Teaching the Hardware Implementation of Cybesecurity Encryption Algorithms on FPGA using Hands-on Projects

Dr. Nader Rafla P.E., Boise State University

Dr. Nader Rafla, P.E., received his MSEE and PhD. in Electrical Engineering from Case Western Reserve University, Cleveland, Ohio in 1984 and 1991 respectively. His Doctoral research concentrated on object recognition and localization from multi sensor data: range image, force-torque, and touch. From 1991 to 1996, he was an Associate Professor at the Department of Manufacturing Engineering at Central State University. Where he taught courses was involved in collaborative research with Wright-Patterson Air Force in applied image processing. In January 1997, he joined the newly developed electrical and computer engineering program at Boise State University where he is currently is the chair and an Associate professor. He led the development and starting of the BS and MS programs. He taught several courses and supervised numerous M.S. thesis and Senior Design Project. He contributed to the start of the PhD program and is currently advising three Ph.D. students and two MS students. He also has been conducting research and consultation in R&D for Micron Technology, Hewlett Packard and others. Dr. Rafla's areas of expertise are: security of systems on programmable chips and embedded systems; advanced methods for improving hardware and physical network security; evolvable hardware; and evolutionary and reconfigurable computing. He is a senior member of the IEEE organization and several societies, a member of the ASEE and ACM organizations.

H. Shelton Jacinto, Boise State University

H S. Jacinto received his B.S. degree in electrical and computer engineering from Boise State University, Boise, Idaho, USA, in 2017, and is currently a Ph.D. candidate in electrical and computer engineering from Boise State University, Boise, Idaho, USA. From 2015 to 2017 he worked with Idaho National Labs in conjunction with the Advanced Energy Lab conducting research on self-powered wireless sensor networks and their security. He has moved over to the Air Force Research Lab Quantum Information Science group in 2018 under a fellowship to work on quantum information processing systems, integrated quantum photonics, and quantum control. His main research focuses on quantum network hardware cybersecurity, quantum informatics, and adaptive hardware anti-tamper and encryption technologies for use in the field of hardware security to create a secure platform for an upcoming quantum era.

Luka Daoud, Boise State University

Luka Daoud received the B.S. degree in Electrical Engineering from Fayoum University, Egypt in 2007, and M.S. degree in Electronics and Communications Engineering from Egypt-Japan University of Science and Technology (E-JUST), Alexandria, Egypt in 2012. Luka is currently a Ph.D. candidate in Electrical and Computer Engineering at Boise State University, Boise, Idaho, USA. His main research focuses on hardware security, Network-on-Chip (NoC), high performance computing, and High Level Synthesis (HLS) design.

Teaching Project-Based Hardware Cybersecurity Encryption Algorithms and Implementations on FPGA

Abstract

Cybersecurity is an important concept in today's age of information and is of major interest to keep information secure, helping to protect sensitive information in the presence of untrusted third-parties. This has presented the need for an implemented hardware variant of secure algorithms with small footprint to help add protection while reducing processing time/overhead on a standard processor.

In this work we present two hands-on projects that are designed specifically to teach these two concepts using project-based learning techniques in an innovative cooperative learning environment. The learning environment served to combine both student-peer learning and jigsaw strategies.

The technical contents of the first project teach students the process and methodologies of designing and testing the hardware implementation of a block cipher encryption, the Advanced Encryption Standard, on a field-programmable gate array. The second project builds on the first by introducing the hardware implementation of hash message authentication codes through the Whirlpool hash function in three different operating modes.

The objective of this work is to present an innovative teaching environment for these hands-on encryption algorithm-based projects using cooperative learning rather than a traditional mode of lecturing with given homework assignments. This environment encouraged students to think thoroughly, out-of-the-box, gain problem-solving skills, and improve their communication of technical concepts to peers through the delivery of student-led lectures.

The assessment of student learning is accomplished by a mixture of presentations with peer evaluations, instructor evaluations, and thorough grading of project reports. End-of-course evaluations were positive regarding the learning environment and technical skills gained by students. For this work one assigned hands-on project for students working in groups resulted in unique per-group implementations, where in the second project, this led to different project perspectives and additions beyond a standard assigned project, enhanced by student-peer teaching. Students effectively learned and comprehended many different implementations of a widely used encryption and authentication algorithm via our modified teaching techniques.

