Promoting the Acquisition of Hardware Reverse Engineering Skills

Carina Wiesen[1,2], Steffen Becker[2], Nils Albartus[2], Christof Paar[2], and Nikol Rummel[1,2]
[1]*Institute of Educational Research* and [2]*Horst Görtz Institute for IT Security*
Ruhr University Bochum
Bochum, Germany
{carina.wiesen, steffen.becker, nils.albartus, christof.paar, nikol.rummel}@rub.de

***Abstract*—This full research paper focuses on skill acquisition in Hardware Reverse Engineering (HRE) – an important field of cyber security. HRE is a prevalent technique routinely employed by security engineers (i) to detect malicious hardware manipulations, (ii) to conduct VLSI failure analysis, (iii) to identify IP infringements, and (iv) to perform competitive analyses. Even though the scientific community and industry have a high demand for HRE experts, there is a lack of educational courses. We developed a university-level HRE course based on general cognitive psychological research on skill acquisition, as research on the acquisition of HRE skills is lacking thus far. To investigate how novices acquire HRE skills in our course, we conducted two studies with students on different levels of prior knowledge. Our results show that cognitive factors (e.g., working memory), and prior experiences (e.g., in symmetric cryptography) influence the acquisition of HRE skills. We conclude by discussing implications for future HRE courses and by outlining ideas for future research that would lead to a more comprehensive understanding of skill acquisition in this important field of cyber security.**

***Index Terms*—skill acquisition in cyber security, hardware reverse engineering**

I. Introduction

In an increasingly digital world, individuals, industry, and governments wrestle with major cyber-security challenges posed by numerous and increasingly frequent cyber attacks at the hardware, software, and network level. Hardware components serve as the basis of trust in virtually any computing system by ensuring its security, integrity, and reliability. Due to the globalized fabrication processes through which they are produced, however, Integrated Circuits (ICs) are vulnerable to attacks such as malicious manipulations or the insertion of hardware Trojans [1], [2]. The deployment of manipulated hardware chips in critical infrastructure such as cellular networks and power grids or in sensitive applications (e.g., aerospace or military) is a major concern for a wide array of stakeholders [3], [4].

A common method to detect such malicious manipulations in ICs is called Hardware Reverse Engineering (HRE). *Reverse engineering* can be described as the process of retrieving information from anything man-made to understand its inner structures and workings [5]. HRE is a multi-layered process which facilitates the security inspection of an (unknown) hardware design [6]. Specifically, HRE is employed for the purpose of Very-Large-Scale Integration (VLSI) failure analysis, detecting counterfeits, identifying IP violations, and searching for potentially implanted backdoors and hardware Trojans [7]. At the same time, malign actors can utilize HRE for illegitimate purposes such as IP fraud or the insertion of backdoors or hardware Trojans.

The continuous evolution of a digital society shaped by a rapidly expanding Internet of Things (IoT) and the proliferation of cyber-physical systems have created a high demand for security experts with a solid background in HRE. Nevertheless, there is an almost complete lack of educational courses in the HRE field and HRE training happens almost entirely on the job [8]. We developed an HRE course based on cognitive psychological research on skill acquisition, as research on the acquisition of HRE skills is lacking thus far. The course was first offered at a German university during the 17/18 winter term. The second iteration of the course was introduced at one German and one North American university during the 18/19 winter term. In order to evaluate if our course actually enables HRE skill acquisition, we conducted two studies with students on different levels of prior knowledge in relevant topics. We argue that research on HRE skill acquisition and how to best foster it through educational courses is essential for enhancing the development of future university-level programs and for addressing the high and unmet demand of HRE experts.

We aim to observe if students of our course are able to acquire HRE skills by taking a first step towards closing the research gap of understanding how HRE skills are acquired. Our research will help to define future goals for teaching and learning in this specific field of cyber security.
In summary, our contributions are to:

- Illustrate the current lack of research on how skills in this important field of cyber security are acquired.
- Provide an overview of prior research from cognitive psychology on the acquisition of skills.
- Develop a course based on the findings from cognitive psychology to enhance skill acquisition in HRE.
- Observe and evaluate if our course enables students to acquire HRE skills. Therefore, we present our two studies by formulating research questions, expound upon our study design and methods, and present the results of our examination.

This work was supported in part through DFG Excellence Strategy grant 39078197 (EXC 2092, CASA), ERC grant 695022 and NSF grant CNS-1563829.

- Discuss the findings of our research on HRE skill acquisition by evaluating our course design and by providing recommendations for future courses and research studies.

II. Background

A. Hardware Reverse Engineering

The term *reverse engineering* refers to the processes of extracting knowledge or design information from anything man-made in order to comprehend its inner structure [5]. In the context of hardware security [9], security engineers (as well as malicious actors) are forced to employ different techniques to extract a gate-level netlist from a given IC or Field Programmable Gate Array (FPGA). The analysis of the gate-level netlist marks the crucial step of HRE enabling human reverse engineers to make sense of an unknown hardware design (e.g., to identify security vulnerabilities or security-circuitry for Trojan insertion [10]) [6]. In the following we define the term gate-level netlist reverse engineering as an important cyber security skill. Additionally, we outline the current lack of research on HRE skill acquisition.

1) Gate-level Netlist Reverse Engineering: During the hardware design process, synthesis tools convert Register Transfer Level (RTL) descriptions of hardware designs into representations of the (Boolean) logic gates of the target gate library and their connectivity [11]. Such representations are called gate-level netlists.

During the different synthesis steps, valuable high-level information such as (1) meaningful descriptive information (e.g., names and comments), (2) boundaries of implemented modules, and (3) module hierarchies is lost. In practice, this loss of information highly complicates the reverse engineering process [12].

