1 Luby-Rackoff Contruction

From last lecture:
\[ \mathcal{G} = \{G_k\}_k = \{(g_{f_4} \circ g_{f_3} \circ g_{f_2} \circ g_{f_1})|f_4, f_3, f_2, f_1 \leftarrow F_k\}. \]
Where \( g_f(x, y) = y|x \oplus f(y) \)

**Theorem 1** If \( F_k \) is pseudorandom, \( G \) is strongly pseudorandom.

**Proof:**

**Definition 2** \( \mathcal{R} = \{R_k\}_k \) where \( R_k = \{(u_{4,1} \circ u_{3,1} \circ u_{2,1} \circ u_{1,1})|u_{4,1}, u_{3,1}, u_{2,1}, u_{1,1} \leftarrow U_k\} \)

Our proof is composed of two parts:

1) \( (G, G^{-1}) \cong (R, R^{-1}) \) (This was proved last lecture using a hybrid argument)

2) \( (R, R^{-1}) \cong (\Pi, \Pi^{-1}) \) will be subsequently proven:

Let D be any PPT distinguisher. Without loss of generality, assume D is non-repeating, since any repeating distinguisher can be wrapped with a cache that responds to repeat queries. Its distinguishing probability is:

\[ |Pr[D_{R_k,R^{-1}_k}(1^k) = 1] - Pr[D^{\Pi_k,\Pi^{-1}_k}(1^k) = 1]| \]

By the triangle inequality,

\[ \leq |Pr[D_{R_k,R^{-1}_k}(1^k) = 1] - Pr[D^{\delta}(1^k) = 1]| + |Pr[D^{\delta}(1^k) = 1] - Pr[D^{\Pi_k,\Pi^{-1}_k}(1^k) = 1]| \]

where \( \delta \) is the random distribution.

The latter term: \( |Pr[D^{\delta}(1^k) = 1] - Pr[D^{\Pi_k,\Pi^{-1}_k}(1^k) = 1]| \leq \frac{\text{time}(D)^2}{2^k} \) which is negligible. This was not proven in lecture, but the intuition for this argument was built last lecture. Thus we will only concern ourselves with the first term.

**Definition 3** A transcript \( \tau \) of D is a representation of all of the queries D makes, and can be represented as \( ((x_1, y_1, b_1), ..., (x_q, y_q, b_q)) \) such that if \( b_i = 0, R_k \) was queried at \( x_i \) and received \( y_i \), and if \( b_i = 1, R_k^{-1} \) was queried at \( y_i \) and received \( x_i \). The transcript of \( D_{R_k,R^{-1}_k}(1^k) \) is symbolized as \( tr(D_{R_k,R^{-1}_k}(1^k)) \)
Definition 4 T is set of all transcripts $\tau$ such that $D$ seeing $\tau$ outputs 1. Note: here we are fixing all of $D$’s coinflips to have the best possible distinguishing probability.

Definition 5 Let $T'$ be set of all transcripts $\tau$ such that $D$ seeing $\tau$ outputs 1, and $\tau$ is consistent with the oracle being a permutation.

Then

$$|Pr[D^{R_k,R_k^{-1}}(1^k) = 1] - Pr[D^S(1^k) = 1]|$$

$$= |\sum_{\tau \in T} Pr[D^{R_k,R_k^{-1}}(1^k) = 1]tr(D^{R_k,R_k^{-1}}) = \tau] - Pr[D^S = 1]tr(D^S) = \tau]Pr[tr(D^S) = \tau]|$$

$$= |\sum_{\tau \in T} Pr[tr(D^{R_k,R_k^{-1}}) = \tau] - Pr[tr(D^S) = \tau]|$$

$$\leq |\sum_{\tau \in T} Pr[tr(D^{R_k,R_k^{-1}}) = \tau] - Pr[tr(D^S) = \tau]| + |\sum_{\tau \notin T} Pr[tr(D^{R_k,R_k^{-1}}) = \tau] - Pr[tr(D^S) = \tau]|$$

by the triangle inequality. The latter term is negligible since a negligible fraction of $\tau \in T$ are $\notin T'$. This wasn’t proven in lecture.

Definition 6 $x_i = (L_i^0, R_i^0) \rightarrow (L_i^1, R_i^1) \rightarrow (L_i^2, R_i^2) \rightarrow (L_i^3, R_i^3) \rightarrow (L_i^4, R_i^4) = y_i$

Definition 7 $u_1$ is good for $\tau$ if $R_1^1, ..., R_q^1$ has no repetitions.

Definition 8 $u_4$ is good for $\tau$ if $L_1^3, ..., L_q^3$ has no repetitions.

Lemma 9 $Pr_{u_1,u_4}|u_1$ or $u_4$ is not good for $\tau| \leq \frac{q^2}{2^r} \forall \tau \in T'$

Proof: We need to show that $Pr[R_i^1 = R_j^1] \leq \frac{1}{2^r} \forall i \neq j$ and $Pr[L_i^3 = L_j^3] \leq \frac{1}{2^r} \forall i \neq j$. We will only prove the former; the latter follows from the same argument.

