Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 05

Zero-Knowledge IPs

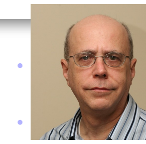
Zero Knowledge IPs

paper that first introduced the notion of zero knowledge →

The Knowledge Complexity of Interactive Proof Systems

Shafi Goldwasser	Silvio Micali	Charles Rackoff
MIT	MIT	University of Toronto





Benefits of interaction and randomness so far:

- capture many languages beyond NP ($coNP$, $P^{\#P}$, PSPACE)
- delegate computation (bounded-depth circuits)

Today we study another benefit: ZERO KNOWLEDGE.

Informally, we seek IPs that protect the privacy of the honest prover.
The honest prover should reveal no information beyond the necessary bit "$x \in L$".

We illustrate this notion via the language $GI = \{(G_0, G_1) \mid G_0 \equiv G_1\}$.
Recall that GI is in NP: the witness is any isomorphism between the graphs.
Hence there is a trivial IP: the IP prover sends an isomorphism to the IP verifier.

CHALLENGE: what if the isomorphism is a private input of the honest prover?

How to design an alternative IP for GI (achieving completeness and soundness)
where the honest prover reveals no information beyond $G_0 \equiv G_1$?

Interactive Proofs for Relations

A relation is a set of instance-witness pairs $R = \{(x,w) : \ldots\}$.

The corresponding language is $L(R) := \{x : \exists\, w \text{ s.t. } (x,w) \in R\}$.

Languages can be viewed as relations with empty witnesses: $L = \{x : \ldots\} \rightarrow R = \{(x,\perp) : \ldots\}$

Example: • GI as a language $L_{GI} = \{(G_0,G_1) : G_0 \equiv G_1\}$.

• GI as a relation $R_{GI} = \{((G_0,G_1),\sigma) : G_0 = \sigma(G_1)\}$. Note that $L_{GI} = L(R_{GI})$.

The definition of an IP directly extends from languages to relations.

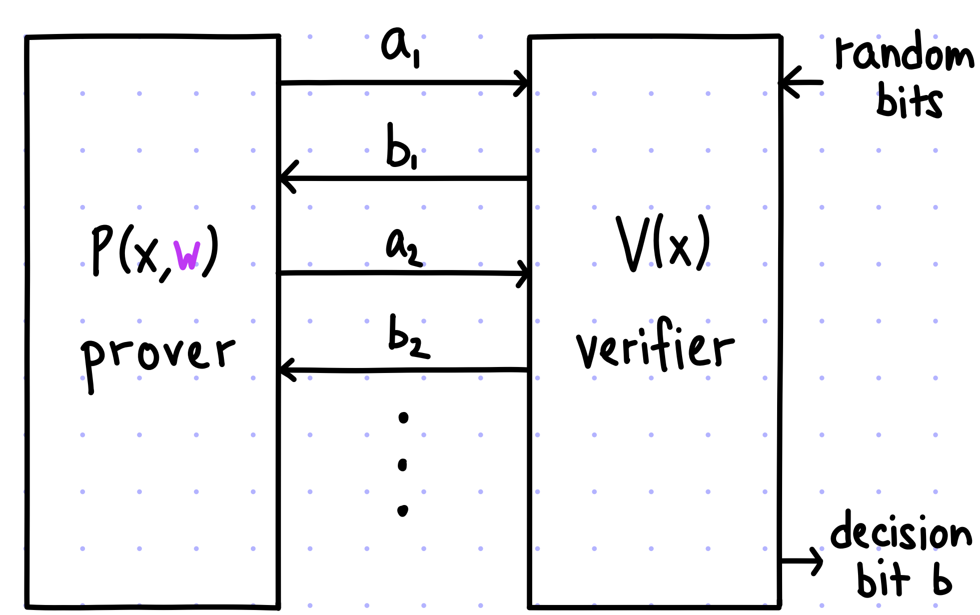
def: (P,V) is an IP for a relation R with completeness error ε_c and soundness error ε_s this holds:

① completeness:

$$\forall (x,w) \in R \quad \Pr_{r_P, r_V}\left[\langle P(x,w;r_P), V(x;r_V)\rangle = 1\right] \geq 1 - \varepsilon_c$$

② soundness:

$$\forall\, x \notin L(R)\ \forall \tilde{P} \quad \Pr_{r_V}\left[\langle \tilde{P}, V(x;r_V)\rangle = 1\right] \leq \varepsilon_s$$



Today we focus on the (more general) case of IPs for relations.

