Homework 2

Due: November 21, 2025 at 11:59pm

CS 6832: Quantum Cryptography

Problems (2) and (3) are based on `https://ia.cr/2022/786` (though that result is more general). Problem (4) is based on `https://cims.nyu.edu/~regev/teaching/quantum_fall_2005/ln/qma.pdf`. We recommend trying to solve the problems without looking at these resources first, but you may refer to them if you get stuck. Solutions must always be presented in your own words.

(1) The Haar Measure and the Symmetric Subspace

Let S_t denote the set of permutations over t elements and let $P_d(\pi)$ be the implementation of a permutation $\pi \in S_t$ over nt-qubits — i.e., for a basis $|x_1, x_2, \ldots, x_t\rangle$ where $x_i \in \{0,1\}^n$,

$$P_d(\pi)\,|x_1, x_2, \ldots, x_t\rangle = \left|x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(t)}\right\rangle$$

Recall the symmetric subspace

$$\mathrm{Sym}_t(\mathbb{C}^d) = \{|\psi\rangle \in (\mathbb{C}^d)^{\otimes t} \mid P_d(\pi)\,|\psi\rangle = |\psi\rangle\,,\ \forall\, \pi \in S_t\}$$

Our goal is to show that $\Pi^{d,t}_{\mathrm{Sym}} = \frac{1}{t!}\sum_{\pi\in S_t} P_d(\pi)$ is the projector onto $\mathrm{Sym}_t(\mathbb{C}^d)$. To do so, it suffices to prove the following three facts.

(a) **(1 Points)** Prove that $\Pi^{d,t}_{\mathrm{Sym}}$ is indeed a projector — i.e., $(\Pi^{d,t}_{\mathrm{Sym}})^2 = \Pi^{d,t}_{\mathrm{Sym}}$.

(b) **(1 Points)** Prove that $\mathrm{Im}(\Pi^{d,t}_{\mathrm{Sym}}) \subseteq \mathrm{Sym}_t(\mathbb{C}^d)$ – i.e., that $\Pi^{d,t}_{\mathrm{Sym}}\,|\psi\rangle$ is invariant under permutation for all $|\psi\rangle$.

(c) **(1 Points)** Prove that $\mathrm{Im}(\Pi^{d,t}_{\mathrm{Sym}}) \supseteq \mathrm{Sym}_t(\mathbb{C}^d)$ – i.e., that $\Pi^{d,t}_{\mathrm{Sym}}\,|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathrm{Sym}_t(\mathbb{C}^d)$.

Definition 1 (Sum Binding)**.** Let $\mathcal{R}$ be the referee for the following game.

1. $\mathcal{R}$ sends $k \leftarrow \mathsf{Gen}(1^\lambda)$ and receives back $|c\rangle_{\mathsf{C}}$.
2. $\mathcal{R}$ sends $|m\rangle_{\mathsf{M}} \leftarrow \{0,1\}$ and receives back $|r\rangle_{\mathsf{R}}$.
3. Output 1 if $\mathsf{Com}(m;r) = c$ and 0 otherwise.

A commitment scheme $(\mathsf{Gen}, \mathsf{Com})$ is (post-quantum) *sum binding* if, for all QPT $\mathcal{A}$,

$$\Pr\Big[\langle \mathcal{R}(1^\lambda) \rightleftarrows \mathcal{A}(1^\lambda)\rangle = 1\Big] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

Definition 2 (Collapse Binding)**.** Let $\mathcal{R}$ be the referee for the following game.

1. $\mathcal{R}$ sends $k \leftarrow \mathsf{Gen}(1^\lambda)$ and receives back the registers $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{C}$.
2. $\mathcal{R}$ measures $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{C}$ with $\{V, I - V\}$ where[a]

$$V = \sum_{m \in \{0,1\}} \sum_{r \in \{0,1\}^\lambda} |m\rangle\langle m|_{\mathsf{M}} \otimes |r\rangle\langle r|_{\mathsf{R}} \otimes |\mathsf{Com}(m;r)\rangle\langle \mathsf{Com}(m;r)|_{\mathsf{C}}$$

   If the outcome is $I - V$, output 0.
3. $\mathcal{R}$ samples $b \leftarrow \{0,1\}$. If $b = 1$, it measures M in the computational basis.
4. $\mathcal{R}$ sends the registers $\mathsf{M} \otimes \mathsf{R}$ and receives back b'.
5. Output 1 if $b = b'$ and 0 otherwise.