In real-world settings, analysts can obtain gate-level netlists in several scenarios: (1) through chip-level reverse engineering in the case of a given IC (involving steps such as (i) decapsulation, (ii) delayering, (iii) image acquisition, and (iv) image processing) [7]; (2) through bitstream reverse engineering in the case of FPGAs (involving steps such as (i) bitstream extraction or interception, (ii) bitstream file format reversing, and (iii) bitstream conversion) [13]; or (3) by direct access at a foundry or through bribery or theft.

Human analysts conducting gate-level netlist reverse engineering are often supported by semi-automatable tools that enable algorithmic graph-based and machine learning methods as well as allow for detailed visual inspection for the purpose of structural and functional analyses [12], [14]. Since no fully automated tools for HRE exist, human engineers are always involved in the process of gate-level netlist reversing.

2) Lack of Research on HRE Skill Acquisition: HRE specialists need to draw upon knowledge from various domains including chip design and manufacturing, image processing and machine learning techniques, Boolean algebra, graph theory, custom tooling, programming languages, Hardware Description Languages (HDLs), computer architectures, cryptography, and cryptanalysis. There are currently very few trained HRE specialists, and due to the lack of educational courses in the field, most have acquired their skills through on-the-job-training or even through their free time pursuits as hobbyists. This ad-hoc training situation is unsatisfactory since there is growing demand in industry and government agencies for HRE specialists, which should be met by structured university-level courses. Therefore, we developed an HRE course which is based on cognitive psychology, since research on the acquisition of HRE skills is missing. In the following, we first address relevant aspects of psychological research on skill acquisition. Second, we apply the psychological research findings in order to develop and present the HRE course design.

B. Psychological Background

Even though industry and the scientific community have a high demand for engineers with HRE expertise, there is a lack of systematic research on the acquisition of HRE skills. We are aware of one relevant prior work on human factors in reverse engineering [15]. The authors focused on exploring human problem-solving processes in reverse engineering of simple Boolean systems in an artificial laboratory setting. Thus, this prior work does not compare to HRE practice. Additionally, the authors did not include research on skill acquisition processes. In the following sections, we present relevant psychological literature on skill acquisition which build the foundation of our HRE course design.

1) Skill Acquisition: According to the Adaptive Control of Thought-Rational (ACT-R) [16], knowledge is represented in two ways [17]: *Declarative* knowledge which consists of facts (e.g., the control path is operationalized as a Finite State Machine (FSM)), and *procedural* knowledge which consists of mappings of stages to actions (e.g., if the goal is to find an FSM, then search for strongly connected components in the netlist). ACT-R includes assumptions about transferring declarative knowledge (*knowing that*) into procedural knowledge (*knowing how*): knowledge is first acquired declaratively, and afterwards transformed into a procedural form [18].

The acquisition of declarative (verbal) and procedural (non-verbal) knowledge is supported by various learning processes [19]. These in turn can be reinforced through specific forms of instruction and course structure [19], which we incorporated into the design of our HRE tasks (see Section III). In the following, we briefly describe the learning processes for declarative and procedural knowledge.

First, *understanding and sense-making processes* involve verbally-mediated and explicit processes in which students attempt to understand and reason. Understanding and sense-making processes are more deliberate, since students need to actively engage in understanding and reasoning [19]. Second, *memory and fluency-building processes* are defined as non-verbal learning processes which involve strengthening memory and compiling knowledge [19]. Fluency building enables solving tasks and problems more efficiently, since knowledge is more strongly composed and automatically accessible [20] [21]. Prior research has shown that people speed up with practice [17]. In this context, the psychological construct behind "speeding up" is called fluency which is defined as the ability to

quickly and accurately solve a problem [22]. Prior findings have shown that students with high scores in fluency maintain their skills over time [20] and perform better on more complex tasks than students with lower fluency [21]. Third, *induction and refinement processes* are non-verbal processes and improve the accuracy of knowledge through generalization, categorization, discrimination, or causal induction [19].

Additionally, individual differences and abilities (e.g., intelligence) play an important role in the development of broad and complex skills [23]. Furthermore, motivation is often described as a central driver of devoting years to deliberate practice and learning [24]. A high level of motivation leads to more cognitive engagement, more learning, and higher levels of achievement [25], and is therefore relevant to the development of a course on HRE which supports students' learning processes.

In the following section, we use concepts described in existing literature on skill and knowledge acquisition and instructional principles which support these learning processes [19] to describe the design of our course in HRE.

2) Psychological Research as the Foundation for HRE Course Design: With the goal of designing the course to enhance the acquisition of HRE skills, we acknowledged the distinction between declarative and procedural knowledge acquisition by assuming that knowledge is first acquired declaratively, and is then transformed into a procedural form [16] [18]. Practically, we divided the course into a lecture phase (acquisition of declarative knowledge) and a practical phase (transformation into procedural knowledge). We developed the learning materials for and instructional principles behind the two phases based on verbally-mediated and non-verbal learning processes as proposed in [19]. Additionally, we considered potential influences upon student motivation as described in the following section.

3) Lecture Phase: During the first six weeks of the course, students acquire declarative knowledge. This phase focuses on the acquisition of verbally-mediated facts, theories, and concepts related to the relevant fields of electrical engineering, Boolean algebra, and graph theory through two 90-minute lectures and one homework assignment per week. We apply the instructional principles of Prompted Self-Explanation [19] and Accountable Talks [26] [19] to support the learning processes of *understanding and sense making* (Section II-B1). We achieve robust learning of declarative knowledge through the integration of verbally-mediated exercises which encourage students to explain the steps of Worked Examples of HRE to themselves and to share their solutions with other students in accountable discussions in tutorial sessions.

4) Practical Phase: Following the lecture phase, students participate in an eight-week practical study consisting of four HRE problems (detailed descriptions in Section III). Our decision to organize the course in two phases reflects our assumption that the declarative knowledge imparted during the lecture phase is transformed into practical knowledge through the non-verbal learning processes of the practical phase. To support non-verbal *memory and fluency-building processes* (Section II-B1), we leverage the instructional principle of Spacing and Testing [27] [19] by directing students to practice recalling target task material over longer time intervals (two weeks per project) to enhance their long-term retention and improve their fluency in solving HRE problems.