Zero Knowledge against Honest Verifiers

An IP (P,V) for a relation R is honest-verifier zero knowledge (HVZK) if

$\exists$ polynomial-time probabilistic algorithm S (known as the simulator) such that

$$\forall (x,w) \in R \quad S(x) \equiv \mathrm{View}(P,V,x,w)$$

Here $\mathrm{View}(P,V,x,w) := (r, x, a_1, \ldots, a_k)$ is all the information seen by V when interacting with $P(x,w)$: its randomness r, its input x, and the prover's messages $a_1, \ldots, a_k$.

INTERPRETATION: The honest verifier could have simulated the interaction by itself, without talking to the honest prover. The simulator captures this by efficiently sampling the honest verifier's view.

NOTES:

- HVZK is a joint property of the honest prover P & honest verifier V.
  (This is like the completeness property, also a joint property of P and V.)
- HVZK is preserved under sequential and parallel repetition of the IP.

Honest-Verifier ZK for Graph Isomorphism [1/2]

$\sigma : [n] \to [n]$ s.t. $G_0 = \sigma(G_1)$ → $P((G_0, G_1), \sigma)$

$V((G_0, G_1))$

sample random permutation $\varphi : [n] \to [n]$

$H := \varphi(G_0)$ $\xrightarrow{\quad H \quad}$

$\xleftarrow{\quad b \quad}$ $b \leftarrow \{0,1\}$

send an isomorphism from G_b to H

$\psi := \varphi \circ \sigma^b$ $\xrightarrow{\quad \psi \quad}$ $H \stackrel{?}{=} \psi(G_b)$

First we argue that this is an IP for GI.

Completeness: Suppose that $((G_0, G_1), \sigma) \in R_{GI}$ (i.e. $\sigma : [n] \to [n]$ is s.t. $G_0 = \sigma(G_1)$).

For every $b \in \{0,1\}$, $H \stackrel{?}{=} \psi(G_b) \longleftrightarrow H \stackrel{?}{=} (\varphi \circ \sigma^b)(G_b) \longleftrightarrow H \stackrel{?}{=} \varphi(G_0)$.

Soundness: Suppose that $(G_0, G_1) \notin L_{GI} = L(R_{GI})$

Then H can be isomorphic to at most one of G_0 and G_1.

Any malicious prover gets caught w.p. $\geq 1/2$.

Honest-Verifier ZK for Graph Isomorphism [2/2]

claim: (P,V) is HVZK

$P((G_0,G_1),\sigma)$		$V((G_0,G_1))$
sample random permutation $\varphi:[n]\to[n]$		
$H:=\varphi(G_0)$	$\xrightarrow{H}$	
	$\xleftarrow{b}$	$b\leftarrow\{0,1\}$
$\psi:=\varphi\circ\sigma^b$	$\xrightarrow{\psi}$	$H\stackrel{?}{=}\psi(G_b)$

proof: Fix $((G_0,G_1),\sigma)\in R_{GI}$.

The honest verifier's view is

$$((G_0,G_1),H,b,\psi)$$

where
- H equals $\psi(G_b)$
- b is a random bit
- ψ is a random permutation on $[n]$ (it is either φ or $\varphi\circ\sigma$)

Consider the following polynomial-time probabilistic algorithm:

$S((G_0,G_1))$:=
1. Sample $b\leftarrow\{0,1\}$.
2. Sample random permutation $\psi:[n]\to[n]$.
3. Compute $H:=\psi(G_b)$.
4. Output $((G_0,G_1),H,b,\psi)$.

Since $G_0\equiv G_1$, the output of S is equidistributed as V's view. ■

Zero Knowledge against Malicious Verifiers [1/2]

We can strengthen zero knowledge to require that even verifiers $\tilde{V}$ that deviate from the prescribed protocol cannot learn any information besides the bit "$x \in L(R)$".

How does the simulator S know about the malicious verifier $\tilde{V}$?

