Frontiers of Quantum Complexity and Cryptography Spring 2022

Lecture 10

Lecturer: Henry Yuen *Scribe: Zoe Himwich*

1 Overview

In this lecture, we discussed at length an example of a classical commitment scheme and its quantum analogue. The key concepts from this lecture are

1. the definition of commitment schemes
2. the computational hiding property
3. the binding property
4. the role of PRGs and PRSs in (1-3)

This lecture builds directly on Lecture 9 by giving us an important use case for the pseudorandom maps we defined there.

2 Definitions, Setup

We ended the first part of the lecture by going through the classical construction of commitment schemes with pseudorandom generators. We will quickly recap this discussion before starting the notes for the second part. In order to be self contained, we make the following definitions, which will be relevant to the rest of the lecture.

Definition 1. *(Classical PRG) A map $G : \{0,1\}^n \to \{0,1\}^m$ for $m > n$ is a pseudorandom generator (PRG) if it is computable in polynomial time and if, for all polynomial time distinguishers D,*

$$\left|\mathbb{P}(D(G(k)) = 1) - \mathbb{P}(D(y) = 1)\right| \leq \textit{negligible}(n).$$

Where negligible(n) is a function which goes to 0 faster than any polynomial, k is a n-bit string picked uniformly at random, and y is an m-bit string picked uniformly at random.

Definition 2. *(PRS) A map $G : \{0,1\}^n \to \mathcal{S}((\mathbb{C}^2)^{\otimes m})$ is a pseudorandom state generator if it can be computed in polynomial time, and for all $t = \textit{poly}(n)$ and all polynomial time distinguishers, D,*

$$\left|\mathbb{P}(D(|\psi_k\rangle^{\otimes t}) = 1) - \mathbb{P}(D(|\theta\rangle^{\otimes t}) = 1)\right| \leq \textit{negligible}(n).$$

Where $G(k) = |\psi_k\rangle$ for k sampled uniformly at random from $\{0,1\}^n$ and where $|\theta\rangle$ is a Haar random state of size m.

Definition 3. *(Commitment Scheme) A commitment scheme is a two-phase cyptographic protocol, that is, a pair of algorithms, C and R which describe a commit phase (C) and a reveal phase (R). In the commit phase, one party commits to a bit $b \in \{0,1\}$. They then randomly pick a key k and use this k and the committed bit b to encode a message r. Finally, they transmit the encoded message $C(b,k,r)$ to the other party. In the reveal phase, the other party also receives b and k and applies the other algorithm, R, to determine whether the bit b was used to encode the message. The output of R is either pass or fail, depending on whether b could have been used to encode the message. The algorithms C and R must satisfy a few properties:*

1. *Computational Hiding — For all messages r and keys k, $C(0,k,r)$ and $C(1,k,r')$ must be indistinguishable from the point of view of any polynomial time distinguishers D*

$$\left|\mathbb{P}(D(C(0,k,r))=1) - \mathbb{P}(D(C(1,k,r))=1)\right| \leq \textit{negligible}(n).$$

2. *Binding — For all messages r and any two keys k,k', it is not possible to adversarially chose k and k' such that the receiver could be convinced with high probability that both choices of b pass*

$$\mathbb{P}(R(0,k,r,C(b,k,r)) = \textit{pass}) + \mathbb{P}(R(1,k',r,C(b,k',r)) = \textit{pass}) \leq 1 - \textit{exp. small error.}$$

Now we display the classical commitment scheme from earlier in the lecture. This construction sets $m = 3n$. We are required to chose m to be reasonably large in order for our commitment scheme to satisfy binding. This requirement will become apparent in the argument.

Commit	**Reveal**
HONEST ALICE commits to bit $b \in \{0,1\}$	HONEST ALICE sends k and b to HONEST BOB
HONEST BOB samples a uniformly random string r of length $3n$ sends it to HONEST ALICE	HONEST BOB $\xleftarrow{k,b}$ HONEST ALICE
HONEST BOB $\xrightarrow{r}$ HONEST ALICE	HONEST BOB checks: if $b=0$, is $c = G(k)$? and, if $b=1$, is $c = G(k) \oplus r$?
HONEST ALICE picks a random key k of length n for G. She evaluates $G(k)$, and sets commitment c to $G(k) \oplus (b \cdot r)$	If both of these checks pass, HONEST BOB believes b is the correct commitment (pass)
HONEST BOB $\xleftarrow{c}$ HONEST ALICE	Otherwise, he outputs an error (fail)

3 Lecture 10 — Part 2

We want to show that our commitment scheme satisfies each of the required properties.

