Section 1

Commitment Schemes
Motivation

- Digital analogue of a safe
- Numerous applications (e.g., zero-knowledge, coin-flipping, secure computations)
Definition

\( \mu \) is negligible, denoted \( \mu(n) = \text{neg}(n) \), if \( \forall p \in \text{poly} \; \exists n' \in \mathbb{N} \; \text{s.t.} \; \mu(n) < \frac{1}{p(n)} \) forall \( n > n' \).

Definition 1 (Commitment scheme)

An efficient two-stage protocol \((S, R)\).

- **Commit stage:** The sender \( S \) has private input bit \( b \in \{0, 1\} \) and a common input is \( 1^n \). Let \( \text{trans} \) be the transcript of this stage.

- **Reveal stage:** \( S \) sends the pair \((r, b)\) to \( R \), and \( R \) accepts if \( \text{trans} \) is consistent with \( S(\sigma, r) \).

**Hiding:** Let \( V_{n}^{R*}(b) \) be \( R^* \)'s view in (the commit stage of) \((S(b), R^*)(1^n)\). Then for any \( R^* \): \( \Delta_{R^*}(V_{n}^{R*}(0), V_{n}^{R*}(1)) = \text{neg}(n) \).

**Binding:** The following happens with negligible probability for any \( S^* \):

\( S^*(1^n) \) interacts with \( R(1^n) \) in the commit stage resulting in transcript \( \text{trans} \). Then \( S^* \) outputs two strings \( r_0 \) and \( r_1 \) such that \( R(\text{trans}, r_0, 0) = R(\text{trans}, r_1, 1) = \text{Accept} \).

**Alternative Binding definition:** Assume that following the interaction \( S^* \) outputs a pair \((r, b)\) with \( R(\text{trans}, r, b) = \text{Accept} \). Let \( V_{S^*} \) be \( S^* \)'s view in (the commit stage of) \((S^*, R^*)(1^n)\). Then \( H(b | V_{S^*}) = \text{neg}(n) \).
Definition cont.

- Naturally extends to strings
- Hiding: Perfect, statistical, computational.
- Binding: Perfect, statistical, computational.
- Impossible to have simultaneously both properties to be statistical.
- OWF is necessary assumption

- OWFs imply both statistically binding and computationally hiding commitments, and (more difficult) computationally binding and statistically hiding commitments.

- We focus on computationally binding, and statistically hiding commitments (SHC)
Section 2

Inaccessible Entropy
Motivation

**Definition 2 (collision resistant hash family (CRH))**

Function family $\mathcal{H} = \{ \mathcal{H}_n : \{0, 1\}^n \mapsto \{0, 1\}^{n/2}\}$ is collision resistant, if $\forall$ PPT $A$

$$\Pr_{h \leftarrow \mathcal{H}_n} \left[ x \neq x' \in \{0, 1\}^* \land h(x) = h(x') \right] = \operatorname{neg}(n)$$

- Implies SHC. (?) Believed not to be implied by OWFs.
- Assume for simplicity that $h \in \mathcal{H}_n$ is $2^{n/2}$ to 1 and that a PPT cannot find a collision in any $h \in \mathcal{H}_n$
- Given $h(U_n)$, the (min) entropy of $U_n$ is $n/2$.
- Consider PPT $A$ that on input $h$ first outputs $h, y$, and then outputs $x \in h^{-1}(y)$ (possibly using additional random coins)
- What is the entropy of $x$ given $(h, y)$ and the coins $A$’s used to sample $y$? (essentially) 0!
- The generator $G(h, x) = (h, h(x), x)$ has inaccessible entropy $n/2$
- Does inaccessible entropy generator implies SHC?
- Does OWF implies inaccessible entropy generator?
Real entropy

- Sample entropy: for rv $X$ let $H_X(x) = -\log \Pr_X[x]$.
- $H(X) = \mathbb{E}_{x \leftarrow X}[H_X(x)]$
- For rvs $X$ and $Y$, let $H_{X|Y}(x|y) = H_{X|Y=y}(x)$.
- $X_1,\ldots,i$ stand for $X_1,\ldots,X_i$

