COS 597A: Quantum Cryptography
Lecture 13 (November, 2018)
Lecturer: Mark Zhandry

Princeton University

Scribe: Kevin Liu

Notes for Lecture 13

We have already seen some difficulties of building or proving cryptography when we switch to quantum world. They are not only about Shor's algorithm but also include how to make proofs work. Last time we have seen one example, random oracle model. This time let us look at rewinding because it is related to no-cloning theorem.

The first example is commitment scheme. In a commitment scheme, there are two parties sender $\mathcal{S}$ and receiver $\mathcal{R}$. The sender $\mathcal{S}$ first sends a commitment $\mathsf{Com}(m)$ for a single bit message m which is called a commit phase. And later the sender $\mathcal{S}$ will send the message m and some other information about the message to reveal the message m. Let us be more precise: there are two algorithms, the first one is $\mathsf{Com}(m;r)$ which takes a message m and randomness r where the randomness prevents an adversary from learning whether m is 0 or 1 by comparing the pre-calculated commitment. The second algorithm is to open the commitment. And we need the following security properties:

1. **Hiding**: If the receiver $\mathcal{R}$ is in the commitment phase, it learns nothing about the message m. That is
$$\mathsf{Com}(0;r) \approx \mathsf{Com}(1;r)$$
We can define perfect/statistical/computational indistinguishable with respect to $\equiv, \approx_c$ or $\approx_s$.

2. **Binding**: We want the sender $\mathcal{S}$ can not later open the commitment to anything they want. We need to be careful here because the sender can come up with a fake commitment that is neither 0 or 1 but can be opened as both 0 or 1. We want a stronger guarantee to get rid of this possibility.

Here we have an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. $\mathcal{A}$ sends c to $\mathcal{C}$ where c can be a commitment of either 0 or 1 or even a fake commitment. $\mathcal{C}$ then sends a random b. And finally $\mathcal{A}$ sends r to $\mathcal{C}$. The adversary wins if and only if $\mathsf{Com}(b;r) = c$. We say it is (t,ϵ)-binding if the probability of $\mathcal{A}$ winning is at most $1/2 + \epsilon$ for all $\mathcal{A}$ running in time $\leq t$.

The definition of binding turns out to have a simpler definition in the classical setting. Let $P_{b'} = \Pr[\mathcal{A}$ wins if the bit $b = b']$ and we know the overall probability is $(P_0 + P_1)/2$. If we have an adversary wins, we know that $(P_0 + P_1) \geq 1 + 2\epsilon$. And because P_0, P_1 are at most 1, we know that $P_0 \geq 2\epsilon$ and $P_1 \geq 2\epsilon$.

So equivalently, we can come up with $\mathcal{A}'$ such that it generates r_0, r_1, such that $\mathsf{Com}(0; r_0) = \mathsf{Com}(1; r_1)$. It gives another (t, ϵ')-binding definition:

$$\Pr[\mathsf{Com}(0; r_0) = \mathsf{Com}(1; r_1); r_0, r_1 \leftarrow \mathcal{A}'] \leq \epsilon'$$

for all $\mathcal{A}'$ running in time $\leq t$.

The later definition is the widely used definition because what $\mathcal{A}'$ does is to find a 'collision'. So it means that $\mathsf{Com}(\cdot, \cdot)$ should be somehow 'collision resistant'. This is a necessary condition but is not sufficient because it does not give you hiding (maybe reveal the first bit of the message).

One construction is let H be a collision resistant function, h be a pairwise independent expanding function, and $\mathsf{Com}(b; r) = H(h(b, r))$. It is statistical hiding and computational binding in the classical setting.

Now we switch to quantum. One key difference is that for opening the commitment, it could incur a measurement. Which means we could destroy the state. (If we can clone a superposition, it can be easily solved by cloning c into two copies.) But we know very little about it.

We are going to define something a little bit stronger, we can prove the binding property of the construction.

