparison of methods that are not commonly used for processing of the chip silicon layer images without the employment of typically used machine-learning methods. Such an approach removes the need for complex training and verification data sets.

## 1.3 Thesis Organization

The text of this extended abstract consists of seven chapters. Chapter 2 states the research goals for the doctoral thesis. The analysis of microchips used in the e-documents is presented in detail in Chapter 3. Chapter 4 is devoted to the analysis of the Czech biometric passport chip. Possible attacks are discussed, and security enhancements are proposed in Chapter 5. Comparison of various methods potentially usable for logic elements recognition without the employment of learning approaches is presented in Chapter 6. Finally, Chapter 7 provides a final summary of the work with a conclusion and future work proposals.

# Chapter 2

# Research Goals

This doctoral thesis is focused on microscopic analysis of chips in general, and subsequently on all stages—decapsulation; deprocessing; image acquisition; image postprocessing; and analysis. The main goals of the doctoral thesis are:

- Microscopic analysis process:
  - Decapsulation of chips.
  - Deprocessing of chips.
  - Acquisition of the layers with the use of microscopes.
  - Analysis—manual analysis and computer-aided analysis.
- Performing microscopic analysis of the Czech biometric passport chip.
- Overview of feasible hardware attacks on microchips.
- Proposals for chips' security improvements.

One of the aims of this doctoral thesis is to prepare a precise methodology usable for microscopic analysis. It will require inter-disciplinary work, including regular visits to chemical and QA laboratories. Within the thesis, we plan to perform the experiments on our own as far as possible. This will enable us to describe the processes in detail in order to provide a proven approach to the microscopic analysis. After creating the methodologies for decapsulation and deprocessing that are feasible in our low-cost setup, the methodologies will be verified by repeated experiments on various chips—first, we intend to use very simple chips in classic packages, and then move on to smartcard chips, e.g., MIFARE Classic, MIFARE Ultralight, and MIFARE DESfire. The microscopic analysis methodology will be completed with an image acquisition process performed with appropriate microscopy, processing of the acquired images, and the image analysis supported by software or algorithmic approaches.

The next aim is to perform microscopic analysis of the chips used in Czech biometric passport implementation. These chips are still in practical use—traveling with Czech citizens virtually all around the globe.

Furthermore, based on the research and knowledge that will be gained while carrying out the experiments and during the theoretical study of available attack scenarios, we will propose possible improvements to the chips' security. This section will primarily aim at hardware-oriented attacks related to microscopic analysis.

# Chapter 3

# Microscopic Analysis

In this chapter, we will go through the whole process of microscopic analysis as we did in our experiments. We will deal with all parts from obtaining the chips up to the final analysis of the acquired images. All of these steps have to be mastered in order to be able to succeed with microscopic analysis performed from scratch[1].

## 3.1 Obtaining Chips from Plastic Cards

Many RFID chips and security-oriented chips are stored in plastic cards. This is also the case for biometric passports or other personal documents. First, parts of the plastic cards with the chips inside have to be cut out from the rest of the plastic cards (see Fig. 3.1). Then, extraction of the encapsulated chips from the plastic cover is carried out. In the early stages, we used only acetone bath in a beaker at normal room temperature. The extraction took several minutes or even tens of minutes. The plastic card was slowly becoming pliable, and it was possible to peel the plastic layers off one after another. We improved the process with the use of a boiling nest (displayed in Fig. 3.1). The time of extraction got shortened to 1–3 minutes per piece. We heated the acetone to its boiling temperature (slightly above 50 °C), the plastic compound was then almost immediately removable. We highly recommend using plastic gloves.

## 3.2 Chip Decapsulation

For the purpose of chips decapsulation, two main approaches are commonly presented—etching and grinding (sometimes stated as polishing). Both are specific, and it is always felicitous to have the capability of performing both. There are several books dealing especially with the chip packages and the related topics, e.g., [73], [17], [78], [8].

It can be said, very briefly, that there are three main types of common chip packages with respect to their material—metal, ceramic and plastic. The most important category for us is the plastic one. These packages are widely used (also because of their low price) and are often suitable for most of the ordinary integrated circuits.

We decided to follow the mainstream packages in this thesis, the plastic packages. The effective approach of obtaining bare chips out of plastic packages with the use of sulphuric and nitric acids was performed within the scope of the Brno University of Technology in cooperation with Faculty of Chemistry and is described herein. [50]

[1]This was exactly our scenario, building all the knowledge at our faculty completely from scratch.

Figure 3.1: Left: Boiling nest with acetone bath. Middle: Two beakers with acids with the decapsulation process is progress in the left one. Right: The result of the decapsulation process—bare chips on their original pads. (Source: author's work.)

### 3.2.1 Chemical Approach for Removal of Plastic Packages

The chemical approach is usually more convenient compared to the other ways of removing plastic packages, because of its simplicity, low time requirements, low price and availability of the chemicals involved. The fact is also that the chemicals are chosen in a manner that they react only with the plastic compounds—the danger of damaging the sample surface is then minimal because the surface of the chip is protected by a passivation layer. There exist different variants of the chemical approach that make use of the same acids, but mostly in a different step order or acids ratio [16]. However, some of them are totally dissimilar, i.e., another technique that is based on using resin instead of acids (briefly described in [67]). It has a significant drawback—it takes a lot of time. In fact, it is not recommended to follow this approach in a chemical lab, because resin vapors can foul up the exhaust. Moreover, the temperature of resin during the etching process should be really high, approx. 350 °C. This temperature may cause serious damage to the chips. On the other hand, the use of dangerous acids is completely avoided in this scenario. [50], [77], [76], [47]

As mentioned above, in our case, there is a need for cooperation with a chemical facility, because we cannot avoid working with chemicals. Let us assume that all the next steps take place in a properly-equipped chemical laboratory. At least a fume cupboard, a chemical sink, and personal protective equipment should be available for the etching process. Passed safety training is also a must. It is strongly recommended to proceed very cautiously while observing the chemical laboratory rules to avoid any injuries or damage to the laboratory equipment or to the chips.

#### The Ratio of Nitric Acid to Sulphuric Acid

Prior to the beginning of the etching itself, it has to be decided what is expected as a result. According to our needs, the correct ratio of the acids mixture has to be chosen. The result is affected not only by the ratio of the acid, but also by the time duration of the active etching (the time period when the specimen is inside the acid bath) and also by the temperature of the acids.

The ratio is always stated as nitric acid to sulphuric acid (the recommended approx. temperature is mentioned in brackets) [49]. Length of active etching has to be determined experimentally for each type of package.

- 5:1–3:1 (ca. 90–94 °C)—preservation of wire bonds from the lead frame to the chip.
- 2:1–1:1 (ca. 90–94 °C)—faster, cheaper, and a more aggressive decapsulation.
- 0:1 (up to ca. 270 °C)—to etch very resistant molding compounds, very aggressive.

**Whole-Package Decapsulation Process.**

First, four beakers should be prepared. Two beakers should be half-filled with the acids in the correct ratio (see Chapter 3.2.1). The third beaker should be half-filled with acetone, and the last one with demineralized water. The cooker must be placed into a fume cupboard because of the production of dangerous vapors. Other recommended equipment should be placed nearby the fume cupboard or even inside if there is enough room for all the items. Only the beakers with acids need to be placed on the cooker in order to reach the desired working temperature. The other steps of the whole process should take place out of the cooker.

The major etching should be performed in the first beaker with the acids. The acids will become non-transparent soon due to the presence of etched molding compounds. The recommendation is to inspect the level of decapsulation during the process often periodically. When the process is almost complete, it is better to use the second beaker with the transparent acids to do the fine etching. It is necessary to monitor the progress permanently at this point. The transparent acid is ideal for this purpose. We do not recommend leaving the specimens in the acid bath longer than is necessary—the lower layers could be damaged by the acid because these layers are usually not protected along the chip edges and thus so-called underetching can occur.

When the chip is bared, it should be washed in the beaker with acetone. In cases where the chip surface is bigger than 5 $mm^2$, we recommend using demineralized water first, acetone and demineralized water again due to safety reasons—a bigger amount of the acid left on the chip can react with acetone. Then, the specimen should be rinsed with flowing demineralized water, and it should be put inside another beaker with demineralized water afterward. The beaker with the demineralized water and the chip or with more chips, as the case may be, should be placed into an ultrasonic cleaner for up to two minutes in the case where there is only one chip in the beaker or for ca. thirty seconds in the case when there are more chips in that beaker. With little exaggeration, the chips act as emery paper to each other. Then a final check should take place. If everything seems to be alright, the chips should be dried with filter paper or nitrogen flow. If there is any problem with the cleanliness of the chip surface or similar, the entire process can be repeated [49].

**Etching of Specific Packaging Part**

A useful approach for some use cases is to etch out only a specific part of the chip package. The entire chip is preserved, and hence, it can be attached to other components as usually. Because of the manual dosing of acid drops to the specific area via a dropper, this process is more demanding. First, a little hollow is made in the surface of the chip, approx. in the center of the area designated for etching. Then, the drops of sulphuric acid are manually applied to the chosen location. Nitric acid is mostly not used in this approach. There has to

be a short period of inactivity between the applications of the acid drops to allow reaction with the surface. [49]

### 3.2.2 Grinding and Polishing of Plastic Packages

The grinding and polishing approach is suitable in cases where we cannot apply the chemicals, or the chip package allows the use of a grinder with its advantages, i.e., the chip is placed deeper in the package and there is a gap above the chip—in that case the wirebonds can be easily preserved also with use of grinder. It is necessary to proceed cautiously to avoid contact of the grinder with the surface of the chip or with wirebonds. For this reason, it is recommended to use an X-ray to inspect the starting situation and then the current level of decapsulation periodically. [50], [77], [76], [47]

## 3.3 Chip Deprocessing

Each conventional chip is a composition of different oxide and metal layers above one transistor layer that is formed on the silicon substrate. Nowadays, we can also encounter various 2.5D or 3D layouts, these are way beyond our capabilities, and thus, we focus on conventional layouts in this thesis. The layers across producers are made of various compounds with respect to the desired functionality and needed properties of the whole layout.

The chip deprocessing (delayering) involves three main techniques: dry etching (plasma etching), wet etching (using different types of chemicals) and polishing. In any case, the best practice is to start with a cross-section analysis, including the thickness of layers measurement and materials analysis. Only after the information is harvested from the cross-section analysis, the correct procedure can be created and carried out.

Although a suitable chemical procedure can be found for each layer, it is sometimes not possible to choose wet etching because of the high risk of damaging other layers, i.e., an underetching problem. In these cases, it is still possible to make progress with a special grinder (capable of parallel polishing) and a decent level of skillfulness. Unfortunately, we were unable to reach such a special grinder within our partners. [51]

### 3.3.1 Cross-Section Analysis

Virtually all laboratory grinder may be suitable for preparation of a specimen cross-section. It is convenient to prepare more cross-sections of one chip type always in a different position in order to gain more information about that chip. When the results are satisfactory, we use an electron microscope to observe the layers in more detail (displayed in Fig. 3.2).

Displaying cross-section immediately after grinding provides the image with hard-to-distinguish borders of some layers and low distinction among these layers. Thus, to make the observability better, there are various etchants used for finishing the sample before scanning. For oxide layers, $NH_4F$, $CH_3COOH$, $H_2O$, and $HF$ can be used; for diffusion semiconductor layers, $HNO_3$ and $HF$ can be used [84]. Recent FIB devices (i.e., TESCAN FERA3) allow for some limited use of this wet etching directly in-situ, however only with some of the chemicals supported.

After the cross-section is made, the next step is to employ one of the spectrometric techniques to acquire the elements' composition. For example, an electron microscope equipped with an X-ray detector can provide such information—see Fig. 3.2. A precise

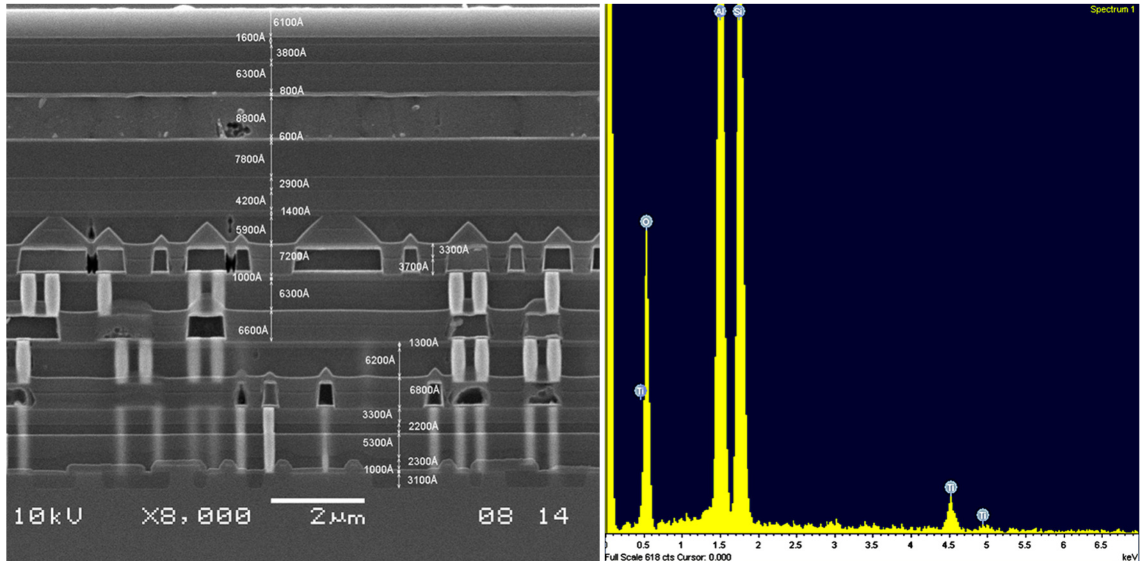


Figure 3.2: Left: Detailed cross-section of NXP P5CD080 V0B chip with measurements of layers given in Angstrom units (1 Å = 0.1 nm). Right: Energy-dispersive X-ray spectroscopy (EDX) of a top layer of NXP P5CD080 V0B chip. (Source: author's work.)

deprocessing procedure can be prepared according to the composition and thickness of each layer.

