Velektronik
Vertrauen ist besser

Fraunhofer
AISEC

# Reference paper

# Trustworthy Electronics

## Part I: Definition, Threats and Assessment of Solution Approaches

10 March 2022

Dr. Johann Heyszl, Prof. Dr. Georg Sigl,
Andreas Seelos-Zankl, Dr. Matthias Hiller

Fraunhofer Institute for Applied and Integrated Security AISEC, Germany

# REFERENCE PAPER

# TRUSTWORTHY ELECTRONICS

—

## Part I: Definition, Threats and Assessment of Solution Approaches


**Authors**

Dr. Johann Heyszl

Prof. Dr. Georg Sigl,

Andreas Seelos-Zankl

Dr. Matthias Hiller

Fraunhofer AISEC

Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstrasse 11, 85748 Garching near München




Project name: Velektronik
Date: 10 March 2022
Project partner: Federal Ministry of Education and Research

**Acknowledgement**

The work was funded by the BMBF under the Trustworthy Electronics Platform project, ID code 16ME0214K. The authors would like to thank all project members, the Industrial Advisory Board, workshop participants and all reviewers from industry and research for their contributions.

Bundesministerium für Bildung und Forschung

# Contents

# Introduction and overview

The reference paper "Trustworthy Electronics" is being developed under the Velektronik[1] project, which is being funded by the Federal Ministry of Education and Research (BMBF)[2]. The aim of the Velektronik project is to support projects under the umbrella of the Trustworthy Electronics (ZEUS) funding program by collecting their content, organizing the results in a holistic manner and identifying gaps. This reference paper makes great contributions to achieving this goal. The paper will be extended in several parts in an annual fashion. Part 1 of the paper covers the following aspects:

- A ***definition of trustworthy electronics*** (Section 1). This definition helps to delimit the topic and to explain the relationship with both IT security and technological sovereignty.
- Then, an ***overview of the electronics value chain*** is illustrated (Section 2). It systematically explains the ***threats to trustworthiness*** based on three essential categories. ***Examples*** clarify these categories in a comprehensible way (Section 2.2). Based on this, threats are prioritized according to their relevance (Section 3).
- In addition, ***three simple assessment criteria*** are defined to set out the ***positive impact*** of solution approaches on trustworthy electronics (Section 4).
- The projects funded by the BMBF under the ZEUS funding program are scrutinized in this context to identify gaps in the fields covered (Sections 4.1 and 4.2).
- A summary is followed by an ***outlook including impetus for further research*** (Section 5).

Future parts of this paper will continue to consider which research topics could be focused on more intensely. In addition, topics will be addressed that are often mentioned in the context of trustworthy electronics. Among others, sections are planned on the topics of open-source hardware, authenticity features, measuring trustworthiness as well as the need for standardization. Practical case studies on representative, anonymized companies will demonstrate how research results increase the trustworthiness of electronic products.

[1] https://www.velektronik.de/
[2] https://www.bmbf.de

# 1 A definition of trustworthy electronics

Smart connected products are based to a large extent on safe and trustworthy software. However, the implementation of such software is only possible if the hardware that runs the software is secure and trustworthy. Likewise, other electronic components such as sensors and actuators must provide trustworthy measurement data or perform actions. Consequently, high-quality products that are typical of the German economy are only possible with trustworthy electronics.

This paper therefore focuses on the *trustworthiness of electronic hardware*. Only permanently built-in software, so-called firmware, is included in this consideration. Trust in electronics means that companies can build products and systems on electronic hardware while ruling out, to the highest degree possible, unexpected behavior and security incidents. As the design and manufacture of high-tech electronics is highly complex and requires specialization, the related value chains from design to production as well as supply chains extend around the globe. Under these circumstances, it is extremely challenging to establish trust in electronic hardware.

*Trustworthy electronics* is defined as satisfying the following properties:

1. Electronic hardware must meet ***high levels of quality and reliability***. It can be operated reliably in its field over its full lifetime.

2. Electronic hardware must comply with a ***known and complete specification***.

- This means that the hardware functionality complies *exactly and exclusively* with the specification. The hardware does not include any functionality that may be used as a backdoor either on purpose or by abusing the functionality specified for other purposes. At no later point in the value chain can the hardware functionality be altered from the specification.

3. Electronic hardware must be ***sufficiently hardened against attacks*** that change its behavior or function without the owner's consent.

   - This requires (1) ***security mechanisms in the specification,*** and (2) that the hardware ***does not exhibit any further relevant vulnerabilities outside the specification*** when confronted with realistic attacks in application. Relevant attacks, such as glitching and side-channel attacks, exploit operating conditions and information sources outside the specification. Trustworthy electronics therefore always require a sufficient degree of hardware security, but the definition goes beyond that as shown by the points above.

***Relation to technological sovereignty.*** Technological sovereignty *within the context of trustworthy electronics* means to be able, on its own account, to ensure a sufficient level of trustworthiness across all internationally sourced electronic products and associated services in the value chain. It is important to note that achieving sovereignty does not require all services to be performed under a country's own control or on its own territory. But it is crucial that the above goals can be achieved through own efforts. In general, the solutions to ensure this can be technological as well as organizational.

Technological sovereignty, however, is more far-reaching: It also implies the capability to source electronics as well as (design) tools and manufacturing capacities *at any time and in any quantity* in terms of supply security. This is fundamental but also difficult to ensure. For example, electronic components were in severely short supply during the COVID-19 pandemic. While availability is not directly covered by the concept of trustworthy electronics, it is an essential sub-aspect of technological sovereignty and of immense importance to the industry. It has an impact on trustworthy electronics because shortages and high prices encourage electronic counterfeiting, which in turn is part of the problem of trustworthy electronics.

# 2 The electronics value chain and threats

The electronics value chain is complex and specific for different components, assemblies, devices, technologies and the companies involved. Yet, we outline a generalized and simplified value chain as a basis for all further considerations of threats to trustworthiness and solutions. This abstracted view includes elements specific for semiconductor fabrication as well as elements representing other electronic components and the manufacture of entire devices. The level of abstraction is deliberately not strictly consistent but rather intended to present the most relevant aspects of the value chain for further discussion. For example, software and firmware are not specifically considered.

