COS433/Math 473: Cryptography

Mark Zhandry
Princeton University
Fall 2020
Announcements/Reminders

HW3 due today

HW4 due Oct 27
Previously on COS 433...
Committments
(Non-interactive)
Commitment Syntax

Message space $\mathcal{M}$
Ciphertext Space $\mathcal{C}$
(suppressing security parameter)

$\text{Com}(m; r)$: outputs a commitment $c$ to $m$

• Why have $r$?
Commitments with Setup

Message space $\mathcal{M}$
Ciphertext Space $\mathcal{C}$
(suppressing security parameter)

$\textbf{Setup}()$: Outputs a key $k$
$\textbf{Com}(k, m; r)$: outputs a commitment $c$ to $m$
Using Commitments

Commit Stage

Reveal Stage

m

r ← R

c ← Com(m; r)

m, r

Check that c = Com(m; r)
Using Commitments (with setup)

1. **Commit Stage**
   - $k \leftarrow \text{Setup}()$
   - $r \leftarrow R$
   - $c \leftarrow \text{Com}(k,m;r)$

2. **Reveal Stage**
   - $m, r$
   - Check that $c = \text{Com}(k,m;r)$
Security Properties

Hiding: \( c \) should hide \( m \)
• Perfect hiding: for any \( m_0, m_1, \)
  \[ \text{Com}(m_0) \overset{d}{=} \text{Com}(m_1) \]
• Statistical hiding: for any \( m_0, m_1, \)
  \[ \Delta(\text{Com}(m_0), \text{Com}(m_1)) < \text{negl} \]
• Computational hiding:

\[ \begin{align*}
  b' & \quad \text{Com}(m_b) \\
  c & \quad \text{Com}(m_0, m_1)
\end{align*} \]
Security Properties (with Setup)

Hiding: \( c \) should hide \( m \)

- Perfect hiding: for any \( m_0, m_1 \),
  \[ k,\text{Com}(k,m_0) \equiv k,\text{Com}(k,m_1) \]

- Statistical hiding: for any \( m_0, m_1 \),
  \[ \Delta( [k,\text{Com}(k,m_0)], [k,\text{Com}(k,m_1)] ) < \text{negl} \]

- Computational hiding:

\[ c \leftarrow \text{Com}(k,m_b) \]
Security Properties

Binding: Impossible to change committed value

- Perfect binding: For any \( c \), \( \exists \) at most a single \( m \) such that \( c = \text{Com}(m;r) \) for some \( r \)

- Computational binding: no efficient adversary can find \( (m_0,r_0),(m_1,r_1) \) such that:
  \[
  \text{Com}(m_0;r_0) = \text{Com}(m_1;r_1) \\
  m_0 \neq m_1
  \]
Security Properties (with Setup)

Binding: Impossible to change committed value
- Perfect binding: For any $k, c$, $\exists$ at most a single $m$ such that $c = \text{Com}(k, m; r)$ for some $r$

- Statistical binding: except with negligible prob over $k$, for any $c$, $\exists$ at most a single $m$ such that $c = \text{Com}(k, m; r)$ for some $r$

- Computational binding: no PPT adversary, given $k \leftarrow \text{Setup}()$, can find $(m_0, r_0), (m_1, r_1)$ such that $\text{Com}(k, m_0; r_0) = \text{Com}(k, m_1; r_1)$, $m_0 \neq m_1$
Today

Commitments continued
Who Runs \textbf{Setup}() \\

Alice? \\
• Must ensure that Alice cannot devise $k$ for which she can break binding \\

Bob? \\
• Must ensure Bob cannot devise $k$ for which he can break hiding \\

Solution: Trusted third party (TTP)
Anagrams as Commitment Schemes

\( \text{Com}(m) = \) sort characters of message

Problems?

• Not hiding: “Jupiter has four moons” vs “Jupiter has five moons”

• Not binding: Kepler decodes Galileo’s anagram to conclude Mars has two moons
Anagrams as Commitment Schemes

\( \text{Com}(m) = \text{add random superfluous text, then sort characters of message} \)

Might still not be hiding
• Need to guarantee, for example that expected number of each letter in output is independent of input string

Still not binding...
Other Bad Commitments

\[ \text{Com}(m) = m \]
- Has (perfect) binding, but no hiding

\[ \text{Com}(m;r) = m \oplus r \]
- Has (perfect) hiding, but no binding
Can a commitment scheme be both statistically hiding and statistically binding?
A Simple Commitment Scheme

