SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

u^b
UNIVERSITÄT BERN

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

I SEE AN IC

A Mixed-Methods Approach to Study Human Problem-Solving Processes in Hardware Reverse Engineering

René Walendy | **Markus Weber** | Jingjie Li | Steffen Becker | Carina Wiesen | Malte Elson | Younghyun Kim | Kassem Fawaz | Nikol Rummel | Christof Paar

HARRIS 2024

March 20, 2024, Bochum, Germany

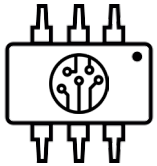
RUHR UNIVERSITÄT BOCHUM
RUB

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

HG HORST GÖRTZ INSTITUT

HARDWARE REVERSE ENGINEERING IS DRIVEN BY HUMANS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



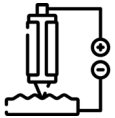
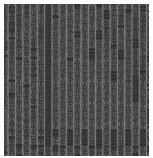
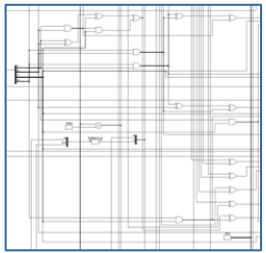


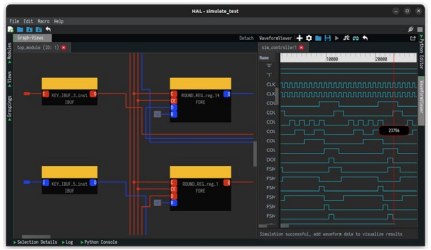
Image Acquisition



Netlist Recovery



Netlist Reversing

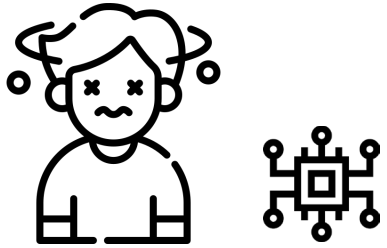


Successful Attack

Chemist icon by monkik on Flaticon
Cybersecurity attack and Analyzer icons by Freepik on Flaticon

BACKGROUND

- Reverse engineering calls for cognitive deduction, induction and creativity
  → special sort of problem solving
- A “best” strategy might not exist



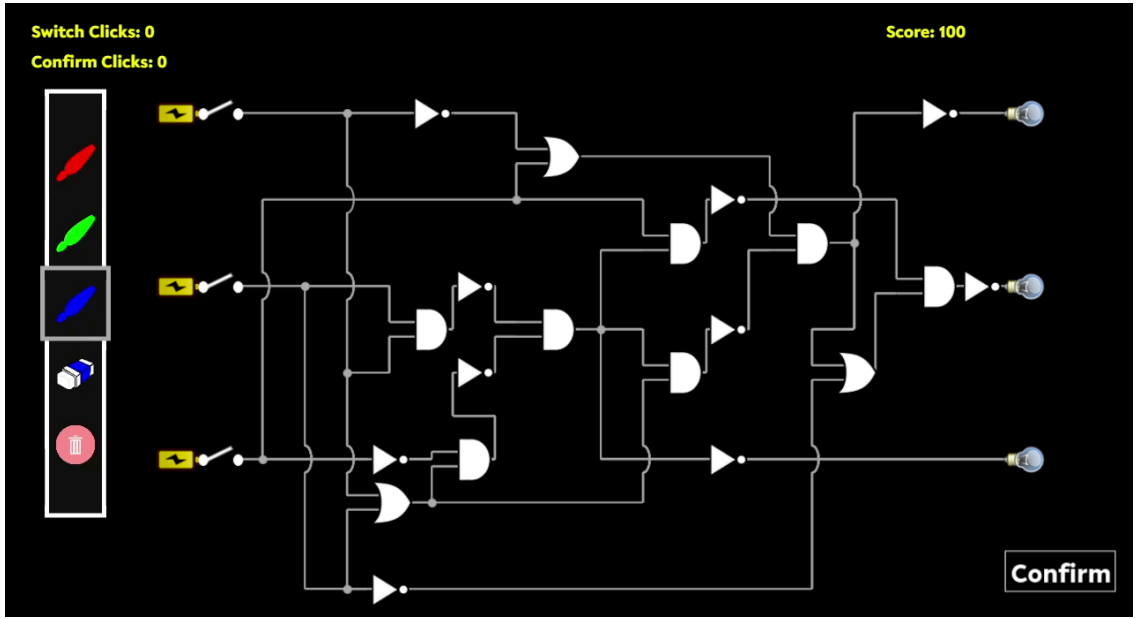
Our general assumption:
Find (cognitive) commonalities → develop (cognitive) obfuscation

