SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

HUMAN FACTORS IN HRE

An Interdisciplinary Approach to Hardware Security

René Walendy, Steffen Becker

HARRIS 2023, 25.01.2023

RUHR UNIVERSITÄT BOCHUM
RUB

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

HG HORST GÖRTZ INSTITUT

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

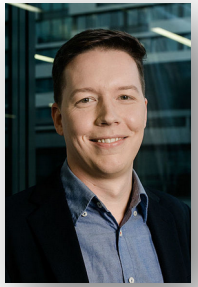
INTERDISCIPLINARY RESEARCH TEAM

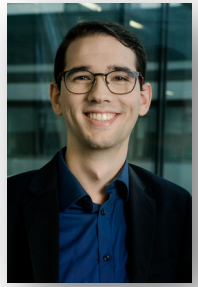
Psychology Squad

SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

Security Squad





Institut für
Erziehungswissenschaft
Ruhr-Universität Bochum

MAX-PLANCK-INSTITUT
FÜR SICHERHEIT UND PRIVATSPHÄRE

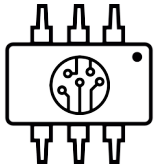
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

THE HRE PROCESS

Camouflaging

Doping Levels

Dummy Contacts



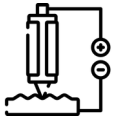
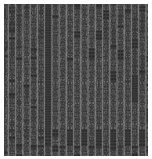
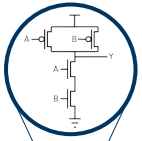


Image Acquisition



Netlist Recovery



Standard Cell Library

SEM

MIST

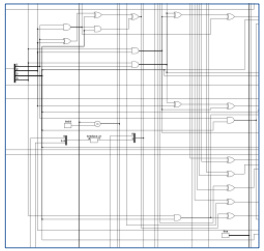
ChipScanner

ChipSuite

Computer Vision

Dummy Wires

Flood Obfuscation



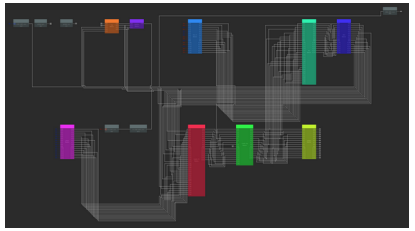
Cyclic Locking

FSM Locking

Logic Locking

Active Metering

Netlist Partitioning



High-Level Description

SAIL

GNN-RE

DANA

SAT Attacks

SMT Attacks

WordRev

Approximate Deobfuscation

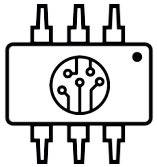
Behavioral Pattern Mining

Protections

RE Techniques

HUMANS DRIVE HRE

Research Gap: Human factors influencing HRE success remain poorly understood



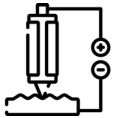
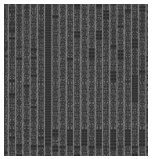
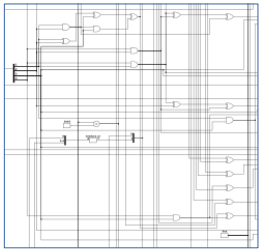


