Course Specification

(Postgraduate Programs)

Course Title: Hardware Security
Course Code: CE6015
Program: Master of Science in Computer Engineering
Department: Computer and Network Engineering
College: College of Computing
Institution: Umm Al-Qura University
Version: 2.0
Last Revision Date: 12/4/2025

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)					
2. Course type					
A.	☐University	☐College	☒ Department	☐ Track	
B.	☐ Required		☒ Elective		
3. Level/year at which this course is offered: (Level 3 or Level 4)					
4. Course General Description:					
This course presents a broad range of topics to provide students with a deep understanding of both theoretical and practical aspects of hardware security. It provides an in-depth exploration of hardware security, focusing on the design, implementation, and analysis of secure hardware systems. It covers all levels of the electronic hardware infrastructure, from basic concepts to advanced attack techniques and countermeasures.					
5. Pre-requirements for this course (if any)**:**					
1. Fundamentals of Digital Design 2. Fundamentals of FPGA Design					
6. Co-requirements for this course (if any)**:**					
None					
7. Course Main Objective(s):					
The objective is to: 1. provide an understanding of hardware security threats and vulnerabilities. 2. Design and implement secure cryptographic hardware systems 3. Develop and evaluate countermeasures against hardware attacks. 4. A comprehensive understanding of hardware security testing and verification					

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	45	100

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	45
	Total	45

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Identify challenges in the design of hardware security autonomously	K1	Lectures, and reading assignments	Written exams, assignments, projects and oral presentations
1.2	Explain fundamentals of hardware security concepts snd terminologies	K2		
2.0	**Skills**			
2.1	Design and implement modern computer systems that are secured using principles of hardware security	S1	Lectures, project, discussions, tutorials	Written exams, assignments, projects and oral presentations
2.2	Apply principles of hardware security to solve complex problems	S2		
2.3	Communicate effectively through a written report embodying the design, implementation, evaluation of secured computer systems using principles of hardware security	S3		
2.4	Evaluate the performance of hardware security	S4		

Code	Course Learning Outcomes	Code of PLOs	Teaching Strategies	Assessment Methods
3.0	**Values, autonomy, and responsibility**			
3.1	Demonstrate commitment to ethical and professional responsibilities in hardware security	V1	Lectures, project, discussions, assignments and projects	Group assignments and projects
3.2	Work in a team to implement a project in hardware security	V2	Group assignments and projects	Group assignments and projects

C. Course Content:

No	List of Topics	Contact Hours
1.	Introduction to Hardware Security	3
2.	Introduction to Cryptography	3
3.	Background on Electronic Hardware and VLSI Design	9
4.	Hardware Attacks: Analysis, Examples, and Threat Models	9
5.	Countermeasures Against Hardware Attacks	9
6.	Emerging Trends in Hardware Attacks and Protections	12
Total		45

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Assignment	3, 6, 9 and 12	40
2.	Projects	13	40
3.	Presentation of scientific article		30

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	Hardware Security: A Hands-On Learning Approach by Swarup Bhunia and Mark M. Tehranipoor, Morgan Kaufmann, 2018, ISBN: 978-0128124772
Supportive References	Hardware Security Primitives 1st ed Edition, Mark Tehranipoor, Springer, 2023, ISBN-10 : 3031191846, ISBN-13 : 978-3031191848 Introduction to Hardware Security and Trust, Mohammad Tehranipoor and Cliff Wang, Springer, 2012, ISBN: 978-1441980793

Electronic Materials	The instructor may provide as per requirements
Other Learning Materials	The instructor may provide as per requirements

2. Educational and Research Facilities and Equipment Required:

Items	Resources
facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms
Technology equipment (Projector, smart board, software)	Projector
Other equipment (Depending on the nature of the specialty)	

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students, Program Leaders	Indirect
Effectiveness of students' assessment	Program Leaders	Direct
Quality of learning resources	Students, Faculty	Indirect
The extent to which CLOs have been achieved	Students, Faculty, Program Leaders	Direct and Indirect
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	**Computer and Network Engineering Department Council**
REFERENCE NO.	**The 18th Session Of The Academic Year 1446**
DATE	**15/4/2025**