A Journey Towards Understanding the Human Aspects of Hardware Security

René Walendy[2], Steffen Becker[1,2], Nikol Rummel[1,3], and Christof Paar[2]

[1] Ruhr University Bochum, Bochum, Germany
[2] Max Planck Institute for Security and Privacy, Bochum, Germany
[3] Center for Advanced Internet Studies, Bochum, Germany

Abstract. As with much of security research, Hardware Reverse Engineering (HRE) has long been viewed as a purely technical field, where innovation occurs in algorithms and engineering. This technology-centric perspective was fundamentally challenged by Angela Sasse and collaborators, who established human-centered security as a rigorous research field. Motivated by this shift and curious about how humans *do* reverse engineering, nearly a decade ago we began investigating the human aspects of HRE. In this article, we recount our methodological journey and the empirical insights gained in developing a human-centric theory of HRE. Drawing on these experiences, we outline directions for future research into HRE and highlight considerations for adopting user-centric perspectives in other traditionally technical domains.

Keywords: Human-Centered Security · Hardware Security · Integrated Circuits · Hardware Reverse Engineering

1 The Human Terra Incognita of IC Reverse Engineering

Integrated Circuits (ICs) are the sophisticated building blocks that enabled the digital revolution and, in turn, today's digital society. Understanding their inner workings is referred to as Hardware Reverse Engineering (HRE), adapting the broader concept of reverse engineering [16] to semiconductors. For a long time, performing HRE was motivated by industry needs such as competitive analysis, patent infringement detection, and failure analysis. More recently, it has emerged as a crucial capability for maintaining digital sovereignty, e. g., for detecting malicious modules such as backdoors. Cases in point are the European Chips Act and the US CHIPS and Science Act, which represent massive investments to foster trust in ICs [7,17]. HRE was long assumed to be a purely technical undertaking drawing from areas such as VLSI design, semiconductor

analysis, computer graphics, and security engineering alone. Although tool developers acknowledged practical human aspects in interactive design [21], the broader research community marginalized such considerations as peripheral to the engineering challenge – a perspective reinforced by the inconsequential reception of Chisholm *et al.*'s [5] 1999 articulation of human creativity in IC analysis.

Around the same time, pioneering work by Angela Sasse and collaborators demonstrated that a purely technology-centric view of security was fundamentally incomplete. Challenging the prevailing tendency to frame users as the "weakest link" in secure systems, Sasse *et al.* showed that many security failures stem not from user shortcomings, but from systems that disregard human capabilities, limitations, and organizational context [1]. This line of work reframed security as a sociotechnical problem and articulated principles for designing security mechanisms that people can – and will – use effectively [19]. By establishing human-centered security as a rigorous and impactful research agenda, Sasse's work did more than reshape security engineering: it legitimized the study of human aspects as a first-class concern in security research and opened the door to interdisciplinary inquiry at the intersection of security, privacy, and HCI.

Following this line of thinking into hardware security, and building on more than two decades of technical work in this domain, our group began in 2017 to investigate how human cognitive abilities and problem-solving strategies shape success in HRE [8,3,29]. This shift was driven by the growing societal importance of trustworthy hardware and by the recognition that progress in HRE depends on approaches that span both hardware security and human cognition.

In this contribution, we reflect on our journey through this still largely uncharted research space. Section 2 recounts the development of a methodological framework for studying human aspects in HRE. Section 3 presents our central empirical findings and lays the foundation for an advanced theory of HRE centered on the human reverse engineer. Finally, Section 4 outlines future directions, including contextual inquiry and educational research, and draws broader lessons on conducting rigorous, interdisciplinary user-centric studies.