- Let $G: \{0,1\}^n \rightarrow (\{0,1\}^{\ell(n)})^{m(n)}$ be an $m$-block generator
- Let $(G_1,\ldots,G_m) = G(U_n)$
- For $g = (g_1,\ldots,g_m) \in \text{Supp}(G_1,\ldots,G_m)$, let
  \[
  \text{RealH}_G(g) = \sum_{i \in [m]} H_{G_i|G_1,\ldots,G_{i-1}}(g_i|g_1,\ldots,g_{i-1})
  \]
- The real Shannon entropy of $G$, wrt security parameter $n$, is
  \[
  \mathbb{E}_{g \leftarrow G(U_n)}[\text{RealH}_{G,n}(g)]
  \]
- $\mathbb{E}_{g \leftarrow G(U_n)}[\text{RealH}_{G,n}(g)] = \sum_{i \in [m]} H(G_i|G_1,\ldots,G_{i-1}) = H(G(U_n))$
Accessible entropy

- Let $G$ be an $m$ block generator.
- Let $\tilde{G}$ be an $m$-block generator, that uses coins $r_i$ before outputting its $i$'th block $(w_i, g_i)$.
- $t = (r_1, w_1, g_1, \ldots, r_m, w_m, g_m)$ is valid with respect to $G$, and $n$, if $w_i \in \{0, 1\}^n$ and $(g_1, \ldots, g_i) = G(w_i)_{1,\ldots,i}$ for every $i \in [m]$.
- We assume for simplicity that $t$ is always valid, and omit $w$'s.
- $\tilde{T} = (\tilde{R}_1, \tilde{G}_1, \ldots, \tilde{R}_m, \tilde{G}_m)$— the rv's induced by random execution of $\tilde{G}(1^n)$
- \[
\text{AccH}_{\tilde{G},n}(t) = \sum_{i \in [m]} H_{\tilde{G}_i|\tilde{R}_1,\tilde{G}_1,\ldots,\tilde{R}_{i-1},\tilde{G}_{r-1}}(g_i|r_1, g_1, \ldots, r_{i-1}, g_{i-1})
\]
- The accessible entropy of $\tilde{G}$ (wrt $G$), and $n$, is at most $k$, if $\Pr_{t \leftarrow \tilde{T}} \left[ \text{AccH}_{\tilde{G},n}(t) > k \right] \leq \text{neg}(n)$. Why not $E_{t \leftarrow \tilde{T}} \left[ \text{AccH}_{\tilde{G},n}(t) \right]$?
- inaccessible entropy
- We will omit $n$ when clear from the context
Example

- Let $\mathcal{H} = \{\mathcal{H}_n : \{0, 1\}^n \mapsto \{0, 1\}^{n/2}\}$ be $2^{n/2}$-to-1 collision resistant, and assume for simplicity that a PPT cannot find a collision for any $h \in \mathcal{H}_n$.
- Let $G$ be the 3-block generator $G(h, x) = (h, h(x), x)$.
- Real entropy of $G$ is $\log |\mathcal{H}_n| + n$.
- Accessible entropy of $G$ is $\log |\mathcal{H}_n| + \frac{n}{2}$. 
Section 3

Manipulating Inaccessible Entropy
Entropy equalization

Let $G$ be $m$-bit generator.

For $\ell \in \text{poly}$ let $G^\otimes \ell$ be the following $(\ell - 1) \cdot m$-bit generator

$$G^\otimes \ell (x_1, \ldots, x_\ell, i) = G(x_1)_i, \ldots, G(x_1)_m, \ldots, G(x_\ell)_1, \ldots, G(x_\ell)_{i-1}$$

- Assume the accessible entropy of $G$ is (at most) $k_A$, then $k_A^\otimes \ell$, the accessible entropy of $G^\otimes \ell$, is at most $k(\ell - 2) + m$.

- Assume the real entropy of $G$ is $k_R$, then
  
  1. For any $i \in [(\ell - 1) \cdot m]$ and $(g_1, \ldots, g_{i-1}) \in \text{Supp}(G_1^\otimes \ell, \ldots, G_{i-1}^\otimes \ell)$:
     $$H(G_i^\otimes \ell \mid G_1^\otimes \ell, \ldots, G_{i-1}^\otimes \ell) \geq k_R / \ell$$
  2. $k_R^\otimes \ell$, the real entropy of $G^\otimes \ell$, is at least $(\ell - 1)K_R$

- Assume $k_R \geq k_A + 1$, then for $\ell = m + 2$, it holds that $k_R^\otimes \ell \geq k_A^\otimes \ell + 1$
Parallel repetition

Let $G$ be an $m$-block generator and for $\ell \in \text{poly}$, let $G^\ell$ be the $\ell$-fold parallel repetition of $G$.

- Assume accessible entropy of $G$ is (at most) $k_A$, then the accessible entropy of $G$ is at most $k_A^\ell = \ell k_A$.

