Quantum Aspects of Cryptography

Endsem Exam

Tuesday, April 29, 2025

Important Instructions.

1. Ground rules.

   (a) *Permitted.* As announced, you are allowed to carry one A4 sheet with handwritten notes (you may write on both sides) but nothing beyond that, to explicitly help you with your exam.

   (b) *Forbidden.* In particular, devices such as a tablet, phone etc. must not be used and no interaction with your peers is allowed. Please call me instead, should there be any confusion.

   (c) *Penalty.* You will immediately lose 50% of your points should any violation of these ground rules be observed. The second violation will cause you to lose all points for this exam.

   (d) *Duration.* Please try to finish your exam within an hour and a half. I will do my best to offer as much extra time as logistically possible.

2. Grading/points.

   (a) 5 points for Assignment Exercises (these are taken verbatim from your assignments with additional explanations)

      i. 1 point for Haar

      ii. 1 point for PRS => Commitments

      iii. 1 point for QMA=BQP and yet PRUs exist

      iv. 1 point for QFHE

      v. 1 point for Self-Testing

   (b) 15 points for 'new' questions (these may overlap with your assignments, but won't be exactly the same).

      i. 3 points for Uncloneable Encryption (security in the ROM)

      ii. 3 points for Haar measure

      iii. 2 points for Pseudorandom States => Commitments

      iv. 3 points for QMA=BQP and yet PRUs exist

      v. 1 point for QFHE

      vi. 1 point for Self-Testing

      vii. 2 points for Verification

Unlike the mid-sem, there are no options this time. Please let me know if you spot a mistake or if something is unclear or feels suspicious. Good luck.

1 Review | Exercises from the Assignment

1.1 Haar Measure

Reminder:

- The moment operator is defined as $\mathcal{M}^{(k)}(\cdot) := \mathbb{E}_{U \leftarrow \mu_H}[U^{\otimes k}(\cdot)U^{\dagger \otimes k}]$ where μ_H is the Haar measure.

- The commutant
$$\mathrm{Comm}(\mathrm{U}(d), k) := \{A \in \mathcal{L}((\mathbb{C}^d)^{\otimes k}) : [A, U^{\otimes k}] = 0 \ \forall \ U \in \mathrm{U}(d)\}$$
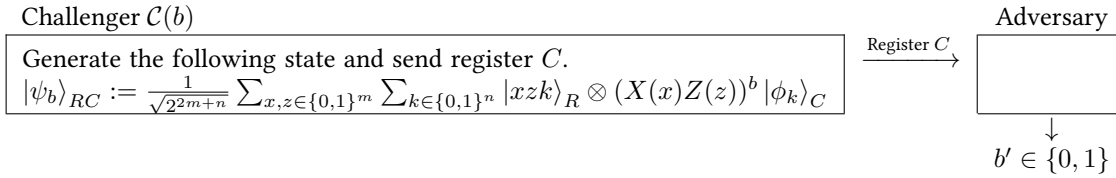is the set of linear operators A that commute with all $U^{\otimes k}$. Also, it holds that

Exercise 1 (1 points; Haar). Show that $\mathcal{M}^{(k)} \in \mathrm{Comm}(\mathrm{U}(d), k)$ and that if $A \in \mathrm{Comm}(\mathrm{U}(d), k)$, then $\mathcal{M}^{(k)}(A) = A$.
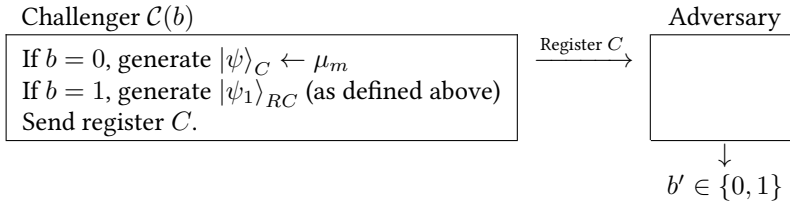
1.2 PRSG $\implies$ Commitments

Reminder: Recall that for proving computational hiding of their commitment scheme, [4] consider the following hybrids. Below, $|\phi_k\rangle$ is an m-qubit state produced by the state generator function of PRSG (with security parameter λ) and μ_m is the Haar measure over m-qubit states.

- $\mathrm{Hyb}_0(b)$

Challenger $\mathcal{C}(b)$		Adversary
Generate the following state and send register C. $\quad$ $\|\psi_b\rangle_{RC} := \frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z \in \{0,1\}^m} \sum_{k \in \{0,1\}^n} |xzk\rangle_R \otimes (X(x)Z(z))^b |\phi_k\rangle_C$	$\xrightarrow{\text{Register } C}$	

$$b' \in \{0,1\}$$

- $\mathrm{Hyb}_1(b)$

Challenger $\mathcal{C}(b)$		Adversary
If $b=0$, generate $\|\psi\rangle_C \leftarrow \mu_m$ If $b=1$, generate $\|\psi_1\rangle_{RC}$ (as defined above) Send register C.	$\xrightarrow{\text{Register } C}$	

$$b' \in \{0,1\}$$

Exercise 2 (1 point; PRSG $\implies$ Commitments). Show that $|\Pr[1 \leftarrow \mathrm{Hyb}_0(b)] - \Pr[1 \leftarrow \mathrm{Hyb}_1(b)]| \leq \mathrm{negl}$ for $b = 1$ (note, $b = 0$ is not asked, only $b = 1$).