2 Act I: Equipping the Expedition

Our Embedded Security research group first touched the domain of circuit-level hardware security around 2009 [13]. Coming from designing cryptographic hardware, analyzing the security of third-party devices first necessitated the use of Hardware Reverse Engineering (HRE) [23,11]. What started as a means to understand those devices then progressed into advancing the field of HRE itself [20]. As we developed expertise in reverse engineering work and created the open-source HRE environment HAL [9,22], we recognized that some questions in HRE research lie beyond purely technical perspectives. Algorithmic solutions are essential tools for HRE. Yet, success ultimately depends on reverse engineers' deep technical knowledge, experience, and problem-solving skills [29]. Recognizing human aspects in HRE as an essential desideratum, we found ourselves in uncharted territory: At the boundary between Human Computer Interac-

tion (HCI), psychology, and engineering, no established methods existed for the empirical investigation of our research questions. The interdisciplinary research school SecHuman [10] gave us the opportunity, over the last decade, to explore this *terra incognita* of human aspects in HRE. The research school paired principal investigators from embedded security and educational psychology in an interdisciplinary project on the "Cognitive Aspects of Hacking." Drawing on early psychological theories of core HRE principles [12], this collaboration set out to characterize HRE as a cognitively demanding HCI process fundamentally driven by problem solving. With little prior art to guide us, our research approach was exploratory, hypotheses-generating, and empirical, while building the methodological vehicles iteratively along the way.

2.1 Designing a Training Vehicle for Skill Development

When we turned to hardware security experts for studies, our expedition hit its first major roadblock. HRE experts are scarce, and even acquaintances met us with skepticism: letting a psychology team peek into their minds? No, thanks – after all, guarding their skill sustains their livelihood. Recognizing that participants in this specialized domain would be hard to access, we began building our first methodological vehicle; a framework supporting our research for years.

At a large research university with a prominent IT security program, student participants were a natural fit for HCI research. However, to study real-world HRE behavior, we could not simply recruit from our Master's and advanced Bachelor's students. We therefore devised a specialized 14-week HRE course, teaching hardware architecture and design, and building skills to create, adapt, and apply HRE strategies. Our interdisciplinary team – combining technical HRE expertise with psychological theories of knowledge and skill acquisition – guided the course design [27]. In take-home projects, students used the HAL toolkit to inspect, understand, and manipulate large netlists. With extensive guidance at first, students progressed to planning and executing a reverse engineering project largely independently, reflecting real-world HRE scenarios [28].

Over eight years, the course has achieved two main objectives: First, it became – and remains – a highly valuable source of students trained in HRE, many of whom now participate in our empirical studies conducted using HAL. Second, the course addresses the long-term scarcity of HRE experts, with several alumni now holding positions in government and industry.

Studies conducted in the context of this HRE course produced qualitative temporal and hierarchical models of reverse engineering strategies [3,29], as well as early quantitative insights into how cognitive factors affect HRE efficiency [3]. We elaborate on these findings in Section 3.

2.2 Building a Test-Track Vehicle for Controlled Observation

After surveying human aspects of HRE in real-world settings and identifying key phenomena, we were ready to launch shorter, controlled, repeatable excursions for quantitative analysis. It was time to assemble a new methodological vehicle.

With ReverSim, we developed a browser-based study environment to model selected aspects of HRE for both lab and larger-scale online studies [2]. Focusing on sense-making in HRE, ReverSim observes how participants understand small Boolean logic circuits in a highly controlled setting. Participants solve a series of HRE puzzles of varying difficulty, while the environment records each step and timing for later analysis. To enable correlation of HRE performance with cognitive factors such as processing speed, ReverSim integrates online psychometric tests directly into the study flow without experimenter supervision. To address participant scarcity, we preface puzzles with an interactive tutorial introducing the necessary concepts of digital circuits, allowing participation with minimal prior knowledge in hardware. Crucially, no specific HRE strategies are provided, allowing participants' strategy development to emerge naturally.

While HAL and the HRE course provided nuanced insights into a wide range of strategies with a small set of participants, ReverSim places participants on carefully designed test tracks, enabling quantification in experimental and quasi-experimental settings with larger sample sizes. This controlled environment allows us to validate real-world, small-sample findings and to more precisely observe how cognitive factors affect HRE accuracy and speed.