For each element in the value chain, we identify *sources of threats* that may undermine or damage the intended trustworthiness.

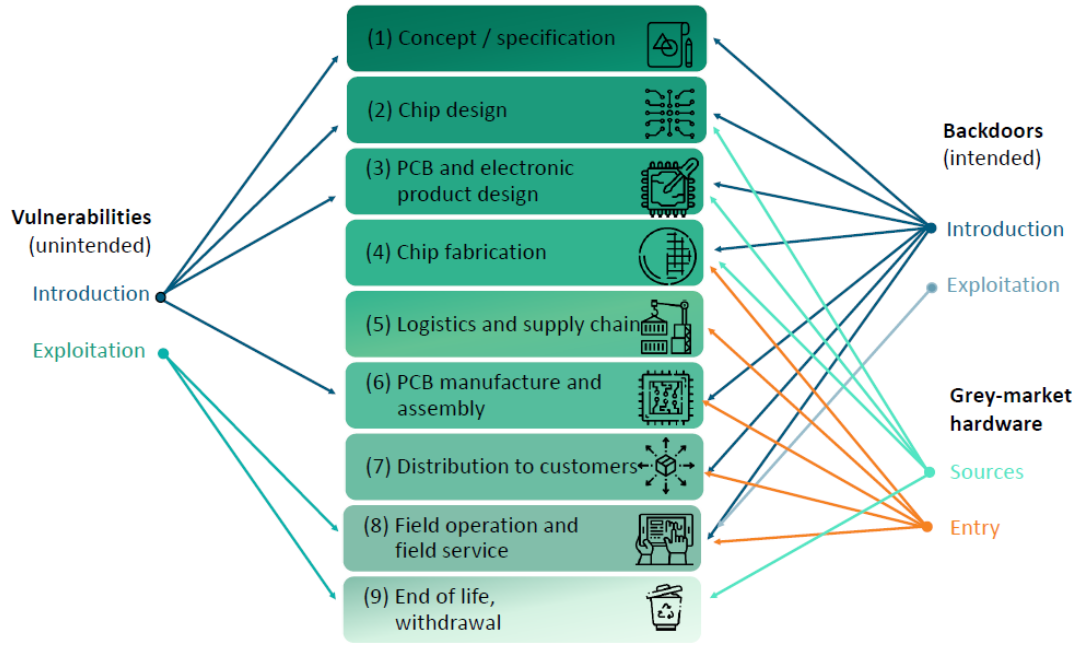



Figure 1: Abstracted electronics value chain and summary of threats to trustworthiness

Figure 1 depicts the elements of an abstracted value chain and summarizes the threats to trustworthiness that can largely be grouped into three categories:

1. ***Vulnerabilities*** which are unintentionally introduced into chips and electronic products and exploited later during operation.
2. ***Backdoors*** which are intentionally introduced into chips and electronic products and exploited later.
3. ***Grey-market hardware*** which describes a group of threats such as the emergence of illegal counterfeit and cloned chips and printed circuit boards (PCBs), low-quality and wrongly labelled rejects as well as IP theft resulting, for example, from reverse engineering.

## 2.1 Threats along the value chain

The elements of the value chain as depicted in Figure 1 are detailed below. Every element is listed with threats and their sources, which are assigned in columns to the three categories identified above. Some elements such as chip design are listed with sub-elements to connect the threats comprehensibly.

*Table 1: Threats to trustworthiness along the electronics value chain*

| Vulnerabilities (unintentional) | Backdoors (intentional) | Grey-market hardware |
|---|---|---|
| **(1) Concept/specification** of chips, modules, assemblies and electronic products | | |
| Gaps/errors in specifications which are abused later | Vulnerabilities in specifications and standards | |
| **(2) Chip design,** analogue/digital/mixed-signal | | |
| - In-house or third-party design | | |
| Implementation errors, functionality with abuse potential, implementation attacks outside the specification in the design phase | Intentionally introduced vulnerabilities or backdoors (HW trojans) in in-house design or outsourced design services | IP theft for illegal clones/counterfeits |
| - Design flow (simulation, synthesis, place & route, layout) | | |
| Design tool optimizations to remove functionally redundant security features | Design tool-based modifications that introduce vulnerabilities/backdoors | (Same as above) |
| **(3) PCB and electronic product design (**in-house and third-party) | | |
| Design errors facilitate access to sensitive interfaces | Embedding of HW trojan chips/unwanted trojan interfaces | (Same as above) |
| **(4) Chip fabrication** | | |
| - Transfer of design data and mask production | | |
| | Manipulation of design or mask data | (Same as above) |
| - Wafer fabrication (front-end/back-end of line) & packaging | | |
| | | Sourcing for grey market from illegal cloning (with potentially different stolen designs), counterfeits (overproduction) or used (recycled) as well as defective chips (re-entry of rejected goods) |
| **(5) Logistics and supply chain** | | |
| | | (Same as above) |
| **(6) PCB manufacture and assembly** including firmware flashing | | |
| Weak hardware root keys or loss of keys | Embedding of HW trojan chips, firmware manipulation (e.g. abuse of boot loader) or manipulated HW root keys | (Same as above) |
| **(7) Distribution** to customers | | |
| (Same as above) | (Same as above) | (Same as above) |
| **(8) Field operation** by customers and **field service** | | |
| Exploitation of vulnerabilities (e.g. after analysis or reverse engineering) | Exploitation of introduced backdoors, introduction of manipulated firmware updates | Introduction of grey-market electronics, reverse engineering for IP theft |
| **(9) End of life**, withdrawal of electronic products, chips, samples etc. | | |
| E.g. illegal reverse engineering instead of disposal/destruction | | Sourcing for grey market by illegal recycling, reverse engineering for IP theft |

## 2.2 Examples

The following examples illustrate the above sources of threats to trustworthiness listing the three identified categories along the value chain.

### 2.2.1 Vulnerabilities (unintentional)

*Concept/specification and chip design*. Many high-tech chips such as CPUs for PCs and servers are highly complex. While companies such as Intel and AMD invest immense efforts to provide high security, chip complexity inevitably leads to unintentional vulnerabilities. The most well-known examples from recent years are the Meltdown and Spectre attacks[3] in CPUs [5, 4]. The attacks exploited complex CPU hardware functionality where relevant implementation details were not publicly documented. The implications were severe because critical software protection mechanisms (isolation mechanisms) could be bypassed.