Additionally, we include non-verbal processes that are associated with the *induction and refinement processes* (Section II-B1), through the incorporation of Worked Examples [28] [19] into the curriculum as students learn more robustly from tasks which are interleaved with problem solving practice [19].

In summary, we designed the HRE course based on general cognitive psychological research on skill acquisition, which is supported by certain types of instructions and assignments as described. Since motivation is a central factor, we also took intentional steps to bolster student motivation in our course design as described in the following.

5) Supporting Students' Motivation in HRE Course: Since motivation is a key element in learning (Section II-B1), we employed the following design principles in our course to enhance students' motivation. In cases where higher levels of motivation are associated with greater cognitive engagement and learning [25] [24], tasks and materials must cater to both personal and situational interest. The HRE tasks we present in the practical phase are stimulating and engaging exercises which are both novel and touch upon a variety of real-world challenges encountered in HRE practice (e.g., finding control logic, retrieving a cryptographic key, etc.). The integration of the HRE software HAL into the course helps students learn HRE processes through the use of realistic graphical representations [8] which should in turn lead to growing interest and involvement. By providing authentic HRE tasks and making connections to students' intended profession, the course design supports an increase in the perceived value of the learning experience which again leads to enhanced motivation [29]. Students who believe they are able to solve a task are more highly motivated in terms of effort and persistence [25]. Thus, it is important to include tasks which are on an appropriate level of difficulty and allow students to use their prior knowledge and skills. We consequently designed the tasks within the project phase to fall within the range of competence achieved by the conclusion of the lecture phase.

In summary, HRE is important in the field of cyber security and specialists with HRE skills are in great demand. In addition to the lack of HRE experts, there is also a lack of educational university-level HRE programs. Thus, we developed a HRE course by referring to prior cognitive psychological research, since research on the acquisition of HRE skills cannot be found. In order to evaluate the effects of our course design on HRE skill acquisition, we run two studies with participants on different levels of prior knowlegde. In the following, we present our research methods and materials.

III. Methods

A. Research Questions

To observe participants' skill acquisition as well as correlations with motivational and cognitive factors, we formulated the following research questions:

1) Does students' performance in solving HRE tasks improve with increasing experience?
   a) Does increasing experience result in students needing less time to solve HRE tasks?
   b) Do students exhibit a higher probability of solving HRE tasks as their experience grows?
2) Are there differences between students with different levels of expertise (undergraduate and graduates) regarding the hypothesized improvements?
3) Do the hypothesized improvements relate to particular aspects of intelligence and related cognitive abilities (e.g., processing speed), or prior experiences in relevant topics?

B. Participants

The first study was conducted at a North American university with 20 students (mean age $M = 23.5$, $SD = 2.3$; 9 undergraduates) who were enrolled in programs in electrical engineering or computer science. The ethics board approved the study. The second study was conducted at a German university with 18 participants (mean age $M = 23.1$, $SD = 1.8$; 9 undergraduates) who studied cyber security or electrical engineering. The institutions were chosen based on their strong programs in cyber security, and computer engineering. Five participants were excluded because they did not complete all the tasks and the amount of data was not sufficient for analyses. Both studies were conducted in winter term of 18/19. In both studies, participants provided written informed consent and received monetary compensation for spending time on answering study related surveys and tests. We ensured privacy by randomly assigning pseudonyms to the participants of both studies. These pseudonyms were consistently used throughout all materials and procedures regarding the two studies.

C. Materials

1) Educational Environment: The HRE framework HAL [30], [31] served as the underlying educational environment for the projects of the practical phase. HAL assists users in the reverse engineering of complex gate-level netlists and its extensibility allows for the development of custom plugins. In particular, HAL employs an interactive Graphical User Interface (GUI) to provide both textual and graph-based representation of the netlist under inspection. While the graph-based representation allows for detailed manual inspection and highlighting of the netlist and its components, an integrated Python shell provides an efficient approach to further interact with and process the netlist via aforementioned plugins.

2) HRE Projects: The practical phase consisted of four projects, of which each contained the following subtasks: (1) the reading of relevant scientific papers, (2) pen & paper exercises, and (3) practical reverse engineering tasks.

In the following, we describe the projects with special emphasis on the practical tasks which had to be solved with HAL. All practical HRE tasks were based on flat FPGA netlists without any high-level information such as variable and signal names, comments, hierarchies, or module boundaries. The netlists were available in VHDL and synthetized for the Xilinx Spartan-6 architecture [32]. They were composed of global input and output buffers, Look-Up Tables (LUTs) and Multiplexers for combinational logic, Flip-Flops (FFs) for sequential logic – hereafter all of them simply referred to as *gates* – and their interconnections.

Project 1 – Introduction to Gate-level Netlist Reverse Engineering: This project introduced the HAL environment and its basic features to the students. In the practical task, students had to analyze the data path of an unknown substitution-permutation-network called *ToyCipher*: they had to determine the block and key sizes of the cipher, to decide if the implementation was round-based or unrolled, and to identify the SBoxes. Due to the relatively low complexity of the design (131 gates) and the straightforwardness of the tasks, this assignment could be solved mostly through manual inspection of the netlist in HAL.

Project 2 – Control Logic Reverse Engineering: In this project, students were directed to reverse engineer the control logic from a slightly modified variant of the *ToyCipher* from project 1. Therefore, students identified the logic gates of which the FSM implementing the control logic was composed via graph-based analysis and manual inspection of the candidates. While the basic functionality as well as the complexity (138 gates) of the underlying netlist was similar to the previous one, this assignment focused on the understanding and implementation of the methods used for semi-automated FSM extraction.

