ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 10

FS 11
Prof. R. Renner

Exercise 10.1 Quantum Key Distribution

1. Find the error rate introduced by the intercept-resend attack for the BB84 QKD protocol.
2. Find the key rate for the six-state QKD protocol.

(This question is worth 8 Testat points, and can be done in groups of up to three people)

The second question can be broken down into the following steps:

1. Turn the P+M (prepare and measure) QKD (quantum key distribution) six-state protocol into an entanglement based one, and find the entangled state Alice and Bob would ideally share many copies of.
2. Find out what the state Alice and Bob actually shared, ρ_{AB}, after Eve has done her attack, and Alice and Bob know they had an error rate Q. You should find that the state is diagonal in the Bell basis.
3. Finally, find what the key rate is using the Devetak-Winter security bound.