COL872
Problem Set 5

Mallika Prabhakar (2019CS50440)
Sayam Sethi (2019CS10399)
Satwik Jain (2019CS10398)

May 2023

Contents

1 Question 1

1.1 Question 1.1

Universal Cloning

Question. *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?*

Proof. We know that T converts a pure state to another pure state. So Application of T on the density matrix $\langle\psi\rangle\,\psi$ will give the density matrix of another pure state.
For a state to be p-good,

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

For $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$,
we have LHS as
$\alpha^2\langle 0|\langle 0|+\alpha\beta(\langle 0|\langle 1|+\langle 1|\langle 0|)+\beta^2\langle 1|\langle 1|\cdot T(|\psi\rangle\langle\psi|)\cdot\alpha^2|0\rangle|0\rangle+\alpha\beta(|0\rangle|1\rangle+|1\rangle|0\rangle)+\beta^2|1\rangle|1\rangle$
where, $T(|\psi\rangle\langle\psi|)=(\alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle)(\alpha\langle 0|\langle 0|+\beta\langle 1|\langle 1|)$

then the LHS becomes $(\alpha^3+\beta^3)^2$
Now we have $\alpha^2+\beta^2=1$, $|\alpha|,|\beta|\leq 1$
Using this we get $(\alpha^3+\beta^3)^2\geq\frac{1}{2}$.
Therefore, T is a half-good cloning device. $\square$

1.2 Question 1.2

Universal Cloning

Question. *Prove that, for all* $|\psi\rangle$, $|\langle\psi|\langle\psi|\rho|\psi\rangle|\psi\rangle|\geq 2/3$

Proof. let the input be $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ with $\alpha^2+\beta^2=1$.
Now applying Unitary on $|\psi\rangle|0\rangle|0\rangle$,

$$U\cdot|\psi\rangle|0\rangle|0\rangle=\left(\alpha\sqrt{\frac{2}{3}}|00\rangle+\frac{\beta}{\sqrt{6}}|10\rangle+\frac{\beta}{\sqrt{6}}|01\rangle\right)|0\rangle+\left(\beta\sqrt{\frac{2}{3}}|11\rangle+\frac{\alpha}{\sqrt{6}}|10\rangle+\frac{\alpha}{\sqrt{6}}|01\rangle\right)|1\rangle$$

Now measuring the last qubit, we get

$$|\phi\rangle=\{(p_i,\frac{1}{\sqrt{p_i}}|\phi_i\rangle)\}_{i\in\{0,1\}}$$

Where,

$$
\begin{aligned}
|\phi_0\rangle &= \alpha\sqrt{\frac{2}{3}}\,|00\rangle + \frac{\beta}{\sqrt{6}}\,|10\rangle + \frac{\beta}{\sqrt{6}}\,|01\rangle \\
|\phi_1\rangle &= \beta\sqrt{\frac{2}{3}}\,|11\rangle + \frac{\alpha}{\sqrt{6}}\,|10\rangle + \frac{\alpha}{\sqrt{6}}\,|01\rangle \\
p_0 &= \frac{2\alpha^2+\beta^2}{3} = \frac{1+\alpha^2}{3} \\
p_1 &= \frac{\alpha^2+2\beta^2}{3} = \frac{1+\beta^2}{3} \\
p_0 + p_1 &= 1
\end{aligned}
$$

Therefore, we get

$$
|\,\langle\psi|\,\langle\psi|\,\rho\,|\psi\rangle\,|\psi\rangle\,| = (|\,\langle\psi|\,\langle\psi|\,|\phi_0\rangle\,\langle\phi_0|\,|\psi\rangle\,|\psi\rangle\,|) + (|\,\langle\psi|\,\langle\psi|\,|\phi_1\rangle\,\langle\phi_1|\,|\psi\rangle\,|\psi\rangle\,|)
$$

$$
\begin{aligned}
|\,\langle\psi|\,\langle\psi|\,|\phi_0\rangle\,\langle\phi_0|\,|\psi\rangle\,|\psi\rangle\,| &= \left(\alpha^3\sqrt{\frac{2}{3}} + \alpha\beta^2\frac{2}{\sqrt{6}}\right)^2 \\
&= \frac{2\alpha^2}{3}\left(\alpha^2+\beta^2\right)^2 \\
&= \frac{2\alpha^2}{3}
\end{aligned}
$$

Similarly,

$$
|\,\langle\psi|\,\langle\psi|\,|\phi_1\rangle\,\langle\phi_1|\,|\psi\rangle\,|\psi\rangle\,| = \frac{2\beta^2}{3}
$$

Therefore,

$$
\begin{aligned}
|\,\langle\psi|\,\langle\psi|\,\rho\,|\psi\rangle\,|\psi\rangle\,| &= \frac{2}{3}(\alpha^2+\beta^2) \\
&= \frac{2}{3}
\end{aligned}
$$

$\square$

2 Question 2

Question 2

Question. *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.*

Proof.

