A Course on Secure Hardware Design of Silicon Chips

Basel Halak[1,2]

[1] Electronics and Computer Science, Southampton University, Southampton, UK
[2] Institute for Learning Innovation and Development, Southampton University, UK
[*] bh9@ecs.soton.ac.uk

Abstract This paper describes the design and evaluation of a secure chip design module for graduate students and junior engineers with an electronics and computer engineering. This course has two broad goals, the first is to teach students how design complex systems on chips using industry standard tools and the second is to educate them on emerging hardware security threats and countermeasures. There are a number of strategies currently been employed to handle the rising complexity of chip design, namely: reuse, abstraction and automation. We aim to show how to employ these approaches to produce working systems within a time-constrained environment similar to that of IC design companies. One of the unique features of this module is its approach of treating hardware security as an integral part of the chip design process and as one of the design metrics which can be evaluated and optimised, this allows students to better understand the root causes of this issue and to think more constructively about potential countermeasures. The course is designed based on the principles of constructive alignment method and Kolb learning cycle. Detailed syllabus and assessment exercises are included. Feedback results from students surveys indicate that the module is very positively received.

1. Introduction

The unyielding demands for silicon chips with cheaper prices and more capabilities have driven the continued scaling of semiconductors technologies for more than sixty years [1]. The use of integrated circuits (ICs) has infiltrated all corners of our lives, homes (TV, kitchens appliances...), workplaces (computers, printers..), cars and even out bodies (e.g. pacemakers). It is now conceivable to fabricate chips which have a billion transistors, which makes it possible to build a complete system on the same silicon die. [2]. This dramatic rise in the chips' complexity meant it was no longer possible for an IC to be designed and implemented by the same team or even in the same country. [3]. The IC production supply chain has become a multinational distributed business, which involves companies from all over the world [4]. Nowadays, the first stage of designing an IC involves outsourcing intellectual property (IP) designs from third party design houses (e.g. ARM or Imagination technologies in the United Kingdom). The second stage is designing additional component and system integration, which is normally done in-house, at the end of this step an IC layout is produced. In the third stage, a blueprint of the design (e.g., GDS-II layout format) is sent to the foundry that develops a costly mask and manufactures the ICs, these are then tested at the manufacturing site and often also at third-party test facilities. It is worth noting that the majority of fabrication facilities are currently based in east Asia in countries such as China and Taiwan . The final stage is IC packaging, which can be also be done at a yet another geographical location. This

distributed nature of the IC supply chain, which relies heavily on the re-use expertise from all over the world, introduces a host of hardware security threats, such as Trojans, sided channel attacks and counterfeiting[5, 6]. The design of modern systems-on-chips requires a range of skills and a very good understanding of numerous areas which spans from high level programming languages down to physical implementation issues [7]. In addition designers need to be well informed of the emerging hardware security threats and possible countermeasures [4]. Therefore, it is expected that the new generation of electronics engineers will need to have knowledge of more interdisciplinary areas and a wider set of skills. A graphical summary of the some of the skills current IC designer need is shown in figure 1.

