DOCTORAL SCHOOL OF WROCŁAW UNIVERSITY OF SCIENCE AND TECHNOLOGY

SUPERVISOR DECLARING/CONDUCTING COURSE: prof. Marek Klonowski
DEPARTMENT: K64/W11
SCIENTIFIC DISCIPLINE: Computer Science and Telecommunication

COURSE CARD

Course name in Polish: Algorytmiczne i matematyczne podstawy ochrony prywatności

Course name in English: **Algorithmic and mathematical foundations of privacy protection**

Course language: Polish~~/ English~~

The course is intended for all PhD students: ~~YES~~ / NO (Mathematics, Computer Science, Computer Science and Telecommunication)

~~1) BASIC COURSE~~
2) SPECIALIST COURSE
~~3) SEMINAR~~
~~4) HUMANISTIC COURSE~~
~~5) LANGUAGE~~
~~6) RESEARCH SKILLS~~

Subject code: ITQ100249W

* delete as applicable

	Lecture	Foreign language course	Seminar	Mixed forms
Number of hours of organized classes in university (ZZU)	30			
Grading	Exam	Exam	Oral presentation	Exam, inspection, evaluation classes

PREREQUISITES RELATING TO KNOWLEDGE, SKILLS AND OTHER COMPETENCES

1. Programming
2. Fundamentals of probability
3. Basic knowledge in algorithms

\

COURSE OBJECTIVES

C1 Learning fundamental paradigms of privacy protection
C2 Learning most important methods of constructing and analysis of privacy protecting algorithms

PROGRAM CONTENTS

	Form of classes	Number of hours
1	Introduction – what is differential privacy ? Different concepts of privacy.	2
2	Probability theory – revision of basic facts	3
3	Differential privacy; Laplace and Gauss mechanism	2
4	Exponential mechanism, Composition theorems	3
5	Privacy for releasing linear queries	4
6	Privacy mechanism design	4
7	Privacy and continual observation	4
8	Lower bounds and computational complexity	2
9	Privacy vs machine learning	4
10	Differential privacy and cryptography	2
	Total hours	**30**

TEACHING TOOLS USED
N1. Lecture N2. Discussion N3. Solving exercises

ACHIEVED SUBJECT LEARNING OUTCOMES		
Type of learning outcome	Code of learning outcome	Assessment of learning outcome
Knowledge	P8S_WG	Exam
Knowledge	P8S_WK	Exam

PRIMARY AND SECONDARY LITERATURE

PRIMARY LITERATURE:

[1] Cynthia Dwork, Aaron Roth, The Algorithmic Foundations of Differential Privacy, Foundations and trends in TCS, 2014
[2] Attoh-Okine Nii O., Big Data and Differential Privacy, John Wiley & Sons Inc, 2017

SECONDARY LITERATURE:

SUBJECT SUPERVISOR (NAME AND SURNAME, E-MAIL ADDRESS)

Marek Klonowski, Marek.Klonowski@pwr.edu.pl