1.3 BQP=QMA yet PRUs exist

Reminder:

- Semi-formally, a pseduorandom unitary is a keyed family of unitaries $\{U_k\}_{k \in \{0,1\}^\kappa}$ acting on $n(\kappa)$-qubits, where κ is a security parameter with the following two properties:

  - It can be applied efficiently (i.e. given k and a quantum state $|\psi\rangle$, one can efficiently compute $U_k |\psi\rangle$) and
  - No efficient quantum algorithm $\mathcal{A}$ can distinguish whether it is given oracle access to a Haar random unitary, i.e. $U \leftarrow \mu_{2^n}$, or a pseudorandom unitary, i.e. U_k where $k \leftarrow \{0,1\}^\kappa$.

- Kretschmer [3] uses $\mathcal{U}$ (quantum oracle) and $\mathcal{C}$ (a classical oracle) which is independent of $\mathcal{U}$. The quantum oracle $\mathcal{U}$ is defined as the set $\{\mathcal{U}_n\}_{n \in \mathbb{N}}$ where for each n, $\mathcal{U}_n$ denotes a direct sum 2^n independent Haar random unitaries, acting on n qubits, i.e. $\mathcal{U}_n \leftarrow \mu_{2^n}^{2^n}$.

Exercise 3 (1 point; BQP=QMA yet PRUs exist). State the construction for the PRU ensemble used by Kretschmer.

1.4 QFHE

Reminder:

- Recall that Mahadev's QFHE scheme encrypts a quantum state $|\psi\rangle$ as $(X^x Z^z |\psi\rangle, (\hat{x}, \hat{z}))$ where x, z are sampled uniformly and $\hat{x}$ and $\hat{z}$ denote classical FHE encryptions of x and z respectively.

Exercise 4 (1 point; QFHE). Explain how the Eval function is implemented for Clifford gates, in Mahadev's construction.
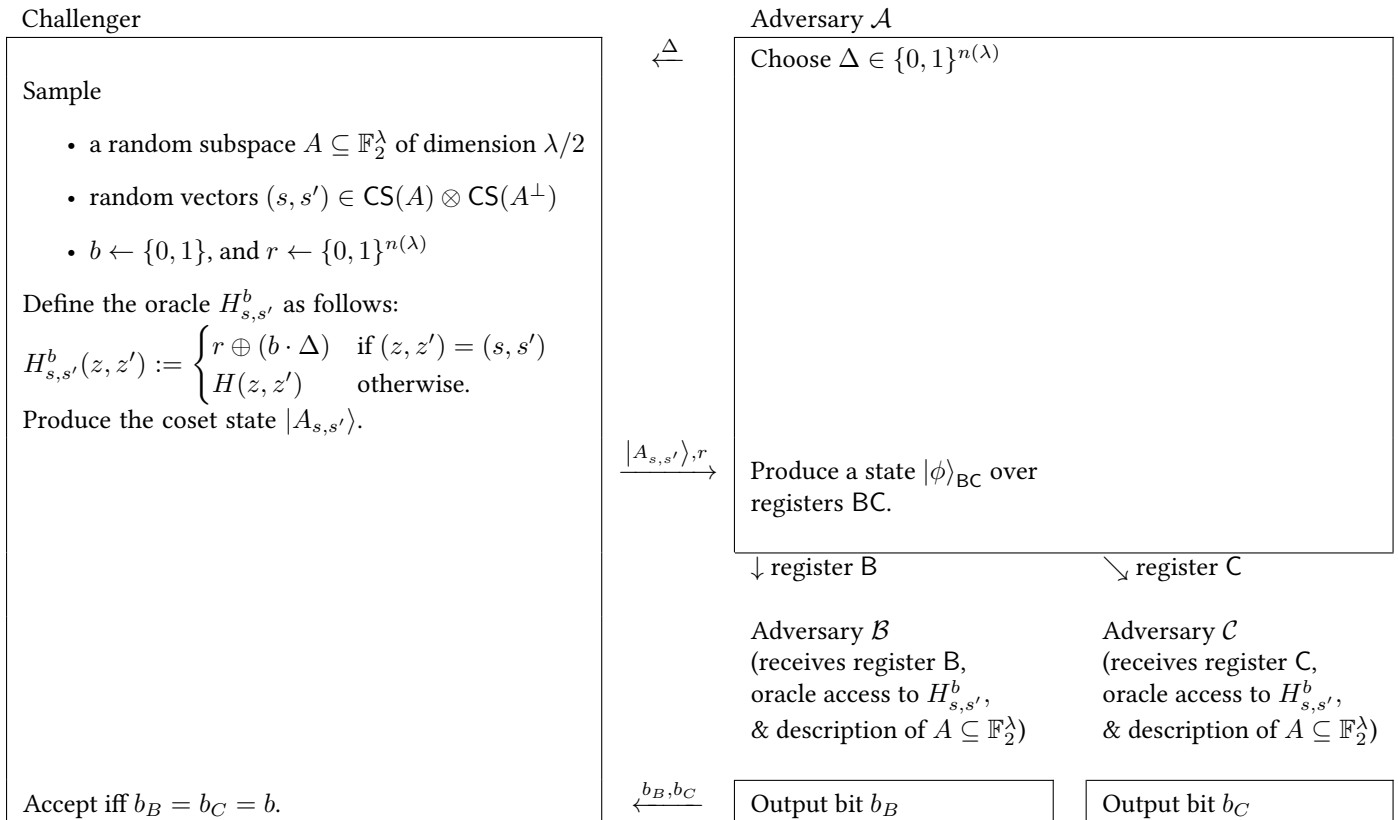
1.5 Self-testing

