Summary
This course will provide students with the knowledge to tackle the design of privacy-preserving ICT systems. Students will learn about existing technologies to protect privacy, and how to evaluate the protection they provide.

Content
The course will delve into the following topics:

• Privacy definitions and concepts, and the socioeconomic context of privacy: economics and incentives, ethics, regulation.

• Cryptographic privacy solutions: identity management and anonymous credentials, zero-knowledge proofs, secure multi-party computation, homomorphic encryption, garbled circuits, Private information retrieval (PIR), Oblivious RAM (ORAM)

• Anonymization and data hiding: k-anonymity, l-diversity, t-proximity; dummy use, differential privacy and Laplacian noise; composable

• Machine learning and privacy: how machine learning can be use to infer private information; and how much information can be learned from machine learning models.

• Protection of metadata: anonymous communications systems, location privacy, censorship resistance.

• Online tracking and massive surveillance.

• Evaluation of privacy preserving systems - notions, definitions, quantification / computation

• Fairness and transparency and their interplay with privacy

Keywords
Privacy, anonymity, homomorphic encryption, ethics

Learning Prerequisites
Recommended courses
COM 402 Information Security and Privacy
Important concepts to start the course
Basic programming skills; basics of probabilities and statistics; basics of cryptography

Learning Outcomes
By the end of the course, the student must be able to:
• Select appropriately privacy mechanisms
• Develop privacy technologies
• Assess / Evaluate privacy protection
• Reason about privacy concerns

Teaching methods
Lectures and mini-projects developing privacy enhancing technologies supervised by assistants.

Expected student activities
Attending lectures
Execute mini-projects

Assessment methods
Written final exam and mini-project during the course

Supervision
Assistants	Yes