- existential simulation: $\forall$ efficient $\tilde{V}$ $\exists$ efficient $S_{\tilde{V}}$ $\forall (x,w) \in R$ $\quad S_{\tilde{V}}(x) \equiv \mathrm{View}(P,\tilde{V},x,w)$
- universal simulation: $\exists$ efficient S $\forall$ efficient $\tilde{V}$ $\forall (x,w) \in R$ $\quad S(\tilde{V},x) \equiv \mathrm{View}(P,\tilde{V},x,w)$
- black-box simulation: $\exists$ efficient S $\forall$ efficient $\tilde{V}$ $\forall (x,w) \in R$ $\quad S^{\tilde{V}}(x) \equiv \mathrm{View}(P,\tilde{V},x,w)$

Note that malicious-verifier ZK is a property of the honest prover P alone.
(Compare with: completeness is of P&V; soundness is of V; HVZK if of P&V.)

REMARK: Preserving malicious-verifier ZK under repetition of the IP is tricky.

- Sequential repetition preserves auxiliary-input malicious-verifier ZK.

  The condition is strengthened to $\begin{cases} \forall aux \;\; S_{\tilde{V}}(x, aux) \equiv \mathrm{View}(P, \tilde{V}(aux), x, w) & \text{for existential simulation} \\ \forall aux \;\; S(\tilde{V}, x, aux) \equiv \mathrm{View}(P, \tilde{V}(aux), x, w) & \text{for universal simulation} \end{cases}$

  Black-box simulation supports auxiliary inputs as is.

- Parallel repetition does NOT, in general, preserve malicious-verifier ZK (assuming plausible crypto).

  This is even for black-box simulation.

Zero Knowledge against Malicious Verifiers [2/2]

We focus on black-box simulation:

$\exists$ efficient S $\forall$ efficient $\tilde{V}$ $\forall (x,w) \in R$ $S^{\tilde{V}}(x) \equiv View(P, \tilde{V}, x, w)$

What is "efficient"?

Ideally: $\tilde{V}$ and S are polynomial-time probabilistic algorithms

Problem: <u>theorem</u> [Barak Lindell 2002]:

If L has an IP with round complexity $k = O(1)$, soundness error $\varepsilon_s = negl(n)$, and $S^{\tilde{V}}(x)$ runs in polynomial time (for polynomial-time $\tilde{V}$) then $L \in BPP$.

Common workaround (there are others): S runs in EXPECTED polynomial time.

<u>def</u>: An IP (P,V) for a relation R is (malicious-verifier) zero knowledge if $\exists$ expected polynomial-time probabilistic algorithm S (called the simulator) such that

$\forall$ polynomial-time probabilistic $\tilde{V}$ $\forall (x,w) \in R$ $S^{\tilde{V}}(x) \equiv View(P, \tilde{V}, x, w)$

LIMITATIONS ON ROUND COMPLEXITY $\longrightarrow$

<u>theorem</u>: Suppose L has a k-round IP with $\varepsilon_s = negl(n)$ and (expected polynomial-time) simulation.

- If $k=2$ then $L \in BPP$ (even for existential simulation). ← [Oren 1987][Goldreich Oren 1993]
- If $k=3$ and simulation is black box then $L \in BPP$. ← [Goldreich Krawczyk 1990]
- If $k=O(1)$, the IP is public-coin, and simulation is black box then $L \in BPP$.

Malicious-Verifier ZK for Graph Isomorphism

claim: (P,V) is MVZK

proof: Fix $((G_0,G_1),\sigma) \in R_{GI}$ and $\tilde{V}$.

The view of the malicious verifier $\tilde{V}$ is

$$((G_0,G_1), H, \tilde{b}, \psi)$$

where
- H equals $\psi(G_{\tilde{b}})$
- $\tilde{b}$ is distributed as $\tilde{V}(H)$
- ψ is a random permutation on $[n]$ (it is either φ or $\varphi \circ \sigma$)

$P((G_0,G_1),\sigma)$		$V((G_0,G_1))$
sample random permutation $\varphi:[n]\to[n]$		
$H := \varphi(G_0)$	$\xrightarrow{\ H\ }$	
	$\xleftarrow{\ b\ }$	$b \leftarrow \{0,1\}$
$\psi := \varphi \circ \sigma^b$	$\xrightarrow{\ \psi\ }$	$H \stackrel{?}{=} \psi(G_b)$

Consider the following EXPECTED polynomial-time probabilistic algorithm:

$S^{\tilde{V}}((G_0,G_1)) :=$
1. Sample $b \leftarrow \{0,1\}$.
2. Sample random $\psi:[n]\to[n]$.
3. Compute $H := \psi(G_b)$.
4. Give H to $\tilde{V}$ to get $\tilde{b}$.
5. If $\tilde{b} \neq b$ then GOTO 1.
6. Output $((G_0,G_1), H, \tilde{b}, \psi)$.