Claim 2.1. *Let H_k be an SSB-hash with input domain $(\{0,1\}^s)^L$, co-domain $\{0,1\}^l$ with hash key k. The same construction of H_k works as a collapsing hash. The property of H_k is that $\Pr[\exists x, x'\ s.t.\ x_i \neq x'_i, H_k(x) = H_k(x')] = negl$ where $x = (x[0], x[1], \ldots x[L-1]), x' = (x'[0], x'[1], \ldots x'[L-1])$*

Proof. We need to show that if an Adversary can break Collapsing hash, SSB-Hash is broken. SSB-Hash game can be defined as finding a collision x, x'. Let us consider the following reduction-

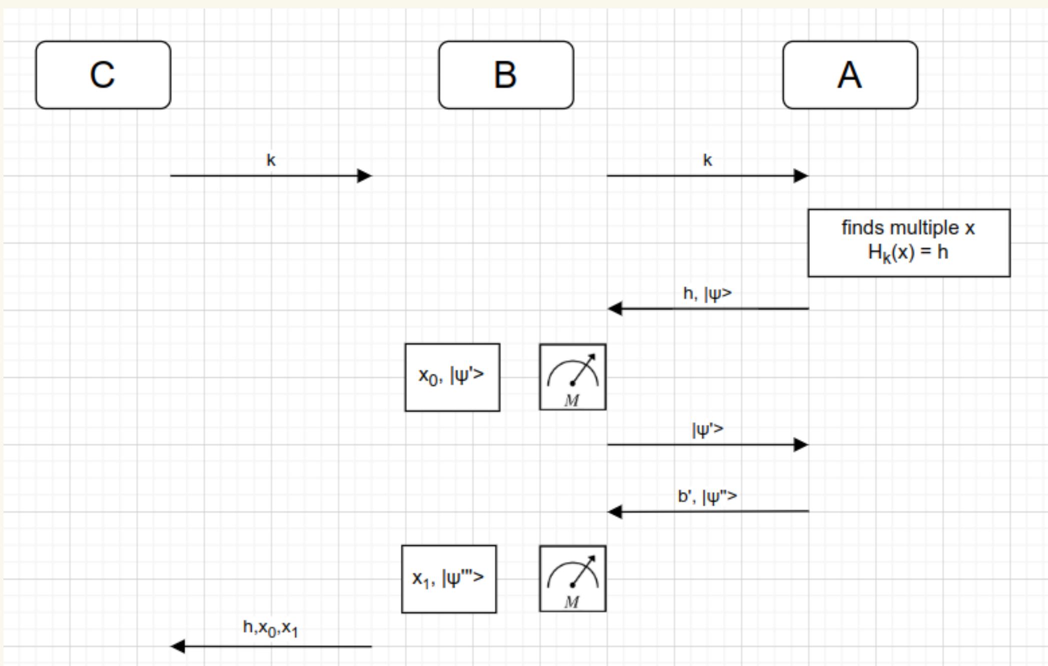

Figure 1: B and C are playing SSB-Hash game, A is playing Collapsing Hash

C gives the key k to B. B forwards it to A and A finds a superposition of $|x\rangle = |\psi\rangle$ such that $H_k(x) = h$ and sends $h, |\psi\rangle$. B measures $|\psi\rangle$ and obtains $|x_0\rangle$ and residual state $|\psi'\rangle$. It sends back $|\psi'\rangle$. A then finds out b' and has a residual state $|\psi''\rangle$ B takes that $|\psi''\rangle$ and measures to obtain $|x_1\rangle$. B then sends $h, |x_0\rangle, |x_1\rangle$ to C.