Project 3 – Reverse Engineering of Obfuscated Control Logic: The underlying 128-gate netlist for this project was a second variant of the *ToyCipher* utilizing the control flow obfuscation method Harpoon [33]. Obfuscation in this context is a transformation which obstructs high-level information without changing functionality [34]. The goal of obfuscation is to impede the reverse engineering processes. Students had to extract the gates implementing the control logic and analyze the obfuscation method by differentiating the obfuscated and the original parts. In the second step, they disabled the obfuscation through initial state patching and verified their result through dynamic analysis of the netlist. While the basic functionality as well as the complexity of the underlying netlist was similar to the previous one, this assignment focused on building understanding of obfuscated control logic as well as practicing dynamic analysis of netlists.

Project 4 – Advanced Encryption Standard (AES) Key Extraction: In the last project, students had to extract a hard-coded key from a netlist implementing a real-world AES design. AES is the most widely used encryption algorithm. The first task was to derive high-level information such as the functionality (encryption or decryption), the presence of the key schedule, the key length, and the hardware architecture

(round-based or unrolled) from this substantially more complex netlist (2176 gates). Secondly, they had to write a script to identify the Sbox logic, since the Sboxes served as a potential anchor for attacks on the hard-coded key. Finally, the hard-coded key had to be extracted through manipulation and dynamic analysis of the underlying circuit. For this project, already learned HRE techniques such as the derivation of high-level information, identification of functional blocks through scripting, and dynamic netlist analysis had to be applied in a significantly larger environment than before.

D. Measures & Instruments

1) Solution Time and Solution Probability: In the studies, we focused on observing changes to and influences on two dependent variables which are traditional measures in cognitive psychology: time on task (solution time), and accuracy in the task (solution probability). In the following, we present how we measured them. HAL automatically tracked participants' behavior through the creation of log files with time stamps for every interaction within HAL (please note that no personal information was recorded). After providing informed consent, participants uploaded their pseudonymized log files. We calculated the solution time per project per student based on these log files. To calculate the solution time accurately, we set an inactivity threshold of $t = 1$ hour and subtract periods longer than t from the total duration between start and finish of the projects. Analyses for solution time were conducted with data of 20 participants, since the data of the remaining participants was not continously available. Every participant received a grading for the four HRE projects, because the projects were embedded in an academic course. The resulting scores were the basis from which we calculated the per-project solution probabilities. The scores from every project were standardized as percentage to enable comparison. The analyses for solution probability were computed with the whole sample of 38 participants.

2) Control Variables: A self-developed questionnaire on socio-demographics asked participants to provide information about their age, major, and target degree. Additionally, students were requested to describe their prior experiences in relevant topics (e.g., Boolean algebra, FSMs, symmetric cryptography, Python programming, etc.) on a 5-point Likert-Scale, ranging from 1 (very low) to 5 (very high). Item scores were summed for analyses.

3) Further Variables of Interest: The Wechsler Adult Intelligence Scale (WAIS-IV) [35] was used to assess the students' cognitive abilities. It consisted of ten tests to measure four sub scores: Verbal Comprehension (VC), Perceptual Reasoning (PR), Working Memory (WM), and Processing Speed (PS). VC quantified abstract verbal reasoning and verbal expression abilities. It was assessed by the three tests: Similarities (participants were asked to describe how two words are similar), vocabulary (participants defined words), and information (participants answered questions about general knowledge). It should be noted, that students who were not native speakers of German did not complete tests on VC. PR measured the ability to accurately interpret and work with visual information. It consisted of three tests: Block design (participants rearranged 3-dimensional blocks to match patterns), matrix reasoning (participants completed 2-dimensional series of figures), and visual puzzles (participants chose three figures from which to build a 2-dimensional geometric shape). WM reflected the ability to memorize information and to perform mental operations using that information. It consisted of two tests: Digit span (participants recalled a series of numbers in a given order), and arithmetic (participants solved arithmetical problems). PS quantified the participants' ability to process visual information quickly and efficiently. It consisted of two tests: Symbol search (participants were asked to search symbols rapidly and accurately), and coding (participants needed to transcribe a unique geometric symbol with its corresponding Arabic number rapidly and accurately). The analyses of the WAIS-IV provided a Full Scale IQ (FSIQ) based on the combined sub scores of VC, PR, WM, and PS.

To investigate the students' level of motivation, we employed the Questionnaire on Current Motivation (QCM) [36] during each of the four projects. The QCM consisted of 18 items which measured the following four motivational factors on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree): expected challenge of a task ("This task is a real challenge for me"), probability of success ("I think I am up to the difficulty of this task"), participants' interest ("I would work on this task even in my free time"), and anxiety of failure ("I'm afraid I will make a fool out of myself"). Students answered the QCM via the online survey provider Soscisurvey. After inverting items that were pooled differently, we computed means of the four sub factors.

As is commonly practiced in current research on Cognitive Load [37], we integrated the Perceived Task Difficulty Scale [38], and the Mental Effort Scale [39]. The Cognitive Load Scales were used to determine if participants recognized the increasing complexity of the HRE projects. Participants were asked to rate their Perceived Task Difficulty on a 7-point Likert Scale, ranging from 1 (very very easy) to 7 (very very difficult). Additionally, students rated their invested amount of mental effort on a 7-point Likert Scale, ranging from 1 (very very low) to 7 (very very high) via the online survey provider Soscisurvey. We computed the means of each scale.

E. Study Procedure

We conducted the quasi-experimental studies with a within-subject design during the winter term 2018/2019 at one German and one North American university. The studies were integrated into the practical phase of the HRE course (Section II-B2). After students signed informed written consent documents and received a randomly-assigned pseudonym, the studies started with online questionnaires on socio-demographics, and prior experiences in relevant topics. Over the course of the semester, the WAIS-IV was administered once in a 90-120 minute face-to-face session with each student. Overall, we used a similar procedure to collect data at four different points in time (four HRE projects) as described in the following. After reading the

assignment of the current HRE project, participants were asked to rate their level of current motivation (QCM) regarding the imminent HRE task. After finishing the task, students uploaded their log files of the current HRE project to the SFTP server and subsequently answered the two Cognitive Load Scales on Mental Effort and Perceived Task Difficulty.