S uses $\tilde{V}$ only as a black-box

$S^{\tilde{V}}((G_0,G_1))$ runs in expected polynomial time:

$G_0 \equiv G_1 \rightarrow H$ is independent of b
$\rightarrow \tilde{b}$ is independent of b
$\rightarrow \Pr[\tilde{b}=b] = \frac{1}{2} \rightarrow \mathbb{E}[\#\text{rewinds}] = 2$.

$S^{\tilde{V}}((G_0,G_1))$ follows the desired distribution:

$$\Pr[\tilde{b}=0 \mid \tilde{b}=b] = \frac{\Pr[\tilde{b}=0 \wedge \tilde{b}=b]}{\Pr[\tilde{b}=b]} = \frac{\Pr[\tilde{b}=0]\cdot\frac{1}{2}}{\frac{1}{2}} = \Pr[\tilde{b}=0]$$

■

Limitations of Zero Knowledge

What happens more generally?

def:
- HVZK-IP = all languages that have IPs with honest-verifier zero knowledge
- (MV)ZK-IP = all languages that have IPs with malicious-verifier zero knowledge

Straightforward: $\mathrm{BPP} \overset{\text{simulator does nothing}}{\subseteq} \text{MVZK-IP} \subseteq \text{HVZK-IP} \subseteq \mathrm{IP}$.

Moreover, we proved that $\mathrm{GI} \in$ MVZK-IP (and GI is not known to be in BPP).

Q: What languages have zero knowledge IPs?

theorem: HVZK-IP $\subseteq \mathrm{AM} \cap \mathrm{coAM}$

Hence we do not expect that $\mathrm{NP} \subseteq$ HVZK-IP. (Since $\mathrm{NP} \subseteq \mathrm{coAM}$ directly implies that $\mathrm{coNP} \subseteq \mathrm{IP}[k=O(1)]$, which implies that the Polynomial Hierarchy collapses [Boppana, Håstad, Zachos 1987].)

So far we discussed PERFECT ZERO KNOWLEDGE (PZK), where $S(x)$ equals the verifier's view.
The above limitation holds even for honest-verifier STATISTICAL ZERO KNOWLEDGE (SZK), which relaxes the requirement on the simulator for the honest verifier: require only that $S(x)$ and $\mathrm{View}(P,V,x,w)$ are statistically close.

Intuition on the Limits of HVZK-IP

Suppose that (P,V) is an HVZK IP for L.

Let S be the HVZK simulator. We know that $\forall x \in L \;\; S(x) \equiv View(P,V,x)$.

Q: What does $S(x)$ do if $x \notin L$?

① $S(x)$ outputs a view $(r, x, a_1, \dots, a_k)$ that is REJECTING (with non-negligible probability)

② $S(x)$ outputs a view $(r, x, a_1, \dots, a_k)$ that is ACCEPTING (but for a negligible probability)

If option ① then $L \in BPP$ (in the weaker "infinitely often" sense): use the simulator to decide.

$\exists$ BPP machine that decides L on infinitely many (maybe not all) input sizes

So suppose that option ② holds.

OBSERVATION: $x \in \bar{L} \rightarrow S(x)$ and $View(P,V,x)$ are statistically far

Indeed, soundness implies that $View(P,V,x)$ is accepting with small probability.

Approach to prove lemma: $V_{\bar{L}}(x)$ samples a view from $S(x)$ and asks $P_{\bar{L}}(x)$ to prove that the sample follows a distribution that is far from the case $x \in L$.

Example: from HVZK-IP for GI to IP for GNI

Consider the HVZK IP for GI and its simulator:

$P_{GI}((G_0,G_1),\sigma)$		$V_{GI}((G_0,G_1))$
sample random permutation $\varphi:[n]\to[n]$		
$H := \varphi(G_0)$	$\xrightarrow{H}$	
	$\xleftarrow{b}$	$b \leftarrow \{0,1\}$
$\psi := \varphi \circ \sigma^b$	$\xrightarrow{\psi}$	$H \stackrel{?}{=} \psi(G_b)$

$S((G_0,G_1)) :=$
1. Sample $b \leftarrow \{0,1\}$.
2. Sample random $\psi:[n]\to[n]$.
3. Compute $H := \psi(G_b)$.
4. Output $((G_0,G_1),H,b,\psi)$.