2.3 Packing the Methodological Toolbox

With our two vehicles in place, it is worthwhile to examine the expedition's packing list: the methods and techniques we brought along. To understand how humans *do* HRE, observing or quantifying behavior was always central, often complemented by approaches characterizing the participants themselves. Choosing the right tools, however, was far from obvious. Our first experiments used think-aloud protocols with colleagues working on reverse engineering problems – yielding little insight into HRE but teaching us a valuable lesson about cognitive overload when participants must reverse engineer while verbalizing. This marked the start of a long process of selecting, designing, and rigorously evaluating a rich set of interdisciplinary quantitative and qualitative techniques.

From a qualitative perspective, we aimed to characterize the HRE process itself. Learning from our initial think-aloud attempts, we tailored our methods to minimize participant burden. Using HAL's instrumentation, we recorded screen captures as well as behavioral logs of circuit navigation and script editing, capturing rich data without disrupting workflow or increasing cognitive load. For analysis, we employed an iterative open coding approach [29] rooted in established principles of Grounded Theory.

While observing behavior reveals what participants do in HRE, it provides limited insight into their underlying reasoning. With ReverSim, we therefore revisited think-aloud protocols in a detailed methodological evaluation with more precisely controlled cognitive load [25]. Even with careful design, participants spoke significantly less under high cognitive load, reducing the value of concurrent think-aloud for content analysis. In contrast, *retrospective* think-aloud – asking participants to verbalize while watching a recording of their work – proved to be a highly effective alternative.

Building on our qualitative insights, we turned to psychometrics to systematically investigate and quantify how cognitive factors influence HRE performance. First, we defined performance metrics such as solution probability and speed. With HAL, measuring these metrics required manual annotation [3], whereas ReverSim records them automatically [2]. Naturally, careful task design is still necessary to avoid artifacts like ceiling or floor effects. Ultimately, both platforms enable researchers to relate HRE performance to established psychometric measures. For example, we have administered the Wechsler Adult Intelligence Scale (WAIS-IV) [26], focusing on perceptual reasoning, working memory, and processing speed sub-scales. As this test battery requires experimenter interaction and thus limits the feasible sample size, we recently developed unsupervised online adaptations, e. g., for the number connection test (ZVT, German: "Zahlen-Verbindungs-Test" [15]) assessing cognitive processing speed [2]. Finally, we have employed a range of survey-based measures, including the established Questionnaire on Current Motivation [18] and Perceived Task Difficulty Scale [4], as well as a custom scale measuring prior HRE knowledge [2]. Descriptive statistics, correlations, and significance testing have proven broadly useful, while ongoing work leverages multilevel modeling for more sophisticated experimental designs.

3 Act II: Exploration of Uncharted Space

With our methodological toolbox and study frameworks in place, we turned to exploring the behavioral aspects of HRE and how they are shaped by human cognition. While this research frequently leads to technical recommendations for improving hardware protection, our point of departure has consistently been the reverse engineer rather than the technology itself. Understanding human behavior is not a byproduct of this work, but its organizing principle.

Conceptualizing and embedding HRE in a broader context of psychological theory, we identified it as a type of problem solving that builds on both domain expertise and cognitive abilities, especially those related to intelligence [3,29], and which is particularly visually demanding [25]. This finding aligns with classical problem-solving research showing that cognitive ability, not just domain knowledge, determines performance in novel, complex tasks.

Our theoretical model is supported by a series of empirical correlates predicting HRE success. Observing students in our HRE course, we found a slight negative correlation between **Working Memory (WM)** scores and solution time in realistic HRE tasks: participants with above-average WM scores as measured by WAIS-IV solved the tasks more efficiently than those with lower scores [3].