A commitment scheme $(\mathsf{Gen}, \mathsf{Com})$ is *collapse binding* if, for all QPT $\mathcal{A}$,

$$\Pr\Big[\langle \mathcal{R}(1^\lambda) \rightleftarrows \mathcal{A}(1^\lambda)\rangle = 1\Big] \leq \frac{1}{2} + \mathsf{negl}(\lambda)$$

[a] This measurement ensures that the state on $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{C}$ is only supported on valid commitments.

(2) Collapse Binding Implies Sum Binding

Given a commitment scheme $(\mathsf{Gen}, \mathsf{Com})$, we have two different notions of a binding property described in Definition 1 and Definition 2. In the next two problems our goal is to prove these are equivalent. First, we show that Definition 2 implies Definition 1.

Let $\mathcal{A}$ be an adversary which achieves ε advantage in the sum binding game. Let ρ_1 be the state of the sum binding game after Step 1 (i.e., the state of the registers $\mathsf{C} \otimes \mathsf{R}$ and an internal workspace register E) and let U_0 (resp. U_1) be the unitary dilation of $\mathcal{A}$ in Step 2 (acting on $\mathsf{R} \otimes \mathsf{E}$) when given $m = 0$ (resp. $m = 1$). Finally, let $U = |0\rangle\langle 0|_{\mathsf{M}} \otimes U_0 + |1\rangle\langle 1|_{\mathsf{M}} \otimes U_1$.

Using $\mathcal{A}$, we construct $\mathcal{B}$ which breaks collapse binding as follows.

1. Receive k and run $\rho_1 \leftarrow \mathcal{A}(1^\lambda, k)$.
2. Prepare $\rho_2 = U(|+\rangle\langle+|_{\mathsf{M}} \otimes \rho_1)U^\dagger$ and perform the measurement $\{V, I - V\}$ from Step 2 of Definition 2. If the outcome is $I - V$, replace the state with $|\mathsf{Com}(0;0)\rangle_{\mathsf{C}} |0\rangle_{\mathsf{M}} |0\rangle_{\mathsf{R}}$.
3. Send $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{C}$.
4. Receive back $\mathsf{M} \otimes \mathsf{R}$ and apply $U^\dagger$ (to $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{E}$).
5. Measure M in the Hadamard basis. Output 0 if the outcome is $|+\rangle$ and 1 otherwise.

(a) **(3 Points)** Say that $\mathcal{R}$ does not measure M (i.e., $b = 0$). Then $\mathcal{B}$ will always succeed when the Hadamard basis measurement is $|+\rangle$ and the measurement outcmoe in Step 2 of the reduction is V[1]. Prove that this event happens with probability $\geq (\frac{1}{2} + \varepsilon)^2$.

Hint: If P and Q are projectors and ρ a density matrix, then $\mathrm{Tr}[QP\rho P] \geq \mathrm{Tr}[P\rho Q]^2$.

(b) **(1 Points)** Say that $\mathcal{R}$ does measure (i.e., $b = 1$) and the state on M collapses to $|m\rangle_{\mathsf{M}}$. Prove that $\mathcal{B}$ will output a uniformly random bit.

(c) **(2 Points)** Combining (a) and (b), show that $\mathcal{B}$ has $\geq \frac{\varepsilon}{2}$ distinguishing advantage.

[1]Note that the outcome in Step 2 of the reduction and Step 2 of the collapse binding game will always agree.

(3) Sum Binding Implies Collapse Binding

Given a commitment scheme $(\mathsf{Gen}, \mathsf{Com})$, we have two different notions of a binding property described in Definition 1 and Definition 2. Now we show that Definition 1 implies Definition 2.

