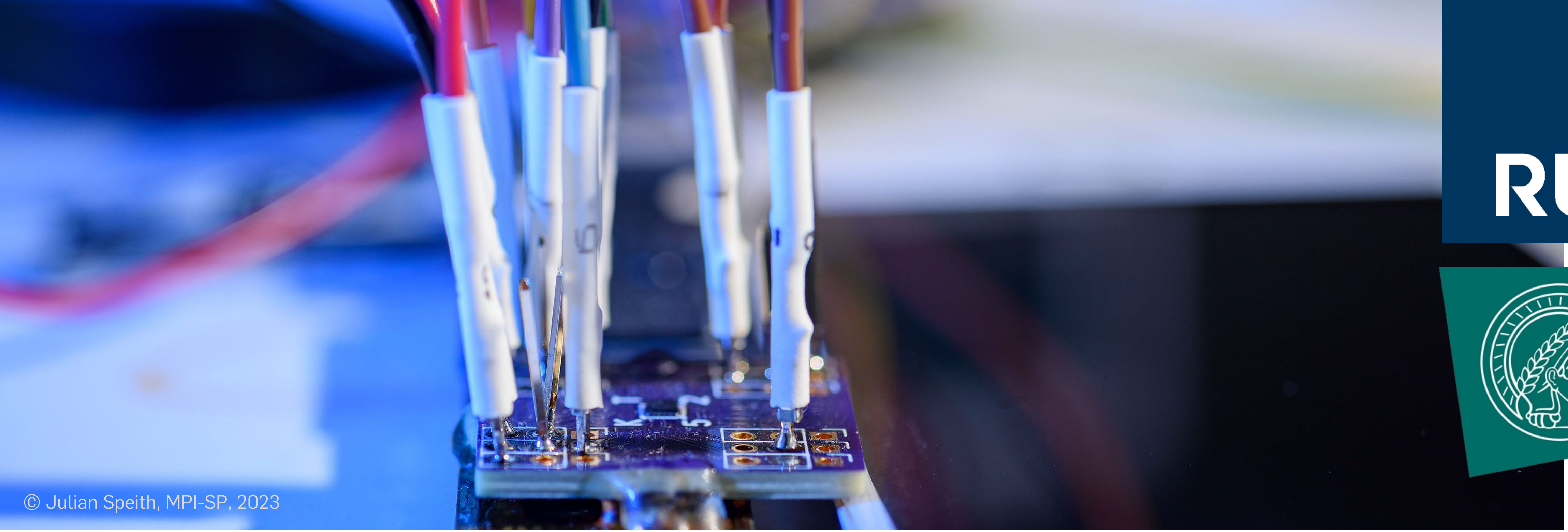

© Julian Speith, MPI-SP, 2023

# Training Hardware Hackers: Insights from the Trenches

René Walendy, Markus Weber, Steffen Becker, Christof Paar, Nikol Rummel

Ruhr University Bochum & Max Planck Institute for Security and Privacy

HARRIS 2025

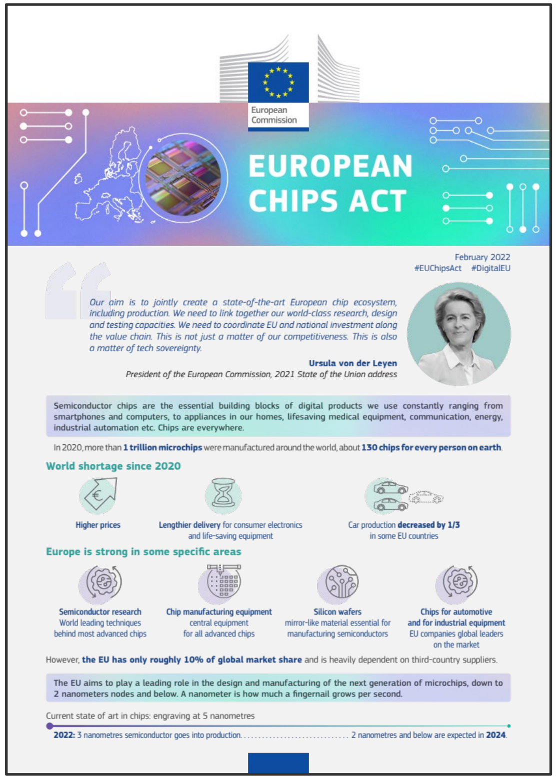
2025-03-18

> “The talent shortage is the biggest challenge to semiconductor industry growth in Europe.”