### 3.3.2 Chemical Deprocessing

For the complete process, it is necessary to have at least two specimens of the chip. At least one specimen is needed for the cross-section analysis and the second one for the main deprocessing. The second chip can be deprocessed according to the information gained from the first step. After removal of each layer, we have to acquire images of the layer with an appropriate microscope before we proceed to remove the next one. However, we strongly recommend preparing more samples than just two. Performing such analysis with only the two samples is not very common and not likely to be successful in real-life. The recommendation is to proceed with ten or more samples, to be able to prepare each sample to a different level of deprocessing—one with preserved passivation, one with removed passivation, one with a removed first metal layer, etc. [51]

#### Deprocessing of Common Layers

With the outcome of the cross-section analysis, an exact sequence of steps can be prepared in order to get to the coveted deprocessed chip. The form of the whole decomposition process naturally depends on our objectives. Usually, pictures of bare transistors and interconnections are desired. [51]

**Passivation**

The very first layer on the top of the chips is mostly a passivation layer—a kind of protection against mechanical and electromagnetic effects of the environment. To remove this layer, it is recommended to use plasma etching, so-called dry etching. The whole process takes about 45 minutes with old plasma etcher TESLA 214 VT

that was available at our disposal. The actual plasma etching lasts only 4 minutes out of the mentioned time period. The rest of the time is devoted to preparing conditions necessary for performing this procedure.

**Conductive compounds**

Conductive layers that are made of aluminum compounds can be taken away by the application of *phosphoric acid etching mixture, PEWS 765-140-57-36*[2]. The recommended working temperature is 50 °C; the common time of the bath should be from 2 to 6 minutes, depending on the layer thickness. There exist also other commercial etchants designated for etching conductive layers, i.e., KMG Mix attaque phosphorique (mix of acetic acid, nitric acid and phosphoric acid), recommended working temperature is also around 50 °C. More of such commercial products can be found in the market.

**Dielectric compounds**

A special chemical mixture is also available for removing oxide compounds—insulating material. Precisely, the mixture consists of ammonium fluoride and hydrofluoric acid in ratio 7:1. The working temperature is 30 °C; the common time of the bath should be from 2 to 6 minutes.

**Deprocessing a chip down to silicon**

To deprocess a chip completely down to silicon, there exists one reliable method employing hydrofluoric acid (HF), 50% concentration. It is usually used at ambient temperature. The HF acid reacts with metals and also with oxides. This acid is not selective and is often used just for this purpose to remove all layers above the silicon. Duration of the etching depends on the chip composition and the amount of material above the silicon. [20]

## 3.4 Layers Scanning

The general possibilities of scanning are always the same. It is possible to use optical, confocal (CLSM—confocal laser scanning microscopy) or electron microscopes. All of the mentioned technologies are suitable for scanning of the chip layers. However, optical technology has reached its limitations, especially with regard to the contemporary technological nodes. The most advanced optical microscope can provide sufficient magnification for structures up to 0.25 $\mu$m [76], [77].

It is nothing extraordinary that the combination of high magnification and the size of the chip requires multiple image tiles of each layer. The images have to be acquired one by one, in the best case automatically by special control software. After that, stitching of the tiles has to take place to get a complex overview—i.e., chip used in e-documents contained more than 1.6 billion pixels after the stitching process.

### 3.4.1 Processed Chips

The information stated in this chapter was verified practically on various simple RFID tags and on smartcard chips, namely MIFARE Ultralight C, MIFARE Classic 1 kB, MIFARE DESfire EV1 and NXP P5CD080 (SmartMX family). The last mentioned is described in detail in Chapter 4. After investigation of the chips, we realized that the MIFARE

[2] http://www51.honeywell.com/sm/em/common/documents/2.6_europe_msds_p_8.pdf

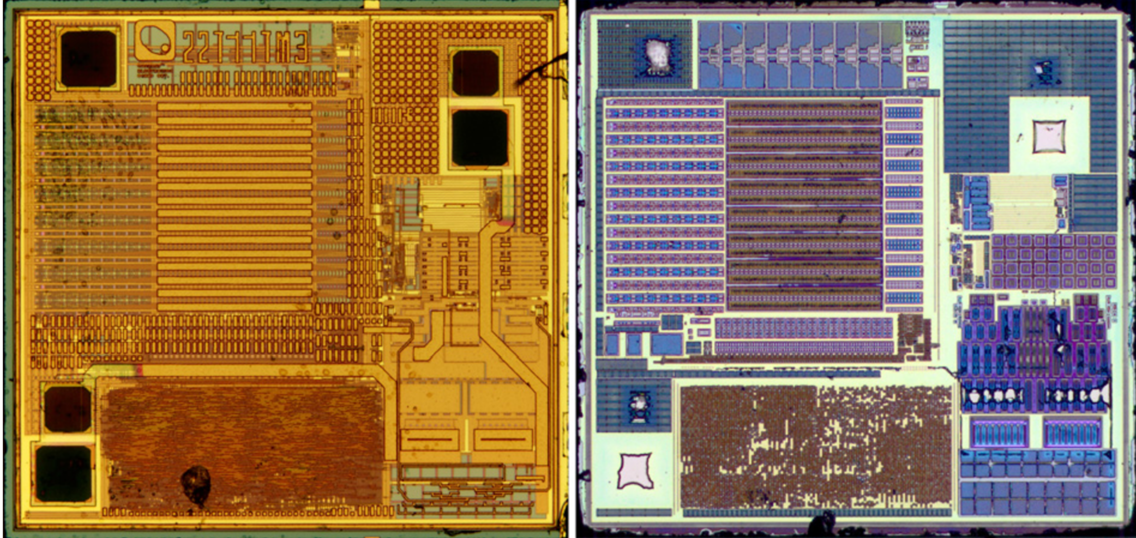

Figure 3.3: Two images of MIFARE Classic 1 kB. Left: The decapsulated chip without any application of decomposition. Right: The same chip after five steps of deprocessing. (Source: author's work.)

Classic samples were not original, but very popular clones produced by Shanghai Quanray Electronics Co., Ltd. The chips were labeled as QR2217.

Fig. 3.3 depicts differences between the decapsulated MIFARE Classic 1 kB with a preserved passivation layer (see the left part of the figure) and the same specimen after five steps of the decomposition process (see the right part of the figure)—all phases of MIFARE Classic deprocessing, including transistor field detail, can be seen in the thesis.

## 3.5 Analysis of The Images

The analysis process depends on the form of image data—separate tiles scanned with/without overlapping, a complete image of each chip layer, etc. Demonstration of such analysis process can be found in Chapter 4.

The software available publicly is usually limited to some kind of technology or technological node, i.e., rompar for parsing masked ROMs[3]; or not maintained properly, e.g., Degate[4], pr0nsweeper[5]. Although Degate tries to be a complex software kit accompanying the researcher up to the scheme reconstruction, it is usable rather for smaller chips with a lot of manual work needed and a lot of patience with its instability.

On the other side, there are commercial software packages that are not publicly available. There exist only presentations and marketing materials promoting the quality of these products—i.e., ChipJuice[6]. Chipworks Inc., a company based in the US (operating web TechInsights.com[7] with analyses of various products), represents one of the biggest players on the market. [77], [76], [47]

[3] https://github.com/ApertureLabsLtd/rompar

[4] https://degate.org

[5] https://github.com/JohnDMcMaster/pr0ntools/tree/master/capture/cf

[6] https://www.texplained.com/about-us/chipjuice-software/

[7] https://techinsights.com

# Chapter 4

# Analysis of The Czech Biometric Passport Chip

In this chapter, we will present results of low-cost physical analysis of the chips used in the Czech biometric passport implementation. These chips were obtained from STATE PRINTING WORKS OF SECURITIES, state enterprise (STÁTNÍ TISKÁRNA CENIN, státní podnik[1]), encapsulated in plastic cards, the same as used in real passports implementation. We had to pass through all the steps beginning with the extraction of the chips from the plastic cards and ending with image processing and data analysis.

## 4.1 Extraction and Decapsulation

The plastic cards used for this particular biometric passport revision are produced in compliance with the recommendations of ICAO (International Civil Aviation Organization) [37], [36] issued in 2008 and 2006. Although there are more recent editions [40], [38], [39] of the documents (these are used in the very recent implementation), we intentionally mentioned the ones that were used as the foundation for the samples that we received.

Extraction from the plastic cards was performed as described in Chapter 3.1. We encountered no extraordinary issues when carrying out this task, which is why it was described so briefly in this chapter.

We approached the decapsulation of these chips experimentally, based on our previous experience with other RFID chips extracted from smartcards. Moreover, we had enough samples of the chips and we were not aiming to preserve the wire bonds. Thus, we decided to go for the simplest method.

We used sulphuric acid ($H_2SO_4$, 96% concentration), heating it inside the fume cupboard to 278 °C. We inspected the degree of decapsulation every minute. It turned out that the compound was very resilient. During the process we had to use 3 separate beakers with the acid bath, because of contamination of the acid with the molding compound. After we were satisfied with the cleanliness of the chip's surface, we rinsed it in an acetone bath and with demineralized water afterwards. The quality was periodically checked with an optical microscope. Finally, we used ultrasonic cleaner to clean the chip. The whole process took 15 minutes, 12 minutes out of the whole process length was the duration of acid bath. The process was verified and confirmed with a second specimen. After the process verification, we successfully decapsulated the other 12 specimens in the same manner.

[1] https://stc.cz/en/

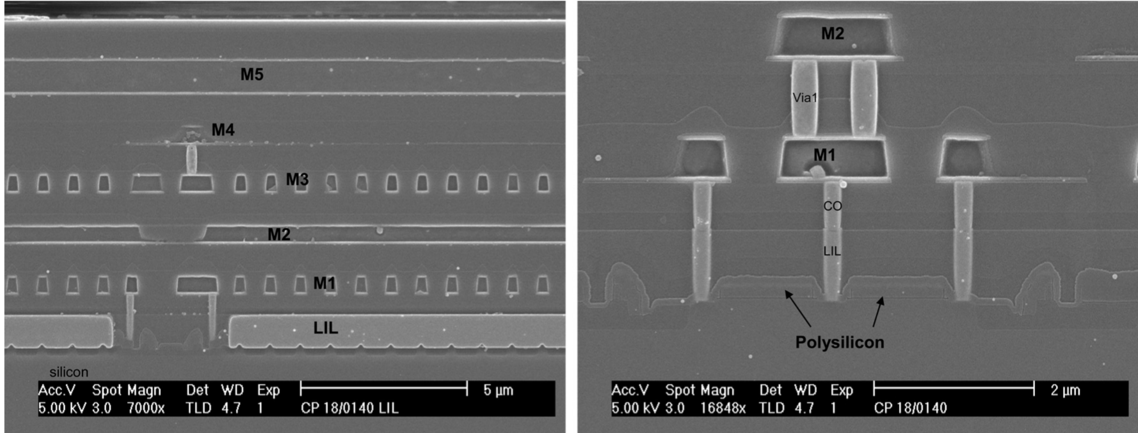


Figure 4.1: Cross-section of the NXP P5CD080 V0B chip. Left: Complete chip structure. Right: Detailed view displaying part of the chip from the silicon level to the M2 layer, also depicting details of the LIL layer and Vias. (Source: author's work.)

## 4.2 Deprocessing

The next step, after obtaining the chips from plastic cards and removing their packages, was to deprocess the samples into separate layers. Because of the size of the die (2.76×2.76 mm.) and because of the expected complexity (due to technological node 0.14 $\mu$m), we decided to go for the cross-section analysis first.

### 4.2.1 Cross-Section Analysis

The cross-section (see Fig. 4.1) was prepared according to our recommendations given in Chapter 3.3.1. The cross-sectioned sample was glued to a glass pad for easier manipulation. The prepared specimen was immediately scanned with an electron microscope in order to provide more details about the layer count and composition. 5 standard metal layers were identified, plus one special layer called LIL (Local Interconnect Level) what was directly above the polysilicon layer. This layer enables extra interconnections among polysilicon structures and also with the M1 layer. In other words, it allows for more connections among the transistors. The metal layers are made of aluminum (Al). LIL layer is made of tungsten (also called wolfram, W), the same as contacts and vias. The detailed structure of the chip including layers' composition and thickness is presented in doctoral thesis.

### 4.2.2 Removing Layers

When we had cross-section analysis done, which gave us information about the chip composition, we advanced to chip deprocessing.

First, we deprocessed one sample completely down to silicon through the use of hydrofluoric acid (HF, 50% concentration, ambient temperature, 40 minutes of etching), which reacts with metals and oxides as well.

Then we continued with one-by-one layer removal performed on a different specimen. The first step was to remove the top passivation ($SiO_2$) with a dry etching technique. Then we continued with the removal of the barrier right above M5 layer (TiN). Dry etching with the ultrahigh frequency (UHF, 2450 MHz) option turned on was used for this task.

The UHF allows for high density plasma generation. After the first barrier, we had to remove the M5 layer. Commercial etchant *Mix attaque phosphorique* from company KMG at temperature 45 °C was successfully used for this purpose. As it is known from the cross-section analysis, another barrier layer follows M5. However, we could no longer use the UHF option with the plasma etcher—it was out of operation shortly after the first barrier removal. The only available option was to use polishing to get rid of the barriers. We had Buehler Ecomet grinder-polisher at our disposal. Unfortunately, without special planar-oriented features. The polishing method was not performed successfully, just because of our inability to maintain planarity across the whole chip surface. Without the prospect of getting the UHF plasma etching fixed within a reasonable time and with problems during polishing attempts, we were unable to acceptably remove the barrier under M5. The UHF plasma etching would likely be the only reliable method available to us.

It has to be concluded that a fully operational laboratory is an inevitable precondition for the successful performance of complete deprocessing such (or more advanced) chips. The final results of deprocessing for the scope of this doctoral thesis are the three layers available for further scanning—the top-level, M5 and silicon layers.

## 4.3 Image Scanning

Although it was not possible to get all layers deprocessed, we were able to scan at least the top-level and the silicon layers. For the main scanning, we were allowed to use TESCAN MIRA3 SEM in our partner's laboratory, TESCAN Brno s.r.o.

For achieving a reasonable scanning speed, we decided to go for a 768×768 resolution of each tile with a 4152× magnification and overlapping between tiles set to 10%. These settings resulted in 3422 tiles, 59 rows×58 columns. The scanning duration of this particular setup was 15 hours and 12 minutes. The overhead with preparation of the sample and searching for the best setup for the scanning took almost two hours. We did not use the built-in stitching software found within the MIRA3 system in order to avoid processing errors that may occur with stitching. Such an error would cause the need for re-scanning the sample.

Side by side the transistor layer scanning, we manually scanned the top surface of the chip as well. For this overview scanning, our local optical microscope, Olympus BX61, was used with the employment of a 10× objective lens. This setup resulted in a 3×3 matrix of tiles with about 60% overlapping. Although the chip's surface was not clean enough, it provided sufficient quality for the needed overview of the surface and position of bond pads. Results of scanning can be observed in the following section.