Besides WM, we discovered that HRE performance depends on **cognitive processing speed**, the rate at which one can scan and sequence information without errors [27]. ReverSim studies replicated this measurement in a more controlled environment using the Zahlen-Verbindungs-Test (ZVT), identifying moderate positive correlations also with solution probability [2]. These correlations indicate that faster cognitive processing may not only predict faster reverse engineering, but also superior accuracy. Processing speed likely mediates the ef-

ficiency with which reverse engineers can acquire new circuit information, test hypotheses iteratively, and navigate between different levels of abstraction.

Beyond overall performance, we investigated the individual problem-solving strategies which reverse engineers apply. We found that strategies vary substantially between efficient and inefficient reverse engineers, with a three-phase model characterizing successful approaches [3]. In Phase 1, *Candidate Identification*, reverse engineers search for regions of interest and potentially relevant components. This phase is characterized by a high reliance on manual exploration, and ultimately yields initial hypotheses about the circuit. Phase 2, *Candidate Verification*, constitutes the most time-intensive and cognitively challenging segment. Here, reverse engineers narrow down their selection of target components, rejecting those which upon closer inspection are revealed as irrelevant. Combining manual inspection with targeted, script-based automation, they reason about and test their initial hypotheses, constructing the meaning of the unlabeled circuit. In the final Phase 3, *Realization*, they apply goal-oriented procedures to the targeted components, for instance, to build a more abstract high-level description, or perhaps to mount an attack on the circuit. This phase is heavily script-driven and relies only minimally on manual inspection. Across all phases, HRE success requires seamless interleaving of manual analysis and semi-automated steps. Manual analysis provides the initial spark for progress and helps generate hypotheses. Script-based automation allows testing hypotheses at scale, as well as aggregating and manipulating information across the broader circuit.

Our empirical observations suggest that the concrete solution strategies are highly individualized [29]. While there certainly exist inefficient strategies due to lack of understanding, poor planning, or even overly complex automation, we did not identify a single most efficient problem-solving strategy. How likely reverse engineers are to produce an efficient strategy depends, at least in part, on their level of expertise [29]. Comparing intermediates with an HRE expert, we observed substantial differences in their problem-solving approaches, which led the expert to the most time-efficient solution. The expert relied more heavily on small-step preparation, breaking down complex HRE problems into simpler sub-problems, and they supported their problem-solving process with frequent development of test cases, more so than most intermediate participants. We further noticed that the expert exhibited a higher level of programming experience, which contributed to their success with automated analyses. Intermediates compensated for their lower experience by outlining their approach in the form of code comments before implementation, allowing them to keep better track of their work. We suggest that overall, the expert's ability to activate a wealth of well-structured domain-specific knowledge enabled them to rapidly identify suitable sub-problems and select appropriate solution strategies.

An important distinction regarding the effect of prior experience is domain relevance. In a study of student performance on four realistic HRE tasks, we found that prior experience with the primary subject of each task was a significantly better predictor of performance than academic seniority [27]. Students self-rated their prior experience with topics such as Boolean algebra, Finite State

Machines (FSMs), symmetric cryptography, and Python programming on a 5-point Likert scale. We found that prior experience with FSMs and symmetric cryptography predicted significantly faster solution times specifically in FSM and cipher reverse engineering tasks, respectively. Conversely, performance did not differ significantly between undergraduate and graduate students.

Which cognitive mechanisms are the key drivers for this correlation between experience and performance is not yet well understood. Within ReverSim, we recently made first advances to this end. Comparing participants with very low self-reported prior knowledge to a sample scoring low to medium, we expectedly found that the more experienced sample generally outperforms novices in both solution time and probability. Strikingly, however, nuances emerge with increasing task complexity: While beginners' performance keeps steadily declining with complexity, intermediates' performance plateaus for the most complex tasks. We suggest that intermediates may have developed skills which help them process known structures within the circuits. Both pattern recognition and domain-specific heuristics may play a role in reducing cognitive load, giving intermediates a disproportionate advantage over novices in these complex tasks.

