COL872: Quantum and Post-Quantum Cryptography

Problem Set 5

Due date: May 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 26/04/23.

Questions

Question 1. ***Universal Cloning*** *(8 marks)*

In our lectures, we saw that universal cloning *is impossible. However, it is impossible only if we require perfect cloning. Let T be a quantum process (includes unitaries, measurements, adding ancilla bits) that takes as input a single qubit, and outputs two qubits. We say that T is a p-good cloning device if for all pure states $|\psi\rangle$ over a single qubit,*

$$|\langle\psi| \langle\psi| \cdot T(|\psi\rangle\langle\psi|) \cdot |\psi\rangle |\psi\rangle| \geq p$$ [1]

1. *Consider the following quantum process: it maps $\alpha |0\rangle + \beta |1\rangle$ to $\alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle$. Is T p-good for some constant p?*
2. *Consider the following quantum process: on input $|\psi\rangle$, it attaches two ancilla bits, initialized to $|0\rangle$. Let $\mathbf{U}$ be a unitary that operates on three qubits as follows:*

$$\mathbf{U} \cdot |0\rangle |0\rangle |0\rangle = \sqrt{\frac{2}{3}} |0\rangle |0\rangle |0\rangle + \sqrt{\frac{1}{6}} |0\rangle |1\rangle |1\rangle + \sqrt{\frac{1}{6}} |1\rangle |0\rangle |1\rangle$$

[1] Here, we are considering the density matrix corresponding to the output of T.

$$\mathbf{U} \cdot |1\rangle |0\rangle |0\rangle = \sqrt{\frac{2}{3}} |1\rangle |1\rangle |1\rangle + \sqrt{\frac{1}{6}} |1\rangle |0\rangle |0\rangle + \sqrt{\frac{1}{6}} |0\rangle |1\rangle |0\rangle$$

Finally, after applying $\mathbf{U}$ *to* $|\psi\rangle |0\rangle |0\rangle$*, it measures the last qubit, and outputs the resulting state* ρ *(over two qubits).*
Prove that, for all $|\psi\rangle$*,*

$$|\langle\psi| \rho |\psi\rangle| \geq 2/3.$$

Question 2. ***Collapsing hash from somewhere-statistically-binding hash*** *(10 marks)*

In this problem, we will see yet another construction of collapsing hash, based on another classically defined primitive called somewhere-statistically-binding (SSB) hash. We have constructions for SSB hash based on many standard assumptions, including LWE.

Let s, ℓ, L *be some parameters such that* $L > \ell$*. An* (s, ℓ, L)*-SSB hash consists of two algorithms* Setup *and a hash function family* $\left\{H_k : (\{0,1\}^s)^L \to \{0,1\}^\ell\right\}_{k \in \mathcal{K}}$ *with the following syntax:*

- $\mathsf{Setup}(i \in [L])$*: outputs a key* $k \in \mathcal{K}$*.*

It must satisfy the following correctness and security properties:

- ***Correctness:*** *There exists a negligible function* negl *such that for every* $i \in [L]$*, if* $k \leftarrow \mathsf{Setup}(i)$*, then*

  $$\Pr\left[\exists \mathbf{x} = (\mathbf{x}_0, \ldots, \mathbf{x}_{L-1}), \mathbf{x}' = (\mathbf{x}'_0, \ldots, \mathbf{x}'_{L-1}) \text{ s.t. } \mathbf{x}_i \neq \mathbf{x}'_i, H_k(\mathbf{x}) = H_k(\mathbf{x}')\right] \leq \mathsf{negl}.$$

  Here, the probability is over the choice of k*. If the above probability is* 0 *for all* $i \in [L]$*, then we say that the hash function is somewhere-perfectly-binding.*

- ***Security:*** *For all* $i \neq i'$*,*

  $$\{k \leftarrow \mathsf{Setup}(i)\} \approx_c \{k \leftarrow \mathsf{Setup}(i')\}.$$

Let (Setup, H) *be an SSB-hash. Construct a collapsing hash function (with appropriate domain and co-domain) using the SSB-hash, and prove security of your construction.*

Question 3. ***Optimal Attack on Wiesner's Scheme*** *(6 marks)*

Problem 4 from here.

Question 4. ***Publicly Verifiable Quantum Money*** *(8 marks)*

In class, we saw a construction of publicly verifiable QM from a hash function family $\mathcal{H}$ *that is collision-resistant but not collapsing. The quantum coin in this case included two classical strings* h, σ*, together with* $|\psi_h\rangle_{\mathsf{X}} |\psi_{st}\rangle_{\mathsf{S}}$*. The verification algorithm uses the collapsing algorithm* $(\mathsf{Alg}_1, \mathsf{Alg}_2)$ *on registers* X, S*.*

In this problem, we will complete the security proof of this construction.