N. Y. L. Lee and P. N. Johnson-Laird, “A theory of reverse engineering and its application to Boolean systems,” Journal of Cognitive Psychology, vol. 25, no. 4, pp. 365–389, 2013
C. Wiesen, S. Becker, R. Walendy, C. Paar, and N. Rummel, “The Anatomy of Hardware Reverse Engineering: An Exploration of Human Factors During Problem Solving,” ACM Trans. Comput.-Hum. Interact., vol. 30, no. 4, p. 62:1-62:44, 2023
Microchip and Confusion icons by Freepik on Flaticon

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

REVERSIM

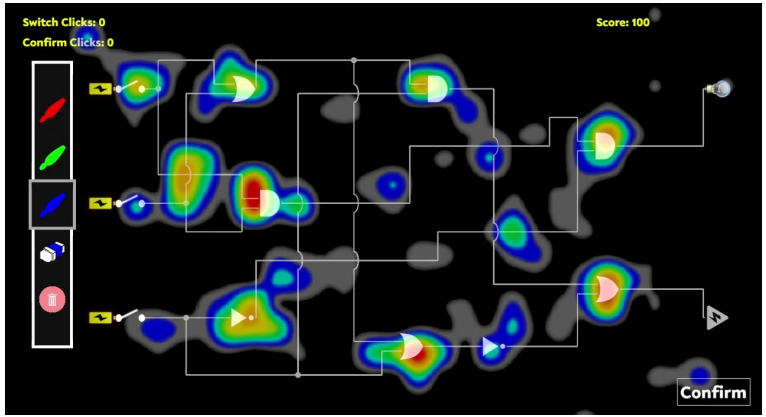
A Hardware Reversing Simulation



Becker, S., Wiesen, C., Walendy, R., Rummel, N., and Paar, C., "REVERSIM: A Game-Based Approach to Accessing Large Populations for Studying Human Aspects in Hardware Reverse Engineering", *arXiv e-prints*, 2023

METHODS TO CAPTURE HRE STRATEGIES

Eye Tracking



Verbal Thought Protocols

speculation backward tracking	286 287 288 289	So which means the output of the unknown gate needs. To be 0.
backward tracking	290 291	And uh, need to be 0.
validating	292 293	This is off.

Visualizations by krasvas/EyeMMV
Protocol listings by VERBI MAXQDA and emsec/maxqdapi

RESEARCH QUESTIONS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

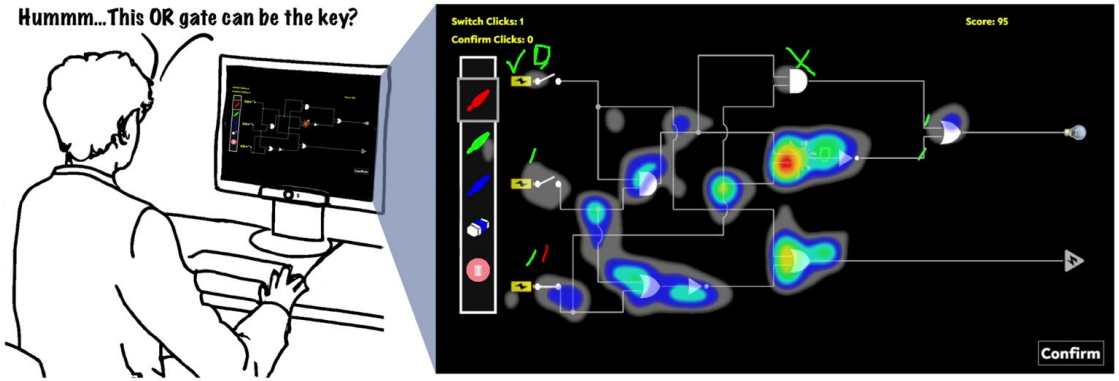
RQ1 - Can fixations obtained from **eye tracking** be used to observe behaviors within HRE problem solving?

