Accessible Entropy and Statistically Hiding Commitments

Handout Mode

Iftach Haitner

Tel Aviv University.

January 23, 2020

1Compiled on 2020/01/26 at 18:00:37.
Section 1

Commitment Schemes
Motivation

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

- $\mu$ is negligible, denoted $\mu(n) = \text{neg}(n)$, if $\forall p \in \text{poly} \ \exists n' \in \mathbb{N}$ s.t. $\mu(n) < \frac{1}{p(n)}$ for all $n > n'$. 
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 \(S(b, r)\).

**Hiding**: Let \(V_{n}^{R^*}(b)\) be \(R^*\)'s view in (the commit stage of) \((S(b), R^*)(1^n)\).

Then for any \(R^*\): \(\text{SD}(V_{n}^{R^*}(0), V_{n}^{R^*}(1)) \leq \text{neg}(n)\).

**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 \(H(b|V^{S^*}) \in \text{neg}(n)\).
- 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
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 \( A \)

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

- Believed not to be implied by OWFs.
- Implies statistically hiding commitment.
- 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 \( h, h(U_n) \), the (min) entropy of \( U_n \) is \( n/2 \).
- Consider PPT \( A \) that outputs \( (h, y) \), and then outputs \( x \in h^{-1}(y) \)
- What is the entropy of \( x \) given \( (h, y) \) and the coins \( A \)'s used to sample them? (essentially) 0!
- The generator \( G(h, x) = (h, h(x), x) \) has “inaccessible entropy” \( n/2 \)
- Inaccessible entropy generators imply statistically hiding commitments?
- OWFs imply inaccessible entropy generators?
Real entropy of a block generator

- 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
  \[
  \text{RealH}_G(g) := \sum_{i \in [m]} H_{G_i|G<i}(g_i|g<i)
  \]
- The real (Shannon) entropy of $G$ is
  \[
  \mathbb{E}_{g \leftarrow G(U_n)} [\text{RealH}_G(g)] = \sum_{i \in [m]} H(G_i|G<i) = H(G(U_n))
  \]
Accessible entropy of a block generator

- Let $G$ be an $m$-block generator, and $\tilde{G}$ be $m$-block generator that uses coins $r_i$ before outputting its $i$'th block $g_i$.

- $\tilde{G}$ is consistent with respect to $G$, if its output is always in support of $G$.

- $\tilde{T} = (\tilde{R}_1, \tilde{G}_1, \ldots, \tilde{R}_m, \tilde{G}_m)$— the rv’s induced by random execution of $\tilde{G}(1^n)$

- 
  \[
  \text{AccH}_{\tilde{G}}(t) := \sum_{i \in [m]} H_{\tilde{G}_i|\tilde{R}_1,\tilde{G}_1,\ldots,\tilde{R}_{i-1},\tilde{G}_{r-1}}(g_i|r_1, g_1, \ldots, r_{i-1}, g_{i-1}) \\
  = \sum_{i \in [m]} H_{\tilde{G}_i|\tilde{R}_{<i}}(g_i|r_{<i})
  \]

- Accessible entropy of $\tilde{G}$: $E_{t \leftarrow \tilde{T}} [\text{AccH}_{\tilde{G}}(t)]$

- Inaccessible entropy of $G$: the gap between the (real) entropy of $G$ and accessible entropy of the best efficient generator consistent with $G$

- We 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

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
  $$\Pr_{x \leftarrow \{0, 1\}^n} [\text{Inv}(f(x)) \in f^{-1}(f(x))] = \text{neg}(n)$$
  for any PPT Inv.
- The real entropy of $G$ is $n$
- Hence, inaccessible entropy gap is $\log n$
- Proof idea
Proving Lem 4

Let $\tilde{G}$ be a PPT $(n + 1)$ block generator consistent with $G$, and assume $E_{t \leftarrow \tilde{T}}[\text{AccH}_{\tilde{G}}(t)] \geq n - \log n$

Algorithm 5 (Inv($z$))

1. For $i = 1$ to $n$, do the following for $n^3$ times:
   1.1 Sample $r_i$ uniformly 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 $i$.
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 (i.e., $n^3$ is replaced by $\infty$)
- $\tilde{T} = (\tilde{R}_1, \tilde{G}_1, \ldots, \tilde{R}_{n+1}, \tilde{G}_{n+1})$ is the (final) values of $(r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ in a random execution of Inv($f(U_n)$).
- $\tilde{T} = (\tilde{R}_1, \tilde{G}_1, \ldots, \tilde{R}_{n+1}, \tilde{G}_{n+1})$ is the coins and output blocks of $\tilde{G}$
- $\tilde{G}_{n+1}|_{R_{\leq n}=r} \equiv \hat{G}_{n+1}|_{\hat{R}_{\leq n}=r}$ for any $r$
- $\tilde{R}_i|_{\tilde{G}_i=g, \tilde{R}_{\leq i}=r} \equiv \hat{R}_i|_{\hat{G}_i=g, \hat{R}_{\leq i}=r}$ for any $g$ and $r$
Bounding $D(\tilde{T} \| \hat{T})$

