ZERO-KNOWLEDGE for NP

ALON ROSEN IDC HERZLIYA

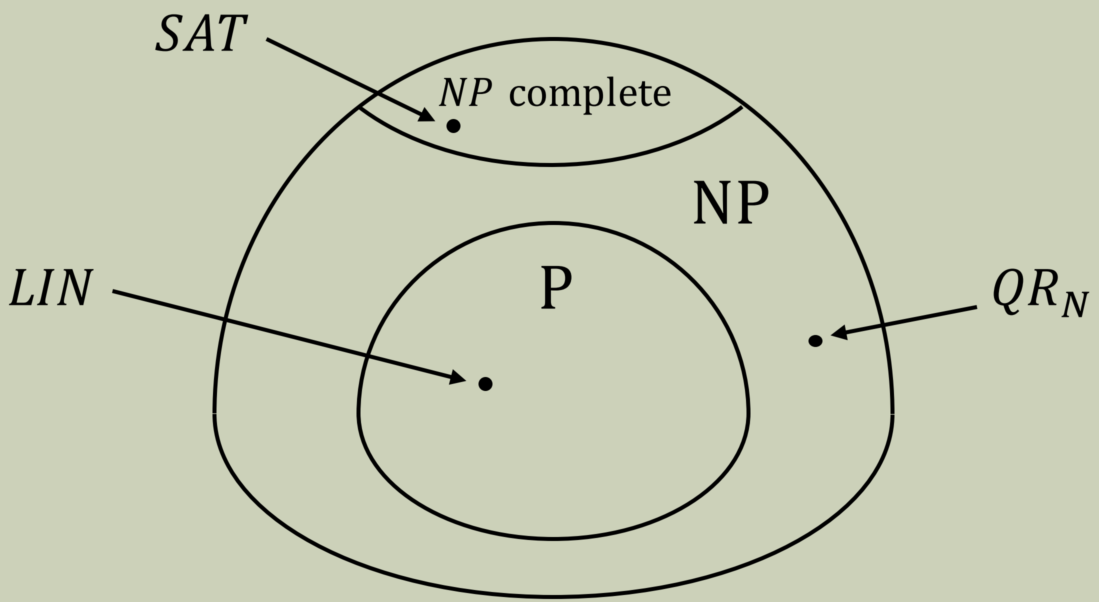
FACT — FOUNDATIONS & APPLICATIONS of CRYPTOGRAPHIC THEORY

Perfect ZK

Perfect ZK: $\forall PPT\ V^* \ \exists PPT\ S\ \forall x \in L\ \forall z$

$$S(x,z) \cong \big(P(w), V^*(z)\big)(x)$$

Proposition: $QR_N \in \mathrm{PZK}$



Can SAT be proved in ZK?

Why do we care?

- QR_N is specific
- SAT is NP-complete
- If $SAT \in \mathrm{ZK}$ then every $L \in \mathrm{NP}$ is provable in ZK

Theorem [F'87, BHZ'87]: If $SAT \in \mathrm{PZK}$ then the polynomial-time hierarchy collapses to the second level

Possible relaxations:

- Computational indistinguishability (now)
- Computational soundness (later)

Statistical Zero-Knowledge

Statistical Indistinguishability

Let X and Y be random variables taking values in a set Ω

Perfect indistinguishability ($X \cong Y$): $\forall T \subseteq \Omega$

$$Pr_X[X \in T] = Pr_Y[Y \in T]$$

ε-**indistinguishability** ($X \cong_s Y$): $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

- $X = X_n$ and $Y = Y_n$
- $\varepsilon = \varepsilon(n)$

Statistical Indistinguishability

Let X and Y be random variables taking values in a set Ω

Perfect indistinguishability ($X \cong Y$): $\forall T \subseteq \Omega$

$$Pr_X[X \in T] = Pr_Y[Y \in T]$$

ε-**indistinguishability ($X \cong_s Y$):** $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \le \varepsilon$$

Triangle inequality: if

- X, Y **are ε_1-indistinguishable and**
- Y, Z **are ε_2-indistinguishable then**
- X, Z **are $(\varepsilon_1 + \varepsilon_2)$-indistinguishable**

