COL872: Quantum and Post-Quantum Cryptography

Problem Set 4

Due date: April 12th, 2023

Instructions

1. Assignments must be done in groups of size at most three. Each group must upload one submission, and mention the names of all group members.
2. You are welcome to discuss with other classmates and instructor, as well as refer to resources online. But if you do, please mention who all you collaborated with, or the online resources used.

This is version 1 of the assignment, uploaded on 02/04/23.

Questions

Question 1. ***Simultaneous Projective Measurements*** *(5 marks)*

In general, quantum measurements are non-commutative. That is, if $\mathcal{P} = \{\mathbf{P}_a\}_{a\in[s]}$ and $\mathcal{Q} = \{\mathbf{Q}_b\}_{b\in[t]}$ are two projective measurements, then applying $\mathcal{P}$ first, followed by $\mathcal{Q}$, need not produce the same distribution (over $[s] \times [t]$) as applying $\mathcal{Q}$ first, followed by $\mathcal{P}$.

1. *Give an example of two projective measurements $\mathcal{P}, \mathcal{Q}$ that are non-commutative.*

However, in certain special cases, the projective measurements are commutative. Let $\{|\mathbf{v}_i\rangle\}_i$ be an orthonormal basis for $\mathbb{C}^N$. Let $S = (S_1, \ldots, S_s)$ and $T = (T_1, \ldots, T_t)$ be two partitions of $[N]$. Let $\mathbf{P}_i = \sum_{j\in S_i} |v_j\rangle\langle v_j|$ for each $i \in [s]$, and $\mathbf{Q}_i = \sum_{j\in T_i} |v_j\rangle\langle v_j|$ for each $i \in [t]$.

2. *Show that the projective measurements $\mathcal{P} = \{\mathbf{P}_i\}_{i\in[s]}$ and $\mathcal{Q} = \{\mathbf{Q}_i\}_{i\in[t]}$ are commutative.*
3. *Is this the only case in which projective measurements are commutative? Prove or disprove.*

Question 2. ***Collapsing hash from claw-free functions*** *(10 marks)*

A claw-free function family $\mathcal{F} = \{f_k : \{0,1\}^{n+1} \to \{0,1\}^n\}_{k\in\mathcal{K}}$ *with the following properties:*

We will use claw-free functions later in the course, for building quantum supremacy protocols.

- *For every* $k \in \mathcal{K}$, $x_0 \in \{0,1\}^n$, *there exists a unique* x_1 *such that* $f_k(0,x_0) = f_k(1,x_1)$. *Moreover, for all* $x \neq y \in \{0,1\}^n$, *all* $k \in \mathcal{K}$ *and* $b \in \{0,1\}$, $f_k(b,x) \neq f_k(b,y)$ *(that is, the functions* $f_k(b,\cdot)$ *are injective for all* $k \in \mathcal{K}, b \in \{0,1\}$*).*
- *Security: given a uniformly random key* $k \leftarrow \mathcal{K}$, *no q.p.t. algorithm can find* x_0, x_1 *such that* $f_k(0,x_0) = f_k(1,x_1)$.

1. *Show that* $\{H_k \equiv f_k\}_{k\in\mathcal{K}}$ *is a collapsing hash function.*

   Hint: see Lemma 1 of this paper.

2. *Construct a hash function family* $\mathcal{H}' = \{H'_k : \{0,1\}^{n+2} \to \{0,1\}^n\}$ *using* $\mathcal{F}$, *and prove that* $\mathcal{H}'$ *is collapsing, assuming* $\mathcal{F}$ *is a claw-free function family.*

Question 3. ***Quantum Proof of Knowledge for Blum's protocol*** *(10 marks)*

In Lectures 21,22, we discussed a quantum extractor that can extract a witness, given access to the prover's unitaries $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_0^\dagger, \mathbf{U}_1^\dagger$. *In this exercise, we will fill in some of the proof details.*

Recall, the extractor was defined as follows:

1. *First, the extractor runs the prover, and receives first message* msg_1. *The prover maintains a state* $|\psi_{\mathsf{msg}_1}\rangle_{\mathsf{A,O,Z}}$. *The registers* A *and* O *consist of* t *qubits, and will contain* ans_b *and the corresponding opening* op_b.
2. *Next, the extractor sends challenge bit* $b = 0$. *The prover applies* $\mathbf{U}_0$ *to* $|\psi_{\mathsf{msg}_1}\rangle$, *measures the registers* A, O, *and sends* $\mathsf{msg}_{3,0} = (\mathsf{ans}_0, \mathsf{op}_0)$.
3. *The extractor checks if* $\mathbf{V}_2(\mathsf{msg}_1, 0, \mathsf{msg}_{3,0}) = 1$. *If so, it asks the prover to apply* $\mathbf{U}_0^\dagger$.
4. *The extractor sends challenge bit* $b = 1$. *The prover applies* $\mathbf{U}_1$ *to* $|\psi_{\mathsf{msg}_1}\rangle$, *measures the registers* A, Z, *and sends* $\mathsf{msg}_{3,1} = (\mathsf{ans}_1, \mathsf{op}_1)$.
5. *Finally, it extracts witness from* ans_0 *and* ans_1.