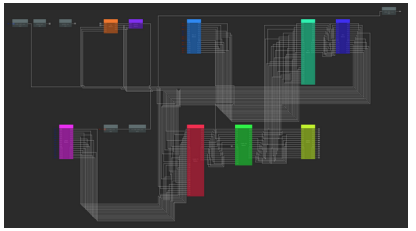
Image Acquisition



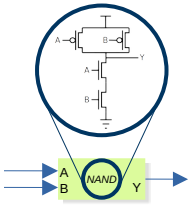
Netlist Recovery



Netlist Partitioning



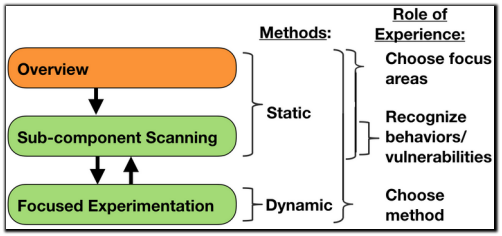
High-Level Description



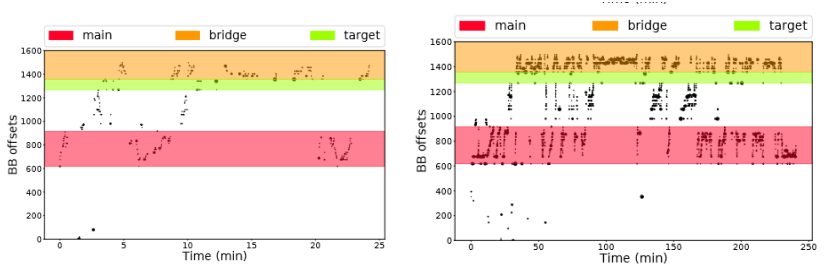
Standard Cell Library

Chemist icon by monkik on Flaticon

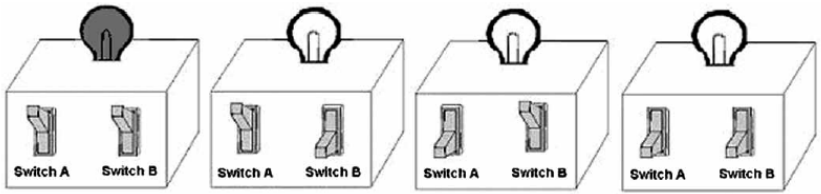
HUMAN FACTORS RESEARCH IN RE

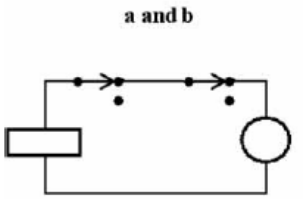


Votipka et al. “An Observational Investigation of Reverse Engineers' Processes.” USENIX Security Symposium (2019).



Mantovani et al. “RE-Mind: a First Look Inside the Mind of a Reverse Engineer.” USENIX Security Symposium (2022).





“Reverse engineering of Boolean functions
= a special kind of **problem solving**”

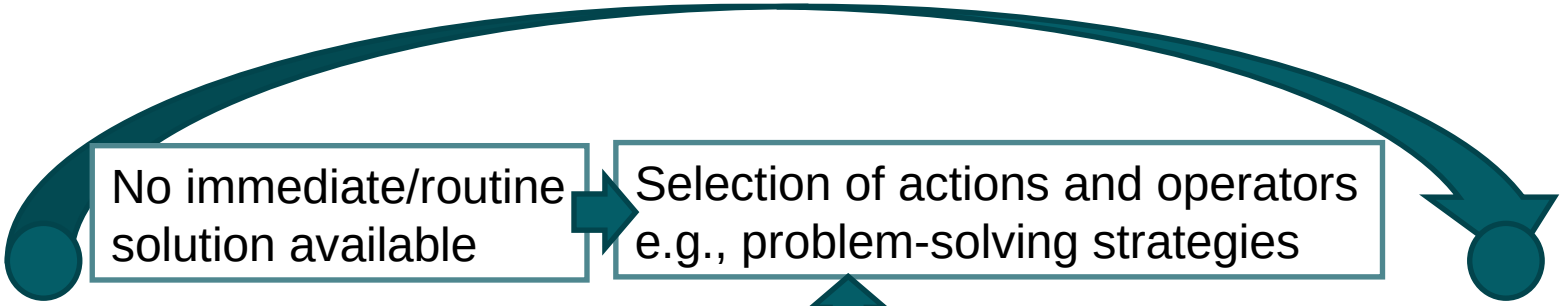
Lee & Johnson-Laird “A theory of reverse engineering and its application to Boolean systems” Journal of Cognitive Psychology (2013).

