FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Elektrotechnik-Elektronik-Informationstechnik

EEI KOLLOQUIUM

How to Use Secret Keys for Secure Broadcasting: One-Time Pad vs. Wiretap Coding

Prof. Dr.-Ing. Rafael Schäfer
TU Berlin

Mittwoch, der 20.07.2016, 14^{00} Uhr
Seminarraum E 1.12, Cauerstraße 7, Erlangen

Diskussionsleitung: Prof. Dr.-Ing. R. Müller

Shannon was the first who studied the problem of secure communication from an information theoretic perspective. In 1949, he showed that a secret key available to transmitter and receiver can be used as a one-time pad to allow perfect security of transmitted information. In the absence of secret keys, it was Wyner who showed 1975 that secure communication can be achieved by so-called wiretap coding which solely exploits the properties of the noisy communication channel to establish security. In this talk, the particular communication scenario is analyzed, where a common message has to be securely broadcasted to two legitimate receivers, while keeping an external eavesdropper ignorant of it. The transmitter shares independent secret keys of arbitrary rates with both legitimate receivers, which can be used in different ways: They can be used as one-time pads to encrypt the common message or they can be interpreted as fictitious messages used as randomization resources for wiretap coding. Both approaches are discussed and the secrecy capacity is derived for various cases. Depending on the qualities of the legitimate channel and eavesdropper channel, either one- time pad, wiretap coding, or a combination of both turns out to be capacity-achieving.