## 4.4 Image Stitching

We performed series of experiments with the following software tools that are publicly available—Microsoft Image Composite Editor 2.0[2]; ImageJ (Image Processing and Analysis in Java)[3]; MIST (Microscopy Image Stitching Tool)[4]. Details of the experiments including computation duration and quality of results evaluation are presented in the doctoral thesis.

[2] https://www.microsoft.com/en-us/research/product/computational-photography-applications/image-composite-editor/

[3] https://imagej.net/

[4] https://pages.nist.gov/MIST/

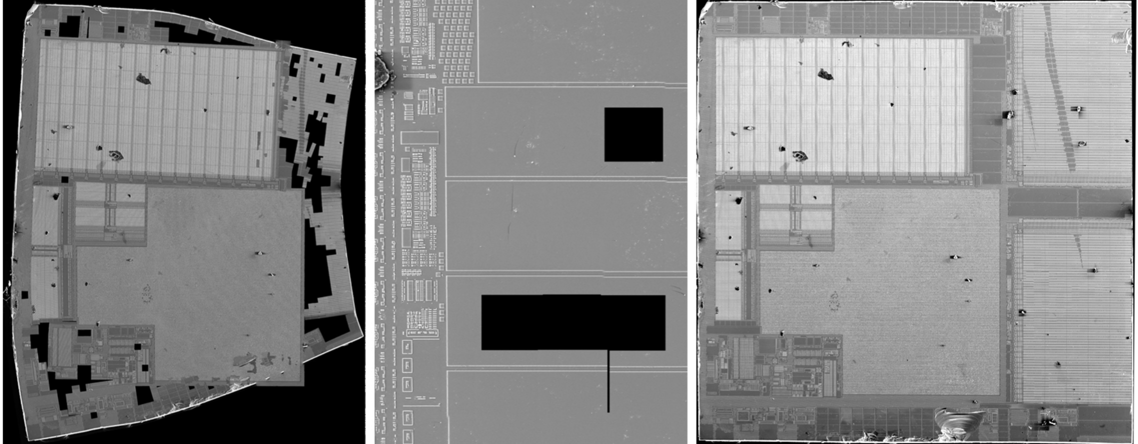

Figure 4.2: Left: Faulty result of stitching performed with Microsoft ICE 2.0. Middle: Missing tiles after a stitching procedure performed with FIJI. Right: Silicon-level layer stitched with FIJI Grid/Collection stitching plugin, overlapping calculation switched on and sub-pixel precision—3422 tiles in total. (Source: author's work.)

As a summary, we can recommend the MIST plugin for fast previews and for manual visual analysis of the chip. However, for software processing of the image data, we strongly recommend using Grid/Collection stitching with overlapping calculation switched on and sub-pixel precision. We do not recommend using Microsoft ICE 2.0 (see Fig. 4.2).

Finally, there was also the need to stitch the manually taken tiles displaying the top-level layer of the chip. We did this manually with Adobe Photoshop, because there were only 9 tiles in the whole matrix, each tile had a resolution of 4140×3096. The manual stitching was chosen because of different color tone of the images. As such, we could control the settings of each individual tile to fit perfectly to the overall image, see Fig. 4.2. The final image resolution was 6400×6400 pixels.

As a result of this portion of the work, we have several versions of the big image displaying the silicon layer of the chip. We also have the single stitched image depicting the top layer of the chip (for both results see Fig. 4.2 and Fig. 4.3).

## 4.5 Analysis

We first had to determine the identity of the chip itself. A few labels were discovered in the chips surface images, mark "T035B" together with "PHILIPS" copyright and another mark, "017", in top left corner of the chip, right between the bond pads. This gave us the first hint as to what to look for. With the help of Google, we found out that the chip was NXP P5CD080 V0B. Based on the chip identification, we were able to gather the chip's specifications. [57]

Regarding the physical security of the chip, there are several measures implemented to avoid or hinder physical attacks. According to the [57], there are protection mechanisms against possible security incidents—inherent information leakage; physical probing; physical manipulation; malfunction due to environmental stress; etc.

There are also several other measures implemented for ensuring the security of the data and functions provided by the chip—separate CPU modes with memory access control mechanisms, multi-application support, strict data separation, etc. For a complete list,

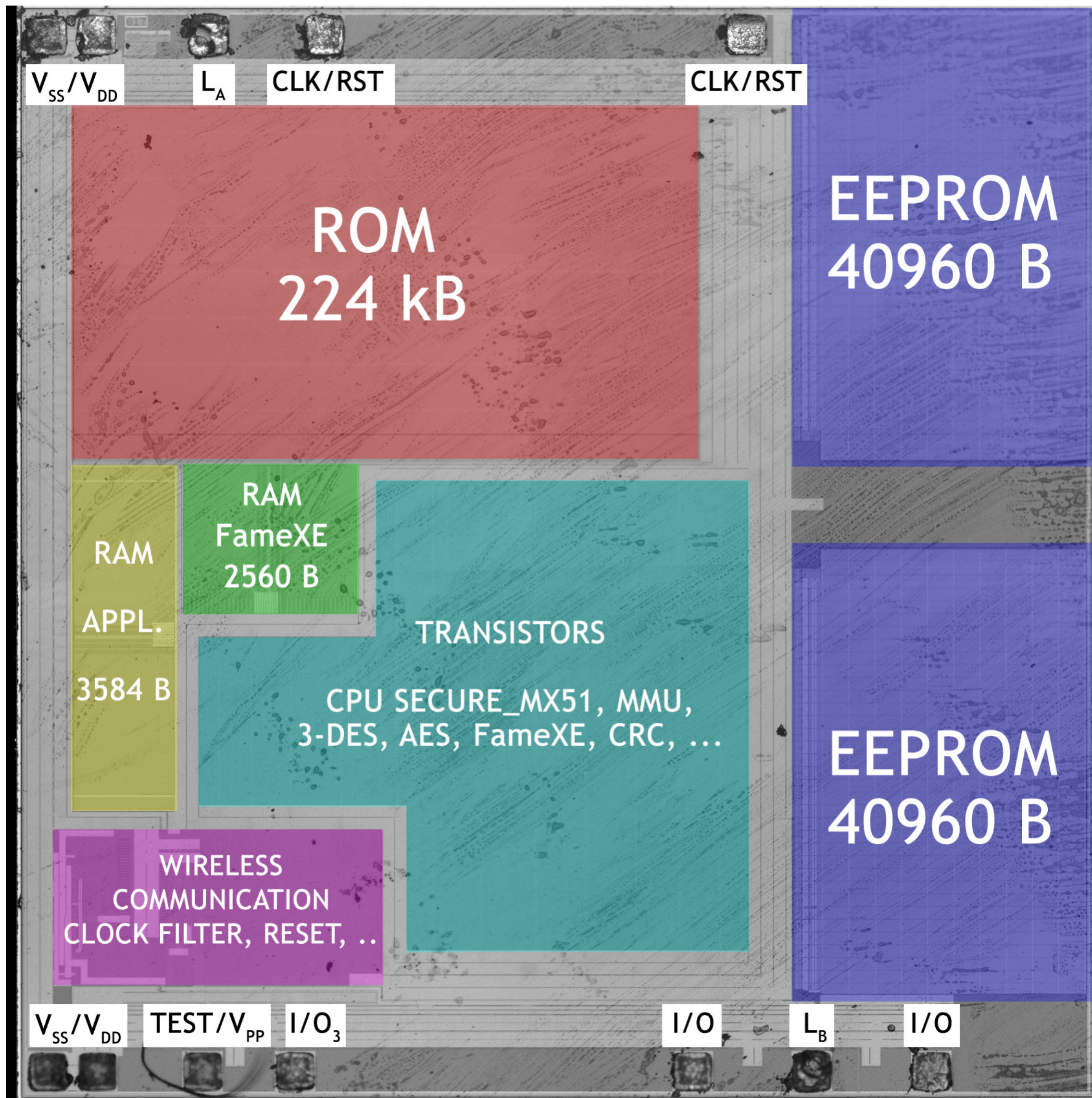


Figure 4.3: Segments of the chip NXP P5CD080 V0B (Source: author's work.)

please see the datasheet [57]. The chip is also compliant with Smartcard IC Platform Protection Profile [57], [4].

Out of the obtained information, one security-related concern has presented itself. Behind the copyright symbol on the chip's surface, there is the year 2006; the datasheet, and also security reports from the year 2007. This means that in the Czech implementation of e-Passports, technologies older than 10 years are still in active use. Although this chip has not been used for production of new passports since the end of 2014, there are valid passports traveling around the world holding the examined chip.

### 4.5.1 Bond Pads Identification

First of all, we need to identify the bond pads and project them from the top layer to the silicon layer. We know that the chip supports two interfaces; contact (ISO 7816) and

contact-less (MIFARE and ISO 14443A). It can be read out from the datasheet [57] that we should observe the following contacts—$V_{DD}$, $V_{SS}$, CLK, RST, I/O1, I/O2, I/O3/SIGN, LA, LB/SIGNOUT.

The contact-less interface requires two pads for the antenna connection. These connections should be ideally on the opposite side of the chip, because of the bonding of the antenna—position of antenna pads can be found in the datasheet [57]. So, we tried to find two pads with similar structures around them on both sides of the chip. Surprisingly, there were just two pads like this. Moreover, when trying to track connection visible from the top layer, both lead to the area of the chip, where we expected communication interface—non-transistor structures with present capacitors. Later, when we identified I/O pads, we estimated also that from the locality perspective, the LB contact could be located somewhere near to the I/O pads.

The rest of the pads belong to the contact interface. Altogether, we identified 12 bond pads on the chip's surface (see Fig. 4.3). What is interesting is that the two top-left pads and two bottom-left pads are very close to each other, whereas the rest of the bond pads maintain a certain mutual distance. The two pairs of close bond pads could be suitable for power transmission ($V_{DD}$, $V_{SS}$) not to overload a single pad with the power needed for the full-power performance of the contact interface. When observing the top-level layer, traces leading from these two couples of pads go around the whole chip. This is also a sign of power routes because these are usually in the top metal layers routed all around the chip.

Based on similarities of the surrounding elements, we experimentally determined the three I/O pads. From the remaining bond pads, two were conspicuously similar in the top; thus both were marked as CLK/RST (we do not know which one is which). Then, there is still one pad remaining, although all pads officially stated in datasheet have been marked. We would expect this pad to be devoted to VPP (according to ISO 7816) or to TEST I/O. The producers reserve very often one or more pads just for testing purposes.

### 4.5.2 Chip Segments Identification

The next step leading to understanding what is under the hood means identifying segments of the chip. Then it is possible to make a decision regarding how to further examine the parts in order to gain more information about the IC.

It was clear at first sight, where the logic can be found. The transistor structures are obvious. Then, there are few sectors that evince repeated, regular patterns. These sectors are very likely the memory parts. Based on the size of each type of memory read out from the datasheet [57], it is possible to distinguish among them—for illustration, see Fig. 4.4.

The ROM memory should contain 224 kB. We were able to identify 224 lines in the presumptive ROM sector, each line holding 1024 bytes. Originally, we thought the bright particles scattered around the ROM structures could reveal the content of the ROM. After deeper investigation, we realized that these particles have to be considered remainders of structures from the layer above, basically telling us nothing about the actual content.

The RAM memory is expected to be as close as possible to the CPU. It was stated in the datasheet [57] that only a certain amount of RAM is accessible for the FameXE co-processor. This RAM could be part of a single block of cells; however, we identified in the image, that this part of RAM is also physically separated. This hypothesis about memory block assignment was confirmed after the precise counting of cells in each block of RAM. We clearly identified 1792 bytes in each of the two rightmost blocks of RAM, that corresponds to the application RAM size—3584 bytes. Consequently, the rest of the RAM

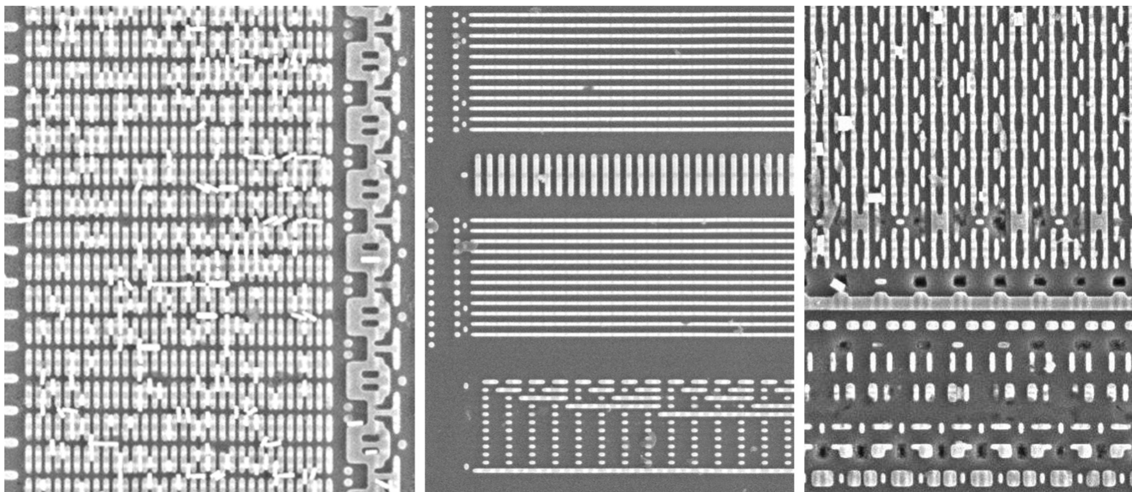

Figure 4.4: Memory elements present in the NXP P5CD080 V0B chip layout. Left: ROM memory. Middle: EEPROM memory. Note the address bits at the bottom. Right: RAM memory. (Source: author's work.)

cells must have been the part accessible for FameXE. It was again confirmed by counting of the cells in the blocks—4×640 bytes were perfectly fitting 2560 bytes of RAM for FameXE.

After determining ROM and RAM, we wanted to confirm EEPROM in the same way, with the counting of the cells. EEPROM is divided into two halves placed on the right, each half containing 40960 bytes. There were 32 segments found in a vertical direction and 320 in a horizontal direction. That would mean 4 bytes per each of the 32 vertical segments—when looking at the vertical segment; it is divided into four similar parts.

The chip was segmented into parts—memory sectors and transistors. Just the last part was not assigned, the violet segment in the bottom left part of the chip displayed in Fig. 4.3. When zooming in to this part, elements resembling capacitors are present in here. Thus, we deduced that this must be the segment responsible for wireless communication (the wireless interface also provides power for the chip). Another hint supporting this hypothesis is the fact that antenna inputs LA, LB both lead to this part.