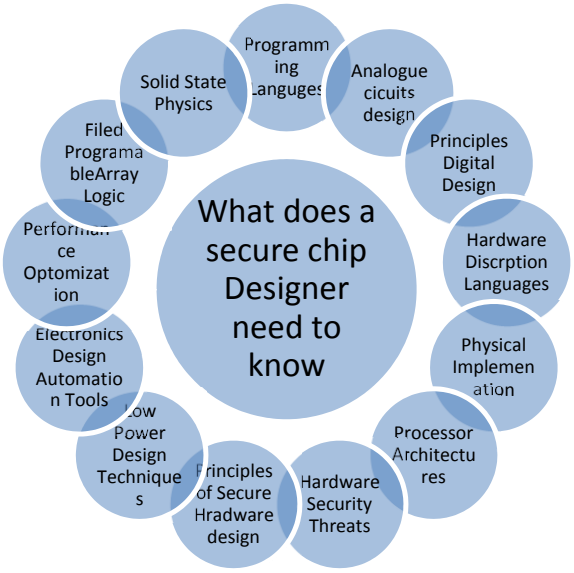

Fig. 1: A summary of Skills Requirements of Secure Chip Designers

It should be noted here is that the skills listed in figure 1 is by no mean comprehensive nor complete, on the contrary, such list is always changing due to the continuous development of the IC design and fabrication processes, that is why microelectronics training courses need to be constantly revised and updated accordingly[1, 3]. This paper describes a secure chip design module which currently being offered to master level students enrolling in electronics engineering courses in Southampton University. The rest of this paper is structured as follows: Section 2 outlines the related works in the literature and explains the main differentiators of the described course. Section 3 describes the design rationale of this module, it also gives an insight into the teaching and assessments approaches we follow in order to enhance the learning experience of our students. Section 4 explains in details the course syllabus including lecture topics and examples of assessment exercises. Section 5 provides a summary of the methods used for course evaluation and the changes, which have been made to ensure and maintain the quality of this

module; it also presents students' feedback scores for the last two academic years. Conclusions are drawn in in section 6.

2. Related Work

We have recently presented a course on the design of modern systems on chips [8], in this work, we describe a significantly updated version of our previously published module in terms of contents and structures. These updates came as natural consequence of the quality assurance process at Southampton University. The aim of these changes was to include several topics on hardware security, a topic which has been overlooked in our previous course. To achieve this, we had to significantly revise lectures' topics, practical labs and the assessment exercise, this is to be able to present security as an integral part of the chip design and optimization processes. Such revision meant the course had to be completely re-designed. There are a number of related works recently reported in the literature. The authors of [7] have described a digital design course which focuses on the use of field programmable gate array (FPGA) devices. The use of programmable SoC platforms (PSoC) for teaching has also been described in [9]. A project-based approach to teaching digital system design has been proposed in [10] which replaces conventional classroom lectures with short laboratory exercises. A number of courses have also been reported which specifically focus on hardware security, one of the earliest work in this area by Farinaz Koushanfar et al. from rice university where they present a course fully dedicated to hardware security threats and potential countermeasures[11]. More recently in [12], the authors reported a three day training course on hardware security for PhD students, which includes theoretical lectures and practical labs, the authors reported good students feedback which indicated high level of interest in this area.

In this paper, the proposed module has two broad goals, the first is to teach students how to design complex systems on chips using industry standard tools and the second is to educate them on important aspects of the chip design process, in particular hardware security and energy efficiency. Another aim of this module to educate students on how to optimise their design in order to meet specific requirements, the course focuses on three metrics: performance, security and energy efficiency. The module described here differs from other courses in the literature in the following aspects:

- It presents emerging hardware security and countermeasures as an integral part of the chip design flow, this helps teaching students how "security" as a design metric can be evaluated and optimised.
- It covers both custom and standard cell design flows, this is important as a system on a chip typically consists of a combination of analogue and digital blocks.
- It emphasises the use of industry-standard tools, which enhances students' employability and equip them with the essential skills to design modern systems-on-chips.

- It focuses on application specific integrated circuit (ASIC) design flow rather than programmable logic (such as FPGAs), There are a number of aspects which are related to the design and optimization process which cannot be appropriately thought using programmable devices, such as low power synthesis, integrity-aware routing methods, therefore ASIC design tools and flows are suitable for covering such issues .

3. Module Design Rationale

One of the most widely used techniques for course design is called constructive alignment [13]. It is an outcome driven method, in which the objectives of each lecture are clearly defined such that students can measure their own success in the learning process by comparing how much they have learned with how much they were supposed to learn. In this approach students are actively encouraged to be independent learners and construct their own knowledge with the help of various learning activities facilitated by the teacher. The course designer needs to ensure that the learning outcomes of the course are well be aligned with those of the learning activities and assessment exercises, such that it becomes possible for students to meet the learning objectives by taking active part the education process and the pedagogic activities. Such alignment must also be present across all level of the education process from program level to the teaching sessions. There are a number of steps to develop a course using the constructive alignment approach (see figure 2).

