REI SAFAVI-NAINI, University of Calgary
cryptographic keys from noisy channels

In Secure Key Establishment (SKE) problem, Alice and Bob want to share a secure key by communicating over a pair of noisy channels that leak information to Eve. We assume parties do not have any other sources of randomness. We derive lower and upper bounds on the secret key capacity of this setup and show that SKE is possible even if in both channels, Eve has a less noisy reception than Alice and Bob's.