COURSE OUTLINE

(1) GENERAL

SCHOOLS	Engineering		
ACADEMIC UNIT/UNITS	Computer Engineering and Informatics Department		
TITLE OF MASTER'S DEGREE			
LEVEL OF STUDIES	Undergraduate		
COURSE CODE	CEID_NE591	SEMESTER	Spring (Core Elective)
COURSE TITLE	Hardware Security		

INDEPENDENT TEACHING ACTIVITIES *if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits*	WEEKLY TEACHING HOURS	CREDITS
Lectures and Tutorials	3	3
Laboratory Exercises	2	2
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).	Total	5

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Specialised general knowledge Skills development
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	Greek
IS THE COURSE OFFERED TO ERASMUS STUDENTS	No
COURSE WEBSITE (URL)	https://eclass.upatras.gr/courses/CEID1101/

(2) LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B*
- *Guidelines for writing Learning Outcomes*

Upon successful completion of the course, a student will be able to:

- ✓ *have the appropriate knowledge and background on cryptography and privacy basic principles, based on hardware integration platforms,*
- ✓ *understand the security integration, as basic target of system's design,*
- ✓ *understand IPs and copyright protection of the design, from external breaks and attackers,*
- ✓ *analyze external attacks on hardware platforms and implementations, and to get experienced with protection methodologies,*
- ✓ *implement detection mechanisms, of harmful, additional integrated circuits and systems,*
- ✓ *evaluate the counterfeit detection.*

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology
Adapting to new situations
Decision-making
Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas
Project planning and management
Respect for difference and multiculturalism
Respect for the natural environment
Showing social, professional and ethical responsibility and sensitivity to gender issues
Criticism and self-criticism
Production of free, creative and inductive thinking
……
Others…
…….

Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas
Production of free, creative and inductive thinking

(3) SYLLABUS

- ✓ Theoretical Background and Basic Principles: Security and Trust on Hardware Devices, Current and Future Applications, New Challenges,
- ✓ Basic Terms: Cryptography and Security,
- ✓ Digital Systems Design, Principles and Methodologies,
- ✓ Hardware Performance,
- ✓ Physical Unclonable Functions (PUFs),
- ✓ Random and Pseudo-Random Number Generators,
- ✓ Watermarking and Hardware IPs,
- ✓ Attacks: Fault Injections, Physical, Tamper Resistance,
- ✓ Side Channels Attacks: Models and Countermeasures,
- ✓ Security of Embedded Systems,
- ✓ Crypto-Processors,
- ✓ FPGAs Secure Designs,
- ✓ RFID Tags Security,
- ✓ Trojans Horses: Circuits and Systems,
- ✓ Secure JTAG.

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY *Face-to-face, Distance learning, etc.*	Face to face
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY *Use of ICT in teaching, laboratory education, communication with students*	Wide use of ICT and more specifically: ▪ The course is backed up by a homepage, providing all course materials. This web page is duly updated. ▪ Course announcements are provided electronically and are available via: online news platform, and e-mail. ▪ The communication with the students is performed electronically: via e-mail. An online course forum, is also supported, for questions/answers, comments etc.
TEACHING METHODS *The manner and methods of teaching are described in detail.* *Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.* *The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS*	*Activity* / *Semester workload* Lectures and Tutorials — 39 hours Laboratory Training — 26 hours Study — 80 hours Exams — 5 hours *Course Total* — *150 hours*
STUDENT PERFORMANCE EVALUATION *Description of the evaluation procedure* *Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other* *Specifically-defined evaluation criteria are given, and if and where they are accessible to students.*	The students' assessment is supported in Greek, through a final written examination, twice in each academic year. The examination is organized by development questions, short answer questions, exercises and problems solving. Within ten days of the examination, scores and indicative answers to the exam questions are announced, and posted electronically. It is defined a day and an hour at which students can see their exams' papers about any questions and doubts they may have, as well as to express their disagreement in rating, if they so wish. Then the rating is validated and finalized.

(5) ATTACHED BIBLIOGRAPHY

- Suggested bibliography:

- *N. Sklavos, R. Chaves, G. Di Natale, F. Regazzoni, Hardware Security and Trust, Springer, ISBN: 978-3-3194-4318-8, 2017.*
- *S. Bhunia, M. Tehranipoor, Hardware Security and Trust, ISBN 9780128124772, Elsevier – Morgan Kaufmann, 2018.*
- *M. Tehranipoor, H. Salmani, X. Zhang, Integrated Circuit Authentication, ISBN 978-3-319-00815-8, Springer, 2014.*
- *F. Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc, Cryptographic Algorithms on Reconfigurable Hardware, ISBN 978-1-4419-8079-3, Springer 2006.*

- Related academic journals:

- *IEEE Transactions on Dependable and Secure Computing,*
- *IEEE Transactions on Information Forensics & Security,*
- *IEEE Security and Privacy,*
- *Journal of Hardware and Systems Security, Springer.*