

Reciprocity, the key to physical-layer key generation

Abstract:

Physical-layer security is based on common randomness. "Common" means reciprocity of the channel. We describe reciprocity as a very basic property that electrical engineering students are typically exposed to at the beginning of their studies as an important characteristic of passive two-ports. We are looking into examples for wireline and wireless transmission. For the first, we are discussing inhouse power lines and the parameters that can be used for key generation. For the latter and usually different view onto the channel, we will look into wireless TDD and FDD systems, also there point out the parameters that show the desired reciprocity.

Non-coding and coding approaches are introduced for key reconciliation, i.e., reciprocity enforcement. Shortly, we will also look into multi-user key distribution.