Quantum Information Theory
Spring semester, 2017

Assignment 11
Assigned: Friday, June 16, 2017
Due: Tuesday, July 4, 2017 M. Skoglund

Problem 11.1: Describe the setup and results for the quantum wiretap channel.

Problem 11.2: Describe the BB84 protocol.

Problem 11.3: Describe the B92 protocol.

Problem 11.4: Since optimal transmission for the quantum wiretap channel can be used to share any message between Alice and Bob, it can also be used for sharing a secret key. Discuss the pros and cons of an approach based on coding for the quantum wiretap channel compared with "simple" protocols such as B84 and B92.

Problem 11.5: The secrecy condition for the quantum wiretap channel can be stated: For any $\varepsilon > 0$ there is an N such that for $n > N$

$$V(\sigma_m, \sigma) < \varepsilon$$

where σ_m is the state observed by Eve when Alice's message is $W = m$ and where $\sigma = M^{-1} \sum \sigma_m$. Using Fanne's inequality, show that this implies that $n^{-1} I(W; \hat{W}) \to 0$ where $\hat{W}$ is any classical information that Eve can extract about Alice's message W.

Problem 11.6: As was done in HW8.6 for classical communication over a quantum channel, one can use a common randomness generation argument to prove an outer bound for the secrecy capacity of the quantum wiretap channel. Based on the same argumentation as in HW8.6, use the result in HW11.5 (above) to show that if $V(\sigma_m, \sigma) < \varepsilon$ then

$$\log M \leq S(\rho_X; \rho_B) - S(\rho_X; \rho_E) + f(M, \varepsilon) \leq \mathcal{P}(\mathcal{R}^{\otimes n}) + 2f(M, \varepsilon)$$

where $f(M, \varepsilon)$ is a function of M and ε that goes to zero in ε. Here M, ρ_X, ρ_B, ρ_E, $\mathcal{P}$ and $\mathcal{R}$ are defined as in Slides 11.6–9.

Problem 11.7: Prove the necessary and sufficient conditions for the Shannon cipher system.