We proved that if $G_0 \equiv G_1$ then $S((G_0,G_1)) \equiv \mathrm{View}(P,V,(G_0,G_1),\sigma)$.

If $G_0 \not\equiv G_1$ then $S((G_0,G_1))$ still outputs accepting views but with a DIFFERENT distribution.

We can use this to recover the protocol for GNI (the complement of GI)!

$P_{GNI}((G_0,G_1))$		$V_{GNI}((G_0,G_1))$
		$b \leftarrow \{0,1\}$
		$\pi \leftarrow \{\text{permutations on vertices}\}$
find $\tilde{b}$ s.t.	$\xleftarrow{H}$	$H := \pi(G_b)$
$H \equiv G_{\tilde{b}}$	$\xrightarrow{\tilde{b}}$	$\tilde{b} \stackrel{?}{=} b$

V_{GNI} runs the simulator for (P_{GI},V_{GI}), and then challenges the prover to show that $G_0 \not\equiv G_1$ by asking the prover to guess the bit b. Indeed H determines b when $G_0 \not\equiv G_1$, and H is independent from b when $G_0 \equiv G_1$.

IPs with Computational Zero Knowledge

We still want zero knowledge for NP (and more). What to do?

One approach is COMPUTATIONAL ZERO KNOWLEDGE: relax the requirement on the simulator to

$\{A_x\}_{x\in S}$ and $\{B_x\}_{x\in S}$ s.t. $\forall$ poly-size circuit family $\{D_n\}_{n\in\mathbb{N}}$
$|\Pr[D_{|x|}(A_x)=1]-\Pr[D_{|x|}(B_x)=1]| = \mathrm{negl}(|x|)$

$S^{\tilde{V}}(x)$ and $\mathrm{View}(P,\tilde{V},x,w)$ are computationally close

This leads to corresponding complexity classes: HVCZK-IP & MVCZK-IP

theorem: if OWFs exist then MVCZK-IP = IP

one-way functions

We sketch a weaker result:

theorem: commitment schemes → NP $\subseteq$ MVCZK-IP

Everything Provable is Provable in Zero-Knowledge

Michael Ben-Or	Hebrew University
Oded Goldreich	Technion – Israel Institute of Technology
Shafi Goldwasser	M.I.T. Laboratory for Computer Science
Johan Håstad	Royal Institute of Technology, Sweden
Joe Kilian	M.I.T. Laboratory for Computer Science
Silvio Micali	M.I.T. Laboratory for Computer Science
Phillip Rogaway	M.I.T. Laboratory for Computer Science

Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems

ODED GOLDREICH SILVIO MICALI AND AVI WIGDERSON

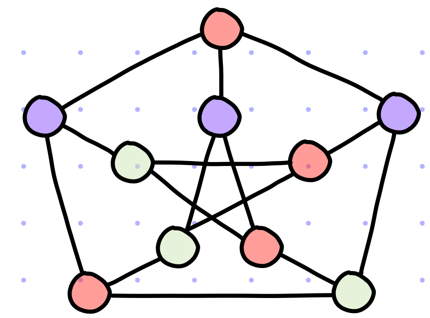
The limitations of [Goldreich Krawczyk 1990] and [Barak Lindell 2002] hold even for CZK.

Circumventing the limitations motivates the study of non-black-box universal simulators.

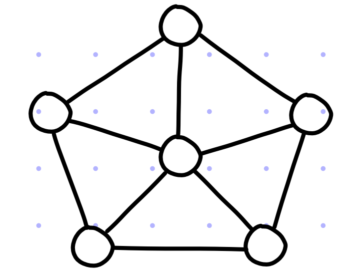
The GMW Protocol for 3COL

Consider the NP-complete 3COL (graph 3-coloring) problem:

- $\mathcal{L}_{3COL} := \{ G=(V,E) : G \text{ is a 3-colorable graph} \}$
- $\mathcal{R}_{3COL} := \{ (G,a) : a : V \to [3] \text{ is a 3-coloring of } G=(V,E) \}$
  $\forall (i,j) \in E \;\; a_i \neq a_j$



3-coloring of the Petersen graph



not 3-colorable

We study the Goldreich–Micali–Wigderson (GMW) protocol for graph 3-colorability.