Introduction

The Electrical and Computer Engineering Department at Boise State University has developed a new undergraduate certificate in cyberphysical-systems security. One of the major courses included in the cyberphysical-systems certificate is a digital hardware design course. The focus of the digital hardware design course is to teach the usage and implementation of digital systems and algorithms onto field-programmable gate arrays (FPGAs); semiconductor devices containing a matrix of reconfigurable logic blocks connected together that can be reprogrammed to any desired function post-manufacturing. This course has been taught, until recently, in a traditional lecture-based manner with periodic hands-on projects and laboratory exercises. The course was recently flipped [1], featuring many new active-learning techniques and overhauled laboratory exercises. To satisfy the new cyberphysical systems security certificate requirements two substitute projects needed to be added to cover both cryptographic algorithms [2] and message authentication [3]. After taking this course, students should be able to:

(a) Describe the operation of an encryption algorithm,

(b) explain the design principles of message authentication mechanisms,

(c) implement and test encryption algorithms on a FPGA, and

(d) debate, criticize, and assess the operation of different implementations of the same encryption algorithm.

Students taking this course are assumed to only have background knowledge in digital system design, without any prior exposure to the mathematical background of encryption and authentication algorithms. The challenge for this course then becomes the development of impactful projects to help achieve the course learning objectives through hardware design and implementation methodologies while maintaining the classroom's active learning environment.

Philosophical Framework and Educational Context

The achievement of our objectives relies on the creation of a project-based learning (PBL) environment rather than the traditional pedagogy of lecturing theory with support of hands-on projects and assignments. The PBL environment will serve to rejuvenate and revitalize student learning success in the classroom since PBL revolves around giving students the opportunity to independently learn subject-matter. By the independent learning opportunities provided, students are able to better-learn the decision making process required for a desired subject. An additional learning opportunity that enhances student learning is the ability to work on small portions of a long-term project. The instructor in this environment acts as a facilitator to provide guidance throughout the design process rather than a director of a classroom. Due to the great variety of PBL activities, research in this area has revealed that there is generally no universal model for PBL [4]. Without a universal model for PBL, this suggests that the planning, managing, enacting, and assessing projects specifically designed for PBL is a challenging problem. On the flip-side, PBL has great impact on self-directed learning skills [5]: Allowing students to work

collaboratively during the research and implementation phases of design problems, and to improve the quality of students' subject-matter knowledge and problem-solving skills.

For the course taught, two challenging projects were developed and given to students. The projects both consisted of several tasks, designed specifically, to facilitate students creative design, problem-solving, and decision-making abilities. The initial project write-ups contained a brief introduction to the concepts and basic principles involved in cryptographic algorithms and authentication measures. The assignments were supplemented by appropriate research papers regarding the provided algorithms to help students gain sufficient background required to perform the design. Students were required to read and discuss among themselves and had the opportunity to attend help-sessions to further enhance their understanding of the operating principles of the algorithms provided. Additional instructional materials and tutorials were also provided regarding a technology-based design suite, Vivado [6]: A software tool-kit produced by Xilinx, Inc. for synthesis and analysis of high-level description language (HDL)-based designs [7].

To perform the pilot-study of this new technique of teaching hardware implementations of cryptographic algorithms, the class enrollment was capped to nine students. The low-cap was chosen due to the number of students interested in the material along with the number and size of teams required, where each of three teams was composed of three members. The arrangement was selected to allow ample time for the instructor to interact with the teams and individual students and to ensure a fair work distribution. The class met for 75 minutes, two days a week, where both instructor and teaching assistant (TA) were present during each class meeting. There is also an additional reason due to the sub-components of design mentioned later.

To help prepare the instructor prior to the beginning of the university's semester, two workshops were attended as offered by the Center for Teaching and Learning (CTL) at Boise State University. The two workshops focused on active learning and collaborative teaching, respectively. The workshops served to provide the instructor with appropriate knowledge and resources regarding classroom management and active learning methodologies. The TA requested for the semester had the added benefit of possessing the required technical expertise, as a Ph.D. candidate, whose interests fell within the scope of the course being taught by having a strong background in secure hardware design.