**Figure 2: Spectre and Meltdown attacks.**
**Source:** https://meltdownattack.com/

Although *unintentional*, the vulnerabilities have serious implications. Typically, access to implementation details of electronic products is limited so that only a few have the opportunity to identify vulnerabilities during a review. When products are certified, e.g. under Common Criteria, more reviewers are involved, but they still remain a small number. Interestingly, vulnerabilities of this type are often discovered in field operation or after withdrawal when specimens are being analyzed, e.g. in reverse engineering. The vulnerabilities are then exploited by attacking the specimens in field operation.

Similar severe vulnerabilities can also be found in less complex chips, such as microcontrollers. For example, it was revealed that USB authentication tokens can be manipulated due to such vulnerabilities during either field operation or after being distributed to the customer, making them completely insecure [9]. Unfortunately, vulnerabilities in electronics permit manipulations at many points in the value chain.

**Figure 3: Unintentional vulnerabilities in USB tokens.**
Source: Schink, Fraunhofer AISEC

A further significant example is from the automotive sector. A popular CPU product exhibited a serious fault in the hardwired firmware (i.e. in the hardware) that allowed the basic protection of the application software to be bypassed and the software to be manipulated in any way[4].

[3] https://meltdownattack.com/

[4] https://blog.quarkslab.com/vulnerabilities-in-high-assurance-boot-of-nxp-imx-microprocessors.html

### 2.2.2 Backdoors (intentional)

*Concept/specification*. There are publicly known examples of backdoors or vulnerabilities that have been introduced deliberately into specifications or products. In one case, a backdoor that remained undiscovered for years was introduced into the standard of a random number generator, Dual_EC_DRBG, in the NIST standard SP 800-90A, which was used in many products, such as the SW cryptographic library by RSA Security Inc.

*Chip design*. Multiple academic publications discuss how hardware trojans *might* be introduced into chips in various steps [2]. The cost/benefit trade-off for most of these manipulations is relatively high, particularly in back-end fabrication steps. The introduction of hardware trojans seems to be primarily relevant in early chip design steps [3], though no specific cases are known in the industry. There was a publicly documented case where a password-protected backdoor in an FPGA was described [10], but it seems to be unclear whether this actually was a backdoor or rather an undocumented debugging interface. Either of these may lead to serious attacks in the field.

*Electronic product design*. An example of this is backdoors built into electronic communication devices distributed by Crypto AG in the 70s, 80s and 90s for encrypted government communication.

*Chip fabrication*. There are no reports of manipulated mask data for chip fabrication. Academic research shows that such manipulations may open well-hidden and severe backdoors. For example, it was shown that the manipulation of only a few transistors (in the random number generator) can fully cancel out all encryption functions of an electronic device [1].

*PCB manufacture and assembly*. A highly acclaimed publication by Bloomberg [7] (along with a follow-up [8]) described that hardware trojans and backdoors were observed to be present in the form of minute, hardly detectable chips implanted on server mainboard PCBs of a particular manufacturer. Such small chips, which would be undetected under normal circumstances, may be used to compromise entire server systems remotely. While evidence for this specific case has never been made public, the scenario is highly realistic given the necessary costs and the impact feared. Reports on counterfeit CISCO network components[5] show very similar manipulations — though in this case for the purpose of counterfeiting instead of as a backdoor. There, too, small chips were implanted on the PCB.

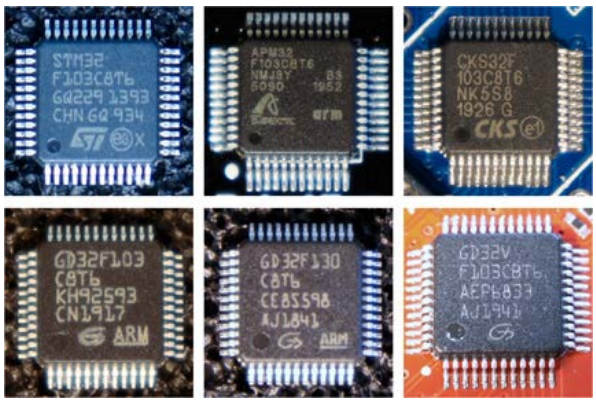
[5] https://www.servethehome.com/fake-cisco-switches-in-the-supply-chain-uncovered/

***Distribution to customers.*** There are comprehensive reports on backdoor implementation in diverse electronic devices by means of small manipulations and implanted chips in the supply chain and during delivery as part of larger government intelligence operations[6]. An example unrelated to this is a USB cable[7] with a Wi-Fi chip implanted in a plastics connector to allow data to be channeled out to an attacker over long distances. The implanted chip can be detected on X-ray images.[8]

### 2.2.3 Grey-market hardware

***Counterfeit/cloned chips.*** There are numerous reports on counterfeit chips of popular products, which are widely distributed. In such cases, the particular specification and quality are extremely insecure so that using these chips is considered high risk. For example, the microcontrollers from STMicroelectronics, which are used in high volumes in IoT devices and embedded devices, are often counterfeited and cloned[9]. Some are marketed as fully compatible replacement chips, others are wrongly labelled as originals [6]. Examples of such counterfeit and cloned STM32F1 chips can be found in [6] [Figure 1 and Figure 2].

**Figure 4: Functionally cloned chips.**
Source: Obermaier, Schink, Moczek [6]




Cloned chips can be made either by reverse engineering or by copying the function. The example of the FTDI chip clones[10] shows that the underlying design was completely different, yet functionally compatible. Another example is a chip from Nordic Semiconductor[11] which was cloned on a different semiconductor process by exact reverse engineering. Counterfeit or cloned chips from the grey market infiltrate and adversely affect the value chain at different stages as depicted in Figure 1.