Let $\mathcal{A}$ be an adversary which achieves ε advantage in the collapse binding game. Let σ_1 be the state of the collapse binding game after Step 1 (i.e., the state of the registers $\mathsf{C} \otimes \mathsf{M} \otimes \mathsf{R}$ and an internal workspace register E) and let $(D, I - D)$ be the distinguishing binary measurement made by $\mathcal{A}$ in Step 4. Finally, let $\Pi_0 = |0\rangle\langle 0|_{\mathsf{M}} \otimes I$ and $\Pi_1 = |1\rangle\langle 1|_{\mathsf{M}} \otimes I$.

Using $\mathcal{A}$, we construct $\mathcal{B}$ which breaks sum binding as follows.

1. Receive k, prepare $\sigma_1 \leftarrow \mathcal{A}(1^\lambda, k)$, and send C.
2. Receive m and measure M in the computational basis to get outcome b.
3. If $b \neq m$, measure $\mathsf{M} \otimes \mathsf{R} \otimes \mathsf{E}$ using $(D, I - D)$.
4. Measure $\mathsf{M} \otimes \mathsf{R}$ in the computational basis and output the outcomes $|m'\rangle_{\mathsf{M}}$ and $|r\rangle_{\mathsf{R}}$.

(a) **(2 Points)** Let $\mathcal{M}(\rho) = \Pi_0\rho\Pi_0 + \Pi_1\rho\Pi_1$ be the measurement channel used in the collapse binding game (when $b = 1$). Show that

$$\mathrm{Tr}[D(\rho - \mathcal{M}(\rho))] = \mathrm{Tr}[\Pi_1 D \Pi_0 \rho] + \mathrm{Tr}[\Pi_0 D \Pi_1 \rho]$$

(b) **(2 Points)** Show the following bound

$$\frac{1}{2}\,\mathrm{Tr}[D(\rho - \mathcal{M}(\rho))]^2 \leq \mathrm{Tr}[\Pi_1 D \Pi_0 \rho \Pi_0 D] + \mathrm{Tr}[\Pi_0 D \Pi_1 \rho \Pi_1 D]$$

Hint: Cauchy-Schwarz for Hilbert-Schmidt is $\left|\mathrm{Tr}\left[A^\dagger B\right]\right| \leq \sqrt{\mathrm{Tr}[A^\dagger A]}\sqrt{\mathrm{Tr}[B^\dagger B]}$ *and for non-negative real numbers is* $(\sqrt{a} + \sqrt{b})^2 \leq 2(a + b)$.

(c) **(2 Points)** Without loss of generality, we can assume that $\mathcal{A}$ never fails the $\{V, I - V\}$ measurement in Step 2 of Definition 2 — i.e., $V\rho = \rho$. Using the bound in (b), prove that $\mathcal{B}$ will succeed with probability $\geq \frac{1}{2} + \frac{1}{2}\varepsilon^2$.

(4) QMA Amplification

In this problem, we consider the task of amplifying the completeness and soundness of a QMA verifier without requiring multiple copies of the witness. Let $\{V_x\}$ be a family of unitaries and $\{\Delta, I - \Delta\}$ be a binary projective measurement[2] which satisfies completeness and soundness with respect to some language $\mathfrak{L} \subseteq \{0,1\}^n$ — i.e.,

Completeness. $\forall\, x \in \mathfrak{L}$, $\exists\ |\psi\rangle$ such that $\|\Delta V_x\, |\psi\rangle\, |0^m\rangle\, \|^2 \geq a$.

Soundness. $\forall\, x \notin \mathfrak{L}$, $\|\Delta V_x\, |\psi\rangle\, |0^m\rangle\, \|^2 \leq b$ for all $|\psi\rangle$.

Given $\{V_x\}$ and Δ, we construct an amplified verifier as follows. Repeat N times:

1. Apply V_x and measure $\{\Delta, I - \Delta\}$. Record 1 if the outcome is Δ and 0 otherwise.
2. Apply $V_x^\dagger$ and measure whether all ancilla qubits are 0. Record 1 if they are and 0 otherwise.