RQ2 - How do Concurrent **Think Aloud** and Retrospective Think Aloud differ in revealing behaviors and approaches within HRE problem solving?

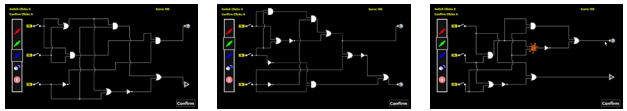
RQ3 - Does Concurrent Think Aloud **influence** participants' performance, user experience, or eye movement?

RQ4 - How can eye tracking and Think Aloud **complement** each other in describing HRE problem solving?

STUDY PROCEDURE



Think Aloud & Eye Tracking

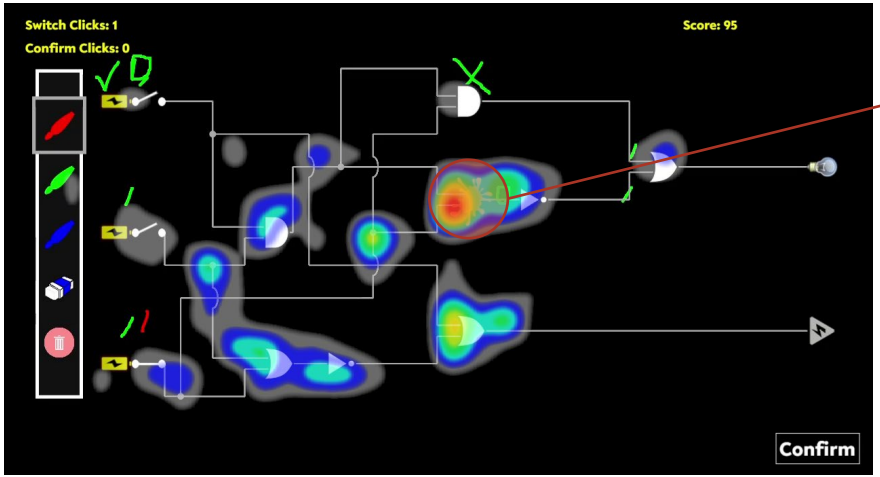
Demographics →  … → Post Survey

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Results

RQ1 – OBSERVING BEHAVIOR USING EYE TRACKING

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



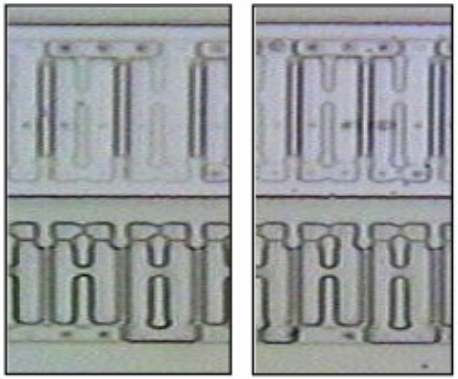
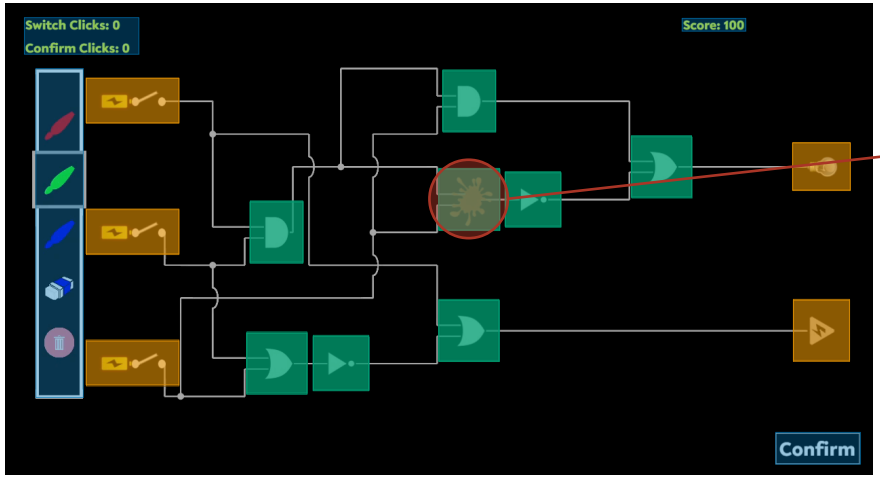