- Assume $H(G_i|G_1,\ldots,G_{i-1}) = k_R$ for any $i \in [m]$, then for any $i \in [m]$ and $(g_1^\ell,\ldots,g_{i-1}^\ell) \in \text{Supp}(G_1^\ell,\ldots,G_{i-1}^\ell)$ it holds that

  $$k_{\min}^\ell = H_\infty(G_i^\ell|G_1^\ell,\ldots,G_{i-1}^\ell) \approx \ell k_R$$

- If $k_A \leq k_R - 1$, then $\forall n \in \text{poly}$ $\exists \ell \in \text{poly}$ such that $\ell k_{\min}^\ell > k_A^\ell + n$
Section 4

Inaccessible Entropy from OWF
The generator

**Definition 3**

Given a function \( f: \{0, 1\}^n \mapsto \{0, 1\}^n \), let \( G \) be the \((n + 1)\)-block generator

\[
G(x) = f(x)_1, \ldots, f(x)_n, x
\]

**Lemma 4**

Assume that \( f \) is a OWF then \( G \) has accessible entropy at most \( n - \log n \).

- Recall \( f \) is OWF if
  \[
  \Pr_{x \leftarrow \{0, 1\}^n} [\text{Inv}(f(x)) \in f^{-1}(f(x))] = \text{neg}(n) \text{ for any PPT Inv.}
  \]
- The real entropy of \( G \) is \( n \)
- Hence, inaccessible entropy gap is \( \log n \)

Proof idea
Proving Lemma 4

Let $\tilde{G}$ be a PPT, and assume $\Pr \left[ \text{AccH}_{G,\tilde{G}}(\tilde{T}) \geq n - \log n \right] \geq \varepsilon = \frac{1}{\text{poly}(n)}$.
(recall $\tilde{T} = (\tilde{R}_1, \tilde{G}_1, \ldots, \tilde{R}_m, \tilde{G}_m)$ is the coins and output blocks of $\tilde{G}$)

Algorithm 5 (Inv($z$))

1. For $i = 1$ to $n$, do the following for $n^2/\varepsilon$ times:
   1.1 Sample $r_i$ uniformly at random and let $g_i$ be the $i$'th output block of $\tilde{G}(r_1, \ldots, r_i)$.
   1.2 If $g_i = z_i$, move to next value of $i$.
   1.3 Abort, if the maximal number of attempts is reached.

2. Finish the execution of $\tilde{G}(r_1, \ldots, r_{n+1})$, and output its $(n+1)$ output block.

- We start by assuming that Inv is unbounded (replace $n^2/\varepsilon$ with $\infty$)
- $\hat{T} = (\hat{R}_1, \hat{G}_1, \ldots, \hat{R}_{n+1}, \hat{G}_{n+1})$ is the (final) values of $(r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ in a random execution of Inv($f(U_n)$).
\( \tilde{T} \) vs. \( \hat{T} \)

- Fix \( t = (r_1, g_1, \ldots, r_{n+1}, g_{n+1}) \in \text{Supp}(\tilde{T}) \)
- Let \( P(t) = \prod_{i=1}^{n+1} \Pr[\tilde{R}_i = r_i \mid (\tilde{R}_1, \ldots, i-1, \tilde{G}_i) = (r_1, \ldots, i-1, g_i)] \)

\[
\Pr[t] = \Pr[\tilde{G}_1 = g_1] \cdot \Pr[\tilde{R}_1 = r_1 \mid \tilde{G}_1 = g_1] \cdot \Pr[\tilde{G}_2 = g_2 \mid \tilde{R}_1 = r_1] \\
\quad \cdot \Pr[\tilde{R}_2 = r_2 \mid \tilde{G}_2 = g_2] \cdots \\
= P(t) \cdot \Pr[\tilde{G}_1 = g_1] \cdot \Pr[\tilde{G}_2 = g_2 \mid \tilde{R}_1 = r_1] \cdots \\
= P(t) \cdot 2^{- \sum_{i=1}^m H_{\tilde{G}_i \mid \tilde{R}_1, \ldots, i-1}(g_i \mid r_1, \ldots, i-1)} \\
= P(t) \cdot 2^{- \text{AccH}_{\tilde{G}}(t)}
\]

- \( \Pr[\hat{T}[t] = \Pr[f(U_n) = g_1, \ldots, n] \cdot \Pr[\tilde{G}_{n+1} = g_{n+1} \mid \tilde{R}_1, \ldots, n = r_1, \ldots, n] \cdot P(t) \)
- \( \Pr[\tilde{T}[t] = \frac{\Pr[f(U_n) = g_1, \ldots, n] \cdot \Pr[\tilde{G}_{n+1} = g_{n+1} \mid \tilde{R}_1, \ldots, n = r_1, \ldots, n]}{2^{- \text{AccH}_{\tilde{G}, \hat{G}}(t)}} \cdot \Pr[\hat{T}[t]) \)
\( \tilde{T} \) vs. \( \hat{T} \) cont.