Definition 1 (Collapsing Hash Function)**.** *(classical algorithms but quantum attacks), We say H is a collapsing hash function if the following game succeeds with probability $1/2 + \epsilon$,*

- *Adversary $\mathcal{A}$ comes up with $|\psi\rangle = \sum_x \alpha_x |x\rangle$ which is a superposition of inputs of the hash function,*
- *$\mathcal{C}$ chooses b in $\{0, 1\}$, if $b = 0$, it measures $|\psi\rangle$ and gets $|x\rangle$. If $b = 1$, it evaluates H in superposition and gets $\sum_x \alpha_x |x, H(x)\rangle$ and measures the output register $(H(x) = y)$.*

  The state collapses to $\sum_{x, H(x)=y} \alpha_x |x\rangle$. As long as H is compressing, this two experiment gives different results.
- *A guesses b', which one is given.*

We say H is (t, ϵ)-collapsing if $\Pr[b = b'] \leq 1/2 + \epsilon$.

Observation: collapsing ⇒ collision resistance.

Proof. If we have an $\mathcal{A}$ that produce x_0, x_1 such that $H(x_0) = H(x_1)$ and $x_0 \neq x_1$. The attack is really simple, just let $|\psi\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)$.

In the case where $b = 0$, the challenger gives random one of these $|x_0\rangle$ or $|x_1\rangle$. In the case where $b = 1$, the challenger gives $|\psi\rangle$. By measuring it under $P_0 = |\psi\rangle\langle\psi|$ and $P_1 = I - P_0$, (another view of look at it by doing QFT on each bit). It gives you probability 3/4 to succeeds. □

Collapsing turns out to be the right definition of hash function in the quantum setting. First it implies collision resistant in the classical setting. And it also turns out to be the right property to let commitment scheme works in the quantum setting.

Now let us look at the construction of collapsing hash functions. It requires the following building blocks:

- h is treated as a random oracle,
- Use lossy and pairwise independent function f,
- The function is defined as $h \circ f$.

Lossy (Trapdoor) Function (where trapdoor is not necessary for this application):

Definition 2. *there is an* Gen *procedure, takes a bit* b *and outputs a function* $f : \{0,1\}^n \to \{0,1\}^m$ *where* $m \geq n$*,*

- *if* $b = 0$*,* f *is injective,*
- *if* $b = 1$*,* f *is lossy which means* $|\{f(x)|\forall x\}| \ll$ *domain size.*

Security: this two modes (two function descriptions) are indistinguishable.

Assume we have a lossy function, let us prove the construction actually gives us collapsing hash functions:

Proof. In the collapsing game, we either measure at the beginning or at the end.

- **Hyb 0**: measure at the beginning on $\sum_x \alpha_x |x\rangle$ (before applying $h \circ f$,
- **Hyb 1**: measure at the middle (after applying f but before applying h). **Hyb 0** and **Hyb 1** are statistically identical because $f = \mathsf{Gen}(0)$ which is injective.
- **Hyb 2**: replace f with $\mathsf{Gen}(1)$. It comes from the security of lossy function.
- **Hyb 3**: f is now lossy but measure at the end. The point is that when f is lossy, the domain $y = h(x)$ comes from is really small. The range of h is significantly larger than the number of image points in lossy f. Once we have done this, h is injective on $f(x)$ with high probability.

- **Hyb 4**: replace f with $\mathsf{Gen}(0)$.

□

Finally, how to build lossy functions? Let $\mathsf{Gen}(0) = A \in Z_q^{mn}$, a very tall matrix. The input x is a zero-one vector $\{0,1\}^n$. And $f_A(x)$ here is $A \cdot x \bmod q$, and take each entry rounded to $q/2$. In other words, it is rounded to 0 if it is closer to 0; it is rounded to 1 if it is closer to $q/2$. We can show that if $n \ll m$, it is injective.

$\mathsf{Gen}(1) = B \cdot C + E$ where $B \in Z_q^{m \cdot r}$, $C \in Z_q^{r \cdot n}$ and $E \in Z_q^{m \cdot n}$ is short where $r \ll n$. This approximately has rank r, which is a low rank matrix. In this case, the matrix is lossy:

$$[A \cdot x] = [(B \cdot C)x + E \cdot x] \approx [B \cdot C \cdot x] \,\text{(because } E \text{ is short)}$$

The number of possible outputs is bounded by the number of possible outputs of $C \cdot x$. It has at most $r \log q$ entropy.

Finally, the indistinguishability is similar to the security of LWE.