— H. Schoder, VP of HR, X-FAB Group, 2022

https://www.semi.org/en/blogs/technology-trends/pact-for-skills-x-fab-on-opportunities-for-Europe%27s-semiconductor-industry-growth

# Regulatory Initiatives: Closing the Workforce Gap



European Commission

EUROPEAN CHIPS ACT

February 2022
#EUChipsAct #DigitalEU

> *Our aim is to jointly create a state-of-the-art European chip ecosystem, including production. We need to link together our world-class research, design and testing capacities. We need to coordinate EU and national investment along the value chain. This is not just a matter of our competitiveness. This is also a matter of tech sovereignty.*
>
> **Ursula von der Leyen**
> *President of the European Commission, 2021 State of the Union address*

Semiconductor chips are the essential building blocks of digital products we use constantly ranging from smartphones and computers, to appliances in our homes, lifesaving medical equipment, communication, energy, industrial automation etc. Chips are everywhere.

In 2020, more than **1 trillion microchips** were manufactured around the world, about **130 chips for every person on earth**.

**World shortage since 2020**

- **Higher prices**
- **Lengthier delivery** for consumer electronics and life-saving equipment
- Car production **decreased by 1/3** in some EU countries

**Europe is strong in some specific areas**

- **Semiconductor research** World leading techniques behind most advanced chips
- **Chip manufacturing equipment** central equipment for all advanced chips
- **Silicon wafers** mirror-like material essential for manufacturing semiconductors
- **Chips for automotive and for industrial equipment** EU companies global leaders on the market

However, **the EU has only roughly 10% of global market share** and is heavily dependent on third-country suppliers.

The EU aims to play a leading role in the design and manufacturing of the next generation of microchips, down to 2 nanometers nodes and below. A nanometer is how much a fingernail grows per second.

Current state of art in chips: engraving at 5 nanometres

**2022:** 3 nanometres semiconductor goes into production. . . . . . . . . . . . . . . . . . . . . . . . . . . . 2 nanometres and below are expected in **2024**.

EU: “Chips Act” of 2023

US: “CHIPS and Science Act” of 2022

| | |
|---|---|
| Public Investments: | $ 8.1 bn |
| Private Investments: | $13.7 bn |

https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_4519

| | |
|---|---|
| Combined Investments: | $ 52.7 bn |
| For Security: | $500 m |

https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/

European Commission. Directorate General for Communications Networks, Content and Technology. LU: Publications Office, 2022

*How many of your new hires have a background in reverse engineering?*

**Zero.**

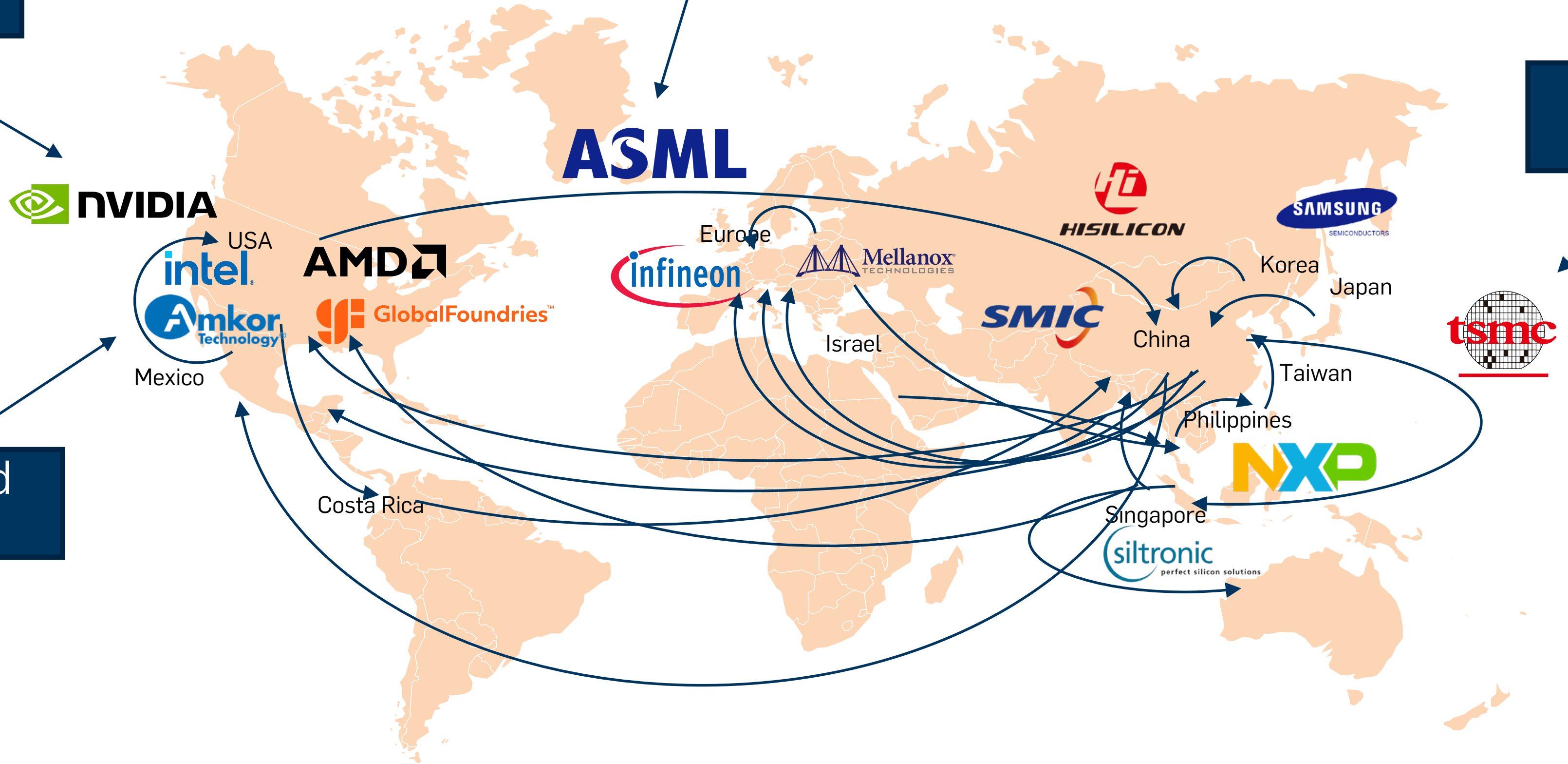
# Threats to the Semiconductor Supply Chain