[6] https://en.wikipedia.org/wiki/NSA_ANT_catalog
[7] https://shop.hak5.org/products/o-mg-cable-usb-c
[8] https://www.vice.com/en/article/k789me/omg-cables-keylogger-usbc-lightning
[9] https://hackaday.com/2020/10/22/stm32-clones-the-good-the-bad-and-the-ugly/
[10] https://zeptobars.com/en/read/FTDI-FT232RL-real-vs-fake-supereal
[11] https://zeptobars.com/en/read/Nordic-NRF24L01P-SI24R1-real-fake-copy

***Counterfeit/cloned electronic devices***. Even entire electronic devices are cloned illegally. For example, illegal counterfeits of CISCO network components[12] were found to be installed at a variety of companies. The report[13] contains pictures of counterfeit devices where the differences of the counterfeit PCBs can be detected to some extent. In part, they contained implanted chips that could theoretically introduce backdoors. In any case, the trustworthiness of such devices is highly questionable. Interestingly, the product forgery in the case described was only possible because one of the main processors had an unintentional hardware vulnerability, which enabled illegal software cloning. So, this example illustrates several threats to trustworthy electronics.

[12] https://www.servethehome.com/fake-cisco-switches-in-the-supply-chain-uncovered/
[13] https://labs.f-secure.com/publications/the-fake-cisco/

# 3 Setting priorities in trustworthy electronics

The threats to trustworthiness along the value chain that were identified in Section 2.1 are displayed as an overview in Table 2 but are now grouped by the three categories. Threats which are similar in different elements of the value chain are grouped together for greater clarity.

Based on this, a simplified risk analysis was performed to understand what threats are particularly relevant. This is to define primary research priorities. The assessment is based on the following properties:

- The estimated ***severity*** quantifies the prospective damage of successful attacks or threats. A greater severity means that a greater number of electronic devices are compromised according to the definition of trustworthy electronics.
- The estimated ***probability of occurrence*** for companies indicates whether a threat is of high practical relevance in the field or rather a risk of academic interest. It is also indicated whether there have been any cases in industry related to a particular threat (as partly described in Section 2).
- The estimated ***cost/benefit ratio*** for the attacker indicates whether a threat is attractive for attackers. For example, if the commercial or strategic benefit is high in relation to the resources needed, such as work, know-how or cost, the ratio is assessed as high. High expenditure for low benefit reduce the cost/benefit ratio accordingly.

Each of the three properties is assessed on three levels as ***high/medium/low***. An ***estimated priority*** is determined based on the three categories. This assessment was performed by experts and reviewed by representatives from research and industry under the Velektronik project. Needless to say, this is an abstracted consideration to the best of their knowledge and belief.

*Table 2: Assessing the priorities of threats to trustworthy electronics.*

| Threats grouped according to elements of the value chain | | Estimated **severity** | Estimated **probability of occurrence** for companies (case reports: yes/no) | Estimated **cost/benefit ratio** for adversaries | Estimated **priority** |
|---|---|---|---|---|---|
| **Vulnerabilities (unintentional)** in the value chain: | | | | | |
| (1) | **Concept/specification** and **chip design** | high | high (yes) | high | **high** |
| (2) | **PCB and electronic product design** | low | medium (no) | medium | medium |
| (3) | **Field operation** (attacks) | high | high (yes) | medium | **high** |
| **Backdoors (intentional)** in the value chain: | | | | | |
| (4) | **Concept/specification** (e.g. standardization) | high | medium (yes) | low | medium |
| (5) | **Chip design** (e.g. third-party) | high | medium (no) | medium | medium |
| (6) | **Chip design** (design flow) and **chip fabrication** (e.g. tool-based, mask manipulation) | medium | low (no) | low | low |
| (7) | **PCB and electronic product design**, **PCB manufacture and assembly**, **distribution** and **field operation** (e.g. implanted HW trojans and FW) | high | high (no) | high | **high** |
| **Grey-market hardware** in the value chain: | | | | | |
| (8) | **Chip design** and **PCB and electronic product design** (e.g. IP theft) | medium | high (yes) | medium | medium |
| (9) | **Chip fabrication** and **end of life** (e.g. overproduction, use of rejects and recycling as well as IP theft) | high | high (yes) | high | **high** |
| (10) | **Logistics and supply chain, PCB manufacture and assembly, distribution** and **field operation** (introduction from grey market) | high | high (yes) | high | **high** |

In summary, the most important threats to trustworthy electronics as assessed in Table 1 are:

- ***Unintentional vulnerabilities in chips*** introduced in early design steps (***concept/specification*** and ***chip design***) and exploited ***in the field***.
- ***Intentional backdoors*** in the form of chips implanted as hardware trojans or manipulated firmware introduced in late value chain steps (from ***PCB and electronic product design, PCB manufacture and assembly*** to ***distribution*** and ***field operation***).
- ***Grey-market hardware*** from ***chip fabrication*** through overproduction and use of rejects as well as illegal recycling after ***end of life***, which infiltrates the value chain at multiple points.

# 4 Assessing solution approaches by criteria

It is not always evident whether solution approaches can have a positive impact on the trustworthiness of electronics. The following criteria are helpful in this assessment:

- Is a ***high-priority threat*** as assessed in the previous section addressed?
- Are ***significant improvements*** achieved?
- What are the ***necessary expenditures***, such as any required additional processes or systems, recurring costs and design work or design complexity (apart from one-off research expenditures)?

An evaluation based on these criteria and their summary makes it possible to assess the (positive) ***overall impact*** of individual solution approaches on trustworthy electronics.

## 4.1 Contextualization of ZEUS research projects

In the following, we briefly present and discuss the research projects funded by the BMBF under the ZEUS funding program. It should be mentioned that the presentation is exclusively based on the aspects of trustworthiness as defined here and research projects inherently often make valuable contributions in other directions.

The discussion was performed by subject matter experts to the best of their knowledge and belief and was reviewed by research project representatives. The presentation is abstracted so that, of course, not every aspect of the projects is presented in detail. In addition, research on these solution approaches is still in progress and the topics are covered in varying degrees by these approaches. The chosen abstraction level should still provide an overview of which threats to trustworthy electronics have not yet been sufficiently addressed and are, in a sense, gaps.

***VE-FIDES: Know-how protection and identifiability of electronic components for trustworthy supply chains.*** The VE-FIDES[14] project deals with improving the security of the supply chain by introducing authenticity features into PCBs and into chips to allow these to be clearly identified both individually and after system assembly. New methods of logic locking and chip obfuscation and their robustness against reverse engineering are also investigated.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by grey-market hardware in all steps of the value chain after chip fabrication (including IP theft) (threats (9) and (10) in Table 2).

