Forschungspraxis

Code Design for Secret Key Generation/ Left over Hash Lemma

The source model of secret key generation deals with the idea of Alice and Bob generating a key in a distributed manner from correlated observations. This key must be kept secret from an eavesdropper. In this internship/thesis the student will start by looking at a simpler model which corresponds to the left over hash lemma. The student will build on some preliminary work done by me to design codes for the extraction of left over hash in a simple setting. After this the student will (if time permits) extend the work to design codes for simple cases of distributed secret key generation for the source model.

Advisors

Rana Amjad