Reminder: In class, we only considered self-testing of the two-qubit maximally entangled state $|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We considered the CHSH game where Alice and Bob are asked questions $x, y \in \{0, 1\}$ and respond with answers $a, b \in \{\pm 1\}$ respectively. To describe the most general quantum strategy, denote the quantum state shared by Alice and Bob by $|\psi\rangle_{AB}$ where Alice holds register A and Bob register B. Denote the observable used by Alice (resp. Bob) to answer question x, by A_x (resp. B_y). We observed that A_x and B_y are Hermitian and unitary.

Exercise 5 (1 point; Self-testing). Suppose $\frac{A_0 \pm A_1}{\sqrt{2}} |\psi\rangle = B_{0/1} |\psi\rangle$ where $\{A_x\}_{x \in \{0,1\}}$ and $\{B_y\}_{y \in \{0,1\}}$ denote Alice's and Bob's operators in a general strategy they follow to play the CHSH game. Prove that B_0 and B_1 anti-commute on $|\psi\rangle$, i.e. $\{B_0, B_1\} |\psi\rangle = 0$.

2 Uncloneable Encryption

A word of advice: Do this one after you've attempted all other questions. It ended up being quite long for a 3 point question. Reminder: Let us recall Hybrid 2 in the security proof of the uncloneable encryption scheme introduced by [1].

Challenger		Adversary $\mathcal{A}$
	$\xleftarrow{\Delta}$	Choose $\Delta \in \{0,1\}^{n(\lambda)}$
Sample • a random subspace $A \subseteq \mathbb{F}_2^\lambda$ of dimension $\lambda/2$ • random vectors $(s, s') \in \mathsf{CS}(A) \otimes \mathsf{CS}(A^\perp)$ • $b \leftarrow \{0, 1\}$, and $r \leftarrow \{0, 1\}^{n(\lambda)}$ Define the oracle $H^b_{s,s'}$ as follows: $H^b_{s,s'}(z, z') := \begin{cases} r \oplus (b \cdot \Delta) & \text{if } (z, z') = (s, s') \\ H(z, z') & \text{otherwise.} \end{cases}$ Produce the coset state $|A_{s,s'}\rangle$.		
	$\xrightarrow{|A_{s,s'}\rangle, r}$	Produce a state $|\phi\rangle_{\mathsf{BC}}$ over registers BC.

	↓ register B	↘ register C
	Adversary $\mathcal{B}$ (receives register B, oracle access to $H^b_{s,s'}$, & description of $A \subseteq \mathbb{F}_2^\lambda$)	Adversary $\mathcal{C}$ (receives register C, oracle access to $H^b_{s,s'}$, & description of $A \subseteq \mathbb{F}_2^\lambda$)

| Accept iff $b_B = b_C = b$. | $\xleftarrow{b_B, b_C}$ | Output bit b_B | Output bit b_C |

where

- H is a random oracle $H : \mathbb{F}_2^\lambda \times \mathbb{F}_2^\lambda \to \{0, 1\}^{n(\lambda)}$,

- $\mathcal{A}, \mathcal{B}, \mathcal{C}$ all get access to P_{A+s} and $P_{A^\perp + s'}$ after the first message is sent by the challenger, and

- $\mathsf{CS}(A)$ is the set of canonical representatives for A, i.e. $\mathsf{CS}(A) = \{\mathsf{Can}_A(s) : s \in \mathbb{F}_2^n\}$.
    - $\mathsf{Can}_A(s)$ is the (lexicographically) smallest vector in $A + s := \{a + s : a \in A\}$.
- $|A_{s,s'}\rangle := \frac{1}{\sqrt{|A|}} \sum_{a \in A} (-1)^{s' \cdot a} |a + s\rangle$

For the proof, we will need to define projectors Π_0^B, Π_1^B and Π_0^C, Π_1^C. For a fixed A, r, Δ, s, s' they are defined as follows:

- Π_0^B: runs $\mathcal{B}$ with oracle access to $H_{s,s'}^0$ (B and A are the same), projects on outcome 0, and undoes the computation.