Statistical Indistinguishability

Let X and Y be random variables taking values in a set Ω

Perfect indistinguishability ($X \cong Y$): $\forall T \subseteq \Omega$

$$Pr_X[X \in T] = Pr_Y[Y \in T]$$

ε-indistinguishability ($X \cong_s Y$): $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

Indistinguishability of multiple samples: if

- **X, Y are ε-indistinguishable then**
- **X^q, Y^q are $q\varepsilon$-indistinguishable**

Hybrid argument: $X^{q-i}\boldsymbol{Y}Y^{i-1} \cong_s X^{q-i}\boldsymbol{X}Y^{i-1}$

Hybrid Argument

$$X^{q-i}\boldsymbol{Y}Y^{i-1} \cong_s X^{q-i}\boldsymbol{X}Y^{i-1}$$

$$
\begin{array}{lll}
(i=0) & X^q \rightarrow & XXXXXXXXXXXXXXXXXXXX \\
(i=1) & \cong_s & YXXXXXXXXXXXXXXXXXXX \\
(i=2) & \cong_s & YYXXXXXXXXXXXXXXXXXX \\
(i=3) & \cong_s & YYYXXXXXXXXXXXXXXXXX \\
 & & \vdots \\
(i=q-1) & \cong_s & YYYYYYYYYYYYYYYYYYYX \\
(i=q) & \cong_s & YYYYYYYYYYYYYYYYYYYY \rightarrow Y^q
\end{array}
$$

By triangle inequality: $\varepsilon + \varepsilon + \cdots + \varepsilon = q\varepsilon$

Statistical ZK

Statistical ZK: $\forall PPT\ V^* \ \exists PPT\ S\ \forall x \in L\ \forall z$

$$S(x,z) \cong_s \big(P, V^*(z)\big)(x)$$

- SZK - all L that have a statistical ZK proof
- $S(x,z)$ and $\big(P, V^*(z)\big)(x)$ are indexed by x, z
- Typically $n = |x|$ (actually, $n = |w|$)

Theorem [F'87, BHZ'87]: If $SAT \in \mathrm{SZK}$ then the polynomial-time hierarchy collapses to the second level

Computational Zero-Knowledge

Computational Indistinguishability

ε-**indistinguishability** **(**$X \cong_s Y$**):** $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

(t, ε)-**indistinguishability** **(**$X \cong_c Y$**):** $\forall T \subseteq \Omega$ **that are "decidable in time** t**"**

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

$T \subseteq A$ **is decidable in time** t **if** $\exists$**time-**t D **such that** $\forall x \in A$

$$x \in T \leftrightarrow D(x) = 1$$

Computational Indistinguishability

ε-**indistinguishability** ($X \cong_s Y$): $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

(t, ε)-**indistinguishability** ($X \cong_c Y$): $\forall$**time**-t D

$$|Pr[D(X) = 1\,] - Pr[D(Y) = 1\,]| \leq \varepsilon$$

Triangle inequality: if

- X, Y **are** (t_1, ε_1)**-indistinguishable and**
- Y, Z **are** (t_2, ε_2)**-indistinguishable then**
- X, Z **are** $(min\{t_1, t_2\}, \varepsilon_1 + \varepsilon_2)$**-indistinguishable**

Computational Indistinguishability

ε-**<u>indistinguishability</u>** **(**$X \cong_s Y$**):** $\forall T \subseteq \Omega$

$$|Pr[X \in T] - Pr[Y \in T]| \leq \varepsilon$$

(t, ε)-**<u>indistinguishability</u>** **(**$X \cong_c Y$**):** $\forall$**time-**t D

$$|Pr[D(X) = 1\ ] - Pr[D(Y) = 1\ ]| \leq \varepsilon$$

<u>Indistinguishability of multiple samples</u>: if

- X, Y **are** (t, ε)**-indistinguishable** **<u>then</u>**
- X^q, Y^q **are** $(t, q\varepsilon)$**-indistinguishable**

<u>Hybrid argument (non-uniform)</u>:

$$X^{q-i}\boldsymbol{Y}Y^{i-1} \cong_s X^{q-i}\boldsymbol{X}Y^{i-1}$$

Computational Indistinguishability

Typically:

- $t = poly(n)$
- $\varepsilon = neg(n)$

Definition: $\varepsilon = \varepsilon(n)$ is **negligible** if it is eventually smaller than $1/p(n)$ for every polynomial p

$$\varepsilon = neg(n), q = poly(n) \;\rightarrow\; q\varepsilon = neg(n)$$

$$X^1 \cong_\varepsilon X^2 \cdots \cong_\varepsilon X^q \;\rightarrow\; X^1 \cong_{q\varepsilon} X^q$$

In practice: concrete choices of t, q and ε

Computational ZK

Computational ZK: $\forall PPT\ V^* \ \exists PPT\ S\ \forall x \in L\ \forall z$

$$S(x,z) \cong_c \big(P, V^*(z)\big)(x)$$

$$\text{PZK} \subseteq \text{SZK} \subseteq \text{CZK}$$

Theorem [GMW'86]: Suppose one-way functions exist. Then $\text{NP} \subseteq \text{CZK}$

One-way Functions

Definition: $f: \{0,1\}^* \to \{0,1\}^*$ is (t, ε)-**one-way** if $\forall$time-t A

$$Pr_X[A \text{ inverts } f(X)] \le \varepsilon$$

Candidate OWFs:

- **Rabin/RSA:** $x^2 \ mod \ N$ $\quad$ $x^e \ mod \ N$
- **Discrete exponentiation:** $g^x \ mod \ P$
- **SIS/LWE:** $Ax \ mod \ q$ $\quad$ $Ax + e \ mod \ q$
- **AES:** $AES_x(0^n)$
- **SHA:** $h(x)$

Commitment Schemes

Commitment Scheme

- **Two-stage protocol between *Committer* and *Receiver***

C

R

Commit

$c = Com(m, r)$ →

Reveal

$(m, r) = Dec(c)$ →

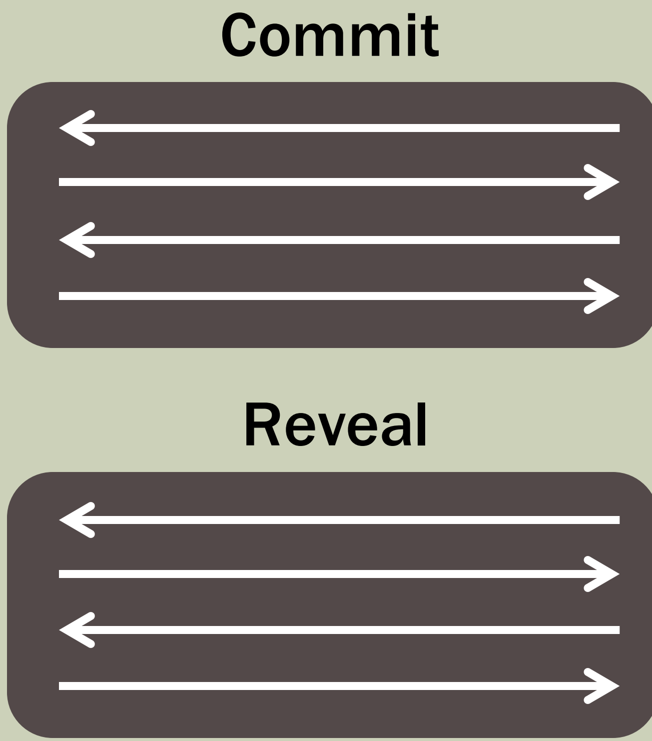
<u>Completeness</u>: C can always generate valid

$$c = Com(m, r)$$

Commitment Scheme

- Two-stage protocol between *Committer* and *Receiver*

C **R**



$Com(m, r)$ is R^*'s view of the commit phase

Canonical reveal:
$Dec(c) = (m, r)$

$Dec(c)$ is R^*'s view of the reveal phase

Statistically-binding Commitments

Definition: A statistically-binding (Com, Dec) **satisfies:**

Computational hiding: $\forall PPT\ R^* \ \forall m_1, m_2$

$$Com(m_1) \cong_c Com(m_2)$$

Statistical binding: $\forall C^* \ \forall m_1 \neq m_2$

$$Pr[C^* \text{ wins the binding game}] \leq neg(n)$$

C^* wins the binding game if it generates c along with

- $(m_1, r_1) = Dec(c)$
- $(m_2, r_2) = Dec(c)$

- Note: hiding holds even if m_1, m_2 are known
- Later: statistically-hiding commitments

