Quantum Information Theory
Solutions 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: $I(C : M) = 0$.
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 $H(K) \geq H(M)$.

First note that

$$\begin{aligned} I(C : M) - I(C : M|K) &= I(M : K) - I(M : K|C) \\ &= I(K : C) - I(K : C|M), \end{aligned}$$

and that mutual information is non-negative. We introduce $x = I(C : M|K)$, $y = I(M : K|C)$ and $z = I(K : C|M)$ and, using $I(C : M) = 0$, we get

$$x - I(C; M) = x = y - I(M; K) = z - I(K; C). \tag{1}$$

Using the two conditions, we write

$$\begin{aligned} H(M) &= H(M|C, K) + I(C : M) + I(K : M|C) = y, \quad \text{and} \\ H(K) &= H(K|M, C) + I(M : K) + I(M : C|K) \geq y - x + z. \end{aligned}$$

However, since $y \geq x$ and $z \geq x$ (from (1)), we get $H(K) \geq H(M)$.

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,

$$p_{key}\delta\left(\rho^{key}_{AE}, \tau_A \otimes \rho^{key}_E\right) \leq \varepsilon_1,$$

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.,

$$\exists \sigma_E \textit{ such that } \pi_A\pi_B(\mathcal{A}\|\mathcal{Q}) \approx_\varepsilon \sigma_E\mathcal{K}. \tag{2}$$

Show that if (2) holds for some ε, then the protocol must be ε-correct and 2ε-secret.
Tip: you cannot assume that (2) is necessarily satisfied by the same simulator used to prove the converse.

Let $\tilde{\rho}_{ABE}$ be the tripartite state held be the distinguisher after interacting with the ideal system $\sigma_E\mathcal{K}$ for an optimal simulator σ_E, and let Γ be the positive operator which projects the AB system on all states with $A \neq B$. Then

$$\varepsilon \geq \delta(\rho_{ABE}, \tilde{\rho}_{ABE}) \geq \delta(\rho_{AB}, \tilde{\rho}_{AB}) \geq \operatorname{tr}[\Gamma(\rho_{AB} - \tilde{\rho}_{AB})] = \Pr[A \neq B]_\rho.$$

The last equality holds because by construction of the ideal key resource $\mathcal{K}$, $\mathrm{tr}(\Gamma\tilde{\rho}_{AB}) = 0$ (for any simulator σ_E).

Let $p_{\mathrm{key}}\rho_{AE}^{\mathrm{key}}$ be the state of the real AE system held by the distinguisher after projecting on the subspace in which a key is generated, and let $\tilde{p}_{\mathrm{key}}\tau_A \otimes \tilde{\rho}_E^{\mathrm{key}}$ be the state of the ideal AE system for the same projection. Note that we cannot assume that $p_{\mathrm{key}} = \tilde{p}_{\mathrm{key}}$ or $\rho_E^{\mathrm{key}} = \tilde{\rho}_E^{\mathrm{key}}$, since we do not know how the simulator σ_E works.

Since

$$\varepsilon \geq \delta(\rho_{ABE}, \tilde{\rho}_{ABE}) \geq \delta(p_{\mathrm{key}}\rho_{AE}^{\mathrm{key}}, \tilde{p}_{\mathrm{key}}\tau_A \otimes \tilde{\rho}_E^{\mathrm{key}}) \geq \delta(p_{\mathrm{key}}\rho_E^{\mathrm{key}}, \tilde{p}_{\mathrm{key}}\tilde{\rho}_E^{\mathrm{key}}),$$

we have

$$\begin{aligned}
p_{\mathrm{key}}\delta\left(\rho_{AE}^{\mathrm{key}}, \tau_A \otimes \rho_E^{\mathrm{key}}\right) &= \delta\left(p_{\mathrm{key}}\rho_{AE}^{\mathrm{key}}, p_{\mathrm{key}}\tau_A \otimes \rho_E^{\mathrm{key}}\right) \\
&\leq \delta\left(p_{\mathrm{key}}\rho_{AE}^{\mathrm{key}}, \tilde{p}_{\mathrm{key}}\tau_A \otimes \tilde{\rho}_E^{\mathrm{key}}\right) + \delta\left(\tilde{p}_{\mathrm{key}}\tau_A \otimes \tilde{\rho}_E^{\mathrm{key}}, p_{\mathrm{key}}\tau_A \otimes \rho_E^{\mathrm{key}}\right) \\
&\leq \varepsilon + \varepsilon.
\end{aligned}$$

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

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

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

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

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

Let $\rho_{XZE} = \sum_{x,z} p_{x,z}|x\rangle\langle x| \otimes |z\rangle\langle z| \otimes \rho_E^{x,z}$ and let $\{\Gamma_x^z\}_x$ be the optimal measurement of the E system to guess x given that $Z = z$. A possible strategy for guessing XZ given E is to pick z uniformly at random then apply the measurement $\{\Gamma_x^z\}_x$ to the E system. This strategy would succeed with probability

$$\sum_{x,z} p_{x,z}\frac{1}{|\mathcal{Z}|}\mathrm{tr}(\Gamma_x^z\rho_E^{x,z}) = \frac{1}{|\mathcal{Z}|}p_{\mathrm{guess}}(X|ZE)_{\rho}.$$

We thus have

$$p_{\mathrm{guess}}(X|E)_{\rho} \geq p_{\mathrm{guess}}(XZ|E)_{\rho} \geq \frac{1}{|\mathcal{Z}|}p_{\mathrm{guess}}(X|ZE)_{\rho},$$

hence

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

To prove the smooth version, let $\bar{\rho}_{XE} \in \mathcal{B}^{\varepsilon}(\rho_{XE})$ be the state which maximizes $H_{\min}(X|E)_{\bar{\rho}}$. Let $\bar{\rho}_{XZE}$ be an extension of $\bar{\rho}_{XE}$ such that $P(\rho_{XZE}, \bar{\rho}_{XZE}) = P(\rho_{XE}, \bar{\rho}_{XE})$. By the property of the purified distance, such a state is guaranteed to exist. Then

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

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

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

Let $\bar{\rho}_{XE} \in \mathcal{B}^{\bar{\varepsilon}}(\rho_{XE})$ be the state which maximizes $H_{\min}(X|E)_{\bar{\rho}}$. Then

$$\delta\left(\bar{\rho}_{F(X,Y)YE}, \tau_U \otimes \tau_Y \otimes \bar{\rho}_E\right) \leq \varepsilon.$$

Furthermore,

$$\delta(\rho_{F(X,Y)YE}, \bar{\rho}_{F(X,Y)YE}) \leq \delta(\rho_{XE} \otimes \tau_Y, \bar{\rho}_{XE} \otimes \tau_Y) \leq P(\rho_{XE}, \bar{\rho}_{XE}),$$
$$\delta(\tau_U \otimes \tau_Y \otimes \rho_E, \tau_U \otimes \tau_Y \otimes \bar{\rho}_E) \leq P(\rho_{XE}, \bar{\rho}_{XE}).$$

The result follows from two uses of the triangle inequality.