COURSE DESCRIPTION CARD - SYLLABUS

Course name

Cryptography and hardware security in computer engineering

Course

Field of study

Computing Science

Area of study (specialization)

Computing Microsystems

Level of study

Second-cycle studies

Form of study

full-time

Year/Semester

1/2

Profile of study

general academic

Course offered in

Polish

Requirements

compulsory

Number of hours

Lecture

15

Laboratory classes

Other (e.g. online)

Tutorials

Projects/seminars

30

Number of credit points

4

Lecturers

Responsible for the course/lecturer:

Michał Melosik, PhD

email: michal.melosik@put.poznan.pl

wydział: Informatyki i Telekomunikacji

adres: Piotrowo 3A 60-965 Poznań

Responsible for the course/lecturer:

Prerequisites

The student should have basic knowledge of: signal processing basics, electronics, VHDL and VHDL-AMS

hardware description language, programming basics. The student should have the ability to solve basic problems in the design and analysis of digital and analog systems. The student should have the ability to search for necessary information in indicated sources. The student should be able to draw conclusions and shape the evaluation of presented solutions. Additionally, the student should also understand the necessity of broadening his competences and should be ready to cooperate within the team. Moreover, in terms of social competences, the student must present such attitudes as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, respect for other people.

Course objective

1. Acquaint students with the basic issues of cryptography and hardware security in computer engineering.

2. To provide students with basic knowledge on the structure of selected cryptographic systems.

3. To develop the ability to create and adapt in the hardware layer of embedded systems of selected cryptographic modules

4. Developing students' ability to select the optimal hardware platform and IPCores.

5. Shaping in students the skills of teamwork through the implementation of project elements and combining them into a whole.

Course-related learning outcomes

Knowledge

The student has an advanced and detailed knowledge of the design of information systems, embedded systems, electronic circuits; he or she has an advanced and detailed knowledge of processes from the boundaries of computer science and electronics occurring in the life cycle of embedded security systems and cryptography; he or she knows advanced methods and techniques used in the design and verification of hardware security systems; he or she has knowledge of codes of ethics related to scientific work in the field of hardware security in computer engineering.

Skills

The student is able to interdisciplinary combine selected issues in electronics and physics with knowledge from various areas of computer science; he or she is able to assess the usefulness of new methods in the design of hardware security systems and use the latest methods to test them; he or she is able to see the limitations of methods and tools used in the design of hardware cryptographic systems in the context of hardware security; using new methods, he or she is able to solve complex threat detection problems in hardware cryptography and hardware data security.

Social competences

The student understands that in computer science, and especially in the design of hardware cryptographic systems, knowledge and skills quickly become obsolete; he or she understands the importance of using the latest IT developments in solving research problems to improve hardware security.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:
Formulation evaluation:

- in terms of lectures: based on answers to questions about the material discussed in previous lectures,

- in terms of projects/exercises: based on the evaluation of the current progress of the tasks and the final project evaluation,

Summary evaluation:

- in the scope of lectures, verification of the assumed educational results is carried out by conducting a written or oral examination

- In the scope of projects/laboratories, verification of the assumed educational results is carried out by evaluating the progress of the project task, continuous evaluation, rewarding the increase in the ability to use the learned principles and methods, evaluation of the level of project implementation. Evaluation of prepared documentation/report.

Obtaining additional points for activity during classes, especially for:

- discussing additional aspects of the issue,

- effectiveness of applying the acquired knowledge while solving a given problem,

- the ability to cooperate within a team practically carrying out a specific task in the laboratory,

- remarks related to the improvement of didactic materials.

Programme content

The following issues will be discussed in the lectures:

- TRBG, PRBG, CSPRBG random generators and their applications of hardware security of embedded systems and computer engineering

- selected cryptographic algorithms

- encryption modes

- cryptographic system design process, security requirements, verification tools, alternative cryptographic methods on the example of chaotic cryptography

- PUF in microelectronics

- PCB hardware security, hardware attacks on PCB

- Hardware Trojans

- directions of development of contemporary cryptography (quantum random generators)

Design classes include the implementation of related projects:

- practical implementation of selected hardware, software and hardware modules.

Teaching methods

lecture: multimedia presentation, traditional lecture,

project activities: project implementation according to guidelines, discussion, teamwork

Bibliography

Basic

1. A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przykładach, wyd. BTC, 2010

2. M. Karbowski, Podstawy kryptografii., wyd. Helion, 2006

3. A. J. Menezs, Kryptografia stosowana, wyd. WNT, 2005

4. C. Parr, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010

Additional

1. M. Melosik, W. Marszalek, "Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators", Electronics Letters 52 (11), 919-921

2. M. Melosik, P. Sniatala, W. Marszalek, "Hardware Trojans detection in chaos-based cryptography", Bulletin of the Polish Academy of Sciences Technical Sciences, 65 (5), 725-732 2017

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4
Classes requiring direct contact with the teacher	45	2
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1]	55	2

1 delete or add other activities as appropriate