It is an MVCZK-IP for $\mathcal{R}_{3COL}$. This yields MVCZK-IPs for all of NP.

Main Tool: Commitment Schemes (for simplicity, non-interactive)

A tuple CM = (CM.Commit, CM.Check) that satisfies these properties:

- **completeness**: $\forall m \in \mathcal{M} \;\; \Pr[\text{CM.Check}(cm,m,pf)=1 \mid (cm,pf) \leftarrow \text{CM.Commit}(m)] = 1$.
- **perfect binding**: $\forall cm \in \mathcal{C} \;\; |\{ m \in \mathcal{M} : \exists pf \in \mathcal{O} \text{ s.t. } \text{CM.Check}(cm,m,pf)=1 \}| = 1$.
- **computational hiding**:

computationally close

$$\forall m_0, m_1 \in \mathcal{M}, \quad \{ cm_0 \mid (cm_0,pf_0) \leftarrow \text{CM.Commit}(m_0) \} \overset{c}{\equiv} \{ cm_1 \mid (cm_1,pf_1) \leftarrow \text{CM.Commit}(m_1) \}$$

Example: El Gamal commitment scheme

$\text{CM.Setup}(1^\lambda) \to (\mathbb{G}, g, h)$

group of prime order q — random group elements in $\mathbb{G}$

$\text{CM.Commit}(m \in \mathbb{G}) \to (cm, r)$

where $cm := (g^r, m \cdot h^r) \in \mathbb{G}^2$ and r is random in $\mathbb{Z}_q$

$\text{CM.Check}(cm, m, r) :=$

$cm \overset{?}{=} (g^r, m \cdot h^r)$

Note: in every commitment scheme, hiding or binding must be computational

The GMW Protocol for 3COL

We describe the GMW protocol for graph 3-colorability.

$P(G, a: V \to [3])$

Sample random permutation $\varphi: [3] \to [3]$

Permute colors: $b := \varphi \circ a$

$\forall v \in V$, $(cm_v, pf_v) \leftarrow CM.\mathrm{Commit}(b_v)$.

$P \xrightarrow{(cm_v)_{v \in V}} V$

$P \xleftarrow{(i,j)} V$ where $(i,j) \leftarrow E$

$P \xrightarrow{(b_i, pf_i, b_j, pf_j)} V$

$V(G)$

$(i,j) \leftarrow E$

$b_i, b_j \in [3]$ $\quad b_i \neq b_j$

$CM.\mathrm{Check}(cm_i, b_i, pf_i) \stackrel{?}{=} 1$

$CM.\mathrm{Check}(cm_j, b_j, pf_j) \stackrel{?}{=} 1$

This protocol is an IP for R_{3COL}.

- completeness error $\varepsilon_c = 0$: If a is a 3-coloring of G then, for every permutation φ, b is also a 3-coloring of G. Hence, $\forall (i,j) \in E$, b_i and b_j are distinct colors in $[3]$.
- soundness error $\varepsilon_s = 1 - \frac{1}{|E|}$: Fix a malicious IP prover $\tilde{P}$. Let $(\tilde{cm}_v)_{v \in V}$ be its commitments. By perfect binding of CM, $(\tilde{cm}_v)_{v \in V}$ defines a partial coloring $\tilde{a}: V \to [3]$. Since G is not 3-colorable, $\exists (i^*, j^*) \in E$ s.t. $a_{i^*} = a_{j^*}$ (or one of a_{i^*} or a_{j^*} is undefined). If V sends (i^*, j^*) then $\tilde{P}$ cannot convince V to accept.

The GMW Protocol for 3COL

lemma: the GMW protocol for R_{3COL} satisfies CZK.

We describe the simulator and only sketch its analysis.

$P(G, a: V \to [3])$		$V(G)$
Sample random permutation $\varphi: [3] \to [3]$		
Permute colors: $b := \varphi \circ a$		
$\forall v \in V$, $(cm_v, pf_v) \leftarrow CM.\mathrm{Commit}(b_v)$.	$\xrightarrow{(cm_v)_{v \in V}}$	
	$\xleftarrow{(i,j)}$	$(i,j) \leftarrow E$
	$\xrightarrow{(b_i, pf_i, b_j, pf_j)}$	$b_i, b_j \in [3]$ $b_i \neq b_j$
		$CM.\mathrm{Check}(cm_i, b_i, pf_i) \stackrel{?}{=} 1$
		$CM.\mathrm{Check}(cm_j, b_j, pf_j) \stackrel{?}{=} 1$

Fix a 3-colorable graph G and a malicious IP verifier $\tilde{V}$.