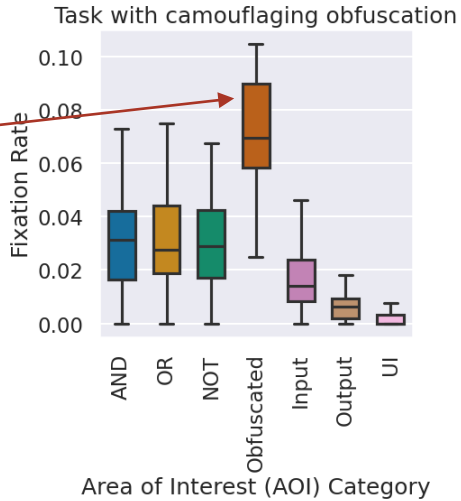
Figure 3. Camouflaged 2-input NAND (left) and NOR (right) gates, active layer

Remarkable
The camouflaged gate draws major attention

R. P. Cocchi, J. P. Baukus, L. W. Chow, and B. J. Wang, "Circuit Camouflage Integration for Hardware IP Protection," in Proceedings of the 51st Annual Design Automation Conference, in DAC '14. New York, NY, USA: Association for Computing Machinery, 2014

RQ1 – QUANTIFYING GAZE BEHAVIOR

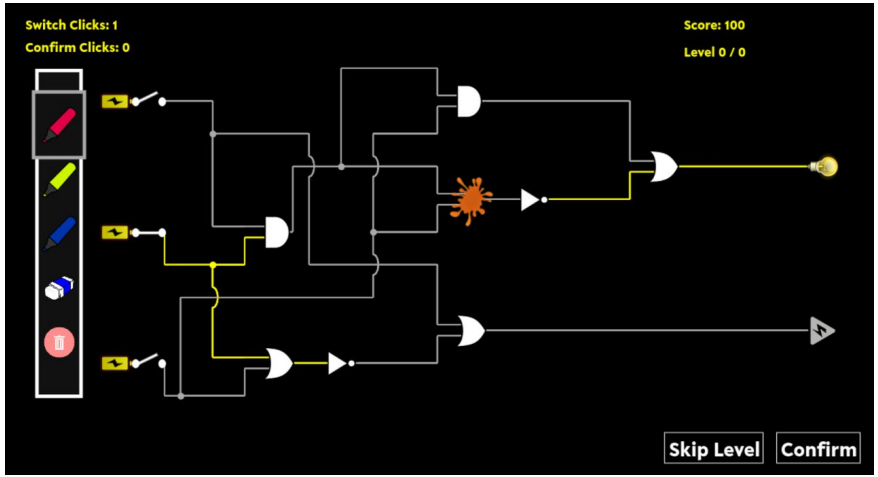


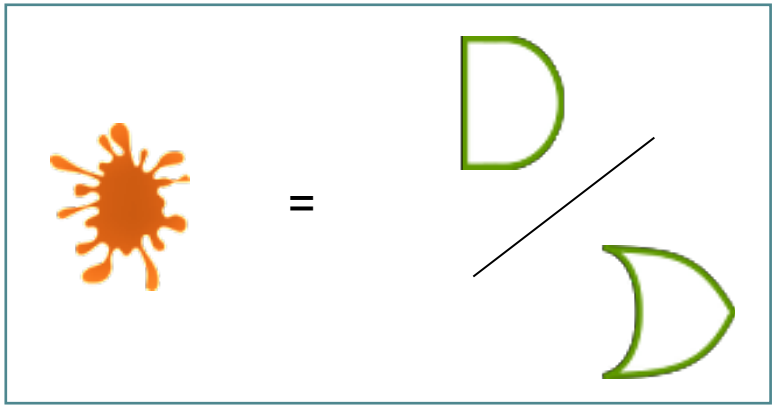


Remarkable

The camouflaged gate draws major attention
across all participants in our study

APPLICATION: DECOY OBFUSCATION





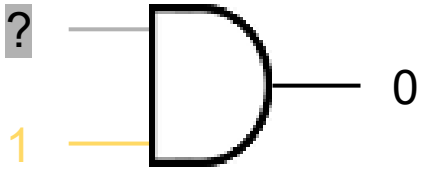
Remarkable

The camouflaged gate draws major attention across all participants in our study
despite being irrelevant for the solution!