Let p_{Ext} *denote the probability of successful extraction. First, we noted that the extractor only needs to verify* $(\mathsf{ans}_b, \mathsf{op}_b)$ *with respect to* msg_1, *but doesn't need* $\mathsf{op}_0, \mathsf{op}_1$ *for extracting the witness. Therefore, instead of measuring the registers* M, O, *one only needs to run* $\mathbf{V}_2(\mathsf{msg}_1, b, \cdot)$ *on registers* M, O, *followed by measuring register* M.

Next, using the security of collapse-binding commitments, we argued that p_{Ext} *is close to seeing an 'accept' in both the projective measurements in the following experiment:*

1. *First, using the prover, we compute the first message* msg_1 *and state* $|\psi_{\mathsf{msg}_1}\rangle_{\mathsf{A,O,Z}}$.

2. *Next, we apply* $\mathbf{U}_0$ *to registers* $\mathsf{A}, \mathsf{O}, \mathsf{Z}$*, followed by two-outcome measurement* $\mathcal{P}_0 = (\mathbf{\Delta}_0, \mathbf{I} - \mathbf{\Delta}_0)$ *where*

$$\mathbf{\Delta}_0 = \sum_{\substack{\mathsf{ans},\mathsf{op}: \\ \mathbf{V}_2(\mathsf{msg}_1,0,(\mathsf{ans},\mathsf{op}))=1}} |\mathsf{ans},\mathsf{op}\rangle\langle\mathsf{ans},\mathsf{op}| \otimes \mathbf{I}.$$

3. *Next, we apply* $\mathbf{U}_1 \cdot \mathbf{U}_0^\dagger$*, followed by two-outcome measurement* $\mathcal{P}_1 = (\mathbf{\Delta}_1, \mathbf{I} - \mathbf{\Delta}_1)$ *where*

$$\mathbf{\Delta}_1 = \sum_{\substack{\mathsf{ans},\mathsf{op}: \\ \mathbf{V}_2(\mathsf{msg}_1,1,(\mathsf{ans},\mathsf{op}))=1}} |\mathsf{ans},\mathsf{op}\rangle\langle\mathsf{ans},\mathsf{op}| \otimes \mathbf{I}.$$

Let p'_{Ext} *denote the probability of seeing 'accept' in both the projective measurements. This probability can be expressed as follows:*

$$p'_{\mathrm{Ext}} = \left\| \mathbf{\Delta}_1 \cdot \mathbf{U}_1 \cdot \mathbf{U}_0^\dagger \cdot \mathbf{\Delta}_0 \cdot \mathbf{U}_0 \left|\psi_{\mathsf{msg}_1}\right\rangle \right\|^2$$

In order to prove a lower bound on p'_{Ext}*, we need to use the fact that the prover succeeds with probability* $1/2 + \epsilon$*. Therefore, assuming the first message is* ϵ-good*, we know that*

$$\left\|\mathbf{\Delta}_0 \cdot \mathbf{U}_0 \left|\psi_{\mathsf{msg}_1}\right\rangle\right\|^2 + \left\|\mathbf{\Delta}_1 \cdot \mathbf{U}_1 \left|\psi_{\mathsf{msg}_1}\right\rangle\right\|^2 \geq 1 + \epsilon.$$

1. *Show that* $p'_{\mathrm{Ext}} \geq \mathrm{poly}(\epsilon)$*.*

Below, we present an alternate proof outline, using the gentle measurement lemma*.*

2. *Let* $|\psi\rangle$ *be a pure state, and* $\mathcal{P} = (\mathbf{P}, \mathbf{I} - \mathbf{P})$ *any projective measurement such that* $\mathsf{Tr}\left(\mathbf{P} \cdot |\psi\rangle\langle\psi|\right) = 1 - \epsilon$*. Let* $\rho = |\psi\rangle\langle\psi|$ *and* ρ' *the post-measurement state, conditioned on measurement output being* 0*. Show a bound on* $\|\rho - \rho'\|_{\mathrm{tr}}$ *in terms of* ϵ*.*