Conceives the design

Makes the tools

Fabricates the circuit

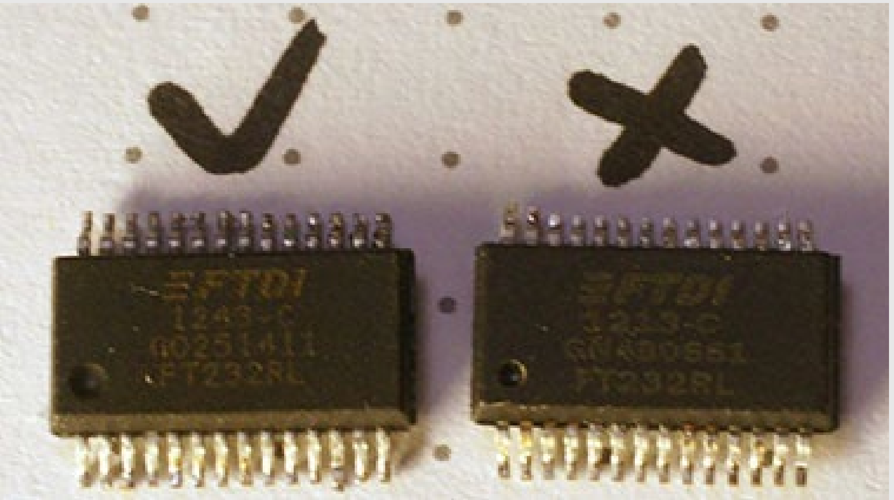
Packages and tests chips



*multitude of not necessarily mutually trusting entities*

# Real-World Cases

## Counterfeit Devices



ZeptoBars, CC BY 3.0, via Wikimedia Commons

**US 2011: $7.5 billion annual loss**

SIA President Brian Toohey, SASC Hearing, November, 2011

## Malicious Manipulations

Bloomberg Businessweek
October 8, 2018
The Big Hack
How [redacted] used a tiny chip to infiltrate [redacted] top companies

2018

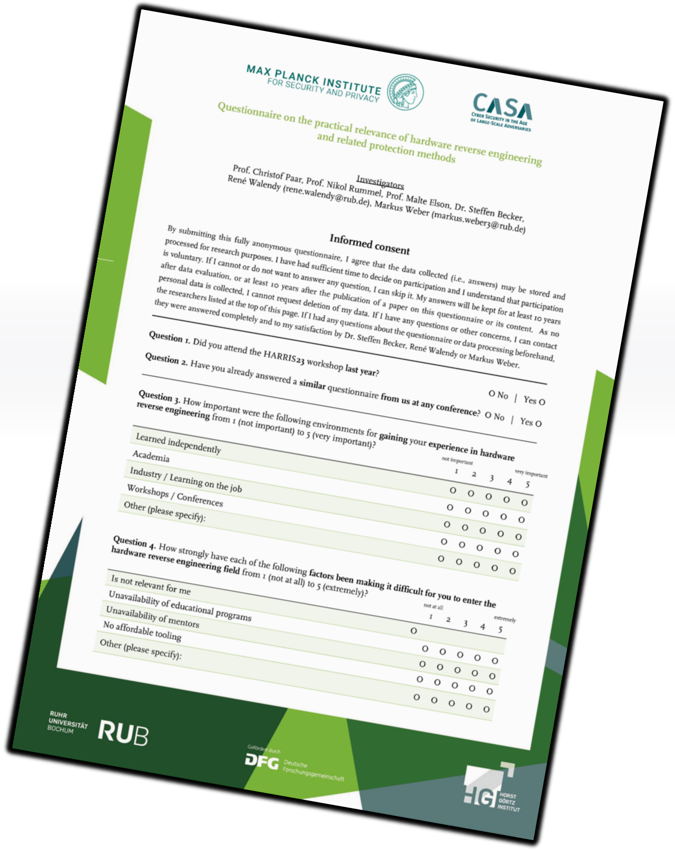
What can we, as a community, do to support the next generation of HRE professionals?