Let $a \in \{0,1\}^{2N}$ be the $2N$ outcomes recorded after N iterations and let ℓ be the number of i such that $a_i = a_{i+1}$. If $\ell \geq L$, then accept; otherwise reject.

Now we analyze the completeness and soundness of this amplified verifier. This heavily relies on the following lemma.

Lemma 1 (Jordan's Lemma)**.** *Let Π_1 and Π_2 be Hermitian projectors on a Hilbert space $\mathcal{H}$. Then there exists an orthogonal decomposition of $\mathcal{H} = \bigoplus_i \mathcal{S}_i$ into one-dimensional and two-dimensional subspaces $\{\mathcal{S}_i\}_i$ where*

- *$\forall\, i$, S_i is invariant under both Π_1 and Π_2 — i.e., $\Pi_b \mathcal{S}_i \subseteq \mathcal{S}_i$ for all b and i;*
- *if $\mathcal{S}_i$ is one-dimensional, Π_1 and Π_2 act as identity or zero on $\mathcal{S}_i$; and*
- *if $\mathcal{S}_i$ is two-dimensional, Π_1 and Π_2 are rank one projectors — i.e., there exists $|u\rangle\ |v\rangle$ such that Π_1 projects onto $|u\rangle$ and Π_2 projects onto $|v\rangle$ within $\mathcal{S}_i$.*

The subspaces $\{\mathcal{S}_i\}_i$ are called the Jordan subspaces *of Π_1 and Π_2.*

(a) **(1 Points)** Fix x and let $\Pi_0 = I \otimes |0^m\rangle\langle 0^m|$ and $\Pi_V = V_x^\dagger \Delta V_x$ correspond to the two measurements made in the amplified verifier. Show that the maximum acceptance probability of the original verifier is exactly the largest eigenvalue of $\Pi_0 \Pi_V \Pi_0$.

(b) **(1 Points)** Without loss of generality, we can assume that all Jordan subspaces of Π_0 and Π_V are two-dimensional. Let $|v_i\rangle$ and $|w_i\rangle$ be the vectors associated with Π_0 and Π_V, respectively, within two-dimensional Jordan subspace $\mathcal{S}_i$. Show that $\Pi_0 \Pi_V \Pi_0$ can be diagonalized as

$$\Pi_0 \Pi_V \Pi_0 = \sum_i p_i \cdot |v_i\rangle\langle v_i|$$

where $p_i = |\, \langle w_i | v_i \rangle\, |^2$.

[2] Δ can simply measure the first qubit the computational basis without loss of generality.

(c) **(2 Points)** Let $|v_i^\perp\rangle, |w_i^\perp\rangle \in \mathcal{S}_i$ such that $\langle v_i^\perp|v_i\rangle = \langle w_i^\perp|w_i\rangle = 0$.

If we perform Step 1 of our amplified verifier on input $|v_i\rangle$, what is the probability of recording each outcome? What is the post-measurement state after each outcome?

If we perform Step 2 of our amplified verifier on input $|w_i\rangle$, what is the probability of recording each outcome? What is the post-measurement state after each outcome?

(d) **(3 Points)** Let i^* be the index such that $p_{i^*} = \max_i p_i$. If $x \in \mathfrak{L}$, show that $|v_{i^*}\rangle$ will be accepted by the amplified verifier with probability $\geq 1 - 2^{-n}$ for some $N = \mathsf{poly}(n)$ and L.

Hint: This can be done using an entirely classical argument using the probabilities from (a) and (d).

(e) **(3 Points)** If $x \notin \mathfrak{L}$, show that, for all i, the amplified verifier will accept $|v_i\rangle$ with probability $\leq 2^{-n}$ for some $N = \mathsf{poly}(n)$ and L.

This suffices to prove soundness, as the general input case can be reduced to a mixture over $|v_i\rangle$ states.