We looked into the transistor filed and checked whether any pattern, segmentation or anything else helping the analysis could be read out just with the availability of the silicon layer. However, the field seems to be continuous, and so for gaining more information about the chip, it is necessary to scan and align images displaying the higher layers.

# Chapter 5

# Chip Security Improvements

Recently, we have seen several papers covering especially a split manufacturing process that allows for the construction of reliable and trustworthy devices, at least from the producers' perspective [85], [41], [26], [25], [32], [69]. A very favorite technique providing protection of the chips emerging in recent years is logic locking [28], [68], [90], [87], [45], [65]. On the other hand, there are attacks aiming at the logic locking and camouflaging techniques—SAT attacks (based on boolean satisfiability) [86], [52], [42], [15], [71], [90], [89], [88], SPS attacks (Signal Probability Skew) [90], [89], [88], CP attacks (Circuit Partitioning) [90], [88], SMT attacks (Satisfiability Modulo Theory) [5], etc.

## 5.1 Reverse Engineering Countermeasures

For a long time, reverse engineering attacks had been neglected through deceptive feelings of the inherent security of microchips. With up-to-date knowledge, we know that adversaries can be very well equipped, as some of the attacks might be, for example, of national interest and thus have strong financial backing and a desire for results [62]. Moreover, there are not only cutting-edge chips available on the market, there are many chips produced with older technological nodes, due to financial reasons or even overhauled outdated specimens secretly used in places where nobody expects them [34], [35], [33], [59], [61], [64], [81], [83], [92], [93]. This allows for many amateur adversaries (e.g., up to Level 2, as described in [55], or up to Level MODL, according to [1]) to perform a cheap, partial reverse-engineering process with success.

## 5.2 Complex Integration and Camouflaging

2.5D and 3D integration is a substantial contribution to a possible security increase in IC fabrication. These chip composition techniques are emerging especially in relation to split fabrication processes that should assure the genuineness of IC production in offshore foundries [85], [41], [26], [25], [32], [69]. Solving supply chain issues is not the aim of this work, however, so we will refer readers to the above-mentioned papers for more information about that subject.

Our intention with the employment of 3D integration is to hinder delayering and the consequent analysis of the inspected specimen. Delayering is already complicated with current state-of-the-art 2D integration—e.g., avoiding unintended cross planar grinding or underetching is tough enough with the recent nodes.

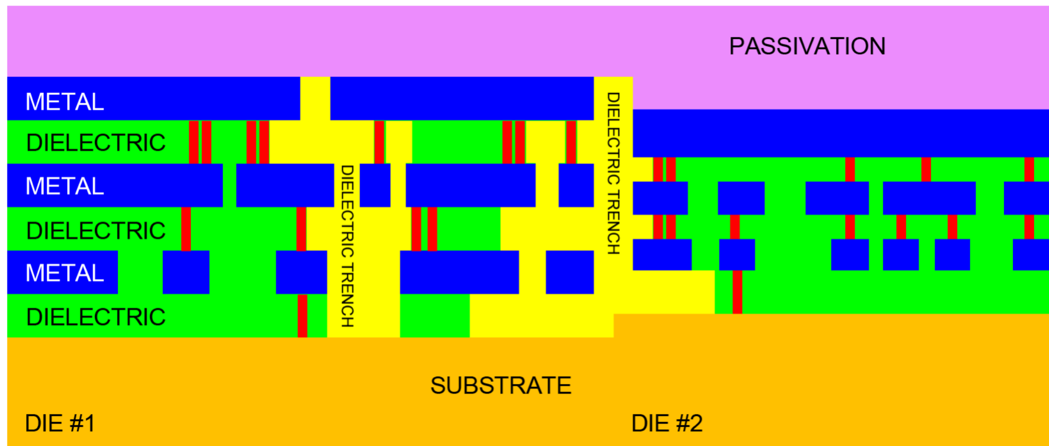


Figure 5.1: Illustration of heterogeneous integration of a chip. (Source: author's work.)

Removing all layers of a 2D design down to the silicon is currently still feasible. We also succeeded with the use of chemical etching on biometric passport chips revealing the silicon layer. Nevertheless, transistors express only a part of the IC blueprint, the same importance lies in the interconnections that add semantics to the whole circuit. Thus, obtaining images of transistors is, in a vast majority of cases, not sufficient. Therefore, adversaries have to concentrate on extracting all of the needed information—transistors and interconnections. And this can be aggravated through the use of 3D integration. Let us name several possible measures on how to make reverse engineering more challenging.

### 5.2.1 Heterogeneous Integration

Heterogeneous integration of dies made with different technologies will certainly make planarization issues much deeper. It would be ideal to utilize a combination of materials at the same planar levels that have very different grinding resistivity. Grinding would require equipment that allows for perfect control over the grinding process (in order to keep grinding absolutely uniform across the whole heterogeneous plane). Wet or plasmatic etching will be even more difficult, especially when the layers will be wisely combined in order to ensure underetching or even direct damage to the adjacent layers. In Fig. 5.1, see the dielectric layer that is a combination of two different materials with a dissimilar resistance to chemicals—the green parts endure for much longer before dissolving, which enables yellow dielectric trenches to initiate underetching. The passivation layer can be of a different thickness across the die to make the decomposition harder from the very beginning.

### 5.2.2 Cell Camouflaging

Cell camouflaging or circuit obfuscation are known techniques described in several research papers [7], [18], [30], [63], [70], [82], [80], [62], [69], [13]. It is known that this technique is expensive because of the aerial demands, so it is impossible to camouflage the whole IC. Furthermore, the security impact can be of a much lower extent than expected during design time due to existing attack scenarios [41], [70], [63], [30], [80]. Furthermore, it is possible to observe obfuscated cells through a series of cross-section slices with a properly set milling

step (step by step cross-section demonstration is presented in the doctoral thesis). With this approach, it can be determined which contacts are really connected and which are just fake. [62], [6], [21], [58].

Let us introduce the possibility to disable this cross-sectional analysis of camouflaged cells with the employment of inductive or capacitive contact-less connections, where some of the contacts in the camouflaged cell can be fake without showing any visual difference. This potential enhancement also has its drawbacks, e.g., spatial and power requirements, heat dissipation, and potential side-channel attack support. Camouflaged cells are spacious even with the physical contacts, so there is not much of a difference. With wise design, we might get to the same spatial needs and potentially a similar camouflage effect. The fake contacts will then be visually indistinguishable from the real ones. It is clear that the use of this type of obfuscation in a single die has to be very limited due to its drawbacks [23], [27], [53], [43].

### 5.2.3 3D Integration with Dummy Dies

There are many unused or recycled old dies available on the market (which are vastly used by fraudster foundries in fallaciously new integrations [34], [35], [33], [59], [61], [64], [81], [83], [92], [93]). These can be wisely used for increasing the complexity of 3D integrations. Although this artificial complexity bloat will not prevent adversaries from performing decomposition and analysis, the intricacy of the integration can be risen. The time consumed for the determination of the dummy part may help discourage adversaries. We propose using dies with diverse technological nodes for 3D integration. Each node requires a distinct approach for delayering and analysis. This approach will make reverse engineering more unfriendly.

## 5.3 Active Tamper Detection

The chip is detached from its package and the power source. The latter does not have to be necessarily the truth in the very near future, due to discoveries and the successful development of micro batteries suitable for direct integration into ICs [10], [46], [56]. Due to the growing complexity of chips, we do not expect batteries to be capable of powering the whole chip for an exceptionally long time. Nevertheless, if we focus strictly on keeping the protective functionality alive only, this might result in a decent duration for active tamper detection endurance, even without an external power source. Moreover, recent endeavors in the field of energy generation can lead us to mechanisms that are capable of refilling the integrated battery and hence allow for the exceptional endurance of active tamper detection. Let us name VEH (Vibration Energy Harvest) based on MEMS (Micro-Electro-Mechanical Systems) [3], [19], [24], thermoelectric generation based on parasitic load of the device [29], [24] and photovoltaic solar power generation [24], [11], [66] which can be sensing the package decapsulation at the same time.

### 5.3.1 Active Tamper Detection with Active Memory Protection

An active tamper detection shield should consist of several layers aimed at the possible ways of intrusion. The partial or complete decapsulation is one of the first steps when targeting chips with invasive investigation. After opening the package, there should be natural light entering and interacting with the chip's surface. Therefore, the very first detector should

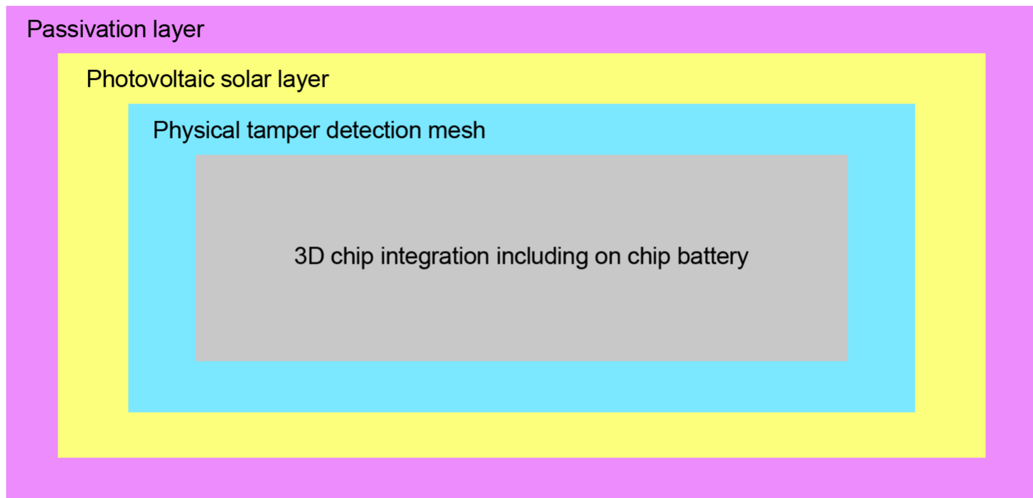


Figure 5.2: Simplified composition of a chip with active tamper detection. (Source: author's work.)

be a light-sensing layer on the top of the chip. Ideally, it should be covering the chip's entire surface to ensure that even partial openings trigger the alarm.

The second anti-tamper layer should be a fine-pitch sensing mesh against attempts of penetration into the chip. Even small-sized FIB editing has to be detectable by this layer in order to not allow for any modifications that could possibly lead to the restriction of active shield functionality, memory bus exposure, etc. This layer should be actively powered by the integrated battery to regularly check the integrity of the mesh. Due to the fact that reverse engineering is not a fast process, the check can be set to be run after a certain period. This interval has to be designed with respect to the power demands of the whole active shield circuit as well as the capacity of the integrated battery. It can be expected that the parameters of the batteries will significantly improve over the next few years. Then this active shield use case will be supported even more.

In Fig. 5.2, we provide a simplified view of a chip's structure with respect to the proposed active protection. As there are many attacks led from the "backside" of a chip, we recommend using 3D integration with a back-to-back connection to have a 3D chip with only the frontal part facing all the edges of the packaging. Passivation, photovoltaic sensing, and physical tamper detection layers are used all throughout the chip's structure. A battery is expected to be integrated inside the 3D integration.

As soon as the outer package is (partially) removed, the photovoltaic solar layer produces energy. This should be the signal to immediately remove memory content. Memory content removal should be a battery-powered action. In cases when the attackers would be able to somehow disable the photovoltaic sensing layer and thus would be able to avoid immediate memory erasure, their next step will be layer-by-layer removal or FIB editing. Once the physical layer tamper detection mesh is touched, the same memory-erase signal will be triggered.

Memory modules should have low energy demand in order to enable this protection scenario with battery-powered memory erasure. When the battery reaches its critical low level of charge (the minimum charge needed for memory erasure), it should automatically

erase the memory content in order to devalue the chip. This low-charge status can occur when the battery is not recharged or in the event of malfunction.

We can more or less rely on battery re-charging mechanisms (TEG, VEH, Photovoltaic, etc.), and thus prolong active shield durability for various scenarios.

### 5.3.2 FPGA Employment with Active Bitstream Protection

Protecting a chip against reverse engineering by implementing its key parts inside a fully integrated FPGA circuit is not a novel idea in principle. The concept is based on the fundamental presumption that FPGA is composed of visually similar cells that change their behavior according to the configuration loaded upon power up. However, there are known attacks against such implementations [62], [31], [54] focusing on the reconstruction of the FPGA configuration bitstream, thus essentially gaining a netlist of the circuit.

To avoid these attacks, we have to protect the main memory that holds the configuration information and buses from micro probing, FIB editing, etc. Our proposal is to physically protect the chip in the same way as described in the previous chapter with the active tamper detection shield.

## 5.4 Active Defense Against Microprobing

Targets in a microprobing attack are mostly internal buses or signals that are not freely accessible via standard contact pads. Our aim is to protect the chips from tampering attempts, intrusion, or the analysis of its physical structure that reveals its internal arrangement. In Chapter 5.3, we proposed the employment of active tamper detection in order to detect the undesirable manipulation with a chip as well as measures protecting the data processed inside the chip from being disclosed.

## 5.5 Disabling Backside Observations

Backside imaging can be considered an easy method of almost directly accessing the transistor layer with further scanning possibilities realized by photon-emission microscopy, laser voltage probing, laser voltage imaging, IR imaging, thermal emission imaging, etc. [9], [14], [72], [75], [79]

The typical first step towards such a backside observation is to decapsulate the back side of a chip. Subsequently, there might be some obstacles in the form of various pads placed below the silicon part of the chip. The silicon substrate has to be thinned down according to the chosen scanning technique (100 $\mu$m–50 nm) [9], [14], [72], [75], [79].

Our proposal for disabling the techniques using backside access is to employ 3D integration, as mentioned in Chapter 5.2, so that there is no real backside of the chip (see Figure 5.2). One can object that one of the chips in the 3D layout can be removed and thus the backside of the other chip might be exposed. Nevertheless, the removal of one of the chips from the 3D layout makes the active backside observations of a specimen under operation practically impossible.

A further proposal in regard to designing security-oriented 3D chips is that these should work only when correctly interconnected, even when using dummy dies. Through silicon vias (TSV) are very likely to be in place for interconnecting the particular chips. These vias can ensure the integrity of the whole setup.

## 5.6 Active Defense Against X-Ray

Lately, X-rays have become a serious technology used in the observation of advanced chips [58], [21], [22]. Protecting a chip against reverse engineering by implementing its key parts inside a fully integrated FPGA circuit was already presented in Chapter 5.3.2. In fact, X-ray exploration is basically a kind of non-invasive reverse engineering. Thus, similar measures, as used for anti-RE, can be taken in order to increase the chips security.