# … so we asked your opinion

Survey with attendees from two leading events in HRE

**HARRIS Workshop 2024, Bochum, Germany**
35 participants

**Hardwear.io USA 2023, Santa Clara, USA**
46 participants



MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

CASA
Cyber Security in the Age of Large-Scale Adversaries

Questionnaire on the practical relevance of hardware reverse engineering and related protection methods

Investigators
Prof. Christof Paar, Prof. Nikol Rummel, Prof. Malte Elson, Dr. Steffen Becker,
René Walendy (rene.walendy@rub.de), Markus Weber (markus.weber3@rub.de)

**Informed consent**

By submitting this fully anonymous questionnaire, I agree that the data collected (i.e., answers) may be stored and processed for research purposes. I have had sufficient time to decide on participation and I understand that participation is voluntary. If I cannot or do not want to answer any question, I can skip it. My answers will be kept for at least 10 years after data evaluation, or at least 10 years after the publication of a paper on this questionnaire or its content. As no personal data is collected, I cannot request deletion of my data. If I have any questions or other concerns, I can contact the researchers listed at the top of this page. If I had any questions about the questionnaire or data processing beforehand, they were answered completely and to my satisfaction by Dr. Steffen Becker, René Walendy or Markus Weber.

**Question 1.** Did you attend the HARRIS23 workshop **last year?** ○ No | Yes ○

**Question 2.** Have you already answered a **similar** questionnaire **from us at any conference?** ○ No | Yes ○

**Question 3.** How important were the following environments for **gaining** your **experience in hardware reverse engineering** from 1 (not important) to 5 (very important)?

| | not important<br>1 | 2 | 3 | 4 | very important<br>5 |
|---|---|---|---|---|---|
| Learned independently | ○ | ○ | ○ | ○ | ○ |
| Academia | ○ | ○ | ○ | ○ | ○ |
| Industry / Learning on the job | ○ | ○ | ○ | ○ | ○ |
| Workshops / Conferences | ○ | ○ | ○ | ○ | ○ |
| Other (please specify): | ○ | ○ | ○ | ○ | ○ |

**Question 4.** How strongly have each of the following **factors been making it difficult for you to enter the hardware reverse engineering field** from 1 (not at all) to 5 (extremely)?

| | not at all<br>1 | 2 | 3 | 4 | extremely<br>5 |
|---|---|---|---|---|---|
| Is not relevant for me | ○ | | | | |
| Unavailability of educational programs | ○ | ○ | ○ | ○ | ○ |
| Unavailability of mentors | ○ | ○ | ○ | ○ | ○ |
| No affordable tooling | ○ | ○ | ○ | ○ | ○ |
| Other (please specify): | ○ | ○ | ○ | ○ | ○ |

RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

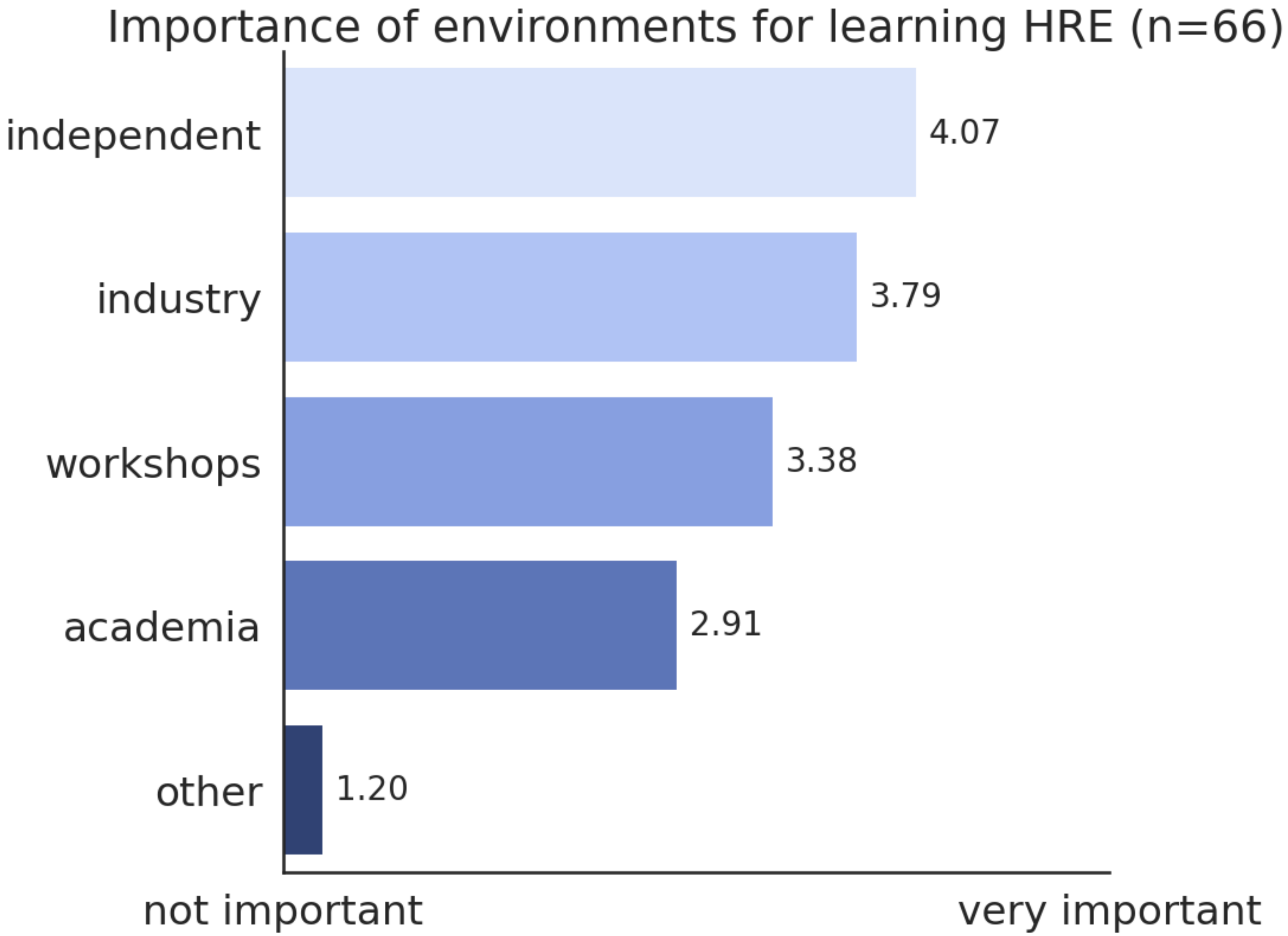
HGI HORST GÖRTZ INSTITUT

# Most Reverse Engineers are Independently Taught

? How important were the following **environments** for gaining your experience in HRE?