Assume $\tilde{T} = (\tilde{G}_1, \tilde{R}_1, \tilde{G}_2, \tilde{R}_2, \ldots, \tilde{G}_{n+1}, \tilde{R}_{n+1})$ and same for $\hat{T}$ (?)

$$D(\tilde{T} \| \hat{T}) = \sum_{i=1}^{2n+2} D(\tilde{T}_i \| \hat{T}_i \mid \tilde{T}_{<i}) = \sum_{i=1}^{n+1} D(\tilde{G}_i \| \hat{G}_i \mid \tilde{R}_{<i})$$

$$= \sum_{i=1}^{n+1} -H(\tilde{G}_i \mid \tilde{R}_{<i}) - \sum_{i=1}^{n} \mathbb{E}_{g_i \leftarrow \tilde{G}_i} \left[ \log \Pr [f(U_n)_i = g_i \mid f(U_n)_{< i} = g_{< i}] \right]$$

$$+ H(\tilde{G}_{n+1} \mid \tilde{R}_{\leq n})$$

$$= - \text{Acc}_{\tilde{G}}(\tilde{T}) - \mathbb{E}_{g \leftarrow \tilde{G}_{\leq n}} \left[ \sum_{i} \log \Pr [f(U_n)_i = g_i \mid f(U_n)_{< i} = g_{< i}] \right]$$

$$+ H(\tilde{G}_{n+1} \mid \tilde{R}_{\leq n})$$

$$= - \text{Acc}_{\tilde{G}}(\tilde{T}) - \mathbb{E}_{g \leftarrow \tilde{G}_{\leq n}} \left[ \log \Pr [f(U_n) = g] \right] + H(\tilde{G}_{n+1} \mid \tilde{R}_{\leq n})$$

$$\leq - \text{Acc}_{\tilde{G}}(\tilde{T}) - \mathbb{E}_{g \leftarrow \tilde{G}_{\leq n}} \left[ \log |f^{-1}(g)| - n \right] + \mathbb{E}_{g \leftarrow \tilde{G}_{\leq n}} \left[ \log |f^{-1}(g)| \right]$$

$$= - \text{Acc}_{\tilde{G}}(\tilde{T}) + n \leq \log n$$
Bounding unbounded $\text{Inv}$ success probability

- Let $w(r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ be the indicator for $g_{n+1} \in f^{-1}(g_n)$
- $\Pr[w(\tilde{T})] = 1$
- $D(w(\tilde{T})||w(\hat{T})) = D(1||w(\hat{T})) \leq D(\tilde{T}||\hat{T}) \leq \log n$

$\implies \Pr[w(\hat{T})] \geq 1/n$

$\implies$ The unbound $\text{Inv}$ inverts $f$ with probability at least $1/n$. 
Bounding $\Inv$ success probability

- Let $w(r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ be the indicator for $g_{n+1} \in f^{-1}(g_n)$
- Let $g(r_1, g_1, \ldots, r_{n+1}, g_{n+1})$ be the indicator that for all $i \in [n]$:
  \[
  \Pr \left[ \tilde{G}_i = g_i \mid R_{<i} = r_{<i} \right] \geq 1/n^2
  \]
- \[
  \Pr \left[ (w \land g)(\tilde{T}) \right] \geq 1 - 1/n
  \]
- \[
  D((w \land g)(\tilde{T}) \Vert (w \land g)(\hat{T})) \leq D(\tilde{T} \Vert \hat{T}) \leq \log n
  \]
  \[
  \Rightarrow \Pr \left[ (w \land g)(\hat{T}) \right] \geq 1/2n
  \]
  \[
  \Rightarrow \Inv \text{ inverts } f \text{ with probability at least } 1/2n - n \cdot 2^{-n}
  \]
  \[
  \text{(which is greater than } 1/3n \text{ for large enough } n)\]
Section 4

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

$$G \otimes \ell (x_1, \ldots, x_\ell, i) = G(x_1)_i, \ldots, G(x_1)_m, G(x_2)_1, \ldots, G(x_2)_m, \ldots, G(x_\ell)_1, \ldots, G(x_\ell)_{i-1}$$

- 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 $k_A(\ell - 2) + m$. (?)

- Assume the real entropy of $G$ is $k_R$, then

1. For any $i \in [(\ell - 1) \cdot m]$ and $(g_{\leq i-1}) \in \text{Supp}(G_{\leq i-1} \otimes \ell)$:

$$H(G_i \otimes \ell | G_{\leq i-1} \otimes \ell) \geq k_R / m$$

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 $H(G_i|G_{\leq i-1}) = k_R$ for any $i \in [m]$, then for any $i \in [m]$ and $(g^\ell_{\leq i-1}) \in \text{Supp}(G^\ell_{\leq i-1})$ it holds that

\[
k_{\min}^\ell = H_\infty(G_i^\ell|G^\ell_{\leq i-1}) \approx \ell k_R
\]

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

Both amplifications are proved by reductions.
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