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 **M**
Ciphertext Space **C**
(suppressing security parameter)

Com(m; r): outputs a commitment **c** to **m**

- Why have **r**?

Commitments with Setup

Message space **M**
Ciphertext Space **C**
(suppressing security parameter)

Setup(): Outputs a key **k**
Com(k, m; r): outputs a commitment **c** to **m**

Using Commitments

Commit Stage

r←R

m

c←Com(m;r)

Reveal Stage

m,r

Check that

c = Com(m;r)

Using Commitments (with setup)

$k \leftarrow \mathrm{Setup}()$

Commit Stage

$r \leftarrow R$

$c \leftarrow \mathrm{Com}(k,m;r)$

m

Reveal Stage

m,r

Check that

$c = \mathrm{Com}(k,m;r)$

Security Properties

Hiding: **c** should hide **m**

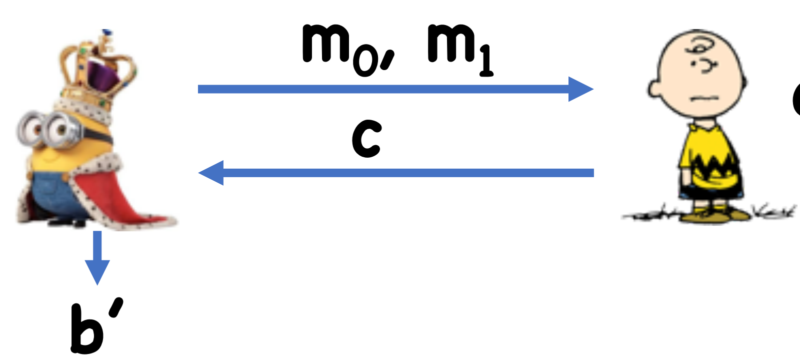
- Perfect hiding: for any $\mathbf{m_0, m_1}$,

$$\mathbf{Com(m_0) \stackrel{d}{=} Com(m_1)}$$

- Statistical hiding: for any $\mathbf{m_0, m_1}$,

$$\mathbf{\Delta(\ Com(m_0), Com(m_1)\ ) < negl}$$

- Computational hiding:



$\mathbf{c \leftarrow Com(m_b)}$

Security Properties (with Setup)

Hiding: **c** should hide **m**

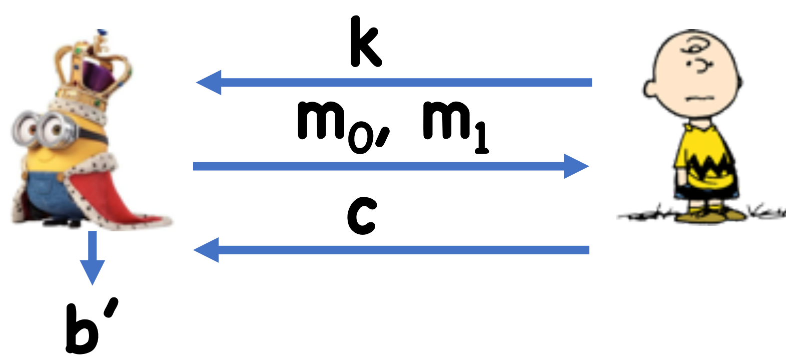
- Perfect hiding: for any $\mathbf{m_0}$, $\mathbf{m_1}$,

$$k, Com(k, m_0) \stackrel{d}{=} k, Com(k, m_1)$$

- Statistical hiding: for any $\mathbf{m_0}$, $\mathbf{m_1}$,

$$\Delta(\ [k, Com(k, m_0)],\ [k, Com(k, m_1)]\ ) < negl$$

- Computational hiding:



$c \leftarrow Com(k, m_b)$

Security Properties

Binding: Impossible to change committed value

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

- Computational binding: no efficient adversary can find $\mathbf{(m_0,r_0),(m_1,r_1)}$ such that:

  $\mathbf{Com(m_0;r_0)=Com(m_1;r_1)}$

  $\mathbf{m_0 \neq m_1}$

Security Properties (with Setup)

Binding: Impossible to change committed value

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

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

- Computational binding: no PPT adversary, given $\mathbf{k \leftarrow Setup()}$, can find $\mathbf{(m_0,r_0),(m_1,r_1)}$ such that