Examples (statistically-binding)

- **El-Gamal (assuming DDH):**

$$Com_{g,h}(m,r) = \ (g^r, h^r \cdot g^m)$$

- **Any OWP:**

$$Com(m,r) = \ (f(r), b(r) \oplus m)$$

- **Any PRG (and hence OWF):**

$$Com_r(b,s) = \begin{cases} G(s) & b = 0 \\ G(s) \oplus r & b = 1 \end{cases}$$

$NP \subseteq CZK$

$HAM \in \mathrm{CZK}$

<u>Theorem [GMW'86]</u>: If statistically-binding commitments exist then $\mathrm{NP} \subseteq \mathrm{CZK}$

<u>Theorem [B'86]</u>: If statistically-binding commitments exist then $HAM \in \mathrm{CZK}$

$$HAM = \{G \mid G \text{ has a Hamiltomian cycle}\}$$

<u>Ham cycle</u>: passes via each vertex exactly once

HAM is NP-complete

Every $L \in \mathrm{NP}$ is poly-time reducible to HAM

$\exists$poly-time computable f such that $\forall x$

$$x \in L \Leftrightarrow f(x) \in HAM$$

To prove $L \in \mathrm{CZK}$, sufficient to prove $HAM \in \mathrm{CZK}$

w **for** $x \in L$

$\updownarrow$

$g(w)$ **for** $f(x) \in HAM$

P

$x \in L$

$\updownarrow$

$f(x) \in HAM$

V

ACCEPT/REJECT

Adjacency Matrix Representation

Graph G

0	**1**	0	0	1	1
1	0	1	**1**	0	0
1	1	0	0	**1**	0
0	0	**1**	0	1	1
1	0	1	1	0	**1**
1	1	0	1	1	0

Ham cycle w

	1				
			1		
				1	
		1			
					1
1					

Committing to G and opening cycle w

Graph G

0	**1**	0	0	1	1
1	0	1	**1**	0	0
1	1	0	0	**1**	0
0	0	**1**	0	1	1
1	0	1	1	0	**1**
1	1	0	1	1	0

$\rightarrow$

$G = Dec(c)$

0	**1**	0	0	1	1
1	0	1	**1**	0	0
1	1	0	0	**1**	0
0	0	**1**	0	1	1
1	0	1	1	0	**1**
1	1	0	1	1	0

An interactive proof for HAM

Ham cycle w **P** $G \in HAM$ **V**

$\pi \in_R S_n$ — $\boldsymbol{c} = Com(\pi(G))$ →

← b — $b \in_R \{0,1\}$

$u = \pi(w)$ — $b = 0$: $u \in Dec(\boldsymbol{c})$ → **Verify that** u **is a cycle**

$b = 1$: $\pi, H = Dec(\boldsymbol{c})$ — **Verify that** $H = \pi(G)$

In either case,
verify hat Dec **are valid**

When $b = 0$

$\underline{b\ =\ 0}$

$\boldsymbol{c} = Com(\pi(G))$

$u \in Dec(\boldsymbol{c})$

	1				
			1		
				1	
		1			
					1
1					

Verify :

- **That** Dec **is valid**
- **That** u **is a cycle**

When $b = 1$

$\underline{b\ =\ 1}$

$\boldsymbol{c} = Com(\pi(G))$

$H = Dec(\boldsymbol{c})$

0	1	0	0	1	1
1	0	1	1	0	0
1	1	0	0	1	0
0	0	1	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0

π

6	1	3	2	5	4

Verify :

- **That** Dec **is valid**
- **That** $H = \pi(G)$

Soundness

Claim: If (Com, Dec) is statistically binding then (P, V) is an interactive proof for HAM