IV. Results

To answer research questions 1a and 1b, we conducted a repeated-measures ANOVA of solution times and probabilities which is a common method for comparing changes over time in psychological research (Fig. 1). Since, we did not find any group differences between students from both universities, we were able to merge the two samples in our analyses. The results showed significant differences across the four times of measure, with $F(3, 17) = 5.66$, p = .03, η^2 = .50 (Fig. 1a). The post-hoc analysis revealed that the solution time differed significantly between all projects, except for solution time between projects 1 and 3, and projects 2 and 4.

The repeated-measures ANOVA for comparing the mean of solution probabilities across the four HRE projects (Fig. 1b) revealed that students' solution probability decreased significantly in the most complex HRE project 4, F (3,35) =7.09, p=.00, η^2 = .38. It should be noted, however, that the mean solution probability (M=77.2, SD=31.4) was still at a satisfactory level. We found no significant correlation between solution time and solution probability across the four projects.

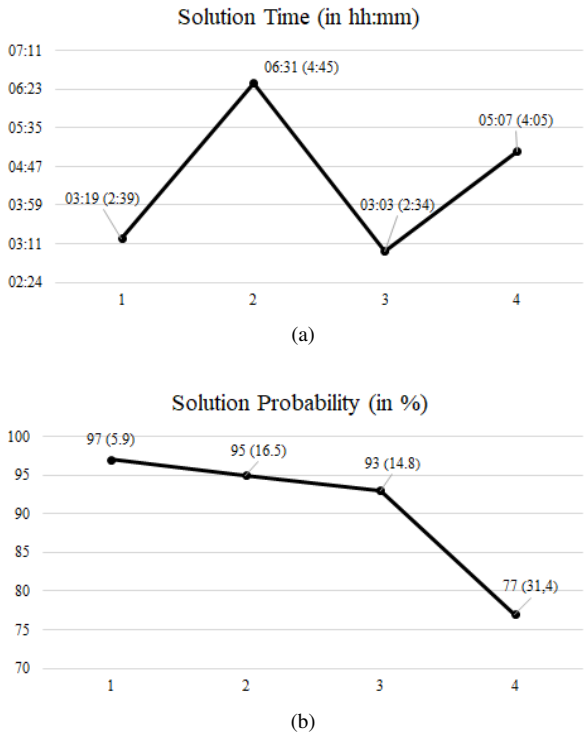

Fig. 1. Means (M) and Standard Deviations (SD) of solution time (a) and solution probability (b) in the format *M (SD)*.

To test, if students perceived the increasing complexity of the single projects, we conducted a repeated-measures ANOVA for the two Cognitive Load scales. The results showed that students reported a significant higher mental effort in project 4 (M=4.26, SD=1.59) compared to project 1 (M=3.45, SD=1.43) with, F (3, 35) = 3.56, p = .024, η^2 = .23. The repeated measures ANOVA for the Perceived Task Difficulty scale showed significant results between the means of project 2 (M=3.61, SD=1.29) compared to project 3 (M=5.39, SD=1.26), and compared to project 4 (M=5.24, SD=1.71), with F(3, 35) = 18.77, p = .000, η^2 = .62. These results showed that students perceived the growing complexity of the projects.

To test if our course design (Section II-B2) supported continuous motivation across the practical phase, we computed the repeated-measure ANOVA of the Questionnaire on Current Motivation (QCM). The analysis revealed no significant differences between the students' levels of motivation across the four times of measure. The descriptive analyses showed above-average levels of motivation over all projects, with Interest (M=3.9, SD=0.38), Challenge (M=3.9, SD=0.46), Anxiety (M=1.59, SD=0.34), and Probability of Success (M=3.65, SD=0.24).

To answer research question 2, we computed the following analyses. To assess differences in the effect of the level of expertise on solution probability we calculated a repeated-measures ANOVA. The analysis revealed no significant effect of expertise on solution probability with (F (3, 34) = 0.17, p = .92,η^2 = .02), nor on solution time with (F (3, 17) = .94, p = .44, η^2 = .15).

We conducted bivariate correlations between Full Scale IQ (FSIQ), IQ sub factors and prior experiences in the light of research question 3. Table I shows the results, which indicate significant correlations between the sub factors Working Memory (WM), and Processing Speed (PS), and prior experiences in FSMs, symmetric cryptography, and students' performances.

Table I
Pearson correlation with correlation coefficients and significances.

	Solution Probability				Solution Time			
	P1	P2	P3	P4	P1	P2	P3	P4
IQ and sub factors								
FSIQ†	.15	.17	.12	.18	.19	.40	.32	.38
WM†	.47	.10	.56	.72*	.01	.19	.43*	.07
PS†	.10	.15	.16	.69*	.03	.02	.59*	.17
PR†	.03	.14	.20	.31	.18	.46	.56	.88
Prior Experiences								
HRE	.10	.18	.20	.19	.09	.19	.25	.01
Bool. Algeb.	.01	.06	.08	.13	.04	.21	.10	.06
FPGAs	.25	.07	.21	.01	.25	.29	.01	.03
FSMs	.01	.06	.14	.01	.18	.19	.42*	.15
Sym. Crypto	.35	.17	.16	.08	.41*	.13	.14	.53*

*Correlation is significant at the 0.05 level.
†Full Scale IQ (FSIQ), Working Memory (WM), Processing Speed (PS), Perceptual Reasoning (PR).

As no factor correlated significantly with time and probabilities across all four projects, the computation of ANCOVAS was not feasible. To explore potential differences between students with different levels of expertise, prior experiences, and

cognitive abilities, we calculated repeated-measures ANOVAS. Each independent variable was transformed by a median split to conduct the calculations. In the following, we only report the calculations with independent variables which showed significant correlations (Table 1).

