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. □

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. The Partial measurement of □

2 Question 2

2.1 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. Let H_k be an SSB-hash with input domain $(\{0,1\}^s)^L$ and co-domain be $\{0,1\}^l$ with hash key k. The same construction of H_k works as a collapsing hash. The property of H_k is that $\Pr[\exists x = (x[0], x[1], \ldots x[L-1])]$ $\square$

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 $\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{5}{8}$ $\square$

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. $\square$

4 Question 4

4.1 Question 4.1

Question 4

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

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

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. proof ☐

4.2 Question 4.1

Question x

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

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

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 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 Test1 on both coins be p_1 and on applying 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 $(= 2\sqrt{\epsilon})$,

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

Thus, the total probability of success is,

$$\begin{aligned} \frac{1}{2}(p_0 + p_1) = \frac{1 + \epsilon \cdot p_0 + 2\sqrt{\epsilon} \cdot (1-\epsilon)}{2} &\leq \frac{1}{2} + \frac{\sqrt{\epsilon}}{2} \cdot (2 + p_0 - \sqrt{\epsilon}) \\ &\leq \frac{1}{2} + c' \end{aligned} \tag{3}$$

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.

□

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 $\cos^2 \frac{\pi}{8}$. □

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. □