Fig.2 Stages of Constructive Alignment-based Course Design [13]

3.1. Aims and Intended Learning Outcomes

The first stage in this process is to write the learning outcomes of the module, which need to accurately describe what students should be able to do at the end of the course, this allows learner to set realistic goals of their learning and focus on what they should achieve rather then what is covered in the class. The learning outcomes must be written using active verbs such as “to

explain", "to design", so that they can be used as a metric which can give instant feedback to both the students and their teacher on how successful the teaching session has been. It may also be helpful for such learning outcomes to explicitly define any associated conditions, quantitative and qualitative criteria. For example, "a student must be able to design digital circuit using system Verilog", in this case it is clear that the expectation is to be able to use a specific hardware description language [13, 14]. The aims and intended learning outcomes of this course are written based on the principles of constructive alignment as shown below:

- **Aims**
  1. To provide students with the experience of applying industry standard software tools to complete IC design from conceptual design through to IC layout using industry standard tools.
  2. To explain the vulnerabilities of modern systems on chip design flow and show how these can become legitimate security threats such as hardware Trojans and physical attacks.
  3. To educate students how to improve the trustworthiness of hardware platforms using countermeasures techniques and cryptographic primitives.
- **Intended Learning Outcomes**

  Having successfully completed the module, you should be able to
  1. Describe the principles of systems on Chip Design.
  2. Use industry standards Synopsys and Cadence tools to implement a design from concept to layout.
  3. Optimise the performance and power consumption of integrated circuits using electronic design automation (EDA) tools.
  4. Explain the states of the arts hardware security threats and countermeasures.
  5. Evaluate the security of a hardware implementation.
  6. Design and implement secure hardware primitives such as encryption blocks and physically unclonable functions.

These aims and ILOs are constructively aligned as the first aim is directly connected to ILOs (1, 2 and 3). The second aim is mapped to ILO 4. The third aim is mapped to ILOs (5 and 6). An important principle in writing learning outcomes is that they should be pitched at an appropriate level of understanding for the context [13, 15]. Biggs and Collis devised the hierarchical SOLO (Structure of Observed Learning Outcome) taxonomy to describe the development of understanding [16]. A related structure was developed by Bloom [17]. Bloom's taxonomy outlines six levels of understandings: know, comprehend, apply, analyse, synthesise, and evaluate. Bloom's taxonomy may lend itself more easily to wording ILOs because of its focus on relevant

verbs. The learning outcomes for the module under consideration spanned a range of levels of understanding. That is, they specified that students will be able to "describe" theories (comprehend), "apply" them in practice (Use), "critically evaluate" theories and research (evaluate), and develop and synthesise new knowledge (design, optimise and implement). It should be noted here half of learning outcomes were placed at or above the (synthesis) level of Bloom taxonomy in order to encourage a deep learning approach to learning.

3.2. Teaching's approaches and Learning's Resources

The second step in this process is to create a suitable environment, which allows students to achieve the stated learning outcomes. In this course, the Kolb learning cycle is adopted [18], where in each lecture is tied to a practical session which allow student to explore and learn at their own pace but in a structured lab settings. This approach has proven very effective for teaching IC design tools , which have very complex flow and many setting options, so instead of explaining all these information in class, we provide students with a work plan which allows them to experiment and explore with the tools and more vitally to learn from their own mistake.

In addition, reading materials, lecture nots and lab documentations are all made available at the start of the term. This makes feasible for students to take a less linear approach to learning and allow more iteration and creativity to take place. Our approach has been inspired by previous research in this field, for example in [19] , it is shown that active learning aids deep understanding and performance. We also actively stimulate the learning process by encouraging students to think about challenging problems in the subject field by setting assignments that require them to read recent scientific research papers.

3.3. Design of the Assessments

The third step in this process is to create appropriate assessment tasks which are capable of testing whether or not a student has achieved the intended learning outcomes of the module. Research findings from the literatures have indicated that students define a curriculum based on the assessment and use it to guide their use of time, attention, and resources [20, 21]. This means appropriate assessment exercises can enable and stimulate students learning. In general, the goal of assessment is twofold: to evaluate learning "summative" and to help learning "formative". [12]. In this module, formative assessment exercises are an integral part of both teaching sessions and the practical labs. During the lecture, an interactive approach to delivery is used, which encourages active participation of students and allow them to think critically about the materials being taught and to define gaps in their knowledge. In addition, at the end of each laboratory

session, students are asked to answer a number of thought-provoking questions about their respective design. Each student is then required to discuss his responses with the teacher. Summative assessments comprise three assignments:

- SoC Design Flow Lab Assessment
- Group SoC Design Project
- Individual Hardware Security Assignment

The lab assessment is aimed to evaluate how well students have understood the custom design and standard cell design flows. The objective of the group project is to give students the experience of working within a team on a substantial piece of design, where each one is responsible for one part of the project. At the end, team members need to integrate these parts to produce the final design, this give students a realistic experience of the chip design process in commercial companies. Finally, for the individual assignment, each student is given a number of exercises in which they need to analyse the security metrics of a given design, evaluate the security of an implement circuits to detect potential Trojans and finally design and implement a hardware security primitive. The variety of assessment both formative and summative helps the students achieve the learning outcomes listed above in a supportive and stimulating learning environment.