Peer-teaching encompasses a broad set of activities where students learn from, and with, each-other. The method of peer-teaching can be both formal or informal but both contribute to a generally equivalent positive outcome [8]. Peer-teaching in general is considered as an instructional methodology of cooperative learning; a process where small student teams cooperate to accomplish a common goal while maintaining independence and individual accountability [9]. This technique is selected and used since there is a larger student involvement in the study of provided materials, allowing students to analyze and select key concepts needed for the design phase of their projects.

Another strategy, namely jigsaw [10], has been used in this study. The jigsaw method is another strategy of cooperative learning in which the class is divided into small groups and the project is broken into pieces such that each group works to assemble the pieces to complete the project. Research shows that by using the jigsaw method, students' attention becomes more focused as they can express ideas and opinions more easily [11].

The First Project

The first project is centered around the design and implementation of a symmetric block-cipher encryption and decryption algorithm called the Advanced Encryption Standard (AES), a long-known specification for the encryption of electronic information established by the National Institute of Standards and Technology (NIST) [12]. AES was adopted by the US government as the replacement for the Data Encryption Standard (DES), and is now commonly used worldwide in everything from archive and compression tools such as WinZip and WinRAR to virtual private networks (VPNs) like NordVPN or Private Internet Access. The standard AES algorithm is quite complex for those unfamiliar with the internal operations, thus an academic variant of AES, named Mini-AES [13] is adopted.

For this project, a student-peer teaching strategy is utilized where teams are formed with small numbers (three students). The same project was assigned to all teams where, initially, each group collaborated in brainstorming and understanding the project requirements by studying the provided literature. The students were then instructed to cooperate in solving the design problem through the analysis of differing techniques to accomplish the task. After the brainstorming and pre-design phases are complete, a two-week period was given to teams to finish their design and implement onto FPGA with verification of functionality. In the meantime, the instructor and a TA were available to provide mentoring to each team by answering any questions regarding aspects and nuances of the algorithm's implementation. At the completion of the project, each team gave a shared lecture to the class providing full insight into their design techniques and the results acquired. The instructor and TA also attended these twice-weekly, 75 minute, lectures to provide comments and ask in-depth questions. Since the teams all had differing approaches to the implementation of the same problem, an active participation of students during peer presentations was observed. A final written submission of a team-report was graded by the instructor using a rubric to assess final learning outcomes of the project.

The Second Project

The second project served to expand on the first project by adding an implementation of hash message authentication codes (HMACs), a mechanism used for the authentication of a message through cryptographic hash functions [14]. Message authentication codes (MACs) provide data integrity and anonymous authentication with the advantage of working with a symmetric block-cipher such as AES. The Whirlpool hash function [15] was identified for usage in this project due to its construction and implementation similarity to AES. There are three main methods, called modes, in which MACs may be generated and applied to messages: Encrypt-then-MAC, MAC-then-Encrypt, and Encrypt-and-MAC.

In this project a modified implementation of the jigsaw strategy is applied to serve our purpose. In the jigsaw strategy a problem is broken into pieces where the team will complete the final assembly. In our case the class was divided into three small groups, each with three team members, and one mode of MAC was assigned to each team. The students were provided a lengthy three-week period to read, discuss, design, and implement their mode. During this period

the instructor and TA met regularly with each team to discuss their progress, provide insight into design problems, and provide general technical assistance. It should be noted that these meeting times were held in addition to the classroom teaching periods as special sessions. The special sessions were held for an average of 90 minutes per team, weekly, for three weeks. At the conclusion of the three-week period, the teams were broken up and a new three-member team was formed with a member from each of the old teams. The switching of teammates made it so that each member was knowledgeable on a different mode of MAC operation and its associated implementation strategy. This modification provided every student with the opportunity to learn and teach his/her own colleagues without losing focus on the material. The modification also fostered increased skills in communication of technical information to teach new material to peers. During the teammate switching phase, the instructor and TA joined each group to monitor the student-lectures and provide assistance in answering any difficult questions that may have arose. Meanwhile, this phase also gave the instructor an opportunity to identify individual students' difficulties to find a commonality with lack of understanding to provide additional information to the entire class. Students were finally asked to highlight any technical feedback that was provided during their given lecture; subsequently graded for outcome assessment.

