

CS-523

**Advanced topics on privacy enhancing technologies**

| Cursus                              | Sem.     | Type |
|-------------------------------------|----------|------|
| Computer and Communication Sciences |          | Opt. |
| Computer science                    | MA2, MA4 | Obl. |
| Cyber security minor                | E        | Opt. |
| Cybersecurity                       | MA2, MA4 | Obl. |
| Data Science                        | MA2, MA4 | Opt. |
| SC master EPFL                      | MA2, MA4 | Opt. |

|                            |                 |
|----------------------------|-----------------|
| Language of teaching       | English         |
| Credits                    | 8               |
| Session                    | Summer          |
| Semester                   | Spring          |
| Exam                       | Written         |
| Workload                   | 240h            |
| Weeks                      | 14              |
| <b>Hours</b>               | <b>6 weekly</b> |
| Courses                    | 3 weekly        |
| Exercises                  | 1 weekly        |
| Project                    | 2 weekly        |
| <b>Number of positions</b> |                 |

**Remark**

Pas donné en 2025-26 - This course is a "depth" for Cyber Security master program and Cyber Security minor.

**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 cryptographic 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 and Privacy  
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

### Assessment methods

- Projects (40%)
- Midterm (20%)
- Final exam (40%)

### Supervision

Assistants                      Yes

### Resources

#### Moodle Link

- <https://go.epfl.ch/CS-523>