Our empirical findings jointly lead to an advanced theory of HRE beyond a procedural, technical description. In summary, we found that HRE comprises aspects of both simple and complex problem-solving. Superior performance is a function of domain-relevant expertise and general cognitive abilities, particularly Working Memory (WM) and processing speed. Given the influence of expertise and WM, we hypothesize that **chunking** [14] may be one of the concrete mechanisms defining reverse engineers' cognitive limitations. For a novice reverse engineer inspecting a circuit diagram, visual working memory capacity may dictate the number of components that they can consider and place into context simultaneously. As they gain experience, reverse engineers may learn to mentally encode common sub-structures within a circuit, rather than individual gates. Although their Working Memory has not grown larger, they can consider a broader, more complex section of the circuit at reduced cognitive load. Thus, more capacity is freed up to drive reasoning processes crucial for problem solving.

4 Epilogue: From Exploration to Charted Routes

4.1 Research Outlook in Hardware Reverse Engineering

Having explored the *terra incognita* of human aspects in HRE, the next step is to move from exploration to systematic hypothesis testing.

One particularly promising domain for such work is *hardware obfuscation*. Techniques such as camouflaged logic gates [6] aim to hinder reverse engineering by obscuring Boolean functionality and introducing uncertainty into circuit representations. If chunking is indeed an essential cognitive component in HRE, embedding camouflaged elements into otherwise familiar structures should erode experts' advantages, forcing a reversion to cognitively demanding strategies. This perspective naturally aligns with the notion of *cognitive obfuscation*.

Beyond obfuscation, we see further directions for research. First, after abstracting real-world HRE into student-based studies with HAL and controlled experiments with ReverSim, a crucial step is to reconnect these findings with real-world practice. We therefore aim to study the lived experiences of industry reverse engineers through contextual inquiry, examining characteristics of expertise, work practices, and knowledge acquisition in situ. Linking these insights with academic models may inform new ways of supporting both researchers and practitioners in addressing technical and human-centered HRE challenges alike. Second, a mature theory of HRE can directly inform education. Despite high demand for reverse engineers, formal HRE courses remain rare [24]. Over the past decade, the community has proposed technical taxonomies of procedures and strategies [29], developed open tooling [22], and gained insight into cognitive mechanisms, expertise development, and human limitations in HRE. Together, these foundations offer fertile ground for evidence-based curricular design and scalable training for the next generation of hardware security professionals.

4.2 Considerations for User-Centric Research

Reflecting on our work on human aspects of HRE, we conclude with observations that may be relevant to user-centric research beyond this domain. In traditionally engineering-driven fields, user research is particularly valuable, as technology invariably is designed, shaped, and used by humans within specific contexts. Empirical research methods – qualitative and quantitative alike – can reveal important insights into these sociotechnical dynamics. Sasse *et al.* 's pioneering work was influential not only in methodological terms, but also in legitimizing interdisciplinary research on human-centered security. By demonstrating that such inquiry can be both rigorous and impactful, it lowered barriers for engaging with human aspects of technical systems. We therefore encourage applying these principles to other sociotechnical domains where human factors remain underexplored. While early efforts may appear "messy" – especially for technically trained researchers – the insights gained can be substantial.

Research at the intersection of technical and human-centered inquiry typically spans disciplines and lacks shared standards or best practices. Assembling and applying interdisciplinary methods therefore requires close collaboration, openness, and sustained effort to build shared understanding. When successful, such collaboration enables insights unlikely to emerge within disciplinary silos and may open new directions for research.

Acknowledgments. We thank Carina Wiesen and Markus Weber for being the key companions on this expedition and for their outstanding contributions throughout. We are grateful to Marc Fyrbiak, Sebastian Strauß, Malte Elson, Nils Albartus, Max Hoffmann, and Julian Speith for their continued collaboration – equal parts co-authors, sparring partners, and reliable navigators when the trail got steep. We also thank Zehra Karadağ, Jannik Schmöle, and Sarah Naqvi for their excellent support as student assistants – our capable ground crew who kept the day-to-day logistics running and ensured that the expedition could actually move forward. We acknowledge the SecHuman graduate school for providing the base camp and interdisciplinary setting that made this

line of work possible. This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972, and by the Research Center Trustworthy Data Science and Security, one of the Research Alliance Centers within the UA Ruhr.