3.4. Grading

The fourth stage in this process is to final stage in designing a constructively aligned module is find an appropriate approach to grade the summative assessments. In general, there exist two distinct grading approaches: criterion referencing and norm referencing [13] Criterion-referencing is based on the "standards model" in which student's achievement is compared to pre-defined standards (e.g., LOs). Each student's result is independent, and it would be possible for all learners to obtain distinction marks, or for all to fail. Norm referencing is based on the "measurement model" in which student's achievement is compared to norms or others' performances. This method makes the assumption that students' capabilities form a normal distribution, and this should be reflected in their results. Such an approach normally leads to adjusting grades so that a pre-determined proportion of students obtain each grade or the overall distribution of marks has a bell shape. In this module the criterion referencing approach is used to grade the lab based assessment, this this because the latter have specific learning outcomes which need to be achieved, specifically students are expected to demonstrate detailed understanding of the chip design process and the tools used at each stage. The criterion referencing method is also used to grade the individual hardware security assignments, as the latter also have pre-defined solutions which

students need to figure out. For the group design project we employ the norm referencing approach, this is because in this assignment students are normally asked to design a system that to meet given specifications, and to optimize the design to achieve the lower power, minimal area and maximum performance. There are many possible ways in which a design can be optimised to achieve a specific requirement. Finding the best approach normally requires a very good comprehension of the design methodologies of integrated circuits and effective usage of the software tools for electronic design automation ; it also requires a high level of creativity, the implementation of the criterion referencing in this case would be too restricting and impractical. On the other hand, the norm referencing approach can ensure that the best design receives the highest mark.

4. Module Syllabus and Assessment Examples

The topics of the lectures have been chosen such that they are aligned with the overall learning outcomes and aims of the course. We have paid particular attention to the schedule of the lectures, such that each teaching session is time-tabled directly before the related practical lab. This to emphasise the link between the theory and implementation and allow for experimental learning to take place. This is shown in Table 1.

In the first week, the theoretical lecture outlines the main principles of modern chip design and fabrication processes with particular emphasis on the method used to tackle the complexity of current systems-on-chip, namely, design abstraction, design re-use and design automation. This lecture is followed by a lab in which students explore the available electronic design automation (EDA) software tools used at each stage of the design process.

In the second week, the lectures explain the principles of cell based design approach using CMOS technology and describe learn how to experimentally characterise the timing parameters(delay, setup times..), area, and power consumption of an integrated CMOS circuit . In the lab session, students learn how design and implement an exemplar library cell (e.g. inverter, nand gate..) using the custom design flow.

In the third week, students are taught the principles of digital synthesis and performance optimization, then they are given the task to implement a digital multiplier circuits, perform static timing analysis and optimise the operation frequency of their implementation. At the end of this practical session, each student is asked to evaluate the effectiveness of his optimization techniques and discuss his findings with the lab demonstrator or the teacher.

In the fourth week, the principles of physical design are explained in the lecture, these include design planning, placement, clock tree synthesis, and routing, in addition students are taught how to perform a

number of design verification on their layout, and this includes design rule checks, timing, and routing congestions. In the lab sessions, students have the chance to apply their knowledge by physically implementing their synthesised multipliers from the third week lab and optimizing its area. A short discussion of the results takes place at the end of this lab.

In the fifth week, design verifications techniques are explained, these include simulations, emulation, prototyping and formal methods, students also learn how to write effective test vectors. The lab sessions consists of , behavioural, post-synthesis and post-layout simulations the implemented multipliers and comparison of the results in terms of timing and functionality.

In the sixth week, the principles of low power design are explained in the lecture, this is followed by a lab session in which students are asked to reduce the power consumption of a given design by applying various methods at different design stages (architecture, RTL and layout).

In the seventh week, students learn the various hardware security threats with a focus on Trojans insertion and detection techniques. In the lab session, they are asked to insert their own Trojans in a given design in the first part, then they are given the opportunity to apply functional detection methods to analyse the behaviour of a Trojan-infected circuit.