- *Suppose the QM adversary always outputs a forgery of the form*

$$\sum_{\substack{x,s,s':\\ H(x)=h}} \alpha_{x,s,x,s'} |x\rangle_{\mathsf{X}_1} |s\rangle_{\mathsf{S}_1} |x\rangle_{\mathsf{X}_2} |s'\rangle_{\mathsf{S}_2} .$$

  Show that if the challenger runs VerifyCoin *on* $(\mathsf{X}_1, \mathsf{S}_1)$ *and* $(\mathsf{X}_2, \mathsf{S}_2)$*, the probability of an accept in both the verifications is at most* c *for some constant* $c < 1$*.*

- *Now consider a general QM adversary that outputs a forgery of the form*

$$\sum_{\substack{x,s,x',s':\\ H(x)=H(x')=h}} \alpha_{x,s,x',s'} |x\rangle_{\mathsf{X}_1} |s\rangle_{\mathsf{S}_1} |x\rangle_{\mathsf{X}_2} |s'\rangle_{\mathsf{S}_2} \text{ where } \sum_{\substack{x,s,s':\\ H(x)=h}} |\alpha_{x,s,x,s'}|^2 > 0.9999.$$

  Show that if the challenger runs VerifyCoin *on* $(\mathsf{X}_1, \mathsf{S}_1)$ *and* $(\mathsf{X}_2, \mathsf{S}_2)$*, the probability of an accept in both the verifications is at most* c' *for some constant* $c' < 1$*.*

Question 5. ***Proofs of Quantumness without adaptive hardcore bit*** *(8 marks)*

Consider the following proofs-of-quantumness protocol, given by [KCVY21]. The protocol is similar to the protocol we saw in class; however it does not use the 'adaptive hardcore bit' property. Let us assume $f_k : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$*.*

1. *V1: The verifier samples* $(k, \mathsf{td}) \leftarrow \mathsf{Setup}(1^\lambda)$ *and sends* k *to the prover.*
2. *P1: The prover sends a string* $y \in \{0,1\}^n$*. It maintains a state* $|\psi_1\rangle = |0\rangle |x_0\rangle + |1\rangle |x_1\rangle$ *(ignoring normalization).*
3. *V2: The verifier picks a challenge bit* $c \leftarrow \{0,1\}$ *and sends to the prover. If* $c = 1$*, it also samples* $r \leftarrow \{0,1\}^n$ *and sends* r *to the prover.*
4. *P2: If* $c = 0$*, the prover measures its state in the standard basis and sends* (b, x) *to the verifier.*

   If $c = 1$*, the prover computes* $|\psi_2\rangle_{\mathsf{B},\mathsf{X},\mathsf{R}} = |0\rangle_{\mathsf{B}} |x_0\rangle_{\mathsf{X}} |r \cdot x_0\rangle_{\mathsf{R}} + |1\rangle_{\mathsf{B}} |x_1\rangle_{\mathsf{X}} |r \cdot x_1\rangle$ *R. It then applies Hadamard on the registers* (B, X)*, measures and sends the output* (b, d) *to the verifier.*
5. *V3: The verifier picks a uniformly random bit* $c' \leftarrow \{0,1\}$ *and sends to the prover.*
6. *P3: If* $c' = 0$*, the prover applies projective measurement*

$$\mathcal{P}_{\pi/8} = (|\pi/8\rangle\langle\pi/8|, \mathbf{I} - |\pi/8\rangle\langle\pi/8|) .$$

   If $c' = 1$*, the prover applies projective measurement*

$$\mathcal{P}_{-\pi/8} = (|-\pi/8\rangle\langle-\pi/8|, \mathbf{I} - |-\pi/8\rangle\langle-\pi/8|) .$$

   Here, $|\theta\rangle = \cos(\theta) |0\rangle + i \sin(\theta) |1\rangle$*.*
7. *V4: The verifier checks the responses of the prover.*

- *Complete Step V_4.*
- *(Completeness) Prove that the honest quantum prover's response is accepted with probability 1 if $c = 0$, else it is accepted with probability $\cos^2(\pi/8)$ if $c = 1$.*
- *(Soundness) Show an upper bound on the success probability of any p.p.t. (classical) prover.*

[KCVY21] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically-Verifiable Quantum Advantage from a Computational Bell Test. *CoRR*, abs/2104.00687, 2021. Pre-print available at arXiv:2104.00687.