PROBLEM SOLVING IN HRE

CASA
Cyber Security in the Age of Large-Scale Adversaries

Problem solving = essential cognitive ability and key competence that enables persons to solve (complex) situations

Funke et al., 2018



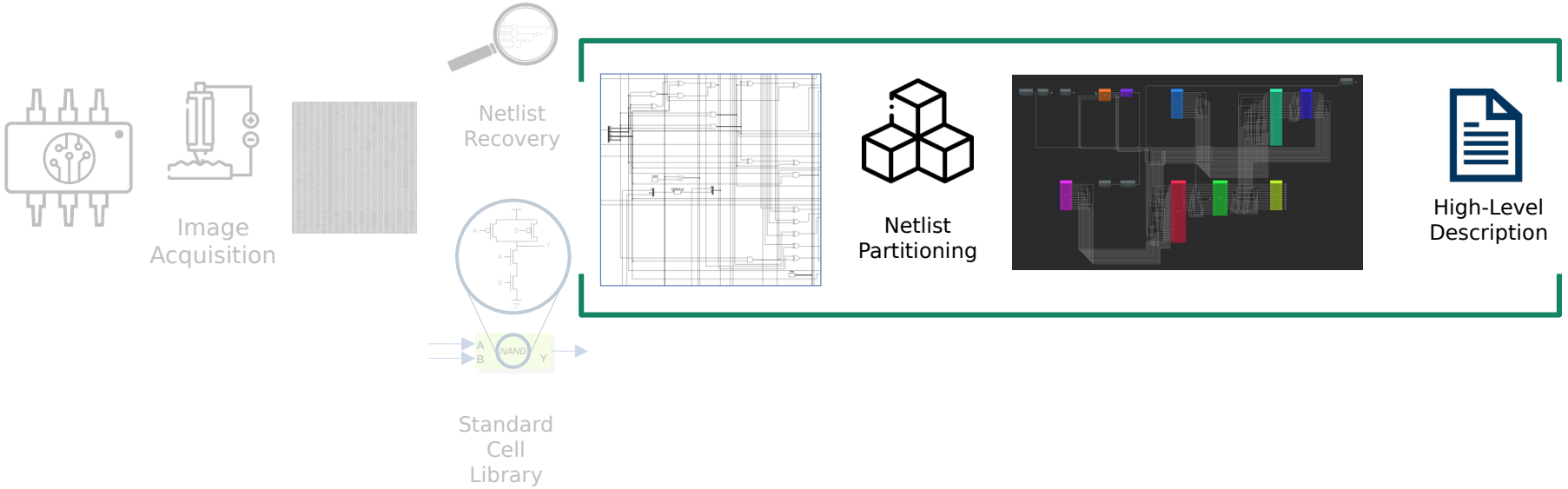
Initial State
e.g., unknown netlist

Influenced by
- Expertise
- Cognitive abilities
- …

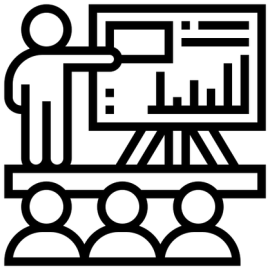
Ericsson et al., 1995
Sternberg et al., 1982

Goal State
e.g., find components of interest

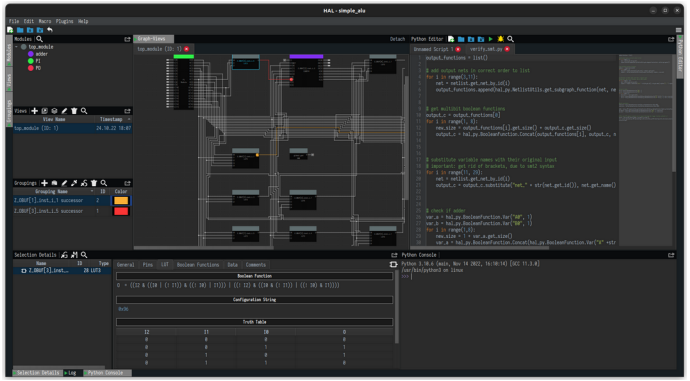
INITIAL WORK: A “COGNITIVE VIEW” OF HRE



RESEARCH ENVIRONMENT: HAL



3-month
HRE course



Practical HRE task in the open hardware analyzer „HAL“

Table 1. Excerpt from the Pre-processed Log File of Participant 8 Showing 6 of 153 Total Events