Protection against X-rays or ionizing radiation has to also employ a protection mechanism against these non-invasive observation techniques. Either radiation detectors have to be placed inside the chip's structure [60], [48]; according to recent research in physical chemistry, it is also possible to turn X-ray radiation directly into electricity through the use of nanomaterial. This might be used as a sensing technique for triggering proposed memory erasure procedures in a similar way as in 5.3.

## 5.7 Passive Defense Against X-Rays

For hindering radiation-based observation techniques, it is possible to use the methods presented in the section devoted to reverse engineering, such as cell camouflaging, inductive or capacitive contact-less connections, key functionality implemented in FPGA, visually unreadable memory cells, increasing complexity with 3D integration, increasing complexity with dummy dies. Among others, it is possible to use materials that are used for radiation hardening in general, especially in the space industry; for example, borophosphosilicate glass [91]. The chip package can be constructed from materials that will make X-ray scanning difficult (however, this research field is not covered in this thesis). Therefore, it would be needed to decapsulate the chip first.

# Chapter 6

# Software tools for Microscopic Analysis

Finally, after all the steps needed for obtaining the image data of the chips, experiments with data processing can be carried out. We will mainly focus on the transistor field, as there are elements that can be recognized and grouped. We would like to compare several approaches and see the results in the form of computation demands, quality of gained output, and also further applicability of the results. We cannot fully reconstruct the cells without interconnection layers; however, we can focus on the elements recognition to lay down the cornerstone for further work.

First of all, because of limited amount of data sets available to us, we have to rule out any form of learning algorithm. These approaches need big data sets for training and separate data sets for evaluation. Moreover, various forms of learning approaches would be very probably the first direction to go for most of the researchers. That is the second strong argument for us to test approaches without the presence of the learning.

Our aim is thus to detect similar elements across the chip, or at least in the transistor field. The further step would be to group these together into bigger similar blocks. This would help the researcher in location of particular logic cells. We would like to evaluate various approaches to this task, from simple template matching, through exploitation of image descriptors to shape or contour detection.

## 6.1 Setup

In order to achieve sustainable, maintainable, and extendable work, we will use very popular Python (Python 3.7.3) programming language with OpenCV library (3.4.2.16—used fro SIFT, SURF, ORB calculation; 4.1.0.25—used for template matching and shape detection), a standard in image processing. We will test the solution on platforms Microsoft Windows (Intel Core i5-4690 with integrated GPU, 32GB DDR3 RAM, 160 GB SSD SATA drive) and Linux (Intel Core i5-4690 with integrated GPU, 16GB DDR3 RAM, 250 GB SSD SATA drive) in order to achieve portability.

Using the full image for development and testing purposes would be too impractical (computationally demanding and lengthy). For the purpose of faster computations and comparisons among various settings, we created a cut-out (1150×966) image from the transistor field, see Fig. 6.1. This model image was used across the examined methods described in the following sections.

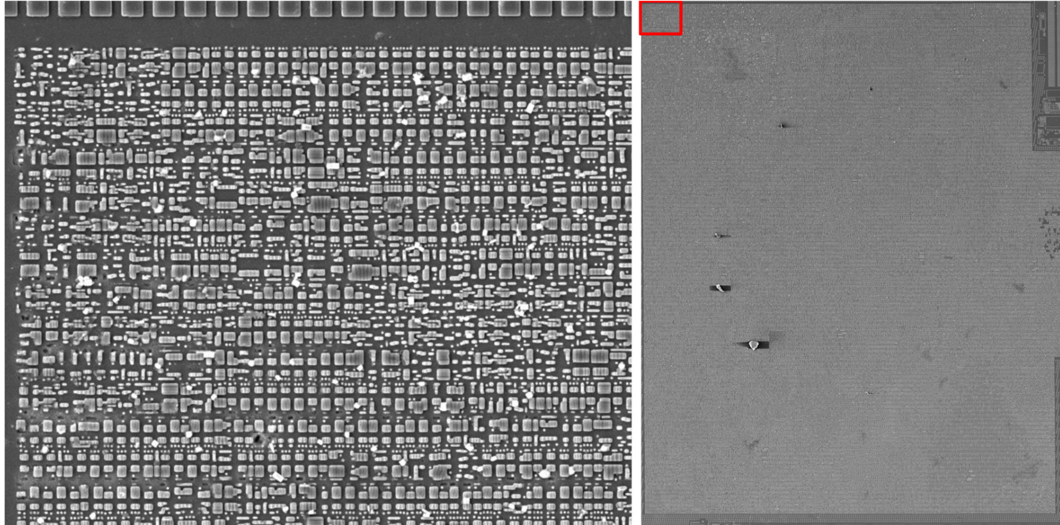

Figure 6.1: Model images used for experiments. Left: Transistor field cut-out taken from chip NXP P5CD080 V0B. This image was used for most of the development and tests. Right: Image with almost the whole transistor filed of the chip NXP P5CD080 V0B. This image was used for verification of developed methods and various measurements on bigger data. Note the red rectangle in top left corner; this highlight denotes exactly the part shown in the left part of this image. (Source: author's work.)

## 6.2 Template Matching

Template matching approach is relatively straightforward. We have to determine a template (a subset of an image in our case), and this template is matched against the selfsame image to find similarities. To find all possible similarities, we take the template window, place it at coordinates 0, 0 (x, y) and take the first template from the image. This template is compared against the whole image itself. Then we move the template window with a certain step to the right to the next position and repeat the comparison part. As soon as we move the template window to the end of the first line, we move it with the set vertical step to the next line and repeat the whole processing of a line. The whole image is scanned in this way.

There are three critical parameters to be tuned for each setup, influencing a number of matches and computation time—template size (including template shape—square vs. rectangle), template shift step, similarity threshold.

We performed several tests with template windows sizes 30×30, 40×40 and 50×50 (note, we always used square windows; the window size has to be determined according to the size of elements we want to pair). Each template size was run with template shift 10% (i.e., 5 pixels shift for 50-pixel wide window) and later with template shift 50% (i.e., 25 pixels shift for 50-pixel wide window). With each setup, we tested threshold settings from 0.75 to 1.0 with step 0.05. The detailed results are presented in the doctoral thesis. Our implementation was optimized in order to utilize all available CPU cores with Python multiprocessing `pool.map_async`.

After all, these computations can be sped up seriously by implementation with CUDA, as it is a perfectly suitable task for parallelization. The computation length can be one of the most significant drawbacks of this method. Running this kind of matching on the

reference cut-out image was acceptable from the computation length perspective (varying from half a minute to 37 minutes, based on settings of the particular calculation). RAM consumption is, in this case, negligible, around 200 MB. This might not seem too much, but when running the same computation on a bigger image displaying substantial part of transistor field of the chip (see the right part of Fig. 6.1), the computation duration with 50 pixel template width and 50% shift gets to circa 55-60 days. 12 GB RAM consumption is, in this case, totally irrelevant.

Applicability of results gained with the use of template matching is suitable for further manual analysis, where the researcher is supported with marked similar parts of the chip. We created a simple matches browser for better evaluation of template matching results. A similar application for evaluation of the results is used also in the following sections.

### 6.2.1 Template Matching Summary

Use of template matching approach is convenient especially for its simplicity, depending on the particular use-case, there are very few variables (size and shape of the template, template shift, similarity threshold and mode of matching) that can be easily tuned in order to get results suitable just for the use-case. On the other hand, the output is usable rather for support of manual research activities, as there is no other output than coordinates of the matched windows (missing semantics).

From the results presented in the thesis, we do not recommend using 10% template shift unless it is truly demanded for spotting very irregular elements. Increased computation demands simply do not payback. Subjectively, the matching results are of good quality, and similar parts are marked correctly. For each data set, it is necessary to find the correct template size and the threshold.

## 6.3 Feature Descriptors

The next idea in image processing or rather in similarities recognition was to use some kind of image descriptors and to investigate whether these can be suitable for cross-matching similarities within a single SEM image depicting microchip silicon layer.

First, we wanted to examine feature-descriptors Scale Invariant Feature Transform (SIFT), Speed up Robust Feature (SURF) and Oriented FAST and Rotated BRIEF (ORB, where FAST means Features from Accelerated Segment Test and BRIEF means Binary Robust Independent Elementary Features). These methods for features detection are known in image matching and computer vision and are also available in openCV library. [74], [2], [44], [12]

Our idea was to investigate particular key-points and descriptors that are ordinarily used for matching a template image against an another image containing the same object in it; usually in a different scene (these methods are invariant to various transformations). The matching in this standard use case is based on finding key-points in both of the images and trying to correlate them mutually. One could propose to follow a similar process as presented in template matching—taking one template after another from the original image and compare against the rest of the image. In such use case, the template matching could be used directly instead. Our aim was to investigate detected features (key-points and descriptors), within a single image and see whether there are any similarities among them. Especially among the ones located in elements that are visually similar.

Table 6.1: The total number of key-points in the testing image, and the number of key-points matched with another key-point. Tests were performed on the testing data described at the beginning of this chapter; the size of the testing image: 1150×966.

| | Total key-points detected | Key-points with at least 1 match with a different key-point |
|---|---|---|
| SIFT | 25200 | 7363 (max. vector distance 150) |
| SURF | 16407 | 4277 (max. vector distance 0,15) |

In the beginning, we ruled out ORB method. The only drawback that predetermines the ORB method for the original purpose of two images mutual matching is the number of key-points it selects. The ORB method chooses only N (500 in our case) key-points [44] that are the best for the image characterization, that is why it is so fast compared to the other methods. From a comparison of extracted key-points from the original image without preprocessing, the densest net of key-points is calculated by the SIFT method, followed by SURF calculation (for comparison, see Table 6.1).

The algorithms calculate a set of descriptors for each of the key-points. Instead of the standard comparison between images,we called the function in the way comparing the key-points against themselves. The maxDistance was determined experimentally, for SIFT calculations, the optimal value was around 150 and for SURF 0.15 (for more details see Table 6.1).

Initially, we played also with the classification of the key-points just based on their size and response with neglecting the descriptors. Based on the results, we do not recommend using this method as the first step of the classification. However, it provides useful information that might help in later stages of the classification for fine-tuning of the results gained from the descriptors matching stage. During these experiments, we investigated the influence of the angle of the key-points on the classification. The angle is always misleading and should be neglected.

Another attempt of classification was to use clustering on the key-points (based on their location) as the first step of the classification with neglecting the descriptors. We experimented with DBSCAN (Density-Based Spatial Clustering of Applications with Noise) and with K-Means clustering. This approach did not lead to any usable result, because the key-points net is too dense, and thus we got either too many or too little clusters.

Although we also experimented with FLANN based matcher (Fast Library for Approximate Nearest Neighbors), we stayed with the standard Brute-Force matcher with default settings at the end as we did not find any better settings of the FLANN matcher.

### 6.3.1 Feature Descriptors Summary

Subjectively, the best matching was performed with SIFT. What we liked about the descriptors was the fact that this method is capable of marking rotated elements. Moreover, it was able to cope with various artifacts and still match the point with a similar one. On the other hand, it is clear that this crude mutual matching is not absolutely sufficient as there are still many false positives and also many points are not matched at all. Nevertheless, it is clear that this approach is definitely worth further examination.

The disadvantage is basically the same as with the simple template matching method presented in the previous section—so far, we have just single points and highlighted areas without deeper semantics. On the other hand, computation length is incomparably shorter than with the template matching (especially when comparing against the 10% template shift).

## 6.4 Shape Matching

The last approach we wanted to examine in the scope of this thesis was to extract shapes of the objects out of the source image. OpenCV library provides several methods usable for this purpose. The first attempts of detecting shapes directly in the original testing image led to many imprecisely detected objects with variable shapes (also among visually similar objects) and objects with holes inside (area marked with another shape as object in object). Therefore, we experimented with image preprocessing in order to get the whole objects correctly marked. There were many trial and error attempts along the way. Let us present an approach that worked well at least with one of the testing data sets.

First, we calculated two thresholds of the input image:
`_, grey_img = cv2.threshold(img, 110, 255, cv2.THRESH_BINARY)`, and
`_, white_img = cv2.threshold(img, 220, 255, cv2.THRESH_BINARY)`. Then, we applied bitwise exclusive OR on the two thresholded images. This helped us to filter out artifacts present in the source image and thus separate the objects. Further, we searched for contours (with approximation mode `cv2.CHAIN_APPROX_TC89_L1`) in the XORed image. At this point, it was possible to perform the correct background separation. The background was flooded with the blue color because we needed to be able to distinguish among background (blue), object contours (black), and inner parts of objects (white). Finally, we could filter out the contours in order to have clean objects (white), and background (blue). The background was turned from blue to black to respect black and white mode standard.

Subsequently, we decided to apply the Watershed algorithm for the pre-processed image segmentation; into separate objects. This algorithm is available in the OpenCV library (`cv::watershed`). The result of the image segmentation is presented in Fig. 6.2. Please note that the preprocessing procedure is essential for successful image segmentation.

Approximation of the shapes is essential in the whole process. Our final approximation is expressed with circles in the image (see Fig. 6.2). Each object is represented by a circle with a radius calculated as the minimal enclosing circle for the object. This allows us to simplify the object representation for the consequent classification. Moreover, we introduced even more tolerance with truncation of the radius value from float to integer.

A simple classification was based on the radius value, all objects with the same radius belong to the same class. To be completely correct, we merged all odd classes with their even predecessors—thus we got only half of the classes, each with more elements. Although it is obvious that there will be the need for further classification steps in order to distinguish among all the shapes of similarly-sized objects, this first classification step based on the presented approximation provides a very good promise for the further research (for illustration, see Fig. 6.3).