The repeated-measures ANOVA revealed significant differences between students with higher and lower Working Memory (WM) scores on solution time (F (3, 17) = 1.27, p = .04, η^2 = .19). Students with higher WM scores were significantly faster in solving project 2 (p = .03), 3 (p = .04), and 4 (p = .05). Additionally, the results revealed significant differences between a higher and lower WM related to solution probability, with (F (3, 34) = 5.85, p = .05, η^2 = .34). Students with higher WM scores were significantly better at solving project 4.

To assess the effects of Processing Speed (PS), we calculated a repeated-measures ANOVAs for solution time and probability. The results revealed significant differences between higher and lower PS scores regarding solution probability (F (3, 34) = 9.43, p = .041, η^2 = .45). Students with higher PS scores had a significant higher solution probability in project 4 (p = .04) than students with lower PS scores. Repeated-measures ANOVA for PS and solution time revealed a significant effect (F (3, 17) = 1.3, p = .04, η^2 = .19). Students with higher scores in PS solved project 3 faster than students with lower PS scores.

Additionally, the calculation for prior experiences showed significant effects. The repeated-measures ANOVA revealed significant differences between students with high and low levels of experiences in symmetric cryptography regarding solution time (F (3, 17) = 4.41, p = .02, η^2 = .45). Students with more experience in symmetric cryptography solved projects 1 and 4 significantly faster than students with less experiences in symmetric cryptography.

The repeated-measures ANOVA did not reveal significant effects of higher and lower experiences in FSMs on solution time (F (3, 17) = 1.8, p = .19, η^2 = .25), nor on solution probability (F (3, 34) = 0.9, p = .43, η^2 = .07)

V. Discussion

In the light of research question 1a, our data showed that students needed significantly more time for solving project 2 than for solving project 1. This is not a surprise, since students were asked to create automated solutions for the first time which might have been challenging and time consuming in comparison to project 1. Interestingly, our data showed that students were able to complete project 3 more quickly than project 2, despite project 3 being the more complex task. We here assume that memory and fluency-building are involved in the development of declarative and procedural HRE knowledge [19]. Students enrolled in our course were able to use their knowledge gained in project 2, for solving project 3 faster, thus demonstrating that they had acquired HRE skills which enabled them to become more fluent. Overall, we observed a significant increase of solution time between projects 1 and 4, and an observable but not significant increase between projects 3 and 4, which account to the growing complexity of the underlying gate-level netlists.

Referring to research question 2, the analyses revealed no significant differences between students with different levels of expertise in regard to solution time and solution probability. It would have been expected, that graduate students had acquired more relevant prior knowledge in important topics which might have resulted in shorter time on task and higher solution probabilities. Nevertheless, our results showed no differences between students on different levels of expertise. We conclude, that graduate students did not acquire more relevant knowledge for solving HRE tasks in previous university courses than undergraduates did. Our results show, that our course taught a sufficient amount of relevant knowledge during the lecture phase which equally enabled both undergraduate and graduate students to solve the HRE projects.

In the light of research question 3 we conducted several computations to observe which cognitive factors or prior knowledge had a significant effect upon solution probability and solution time. Working Memory (WM) is one important cognitive factor in acquiring HRE skills. Our data showed that higher WM scores led to faster solutions in projects 2, 3, 4, and higher solution probability in project 4. Referring to the key characteristics of WM helps to illustrate how a good WM is important to the successful completion of HRE projects. WM is defined as a system for storing and manipulating information in the context of complex tasks such as learning and problem solving [40]. It enables the retrieval of learned information from long term memory [41], and keeps both relevant old and novel facts in memory during the activity of problem solving while at the same time ignoring irrelevant information [42]. By taking this into account, we can explain why students with higher WM scores solved the HRE projects more quickly – namely because they were better able to combine novel and stored information and ignore irrelevant information, thereby increasing the speed with which they reached solutions in the individual projects. A good WM also supported students in reaching higher solution probabilities in project 4. Briefly revisiting the specific requirement of that project makes it rather obvious why that was the case: to successfully complete the project, students had to recall knowledge, work flows, and problem-solving strategies that they had learned during projects 1-3. For example, during project 4, students had to recall the derivation of high-level information and Sbox identification skills taught in project 1, as well as the dynamic netlist analysis competencies fostered during project 3. Students with a good WM were supported in recalling relevant information that they learned earlier in the course, leading them to achieve higher solution probabilities and shorter solution times.

Processing Speed (PS) is another relevant cognitive factor in the context of acquiring HRE skills as demonstrated by the observation that students with higher PS scores had a significantly higher solution probability in project 4 and solved project 3 significantly faster than did students with lower PS scores. PS is defined as the ability to process visual information

quickly and efficiently, and research on PS has shown that it can be a good predictor of how quickly and accurately students can perform a task [43]. Higher PS scores therefore contributed to solving project 4 more accurately and project 3 more quickly.

In the context of research question 3, our analysis established the significant effects that prior experience with FSMs and symmetric cryptography had upon student outcomes, with students who had more experience in both areas performing better than students with less experience. Our data showed a significant correlation between prior experiences in FSMs and solution time in project 3. The twofold challenge of project 3 consisted of first detecting an FSM and second breaking the FSM obfuscation. A higher prior knowledge in FSMs might have been helpful to solve the first challenge more quickly, since students did not need to acquire knowledge on FSMs during their work on project 3. Additionally, our analyses showed that prior knowledge in symmetric cryptography enabled students to solve projects 1 and 4 more quickly. Prior knowledge on the inner workings of symmetric ciphers is advantageous regarding the contents of projects 1 and 4, e. g. data path analysis, the detection of Sboxes, or general attack strategies on such ciphers.