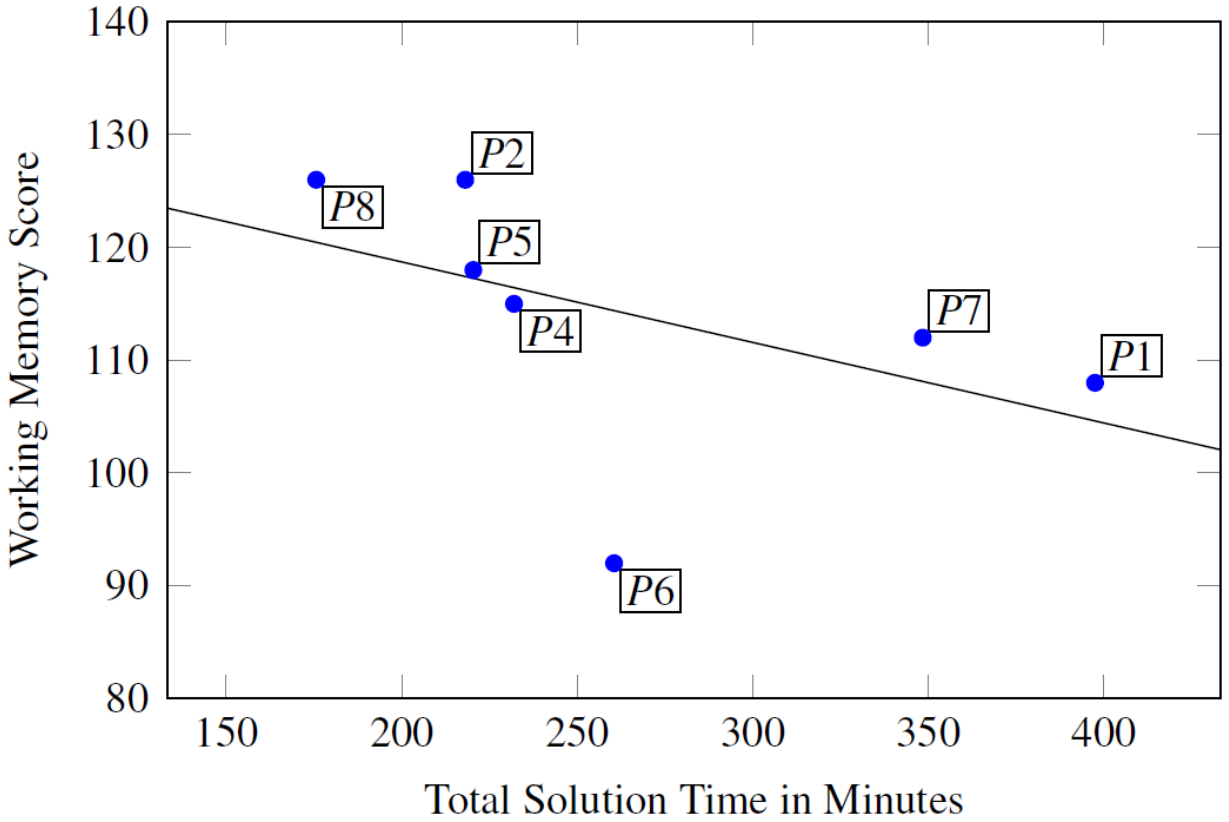
Timestamp	Type	Attribute	Component ID or File Name
...	...	...	...
3,822 s	Script	Working	003822_Participant8.py
3,856 s	Manual	Gate	514
4,240 s	Script	Erroneous	004240_Participant8.py
4,268 s	Script	Working	004268_Participant8.py
4,334 s	Manual	Gate	531
4,341 s	Manual	Net	2,437
...	...	...	...