3. *Show that if two states* ρ, ρ' *satisfy* $\|\rho - \rho'\|_{\mathrm{tr}} \leq \epsilon$*, then for any unitary matrix* $\mathbf{U}$*,* $\left\|\mathbf{U} \cdot \rho \cdot \mathbf{U}^\dagger - \mathbf{U} \cdot \rho' \cdot \mathbf{U}^\dagger\right\|_{\mathrm{tr}} \leq \epsilon$*.*

4. *Using the gentle measurement lemma, give an alternate proof for Part 1.*

Question 4. ***Collapse-binding commitments imply prof-binding commitments*** *(5 marks)*

In Lecture 1, we saw two definitions for the binding property of commitments. One is the usual notion of computational binding (the adversary cannot produce a commitment together with openings for two different messages). Another was prof-binding *commitments (for single-bit messages), which are characterized by the following security game: the adversary sends a commitment, then the challenger sends a uniformly random challenge bit. The adversary must produce an opening for this challenge bit. We saw that, in the classical setting, these two notions are equivalent, since*

we can rewind the adversary for the prof-binding security game. This is not true if the prof-binding adversary is a quantum algorithm. Even if our commitment scheme is computationally binding w.r.t. quantum adversaries, it may not be prof-binding w.r.t. a quantum adversary.

However, if a commitment scheme is collapse-binding (instead of just comp. binding), then it is also prof-binding wrt quantum adversaries. Therefore, this is yet another setting that illustrates why collapse-binding is the right definition for commitments in the quantum setting.

Prof-binding commitments have a better name in crypto literature: sum-binding commitments.

1. *Let* Commit *be a single-bit commitment scheme. Show that if* Commit *satisfies the collapse-binding property, then it also satisfies prof-binding.*

   Hint: the solution is along the lines of what we discussed in class for Blum's protocol's computational soundness. Additionally, you can refer to this paper.

Question 5. ***Blum's protocol: Post-Quantum ZK*** *(10 marks)*

In class, we saw a post-quantum zero-knowledge proof for the graph-isomorphism protocol. For this proof, we used the verifier's circuit to build a unitary $\mathbf{Q}$ *such that*

$$\mathbf{Q}\,|\mathbf{0}\rangle\,|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle\,|\psi_0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|\psi_1\rangle\,.$$

Using the unitary $\mathbf{Q}$ *and its inverse, we discussed how to output* $|\psi_0\rangle$ *with overwhelming probability.*

In this problem, we will apply the alternating projectors idea for proving that Blum's protocol satisfies post-quantum zero-knowledge.

1. *Similar to the graph-isomorphism protocol, construct a unitary* $\mathbf{Q}$ *for Blum's protocol such that*

$$\mathbf{Q}\,|\mathbf{0}\rangle\,|\psi\rangle = \sqrt{p_\psi}\,|0\rangle\,|\psi_0\rangle + \sqrt{1-p_\psi}\,|1\rangle\,|\psi_1\rangle\,.$$

2. *Unlike the GI protocol, we cannot say that* $p_\psi = 0.5$ *for all* $|\psi\rangle$*. Prove that if* $|p_\psi - 0.5|$ *is non-negligible, then there exists a q.p.t. algorithm that can break computational hiding property of the commitment scheme.*

3. *Use the above to prove that the simulator's output is computationally indistinguishable from the verifier's view in the real-world.*
   Hint: This part is a bit challenging, you can refer to Watrous' proof here, or discuss with me.

Bonus Questions

Bonus Question 1. ***Post-quantum extraction for protocols with*** k***-special soundness*** *(5 marks)*

Consider a 3-round protocol with the following properties:

- *The challenge space is* $\{0, 1, \ldots, k-1\}$. *Given k transcripts* $\left((\mathsf{msg}_1, i, \mathsf{msg}_{3,i})\right)_{i \leq k}$ *with the same first message* msg_1, *there exists an efficient extractor that can extract a witness.*

Use this base protocol to construct a protocol with post-quantum extraction. What is the knowledge-error, and what is the probability of successful extraction?

Bonus Question 2. ***Combiners for collapsing hash functions*** *(5 marks)*

Suppose H_0, H_1 *are (keyed) functions mapping t bits to n bits. We are given that at least one of these two functions is a CRHF, and our objective is to build a CRHF using* H_0 *and* H_1. *The simplest* combiner *is to concatenate the outputs of* H_0 *and* H_1. *That is, consider the function* $H(x) = H_0(x) \mid\mid H_1(x)$. *If there exists an adversary that can find a collision for H, then the adversary can find a collision for both* H_0 *and* H_1.

We can ask the same question for collapse-binding hash functions. Is the above combiner a good combiner for the collapse-binding property? Prove, or provide a counterexample. Any other candidates for collapse-binding hash functions?