□

Claim 2.2. *B wins SSB-Hash game with non-negligible probability since $H_k(x_0) = H_k(x_1) = h$ with non-negligible probability.*

Proof. In the good case, when the A sends a valid superposition $|\psi\rangle$, B measures $|\psi\rangle$ to obtain $|x_0\rangle$ and $H_k(x_0) = h$ with probability 1. When the measured state $|\psi\rangle$ is operated on by A to obtain, it finally has a state $|\psi''\rangle)$. This is measured by B to obtain $|x_1\rangle$. Probability of getting a valid x_1 such that $H_k(x_1) = h$ is non-negligible (p) (proven in PS4, Q2.1). This is true only if it is not a collapsing hash. Hence:

$$\Pr[\text{finding a collision}] = \Pr[H_k(x_0) = h] \times \Pr[H_k(x_1) = h] = p$$

which is non-negligible. □

This is a contradiction of our assumption that the given SSB-Hash scheme is secure. Therefore, our proposed use of SSB-Hash as a collapsing hash must be valid.

□

3 Question 3

3.1 Question 3.1

Optimal Attack on Wiesner's Scheme

Question. *Give a procedure that succeeds in attacking Weisner's Scheme with probability at least* $\frac{5}{8}$

Proof. The Procedure is as follows:

1. Bank sends a qubit $|\psi\rangle$ to adversary.
2. Adversary measures the qubit in $\{|0\rangle, |1\rangle\}$ basis.
3. Adversary creates two identical copies based on the measured value and sends the qubits to the Bank.

If the qubit is in $\{|0\rangle, |1\rangle\}$ basis, we will get the correct measurement and will be able to model copies correctly and fool the bank.
If the qubit is in $\{|+\rangle, |-\rangle\}$ basis, The adversary measures in $\{|0\rangle, |1\rangle\}$ basis and models the qubit in the same basis. When the bank measures the copies in $\{|+\rangle, |-\rangle\}$ basis, there is a 1/2 probability of getting the correct measurement for each copy.
Therefore, the overall probability of fooling the Bank is $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{5}{8}$ □

3.2 Question 3.2

Optimal Attack on Wiesner's Scheme

Question. *Show that the probability of success for new procedure is higher than what was achieved in part 3.1.*

Proof. Let us find the probability to fool the bank in the cases when qubit is $|0\rangle$ & $|+\rangle$. the other two cases follow from it.
When qubit is $|0\rangle$,
After applying the unitary and discarding the first qubit, we get $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ with probability $\frac{1}{6}$ and $\frac{3|00\rangle+|11\rangle}{\sqrt{10}}$ with probability $\frac{5}{6}$.
From here the chance of the strategy succeeding $= \frac{1}{6} \times 0 + \frac{5}{6} \times \frac{9}{10} = \frac{3}{4}$.
Similarly the probability for $|1\rangle$ is also $\frac{3}{4}$.

Now when qubit is $|+\rangle$,
After applying the unitary and discarding the first qubit, we get $\frac{3|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{12}}$ with probability $\frac{1}{2}$ and $\frac{|00\rangle+|01\rangle+|10\rangle+3|11\rangle}{\sqrt{12}}$ with probability $\frac{1}{2}$.
working with first factor, we apply Hadamard on the two qubits, and then find the probability of getting $|00\rangle$(which corresponds to $|{++}\rangle$ in the original case).

Applying Hadamard, we get $\frac{3|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{12}}$ and probability of getting $|00\rangle$ is $\frac{3}{4}$ in this case.
Similarly for the other factor Applying Hadamard, we get $\frac{3|00\rangle-|01\rangle-|10\rangle+|11\rangle}{\sqrt{12}}$ and probability of getting $|00\rangle$ is $\frac{3}{4}$ in this case as well.
Therefore the overall probabilty for this case comes out to be $\frac{3}{4}$.
Similarly for the case when qubit is $|-\rangle$, we get the probability as $\frac{3}{4}$.
Therefore the probability in all the four cases comes out to be $\frac{3}{4}$ which ultimately is the overall probability. $\square$

4 Question 4

4.1 Question 4.1

Question 4

Question. *Suppose the QM adversary always outputs a forgery of the form*

$$\sum_{x,s,s' H(x)=h} \alpha_{x,s,x,s'} |x\rangle_{x_1} |s\rangle_{s_1} |x\rangle_{x_2} |s'\rangle_{s_2}$$

Show that if the challenger runs $VerifyCoin$ on (X_1, S_1) and (X_2, S_2), the probability of an accept in both the verifications is at most c for some constant $c < 1$.