Let $H$ be a hash function

$\text{Com}(m;r) = H(m \ || \ r)$

**Theorem:** $\text{Com}(m;r) = H(m \ || \ r)$ has:
- Perfect binding assuming $H$ is injective
- Computational binding assuming $H$ is collision resistant
- Computational hiding in “random oracle model”: $H$ is modeled as a random function
“Standard Model” Commitments
Single Bit to Many Bit

Let \((\text{Setup, Com})\) be a commitment scheme for single bit messages

Let \(\text{Com'}(k, m; r) = (\text{Com}(k, m_1; r_1), \ldots, \text{Com}(k, m_t; r_t))\)

- \(m = (m_1, \ldots, m_t), \ m_i \in \{0, 1\}\)
- \(r = (r_1, \ldots, r_t), \ r_i\) are randomness for \(\text{Com}\)
Theorem: If \((\text{Setup}, \text{Com})\) is statistically/computationally binding, then \((\text{Setup}, \text{Com}’)\) is statistically/computationally binding.

Theorem: If \((\text{Setup}, \text{Com})\) is statistically/computationally hiding, then \((\text{Setup}, \text{Com}’)\) is statistically/computationally hiding.

Therefore, suffices to focus on commitments for single bit messages.
Statistically Binding Commitments

Let $G$ be a PRG with domain $\{0,1\}^\lambda$, range $\{0,1\}^{3\lambda}$

$\textbf{Setup():}$ choose and output a random $3\lambda$-bit string $k$

$\textbf{Com}(b; r):$ If $b=0$, output $G(r)$, if $b=1$, output $G(r) \oplus k$
Theorem: \((\text{Setup,Com})\) is statistically binding

Proof: For any \(r,r'\), \(\Pr[G(r) = G(r') \oplus k] = 2^{-3\lambda}\)

By union bound:

\[
\Pr[ \exists r,r' \text{ such that } \text{Com}(k,0) = \text{Com}(k,1)] = \Pr[ \exists r,r' \text{ such that } G(r) = G(r') \oplus k] < 2^{-\lambda}
\]

Theorem: If \(G\) is a secure PRG, then \((\text{Setup,Com})\) is computationally hiding

Proof: basically stream cipher security
Statistically Hiding Commitments?

Let \( H \) be a collision resistant hash function with domain \( X = \{0,1\} \times \mathbb{R} \) and range \( Z \).

**Setup()**: \( k \leftarrow K \), output \( k \)

\[ \text{Com}(k, m; r) = H(k, (m, r)) \]

Binding?

Hiding?
Statistically Hiding Commitments

Let $\mathbf{F}$ be a pairwise independent function family with domain $\mathbf{X} = \{0,1\} \times \mathbb{R}$ and range $\mathbf{Y}$

Let $\mathbf{H}$ be a collision resistant hash function with domain $\mathbf{Y}$ and range $\mathbf{Z}$

$\text{Setup}()$: $\mathbf{f} \leftarrow \mathbf{F}$, $\mathbf{k} \leftarrow \mathbf{K}$, output $(\mathbf{f}, \mathbf{k})$

$\text{Com}( (\mathbf{f}, \mathbf{k}), \mathbf{m}; \mathbf{r}) = \mathbf{H}(\mathbf{k}, \mathbf{f}(\mathbf{m}, \mathbf{r}))$
Theorem: If $|Y|$ is “sufficiently large” relative to $|X|$ and $H$ is collision resistant, then $(\text{Setup,Com})$ is computational binding.

Theorem: If $|X|$ is “sufficiently large” relative to $|Z|$, then $(\text{Setup,Com})$ is statistically hiding.
Proof:
- Suppose \(|Y| \times \gamma = |X|^2\)
- For any \(x_0 \neq x_1\), \(\Pr[f(x_0) = f(x_1)] < \gamma/(|X|^2)\)
- Union bound:
  \[ \Pr[ \exists x_0 \neq x_1 \text{ s.t. } f(x_0) = f(x_1)] < \gamma \]
- Therefore, \(f\) is injective \(\Rightarrow\) any collision for \(\text{Com}\) must be a collision for \(H\)

**Theorem:** If \(H\) is collision resistant and \(|X|^2/|Y|\) is negligible, then \((\text{Setup}, \text{Com})\) is computationally binding.
Theorem: If $|X|$ is “sufficiently large” relative to $|Z|$, then $(\text{Setup,Com})$ has statistical hiding.

Goal: show $(f, k, H(k, f(0,r)))$ is statistically close to $(f, k, H(k, f(1,r)))$. 