- *Are significant improvements achieved?*

  A combination of various authenticity features in different electronic subcomponents provides a high level of security because many parts of a device are included. Insights into the capabilities of reverse engineering are helpful for a better assessment of the threat.

- *Are high costs to be expected?*

  Integrating authenticity features into all relevant chips and their designs significantly increases the expenses for the design and quality assurance of each part (in particular for authenticity features using physical unclonable functions).

  Logic locking only prevents IP theft if we assume that adversaries with the necessary reverse engineering capabilities do not get hold of specimens from the field including matching keys. This scenario seems unrealistic. However, exploring the limits of such methods appears to be useful.

- *Overall impact on trustworthy electronics*: The potential overall impact is high but the required expenses for necessary authenticity features seem just as significant.

***VE-HEP: Trust by transparency: methods and tools for the design of trustworthy open-source processors.*** The VE-HEP[15] project develops an open-source microcontroller hardened against physical implementation attacks by using advanced open-source EDA, hardening and verification tools.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness by unintentional vulnerabilities in the concept/specification and chip design steps (threat (1) in Table 2).

- *Are significant improvements achieved?*

  All open-source designs and tools improve the prospects for trustworthiness because they can be thoroughly reviewed at any time. In addition, they have a positive effect on technological sovereignty since they help to reduce the level of dependencies on commercial suppliers.

- *Are high costs to be expected?*

  The results allow the design expenses to be reduced by tools and automation as well by accessible designs, providing more choices in general. In some cases, however, using open-source EDA tools may require additional expenditure due to inferior maturity.

[14] https://www.elektronikforschung.de/projekte/ve-fides
[15] https://www.elektronikforschung.de/projekte/ve-hep

- *Overall impact on trustworthy electronics*: The potential overall positive impact is high.

***VE-CirroStrato: Novel reconfigurable transistors for know-how protection of electronic components.*** The VE-CirroStrato[16] project aims to develop transistors and logic cells that are configurable in chip fabrication processes, allowing the functionality of a circuit to be concealed even from the foundry which, of course, can see all mask data, as long as the appropriate configuration key is not loaded into the circuit before field use.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threat to trustworthiness posed by IP theft during chip fabrication (threat (9) in Table 2).

- *Are significant improvements achieved?*

  Similar to logic locking, the design (mask data) is worthless at best without the key.

- *Are high costs expected?*

  The protective effect is lost if an adversary, such as a chip foundry, gets hold of a single device from the field including the configuration key because the adversary is then able to extract the key (similar to logic locking). This solution approach requires the additional design of dedicated transistors and cells in each new technology to be protected, thus requiring a high expenditure (similar to the development of a CMOS library)

- *Overall impact on trustworthy electronics*: Addresses a relevant threat. Research results will reveal whether the cost/benefit ratio will make the approach attractive.

***VE-REWAL: Know-how protection for trustworthy heterogeneous electronic systems using chiplets.*** The VE-REWAL[17] project focuses on partitioning the chip functionality into multiple chiplets which are interconnected in a chip package by interposers. Partitioning helps prevent IP theft since no chiplet alone holds the full functionality and an attacker would only get access to one foundry.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threat to trustworthiness posed by IP theft during chip fabrication (threat (9) in Table 2).

- *Are significant improvements achieved?*

  The integration of chiplets into a chip package is advantageous due to the strong specialization of foundries and is increasing in importance. It is possible to integrate chiplets from differently specialized technologies.

- *Are high costs to be expected?*

  In order to significantly impact IP protection, functionality would probably need to be split across different foundries of similar technologies, thus eliminating the advantage of the original motivation for partitioning. The corresponding addition of further foundries would require significant expenditure.

- *Overall impact on trustworthy electronics*: Addresses a relevant threat. Added value only exists as long as the attacker does not get hold of the final product.

[16] https://www.elektronikforschung.de/projekte/ve-cirrostrato
[17] https://www.elektronikforschung.de/projekte/ve-rewal

***VE-ASCOT: Novel secure electronic components for the chain of trust.*** The VE-ASCOT[18] project aims to contribute to the security of the supply chain and to the commissioning of electronic products by integrating trust anchor chips in order to be able to identify products as authentic and track them by a back-end system. To achieve this, a software infrastructure is being established, including a database.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by grey-market hardware (threat (10) in Table 2).

- *Are significant improvements achieved?*

  Being able to check the authenticity of electronic devices reliably using cryptographic methods and a back-end infrastructure makes counterfeiting more difficult.

- *Are high costs to be expected?*

  An additional dedicated trust anchor chip needs to be integrated into each device on the PCB. The necessary infrastructure must be operated and all PCB manufacturers and assemblers must be trustworthy since they connect the additional chip with the device. Once integrated, such chips help to suppress counterfeiting, though they do not prevent any grey-market chips.

- *Overall impact on trustworthy electronics*: Convincing on a device level. The approach does not cover threats posed by grey-market chips.

***VE-SAFE: Preventing attacks on electronic systems using innovative multi-sensor technology.*** The VE-SAFE[19] project aims to protect electronic devices against tampering and side-channel attacks by integrating multiple sensors into PCBs using advanced manufacturing processes. The project also investigates possibilities for targeted destruction in the case of an attack.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by the exploitation of unintentional vulnerabilities in the field (threat (3) in Table 2), inter alia by making reverse engineering more difficult.

- *Are significant improvements achieved?*

  The sensors promise protection against attacks. Instead of resorting to complex chip design, only the PCBs need to be modified or supplemented. However, any functions for erasing sensitive information in the case of attack require arrangements to be made in the chip.

- *Are high costs to be expected?*

  PCB modification requires moderate expenditure and additional sensors. These sensors need to be initially calibrated and also probably continually during operation in order to effectively protect against attacks.

- *Overall impact on trustworthy electronics*: The project addresses important attacks in the field. Research results will show how effectively attacks can be detected. Any expenses for

[18] https://www.elektronikforschung.de/projekte/ve-ascot
[19] https://www.elektronikforschung.de/projekte/ve-safe

additional components and modifications as well as calibration should also be taken into account.