Proof. Given coins (X_1, S_1) and (X_2, S_2), since $X_1 = X_2$, there are no collisions to be found, hence we look at the probabilities of successful validation. On running $\mathsf{Test1}$ on the state $|\phi\rangle = \sum_{x,s,s',H(x)=h} \alpha_{x,s,s'} |x\rangle_{X_1} |s\rangle_{S_1} |x\rangle_{X_2} |s'\rangle_{S_2}$, the probability of validation passing is obtained as follows:

$$\begin{aligned}
& p_1 = \Pr\left[\mathsf{Measure}(\mathsf{Alg}_2(|\phi\rangle, |00\rangle)) = 11\right] \\
\implies & p_1 = \Pr\left[\mathsf{Measure}\left(\sum_{x,s,s',b_0,b_1} \alpha_{x,s,s'} \cdot \beta_{x,s,s',b_0,b_1} |y_x\rangle |t_s\rangle |z_x\rangle |u_{s'}\rangle |b_0 b_1\rangle\right) = 11\right] \\
\implies & p_1 = \sum_{x,s,s'} |\alpha_{x,s,s'} \cdot \beta_{x,s,s',1,1}|^2
\end{aligned} \tag{1}$$

For $\mathsf{Test2}$, let ρ be the state after measuring $|\phi\rangle$, the probability of validity is as follows:

$$\begin{aligned}
p_2 &= \Pr\left[\mathsf{Measure}(\mathsf{Alg}_2(\rho, |00\rangle)) = 00\right] \\
&\leq 1 - \Pr\left[\mathsf{Measure}(\mathsf{Alg}_2(\rho, |00\rangle)) = 11\right] \\
&\leq 1 - \sum_{x,s,s'} \alpha^2_{x,s,s'} \Pr\left[\mathsf{Measure}\left(Alg_2\left(|x\rangle |s\rangle |x\rangle |s'\rangle, |00\rangle\right)\right) = 00\right] \\
&\leq 1 - \sum_{x,s,s'} \alpha^2_{x,s,s'} \Pr\left[\mathsf{Measure}\left(|y_x\rangle |t_s\rangle |z_x\rangle |u_{s'}\rangle \left(\sum_{b_0,b_1} \beta_{x,s,s',b_0,b_1} |b_0 b_1\rangle\right)\right) = 00\right] \\
&\leq 1 - \sum_{x,s,s'} |\alpha_{x,s,s'} \cdot \beta_{x,s,s',1,1}|^2 \\
&\leq 1 - p_1
\end{aligned} \tag{2}$$

Therefore, the probability of the adversary succeeding is $(p_1 + p_2)/2 \leq 1/2 (= c)$. $\square$

4.2 Question 4.2

Question 4.2

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

$$\sum_{\substack{x,s,x',s':\\ H(x)=H(x')=h}} \alpha_{x,s,x',s'} \left|x\right\rangle_{X_1} \left|s\right\rangle_{S_1} \left|x'\right\rangle_{X_2} \left|s'\right\rangle_{S_2} \ \textit{where} \sum_{\substack{x,s,s'\\ H(x)=h}} \left|\alpha_{x,s,x,s'}\right|^2 > 1-\epsilon \tag{3}$$

Show that if the challenger runs $\mathsf{VerifyCoin}$ *on* (X_1, S_1) *and* (X_2, S_2)*, the probability of an accept in both the verifications is at most c0 for some constant* $c' < 1$*.*

Proof. (Note: we prove a general result for any $1 \geq \epsilon > 0$)
Let the probability of success on applying $\mathsf{Test1}$ on both coins be p_1 and on applying $\mathsf{Test2}$ be p_2. Now, we find a bound on p_2 in terms of p_1 using the trace distance between the adversary's state and the state obtained after measuring the register x $(= 2\sqrt{\epsilon})$,

$$\begin{aligned} p_1 &\leq \Pr\left[x = x'\right] \cdot (1 - p_0 + \mathsf{Tr}_{dist}) + \Pr\left[x \neq x'\right] \cdot 1 \\ &= (1-\epsilon) \cdot (1 - p_0 + 2\sqrt{\epsilon}) + \epsilon \end{aligned} \tag{4}$$

Thus, the total probability of success is,

$$\begin{aligned} \frac{1}{2}(p_0 + p_1) = \frac{1 + \epsilon \cdot p_0 + 2\sqrt{\epsilon} \cdot (1-\epsilon)}{2} &\leq \frac{1}{2} + \frac{\sqrt{\epsilon}}{2} \cdot (2 + p_0 - \sqrt{\epsilon}) \\ &\leq \frac{1}{2} + c' \end{aligned} \tag{5}$$