In the eighth week, students are taught the principles of IC counterfeiting, then they are shown how to use physically unclonable functions(PUFs) to protect hardware against this security threat. In the lab session they are asked to design and evaluate the reliability and security metrics of an Arbiter PUF.

Side channels attacks are explained in details in week 9, this is followed by a practical session which focuses on the application of power analysis attack on a cryptographic function.

In the final two weeks, students learn the principles of secure processor design and how to design and implement security cryptographic primitives. The lab session in this week are replaced with tutorial sessions on finite field mathematics, an essential core knowledge for building cryptographic hardware such as AES and elliptic curves blocks.

As stated in section 3, this course has two major design exercises, one is a group design project and the second is an individual security assignments. The specifications of these assignments change every year to limit potential plagiarism. Examples of a group design project include compression hardware, processor implementation, and encryption system design. The individual assignment typically include a number of exercises, each of which is related to one specific aspects of the hardware security topics covered in the lectures such as Trojan detection, design of a cryptographic primitive and side channels analysis.

Table 1: Overview of Course Contents

Week	Lecture Topic	Allocated Time (Hours)	Practical Lab Sessions	Allocated Time (Hours)
1	SoC Design and Fabrication Flow	2	EDA Tool Chains and Design Environment Setup	3
2	CMOS Technology Design and Characterization	2	Inverter Design and Optimization using Tools	3
3	Principles of Digital System Synthesis	1	Implementation of a Digital Multiplier	2
	Performance Optimization Methods	1	Static Timing Analysis and Performance Optimization	1
4	Physical Design Flow	2	Physical design and Optimization of a synthesized multiplier	3
5	Power Reduction Techniques	2	Low Power Design	3
6	Principles of Design Verifications	2	Post-synthesis and poste layout simulation	3
7	A Primer on Hardware Security	1	Insertion and Detection of hardware Trojans	3
	Hardware Trojans Insertion and Detection Techniques	1		
8	Principles IC Counterfeit	1	Design and analysis of an Arbiter PUF	3
	Physical Unclonable Functions	1		
9	Side Channels Physical Attacks	2	Power Analysis of a Secure Core	3
10	Principles of Secure Processor Design	2	N/A	
11	Hardware design of Cryptographic Primitives	2	N/A	

5. Evaluation of Teaching and Learning

The module described above is a result evolution process, which has lasted for more than ten years, during which both its structure and contents have undergone significant changes, most recently in 2015/2016. These modifications are primarily triggered by the quality assurance process at Southampton University. There are a number of objectives for evaluating the teaching and learning process, quality development, quality insurance and finally quality assurance(i.e. to provide evidence for the quality of teaching and learning). To achieve this, information need to be collected about our education process, these will also need to be insightfully analysed in order to make reasonable judgements about which actions to be taken to develop best practices [14]. In contemporary practice in higher education, three

principal sources of feedback information are widely recognized and can be used for evaluation purposes [15], namely: feedback from students, feedback from peers, and self-generated feedback, which comprises reflections and observations by an individual or a group of colleagues on their teaching. All three approaches have been implemented to improve this module, and have led to some specific changes. For example, student's feedback has led to the inclusion of formative assessment at the end of each practical session. The use of referencing approach to grad group projects is adopted based on an advice form a teaching colleague. The reflections of the teaching team have led to a change in the module structure to emphasise emerging hardware threats and to provide countermeasures. This module has been positively received by students as reflected in their feedback scores for the last two academic years, as listed in Table 2, where in, each question is scored from 1 (to indicate a strong disagreement) to 5 (to indicate strong agreement).

Table 2: Student Survey Results

Academic Year	**2014/2015**	**2015/2016**
The module was well organized and ran	4.2	4.6
I was comfortable with the amount of material covered.	4.4	4.6
I was comfortable with the level of prior Knowledge assumed of me.	4.8	4.5
I understood at the beginning of the module what the assessment criteria would be.	4.2	4.6
I found that the resources I needed for the module were easily accessible.	4.8	4.5
I received sufficient feedback during the module to have a sense of what I understood and what I still needed to work on.	4	4.5
The information I received about the module provided an accurate description of what was expected of me.	4.4	4.8
I feel that this was very good module overall.	4	4.5