Assessment and Evaluation

Commonly utilized assessment methods were not suitable for project-based learning techniques. Instead, survey instruments were designed specifically to assess the technical understanding were administered to students. One survey was used for self-evaluation and team-member peer-evaluation. Using this survey students are assessed based on five parameters: *1*) Participation, *2*) collaboration, *3*) contribution, *4*) quality, and *5*) team-work as shown in Table 1.

The second survey was used during student lectures for the assessment of contents, the presenter, and technical knowledge. The survey tool is shown in Table 2. In addition, rubrics were used for the grading of technical reports where the rubric covered the technical details of the design tasks, implementation, and verification.

For the first survey each teammate evaluated themselves and other teammates, where all students evaluated each presenter. The instructor and TA also evaluated the presenter independently. The average values of student self-evaluations/peer-evaluations, and instructor/TA evaluations were calculated along with the overall averages as shown in Table 3.

The total percentages of the class were calculated based on a total of 30 points (6 items $\times$ 5 maximum points each). Students performed above average in all cases, with the overall range between 3.28 – 4.0, indicating very good performance in all attributes. The results indicate that students attained the intended outcomes, also noticeable in the total percentage values. Participation throughout discussion received the highest overall average, indicating that students' knowledge about subject-matter was the result of substantial time investment to understand the technical aspects of the projects. The lowest average received was for the timely completion of tasks, common among hands-on projects since students tend to under-estimate the time needed for any given technical tasks' completion.

Table 1: Team evaluation form.

Instructions: Write your name in the evaluator column and the name of each of your teammates in the following two columns. For each team member, including yourself, assign a value on a scale (1 – 5), where (1=mediocre; 2=below average; 3= average; 4=above average; 5= superior).

*Name of Evaluator:*_____

Attribute	**Evaluator**	**Group Member 1:** _____	**Group Member 2:** _____
Group meeting attendance			
Collaboration with other teammates			
Active participation in discussions			
Timely completion of tasks			
Quality of completed tasks			
Contributed significantly to the success of the project			
TOTAL			

Table 2: Student-lecturer evaluation items

Instructions: Write your name in the space provided for that and the name of the person being evaluated in the appropriate column in the table. Assign a value for each criterion item on a scale (1– 5), where (1=mediocre; 2=below average; 3= average; 4=above average; 5= superior).

*Name of Evaluator:*_____

Criteria	**Evaluated Individual:** _____
Clarity of presentation	
Quality and use of visual aid	
Well-organized main points	
Mastery of subject presented	
Well-explained technical details	
Ability to respond to questions	
Timely completion of presentation	
Overall effectiveness of presentation	
TOTAL:	

Mean values for the students' lectures in the class was also calculated, with results shown in Table 4. These evaluations were completed by students only (as is always the case for any course evaluation). The professor and TA attended the lectures and drew their own conclusions about the material presented but did not participate in filling out the survey.

We see from Table 4 that the highest mean is for the explanation of technical details, closely followed by mastery of the subject presented. This result clearly shows that the effectiveness of the methods used for teaching are high, with the technical outcomes achieved by 82.4% (average of both of these items).

In addition to the survey, the technical reports for each project were graded based on a technical rubric and a grade was assigned. For project 1, each group of students wrote a formal report about their technical experience with the inclusion of individual conclusions addressing the performance of their teammates. The conclusion was used as feedback to the instructor on the team-work aspect of the projects. The total project grades were thus calculated as follows: 25% based on self/peer/instructor evaluations, 25% based on student lecture evaluations, and 50% for the written reports.

The calculated grades for the two projects revealed that seven students achieved 90% or better while the other two students achieved 80% or better. The results were satisfactory and indicated that the students understood the technical principles behind the chosen encryption and

Table 3: Teammate evaluation results (Average Values)

Attribute	**Self/Peer Students**	**Professor/TA**	**Overall**
Group meeting attendance	3.92	4.08	4.0
Collaboration with other teammates	3.87	3.48	3.68
Active participation in discussions	3.75	3.78	3.77
Timely completion of tasks	3.27	3.29	3.28
Quality of completed tasks	3.85	3.54	3.70
Contributed significantly to the success of the project	3.67	3.17	3.43
TOTAL:	74.43%	71.13%	72.87%