Therefore, any adversary has atmost a constant probability of giving a valid forgery for the publically-verifiable QM scheme. ☐

5 Question 5

5.1 Question 5.1

Question 5.1

Question. *Complete Step V_4.*

Proof. We assume that V_4 executes iff $c = 1$. In the case when $c = 0$, the verifier simply checks if the obtained x_b is one of x_0 or x_1 (the verifier knows the two pre-images using $\mathtt{td}$ and y). The steps of V_4 are:

1. The verifier first computes x_0, x_1 using $\mathtt{td}, y$.
2. Using r, b, d, x_0, x_1, the verifier can uniquely determine the state $|\psi_2\rangle$. Note that $|\psi_2\rangle = |b\rangle |d\rangle |\psi\rangle$, where $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.
3. Based on c', the verifier knows what should be the most-likely response of the prover. If the response is the same, the verifier accepts, else it rejects.

$\square$

5.2 Question 5.2

Question 5.2

Question. *(Completeness) Prove that the honest quantum prover's response is accepted with probability* 1 *if* $c = 0$, *else it is accepted with probability* $\cos^2 \frac{\pi}{8}$ *if* $c = 1$.

Proof. If $c = 0$, then, if the prover followed the protocol honestly, on measuring $|\psi_1\rangle$ it will definitely get one of the pre-images of y. Thus, the verifier will always accept in that case. Otherwise, if $c = 1$, then the measurement is at a distance of $\pi/8$ from the actual state $|\psi\rangle$ (which is at an angle $\theta \in \{-\pi/4, 0, \pi/4, \pi/2\}$ with respect to $|0\rangle$). Therefore, the probability of an honest prover outputting the correct bit is $\cos^2 \frac{\pi}{8}$. $\square$

5.3 Question 5.3

Question 5.3

Question. *(Soundness) Show an upper bound on the success probability of any p.p.t. (classical) prover.*

Proof. $\square$

6 Bonus Question 2 (PS4)

Combiners for collapsing hash functions

Question. *Is the concatenating combiner a good combiner for the collapse-binding property?*

Proof. Let $\mathcal{H}_0, \mathcal{H}_1 : \{0,1\}^n \rightarrow \{0,1\}^{n/2}$.
Let $\mathcal{H} = \mathcal{H}_0 \| \mathcal{H}_1$ where at-least one of $\mathcal{H}_0, \mathcal{H}_1$ is a collapse binding hash function. We will prove that $\mathcal{H}$ is also a collapse binding hash function through contradiction.
Suppose $\mathcal{H}$ is not a collapse binding hash function. then Using an adversary $\mathcal{A}$ that breaks the collapsing property of $\mathcal{H}$, we can achieve a reduction $\mathcal{B}$ that breaks collapsing property of $\mathcal{H}_0$ if applicable.
Reduction:

1. Challenger sends a hash key k to $\mathcal{B}$ who forwards the same to $\mathcal{A}$.
2. $\mathcal{A}$ sends a string $h \in \{0,1\}^n, h = h_0 \| h_1$ to $\mathcal{B}$ along with a quantum state $|\psi\rangle = \Sigma_{x:H(x)=h} |x\rangle$.
3. $\mathcal{B}$ sends h_0 along with $|\psi\rangle$ to Challenger.
4. Challenger chooses a bit b, if $b = 0$ it measures $|\psi\rangle$ and sends it back otherwise it sends back $|\psi\rangle$ to $\mathcal{B}$.
5. $\mathcal{B}$ forwards the message from Challenger to $\mathcal{A}$.
6. $\mathcal{A}$ sends a bit b' to $\mathcal{B}$ who forward it to Challenger and wins if $b = b'$.

As Reduction is just passing the messages to $\mathcal{A}$, $|\psi\rangle$ is a also a valid superposition for $\mathcal{H}_0$. As $\mathcal{A}$ is able to win with a non-negligible probability, $\mathcal{B}$ will also win with a non-negligible probability.
Similarly a reduction can be shown for $\mathcal{H}_1$.
But Since atleast one of $\mathcal{H}_0, \mathcal{H}_1$ is collapse binding, we reach a contradiction. Therefore $\mathcal{H}$ is also a collapse binding hash function.

□