A. Implications for Future HRE Course Designs

The integration of Spacing and Testing [19], [27] throughout the four HRE projects supported students' development of memory and fluency, and the inclusion of Worked Examples [19], [28] enabled students to acquire HRE skills from tasks with problem solving practice. These two instructional principles should be part of future HRE courses. We also assume that the integration of stimulating and realistic exercises of an appropriate difficulty level as well as the integration of HAL led to the above-average levels of student motivation we observed during the course and should be included in future HRE courses. We found significant differences between students on different levels of prior knowledge. To compensate these differences, future HRE courses should include special programs for students with lower levels of prior knowledge in relevant topics, e.g., basic knowledge lectures and exercises regarding symmetric cryptography or tutorials for practicing Python programming, since HRE is automatable in HAL via Python. Our results revealed significant differences between students with higher and lower scores in Working Memory (WM). Due to time factors, a course on HRE cannot not include training to improve WM performance. Nevertheless, we could structure the HRE course in a way, which supports students with lower scores in WM. By referring to the fact that the capacity of WM is limited, we can design our assignments and projects by supportive knowledge, students already learned in earlier stages of the course. This could be a possible way to support students with lower scores in WM to focus on the current task instead of struggling in recalling information from prior lectures and projects.

B. Limitations and Implications for Future Research

This presented work has limitations that should be investigated. In the future, studies on human processes in HRE with a larger sample size would be preferable to produce results with a higher impact and significance. Since this study is a first investigation to fill the research gap of skill acquisition in HRE, the generalizability to other areas is limited. Our research prompted us to make several observations about potential future research on skill acquisition in the field of HRE. It would be preferable to further analyze problems, errors, or difficulties of human reverse engineers (e.g., process modelling of applied problem solving strategies). Doing so would allow us to offer specific support via instructions, exercises, or training. If Working Memory (WM) and Processing Speed (PS) are relevant factors in predicting expertise development, a differential examination of the central executive [44] might shed more light on the role of cognitive factors in acquiring HRE skills. Since our data led us to assume that declarative knowledge had been transformed into procedural knowledge, a closer examination of the types of knowledge presented in the two phases of the course might prove interesting. Finally, the integration of a second complex task into a future study would help reveal more individual differences between students as well as help ascertain whether differences in solution time and solution probability are stable over a longer time horizon consisting of multiple complex projects.

VI. Conclusion

HRE is important in the field of cyber security and therefore HRE skills are in high demand across industries and around the world. Despite the clear and unmet worldwide demand for HRE experts, there is a surprising lack of educational HRE courses, and research on the acquisition of HRE skills is lacking thus far. Against this background, we developed a HRE course based on psychological cognitive research and augmented through the integration of specific instructional methods which are known to support the development of declarative and procedural knowledge. Through the conduction of two quasi-experimental studies, we demonstrated that our course supported the acquisition of HRE skills. Our students demonstrated increased fluency in HRE skills by solving increasingly complex tasks in successively shorter time intervals. Statistical analyses established that differences in individual student outcomes were a function of differences in Working Memory (WM), Processing Speed (PS), and prior knowledge in relevant topics. Finally, we derived ideas for future course designs and research aimed at achieving a deeper understanding of the underlying psychological factors behind the acquisition of HRE skills, such as observing the central executive of the WM or by observing the impact that the integration of further complex tasks has upon solution time and solution probability.

References

[1] M. Rostami *et al.*, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[2] G. T. Becker *et al.*, "Stealthy Dopant-level Hardware Trojans," in *CHES*, pp. 197–214, Springer, 2013.

[3] U. Guin, K. Huang, D. DiMase, *et al.*, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. of the IEEE*, vol. 102, pp. 1207–1228, Aug 2014.

[4] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *J. of Electron. Testing*, vol. 30, pp. 9–23, Feb 2014.

[5] M. G. Rekoff, "On Reverse Engineering," *IEEE Trans. on Systems, Man, and Cybern.*, no. 2, pp. 244–252, 1985.

[6] M. Fyrbiak *et al.*, "Hardware Reverse Engineering: Overview and Open Challenges," in *IVSW*, 2017.

[7] R. Torrance and D. James, "The State-of-the-Art in IC Reverse Engineering," in *CHES*, pp. 363–381, Springer, 2009.

[8] C. Wiesen, S. Becker, M. Fyrbiak, N. Albartus, M. Elson, N. Rummel, and C. Paar, "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, Dec 2018.

[9] B. Shakya *et al.*, *Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation*, pp. 3–32. Springer, 2017.

[10] S. Wallat *et al.*, "A Look at the Dark Side of Hardware Reverse Engineering – A Case Study," in *IVSW*, 2017.

[11] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*. USA: Addison-Wesley Publishing Company, 4th ed., 2010.

[12] P. Subramanyan *et al.*, "Reverse Engineering Digital Circuits Using Structural and Functional Analyses," *IEEE Trans. Emerging Topics Comput.*, vol. 2, no. 1, pp. 63–80, 2014.

[13] J.-B. Note and É. Rannaud, "From the bitstream to the netlist," in *ACM FPGA*, pp. 264–264, 2008.

[14] C. Wiesen, N. Albartus, M. Hoffmann, S. Becker, S. Wallat, M. Fyrbiak, N. Rummel, and C. Paar, "Towards Cognitive Obfuscation: Impeding Hardware Reverse Engineering Based on Psychological Insights," in *Proceedings of the 24th Asia and South Pacific Design Automation Conference*, ASPDAC '19, (New York, NY, USA), pp. 104–111, ACM, 2019.

[15] N. L. Lee and P. 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.

[16] J. R. Anderson, "Acquisition of cognitive skill.," *Psychological review*, vol. 89, no. 4, p. 369, 1982.

[17] C. Tenison and J. R. Anderson, "Modeling the distinct phases of skill acquisition.," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 42, no. 5, p. 749, 2016.

[18] F. Gobet, "Chunking models of expertise: Implications for education," *Applied Cognitive Psychology*, vol. 19, no. 2, pp. 183–204, 2005.

