Master Thesis

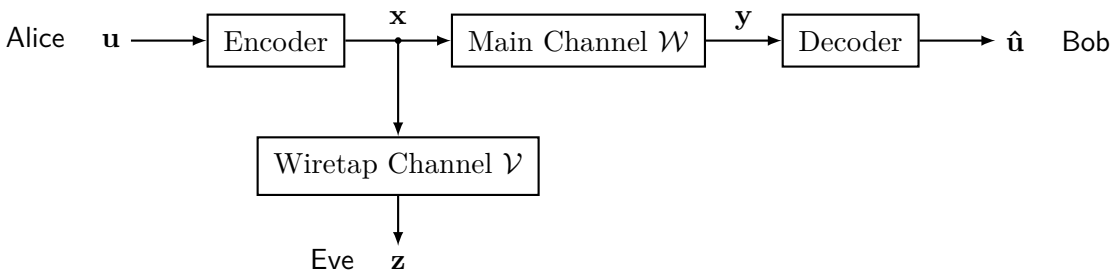
Chair for Theoretical Information Technology | RWTH AACHEN UNIVERSITY

Coding on Wiretap Channels

Research Area:
Information theory, coding theory, cryptography

Keywords:
Wiretap channels, secrecy capacity, physical layer security

Description:
With the advent of quantum computers marginalizing (some) cryptographic approaches relying on computational hardness assumptions, attention turns to other measures to ensure private communications. A classical approach is to inspect wiretap channel models, introduced by Wyner and others. Based on certain relations between the legitimate channel $\mathcal{W}$ and the channel $\mathcal{V}$ accessible to an eavesdropper, the information-theoretic notion of a secrecy capacity of this arrangement may be put forward.



Goal:
As a starting point, wiretap channel models and information-theoretic notions of secrecy shall be analysed. To realize practical systems, approaches to achieve, *e.g.*, secrecy capacity in certain scenarios have to be evaluated and may be extended. Several such concepts can be exploited. To support the analysis, a review of the mathematical techniques involved will prove helpful.

Prerequisites:

- Fundamentals of information theory and coding, and willingness to pick up modern coding theory.
- Strong background in mathematics and statistics in particular.
- Programming in Python (preferred) or MATLAB.

We offer a friendly work environment, intensive support and guidance, and good equipment. Depending on the candidate's interest, the focus of this thesis may be varied between purely theoretical work and a more practical, applied approach to the topic.

Supervisor:

- Christopher Schnelling ✉ schnelling@ti.rwth-aachen.de ☎ +49 241 80 20750