Claim 4. *The commitment scheme above (2) satisfies computational hiding (1).*

Proof. We consider the case in which Alice is honest, and Bob cheats. CHEATING BOB may have picked a string in an adversarial way, so r may not be random. HONEST ALICE performs all of her steps as usual, and transmits c to CHEATING BOB. At this stage, CHEATING BOB still does not know what b is, because he does not know k. He knows he is seeing $G(k)$ for some k which he does not know, or $G(k) \oplus r$. Both $G(k)$ and $G(k) \oplus r$ look like uniformly randomly selected strings of size m to CHEATING BOB, because they pass through the pseudorandom generator, G. □

Claim 5. *The commitment scheme above (2) satisfies binding (2).*

Proof. Now we consider the case where Bob is honest and Alice cheats. We fix c and, similarly, fix r, assuming it was generated uniformly at random. We will use (k_b, b) to denote CHEATING ALICE's message in the reveal phase. We want to evaluate the probability that CHEATING ALICE can convince HONEST BOB to believe the b she transmits. We denote by E_b the event in which HONEST BOB believes b,

$$\begin{aligned}\mathbb{P}(E_0) &= \mathbb{P}(c = G(k_0)),\\ \mathbb{P}(E_1) &= \mathbb{P}(c = G(k_1) \oplus r).\end{aligned}$$

In the last equation, $\oplus$ is used to denote XOR. Therefore, CHEATING ALICE's total probability of success is

$$\begin{aligned}\mathbb{P}(E_0) + \mathbb{P}(E_1) &= \mathbb{P}(E_0) + \mathbb{P}(E_1|E_0)\mathbb{P}(E_0) + \mathbb{P}(E_1|\neg E_0)\mathbb{P}(\neg E_0)\\ &\leq \mathbb{P}(E_0) + \mathbb{P}(\neg E_0) + \mathbb{P}(E_1|E_0)\\ &= 1 + \mathbb{P}(E_1|E_0).\end{aligned}$$

We can further analyze the $\mathbb{P}(E_1|E_0)$ term. This probability conditions on $c = G(k_0)$ and requires $c = G(k_1) \oplus r$. Therefore, we can rewrite this term as

$$\mathbb{P}(E_1|E_0) = \mathbb{P}(G(k_0) \oplus G(k_1) = r).$$

We consider the possible outcomes of $G(k_0) \oplus G(k_1)$. There are at most 2^{2n} possible inputs to this expression. Consequently, there are at most 2^{2n} possible strings of the form $G(k_0) \oplus G(k_1)$. Since r has length $3n$, our final expression must include a multiplicative factor which gives the probability that a randomly selected $3n$-bit string will a set of size 2^{2n}. This probability is $2^{2n}/2^{3n} = 2^{-n}$.

The last calculation is where our choice of $m = 3n$ was necessary. We could also have picked m to be something larger.

Finally, we find $\mathbb{P}(E_1|E_0) \leq 2^{-n}$. Thus, we have the bound $\mathbb{P}(E_0)+\mathbb{P}(E_1) \leq 1-$exp. small error. □

3.1 Quantum analogue of the commitment scheme

We define a new commitment scheme, described below. Instead of using a pseudorandom generator (PRG), we use a pseudorandom state generator (PRS) (2) (which we also denote by G).

Commit	**Reveal**
HONEST ALICE commits to bit $b \in \{0,1\}$	HONEST ALICE sends b and k to HONEST BOB
HONEST BOB randomly samples two strings, $u, v \in \{0,1\}^n$, and sends them to HONEST ALICE	HONEST BOB $\xleftarrow{b,k}$ HONEST ALICE
HONEST BOB $\xrightarrow{u,v}$ HONEST ALICE	If $b = 0$, HONEST BOB checks $\|\psi\rangle = G(k)$ If $b = 1$, HONEST BOB checks $\|\psi\rangle = XZG(k)$
HONEST ALICE randomly samples $k \in \{0,1\}^n$ If $b = 0$, she computes $c = G(k) = \|\psi\rangle$ If $b = 1$ she computes $c = X^u Z^v G(k) = \|\psi\rangle$	If these checks pass, HONEST BOB believes b is the correct commitment (pass)
HONEST BOB $\xleftarrow{c}$ HONEST ALICE	Otherwise, he outputs an error (fail)

In the commitment scheme above $m = 5n$. This is required for the same reason that $3n$ was required in the classical case (it will be necessary to show that our commitment scheme satisfies binding). We also made use of the Pauli matrices X and Z. To understand their role in the commitment scheme, we will discuss the Pauli matrices and their properties in greater detail.