- Π_1^B : runs $\mathcal{B}$ with oracle access to $H_{s,s'}^1$ (B and A are the same), projects on outcome 1, and undoes the computation.

- Π_0^C and Π_1^C are defined similarly, with $\mathcal{B}$, B replaced with $\mathcal{C}$, C.

We will need some more notation.

- Denote by $\{(|\phi_i\rangle, \lambda_i)\}_i$ the (eigenvectors, eigenvalues) of $(\Pi_0^B + \Pi_1^B)/2$. Similarly, let $\{(|\psi_j\rangle, \mu_j)\}_j$ denote the corresponding quantities for $(\Pi_0^C + \Pi_1^C)/2$.

- NB: $|\phi\rangle_{BC} = \sum_{ij} \alpha_{ij} |\phi_i\rangle_B \otimes |\psi_j\rangle_C$ without loss of generality.

Finally, we will assume the following holds about the state $|\phi\rangle_{BC}$ produced by $\mathcal{A}$: for every polynomial p, we have

$$\sum_{\substack{i:|\lambda_i - 1/2| > 1/p \\ j:|\mu_j - 1/2| > 1/p}} |\alpha_{ij}|^2 \leq \operatorname{negl}(n).$$

Question 1 (3 points). *Denote by p_2 the probability that Hybrid 2 above outputs accept. We will show some of the main steps in establishing that $p_2 \leq \frac{1}{2} + \operatorname{negl}(\lambda)$.*

1. *Show that the state $|\phi\rangle_{BC}$ is negligibly close to*

$$|\phi'\rangle_{BC} := \sum_{i:|\lambda_i - 1/2| \leq 1/p} \alpha_{ij} |\phi_i\rangle_B \otimes |\psi_j\rangle_C + \sum_{\substack{i:|\lambda_i - 1/2| > 1/p \\ j:|\mu_j - 1/2| \leq 1/p}} \alpha_{ij} |\phi_i\rangle_B \otimes |\psi_j\rangle_C.$$

2. *Show that*

$$\frac{\left(\left|(\Pi_0^B \otimes \Pi_0^C) |\phi'\rangle_{BC}\right|^2 + \left|(\Pi_1^B \otimes \Pi_1^C) |\phi'\rangle_{BC}\right|^2\right)}{2} \tag{1}$$

   is negligibly close to the probability that $(\mathcal{A}, \mathcal{B}, \mathcal{C})$ is accepted by the Challenger.

3. *Show that the expression above (Eq 1) can be upper bounded by*

$$\frac{1}{2} \cdot \left(\underbrace{\langle\phi'_B| (\Pi_0^B \otimes I) |\phi'_B\rangle + \langle\phi'_B| (\Pi_1^B \otimes I) |\phi'_B\rangle}_{\text{I}} + \underbrace{\langle\phi'_C| (I \otimes \Pi_0^C) |\phi'_C\rangle + \langle\phi'_C| (I \otimes \Pi_1^C) |\phi'_C\rangle}_{\text{II}} \right)$$

$$+ \Re\left(\underbrace{\langle\phi'_C| (\Pi_0^B \otimes \Pi_0^C) |\phi'_C\rangle}_{\text{III}} + \underbrace{\langle\phi'_B| (\Pi_1^B \otimes \Pi_1^C) |\phi'_C\rangle}_{\text{IV}} \right).$$

4. *Establish that* I *(resp.* II*) is at most $\left(\frac{1}{2} + \frac{1}{p}\right) ||\phi'_B\rangle|^2$ (resp. $\left(\frac{1}{2} + \frac{1}{p}\right) ||\phi'_C\rangle|^2$).*

5. *Suppose it holds that for indices i, i' satisfying $\lambda_i + \lambda_{i'} \neq 1$, we have $\langle\phi_i| \Pi_0^B |\phi_{i'}\rangle = 0$ (we proved this in class). Using this, show that both* III *and* IV *are zero.*

6. *Quick conceptual questions:*

    (a) *In your answers above, where did you (most directly) use properties of the coset state $|A_{s,s'}\rangle$?*
    (b) *Assertion: $\Pi_0^B + \Pi_1^B = \mathbb{I}$. Either prove the assertion or justify why you don't expect the projectors to sum to identity.*

(NB. Combining these, you should be able to deduce that $p_2 \leq \left(\frac{1}{2} + \frac{1}{p}\right) \left(||\phi'_B\rangle|^2 + ||\phi'_C\rangle|^2\right) + \operatorname{negl} \leq \frac{1}{2} + \frac{1}{p} + \operatorname{negl}$ and since this is true for all polynomials p, we have proved $p_2 \leq \frac{1}{2} + \operatorname{negl}$.)

