COM-440, Introduction to Quantum Cryptography, Fall 2025

Partial Midterm Solutions

1. **Superdense Coding.**

   (a) Here one has to be careful about the task. Clearly you are being asked to evaluate a guessing probability. On what state? If we label Alice's two bits as $x, \theta \in \{0,1\}$ then we can write the qubit that encodes them as $|x\rangle_\theta$. The joint state of Alice's bits and the encoded qubit is a cq state $\rho_{X\Theta E} = \frac{1}{4}\sum_{x,\theta} |x\rangle\langle x| \otimes |\theta\rangle\langle\theta| \otimes |x\rangle\langle x|_\theta$. We know that $P_{guess}(X\Theta|E) = 2^{-H_{min}(X\Theta|E)}$. To evaluate this last term, we note that by the chain rule $H_{min}(X\Theta|E) \geq H_{min}(X\Theta) - \log|E|$. The first term is the min-entropy of two uniformly random bits, so it equals 2; and the second term is the size of E in qubits, which is 1. Therefore, we have established $P_{guess}(X\Theta|E) \leq \frac{1}{2}$. To show that there is equality we design a guessing strategy: Eve measures E in the standard basis, obtains an outcome $y \in \{0,1\}$ and returns $(y,0)$ as her two bits. This is correct with probability 1 in case the basis was indeed the standard basis, i.e. $\theta = 0$, and it is correct with probability 0 in case $\theta = 1$. Overall, the success probability is $\frac{1}{2}$.

   The other questions were solved well and we do not detail the solution.

2. **Secret sharing among three people.**

   (a) We directly calculate one matrix and use the symmetry among A, B, C to extrapolate the others.

   $$\begin{aligned}\rho_A &= \mathrm{Tr}_{BC}(|\Psi\rangle\langle\Psi|)\\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes \mathrm{tr}(|0\rangle\langle 0|_B) \otimes \mathrm{tr}(|0\rangle\langle 0|_C) + (-1)^{2b}|1\rangle\langle 1|_A \otimes \mathrm{tr}(|1\rangle\langle 1|_B) \otimes \mathrm{tr}(|1\rangle\langle 1|_C))\\ &= \frac{1}{2}(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A)\\ &= \frac{\mathbb{I}}{2}\end{aligned}$$

   We similarly have $\rho_B = \frac{1}{2}(|0\rangle\langle 0|_B + |1\rangle\langle 1|_B) = \frac{\mathbb{I}}{2}$ and $\rho_C = \frac{1}{2}(|0\rangle\langle 0|_C + |1\rangle\langle 1|_C) = \frac{\mathbb{I}}{2}$. This state is independent of b and so any measurement on a single system will lead to an outcome distribution that is independent of b: the secret cannot be retrieved by one party only.

(b) Again calculate one matrix and use the symmetry among A, B, C to extrapolate the others.

$$\begin{aligned}\rho_{AB} &= \mathrm{Tr}_C(|\Psi\rangle\langle\Psi|) \\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B \otimes \mathrm{tr}(|0\rangle\langle 0|_C) + (-1)^{2b}\,|1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \otimes \mathrm{tr}(|1\rangle\langle 1|_C)) \\ &= \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B) \\ &= \frac{1}{2}(|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB})\end{aligned}$$

and similarly $\rho_{BC} = \frac{1}{2}(|00\rangle\langle 00|_{BC} + |11\rangle\langle 11|_{BC})$ and $\rho_{AC} = \frac{1}{2}(|00\rangle\langle 00|_{AC} + |11\rangle\langle 11|_{AC})$. These densities are independent of b, so any measurement made by any pair will not give information about b.

(c) Have Alice, Bob, and Charlie apply the Hadamard operation on their qubit to get the new state

$$|\Psi_0\rangle = \frac{1}{4}((|0\rangle + |1\rangle)^3 + (|0\rangle - |1\rangle)^3) = \frac{1}{4}((|000\rangle + |011\rangle + |110\rangle + |101\rangle)$$

if $b = 0$ and the new state

$$|\Psi_1\rangle = \frac{1}{4}((|0\rangle + |1\rangle)^3 - (|0\rangle - |1\rangle)^3) = \frac{1}{4}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)$$

if $b = 1$. Next, we have Alice, Bob, and Charlie measure their qubits. Note by inspection, the tensor product of all three observations must either be in the set

$$S_0 = \{|0\rangle_A |0\rangle_B |0\rangle_C, |0\rangle_A |1\rangle_B |1\rangle_C, |1\rangle_A |1\rangle_B |0\rangle_C, |1\rangle_A |0\rangle_B |1\rangle_C\}$$

if $b = 0$, and must be in the set

$$S_1 = \{|0\rangle_A |0\rangle_B |1\rangle_C, |0\rangle_A |1\rangle_B |0\rangle_C, |1\rangle_A |0\rangle_B |0\rangle_C, |1\rangle_A |1\rangle_B |1\rangle_C\}$$

if $b = 1$.