6. Conclusions

The complexity of chip design process has increased significantly in the last two decades driven by the continuous rise of demands for systems that are more complex and the decrease in the time-to-market available to deliver those designs. This has led to a fundamental change in the nature IC industry production chain; it has become multinational distributed business, which involves companies from all over the word, this brought a whole set of issues related to the security of the hardware and the amount of trust we can place in it. Therefore, the next generation of the IC design engineers will be expected to have knowledge of multidisciplinary areas and a wider set of skills in order to deal with these challenges and continue to be able to design trustworthy systems. This paper has described a course on secure hardware design of silicon chips, which covers all aspects of system design from specifications

to the final silicon implementation, with particular focus on hardware security. Details syllabus and examples of assessment exercises have also been provided. The paper has also described the quality assurance processes used to continuously improve this module. Feedback from students form the past two years indicated the course has been well received.

7. Acknowledgments

I would like to thank the industrial partners for licenses and technical support in particular; we thank Cadence, Synopsys, Mentor Graphics and Euro-practice IC Service. I would also like to thank my colleagues Iain Mcnally, Professor Peter Wilson and Professor Mark Zwolinski for their support.

8. References

[1] S. Sutardja, "1.2 The future of IC design innovation," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, 2015, pp. 1-6.
[2] "International Technology Roadmap for Semiconductors (www.itrs.net)."
[3] J. Erickson and M. Warren, "Modern system on chip challenges demand development of new skills in electronic engineering graduates," in *Interdisciplinary Engineering Design Education Conference (IEDEC), 2013 3rd*, 2013, pp. 32-35.
[4] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proceedings of the IEEE,* vol. 102, pp. 1283-1295, 2014.
[5] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans," *Computer,* vol. 43, pp. 39-46, 2010.
[6] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design & Test of Computers,* vol. 27, pp. 10-25, 2010.
[7] L. E. M. Brackenbury, L. A. Plana, and J. Pepper, "System-on-Chip Design and Implementation," *IEEE Transactions on Education,* vol. 53, pp. 272-281, 2010.
[8] B. Halak and P. Wilson, "Design and evaluation of a system-on-a-chip course," in *2016 11th European Workshop on Microelectronics Education (EWME)*, 2016, pp. 1-6.
[9] Z. Ye and C. Hua, "An Innovative Method of Teaching Electronic System Design With PSoC," *IEEE Transactions on Education,* vol. 55, pp. 418-424, 2012.
[10] O. B. Adamo, P. Guturu, and M. R. Varanasi, "An innovative method of teaching digital system design in an undergraduate electrical and computer engineering curriculum," in *Microelectronic Systems Education, 2009. MSE '09. IEEE International Conference on*, 2009, pp. 25-28.
[11] F. Koushanfar and M. Potkonjak, "Hardware Security: Preparing Students for the Next Design Frontier," in *2007 IEEE International Conference on Microelectronic Systems Education (MSE'07)*, 2007, pp. 67-68.
[12] F. Bruguier, P. Benoit, L. Torres, and L. Bossuet, "Hardware security: From concept to application," in *2016 11th European Workshop on Microelectronics Education (EWME)*, 2016, pp. 1-6.
[13] J. Biggs, *Teaching For Quality Learning At University*, 4 ed. vol. 4: Open University Press; .
[14] P. Ramsden, *Learning to Teach in Higher Education*, 2 ed.: Routledge, 2003.
[15] H. Fry, *A Handbook for Teaching and Learning in Higher Education: Enhancing academic practice*, 4 ed.: Routledge, 2014.

[16] J. B. Biggs and K. F. Collis, "1 - The Evaluation of Learning: Quality and Quantity in Learning," in *Evaluating the Quality of Learning*, ed: Academic Press, 1982, pp. 3-15.
[17] D. R. K. Lorin W. Anderson , Peter W. Airasian, *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives* Pearson, 2000.
[18] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*, 1 ed.: Prentice Hall, 1983.
[19] W. J. Matthews, "Constructivism in the classroom: Epistemology, history, and empirical evidence," *Teacher Education Quarterly,* vol. 30, pp. 51-64, 2003.
[20] R. Hernández, "Does continuous assessment in higher education support student learning?," *Higher Education,* vol. 64, pp. 489-502, 2012.
[21] G. Gibbs, "Does your assessment support your students' learning," *Journal of Learning and Teaching in Higher Education,* pp. 3-31, 2004.