***VE-DIVA-IC: Novel design methods for trustworthy electronic circuits.*** The VE-DIVA-IC[20] project focuses on secure analogue and digital designs (e.g. hardened open processors, shielded analogue interfaces, system-level security measures such as software attestation) and on tools and methods for formal and empirical verification, e.g. against side-channel attacks and hardware trojans.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by unintentional vulnerabilities in the concept/specification and chip design steps and in field operation (threats (1) and (3) in Table 2).

- *Are significant improvements achieved?*

  Progress in the form of open designs and tooling can expediently reduce unintentional vulnerabilities.

- *Are high costs to be expected?*

  Tool-based verification during design requires relatively low additional expenditure.

- *Overall impact on trustworthy electronics*: The potential overall positive impact is high since tooling and open design can be widely used.

***VE-CeraTrust: Prevention of attacks against electronic systems by novel ceramic multi-layer systems.*** The VE-CeraTrust[21] project intends to embed unique identification features into various types of PCBs, subsystems and packages, which are partly built using novel ceramic processes. This helps to identify the authenticity of parts and devices built upon them at various points in the supply chain.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by grey-market hardware along the supply chain (PCBs, subsystems, packages) (threats (9) and (10) in Table 2).

- *Are significant improvements achieved?*

  The mentioned components are integral parts of electronic products, therefore ensuring their authenticity makes counterfeiting in the supply chain more difficult.

- *Are high costs to be expected?*

  The solution approach requires modifications to all these components plus the integration of appropriate features as well as read-out facilities. Ensuring the stability of the features requires quality assurance work. Initial read-out must be done in a trustworthy environment. A back-end system to compare the features must be operated and secured.

- *Overall impact on trustworthy electronics*: The protection of PCBs, subsystems and packages along the supply chain is advantageous although requiring certain expenditures.

[20] https://www.elektronikforschung.de/projekte/ve-diva-ic
[21] https://www.elektronikforschung.de/projekte/ve-ceratrust

Other threats posed by the grey market, such as counterfeit chips, are not within the scope of this consideration.

***VE-Jupiter: Distinct identifiability for trustworthy microelectronics with chiplets.*** The VE-Jupiter[22] project aims to integrate authenticity features into chips in the form of physical unclonable functions to prove their authenticity and to detect design manipulations. The project also integrates trust anchors and further isolation mechanisms into designs to prevent attacks.

- *Is a high-priority threat addressed?*

  The project addresses the medium-priority threat to trustworthiness posed by backdoors introduced in late chip design stages (threat (6) in Table 2) and the high-priority threats posed by grey-market hardware for all steps after chip fabrication (threats (9) and (10) in Table 2) as well as the high-priority threat by unintended vulnerabilities exploited in the field (threat (3) in Table 2).

- *Are significant improvements achieved?*

  The additional circuitry of authentication features allows the authenticity of a chip to be verified in the value chain after initial read-out. Trust anchors and isolation mechanisms improve security.

- *Are high costs to be expected?*

  Authenticity features in the form of physical unclonable functions require significant expenditure in order to qualify and ensure proper functionality and quality. A back-end system is also required including a database to store and compare the features that is securely accessible for all relevant stakeholders in the value chain. Initial read-out must be done in a secure environment. Protection against design manipulations would require very precise simulations.

- *Overall impact on trustworthy electronics*: The solution approaches to counter unintended vulnerabilities are promising. The approaches against threats by grey-market hardware entail non-negligible expenditures.

***VE-ARiS: Electronic know-how protection for innovative sensor systems.*** The VE-ARiS[23] project aims to protect intellectual property in chips and PCBs against theft by reverse engineering and subsequent cloning. It investigates methods of obfuscating chip designs and ways of decomposition as well as watermarking during fabrication.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness posed by grey-market hardware in all stages after chip fabrication (threats (9) and (10) in Table 2) by making IP theft more difficult.

- *Are significant improvements achieved?*

  Making reverse-engineering more difficult is assessed as positive, even if it remains unclear how high the protection ultimately is.

- *Are high costs to be expected?*

  The measures require significant modifications of the chip design flow and PCB manufacture.

[22] https://www.elektronikforschung.de/projekte/ve-jupiter
[23] https://www.elektronikforschung.de/projekte/ve-aris

- *Overall impact on trustworthy electronics*: The solution approaches make IP theft more difficult, although this will be dependent on the capabilities of adversaries. Other threats by grey-market chips such as overproduction are not considered.

***VE-VIDES: Design methods and HW/SW co-verification for the identifiability of electronic components.*** The VE-VIDES[24] project focuses on improving EDA tools and design flows, such as formal verification methods, to integrate protective measures against attacks in an automated process. In addition, the project considers electronic authenticity features in MEMS chips.

- *Is a high-priority threat addressed?*

  Yes, the project addresses the highly prioritized threats to trustworthiness by unintentional vulnerabilities in the concept/specification and chip design steps (threats (1) in Table 2). The authenticity features address the highly prioritized threats by grey-market hardware (threat (9) in Table 2).

- *Are significant improvements achieved?*

  Automated and tool-based approaches can have a positive impact on multiple designs.

- *Are high costs to be expected?*

  The costs associated with the application of tools are relatively low. Authenticity features require expenditures for quality assurance, back-end systems and initial read-out in a secure environment.

- *Overall impact on trustworthy electronics*: The solution approaches based on automated tools address highly prioritized threats to trustworthiness. Authenticity features are a trade-off between expenditure and benefit (see also VE-FIDES and VE-Jupiter).

***VE-Silhouette: Heterogeneous photonic electronics platform for trustworthy open-source processors.*** The VE-Silhouette[25] project focuses on creating interfaces between photonic electronics and electronic circuits (such as open-source processors) for their integration. The project also works on integrated manufacturing processes for the two different technologies.

- *Is a high-priority threat addressed?*

  While the content seems to be reasonable, the project does not address any threats to the trustworthiness of electronics (see Table 2).

- *Are significant improvements achieved?* (Not relevant since trustworthiness is not directly addressed.)

- *Are high costs to be expected?* (Not relevant since trustworthiness is not directly addressed.)