Hence we can have Alice and Bob send their measurement to Charlie, and Charlie will see whether their collective measurements are in S_0 or S_1 to recover b.

3. **Quantum money security variant.** The scheme is *not* secure under the new security definition. Consider the following adversary, which runs in exponential time. The adversary ignores the quantum bill sent by the challenger. Instead, for every possible pair $x, \theta \in \{0,1\}^n$ the adversary does the following: prepare the n-qubit state $|x\rangle_\theta$ and send it for verification. If verification fails, proceed to the next pair x, θ. If it succeeds, then prepare two fresh copies of $|x\rangle_\theta$ (which is possible since x, θ are known) and submit them as response to the challenger. This adversary succeeds with probability 1, after at most $2^n \times 2^n$ attempts at verification.

4. **Inner product extractor.**

(a) The family is not 2-universal (in fact, it is not even 1-universal) because for the case where $x = 0^n$, $x' \neq x$, $z = 1$ and z' arbitrary we calculate $\mathbf{Pr}_y[f_y(x) = z \wedge f_y(x') = z'] = 0$ (because $f_y(0^n) = 0$ for all y), and not $\frac{1}{4}$ as would be required for a 2-universal family (note that here the parameter $m = 1$).

i. This question could be approached in different ways. One possibility is to use the characterization of the trace norm as $\|\sigma_{0,y} - \sigma_{1,y}\|_{tr} = \sup_{0 \leq M \leq \mathbb{I}} \mathrm{Tr}(M(\sigma_{0,y} - \sigma_{1,y}))$. Because $0 \leq M \leq \mathbb{I}$ the right-hand side is always at most 1. For there to be equality, for the optimal M we must have $\mathrm{Tr}(M\sigma_{0,y}) = 1$ and $\mathrm{Tr}(M\sigma_{0,y}) = 0$. Now we can see that if we replace M by the projection P on its support (i.e. round the singular values to 1, unless they are 0) the condition $\mathrm{Tr}(P\sigma_{0,y}) = 0$ still holds but $\mathrm{Tr}(P\sigma_{1,y}) \geq \mathrm{Tr}(M\sigma_{1,y}) = 1$. Since of course $\mathrm{Tr}(P\sigma_{1,y}) \leq \mathrm{Tr}(\sigma_{1,y}) = 1$, we are done.

ii. Let P_y be the projection obtained in the previous question. We verify that the map

$$U : |\psi\rangle_E |y\rangle_Y |0\rangle_A \mapsto P_y |\psi\rangle_E |y\rangle_Y |0\rangle_A + (\mathbb{I} - P_y) |\psi\rangle_E |y\rangle_Y |1\rangle_A \ ,$$

defined as such on every state $|\psi\rangle_E$ and $|y\rangle$, can be extended into a valid unitary. This is verified by checking that inner products are preserved, i.e. for any $|\psi\rangle_E$, $|\psi'\rangle_E$ and y, y',

$$\begin{aligned}\big(P_y |\psi\rangle_E |y\rangle_Y |0\rangle_A + (\mathbb{I} - P_y) |\psi\rangle_E |y\rangle_Y |1\rangle_A\big)^\dagger \cdot \big(P_{y'} |\psi'\rangle_E |y'\rangle_Y |0\rangle_A \\ + (\mathbb{I} - P_{y'}) |\psi'\rangle_E |y'\rangle_Y |1\rangle_A\big) \\ = \delta_{yy'} \langle\psi|_E P_y |\psi'\rangle_E + \langle\psi|_E (\mathbb{I} - P_y) |\psi'\rangle_E \\ = \delta_{yy'} \langle\psi|\psi'\rangle_E \ ,\end{aligned}$$

where for the last two lines we used that P_y is an orthogonal projection (and in particular $P_y(\mathbb{I} - P_y) = 0$).

iii. This is a direct calculation and we find

$$U' |\psi_x\rangle_E |y\rangle_Y |0\rangle_A |-\rangle_B = (-1)^{x \cdot y} |\psi_x\rangle_E |y\rangle_Y |0\rangle_A |-\rangle_B \ .$$

iv. Given $|\psi_x\rangle$, V first applies some Hadamards on the Y register to create $\frac{1}{\sqrt{2^n}} \sum_y |y\rangle$. It also applies an X followed by a Hadamard on B to create a $|-\rangle$. It then applies U' from the previous question, and undoes all the Hadamards and the X. This amounts to performing a QFT and the result is exactly the one desired.

v. We see that assumption (2) implies that it is possible to exactly recover X from E, and thus this is only possible in case $H_{min}(X|E) = 0$.