In HW5, out HW6
* hybrid argument
* El Gamal
* PRG

Lecture 9

* From last lecture: more than just dists b/c

A can interact

Let $D^A(k)$, $E^A(k)$, $F^A(k)$ be experiments w/ challenger.
in which a challenger interacts w/ $A$, and
$A$ produces an output.

Let $Z_D^A(k)$, $Z_E^A(k)$, $Z_F^A(k)$ be the probabilities that
$A$ outputs zero in experiments $D^A(k)$, $E^A(k)$, and $F^A(k)$

Then, $|Z_D^A(k) - Z_F^A(k)| \leq |Z_D^A(k) - Z_E^A(k)| + |Z_E^A(k) - Z_F^A(k)|$

\[ \text{This is generally true, not just when } z\text{'s are bounded by a negl. function} \]

Pf of Lem 1: $|Z_D - Z_F| = |Z_D - Z_E + Z_E - Z_F|$

\[ \leq |Z_D - Z_E| + |Z_E - Z_F| \]

Cor 1

If $|Z_D - Z_E| = \mathcal{O}_1(k)$

$|Z_E - Z_F| = \mathcal{O}_2(k)$ \& both are negl.

then $|Z_D - Z_F| \leq \mathcal{O}_1(k) + \mathcal{O}_2(k)$, also negl.

Cor 2

To show that $D \approx F$,

it's sufficient to provide some exp $E$ s.t. $D \approx E$, and $E \approx F$. 
Proving security of ElGamal

We want to show: \( \text{Exp} 0(1^k) = \text{Exp} \frac{1}{2}(1^k) \), so we define \( \text{Exp} \frac{1}{2}(1^k) \)

\[ \text{Exp}_0 \]

\[ \text{Exp} \frac{1}{2} \]

\[ \text{Exp}_1 \]

\[
\begin{array}{c}
\text{Ch} \xrightarrow{\text{pk}} A \\
\text{Ch} \xleftarrow{m_0, m_1} A \\
\text{Ch} \xrightarrow{b'} A \\
\text{Ch} \xleftarrow{b'} A
\end{array}
\]

Recall: In ElGamal, \( \text{pk} = (G, g, q, y) \) s.t. \( y = g^x \)

\[ \text{Enc}(\text{pk}, m) = (g^x, y^r m) = (u, v) \]

DDH assumption says

\[ (G, g, g^a, g^b, g^c, g^{ab}) \neq (G, g, g^a, g^b, g^c, g^{ac}) \]

\[ \text{random} \]

\[ \text{Pf:} \quad \text{that} \ \text{Exp}_0 \ \text{is} \ \text{Exp} \frac{1}{2} \]

Let \( A \) be PPT algorithm that can distinguish \( \text{Exp}_0 \) from \( \text{Exp} \frac{1}{2} \).

Consider reduction \( B \):

\[ \begin{array}{c}
G, g, q, A, B, C \\
B \xrightarrow{\text{pk} = (\ldots, y^x A)} A \\
B \xleftarrow{m_0, m_1} A \\
B \xrightarrow{u = B, v = C m_0} A \\
B \xrightarrow{b'} A \\
B \xleftarrow{b'} A
\end{array} \]
Analysis: $Z_{DH}^\beta(k) = Z_{Exp}^\beta(k)$ bc

$(u,v) = (q^\beta, q^\alpha \beta \cdot m_0)$ same as in Exp o

$Z_{Rand}^\beta(k) = Z_{Exp \frac{1}{2}}^\beta(k)$ bc

$\nu = c \cdot m_0 = q^r \cdot q^m$

$= q^{r+m}$

$= q^5$

$\therefore |Z_o^A - Z_{\frac{1}{2}}^A| = |Z_{DH}^\beta - Z_{Rand}^\beta| = \text{negl. by DDH assumption} \square$

$\Rightarrow$ Pf of Exp $\frac{1}{2}$ $\approx$ Exp 1 is similar.

and so security of El Gamal follows from Cor 2.

\begin{itemize}
  \item \textbf{Lem 2} Let $A$ be the adversary.
  \item Let $k$ be the security parameter, $\& p(k)$ is a function.
  \item Let $E_{k,1}, \ldots, E_{k,p(k)}$ be a series of experiments in which a challenger interacts $w/ A$ and $A$ produces an output.
  \item $\forall i \in [p(k)]$, let $Z_E^A(k,i)$ be the probability that $A$ outputs zero in experiment $E_{k,i}(k,A)$.
  \item Then, $|Z_E^A(k,1) - Z_E^A(k,p(k))| \leq \sum_{i=1}^{p(k)-1} |Z_E^A(k,i) - Z_E^A(k,i+1)|$
\end{itemize}
Proof intuition

If the advantage for neighboring experiments is negligible, then end-to-end is also negligible.

**Proof of Lemma**

\[ |Z(1) - Z(p(k))| = \left| Z(1) - Z(2) + Z(3) - Z(4) + \cdots + Z(p(k) - 1) - Z(p(k)) \right| \leq \sum_{\lambda=1}^{p(k) - 1} |Z(\lambda) - Z(\lambda + 1)| \]

From HW1, summing a poly number of negligible functions is not guaranteeing us a negligible function.

For example, if \( Y_{\lambda}(k) = \begin{cases} \frac{1}{2} & \text{for } k \leq i \\ 2^{-k} & \text{otherwise} \end{cases} \) and \( Y(k) = \sum_{\lambda=1}^{p(k)} Y_{\lambda}(k) \)

\[ \text{BUT: If } \forall \lambda, \sum_{\lambda=1}^{p(k)} \sum_{\lambda=1}^{p(k)} Y_{\lambda}(k) \leq Y(k) \text{ for some negligible } Y \]

then, \[ \sum_{\lambda=1}^{p(k)} Y_{\lambda}(k) \leq \sum_{\lambda=1}^{p(k)} Y(k) = p(k) Y(k) = \text{negl.} \]
**Cor 3** If $E$ s.t. $|Z^A_E(k, i) - Z^A_E(k, i+1)| \leq \nu(k)$ then $|Z_1 - Z_{p(k)}| \leq \rho(k) \cdot \nu(k)$, also neg.

**Cor 4** If we wish to show that $D \& F$, it is sufficient to provide some experiments $E_1, \ldots, E_{p(k)}$ and show $D \& E_1 \approx E_2 \approx \ldots \approx E_{p(k)} \approx F$ for some negl function, i.e., $A$'s adv $\leq \nu(k)$ for some $\nu$.

**Def.** (Pseudorandom generator) An algorithm $G : \{0, 1\}^k \rightarrow \{0, 1\}^{p(k)}$ is a pseudorandom generator (PRG) if $G(s) \approx R$, a truly random $p(k)$-bit string.

**Blum–Micali PRG** Let $f$ be a OWP w/ hardcore bit $B$.

- **Input**: sample $s \leftarrow \{0, 1\}^k$
- $s_0 \xrightarrow{f} s_1 = f(s_0) \xrightarrow{f} s_2 = f(s_1) \xrightarrow{f} \ldots \xrightarrow{f} s_{k-1} \xrightarrow{f} s_k$
- $b_1 = B(s_0)$, $b_2 = B(s_1)$, $b_3 = B(s_2)$, $\ldots$, $b_k = B(s_{k-1})$

- **Output**: $s_k, b_1, \ldots, b_k$

**Pf.** HW6