

Two PhD Positions in Information-Theoretic Security

ETIS Laboratory, Cergy-Pontoise, France

Recently, there has been growing interest in physical-layer security, which is indicated as a possible way to emancipate networks from classic, complexity-based security approaches. Practical motivations for exploring physical-layer security include, e.g., the need for low-latency and low-cost communications in IoT, and the breakthrough in quantum computing.

Each PhD student recruited for the PHEBE project (Physical-Layer Security for Beyond 5G) will focus on one or more of the following topics.

- **Covert communication.** Also known as “communication with low probability of detection,” this is a scenario where the eavesdropper attempts to guess whether the transmitter is sending a message or not, while the transmitter tries to prevent the eavesdropper from making a good guess. In this project, we shall study covert communication over realistic channels whose noise fluctuates with time. We shall also design error-correcting codes for covert communication.
- **State masking and location privacy.** We seek communication schemes that can hide the sender’s physical location from a potential eavesdropper. We model the location as a parameter in the channel model, i.e., a “channel state.” The problem hence can be formulated as one where the transmitter wishes to convey a message without letting the eavesdropper learn the channel state.
- **Fuzzy extractors for key generation.** Physical measurements are a widely available source of randomness in nature, but they are not uniformly random and are affected by noise. Fuzzy extractors can convert such noisy measurements into uniformly random strings which can be reproduced reliably. In this project, we will focus on fuzzy extractors for continuous sources, and investigate how to extract most of the entropy from the sources while reducing the noise.

Starting date: October 1st, 2020 (can be postponed).

Requirements: The candidates should have completed a master’s degree (or equivalent) in Electrical Engineering, Computer Science, Applied Mathematics, or related areas by the starting time of their PhD. Good ability in mathematical reasoning is very important. Knowledge of Information Theory and Coding Theory is desirable though not mandatory.

Application: A CV and a cover letter should be sent to one of the email addresses below.

Contact: **Ligong Wang** (ligong.wang@ensea.fr), **Maël Le Treust** (mael.le-treust@ensea.fr),
Laura Luzzi (laura.luzzi@ensea.fr)

Laboratoire ETIS (UMR 8051) – Equipe Information, Communication et Imagerie (ICI)
6, avenue du Ponceau, 95014 Cergy-Pontoise