- *Overall impact on trustworthy electronics*: (Not relevant since trustworthiness is not directly addressed.)

***VE-sensIC: Unique identifiability for trustworthy hybrid electronic sensors with additive manufacturing.*** The VE-sensIC[26] project focuses on the integration of sensors (e.g. for temperature) into plastic tubes for the detection of operational faults. It also includes integrating identification features into such tubes.

[24] https://www.elektronikforschung.de/projekte/ve-fides
[25] https://www.elektronikforschung.de/projekte/ve-silhouette
[26] https://www.elektronikforschung.de/projekte/ve-sensic

- *Is a high-priority threat addressed?*

  While the content seems to be reasonable, the project does not address any threats to the trustworthiness of electronics (see Table 2).
- *Are significant improvements achieved?* (Not relevant since trustworthiness is not directly addressed.)
- *Are high costs to be expected?* (Not relevant since trustworthiness is not directly addressed.)
- *Overall impact on trustworthy electronics*: (Not relevant since trustworthiness is not directly addressed.)

***VE-TRUST-E: Trustworthy sensor systems for mobile and industrial applications.*** The VE-TRUST-E[27] project focuses on integrating machine learning methods into chips for sensors so that data can be processed directly at the sensor of various application domains, decisions can be made at this location and the necessary data transfer can be reduced.

- *Is a high-priority threat addressed?*

  While the content seems to be reasonable, the project does not address any threats to the trustworthiness of electronics (see Table 2).
- *Are significant improvements achieved?* (Not relevant since trustworthiness is not directly addressed.)
- *Are high costs to be expected?* (Not relevant since trustworthiness is not directly addressed.)
- *Overall impact on trustworthy electronics*: (Not relevant since trustworthiness is not directly addressed.)

[27] https://www.edacentrum.de/trust-e/

## 4.2 Preliminary identification of gaps

The projects described in the following are mapped to the threats they address. This allows high-priority threats to be identified that have so far been addressed to a minor extent by ZEUS research projects. Table 2 is supplemented accordingly, resulting in Table 3. An analysis of Table 3 reveals:

1. ***Most high-priority threats to trustworthy electronics are addressed by several projects.*** The ZEUS projects almost exclusively address threats classified as high and thus very relevant based on the analysis.
2. Threat (7) " intentional backdoors, e.g. by implanted HW trojan chips and FW" in late steps of the value chain, ***PCB and electronic product design***, ***PCB manufacture and assembly***, ***distribution*** and ***field operation***, is only addressed in one of the projects. This shows a potential gap in threat coverage despite the strongly abstracted consideration.
3. In addition, there are some gaps in medium-priority threats. These threats should continue to be observed in order to determine if, for instance, the basic conditions (e.g. necessary efforts by adversaries) and thus the overall assessment change in the future.

Of course, this is an abstracted view and at this point we cannot analyze in detail to what extent individual solution approaches ensure sufficient coverage or whether solutions from other research projects can be considered a sufficiently effective alternative. Nor does this abstracted view consider, for example, whether solution approaches are particularly complex. Nonetheless, the overview provides preliminary insights into which threats should be addressed more strongly.

*Table 3: Assessing the priorities of threats to trustworthy electronics*

| Threats grouped by elements of the value chain | Estimated **priority** | Addressed by ZEUS project |
|---|---|---|
| **Vulnerabilities (unintentional)** in the value chain: | | |
| (1) **Concept/specification** and **chip design** | **high** | VE-VIDES<br>VE-DIVA-IV<br>VE-HEP |
| (2) **PCB and electronic product design** | medium | |
| (3) **Field operation** (attacks) | **high** | VE-Jupiter<br>VE-DIVA-IC<br>VE-SAFE |
| **Backdoors (intentional)** in the value chain | | |
| (4) **Concept/specification** (e.g. standardization) | medium | |
| (5) **Chip design** (e.g. third-party) | medium | |
| (6) **Chip design** (design flow) and **chip fabrication** (e.g. tool-based, mask manipulation) | low | VE-Jupiter |
| (7) **PCB and electronic product design**, **PCB manufacture and assembly**, **distribution** and **field operation** (e.g. implanted HW trojans and FW) | **high** | VE-FIDES |
| **Grey-market hardware** in the value chain: | | |
| (8) **Chip design** and **PCB and electronic product design** (e.g. IP theft) | medium | |
| (9) **Chip fabrication** and **end of life** (e.g. overproduction, use of rejects and recycling as well as IP theft) | **high** | VE-ARis<br>VE-Jupiter<br>VE-CeraTrust<br>VE-REWAL<br>VE-CirroStrato<br>VE-FIDES |
| (10) **Logistics and supply chain, PCB manufacture and assembly, distribution** and **field operation** (introduction from grey market) | **high** | VE-ARis<br>VE-Jupiter<br>VE-CeraTrust<br>VE-ASCOT<br>VE-FIDES |

# 5 Summary and outlook

The trustworthiness of electronics is often given high importance. Sometimes, different topics such as trustworthiness, IT security, technological sovereignty and further research are sometimes lumped together in the context of general technological progress. The definition in Section 1 as well as the systematic presentation of threats to trustworthiness, including the examples in Section 2, make it easier to differentiate between the various concepts.

***Which research approaches can improve the trustworthiness of electronics?*** Research can contribute to the *trustworthiness of electronics* in various regards. The three criteria described in Section 4 help to assess the effectiveness of approaches:

- *Is a **high-priority threat** to trustworthiness addressed (acc. to Section 2)?*
- *Are **significant improvements** achieved?*
- *What are the **necessary expenditures**, such as additionally required processes or systems, recurring costs and design work or design complexity (apart from one-off research expenditures)?*

The recurring costs of solution approaches in production or for the operation of additional IT infrastructure are often given too little attention in research but are a decisive factor when it comes to their implementation in the industry. While trustworthiness is fundamental for electronics and companies, it is still difficult to price the related costs appropriately in the market. Consequently, it is advisable to make a superficial estimation of costs and work, particularly when comparing research approaches. Fields of research that increase trustworthiness and also contribute to technological sovereignty or to general technological progress are especially attractive. One example is research on open-source tools and designs.