Min-entropy

**Definition:** Given a distribution \( \mathcal{D} \) over a set \( \mathcal{X} \), the min-entropy of \( \mathcal{D} \), denoted \( H_\infty(\mathcal{D}) \), is

\[
\min_x -\log_2(Pr[x \leftarrow \mathcal{D}])
\]

**Examples:**
- \( H_\infty(\{0,1\}^n) = n \)
- \( H_\infty(\text{random } n \text{ bit string with parity 0}) = ? \)
- \( H_\infty(\text{random } i>0 \text{ where } Pr[i] = 2^{-i}) = ? \)
Lemma: Let $\mathcal{D}$ be a distribution on $\mathbf{X}$, and $\mathcal{F}$ a family of pairwise independent functions from $\mathbf{X}$ to $\mathbf{Y}$. Then
\[ \Delta( (f, f(\mathcal{D})) , (f, R) ) \leq \varepsilon \]
where
- $f \leftarrow \mathcal{F}$
- $R \leftarrow \mathbf{Y}$
- $\log |\mathbf{Y}| \leq H_\infty(\mathcal{D}) + 2 \log \varepsilon$
“Crooked” Leftover Hash Lemma

**Lemma:** Let $D$ be a distribution on $X$, and $F$ a family of pairwise independent functions from $X$ to $Y$, and $h$ be any function from $Y$ to $Z$. Then

$$
\Delta( (f, h(f(D))) , (f, h(R)) ) \leq \varepsilon
$$

where

- $f \leftarrow F$
- $R \leftarrow Y$
- $\log |Z| \leq H_\infty(D) + 2 \log \varepsilon - 1$
Theorem: If we set $|R|=|Z|^3$ and $|Z|$ is super-poly, then $(\text{Setup},\text{Com})$ is statistically hiding.

Goal: show $(f, k, H(k, f(0,r)))$ is statistically close to $(f, k, H(k, f(1,r)))$

Let $D_b = (b,r)$, min-entropy $\log |R|$
Set $R = |Z|^3$, $\varepsilon = 2/|Z|$

Then $\log |Z| \leq H_\infty(D_b) + 2 \log \varepsilon - 1$
Theorem: If we set $|R| = |Z|^3$ and $|Z|$ is super-poly, then $(\text{Setup}, \text{Com})$ is statistically hiding.

For any $k, b$,

\[ \Delta( (f, H(k, f(b, r))) , (f, H(k, U))) \leq \varepsilon \]

Thus (for any $k$)

\[ \Delta( (f, H(k, f(0,r))) , (f, H(k, f(1,r))) ) \leq 2\varepsilon \]

Therefore

\[ \Delta( (f, k, H(k, f(0,r))) , (f, k, H(k, f(1,r))) ) \leq 2\varepsilon \]
Number Theory and Crypto
(Handout on course website with basic number theory primer)
So Far...

Two ways to construct cryptographic schemes:

• Use others as building blocks
  • PRGs $\rightarrow$ Stream ciphers
  • PRFs $\rightarrow$ PRPs
  • PRFs/PRPs $\rightarrow$ CPA-secure Encryption
  • ...

• From scratch
  • RC4, DES, AES, etc

In either case, ultimately scheme or some building block built from scratch
Cryptographic Assumptions

Security of schemes built from scratch relies solely on our inability to break them
• No security proof
• Perhaps arguments for security

We gain confidence in security over time if we see that nobody can break scheme
Number-theory Constructions

Goal: base security on hard problems of interest to mathematicians

• Wider set of people trying to solve problem
• Longer history
• Ultimately, new applications
Number Theory

$\mathbb{Z}_N$: integers mod $N$
$\mathbb{Z}_N^*$: integers mod $N$ that are relatively prime to $N$

• $x \in \mathbb{Z}_N^*$ iff $x$ has an “inverse” $y$ s.t. $xy \mod N = 1$
  $\Rightarrow \mathbb{Z}_N^*$ is a multiplicative group

• For prime $N$, $\mathbb{Z}_N^* = \mathbb{Z}_N \setminus \{0\} = \{1, \ldots, N-1\}$
  $\Rightarrow \mathbb{Z}_N$ for prime $N$ is a field

Totient function: $\Phi(N) := |\mathbb{Z}_N^*|$

Euler’s theorem: for any $x \in \mathbb{Z}_N^*$, $x^{\Phi(N)} \mod N = 1$
Announcements/Reminders

HW3 due Today

HW4 due Oct 27