hardwear.io
Hardware Security Conference and Training

# Most Reverse Engineers are Independently Taught

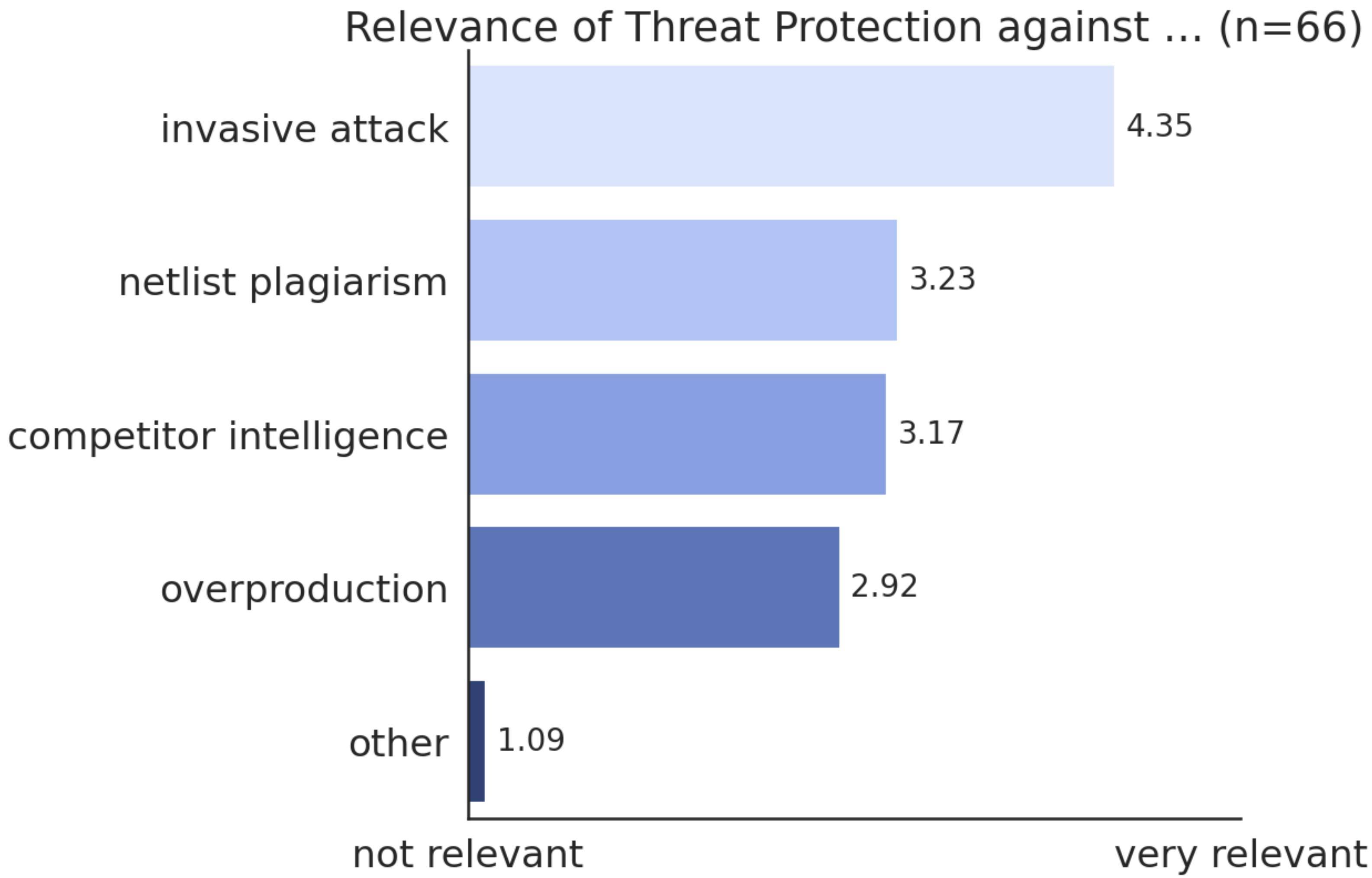


# Central Threat Protection Goals

hardwear.io
Hardware Security Conference and Training

? How would you rate the **practical relevance** of protecting integrated circuits against the following **attack scenarios**?

# Central Threat Protection Goals



hardwear.io
Hardware Security Conference and Training

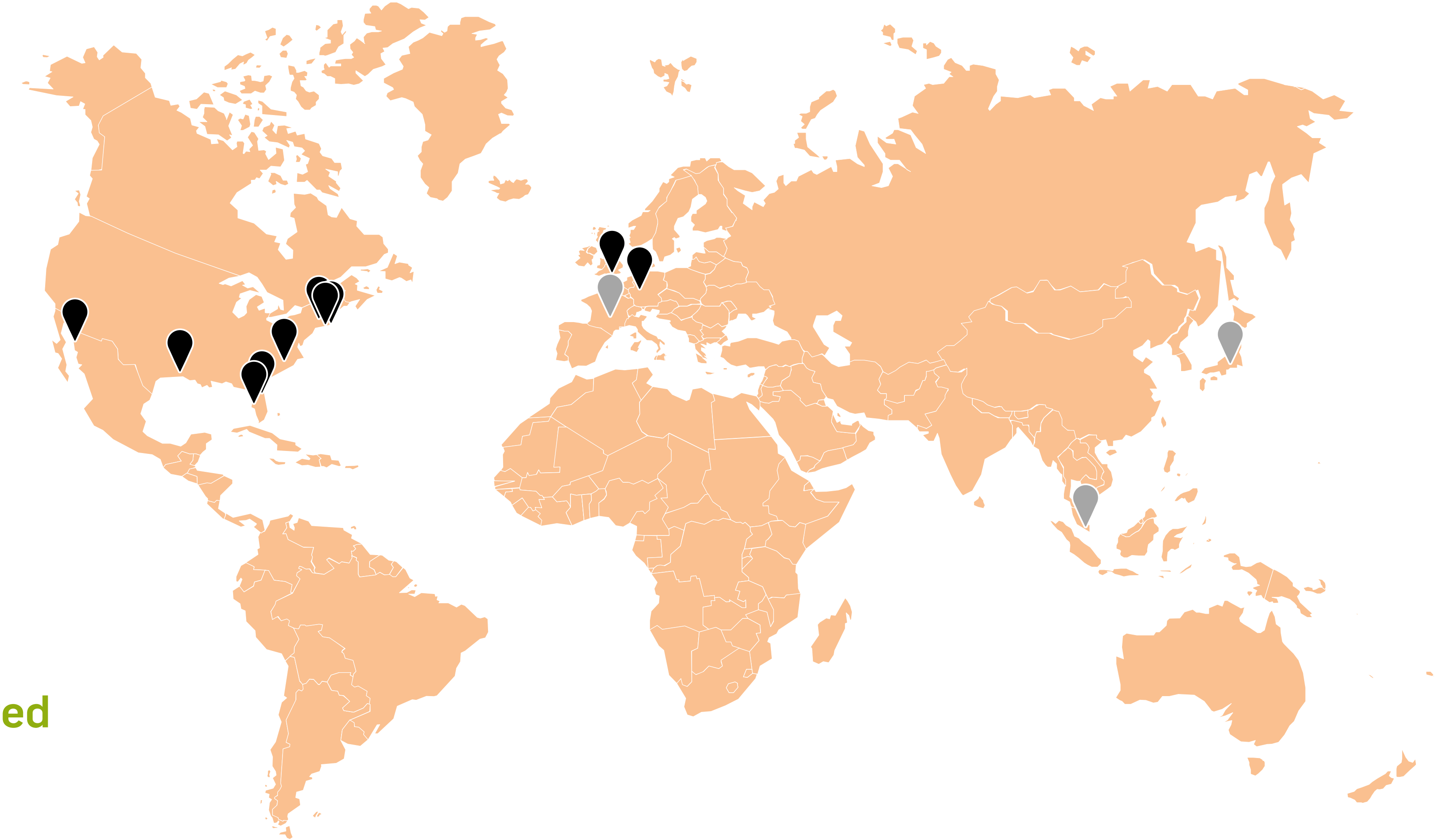
# Can current hardware security education meet this demand?