P*

V

$Com(\pi(G))$ →

← b

$b = 0$: u →
$b = 1$: (π, H)

u is a cycle

$H = \pi(G)$

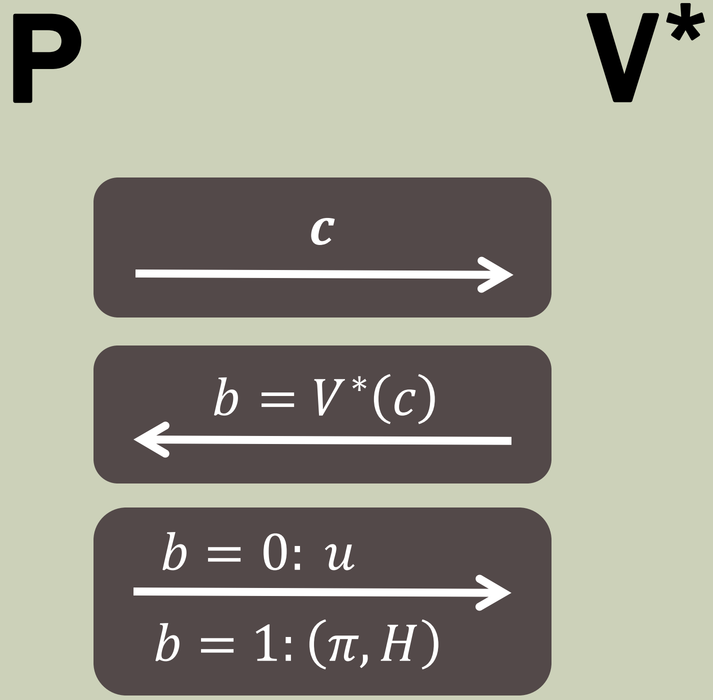
Soundness:

If $Pr_b[(P^*, V)$ accepts $x] > 1/2$ then both

- u is a cycle in H
- and $H = \pi(G)$

So $\pi^{-1}(u)$ is a cycle in G

Computational ZK



<u>Simulator $S^{V^*}(G)$</u>:

1. **Set** $G_0 = u$ **for** $u \in_R cycle_n$
2. **Set** $G_1 = \pi(G)$ **for** $\pi \in_R S_n$
3. **Sample** $b \in_R \mathbb{Z}_N^*$

   $b = 0$: **Set** $\boldsymbol{c} = Com(G_0)$

   $b = 1$: **Set** $\boldsymbol{c} = Com(G_1)$
4. **If** $V^*(\boldsymbol{c}) = b$

   $b = 0$: **Output** $(\boldsymbol{c}, b, u)$

   $b = 1$: **Output** $\left(\boldsymbol{c}, b, (\pi, G_1)\right)$
5. **Otherwise <u>repeat</u>**

Computational ZK

$\underline{b = 0}$

G_0

0	**1**	0	0	0	0
0	0	0	**1**	0	0
0	0	0	0	**1**	0
0	0	**1**	0	0	0
0	0	0	0	0	**1**
1	0	0	0	0	0

$\underline{b = 1}$

G_1

0	1	0	0	1	1
1	0	1	1	0	0
1	1	0	0	1	0
0	0	1	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0