3 Haar Measure

Reminder:

- $P_{\text{sym}} := \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi)$ where S_k is the symmetric group (group of permutations over k indices), and $V_d(\pi) = \sum_{i_1, \ldots i_k \in [d]} |i_{\pi^{-1}(1)} \ldots i_{\pi^{-1}(k)}\rangle \langle i_1 \ldots i_k|$ affects this permutation on k many d-dimensional quantum systems.

- Schur-Weyl duality says that $\mathcal{M}^k(O) = \mathbb{E}_{U \leftarrow \mu_H}[U^{\otimes k} O U^{\otimes k}]$ can be expressed as a linear combination of $V_d(\pi)$, where O is a linear operator on $(\mathbb{C}^d)^{\otimes k}$.

Question 2 (3 points). *Prove that*

$$\mathcal{M}^k(|\phi\rangle \langle\phi|^{\otimes k}) = \mathbb{E}_{U \leftarrow \mu_H}[U^{\otimes k} |\phi\rangle \langle\phi|^{\otimes k} U^{\dagger \otimes k}] = \frac{P_{\text{sym}}}{\text{tr}(P_{\text{sym}})}$$
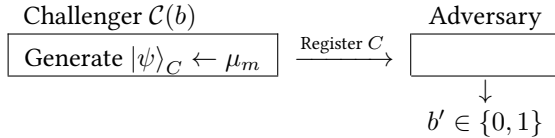
where $|\phi\rangle \in \mathbb{C}^d$. You could either do this directly yourself, or do it by establishing the following sub-steps.

1. *Show that $V_d(\sigma^{-1})\mathcal{M}(\phi) = \mathcal{M}(\phi)$ where we use $\mathcal{M}$ to denote $\mathcal{M}^k$ and ϕ to denote $|\phi\rangle \langle\phi|$.*

2. *Show that $\sum_{\pi \in S_k} c_\pi V_d(\sigma^{-1}) V_d(\pi) = \sum_{\pi \in S_k} c_{\sigma\pi} V_d(\pi)$.*

3. *Can you use these two observations to conclude that $\mathcal{M}(\phi) = \sum_{k \in S_k} c_{\sigma\pi} V_d(\pi)$.*

4. *Using your result above, reason that $c_\sigma = c_I$ for all $\sigma \in \pi$ (here I is the identity permutation)?*

5. *Now, show that $\mathcal{M}^k(\phi) \propto P_{\text{sym}}$*

6. *Finally, establish the normalisation to complete the proof.*

4 PRS $\implies$ Commitments

Reminder (PRSG $\implies$ Commitments). In addition to $\text{Hyb}_0, \text{Hyb}_1$ as defined above 2, [4] also define Hyb_2 as follows.

- $\text{Hyb}_2(b)$

Challenger $\mathcal{C}(b)$		Adversary
Generate $|\psi\rangle_C \leftarrow \mu_m$	$\xrightarrow{\text{Register } C}$	

$$b' \in \{0, 1\}$$

Question 3 (2 points). *We want to establish computational hiding of [4]'s commitment scheme by showing*

$$|\Pr[1 \leftarrow \text{Hyb}_0(0)] - \Pr[1 \leftarrow \text{Hyb}_0(1)]| \leq \text{negl}(\lambda). \tag{2}$$

To this end, prove the following sub-claims (where we use $a \approx b$ to denote $|a - b| \leq \text{negl}$).

1. $\Pr[1 \leftarrow \text{Hyb}_0(b)] \approx \Pr[1 \leftarrow \text{Hyb}_1(b)]$ *for $b = 0$ as well. Show that if this were not the case, then one can construct an adversary $\mathcal{A}'$ that breaks the security of the underlying PRSG (pseudorandom state generator) by distinguishing a pseudorandom state from a Haar random state.*

2. $\Pr[1 \leftarrow \text{Hyb}_1(b)] \approx \Pr[1 \leftarrow \text{Hyb}_2(b)]$ *for $b = 0$ should be immediate (write one line justifying it). How will you modify $\mathcal{A}'$ above to establish the $b = 1$ case? Using these observations, establish (2).*

5 QMA=BQP and yet PRUs exist

Question 4 (3 points). *The answers to the following, should be enough for you to prove that the relative to $\mathcal{U}$ (as defined above Exercise 3), PRUs exist.*
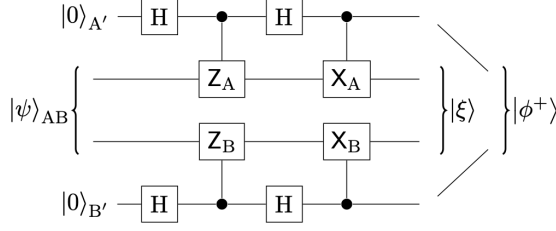
Figure 1: Local Isometry Φ taken form [5].