Behavioral log files and executed scripts

Training icon by Eucalyp on Flaticon

SELECTED RESULTS (COGNITIVE FACTORS)

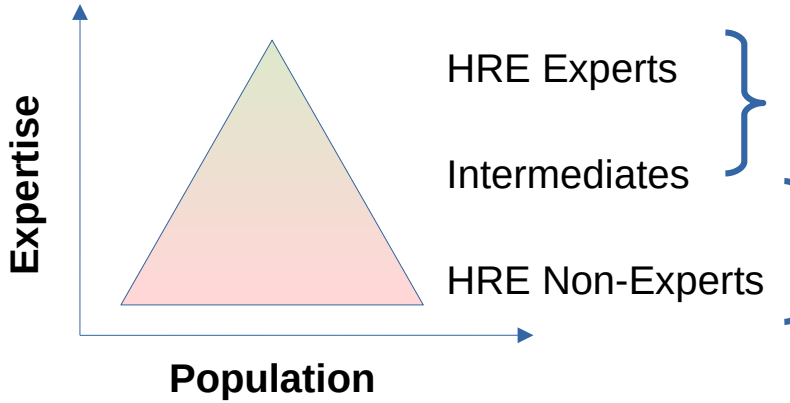
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



Becker et al. "An Exploratory Study of Hardware Reverse Engineering – Technical and Cognitive Processes." SOUPS (2020).

Disclaimer: only descriptive analysis; further research needed!