Table 4: Student lecturer evaluation results (Mean Values)

Criteria	**Mean value of student evaluators**
Clarity of presentation	3.87
Quality and use of visual aid	3.54
Well-organized main points	3.28
Mastery of subject presented	3.93
Well-explained technical details	4.31
Ability to respond to questions	2.87
Timely completion of presentation	4.86
Overall effectiveness of presentation	3.16
TOTAL (Percentage out of 40 points):	74.55%

cybersecurity algorithms. Unfortunately, since this was the first time these projects were offered in this new format of teaching, there is no previous result available for comparison. Positively, end-of-semester evaluations revealed great student satisfaction with the new teaching strategy and technical understanding gained through quality projects.

Conclusion and Future Work

The purpose of this paper was to present an innovative method of applying project-based learning techniques and two cooperative learning strategies: Student-peer learning and jigsaw within the scope of teaching the design and FPGA implementation of encryption and authentication algorithms through hands-on projects. Topics in cybersecurity and secure algorithms have a steep learning curve and require dedication both on the students' and instructors part. The employed cooperative learning strategies are shown to be effective in teaching and accomplishing the desired technical knowledge in addition to fostering students' critical thinking and problem-solving skills. Comments from student evaluations and one-to-one discussions demonstrated that these modified learning techniques helped to develop an in-depth understanding of concepts and helped to gain valuable hands-on experience in digital systems design and verification. The modified learning experience also helped to provide students with additional self-confidence and useful communication skills of technical information through lecturing to their peers. In the future we will continue to deliver the course in this format with improvements, deemed fit, when the class enrollment is open to a larger student-body.

References

[1] N. I. Rafla and H. S. Jacinto, "Flipping a Hardware Design Class: An Encouragement of Active Learning. Should It Continue?," *2018 ASEE Annual Conference & Exposition*, June 2018. https://peer.asee.org/30527.

[2] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 8, no. 7, pp. 495–516, 2018.

[3] S. Bakhtiari, R. Safavi-Naini, J. Pieprzyk, *et al.*, "Cryptographic Hash Functions: A Survey," technical report, Department of Computer Science, University of Wollongong, 1995.

[4] J. W. Thomas, "A Review of Research on Project-Based Learning," San Rafael, California: The Autodesk Foundation, March 2000.

[5] M. Bagheri, W. Z. W. Ali, M. C. B. Abdullah, and S. M. Daud, "Effects of project-based learning strategy on self-directed learning skills of educational technology students.," *Contemporary Educational Technology*, vol. 4, no. 1, pp. 15–29, 2013.

[6] Xilinx Inc., "Vivado Design Suite: User Guide," January 2018.

[7] R. Boute, "Fundamentals of hardware description languages and declarative languages," in *Fundamentals and Standards in Hardware Description Languages*, pp. 3–38, Springer, 1993.

[8] D. Boud, R. Cohen, and J. Sampson, *Peer learning in higher education: Learning from and with each other*. Routledge, 2 ed., 2014.

[9] D. Johson and R. Johnson, *Learning Together and Alone: Cooperative, Competitive, and Individualistic Learning*. Pearson, 5 ed., 1998.

[10] E. Aronson and S. Patnoe, *The Jigsaw Classroom: Building Cooperation in the Classroom*. Longman, 2 ed., 1997.

[11] M. Marhamah and M. Mulyadi, "Jigsaw cooperative learning: A viable teaching-learning strategy?," *Journal of Educational and Social Research*, vol. 3, no. 7, p. 710, 2013.

[12] V. J. Harris and U. S. Department of Commerce, "FIPS 197. Advanced Encryption Standard (AES)," technical report, Computer Security Lab, National Institute of Standards and Technology, November 2001.

[13] R. C.-W. Phan, "Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students," *Cryptologia*, vol. 26, no. 4, pp. 283–306, 2002.

[14] J. M. Turner, C. Furlani, and U. S. Department of Commerce, "FIPS 198-1. The Keyed-Hash Message Authentication Code (HMAC)," technical report, Information Technology Lab, National Institute of Standards and Technology, July 2008.

[15] W. Stallings, "The Whirlpool Secure Hash Function," *Cryptologia*, vol. 30, no. 1, pp. 55–67, 2006.