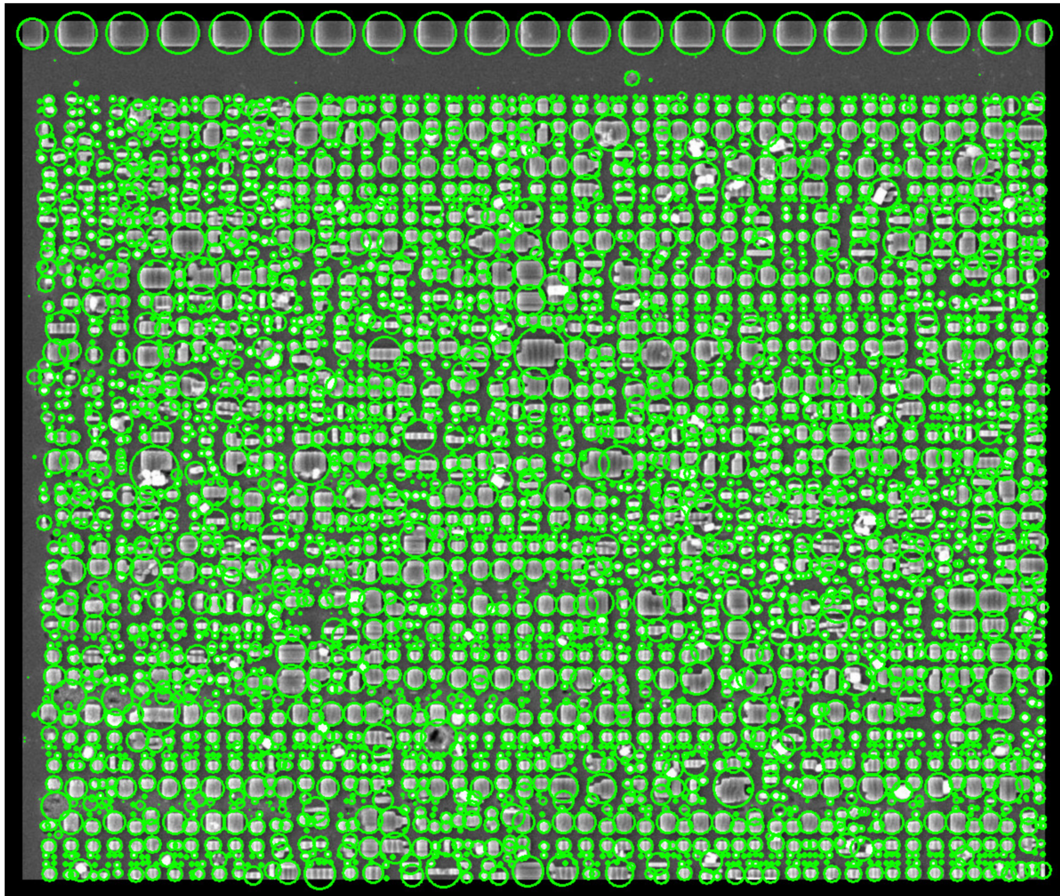

Figure 6.2: The source image was successfully segmented into separate objects. (Source: author's work.)

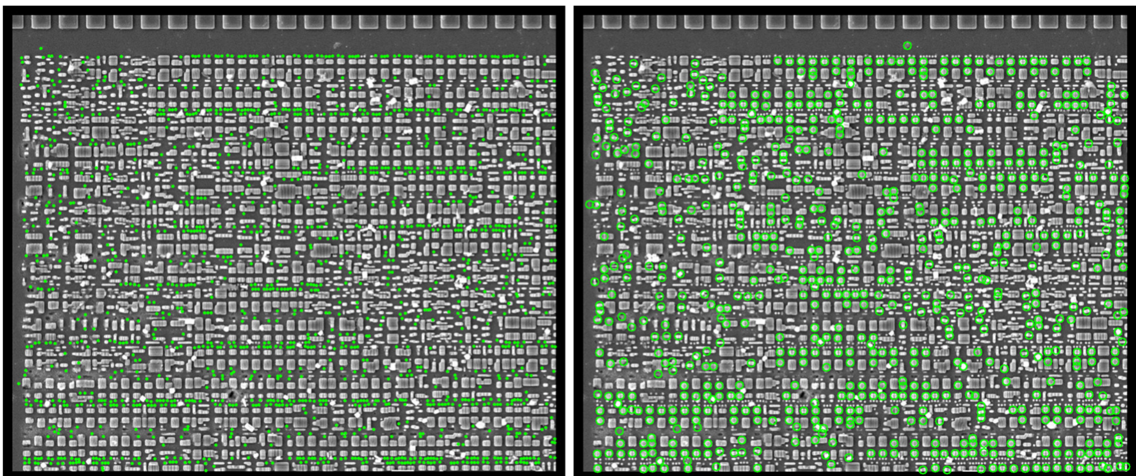

Figure 6.3: Simple classification of the objects detected in the image. Left: Very good results were achieved with the smallest objects (and also with the biggest objects—not displayed). Right: Classification of the mid-sized objects will need further classification steps. (Source: author's work.)

Table 6.2: Comparison of computation length and RAM demands—SIFT, SURF and Shape Matching are measured including the classification part. SIFT and SURF have the used max. distance between vectors in brackets. Tests were performed on the testing data described at the beginning of this chapter; the size of the testing image: 1150×966.

| | Template Matching 50x50 template; 50% shift | Template Matching 50x50 template; 10% shift | SIFT (150) | SURF (0.15) | Shape Matching |
|---|---|---|---|---|---|
| Time | 534 s | 34 s | 14 s | 4 s | 16 s |
| RAM | 200 MB | 200 MB | 2400 MB | 1000 MB | 200 MB |

### 6.4.1 Shape Matching Summary

We were able to segment the input image and perform classification based on approximation of the object shapes with relatively good results—very good classification of the small and big objects; the mid-sized objects still need further step(s) in classification.

On the other hand, it has to be noted that this approach failed completely with our second data set. It was not possible to segment the image in the way we presented. Most probably due to very different production technology—the elements are interconnected, and thus segmentation is not possible in the presented way.

## 6.5 Summary and Future Work

Let us present a final summary of the examined techniques—the performance and RAM demands are presented in Table 6.2. It can be concluded out of the results, that the classic template matching is not convenient neither from performance perspective nor from the gained results. The template matching can be relatively precise with high threshold settings; however, we are missing artifact tolerance then. Let alone the detection of rotated elements.

Image descriptors perform very well. Nevertheless, quality of the output still needs to be moved forward—namely, better classification of the key-points and descriptors, and potential future clustering of similar areas. We would like to continue with experiments and further examination of this approach. The same as with the shape-based matching, where we showed that it was possible to segment the image and prepare the objects for advanced classification. We will also try to combine these two approaches. The particular steps for future work within this approach are outlined in the thesis.

# Chapter 7

# Conclusion

This thesis primarily tackles microscopic analysis of chips with respect to their security. Consequently, tasks affiliated to this topic, e.g., decapsulation, deprocessing, image acquisition and processing, had to be managed as well. The research topic was more applied research than a theoretical one. Despite being at an IT faculty, we had to dive deeply into chemistry and physics in order to be able to proceed with the experiments. Moreover, due to the fact that we were performing all steps in a low-cost regime, we had to deal with all stages primarily on our own. Last but not least, we had to perform the experiments and research basically barehanded compared to the top-notch laboratories that are specialized in this sphere.

Because the efforts in the academic sphere regarding decapsulation and deprocessing were rather scattered and disconnected from each other, we prepared a detailed overview of the decapsulation and deprocessing techniques. Moreover, all processes that were mapped in detail were also verified several times during the experiments in the chemical laboratory. We were able to polish details of the procedures based on our practical experience. During the experiments, we significantly improved the process of obtaining the chips from thermoplastic compounds resulting in approximately 10× speedup. These compounds are used for the production of the plastic cards holding the smartcard chips. With respect to the number of smartcards used all over the globe, we expect this improvement to be practically usable on a daily basis.

The decapsulation techniques that were presented in this thesis are feasible in low-cost, and thus, anybody should be able to carry out this part of the analysis with the use of the provided detailed description. We must also add that observing safety rules is a must, and we do not advise to perform any experiments without proper laboratory equipment and without proper training.

The deprocessing techniques were prepared mainly for the low-cost scenario we worked in. However, as we were getting to the more recent chips, it was clear that obtaining good quality results at a low-cost (without advanced equipment) is based rather on luck than on reproducible processes. Therefore, we also mapped possibilities that are used in professional laboratories. Nevertheless, we cannot consider this low-cost anymore because of the costs of the needed equipment. The older chips can be deprocessed in a chemical laboratory with acceptable effort (after some practice) and still in low-cost—using inexpensive chemicals and an ordinary optical microscope for inspections. Nevertheless, when getting to more recent chips with technological node below 200 nm, proper cross-section analysis has to be done. Afterward, the precise work based on the results of the cross-section is needed—a cross-section analysis is also covered in the thesis. Such work cannot

be performed just with beakers and some chemicals. There is the need for an advanced plasmatic etching station and ideally also a parallel polishing station. Furthermore, optical microscopes are not sufficient for observations of such devices; thus SEM, CLSM, or similar microscopy is required. The detailed description of the procedures was provided to shorten the learning curve of other researchers. The presented procedures were practically verified with experiments—we successfully decapsulated and deprocessed several chips, e.g., simple RFID tags, MIFARE Ultralight C, MIFARE Classic 1 kB; partially also MIFARE DESfire EV1 and the SmartMX chip NXP P5CD080 V0B.

Further, we managed the acquisition process of large dies with SEM microscopy and subsequent post-processing of this data. A comparison of publicly available tools for processing of this type of data is presented, we focused mainly on the stitching of the SEM microscopy outcomes—separated tiles representing the overall chip layer image. We compared the tools with respect to computing time, RAM demands, and the quality of output perspectives.

Finally, we tackled the actively used chip from SmartMX family—NXP P5CD080 V0B, that can be found in the Czech biometric passport implementation. As we found out later, the same chip was also used in the German electronic ID card (Personalausweis) implementation. Compared to the other smartcard chips, this chip was significantly larger in area. We were able to perform decapsulation of 15 samples followed by a detailed cross-section analysis, which revealed the chip's structure, used materials, thickness of layers and vias, and the layout of the chip. Based on this analysis, we were able to create the exact recipe for the chip deprocessing. However, performing the whole process was not possible due to a missing ultra-high frequency plasmatic etcher. It was shown that barrier layers protecting each metal layer are removable with this procedure. Nevertheless, we were able to obtain at least two layers—the silicon level layer and the M5 metal layer. Consequent analysis of this limited data set allowed us to collect a decent portion of information though. The whole analysis process and its results are presented in this doctoral thesis.

An evaluation of various potentially viable methods for (semi-)automatic logic element recognition is also presented. We focused on methods other than the employment of machine-learning. We decided to explore this approach because the common first choice would be to employ learning mechanisms such as, for example, neural networks. The second reason for taking this direction was the limited testing data set availability. It was shown that there were non-learning-based methods usable for aiding microscopic analysis—particularly, image segmentation and object classification suitable for silicon layer image processing. We also outlined the future plan for further research in this field.

An overview of attack classes is given in the thesis, followed by a discussion regarding particular attacks and proposals of possible countermeasures. These countermeasures are supposed to hinder primarily the microscopic analysis. We presented several scenarios based on recently emerging 3D integration, battery-backed memory protection, active tamper detection system, FPGA employment with memory protection mechanisms to shield the bitstream, etc. Finally, we also discussed a possible scenario for the next generation of e-Passports—when the RFID passport chips will be implanted into human bodies.

## 7.1 Future Work

We would like to establish strong partnerships with other faculties and facilities at Brno University of Technology in order to perform the chemical-related parts and scanning part of the microscopic analysis in professional environments. We have created a very good starting

point for this cooperation with the detailed description of the whole process. Furthermore, we would like to focus purely on understanding the data and creating software aiding reverse engineering of the chips.

Based on the thesis outcomes, there are several targets emerging for future research work. First of all, we would like to finalize the complete decomposition of the NXP P5CD080 V0B chip. Afterward, the missing layers can be scanned (LIL, M1, M2, M3, M4), stitched, and aligned to provide the complete chip structure representation.

Deeper investigation can begin, for example, with a proper investigation of the ROM memory structure. We would like to see whether there is any observable border or splitting between boot ROM, test ROM, and application ROM parts. The test ROM should not be accessible after delivery to the customer; however, it can definitely provide a lot of valuable information to the analysts. The next point of interest will be the mechanism of disabling access to the test ROM after production and testing phases. Another target will be reading the ROM content and examination of the obtained data. The data could be encrypted; the potential data encryption would be another target.

The next focus will be directed towards the transistor field. With the information from LIL, M1, and M2 layers, we should be able to distinguish separate blocks (based on the locality of the interconnections). This should allow us to distinguish among components on the chip—CPU, co-processors, etc. It is known that the CPU works in several modes with restricted or unrestricted memory accesses; this can lead to another target in the investigation. Last but not least, the chip supports the running of MIFARE Operating System. This deserves a proper investigation as well.

To conclude, there are numerous other microchips worth investigating, which is the overall motivation for our future work.

# Bibliography

[1] Abraham, D. G.; Dolan, G. M.; Double, G. P.; et al.: Transaction Security System. vol. 30. Feb 1991: pp. 206–229. doi:10.1147/sj.302.0206.

[2] Ahmed, M.; Shaukat, A.; Akram, M. U.: Comparative analysis of texture descriptors for classification. In *2016 IEEE International Conference on Imaging Systems and Techniques (IST)*. Oct 2016. pp. 24–29. doi:10.1109/IST.2016.7738192.

[3] Ali, I.; Khir, M. H. M.; Baharudin, Z.; et al.: CMOS-MEMS multiple resonant vibration energy harvester for wireless sensor network. In *2015 IEEE Regional Symposium on Micro and Nanoelectronics (RSM)*. Aug 2015. pp. 1–4. doi:10.1109/RSM.2015.7354963.

[4] Atmel Smart Card ICs and Hitachi Europe Ltd. and Infineon Technologies AG and Philips Semiconductors: *Smartcard IC Platform Protection Profile*. Jul 2001. version 1.0.
Retrieved from:
https://www.commoncriteriaportal.org/files/ppfiles/ssvgpp01.pdf

[5] Azar, K. Z.; Kamali, H. M.; Homayoun, H.; et al.: SMT Attack: Next Generation Attack on Obfuscated Circuits with Capabilities and Performance Beyond the SAT Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. vol. 2019, no. 1. 2019: pp. 97–122. ISSN 2569-2925. doi:10.13154/tches.v2019.i1.97-122.

[6] Bajura, M.; Boverman, G.; Tan, J.; et al.: Imaging Integrated Circuits with X-ray Microscopy. In *36th GOMACTech Conference*. Apr 2011.

[7] Bi, Y.; Shamsi, K.; Yuan, J.-S.; et al.: Emerging Technology-Based Design of Primitives for Hardware Security. *J. Emerg. Technol. Comput. Syst.*. vol. 13, no. 1. Apr 2016: pp. 3:1–3:19. ISSN 1550-4832. doi:10.1145/2816818.
Retrieved from: http://doi.acm.org/10.1145/2816818

[8] Blackwell, G. R.: *The Electronic Packaging Handbook*. CRC Press. 1999. ISBN 978-0849385919. 640 p.