1. *Fix the system size (on which the unitaries act) to be n qubits. Denote the PRU ensemble you defined in Exercise 3 as $\tilde{U} := \{\tilde{U}_k\}_{k \in \{0,1\}^n}$. To establish that $\tilde{U}$ is a PRU, does it suffice to show that for all efficient quantum oracle-algorithms $\mathcal{A}$,*

$$\mathsf{adv}(\mathcal{A}) := \Pr_{k \leftarrow \{0,1\}^n}[1 \leftarrow \mathcal{A}^{\tilde{U}_k}] - \Pr_{U \leftarrow \mu_{2^n}}[1 \leftarrow \mathcal{A}^U] \leq \mathsf{negl}(n)?$$

   If so, justify your answer (Hint: Do you need an $\mathcal{U}$ to efficiently generate $\tilde{U}$? If so, should that appear somewhere in your definition of a secure PRU, relative to $\mathcal{U}$).
   If not, how will you modify adv? (Hint: Note that $\mathcal{C}$ is uncorrelated to $\mathcal{U}$)
   (NB. You can neglect non-uniformity considerations i.e. it suffices, in the definition of PRUs to be secure against uniform adversaries—no need to consider advice, for the purposes of this exam).

2. *Suppose $\mathcal{A}^{O,U}$ is an oracle algorithm that makes queries to $U = (U_1, \ldots U_N) \in \mathbb{U}(D)^N$. Prove that*

$$\mathbb{E}_{U \leftarrow \mu_D^N}\left[\Pr_{k \leftarrow [N]}[1 \leftarrow \mathcal{A}^{U_k, U}]\right] = \Pr_{k \leftarrow [N]}[1 \leftarrow \mathcal{B}^{e_k}] \tag{3}$$

   where $[N] = \{1, \ldots, N\}$, $e_k = (0, 0 \ldots, 0, 1, 0, \ldots 0)$ with 1 at the kth position, and $\mathcal{B}$ is defined as follows:

   - *$\mathcal{B}$ samples $(V_0, V_1 \ldots V_N) \leftarrow \mu_D^{N+1}$ (which are unitaries in $\mathbb{U}(D)^{N+1}$).*
   - *$\mathcal{B}$ runs $\mathcal{A}$, replacing queries to O by queries to V_0 and queries to $U_k \in U$ by V_0 if $x_k = 1$, and by V_k if $x_k = 0$.*

   Prove also that

$$\mathbb{E}_{U \leftarrow \mu_D^N}\left[\Pr_{O \leftarrow \mu_D}[1 \leftarrow \mathcal{A}^{O,U}]\right] = \Pr[1 \leftarrow \mathcal{B}^{0^N}]. \tag{4}$$

   (NB. Using a bound on unstructured search, one can now argue that the difference between Eq. (3) and (4) must be at most cT^2/N, where T is the number of queries made by $\mathcal{A}$ and c is a universal constant.).

5.1 Self-testing

Reminder: Continuing with the discussion preceding Exercise 5, recall that we explicitly defined the local isometry Φ as shown in Figure 1. For $Z_A = \frac{1}{\sqrt{2}}(A_0 + A_1), Z_B = B_0, X_A = \frac{1}{\sqrt{2}}(A_0 - A_1), X_B = B_1$, we proved in class that

$$\Phi[|\psi\rangle] = \sum_{i,j \in \{0,1\}} |ij\rangle_{A'B'} \otimes \underbrace{\left(\frac{1}{4}X_A^i(\mathbb{I} + (-1)^i Z_A)X_B^j(\mathbb{I} - (-1)^j Z_B)\right)}_{=:\hat{f}_{ij}} |\psi\rangle_{AB}.$$

It may help to also recall that we proved the following:

- $\{Z_A, X_A\} = 0, \{Z_B, X_B\}|\psi\rangle = 0$

- $Z_A |\psi\rangle = Z_B |\psi\rangle$ and $X_A |\psi\rangle = X_B |\psi\rangle$

Question 5 (1 point; self-testing). *Using the aforementioned, show that that $\hat{f}_{01} |\psi\rangle = \hat{f}_{10} |\psi\rangle = 0$ and $\hat{f}_{11} |\psi\rangle = \hat{f}_{00} |\psi\rangle$.*

5.2 QFHE

Reminder: We look at some of the steps that go into applying the encrypted CNOT operation in Mahadev's QFHE scheme. The question will ask you to fill in a detail or two. Let $|\psi\rangle = \sum_{a,b\in\{0,1\}} \alpha_{ab}|ab\rangle$ be an arbitrary pure two qubit state. The goal is to apply CNOT^s where $\hat{s}$ is given (recall $\hat{s}$ is a classical FHE encryption of s).