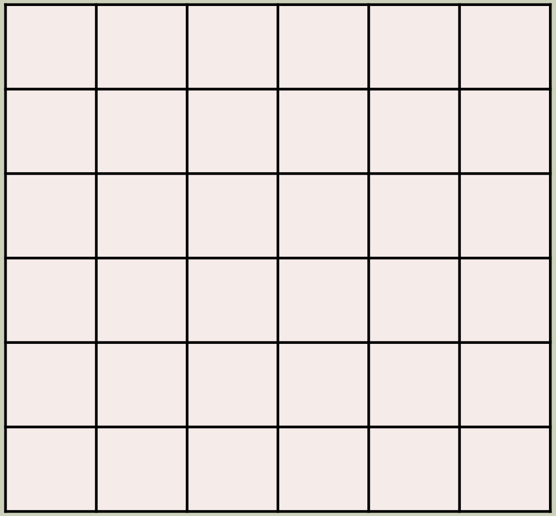
π

6	1	3	2	5	4

Computational ZK

$\underline{b\ =\ 0}$

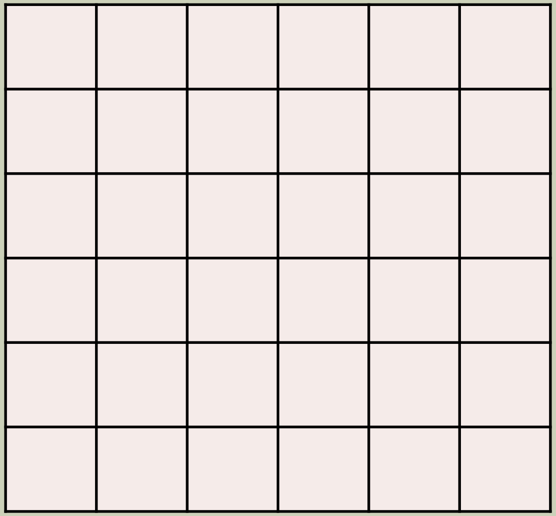
$\boldsymbol{c} = Com(G_0)$



$\cong_c$

$\underline{b\ =\ 1}$

$\boldsymbol{c} = Com(G_1)$



Computational ZK

If $V^*(\boldsymbol{c}) = 0$

(otherwise repeat)

$G_0 = u$

	1				
			1		
				1	
		1			
					1
1					

If $V^*(\boldsymbol{c}) = 1$

(otherwise repeat)

$G_1 = \pi(G)$

0	1	0	0	1	1
1	0	1	1	0	0
1	1	0	0	1	0
0	0	1	0	1	1
1	0	1	1	0	1
1	1	0	1	1	0

π

6	1	3	2	5	4

Computational ZK

<u>Claim:</u> If Com is computationally hiding then $S^{V^*}(G)$ runs in polynomial time

1. From hiding of Com and the fact that V^* is PPT:

$$Pr_{\boldsymbol{c},b}\left[V^*\left(Com(G_b)\right) = b\right] \approx 1/2$$

<u>Exercise</u>: otherwise V^* distinguishes between $Com(G_0)$ and $Com(G_1)$

2. This implies: $\mathbb{E}[\text{\#repetitions}] \approx 2$

Computational ZK

Claim: If Com is computationally hiding then $\forall G \in HAM$

$$S^{V^*}(G) \cong_c (P(w), V^*)(G)$$

1. Let $H^{V^*}(G, w)$ act identically to $S^{V^*}(G)$ except that:
   - H commits to G_1 instead of G_0
   - When $V^*(c) = 0$, H outputs $\pi(w)$ instead of u

2. <u>Exercise</u>:

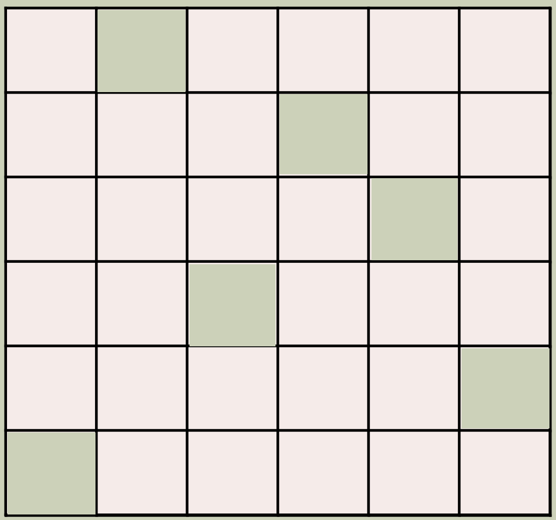
$$S^{V^*}(G) \cong_c H^{V^*}(G, w) \cong (P(w), V^*)(G)$$

<u>Hint</u>: $Com(G_0) \cong_c Com(G_1)$ even if G, w, π are known.