[9] Boit, C.; Schlangen, R.; Glowacki, A.; et al.: Physical IC debug - Backside approach and nanoscale challenge. *Advances in Radio Science - Kleinheubacher Berichte*. vol. 6. May 2008. doi:10.5194/ars-6-265-2008.

[10] Carmo, J. P.; Rocha, R. P.; Silva, A. F.; et al.: Integrated thin-film rechargeable battery in a thermoelectric scavenging microsystem. In *2009 International Conference on Power Engineering, Energy and Electrical Drives*. Mar 2009. ISSN 2155-5516. pp. 359–362. doi:10.1109/POWERENG.2009.4915179.

[11] Carvalho, C.; Paulino, N.: CMOS Indoor Light Energy Harvesting System for Wireless Sensing Applications: An Overview. In *Technological Innovation for Cyber-Physical Systems*, edited by L. M. Camarinha-Matos; A. J. Falcão; N. Vafaei; S. Najdi. Cham: Springer International Publishing. 2016. ISBN 978-3-319-31165-4. pp. 178–194.

[12] Cavalin, P.; Oliveira, L. S.: A Review of Texture Classification Methods and Databases. In *2017 30th SIBGRAPI Conference on Graphics, Patterns and Images Tutorials (SIBGRAPI-T)*. Oct 2017. ISSN 2474-0705. pp. 1–8. doi:10.1109/SIBGRAPI-T.2017.10.

[13] Chen, S.; Chen, J.; Forte, D.; et al.: Chip-level anti-reverse engineering using transformable interconnects. In *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. Oct 2015. ISSN 1550-5774. pp. 109–114. doi:10.1109/DFT.2015.7315145.

[14] Chen, S.; Shinseki, B.; Barutha, C.; et al.: Infrared imaging and backside failure analysis techniques on multilayer CMOS technology. In *Proceedings of the 1997 6th International Symposium on the Physical and Failure Analysis of Integrated Circuits*. Jul 1997. pp. 17–20. doi:10.1109/IPFA.1997.638066.

[15] Chen, Y.-C.: Enhancements to SAT Attack: Speedup and Breaking Cyclic Logic Encryption. *ACM Trans. Des. Autom. Electron. Syst.*. vol. 23, no. 4. May 2018: pp. 52:1–52:25. ISSN 1084-4309. doi:10.1145/3190853.
Retrieved from: http://doi.acm.org/10.1145/3190853

[16] Chernyy, N.: HOW TO: write an IC Friday post. Online. [accessed 01-Oct-2014].
Retrieved from: https://web.archive.org/web/20110710033130/http://microblog.routed.net/2008/07/15/how-to-write-an-ic-friday-post/

[17] Chung, D.: *Materials for electronic packaging*. Butterworth-Heinemann. 1995. ISBN 978-0750693141.

[18] Cocchi, R. P.; Baukus, J. P.; Chow, L. W.; et al.: Circuit camouflage integration for hardware IP protection. In *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*. Jun 2014. ISSN 0738-100X. pp. 1–5. doi:10.1145/2593069.2602554.

[19] Cottone, F.; Basset, P.; Guillemet, R.; et al.: Non-linear MEMS electrostatic kinetic energy harvester with a tunable multistable potential for stochastic vibrations. In *2013 Transducers Eurosensors XXVII: The 17th International Conference on Solid-State Sensors, Actuators and Microsystems (TRANSDUCERS EUROSENSORS XXVII)*. Jun 2013. ISSN 2159-547X. pp. 1336–1339. doi:10.1109/Transducers.2013.6627024.

[20] Courbon, F.: Practical Partial Hardware Reverse Engineering Analysis. *Journal of Hardware and Systems Security*. Apr 2019. ISSN 2509-3436. doi:10.1007/s41635-019-00068-8.
Retrieved from: https://doi.org/10.1007/s41635-019-00068-8

[21] Courtland, R.: 3D X-ray Tech for Easy Reverse Engineering of ICs, IEEE Spectrum. Online. 2017. [accessed 23-Jul-2018].

Retrieved from: https://spectrum.ieee.org/semiconductors/processors/3d-xray-tech-for-easy-reverse-engineering-of-ics

[22] Courtland, R.: X-rays map the 3D interior of integrated circuits. IEEE Spectrum. Mar 2017.

[23] Davis, W. R.; Wilson, J.; Mick, S.; et al.: Demystifying 3D ICs: the pros and cons of going vertical. *IEEE Design Test of Computers*. vol. 22, no. 6. Nov 2005: pp. 498–510. ISSN 0740-7475. doi:10.1109/MDT.2005.136.

[24] Dini, M.: *Nano-Power Integrated Circuits for Energy Harvesting*. PhD. Thesis. alma. Maggio 2015.
Retrieved from: http://amsdottorato.unibo.it/6947/

[25] Dofe, J.; Gu, P.; Stow, D.; et al.: Security Threats and Countermeasures in Three-Dimensional Integrated Circuits. In *Proceedings of the on Great Lakes Symposium on VLSI 2017*. GLSVLSI '17. New York, NY, USA: ACM. 2017. ISBN 978-1-4503-4972-7. pp. 321–326. doi:10.1145/3060403.3060500.
Retrieved from: http://doi.acm.org/10.1145/3060403.3060500

[26] Dofe, J.; Yu, Q.; Wang, H.; et al.: Hardware security threats and potential countermeasures in emerging 3D ICs. In *2016 International Great Lakes Symposium on VLSI (GLSVLSI)*. May 2016. pp. 69–74. doi:10.1145/2902961.2903014.

[27] Drost, R. J.; Hopkins, R. D.; Ho, R.; et al.: Proximity communication. *IEEE Journal of Solid-State Circuits*. vol. 39, no. 9. Sep 2004: pp. 1529–1535. ISSN 0018-9200. doi:10.1109/JSSC.2004.831448.

[28] Dupuis, S.; Flottes, M.-L.: Logic Locking: A Survey of Proposed Methods and Evaluation Metrics. *Journal of Electronic Testing*. vol. 35, no. 3. Jun 2019: pp. 273–291. ISSN 1573-0727. doi:10.1007/s10836-019-05800-4.
Retrieved from: https://doi.org/10.1007/s10836-019-05800-4

[29] Fahad, H.; Hasan, M.; Li, G.; et al.: Thermoelectricity from wasted heat of integrated circuits. *Applied Nanoscience*. vol. 3, no. 3. Jun 2013: pp. 175–178. ISSN 2190-5517. doi:10.1007/s13204-012-0128-2.
Retrieved from: https://doi.org/10.1007/s13204-012-0128-2

[30] Forte, D.; Bhunia, S.; Tehranipoor, M. M.: *Hardware Protection Through Obfuscation*. Springer Publishing Company, Incorporated. first edition. 2017. ISBN 3319490184, 9783319490182.

[31] Fyrbiak, M.; Strauß, S.; Kison, C.; et al.: Hardware reverse engineering: Overview and open challenges. In *2017 IEEE 2nd International Verification and Security Workshop (IVSW)*. Jul 2017. pp. 88–94. doi:10.1109/IVSW.2017.8031550.

[32] Gu, P.; Li, S.; Stow, D.; et al.: Leveraging 3D technologies for hardware security: Opportunities and challenges. In *2016 International Great Lakes Symposium on VLSI (GLSVLSI)*. May 2016. pp. 347–352. doi:10.1145/2902961.2903512.

[33] Guin, U.; DiMase, D.; Tehranipoor, M.: Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead. *J. Electron. Test.*. vol. 30, no. 1. Feb 2014: pp.

9–23. ISSN 0923-8174. doi:10.1007/s10836-013-5430-8.
Retrieved from: http://dx.doi.org/10.1007/s10836-013-5430-8

[34] Guin, U.; Huang, K.; DiMase, D.; et al.: Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proceedings of the IEEE*. vol. 102, no. 8. Aug 2014: pp. 1207–1228. ISSN 0018-9219. doi:10.1109/JPROC.2014.2332291.

[35] Guin, U.; Zhang, X.; Forte, D.; et al.: Low-cost on-chip structures for combating die and IC recycling. In *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*. Jun 2014. ISSN 0738-100X. pp. 1–6. doi:10.1145/2593069.2593157.

[36] ICAO: *Machine Readable Passports; Passports with Machine Readable Data Stored in Optical Character Recognition Format (Part 1, Volume 1)*. vol. 1. International Civil Aviation Organization. sixth edition. 2006. ISBN 978-92-9231-139-1.

[37] ICAO: *Machine Readable Official Travel Documents; MRtds with Machine Readable Data Stored in Optical Character Recognition Format (Part 3, Volume 1)*. vol. 1. International Civil Aviation Organization. third edition. 2008. ISBN 978-92-9231-139-1.

[38] ICAO: *Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*. International Civil Aviation Organization. seventh edition. 2015. ISBN 978-92-9249-798-9.

[39] ICAO: *Part 11: Security Mechanisms for MRTDs*. International Civil Aviation Organization. seventh edition. 2015. ISBN 978-92-9249-799-6.

[40] ICAO: *Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs*. International Civil Aviation Organization. seventh edition. 2015. ISBN 978-92-9249-797-2.

[41] Imeson, F.; Emtenan, A.; Garg, S.; et al.: Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. Washington, D.C.: USENIX. 2013. ISBN 978-1-931971-03-4. pp. 495–510.
Retrieved from: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/imeson

[42] Juretus, K.; Savidis, I.: Importance of Multi-parameter SAT Attack Exploration for Integrated Circuit Security. In *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. Oct 2018. pp. 366–369. doi:10.1109/APCCAS.2018.8605696.

[43] Kanda, K.: 1.27Gb/s/pin 3[mgr]W/pin Wireless Superconnect (WSC) Interface Scheme. In *2003 IEEE International Solid-State Circuits Conference, 2003. Digest of Technical Papers. ISSCC.*. Feb 2003. ISSN 0193-6530. pp. 186–187. doi:10.1109/ISSCC.2003.1234193.

[44] Karami, E.; Prasad, S.; Shehata, M. S.: Image Matching Using SIFT, SURF, BRIEF and ORB: Performance Comparison for Distorted Images. *CoRR*. vol. abs/1710.02726. 2017. 1710.02726.
Retrieved from: http://arxiv.org/abs/1710.02726

[45] Karmakar, R.; Kumar, H.; Chattopadhyay, S.: On Finding Suitable Key-Gate Locations In Logic Encryption. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. May 2018. ISSN 2379-447X. pp. 1–5. doi:10.1109/ISCAS.2018.8351235.

[46] Ke, S.; Teng-Sing, W.; Yeop, A. B.; et al.: 3D Printing of Interdigitated Li-Ion Microbattery Architectures. *Advanced Materials*. vol. 25, no. 33. 2013: pp. 4539–4543. doi:10.1002/adma.201301036.
Retrieved from:
https://onlinelibrary.wiley.com/doi/abs/10.1002/adma.201301036

[47] Kumagai, J.: Chip detectives [reverse engineering]. *Spectrum, IEEE*. vol. 37, no. 11. Nov 2000: pp. 43–48. ISSN 0018-9235. doi:10.1109/6.880953.

[48] Kwon, I.: *Integrated Circuit Design for Radiation Sensing and Hardening*. PhD. Thesis. University of Michigan. 2015.

[49] Malčík, D.: *Microscopic analysis of chips security*. Master's Thesis. Faculty of Information Technology, Brno University of Technology. 2011.

[50] Malčík, D.; Drahanský, M.: Microscopic Analysis of Chips. In *Security Technology*. Communications in Computer and Information Science. Springer Verlag. 2011. ISBN 978-3-642-27188-5. pp. 113–122. doi:10.1007/978-3-642-27189-2_12.
Retrieved from: http://www.fit.vutbr.cz/research/view_pub.php?id=9848

[51] Malčík, D.; Drahanský, M.: Microscopic Analysis of The Chips: Chips deprocessing. *Advanced Science and Technology Letters*. vol. 2012, no. 7. 2012: pp. 80–85. ISSN 2287-1233.
Retrieved from: http://www.fit.vutbr.cz/research/view_pub.php?id=10041

[52] Massad, M. E.; Garg, S.; Tripunitara, M.: Reverse engineering camouflaged sequential circuits without scan access. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov 2017. ISSN 1558-2434. pp. 33–40. doi:10.1109/ICCAD.2017.8203757.

[53] Mick, S.; Wilson, J.; Franzon, P.: 4 Gbps high-density AC coupled interconnection. In *Proceedings of the IEEE 2002 Custom Integrated Circuits Conference (Cat. No.02CH37285)*. 2002. pp. 133–140. doi:10.1109/CICC.2002.1012783.

[54] Moradi, A.; Barenghi, A.; Kasper, T.; et al.: On the Vulnerability of FPGA Bitstream Encryption Against Power Analysis Attacks: Extracting Keys from Xilinx Virtex-II FPGAs. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*. CCS '11. New York, NY, USA: ACM. 2011. ISBN 978-1-4503-0948-6. pp. 111–124. doi:10.1145/2046707.2046722.
Retrieved from: http://doi.acm.org/10.1145/2046707.2046722

[55] National Institute of Standards and Technology: FIPS 140-2: Security requirements for cryptographic modules. Information Technology Laboratory. 2001.

[56] Ning, H.; H Pikul, J.; Zhang, R.; et al.: Holographic patterning of high-performance on-chip 3D lithium-ion microbatteries. *Proceedings of the National Academy of Sciences of the United States of America*. vol. 112. May 2015.

[57] NXP Semiconductors: *P5CD080/P5CN080/P5CC080/P5CC073V0B*. May 2007. rev. 1.1.
Retrieved from:
https://www.commoncriteriaportal.org/files/epfiles/0410_ma1b.pdf

[58] Odstrcil, M.; Holler, M.; Raabe, J.; et al.: High resolution 3D imaging of integrated circuits by x-ray ptychography. 2018. pp. 10656–10658. doi:10.1117/12.2304835.
Retrieved from: https://doi.org/10.1117/12.2304835

[59] Pecht, M.; Tiku, S.: Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum*. vol. 43, no. 5. May 2006: pp. 37–46. ISSN 0018-9235. doi:10.1109/MSPEC.2006.1628506.

[60] Pikhay, E.; Roizin, Y.; Nemirovsky, Y.: Ultra-Low Power Consuming Direct Radiation Sensors Based on Floating Gate Structures. *Journal of Low Power Electronics & Applications*. vol. 7, no. 3. 2017: pp. 20–22. doi:10.3390/jlpea7030020.