[BEGIN SNIPPET]

1. Clasically, compute a description of the claw-free pair (f_0, f_1) corresponding to $\hat{s}$ (a reminder about the claw-free pair is appended, just in case).

2. Prepare the state

$$|\psi_1\rangle = \sum_{\substack{a,b,\mu\in\{0,1\}\\ r\in\mathcal{R}}} \alpha_{ab}|ab\rangle|\mu r\rangle|f_a(\mu, r)\rangle$$

   and measure the last register to obtain a y. Denote by $|\psi_{1'}\rangle$ the resulting state.

3. XOR μ_a into the second register. This should result in

$$|\psi_3\rangle := \sum_{ab\in\{0,1\}} \alpha_{ab}(\mathbb{I}\otimes X^{\mu_0})\mathsf{CNOT}^s_{12}|a,b\rangle|\mu_a r_a\rangle$$

   where $f_0(\mu_0, r_0) = f_1(\mu_1, r_1) = y$.

4. The last register is measured in Hadamard basis...

[END SNIPPET]

Question 6 (1 point; QFHE). *Write down $|\psi_{1'}\rangle$ and prove that following step 3, one indeed gets the state $|\psi_3\rangle$ (up to a change in variable names, depending on the choice you make in specifying $|\psi_{1'}\rangle$).*
(Hint: it may help to observe that $|b\oplus\mu_a\rangle = X^{\mu_0}|b + a\cdot s\rangle$; if you use this, prove that it is true first)

Reminder: Additional properties we need from (N)TCFs (Noisy Trapdoor Claw-free Functions), given encryption $\hat{s}$ of a bit s.

1. One can efficiently compute trapdoor claw-free functions $f_0, f_1 : \{0,1\}\times\mathcal{R} \to \mathcal{Y}$ s.t. $\forall (\mu_0, r_0), (\mu_1, r_1) \in \{0,1\}\times\mathcal{R}$ which is a claw (i.e. $f_0(\mu_0, r_0) = f_1(\mu_1, r_1)$), it holds that $\mu_0 \oplus \mu_1 = s$.

2. One can also compute a classical FHE encryption of the trapdoor (which allows one to invert the function) corresponding to the pair (f_0, f_1).

5.3 Verification

Reminder:

- An XZ Local Hamiltonian acting on n qubits is of the form $H = \sum_{\ell\in[m]} \gamma_\ell H_\ell$ where H_ℓ consists of tensor products of σ_x and σ_z (and $\mathbb{I}$) matrices, acting non-trivially (i.e. non $\mathbb{I}$) on at most k qubits, i.e. for each ℓ, $H_\ell = \otimes_{j\in n}\sigma_{W_{j,\ell}} \in \{\sigma_x, \sigma_z, \sigma_I\}^{\otimes n}$ with $\left|\{j|j\in[n]\wedge\sigma_{W_{j,\ell}}\neq\sigma_I\}\right| \leq k$.

- The Hamiltonian Test $G(H)$ for such Hamiltonians, as constructed by [2], is as shown in Figure 2 (t below is taken to be something like $n\log n$).

- In class, we proved the following (as Lemma 7). Let $\omega_h(H) := 1 - p\left(\frac{1}{2m}\sum_{\ell\in[m]}|\gamma_\ell| - \frac{1}{2}\lambda_0(H)\right)$ where $\lambda_0(H)$ denotes the smallest eigenvalue of H. If the provers use the honest strategy in the Pauli-Braiding test, then the maximum acceptance probability in $G(H)$ is $\omega_h(H)$. We now write down some of the main steps that go into this proof and you will be asked to fill in some of the gaps in the argument.

Question 7 (2 points, Verification). *Prove the following assertions.*

1. *Assertion: The acceptance probability in $G(H)$ depends uniquely on the strategy of the first prover in the energy test (in particular, it does not depend on the strategy of the second prover in the energy test).*

2. *Assertion: For a fixed H_ℓ, the verifier rejects with probability*

$$\frac{|\gamma_\ell| + \gamma_\ell \mathbb{E}[\Pi_{i\in[n]} d_i]}{2}. \tag{5}$$

Denote by τ the reduced state held by the second prover on qubits $\mathcal{T} := (\mathcal{T}_1, \ldots \mathcal{T}_n)$ of his EPR halves (after 'teleportation').