[19] K. R. Koedinger, A. T. Corbett, and C. Perfetti, "The Knowledge-Learning-Instruction framework: Bridging the science-practice chasm to enhance robust student learning," *Cognitive science*, vol. 36, no. 5, pp. 757–798, 2012.

[20] J. Singer-Dudek and R. D. Greer, "A long-term analysis of the relationship between fluency and the training and maintenance of complex math skills," *The Psychological Record*, vol. 55, no. 3, pp. 361–376, 2005.

[21] C. H. Skinner, P. A. Fletcher, and C. Henington, "Increasing learning rates by increasing student response rates: A summary of research.," *School Psychology Quarterly*, vol. 11, no. 4, p. 313, 1996.

[22] J. Kilpatrick, J. Swafford, and B. Findell, "The strands of mathematical proficiency. Adding it up: Helping children learn mathematics (pp. 115–155)," 2001.

[23] P. C. Kyllonen and D. J. Woltz, "Role of cognitive factors in the acquisition of cognitive skill," in *Abilities, motivation, and methodology: The Minnesota symposium on learning and individual differences*, pp. 239–280, Erlbaum Hillsdale, NJ, 1989.

[24] T. Litzinger, L. R. Lattuca, R. Hadgraft, and W. Newstetter, "Engineering education and the development of expertise," *Journal of Engineering Education*, vol. 100, no. 1, pp. 123–150, 2011.

[25] P. R. Pintrich, "A motivational science perspective on the role of student motivation in learning and teaching contexts.," *Journal of educational Psychology*, vol. 95, no. 4, p. 667, 2003.

[26] S. Michaels, C. O'Connor, and L. B. Resnick, "Deliberative discourse idealized and realized: Accountable talk in the classroom and in civic life," *Studies in philosophy and education*, vol. 27, no. 4, pp. 283–297, 2008.

[27] H. Pashler, P. M. Bain, B. A. Bottge, A. Graesser, K. Koedinger, M. McDaniel, and J. Metcalfe, "Organizing Instruction and Study to Improve Student Learning. IES Practice Guide. NCER 2007-2004.," *National Center for Education Research*, 2007.

[28] J. Sweller and G. A. Cooper, "The use of worked examples as a substitute for problem solving in learning algebra," *Cognition and instruction*, vol. 2, no. 1, pp. 59–89, 1985.

[29] S. A. Ambrose, M. W. Bridges, M. DiPietro, M. C. Lovett, and M. K. Norman, *How learning works: Seven research-based principles for smart teaching*. John Wiley & Sons, 2010.

[30] M. Fyrbiak *et al.*, "HAL – The Missing Piece of the Puzzle for Hardware Reverse Engineering, Trojan Detection and Insertion," *IEEE Trans. on Dependable and Secure Computing*, pp. 1–1, 2018.

[31] S. Wallat, N. Albartus, S. Becker, M. Hoffmann, M. Ender, M. Fyrbiak, A. Drees, S. Maaßen, and C. Paar, "Highway to HAL: open-sourcing the first extendable gate-level netlist reverse engineering framework," in *Proceedings of the 16th ACM International Conference on Computing Frontiers*, pp. 392–397, ACM, 2019.

[32] Xilinx, Inc., *Spartan-6 FPGA Configurable Logic Block*, February 2010. [Online; accessed 20-March-2019].

[33] R. S. Chakraborty *et al.*, "HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection," *IEEE Trans. CAD of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493–1502, 2009.

[34] C. Wiesen, N. Albartus, M. Hoffmann, S. Becker, S. Wallat, M. Fyrbiak, N. Rummel, and C. Paar, "Towards cognitive obfuscation: impeding hardware reverse engineering based on psychological insights," in *Proceedings of the 24th Asia and South Pacific Design Automation Conference*, pp. 104–111, ACM, 2019.

[35] D. Wechsler, "Wechsler adult intelligence scale–Fourth Edition (WAIS–IV)," *San Antonio, TX: NCS Pearson*, vol. 22, p. 498, 2008.

[36] F. Rheinberg, R. Vollmeyer, and B. D. Burns, "QCM: A questionnaire to assess current motivation in learning situations," *Diagnostica*, vol. 47, no. 2, pp. 57–66, 2001.

[37] A. Schmeck, M. Opfermann, T. van Gog, F. Paas, and D. Leutner, "Measuring cognitive load with subjective rating scales during problem solving: differences between immediate and delayed ratings," *Instructional Science*, vol. 43, no. 1, pp. 93–114, 2015.

[38] O. Bratfisch *et al.*, *Perceived Item-Difficulty in Three Tests of Intellectual Performance Capacity*. ERIC Clearinghouse, 1972.

[39] F. G. Paas, "Training Strategies for Attaining Transfer of Problem-solving Skill in Statistics: A Cognitive-load Approach," *J. of Educ. Psychology.*, vol. 84, pp. 429–434, 1992.

[40] A. D. Baddeley and G. Hitch, "Working memory," in *Psychology of learning and motivation*, vol. 8, pp. 47–89, Elsevier, 1974.

[41] M. J. Dehn, *Working memory and academic learning: Assessment and intervention*. John Wiley & Sons, 2011.

[42] B. Hill, E. M. Elliott, J. T. Shelton, R. D. Pella, J. R. O'Jile, and W. D. Gouvier, "Can we improve the clinical assessment of working memory? An evaluation of the Wechsler Adult Intelligence Scale–Third Edition using a working memory criterion construct," *Journal of Clinical and Experimental Neuropsychology*, vol. 32, no. 3, pp. 315–323, 2010.

[43] E. O. Lichtenberger and A. S. Kaufman, *Essentials of WAIS-IV assessment*, vol. 50. John Wiley & Sons, 2009.

[44] A. Baddeley, "The fractionation of working memory," *Proceedings of the National Academy of Sciences*, vol. 93, no. 24, pp. 13468–13472, 1996.