[61] Powell, D.: Finding Solutions to China's E-waste Problem. Online. 2013. [accessed 19-Jul-2018].
Retrieved from: https://ourworld.unu.edu/en/assessing-and-improving-the-e-waste-problem-in-china

[62] Quadir, S. E.; Chen, J.; Forte, D.; et al.: A Survey on Chip to System Reverse Engineering. *J. Emerg. Technol. Comput. Syst.*. vol. 13, no. 1. Apr 2016: pp. 6:1–6:34. ISSN 1550-4832. doi:10.1145/2755563.
Retrieved from: http://doi.acm.org/10.1145/2755563

[63] Rajendran, J.; Sam, M.; Sinanoglu, O.; et al.: Security Analysis of Integrated Circuit Camouflaging. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. CCS '13. New York, NY, USA: ACM. 2013. ISBN 978-1-4503-2477-9. pp. 709–720. doi:10.1145/2508859.2516656.
Retrieved from: http://doi.acm.org/10.1145/2508859.2516656

[64] Rajendran, J.; Sinanoglu, O.; Karri, R.: Is split manufacturing secure? In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*. Mar 2013. ISSN 1530-1591. pp. 1259–1264. doi:10.7873/DATE.2013.261.

[65] Roshanisefat, S.; Mardani Kamali, H.; Sasan, A.: SRCLock: SAT-Resistant Cyclic Logic Locking for Protecting the Hardware. In *Proceedings of the 2018 on Great Lakes Symposium on VLSI*. GLSVLSI '18. New York, NY, USA: ACM. 2018. ISBN 978-1-4503-5724-1. pp. 153–158. doi:10.1145/3194554.3194596.
Retrieved from: http://doi.acm.org/10.1145/3194554.3194596

[66] Sabarillo, R. M.; Mocorro, C. O.: Indoor light energy harvesting system for battery recharging and wireless sensor networks implemented in 90nm CMOS technology. In *2015 International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*. Dec 2015. pp. 1–5. doi:10.1109/HNICEM.2015.7393174.

[67] Schobert, M.: All Chips Reversed. *Die Datenschleuder*. vol. 94. 2010: pp. 17–36. ISSN 0930-1054.

[68] Sengupta, A.; Mazumdar, B.; Yasin, M.; et al.: Logic Locking with Provable Security Against Power Analysis Attacks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. 2019: pp. 1–1. ISSN 0278-0070. doi:10.1109/TCAD.2019.2897699.

[69] Shakya, B.; Asadizanjani, N.; Forte, D.; et al.: Chip editor: Leveraging circuit edit for logic obfuscation and trusted fabrication. In *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Nov 2016. pp. 1–8. doi:10.1145/2966986.2967014.

[70] Shakya, B.; Tehranipoor, M. M.; Bhunia, S.; et al.: *Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation*. Cham: Springer International Publishing. 2017. ISBN 978-3-319-49019-9. pp. 3–32. doi:10.1007/978-3-319-49019-9_1.
Retrieved from: https://doi.org/10.1007/978-3-319-49019-9_1

[71] Shamsi, K.; Li, M.; Meade, T.; et al.: AppSAT: Approximately deobfuscating integrated circuits. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. May 2017. pp. 95–100. doi:10.1109/HST.2017.7951805.

[72] Skvortsov, D.; Yin Shyang Ng, M.; Lundquist, T.; et al.: Laser Voltage Imaging: A New Perspective of Laser Voltage Probing. Nov 2010.

[73] Szendiuch, I.: *Základy technologie mikroelektronických obvodů a systémů*. VUTIUM. 2006. ISBN 80-214-3292-6.

[74] Tareen, S. A. K.; Saleem, Z.: A comparative analysis of SIFT, SURF, KAZE, AKAZE, ORB, and BRISK. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. Mar 2018. pp. 1–10. doi:10.1109/ICOMET.2018.8346440.

[75] Thorne, S.; Ippolito, S.; Eraslan, M.; et al.: High resolution backside thermography using a numerical aperture increasing lens. Jan 2003.

[76] Torrance, R.; James, D.: Reverse Engineering in the Semiconductor Industry. In *Custom Integrated Circuits Conference, 2007. CICC '07. IEEE*. Sep 2007. ISSN 0886-5930. pp. 429–436. doi:10.1109/CICC.2007.4405767.

[77] Torrance, R.; James, D.: The state-of-the-art in semiconductor reverse engineering. In *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*. Jun 2011. ISSN 0738-100x. pp. 333–338.

[78] Tummala, R.: *Fundamentals of Microsystems Packaging*. McGraw Hill Professional. 2001. ISBN 978-0071371698. 967 p.

[79] Vigil, K.; Lu, Y.; Yurt, A.; et al.: Integrated circuit super-resolution failure analysis with solid immersion lenses. *Electronic Device Failure Analysis*. vol. 16. Jan 2014: pp. 26–32.

[80] Vijayakumar, A.; Patil, V. C.; Holcomb, D. E.; et al.: Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques. *IEEE Transactions on Information Forensics and Security*. vol. 12, no. 1. Jan 2017: pp. 64–77. ISSN 1556-6013. doi:10.1109/TIFS.2016.2601067.

[81] Villasenor, J.; Tehranipoor, M.: The Hidden Dangers of Chop-Shop Electronics. Online. 2013. [accessed 19-Jul-2018].
Retrieved from: https://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics

[82] Wang, X.; Gao, M.; Zhou, Q.; et al.: *Gate Camouflaging-Based Obfuscation*. Cham: Springer International Publishing. 2017. ISBN 978-3-319-49019-9. pp. 89–102. doi:10.1007/978-3-319-49019-9_4.
Retrieved from: https://doi.org/10.1007/978-3-319-49019-9_4

[83] Watson, I.: China: The electronic wastebasket of the world. Online. 2013. [accessed 19-Jul-2018].
Retrieved from: https://edition.cnn.com/2013/05/30/world/asia/china-electronic-waste-e-waste/index.html

[84] www.microchemicals.eu: Wet-Chemical Etchingof Silicon. Online. 2012. [accessed 31-Apr-2019].
Retrieved from:
https://www.seas.upenn.edu/~nanosop/documents/silicon_etching.pdf

[85] Xie, Y.; Bao, C.; Serafy, C.; et al.: Security and Vulnerability Implications of 3D ICs. *IEEE Transactions on Multi-Scale Computing Systems*. vol. 2, no. 2. Apr 2016: pp. 108–122. doi:10.1109/TMSCS.2016.2550460.

[86] Xie, Y.; Srivastava, A.: Anti-SAT: Mitigating SAT Attack on Logic Locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. vol. 38, no. 2. Feb 2019: pp. 199–207. ISSN 0278-0070. doi:10.1109/TCAD.2018.2801220.

[87] Yasin, M.; Mazumdar, B.; Rajendran, J. J. V.; et al.: SARLock: SAT attack resistant logic locking. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. May 2016. pp. 236–241. doi:10.1109/HST.2016.7495588.

[88] Yasin, M.; Mazumdar, B.; Sinanoglu, O.; et al.: Removal Attacks on Logic Locking and Camouflaging Techniques. *IEEE Transactions on Emerging Topics in Computing*. 2017: pp. 1–1. ISSN 2168-6750. doi:10.1109/TETC.2017.2740364.

[89] Yasin, M.; Mazumdar, B.; Sinanoglu, O.; et al.: Security analysis of Anti-SAT. In *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*. Jan 2017. ISSN 2153-697X. pp. 342–347. doi:10.1109/ASPDAC.2017.7858346.

[90] Yasin, M.; Sinanoglu, O.: Evolution of logic locking. In *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. Oct 2017. ISSN 2324-8440. pp. 1–6. doi:10.1109/VLSI-SoC.2017.8203496.

[91] Yu, F.-X.; Jia-Rui, L.; Zheng-Liang, H.; et al.: Overview of Radiation Hardening Techniques for IC Design. *Information Technology Journal*. vol. 9. Jun 2010. doi:10.3923/itj.2010.1068.1080.

[92] Zhang, X.; Tehranipoor, M.: Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. vol. 22, no. 5. May 2014: pp. 1016–1029. ISSN 1063-8210. doi:10.1109/TVLSI.2013.2264063.

[93] Zhang, X.; Tuzzio, N.; Tehranipoor, M.: Identification of Recovered ICs Using Fingerprints from a Light-weight On-chip Sensor. In *Proceedings of the 49th Annual Design Automation Conference*. DAC '12. New York, NY, USA: ACM. 2012. ISBN 978-1-4503-1199-1. pp. 703–708. doi:10.1145/2228360.2228486.
Retrieved from: http://doi.acm.org/10.1145/2228360.2228486

# Appendix A

# Relevant Publications

## A.1 Publications

### A.1.1 Conferences

1. Malčík, D.: Mikroskopická analýza čipů *(Microscopic Analysis of Chips)*, In: Proceedings of the 17th Conference STUDENT EEICT 2011, Brno, CZ, FIT VUT, 2011, p. 306–308. ISBN 978-80-214-4272-6.

2. Malčík, D., Drahanský, M.: Microscopic Analysis of Chips, In: Security Technology, Jeju, Jeju Island, KR, Springer, 2011, p. 113–122. ISBN 978-3-642-27188-5.

3. Malčík, D., Drahanský, M.: Anatomy of Biometric Passports, In: Information Science and Industrial Applications 2012, Cebu, PH, Springer, 2012, p. 258–263. ISSN 2287-1233.

4. Malčík, D., Drahanský, M.: Microscopic Analysis of The Chips: Chips deprocessing, In: The Third International Conference Ubiquitous Computing and Multimedia Applications 2012, Bali, ID, Springer, 2012, p. 80–85. ISSN 2287-1233.

### A.1.2 Journals

1. Malčík, D., Drahanský, M.: Anatomy of Biometric Passports, In: Journal of Biomedicine and Biotechnology, Vol. 2012, No. 1, New York, US, p. 1–8. ISSN 1110-7243. *IF: 2,436*

2. Malčík, D., Drahanský, M.: Microscopic Analysis of Chips, In: International Journal of Security and Its Applications, Vol. 2016, No. 11, p. 47–66. ISSN 1738-9976.

3. Malčík, D., Drahanský, M.: Improving The Physical Security Of Microchips Against Side-Channel Attacks, In: International Journal of Advanced Science and Technology, Vol. 2019, No. 127, p. 13–24. ISSN 2207-6360.

### A.1.3 Submitted Publications

1. Malčík, D., Drahanský, M.: Improving the Physical Security of Microchips, In: International Journal of Security and its Applications, Vol. 13, Number 2, ISSN 2207-9629. *Accepted; publishing is expected in September 2019.*

# Appendix B

# Curriculum Vitae

## B.1 Education

- Ph.D. of Computer Science and Engineering, Faculty of Information Technology, Brno University of Technology, Supervisor: prof. Ing., Dipl.-Ing. Martin Drahanský, Ph.D., 2011–present
- Master of Information Technology Security, Faculty of Information Technology, Brno University of Technology, Supervisor: prof. Ing., Dipl.-Ing. Martin Drahanský, Ph.D., 2009–2011
- Bachelor of Information Technology, Faculty of Information Technology, Brno University of Technology, Supervisor: doc. RNDr. Pavel Smrž, Ph.D., 2006–2009
- Gymnasium in Uherské Hradiště, 2002–2006

## B.2 Conferences, Summer Schools, Presentations

- Technische Universität Dresden (TU Dresden), Dresden, DE, 12 / 2014
- Fakultät für Mathematik, Informatik und Physik (Faculty of Mathematics, Computer Science and Physics), University of Innsbruck, Innsbruck, AT, 12 / 2014
- FH Campus Wien, Vienna, AT, 10 / 2014
- Information Science and Industrial Applications (ISI 2012), Cebu, PH, 29. 05. 2012–31. 05. 2012
- BUSLAB, Brno University Security Laboratory, Brno, CZ, 04 / 2012
- Technische Universität Wien (TU WIEN), Vienna, AT, 02 / 2012
- Technische Universität Graz (TU GRAZ), Graz, AT, 12 / 2011
- International Conference on Security Technology (SecTech 2011), Jeju, KR, 8. 12. 2011–10. 12. 2011
- Intensive Program on Information Communication Security (IPICS 2011), Corfu, GR, 20. 8. 2011–2. 9. 2011

## B.3 Projects

- FIT-S-17-4014—Secure and Reliable Computer Systems, BUT
- LD14013—New solutions for multimodal biometrics—enhancement of security and reliability of biometric technologies, COST
- FIT-S-14-2486—Reliability and Security in IT, BUT
- CZ.1.05/1.1.00/02.0123—St. Anne's University Hospital in Brno, International Clinical Research Center
- FR-TI1/195—Research and development of technologies for intelligent optical tracking systems, MPO
- FR1239/2013/Aa—Innovation of laboratory of chips security analysis—SEM Phenom Pure G2, *Preparation of the project application in cooperation with prof. Drahanský.*
- GD102/09/H083—Information Technology in Biomedical Engineering, GACR

## B.4 Teaching

- BIO—Biometric Systems (Biometrické systémy): laboratory exercises
- BIO—Biometric Systems (Biometrické systémy): lectures
- SEN—Intelligent Sensors (Inteligentní senzory): numeric exercises
- SEN—Intelligent Sensors (Inteligentní senzory): laboratory exercises
- SEN—Intelligent Sensors (Inteligentní senzory): lectures
- Bachelor students
  - Tomáš Ševčovič—System for detection of websites with phishing and other malicious content (consultant, FI MUNI)
  - David Raška—Administration of DNS Servers for FreenetIS Project (supervisor)
  - Ondřej Svačina—Microscopic Analysis on RFID Chips (supervisor)
  - Martin Činčala—Performing a Relay Attack on Mifare Smart Cards (supervisor)
  - Martin Michálek—Microscopic Analysis of Smart Cards (supervisor)
  - Jan Rychnovský—Power Analysis on Smart Cards (supervisor)
- Master students
  - Radek Lát—Automated Web Page Categorization Tool (supervisor)
  - Jan Klement—Performing a Microscopic Analysis of Smart Card Chips (consultant)
  - Peter Kovalič—Performing a Fault-Injection Attack on a Smart Card (consultant)
  - Petr Musil—Microscopic Analysis of Mifare Classic (consultant)

## B.5 Work Experience

- Anovis CZ s.r.o., *Networks security*, Managing Director, 05/2016–present
- CYAN Research & Development s.r.o., *Internet Security Software Development*, Managing Director, 08/2014–present
- ICT & MEDIA, s.r.o., *Security Software Development; Data Analysis*, Chief Executive Officer, 01/2012–present
- Self-Employed, 01/2007–09/2012