$S^{\tilde{V}}(G) :=$
1. Sample $(i,j) \leftarrow E$.
2. Sample $b_i, b_j \leftarrow [3]$ s.t. $b_i \neq b_j$.
3. $\forall v \in V \setminus \{i,j\}$, set $b_v := 1$.
4. $\forall v \in V$, $(cm_v, pf_v) \leftarrow CM.\mathrm{Commit}(b_v)$.
5. Give $(cm_v)_{v \in V}$ to $\tilde{V}$ to get $(\tilde{\imath}, \tilde{\jmath})$.
6. If $(\tilde{\imath}, \tilde{\jmath}) \neq (i,j)$ then GOTO 1.
7. Output $(G, (cm_v)_{v \in V}, (\tilde{\imath}, \tilde{\jmath}), (b_{\tilde{\imath}}, pf_{\tilde{\imath}}, b_{\tilde{\jmath}}, pf_{\tilde{\jmath}}))$.

EASY: the output of $S^{\tilde{V}}(G)$, if it halts, follows the desired distribution.

HARD: Does $S^{\tilde{V}}(G)$ run in expected polynomial-time (or even halt)? Computational hiding of CM implies that $\tilde{V}$ cannot "force" $(\tilde{\imath}, \tilde{\jmath}) \neq (i,j)$ too often. Arguing this is delicate.

Zero Knowledge Beyond IPs

Zero Knowledge can be defined for other models of probabilistic proof.

The capabilities and limitations of zero knowledge are (very) different in each setting.

Example: zero knowledge IA

An interactive argument (IA) is an IP whose soundness is relaxed to computational soundness (consider only malicious provers that are efficient).

theorem: OWFs $\rightarrow$ NP $\subseteq$ MVZK-IA

Idea: modify the GMR protocol to use CM that is perfectly hiding & computationally binding.
Example: Pedersen commitment scheme

Example: zero knowledge MIP

A multi-prover interactive proof (MIP) is a generalization of an IP where the verifier interacts with multiple non-communicating provers.

theorem: MVZK-MIP = MIP

Multi-Prover Interactive Proofs:
How to Remove Intractability Assumptions

Michael Ben-Or* Hebrew University
Shafi Goldwasser† MIT
Joe Kilian‡ MIT
Avi Wigderson§ Hebrew University

Cryptography is replaced by a physical assumption (the provers cannot communicate).

One ingredient of the theorem: unconditional commitments in the MIP model.

Bibliography

Zero-Knowledge

- [GMR 1985]: The knowledge complexity of interactive proof-systems, by Shafi Goldwasser, Silvio Micali, Charles Rackof.
- [GMW 1991]: Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems, by Oded Goldreich, Silvio Micali, Avi Wigderson.
- [Goldreich 2010]: Zero-knowledge: a tutorial, by Oded Goldreich.
- (▸Computer scientist explains zero knowledge proofs in 5 levels of difficulty), by Amit Sahai.
- (▸History of ZK), by Shafi Goldwasser.

Power of ZK

- [BGGHKMR 1988]: Everything provable is provable in zero-knowledge, by Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, Phillip Rogaway.
- [BGKW 1988]: Multi-prover interactive proofs: how to remove intractability assumptions, by Michael Ben-Or, Shafi Goldwasser, Joe Kilian, Avi Wigderson.

Limitations of ZK

- [Fortnow 1987]: The complexity of perfect zero-knowledge, by Lance Fortnow.
- [AH 1987]: Perfect zero-knowledge languages can be recognized in two rounds, by William Aiello, Johan Håstad.
- [GO 1994]: Definitions and properties of zero-knowledge proof systems, by Oded Goldreich, Yair Oren.
- [GK 1998]: On the composition of zero-knowledge proof systems, by Oded Goldreich, Hugo Krawczyk.
- [BL 2002]: Strict polynomial-time in simulation and extraction, by Boaz Barak, Yehuda Lindell.