3.2 Pauli matrix interlude

The Pauli matrices X and Z are 2×2 matrices which act on qubits. The following equations are definitions as 2×2 matrices and a description of how X and Z act on $|0\rangle$ and $|1\rangle$.

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad X|0\rangle = |1\rangle, \qquad X|1\rangle = |0\rangle,$$
$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Z|0\rangle = Z|0\rangle, \qquad Z|1\rangle = -|1\rangle.$$

We randomly select two bits, $u, v \in \{0,1\}$, and let $|\psi\rangle$ be an arbitrary state. Consider the result of applying $X^u Z^v |\psi\rangle$. It is a probabilistic mixture of states,

$$2^{-2} \sum_{u,v} X^u Z^v |\psi\rangle\langle\psi| Z^v X^u = 2^{-1}\mathbf{1}.$$

In other words, this application of the product of Pauli matrices above completely scrambles the original state.

Now we extend this for $u, v \in \{0,1\}^m$ and $|\psi\rangle$ an m-qubit.

$$X^u Z^v |\psi\rangle := (X^{u_1} Z^{v_1}) \otimes \cdots \otimes (X^{u_m} Z^{v_m}) |\psi\rangle.$$

If we choose $u, v \in \{0,1\}^m$ randomly and average over all possible choices this will also result in a completely scrambled state.

$$4^{-m} \sum_{u,v} X^u Z^v |\psi\rangle\langle\psi| Z^v X^u = 2^{-m}\mathbf{1}, \tag{1}$$

(in fact, (1) was the bonus result on the first homework).

The following lemma shows an important property of the Pauli matrices.

Lemma 6. *If $|\alpha\rangle$, $|\beta\rangle$ are m-qubit states and*

$$H_{u,v} := |\langle\alpha|X^u Z^v|\beta\rangle|^2,$$

then

$$\mathbb{P}_{u,v}(H_{u,v} > 2^{-m/2}) \leq 2^{-m/2}.$$

This lemma essentially measures the size of the overlap between $|\alpha\rangle$ and $X^u Z^v|\beta\rangle$. The lemma says that even if $|\alpha\rangle$ and $|\beta\rangle$ start out as the same state, applying X^u and Z^v will cause the probability of reasonably sized overlap to be extremely small. We can interpret this to mean that $|\alpha\rangle$ and $X^u Z^v|\beta\rangle$ are close to orthogonal with high probability. Before proving this lemma, we state Markov's inequality.

Theorem 7. *(Markov) For a non-negative random variable X,*

$$\mathbb{P}(X > \delta) \leq \frac{\mathbb{E}(X)}{\delta}.$$

Proof. (of Lemma 6) We rewrite

$$H_{u,v} = \langle\alpha|X^u Z^v|\beta\rangle\langle\beta|Z^v X^u|\alpha\rangle.$$

We can take the expectation

$$\mathbb{E}_{u,v}(H_{u,v}) = \langle\alpha|\mathbb{E}\left(X^u Z^v|\beta\rangle\langle\beta|Z^v X^u\right)|\alpha\rangle = \langle\alpha|\frac{1}{2^m}\mathbf{1}|\alpha\rangle = \frac{1}{2^m}.$$

Applying Markov's inequality finishes the argument:

$$\mathbb{P}(H_{u,v} > 2^{-m/2}) \leq 2^{m/2}/2^m = 2^{-m/2}.$$

□

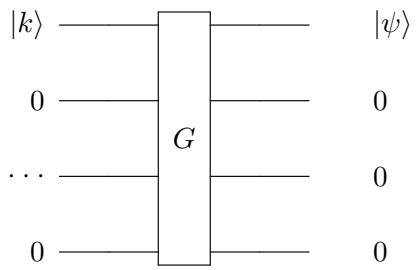
3.3 Hiding and binding for the quantum algorithm

We prove the same properties for the quantum algorithm.