3. *Assertion: Given the answers (a, b) of the first prover, the following behaviours of the second prover are equivalent:*

   (a) *Measure τ using H_ℓ and obtain outcome $\Pi_{i\in\mathcal{T}} c_i$.*

   (b) *Measure $\rho = Z^b X^a \tau X^a Z^b$ using H_ℓ and obtain outcome $\Pi_{i\in\mathcal{T}} d_i$.*

   Hint: Measuring a qubit $|\phi\rangle$ in the Z-basis w/ outcome $f \in \{\pm 1\}$ is equivalent to getting outcome $(-1)^g f$ when measuring $Z^h X^g |\phi\rangle$ in the Z-basis. Similarly, measuring $|\phi\rangle$ in the X-basis w/ outcome $f \in \{\pm 1\}$ is equivalent to getting outcome $(-1)^h f$ when measuring $Z^h X^g |\phi\rangle$ in the X-basis. (Equivalence as in the output distribution is identical).

4. *Assertion: The rejection probability in Eq (5), averaged over ℓ, is*

$$\frac{1}{2m} \sum_{\ell\in[m]} |\gamma_\ell| + \frac{1}{2}\mathsf{tr}(\rho H).$$

   The acceptance *probability in $G(H)$ is at most*

$$1 - p\left(\frac{1}{2m} \sum_{\ell\in[m]} |\gamma_\ell| - \frac{1}{2}\lambda_0(H)\right) = w_h(H).$$

References

[1] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the feasibility of unclonable encryption, and more. Cryptology ePrint Archive, Paper 2022/884, 2022.

[2] Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round, 2020.

[3] William Kretschmer. Quantum pseudorandomness and classical complexity. 2021.

[4] Tomoyuki Morimae and Takashi Yamakawa. *Quantum Commitments and Signatures Without One-Way Functions*, page 269–295. Springer Nature Switzerland, 2022.

[5] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020.

(a) Pauli-Braiding Test: (We don't need the details here, except that the view of Prover 2 is exactly the same as that in the Energy Test).
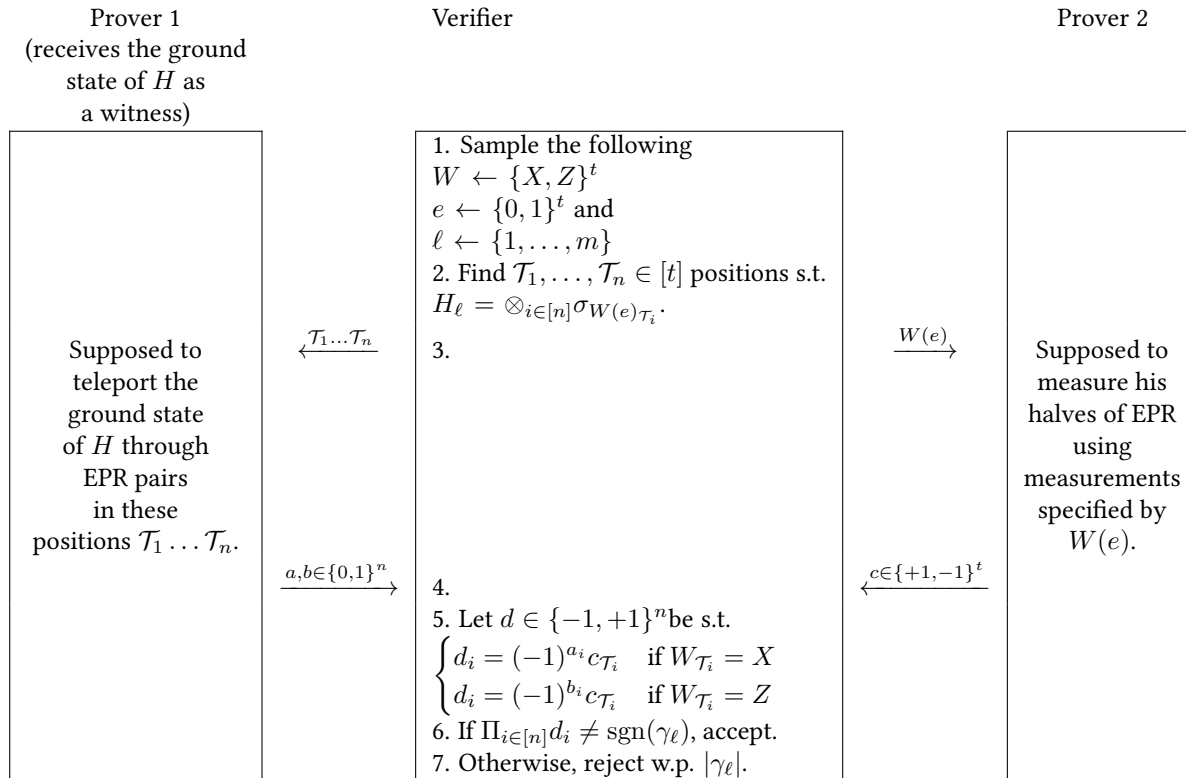
(b) Energy Test

Prover 1 (receives the ground state of H as a witness)		Verifier		Prover 2

Figure 2: The verifier performs the Pauli-Braiding Test with probability $1 - p$ and the Energy Test with probability p. The provers are assumed to share t EPR pairs.