RQ2,3 – TWO FUNDAMENTAL BEHAVIORS

Forward Tracking

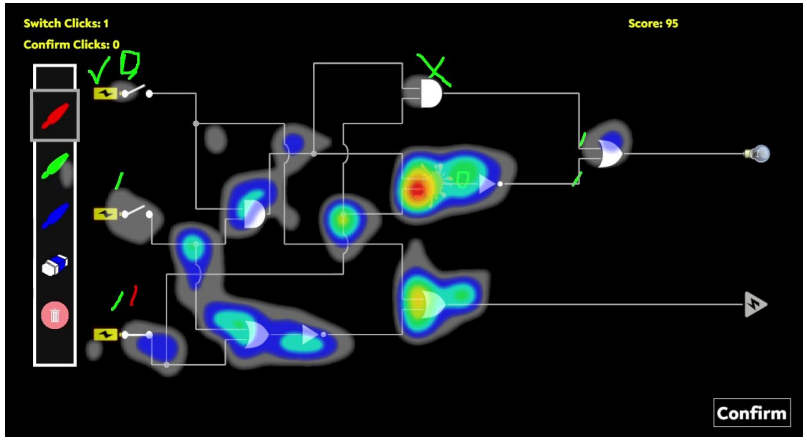
Backward Tracking



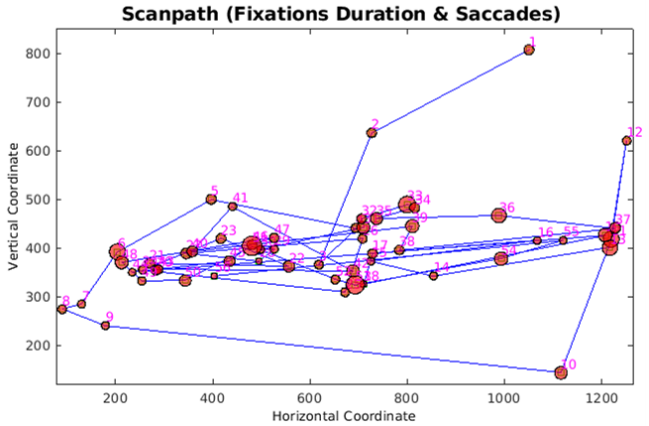
RQ4 – USING MIXED-METHODS TO DESCRIBE HRE STRATEGIES

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

From heatmaps …



… to scanpaths



Spatial Information

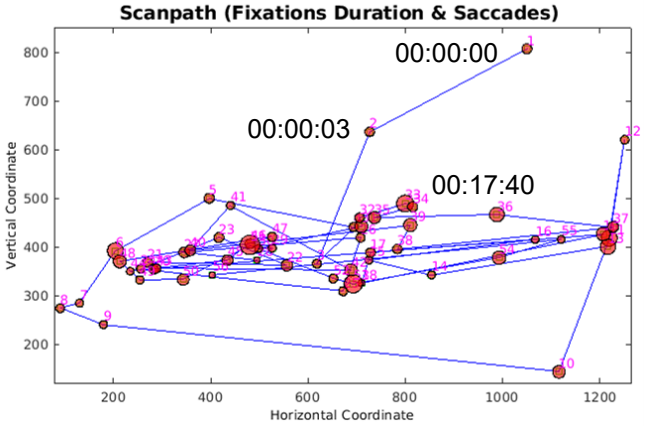
Temporal Information

Visualizations by krasvas/EyeMMV

RQ4 – USING MIXED-METHODS TO DESCRIBE HRE STRATEGIES

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Eye Tracking



Spatial Resolution
Temporal Resolution
Researcher Effort
Explanatory Power

Verbal Thought Protocols

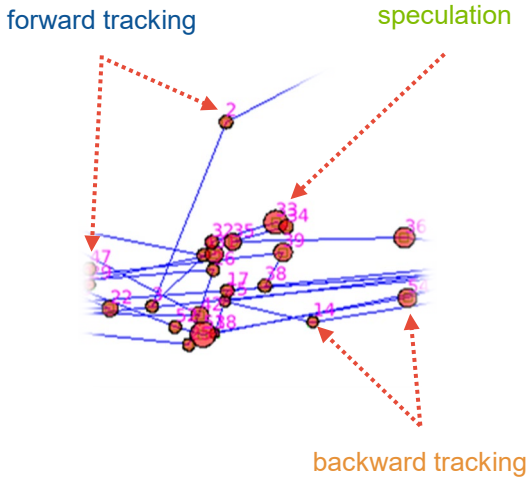
	286	00:17:42
speculation	287	So which means the output of the unknown gate needs.
backward tracking	288	00:17:45
	289	To be 0.
backward tracking	290	00:17:51
	291	And uh, need to be 0.
validating	292	00:18:02
	293	This is off.