# Mapping the Trenches

SEMANTIC **SCHOLAR**

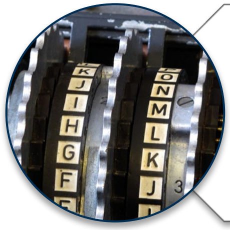
**13 courses discovered**

at 10 institutions



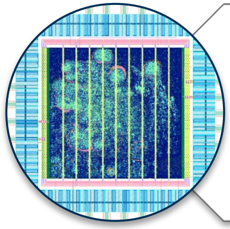
# Educational Focus

Fundamentals & *Forward* Engineering



Cryptology & IT Security

10/13



Very-Lage-Scale Integration (VLSI)

8/13

Hardware Security

Attacks & Defenses

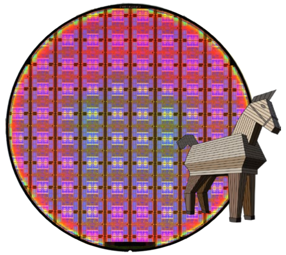
13/13

Hardware Reverse Engineering

~~7/13~~ **3/13**

# Threat Models

Cryptographic secret extraction (12/13)



Hardware Trojans (11/13)

Intellectual property infringement (8/13)

**Defenses taught under those models assume well-known attacks!**

HRE methods can help with forensics and attribution.

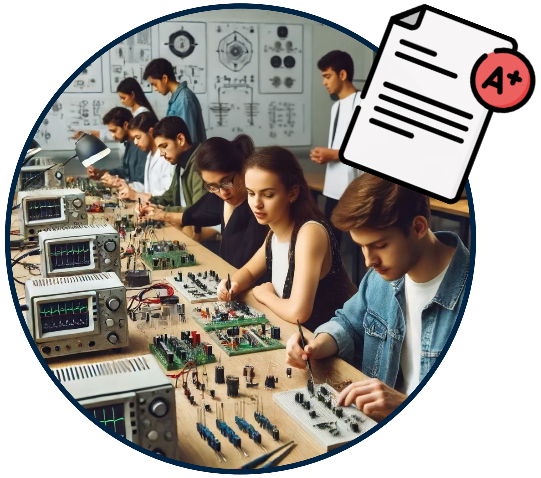
Key and Pirate Flag icons created by Freepik on Flaticon

