Summary
This advanced 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 cover the following topics:
- Privacy definitions and concepts
- Privacy-preserving cryptographics solutions: anonymous credentials, zero-knowledge proofs, secure multi-party computation, homomorphic encryption, Private information retrieval (PIR), Oblivious RAM (ORAM)
- Anonymization and data hiding: generalization, differential privacy, etc
- Machine learning and privacy
- Protection of metadata: anonymous communications systems, location privacy, censorship resistance
- Online tracking and countermeasures
- Privacy engineering: design and evaluation (evaluation metrics and notions)
- Legal aspects of privacy

Keywords
Privacy, anonymity, homomorphic encryption, secure multi-party computation, anonymous credentials, ethics

Learning Prerequisites
Required courses
COM-301 Computer security
COM-402 Information security and privacy

Recommended courses
COM-401 Cryptography and security

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 written exercises to deepen understanding of concepts
Programming-oriented assignments to practice use of privacy technologies

**Expected student activities**
Participation in the lectures. Active participation is encouraged.
Participation in exercise session and complete the exercises regularly
Completion of programming assignments

**Supervision**
Assistants Yes

**Resources**
Moodle Link
• https://go.epfl.ch/CS-523