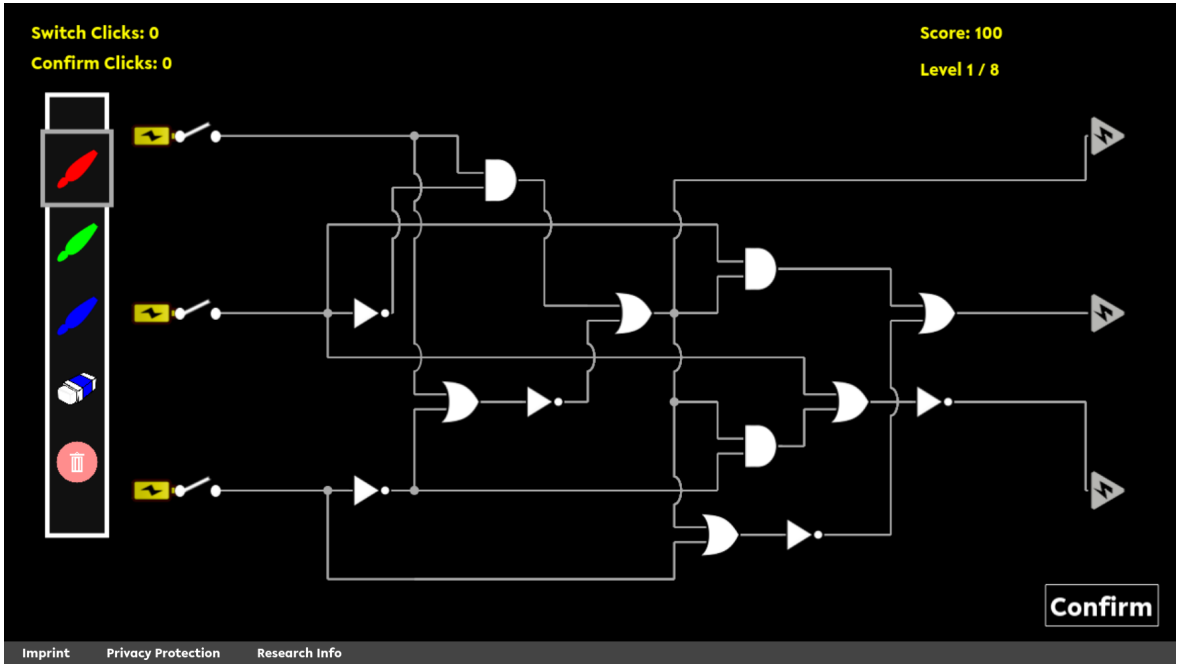
FROM QUALITATIVE TO QUANTITATIVE



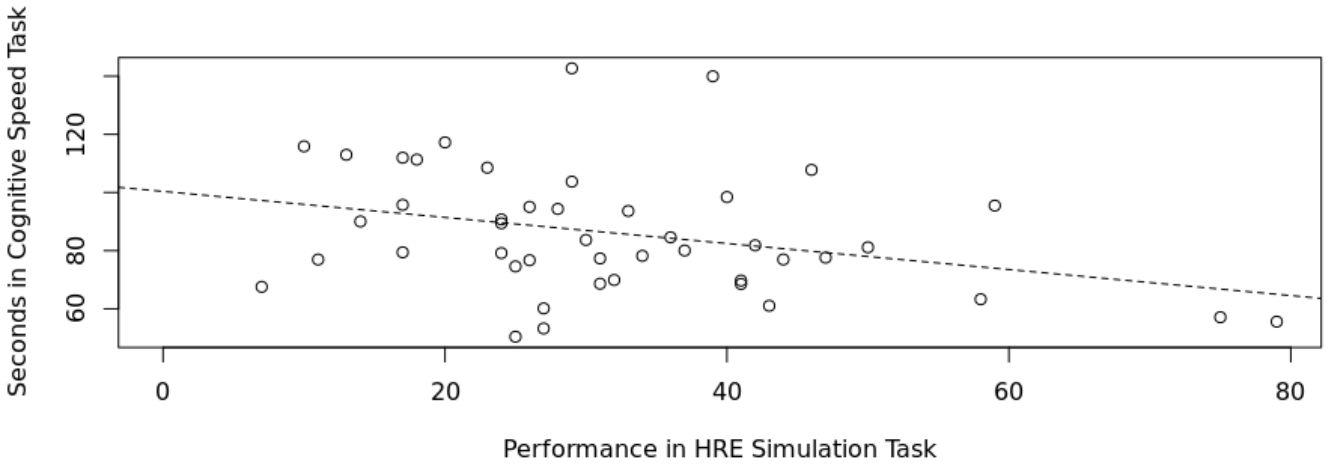
- **Qualitative** models
- First small-sample indications

- **Quantitative** models
- Needs larger sample sizes

HRE SIMULATION: REVERSING GAME



HRE SIMULATION: COGNITIVE FACTORS



corr. = -.33
n = 51

- Observations corroborate findings from the prior study
- Test bed for future cognitive factors research