# First Insights: How to Teach HRE?

**Lectures**
Conveying *declarative* knowledge
(“facts about the skill”)

**Practical Projects & Exercises**
Building *procedural* knowledge
(skills & fluency)

# First Insights: How to Teach HRE?

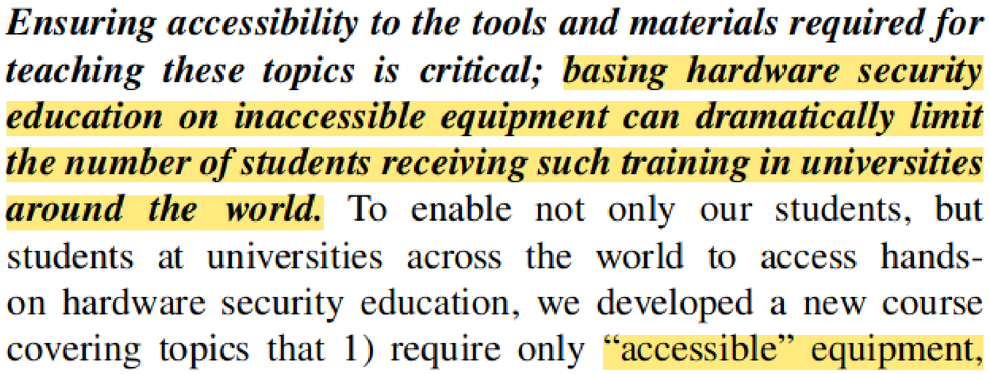


**Practical Projects & Exercises**
Building *procedural* knowledge
(skills & fluency)

**Cost-effective approaches:**

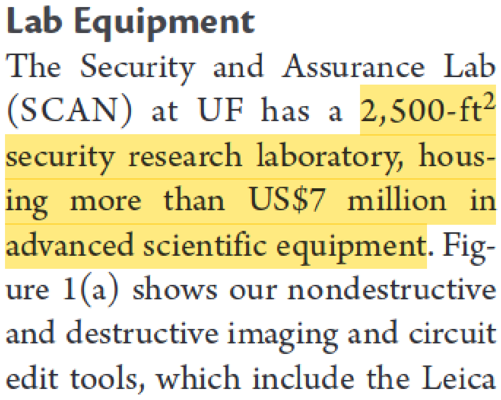
- Hardware simulations
- Reprogrammable hardware (FPGA)

Qualification icon created by Freepik on Flaticon



***Ensuring accessibility to the tools and materials required for teaching these topics is critical; basing hardware security education on inaccessible equipment can dramatically limit the number of students receiving such training in universities around the world.*** To enable not only our students, but students at universities across the world to access hands-on hardware security education, we developed a new course covering topics that 1) require only “accessible” equipment,

– Karam et al. 2022



**Lab Equipment**
The Security and Assurance Lab (SCAN) at UF has a 2,500-ft$^2$ security research laboratory, housing more than US$7 million in advanced scientific equipment. Figure 1(a) shows our nondestructive and destructive imaging and circuit edit tools, which include the Leica

– True et al. 2023

# Where to go from here?

# Recommendations

### On materials & pedagogical principles

- Extend coverage of HRE content in hardware security courses
- Lectures & Labs – Use simulations & reprogrammable hardware

### On labs & real-world experience

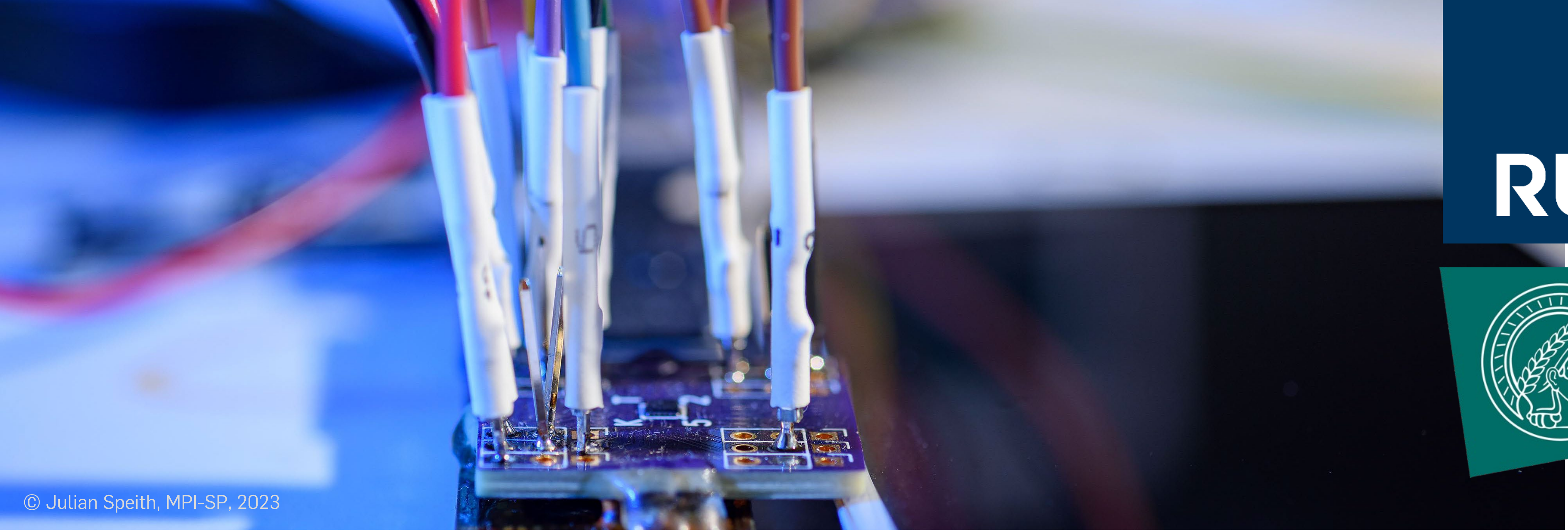
- Release interesting datasets under open license
- Align courses more closely with industry requirements

### On resources & transparency

- Archive your materials & make them discoverable
- Upcoming guidelines should include evaluation criteria

Teaching icon created by by rddrt on Flaticon
Microscope icon created by Freepik on Flaticon
Public Data icon created by Elzicon on Flaticon

Let’s work towards sharing hardware security materials more freely!


© Julian Speith, MPI-SP, 2023

# Thanks for your attention!
# Any questions?

**Check out our paper**

s.gwdg.de/QBx7cL