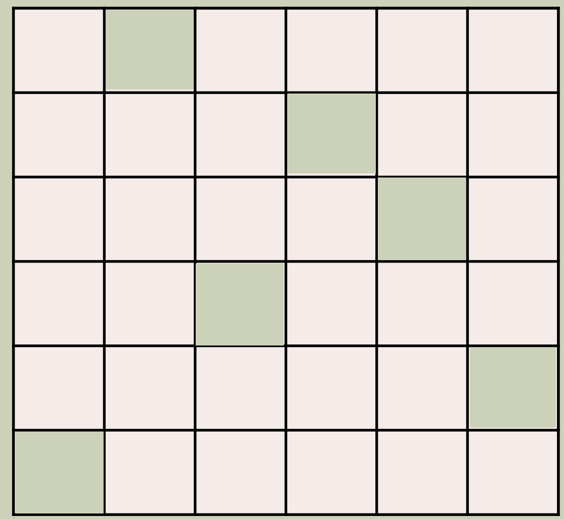
Computational ZK

$\underline{S^{V^*}(G) \mid b = 0}$ $\underline{H^{V^*}(G, w) \mid b = 0}$

$\boldsymbol{c} = Com(G_0) - Com(\pi(w))$ $\boldsymbol{c} = Com(G_1) - Com(\pi(w))$



$\cong_c$



Computational ZK – some more

One-way functions (or rather some weak form of them) are necessary for non-trivial ZK

Theorem [OW'90]: If $\exists\mathsf{ZK}$ proofs for languages outside of BPP then there exist functions with one-way instances

Theorem [OW'90]: If $\exists\mathsf{ZK}$ proofs for languages that are hard on average then there exist one-way functions

Unconditional characterization of ZK [Vad'06]:

- $\mathsf{HVZK} = \mathsf{ZK}$
- ZK is closed under union
- Public-coin ZK equals private-coin ZK
- ZK w/ imperfect compl. equals ZK w/ perfect compl.

Techniques borrowed from the study of SZK [SV'90's]

Summary

$$\mathrm{BPP} \subseteq \mathrm{PZK} \subseteq \mathrm{SZK} \subset \mathrm{CZK} = \mathrm{IP}$$

Defined:

- **Statistical indistinguishability**
- **Computational indistinguishability**
- $\mathrm{SZK}, \mathrm{CZK}$
- **One way-functions**
- **Statistically-binding commitments**

Saw:

- **Examples of statistically-binding commitments**
- $\mathrm{NP} \subseteq \mathrm{CZK}$ **via** $HAM \in \mathrm{CZK}$

Food for Thought

Other considerations

- **Efficiency of reduction to HAM**
  - Classic reduction from SAT to HAM has quadratic blowup
  - Ideally: linear blowup (with small constants)
- **Communication complexity**
  - Statistically-binding commitments imply linear communication
  - Next lecture: statistically-hiding commitments
  - Open up the possibility of sublinear communication
- **Efficiency of prover and/or verifier**
  - May have to optimize P, V even if sublinear communication
  - Both time and space complexities – tradeoff between P, V
- **Round complexity**
  - Much research devoted to minimizing rounds (see next lecture)

Modern Crypto Methodology

<u>Define</u>

- what it means to break the system
- Adversary's access/resources

<u>Build</u>

- In ZK first there were protocols, only then defs

<u>Prove</u>

- We still do not have good "language" for proofs
- ML theory vs Crypto theory (crypto theory is *essential*)

First *feasibility* then *efficiency*

- *Optimize (round/comm. complexity, verifier time/space)*

Relax definition (Argument/WI/WH/NIZK)

Auxiliary input to D and Non-uniform V^*

Computational ZK: $\forall PPT\ V^*\ \exists PPT\ S\ \forall \boldsymbol{PPT}\ \boldsymbol{D}\ \forall x \in L\ \forall z$

$$\left|Pr[D(x,z,S(x,z)\,) = 1\,] - Pr\left[D\left(x,z,\left(P,V^*(z)\right)(x),z\right) = 1\,\right]\right| \leq neg(|x|)$$

Advanced comment:

- D is also given z
- If z is sufficiently long, D can make use of its suffix
- V^* and S cannot (D is determined after them)
- implies indistinguishability against non-uniform circuits D
- Making V^* also non uniform yields “weaker” security reduction (from V^* to S)

History


Oded Goldreich


Avi Wigderson


Manuel Blum


Moni Naor


Rafail Ostrovsky


Amit Sahai


Salil Vadhan

The End

Questions?