CASA
Cyber Security in the Age of Large-Scale Adversaries

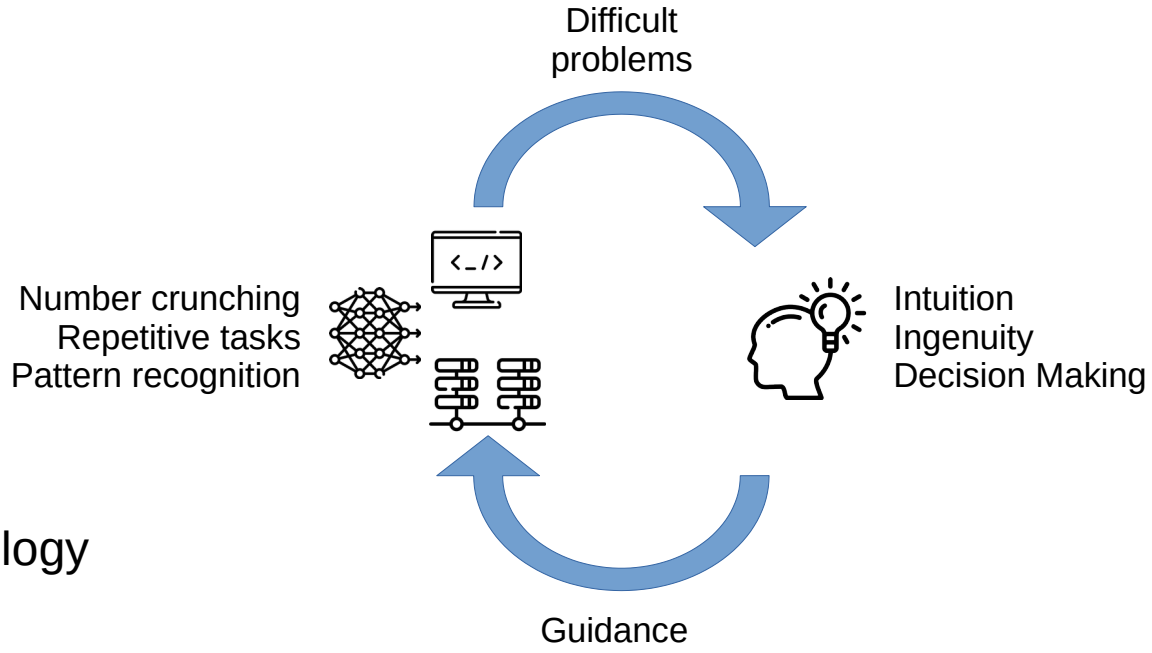
Challenges and Opportunities

for practical applications
and further research

“OFFENSIVE” SECURITY

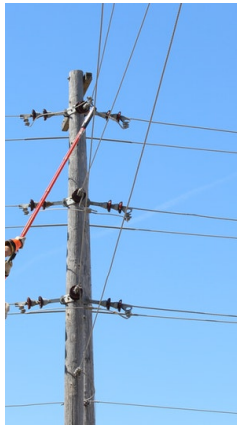
- More efficient(ly usable) HRE tooling

- Human-in-the-loop technology



DEFENSIVE SECURITY

- Current obfuscation: based on **algorithmic complexity**
- What if we add a **cognitive complexity** component?
- **Cognitive obfuscation:** protecting intellectual property by impeding human sensemaking



Thanks @ Max Hoffmann

Source: www.constructionknowledge.net

WE WANT YOUR INPUT!

We’re interested in …

- … **exchange of ideas** with experts
- … **volunteers** for our studies

- … the **relevance of hardware obfuscation** (**and**, on the other side of the same coin, **hardware Trojans**) for the industry
- … real-world **netlists & problem settings**


Practical relevance of hardware reverse engineering

1. How would you rate the **practical relevance** of the following reverse engineering goals from 1 (not relevant) to 5 (very relevant)?

	1	2	3	4	5
Failure analysis	O	O	O	O	O
Detecting IP violations (functional blocks, counterfeit ICs)	O	O	O	O	O
Detecting hardware Trojans / supply chain verification	O	O	O	O	O
Extracting secret keys, ROM, or Flash memory contents	O	O	O	O	O
Detailed analysis of individual nano devices (transistors, contacts, etc.)	O	O	O	O	O
Identification of functional units or areas of interest	O	O	O	O	O
High-level understanding of individual circuit blocks or the entire design	O	O	O	O	O
Accurately recovering (parts of) a netlist from an ASIC or FPGA	O	O	O	O	O
Red teaming	O	O	O	O	O
Circuit manipulation	O	O	O	O	O
Obsolescence management	O	O	O	O	O
Other (please specify):	O	O	O	O	O

2. How would you rate the **practical relevance** of protecting ICs against the following attack scenarios from 1 (not relevant) to 5 (very relevant)?

	1	2	3	4	5
Unauthorized overproduction by the foundry	O	O	O	O	O
Netlist recovery by a third party for purposes of plagiarism	O	O	O	O	O
Competitive analysis	O	O	O	O	O
Invasive attacks seeking to compromise security	O	O	O	O	O
Other (please specify):	O	O	O	O	O

3. How **common** do you think the following starting points are in a hardware reverse engineering project from 1 (very rare) to 5 (very common)?

	1	2	3	4	5
Analysis of an unknown ASIC	O	O	O	O	O
Analysis of an ASIC with available (developer) documentation, and/or information about the system that the IC is built into	O	O	O	O	O
Analysis of (parts of) a netlist, acquired from an ASIC or FPGA	O	O	O	O	O
Analysis of (parts of) a netlist, acquired from design files	O	O	O	O	O
Other (please specify):	O	O	O	O	O

4. How many **years of experience** do you have in…

	none	≤ 3	4-6	7-9	≥ 10
…designing / researching hardware?	O	O	O	O	O
…designing / researching hardware security mechanisms?	O	O	O	O	O
…hardware reverse engineering / failure analysis?	O	O	O	O	O
…developing tools or equipment for analyzing hardware?	O	O	O	O	O
…other (please specify):	O	O	O	O	O

If multiple apply per row, indicate the maximum

SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

THANK YOU

For your attention!

Please contact us:
Steffen.Becker@rub.de and
Rene.Walendy@rub.de

RUHR UNIVERSITÄT BOCHUM
RUB

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

HGI HORST GÖRTZ INSTITUT