Spatial Resolution
Temporal Resolution
Researcher Effort
Explanatory Power

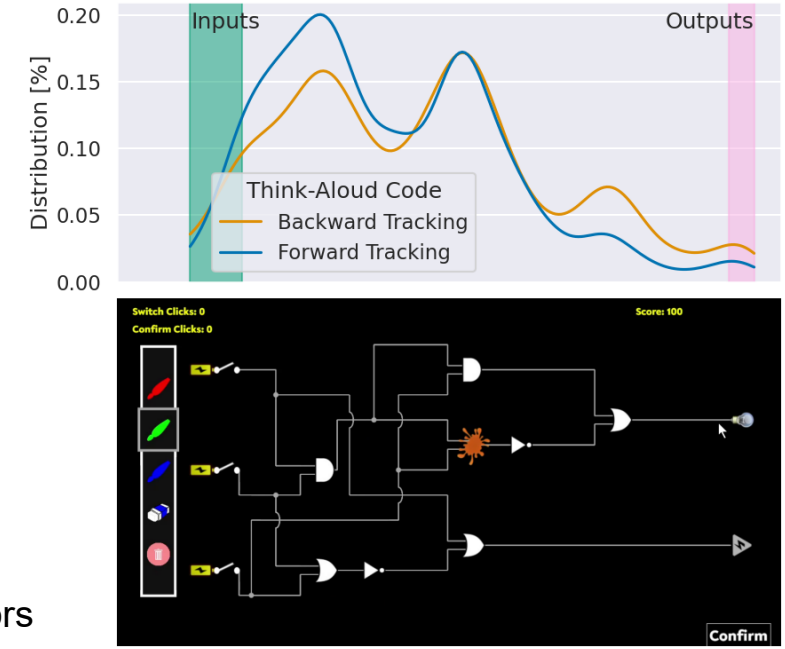
Visualizations by krasvas/EyeMMV
Protocol listings by VERBI MAXQDA and emsec/maxqdapi

RQ4 – USING MIXED-METHODS TO DESCRIBE HRE STRATEGIES

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



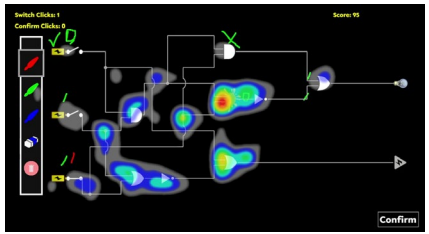
Kernel Density Estimation



Eye tracking and think aloud can correctly locate different reverse engineering behaviors

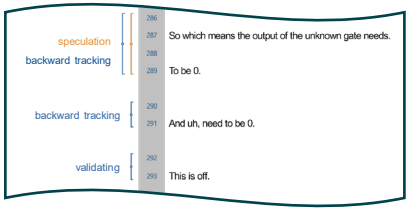
Bell Curve icon by Muhammad_Usman on Flaticon

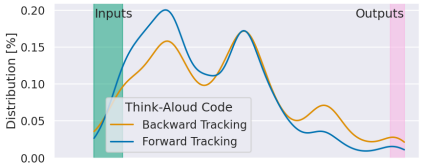
TAKEAWAYS



Eye tracking can tell us about attention when navigating a circuit, and discover what slows down reversing
→ *a quantitative method*

Verbal protocols allow deep insights into cognitive processes during reversing
→ *a qualitative method*





Combining both techniques can yield rapid insight into reversing approaches and obfuscation effectiveness
→ *a mixed-methods approach*

SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

UNIVERSITÄT
BERN

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

Thank you!

RUHR-UNIVERSITÄT BOCHUM
Horst-Görtz-Institut für IT-Sicherheit
Exzellenzcluster CASA
ID 2/150 | Universitätsstr. 150 | 44780 Bochum | Germany
www.casa.rub.de | www.hgi.rub.de

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR
UNIVERSITÄT
BOCHUM
RUB

HG HORST GÖRTZ INSTITUT