	UE-SEC2: Secure Communications	Semester 1
Contributes to	MICAS	

Coordinators:	Olivier RIOUL, Telecom Paris Mireille SARKISS, Telecom SudParis	
Volume:	30h	**3 ects**
Hours:	Lectures: 19.5h, Exercises: 6h, Seminars: 3h	
Assessment:	2 Quizzes and 1 Final Exam	
Language:	English	

Objectives:
The course describes the information-theoretic basics to secure communications. A first part covers physical layer security techniques exploiting the physical properties of wireless channels. It includes the introduction of wiretap channels, secrecy criteria and measures, coding designs to achieve secrecy, secret key generation and other advanced topics in wireless networks. Then, a second part overviews the problem of side-channel with its main attacks, countermeasures and applications.

Outcomes:
On completion of the course students should be able to:
- Understand and familiarise with the information-theoretic foundations of secure communications
- Analyse the practical physical layer security techniques and describe their limits
- Explain the side-channel analysis attacks and discuss the different countermeasures
- Acquire the current state of research on secure communications and their applications in real scenarios

Prerequisite
- Introduction to Information Theory
- Introduction to Communication Theory

Syllabus
- Physical Layer Security for wireless communications: Wyner's Wiretap channel
- Secrecy metrics: weak/strong secrecy, secrecy capacity, secrecy outage probability
- Specific wiretap channels: Gaussian, MIMO, Broadcast Channels (BC) and Multiple-Access Channels (MAC)
- Lattice coding for PHY security and introduction to lattice-based cryptography
- Secure coding schemes: LDPC codes, Polar codes
- Secure network coding
- Secret key generation and secret key agreement
- Other topics: cooperative jamming, secure coding for distributed storage, secure coded caching
- Side-Channel Analysis: physical setup: probing, timing, sounding
  - Leakage models in embedded symmetric crypto : monobit, Hamming weight
  - Success rate vs. guessing entropy
  - Best attacks (Maximum Likelihood (ML), template attacks, Difference of Means (DoM), ...) and countermeasures (masking, shuffling, ...)
  - Asymptotic results: confusion coefficients, exponents
  - Information leakage theory and applications

Bibliography:

- M. Bloch and J. Barros, "Physical layer security: From information theory to security engineering", 2011.
- Y. Liang, H. V. Poor and S. Shamai, "Information theoretic security", 2009.
- X. Zhou, L. Song and Y. Zhang, "Physical Layer Security in Wireless Communications", 2013.
- S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks", 2007.