***What threats are given too little attention?*** The analysis of the threats in Table 2 and the comparison with the ZEUS projects show:

- ***Unintentional vulnerabilities in chips*** pose a threat, but ***mainly in early design steps***.

  Approaches such as open-source hardware designs and tool-based protection measures address these risks, cause low additional expenditure and have a positive impact on technological sovereignty. Some ZEUS projects address these aspects.

- ***Grey-market hardware*** seems highly problematic due to illegal overproduction, use of rejects and illegal recycling. Illegal cloning after reverse engineering is also frequently observed in the field.

  Some solution approaches address these risks. One example is the introduction of authenticity features. However, the associated expenditure (e.g. quality assurance of an additional feature or cost of an additional chip) and the restrictions (e.g. need for a trustworthy foundry) are drawbacks. Here the focus should be on solution approaches with the lowest possible expenditure.

- ***Intended backdoors*** are extremely relevant, ***but only in late stages of the value chain*** (e.g. as implanted hardware trojan chips).

  This topic is addressed less intensively by the ongoing ZEUS projects. While being suitable for automatic electronics inspection, existing imaging methods require high expenditure. Authenticity features have so far hardly protected against implants and are also associated with significant expenditure.

***Which direction should additional research take?*** The discussions in the Velektronik project panels and workshops with participants from research and industry have resulted in the following inputs towards suggested additional research directions:

- ***Open-source hardware/RISC-V***: The increasing popularity of the open-source RISC-V architecture specification and of the hardware designs and tools built on it are probably strongly driven by aspects such as general technological potential, technological sovereignty and the will to shift away from proprietary processor technologies that lie in the hands of individual companies. Much like in the area of operating systems, where open-source Linux has gained extremely high importance, something fundamental seems to be changing in the field of hardware processors. The potential gain in trustworthiness by open-source hardware designs (better possibility to review designs and faster design cycles for security improvements) is not emphasized much, yet the whole evolution is highly advantageous for the trustworthiness of electronics for these very reasons. Research in this field is therefore attractive in many ways.
- ***Fabrication processes, analogue open-source hardware and design tools***: Digital open-source hardware, such as that based on the open-source RISC-V architecture, is highlighted in many areas. But in addition to this, a number of other circuit blocks, such as analogue/digital converters, interfaces, storage devices, sensors, etc., are necessary for a functioning chip. Only a few research results are published as open source in this field. Moreover, research within this area is generally restricted in that both tool licenses and the fabrication parameters of chip technologies needed for the designs, termed as *process design kits*, are typically subject to confidentiality, and thus no results may be published. A change of these basic conditions, possibly promoted by more open *process design kits* as well as open-source design tools, for example, would facilitate more research on these essential circuit components.
- ***Gap between open-source design and fabricated chip:*** Even if a (digital) design is open source, essential subsequent steps in the value chain remain closed for the aforementioned reasons. So far, only a few attractive solutions exist to prove that fabricated chips truly comply with specific open-source designs. Imaging and solutions based on random sampling are very costly and therefore do not seem to be particularly attractive. This is a gap which has not been addressed enough. Open chip fabrication process technologies (*process design kits*) would make it possible to disclose information such as mask data and create more possibilities for providing evidence.
- ***Heterogeneous integration, chiplets and split manufacturing***: Heterogeneous integration, i.e. the integration of silicon chiplets from different technologies and foundries, is very relevant for economic reasons. Here, a stronger research focus to increase trustworthiness and IT security seems advantageous.

  Split manufacturing as an approach for increasing trustworthiness by making IP theft and the introduction of backdoors more difficult seems to have a significant negative impact on the profitability of electronics manufacturing. The protective effect is also limited because the finished chip is accessible in the field and splitting the fabrication offers new points of attack in organizations and processes. The approach seems predominately attractive for niche applications.
- ***Authenticity features***: Research on authenticity features often fails to take the significant expenditure associated with their implementation into account. Ensuring the quality of features derived from fabrication variations requires high recurring costs. Apart from that, practical implementation seems to require the standardization and international harmonization of back-end infrastructure to store and compare features. This all represents a major hurdle.
- ***Zero Trust***: Applying the ever more popular 'zero trust' concept to the field of electronics could mean that trustworthiness is to be primarily ensured through technological

measures, whether effective protective measures or meaningful test procedures, rather than through organizational measures such as contractual guarantees. In this context, it could be understood that IT security as part of trustworthiness should be ensured as minimally as possible by the required confidentiality of information. To date, however, important certification procedures such as Common Criteria have attached great importance to confidentiality and rely heavily on organizational aspects and processes. In contrast, open-source designs strive to provide IT security with full transparency, which might be more advantageous in the long term.

# 6 References


[1] Georg T Becker, Francesco Regazzoni, Christof Paar and Wayne P Burleson. Stealthy dopant-level hardware trojans. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 197–214. Springer, 2013.

[2] Swarup Bhunia, Michael S. Hsiao, Mainak Banga and Seetharam Narasimhan. Hardware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, 2014.

[3] Nisha Jacob, Dominik Merli, Johann Heyszl and Georg Sigl. Hardware trojans: current challenges and approaches. *IET Comput. Digit. Tech.*, 8(6):264–273, 2014.

[4] Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, et al. Spectre attacks: Exploiting speculative execution. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1–19. IEEE, 2019.

[5] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom and Mike Hamburg. Meltdown: Reading kernel memory from user space. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 973–990, Baltimore, MD, August 2018. USENIX Association.

[6] Johannes Obermaier, Marc Schink and Kosma Moczek. One exploit to rule them all? On the security of drop-in replacement and counterfeit microcontrollers. In *14th {USENIX} Workshop on Offensive Technologies ({WOOT} 20)*, 2020.

[7] Jordan Robertson and Robertson Riley. The big hack: How china used a tiny chip to infiltrate U.S. companies, 2018.

[8] Jordan Robertson and Robertson Riley. The long hack: How china exploited a U.S. tech supplier, 2021.

[9] Marc Schink, Alexander Wagner, Florian Unterstein and Johann Heyszl. Security and trust in open-source security tokens. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):176–201, 2021.

[10] Sergei Skorobogatov and Christopher Woods. Breakthrough silicon scanning discovers backdoor in military chip. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 23–40. Springer, 2012.