- \( t = (r_1, g_1, \ldots, r_{n+1}, g_{n+1}) \in \text{Supp}(\tilde{T}) \)

- \[
\Pr[\tilde{T} | t] = \frac{\Pr[f(U_n) = g_1, \ldots, n] \cdot \Pr[\tilde{G}_{n+1} = g_{n+1} | \tilde{R}_1, \ldots, n = r_1, \ldots, n]}{2^{-\text{Acc}_{G, \tilde{G}}(t)}} \cdot \Pr[\tilde{T} | t]
\]

- Note that \( \Pr[f(U_n) = g_1, \ldots, n] \cdot \frac{1}{|f^{-1}(g_1, \ldots, n)|} = 2^{-n} \)

- Hence, for \( t \) with \( \text{Acc}_{G, \tilde{G}}(t) \geq n - \log n \) and

\[
\Pr[\tilde{G}_{n+1} = g_{n+1} | \tilde{R}_1, \ldots, n = r_1, \ldots, n] \geq \frac{\alpha}{|f^{-1}(g_1, \ldots, n)|}:
\]

\[
\Pr[t] \geq \frac{\alpha}{n} \cdot \Pr[\tilde{T} | t] \tag{1}
\]
**Inv’s success probability**

Let $S \subseteq \text{Supp}(\tilde{T})$ denote the set of transcripts $t = (r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ with

1. $\text{Acc}_{\tilde{G}}(t) \geq n - \log n$,

2. $H_{\tilde{G}_i | \tilde{R}_1, \ldots, i-1}(g_i | r_1, \ldots, i-1) \leq \log\left(\frac{4n}{\varepsilon}\right)$ for all $i \in [n]$,

3. $H_{\tilde{G}_{n+1} | \tilde{R}_1, \ldots, n}(g_{n+1} | r_1, \ldots, n) \leq \log\left(\frac{4}{\varepsilon} \cdot |f^{-1}(g_1, \ldots, n)|\right)$.

- $\Pr_{\tilde{T}}\left[\exists i \in [n]: H_{\tilde{G}_i | \tilde{R}_1, \ldots, i-1}(g_i | r_1, \ldots, i-1) > \log\left(\frac{4n}{\varepsilon}\right)\right] \leq n \cdot \frac{\varepsilon}{4n} = \varepsilon/4$
- $\Pr_{\tilde{T}}\left[H_{\tilde{G}_{n+1} | \tilde{R}_1, \ldots, n}(g_{n+1} | r_1, \ldots, n) > \log\left(\frac{4}{\varepsilon} \cdot |f^{-1}(g_1, \ldots, n)|\right)\right] \leq \varepsilon/4$
- $\Pr_{\tilde{T}}[S] \geq \Pr\left[\text{Acc}_{\tilde{G}, \tilde{G}}(T) \geq n - \log n\right] - 2 \cdot \frac{\varepsilon}{4} \geq \frac{\varepsilon}{2}$
- By Eq. (1): $\Pr_{\tilde{T}}[S] \geq \frac{\varepsilon/4}{n} \cdot \Pr_{\tilde{T}}[S] \geq \frac{\varepsilon^2}{8n} \ldots$

Back the bounded version of $\text{Inv}$.

- For $z \in \{0, 1\}^n$ for which $\exists (r_1, z_1, \ldots, r_n, z_n, \ldots) \in S$:
  \[\Pr[\text{Inv}(z) \text{ aborts}] \leq n \cdot \left(1 - \frac{\varepsilon}{4n}\right)^n \leq \frac{1}{2}\]
- Hence, $\Pr_{\tilde{T}}[S] \geq \frac{\varepsilon^2}{16n} \implies \Pr_{x \leftarrow \{0,1\}^n}[\text{Inv}(f(x)) \in f^{-1}(f(x))] \geq \frac{\varepsilon^2}{16n}$
Section 5

Statistically Hiding Commitment from Inaccessible Entropy Generator
High-level description

- Entropy equalization + gap amplification to get generator that has the same min-entropy in each block and whose accessible entropy is $n$-bit smaller than the sum of the min entropies.
- Use "hashing protocol" to get a "generator" with zero accessible entropy block
- Use a random block to mask the committed bit, to get a weakly binding SHC
- Amplify the above into full-fledged SHC