  $\mathbf{Com(k,m_0;r_0)=Com(k,m_1;r_1)}$

  $\mathbf{m_0 \neq m_1}$

Today

Commitments contintuted

Who Runs **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

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

Com(m) = 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

Com(m) = m

- Has (perfect) binding, but no hiding

Com(m;r) = m⊕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

Com(m;r) = H(m || r)

Theorem: 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 **(Setup,Com)** be a commitment scheme for single bit messages

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

- $\mathbf{m = (m_1,\ldots,m_t),\ m_i \in \{0,1\}}$
- $\mathbf{r = (r_1,\ldots,r_t),\ r_i}$ are randomness for **Com**

Theorem: If **(Setup,Com)** is statistically/ computationally binding, then **(Setup,Com')** is statistically/computationally binding

Theorem: If **(Setup,Com)** is statistically/ computationally hiding, then **(Setup,Com')** is statistically/computationally hiding

Therefore, suffices to focus on commitments for single bit messages

Statistically Binding Commitments

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

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

Com(b; r): If $\mathbf{b=0}$, output $\mathbf{G(r)}$, if $\mathbf{b=1}$, output $\mathbf{G(r)}\oplus\mathbf{k}$

Theorem: (Setup,Com) is statistically binding

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

By union bound:

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

Theorem: If **G** is a secure PRG, then **(Setup,Com)** is computationally hiding

Proof: basically stream cipher security

Statistically Hiding Commitments?

Let $\mathbf{H}$ be a collision resistant hash function with domain $\mathbf{X=\{0,1\}\times R}$ and range $\mathbf{Z}$

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

$\mathbf{Com(\ k,\ m;\ r) = H(k,\ (m,r))}$

Binding?

Hiding?

Statistically Hiding Commitments

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

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

Setup(): f←F, k←K, output **(f,k)**
Com((f,k), m; r) = H(k, f(m,r))

Theorem: If **|Y|** is "sufficiently large" relative to **|X|** and **H** is collision resistant, then **(Setup,Com)** is computational binding

Theorem: If **|X|** is "sufficiently large" relative to **|Z|**, then **(Setup,Com)** is statistically hiding

Theorem: If $\mathbf{H}$ is collision resistant and $|X|^2/|Y|$ is negligible, then **(Setup,Com)** is computationally binding

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, $\mathbf{f}$ is injective $\Longrightarrow$ any collision for **Com** must be a collision for $\mathbf{H}$

Theorem: If **|X|** is "sufficiently large" relative to **|Z|**, then **(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 $\mathbf{D}$ over a set $\mathbf{X}$, the min-entropy of $\mathbf{D}$, denoted $\mathbf{H_\infty(D)}$, is

$$\min_x -\log_2(\Pr[x \leftarrow D])$$

Examples:

- $H_\infty(\{0,1\}^n) = n$
- $H_\infty($ random n bit string with parity $0) = ?$
- $H_\infty($ random $i>0$ where $\Pr[i] = 2^{-i}) = ?$

Leftover Hash Lemma

Lemma: Let $\mathbf{D}$ be a distribution on $\mathbf{X}$, and $\mathbf{F}$ a family of pairwise independent functions from $\mathbf{X}$ to $\mathbf{Y}$. Then

$$\Delta(\ (f,\ f(D))\ ,\ (f,\ R)\ ) \leq \varepsilon \text{ where}$$

- $f \leftarrow F$
- $R \leftarrow Y$
- $\log |Y| \leq H_\infty(D) + 2 \log \varepsilon$

"Crooked" Leftover Hash Lemma

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

$$\Delta(\ (f,\ h(f(D)))\ ,\ (f,\ h(R))\ ) \leq \varepsilon \text{ where}$$

- $f \leftarrow F$
- $R \leftarrow Y$
- $\log |Z| \leq H_\infty(D) + 2 \log \varepsilon - 1$

Theorem: If we set $|R|=|Z|^3$ and $|Z|$ is super-poly, then **(Setup,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 **(Setup,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 → Stream ciphers
  - PRFs → PRPs
  - PRFs/PRPs → 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

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

- $x \in \mathbb{Z}_\mathbf{N}^*$ iff **x** has an "inverse" **y** s.t. $\mathbf{xy \bmod N = 1}$
  $\Rightarrow \mathbb{Z}_\mathbf{N}^*$ is a multiplicative group

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

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

Euler's theorem: for any $\mathbf{x} \in \mathbb{Z}_\mathbf{N}^*$, $\mathbf{x^{\Phi(N)} \bmod N = 1}$

Announcements/Reminders

HW3 due Today

HW4 due Oct 27