$(R_i^1 = R_j^1) \rightarrow L_i^0 \oplus U_1(R_i^0) = L_j^0 \oplus U_1(R_j^0)$. Our initial assumption that $D$ is non-repeating affirms that $(L_i^0, R_i^0) \neq (L_j^0, R_j^0)$. Since $(R_i^0 = R_j^0) \rightarrow (L_i^0 = L_j^0)$, $R_i^0 \neq R_j^0$. Thus, since $U$ is a random function, $Pr[L_0^i \oplus U_1(R_i^0) = L_0^j \oplus U_1(R_j^0)] \leq \frac{1}{2^r}$ The rest of the argument follows similarly. \(\square\)

Lemma 10 $Pr_{u_2,u_3}|tr(D^{R_k,R_k^{-1}}) = \tau] = Pr[tr(D^S) = \tau] \forall \tau, \text{ good } u_1, u_4$

Proof: For each i,

$$L_i^3 = R_i^2 = L_i^1 \oplus u_2(R_i^1)$$

$$R_i^3 = L_i^2 \oplus u_3(R_i^2) = R_i^1 \oplus u_3(L_i^3)$$

So

$$u_2(R_i^1) = L_i^1 \oplus L_i^3$$

7-2
Thus, since $u_1$ and $u_4$ are good,

$$Pr_{u_2,u_3}[tr(D^{R_k,R_{k-1}}) = \tau] = \frac{1}{2^{2qk}} = Pr[tr(D^\delta) = \tau]$$

So the initial expression that we’ve summed over, $Pr[tr(D^{R_k,R_{k-1}}) = \tau] - Pr[tr(D^\delta) = \tau]$

$= Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1, u_4 \text{ are good}]Pr[u_1, u_4 \text{ are good}] + Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1 \text{ or } u_4 \text{ is not good}]Pr[u_1 \text{ or } u_4 \text{ is not good}] - Pr[tr(D^\delta) = \tau]$

$= Pr[u_1 \text{ or } u_4 \text{ is not good for } \tau]|(-Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1, u_4 \text{ are good}] + Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1 \text{ or } u_4 \text{ is not good}])$

Thus, the summed expression, $|\sum_{\tau \in T'} Pr[tr(D^{R_k,R_{k-1}}) = \tau] - Pr[tr(D^\delta) = \tau]|$, by lemma 9, is

$= \frac{q^2}{2\pi^2} |\sum_{\tau} Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1 \text{ or } u_4 \text{ is not good}] - Pr[tr(D^{R_k,R_{k-1}}) = \tau|u_1, u_4 \text{ are good}]|$

which by lemma 10 is

$\leq \frac{q^2}{2\pi^2}r$, which is negligible in $k$.

\[\square\]

\section{Commitment Schemes}

\textbf{Definition 11} A commitment scheme is a two-phase protocol between a sender and a receiver.

1) In the commitment phase, the sender commits to a message $m$ to produce commitment $c$.

2) In the reveal phase, the sender reveals the message $m$ in the commitment $c$.

There are two properties of a commitment scheme: hiding and binding. Conceptually, hiding requires a commitment to $m$ to leak nothing about $m$, and binding requires a commitment to not be openable in two ways. Hiding and binding can each be done statistically or computationally.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
 & Statistical Hiding & Computational Hiding \\
\hline
Statistical Binding & Impossible & Possible using one-way permutations as we will see later \\
\hline
Computational Binding & Pedersen Commitment Scheme & Possible \\
\hline
\end{tabular}
\end{table}

\textbf{Definition 12} A computationally hiding statistically binding commitment scheme is a pair of PPT algorithms (Commit($C$), Reveal($R$)) satisfying the followin:

1) Completeness: $\forall k, \forall m \in \{0, 1\}^{(k)}, \forall s \in \{0, 1\}^{r(k)}, R(1^k, s, C(1^k, s, m)) = m$

2) Hiding: $\forall\{m_k^{(1)}\}, \{m_k^{(2)}\}$ such that $|m_k^{(1)}| = |m_k^{(2)}|, \{C(1^k, u_{r(k)}, m_k^{(1)})\} \equiv \{C(1^k, u_{r(k)}, m_k^{(2)})\}$
3) Binding: \( \forall k, \forall s, s' \in \{0,1\}^{n(k)}, \forall m \in \{0,1\}^{l(k)}, R(1^k, s', C(1^k, s, m)) \in \{m, \bot\} \)

**Theorem 13** If One Way Permutations Exist, there exists a computationally hiding, statistically binding encryption scheme with \( l(k) = 1 \)

**Proof:** Let \( f_k \) be a one way permutation mapping \( \{0,1\}^{n(k)} \) to \( \{0,1\}^{n(k)} \)

Let \( b_k \) be a hardcore bit on \( f_k \)

Let \( C(1^k, s, m) = f_k(s), b_k(s) \oplus m \)

Let \( R(1^k, s, (c_1, c_2)) := \)

\[
\begin{align*}
&\quad \text{if } f_k(s) \neq c_1 \rightarrow \bot \\
&\quad \text{else } \rightarrow c_2 \oplus b_k(s)
\end{align*}
\]

**Claim 14** \((C, R)\) is a computationally hiding statistically binding commitment scheme.

**Proof:** \( \forall c_1, c_2, \exists s, m \) such that \( C(1^k, s, m) = c_1, c_2 \) since \( s := f_k^{-1}(c_1), m := b_k(f_k^{-1}(c_1)) \oplus c_2 \).

Thus \((C, R)\) is statistically binding.

We didn’t finish the proof that the commitment scheme is computationally hiding. That will be covered next lecture.