References

1. Adams, A., Sasse, M.A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999). https://doi.org/10.1145/322796.322806
2. Becker, S., Walendy, R., Weber, M., Wiesen, C., Rummel, N., Paar, C.: ReverSim: An Open-Source Environment for the Controlled Study of Human Aspects in Hardware Reverse Engineering. In: Proc. of the CHI Conference on Human Factors in Computing Systems. CHI '25, ACM, New York, NY, USA (2025). https://doi.org/10.1145/3706598.3714160
3. Becker, S., Wiesen, C., Albartus, N., Rummel, N., Paar, C.: An exploratory study of hardware reverse engineering technical and cognitive processes. In: Proc. of the Sixteenth USENIX Conference on Usable Privacy and Security. pp. 285–300. SOUPS'20, USENIX Association, USA (2020), https://www.usenix.org/conference/soups2020/presentation/becker
4. Bratfisch, O., et al.: Perceived item-difficulty in three tests of intellectual performance capacity (1972)
5. Chisholm, G., Eckmann, S., Lain, C., Veroff, R.: Understanding integrated circuits. IEEE Design & Test of Computers **16**(2), 26–37 (April-June/1999). https://doi.org/10.1109/54.765201
6. Cocchi, R.P., Baukus, J.P., Chow, L.W., Wang, B.J.: Circuit Camouflage Integration for Hardware IP Protection. In: Proc. of the 51st Annual Design Automation Conference. pp. 1–5. DAC '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2593069.2602554
7. European Parliament and Council: EU regulation 2023/1781 (chips act) on strengthening europe's semiconductor ecosystem (2023), http://data.europa.eu/eli/reg/2023/1781/oj/eng
8. Fyrbiak, M., Strauß, S., Kison, C., Wallat, S., Elson, M., Rummel, N., Paar, C.: Hardware Reverse Engineering: Overview and Open Challenges. In: 2017 IEEE 2nd International Verification and Security Workshop (IVSW). vol. 557, pp. 88–94. IEEE, Thessaloniki, Greece (2017). https://doi.org/10.1109/IVSW.2017.8031550
9. Fyrbiak, M., Wallat, S., Swierczynski, P., Hoffmann, M., Hoppach, S., Wilhelm, M., Weidlich, T., Tessier, R., Paar, C.: HAL—The Missing Piece of the Puzzle for Hardware Reverse Engineering, Trojan Detection and Insertion. IEEE Trans. on Dependable and Secure Computing **16**(3), 498–510 (2019). https://doi.org/10.1109/TDSC.2018.2812183
10. Hielscher, J., Menges, U., Lassak, L., Püschel, H., Skrebec, O., Utz, C.: Interdisciplinary Human-Centered Security Research: Learning From Opportunities and Challenges of a German Graduate Program. In: Symposium on Usable Privacy and Security (SOUPS) (2023), https://www.usenix.org/conference/soups2023/presentation/hielscher-poster
11. Kison, C., Frinken, J., Paar, C.: Finding the AES Bits in the Haystack: Reverse Engineering and SCA Using Voltage Contrast. In: Cryptographic Hardware and Embedded Systems – CHES 2015. pp. 641–660. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48324-4_32

