Quantum Information Theory
Series 11

Exercise 11.1 One-time Pad

Consider three random variables: a message M, a secret key K and a ciphertext C. We want to encode M as a ciphertext C using K with perfect secrecy, so that no one can guess the message from the cipher: $I(M:C) = 0$.
After the transmission, we want to be able to decode the ciphertext: someone that knows the key and the cipher should be able to obtain the message perfectly, i.e. $H(M|C,K) = 0$.
Show that this is only possible if the key contains at least as much randomness as the message, namely $H(K) \geq H(M)$.

Exercise 11.2 Tightness of secrecy and correctness

Let ρ_{ABE} be the tripartite ccq-state held by Alice, Bob and Eve after a run of a QKD protocol. We showed in the lecture that if the protocol is ε_1-secret,

$$\delta\left(\rho_{AE}^{\text{key}}, \tau_A \otimes \rho_E^{\text{key}}\right) \leq \varepsilon_1,$$

and ε_2-correct,

$$\Pr[A \neq B] \leq \varepsilon_2,$$

then the real and ideal systems are $\varepsilon = \varepsilon_1 + \varepsilon_2$ indistinguishable, i.e.,

$$\exists \sigma_E \text{ such that } \delta(\rho_{ABE}, \tilde{\rho}_{ABE}) \leq \varepsilon \tag{1}$$

where $\tilde{\rho}_{ABE}$ is the tripartite state held be the distinguisher after interacting with the ideal system $\sigma_E \mathcal{K}$ for an optimal simulator σ_E.
Show that if (1) holds for some ε, then the protocol must be ε-correct and 2ε-secret.
Tip: you cannot assume that (1) is necessarily satisfied by the same simulator used to prove the converse.

Exercise 11.3 A min-entropy chain rule

Let ρ_{XZE} be a ccq-state. Show that the following holds:

$$H_{\min}^{\varepsilon}(X|ZE)_\rho \geq H_{\min}^{\varepsilon}(X|E)_\rho - \log|\mathcal{Z}|.$$

Recall that

$$\begin{aligned}
H_{\min}(X|E)_\rho &:= -\log p_{\text{guess}}(X|E)_\rho, \\
H_{\min}^{\varepsilon}(X|E)_\rho &:= \max_{\bar{\rho} \in \mathcal{B}^{\varepsilon}(\rho)} H_{\min}(X|E)_{\bar{\rho}}, \\
\mathcal{B}^{\varepsilon}(\rho) &:= \{\bar{\rho} : P(\rho, \bar{\rho}) \leq \varepsilon\},
\end{aligned}$$

and that the purified distance $P(\rho, \sigma)$ satisfies the following property. Let $|\varphi\rangle$ be a purification of ρ, then

$$P(\rho, \sigma) = \max_{|\psi\rangle} \delta(|\varphi\rangle, |\psi\rangle),$$

where $|\psi\rangle$ is a purification of σ.

Exercise 11.4 Privacy amplification with smooth min-entropy

A function $F : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (quantum-proof, strong) (k, ε)-extractor if for all cq states ρ_{XE} with $H_{\min}(X|E) \geq k$ and a uniform Y,

$$\delta\left(\rho_{F(X,Y)YE}, \tau_U \otimes \tau_Y \otimes \rho_E\right) \leq \varepsilon.$$

Show that for any (k, ε)-extractor F, if a cq state ρ_{XE} has smooth min-entropy $H_{\min}^{\bar{\varepsilon}}(X|E) \geq k$, then

$$\delta\left(\rho_{F(X,Y)YE}, \tau_{F(X,Y)} \otimes \tau_Y \otimes \rho_E\right) \leq \varepsilon + 2\bar{\varepsilon}.$$