Claim 8. *The quantum commitment scheme above (3.1) satisfies computational hiding (1).*

Proof. When $b = 0$, HONEST BOB sees $G(k)$, which is a state generated by a pseudorandom state generator, and when $b = 1$, HONEST BOB sees $X^u Z^v|\psi\rangle$. Since $G(k)$ is given by a pseudorandom state generator, this state is Haar random. Similarly, since $X^u Z^v|\psi\rangle$ is unitarily invariant, we can also conclude that it is Haar random. □

The reveal phase of the commitment scheme requires HONEST BOB to check whether something is equal to $|\psi\rangle$. This motivates the question:



Question 9. *What does it mean to check whether a state is equal to $G(k)$ in the quantum setting?*

One possible answer is that we can run a quantum circuit on $|\psi\rangle$ which accepts with probability $|\langle\psi|G(k)\rangle|^2$. An example of one circuit which performs this task appears below. It depicts the circuit associated to the map G (as a black-box). If we are given a state $|\phi\rangle$, we can run the circuit in reverse and check whether we get k followed by zeros. The probability that this operation succeeds is exactly the overlap $|\langle\phi|G(k)\rangle|^2$, as we can see because $|\langle k|\langle 0\cdots 0|G^{-1}|\phi\rangle|0\cdot\cdot\rangle|^2 = |\langle\psi|\phi\rangle|^2$.

Claim 10. *The quantum commitment scheme above (3.1) satisfies binding (2).*

Proof. (A sketch) We are in the situation where Alice cheats and Bob is honest. CHEATING ALICE tries to convince HONEST BOB she commited to a particular bit $b \in \{0,1\}$. The probability that HONEST BOB believes that HONEST ALICE made commitment b is given by

$$\mathbb{P}(E_0) = |\langle\psi|\psi_{k_0}\rangle|^2$$
$$\mathbb{P}(E_1) = |\langle\psi|X^u Z^v|\psi_{k_1}\rangle|^2$$

In this notation k_1 is the revealed key that CHEATING ALICE uses when she tries to convince him the commitment was $b = 1$, and similarly for k_0 and $b = 0$. Likewise, $|\psi_{k_b}\rangle$ is the state that CHEATING ALICE sends to convince him she commited to b. E_0 and E_1 are the events, respectively, that HONEST BOB is convinced of $b = 0$ and $b = 1$. We want to evaluate whether

$$\mathbb{P}(E_0) + \mathbb{P}(E_1) = \mathbb{E}_{u,v}\left(\mathbb{E}_{|\psi\rangle,k_0,k_1}\left(|\langle\psi|\psi_{k_0}\rangle|^2 + |\langle\psi|X^u Z^v|\psi_{k_1}\rangle|^2\right)\right)$$

is bounded above by $1 +$ exp. small error.

The following is a sketch of the proof: We consider the case when $|\psi_{k_0}\rangle$ and $X^u Z^v|\psi_{k_1}\rangle$ are orthogonal. In that case, the expectation in our equation is simply 1. Using our previous lemma (6), we know that the states are nearly orthogonal with high probability. Specifically, the probability that there exist k_0 and k_1 such that these states are **not** nearly orthogonal is

$$\mathbb{P}_{u,v}\left(\exists k_0, k_1 || \psi_{k_0}\rangle, X^u Z^v|\psi_{k_1}\rangle \text{ not orthogonal}\right) \leq 2^{2n}2^{-m/2}.$$

When $|\psi_{k_0}\rangle$ and $X^u Z^v|\psi_{k_1}\rangle$ are nearly orthogonal we can bound the expectation term in our expansion of $\mathbb{P}(E_0) + \mathbb{P}(E_1)$ by 1 and something exponentially small. We won't calculate this explicitly right now, but will assume we can use $1 + 2^{-m/2}$. In that case

$$\mathbb{P}(E_0) + \mathbb{P}(E_1) \leq 1 + 2^{-m/2} + 2^{2n}2^{-m/2} = 1 + O(2^{2n}2^{-m/2}) = 1 + O(2^{-n/2})$$

The last step required that we chose a large enough m so that the final term is small enough. □