12. Lee, N.L., Johnson-Laird, P.: A theory of reverse engineering and its application to boolean systems. Journal of Cognitive Psychology **25**(4), 365–389 (2013)
13. Lin, L., Kasper, M., Güneysu, T., Paar, C., Burleson, W.: Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering. In: Proc. of the 11th International Workshop on Cryptographic Hardware and Embedded Systems. pp. 382–395. CHES '09, Springer-Verlag, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04138-9_27
14. Miller, G.A.: The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review **63**(2), 81–97 (1956). https://doi.org/10.1037/h0043158
15. Oswald, W.D.: Zahlen-Verbindungs-Test ZVT. 3. Auflage. Hogrefe (2016)
16. Rekoff, M.G.: On reverse engineering. IEEE Transactions on Systems, Man, and Cybernetics **15**(2), 244–252 (1985). https://doi.org/10.1109/TSMC.1985.6313354
17. Rep. Ryan, T.: H.R.4346 - 117th Congress (2021-2022): Chips and Science Act (2022), https://www.congress.gov/bill/117th-congress/house-bill/4346/text
18. Rheinberg, F., Vollmeyer, R., Burns, B.: QCM: A questionnaire to assess current motivation in learning situations. Diagnostica **47** (2001)
19. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal **19**(3), 122–131 (2001). https://doi.org/10.1023/A:1011902718709
20. Schellenberg, F., Finkeldey, M., Richter, B., Schäpers, M., Gerhardt, N., Hofmann, M., Paar, C.: On the Complexity Reduction of Laser Fault Injection Campaigns Using OBIC Measurements. In: 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography. pp. 14–27 (2015). https://doi.org/10.1109/FDTC.2015.10
21. Schobert, M.: Interactive Functions of the Degate Software Package (2012), https://github.com/nitram2342/degate/blob/master/doc/degate_rough_translation_of_appendix_a.pdf
22. Speith, J., Langheinrich, J., Fyrbiak, M., Hoffmann, M., Wallat, S., Klix, S., Albartus, N., Walendy, R., Becker, S., Paar, C.: HAL – An Open-Source Framework for Gate-Level Netlist Analysis (2025). https://doi.org/10.48550/arXiv.2512.14139
23. Strobel, D., Driessen, B., Kasper, T., Leander, G., Oswald, D., Schellenberg, F., Paar, C.: Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System. In: CRYPTO 2013. pp. 147–164. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40041-4_9
24. Walendy, R., Weber, M., Becker, S., Paar, C., Rummel, N.: An Evidence-Based Curriculum Initiative for Hardware Reverse Engineering Education. In: Proc. of the 56th ACM Tech. Symposium on Computer Science Education V. 1. pp. 1176–1182. ACM, New York, NY, USA (2025), https://doi.org/10.1145/3641554.3701797
25. Walendy, R., Weber, M., Li, J., Becker, S., Wiesen, C., Elson, M., Kim, Y., Fawaz, K., Rummel, N., Paar, C.: I see an IC: A Mixed-Methods Approach to Study Human Problem-Solving Processes in Hardware Reverse Engineering. In: Proc. of the CHI Conference on Human Factors in Computing Systems. pp. 1–20. CHI '24, ACM, New York, NY, USA (2024). https://doi.org/10.1145/3613904.3642837
26. Wechsler, D.: Wechsler Adult Intelligence Scale–Fourth Edition (2008). https://doi.org/10.1037/t15169-000
27. Wiesen, C., Becker, S., Albartus, N., Paar, C., Rummel, N.: Promoting the Acquisition of Hardware Reverse Engineering Skills. In: 2019 IEEE Frontiers in Ed-

ucation Conference (FIE). pp. 1–9. IEEE, Covington, KY, USA (2019). https://doi.org/10.1109/FIE43999.2019.9028668
28. Wiesen, C., Becker, S., Fyrbiak, M., Albartus, N., Elson, M., Rummel, N., Paar, C.: Teaching Hardware Reverse Engineering: Educational Guidelines and Practical Insights. In: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp. 438–445. IEEE, Wollongong, NSW (2018). https://doi.org/10.1109/TALE.2018.8615270
29. Wiesen, C., Becker, S., Walendy, R., Paar, C., Rummel, N.: The Anatomy of Hardware Reverse Engineering: An Exploration of Human Factors During Problem Solving. ACM Transactions on Computer-Human Interaction **30**(4), 62:1–62:44 (2023). https://doi.org/10.1145/3577198