WITNESS-INDISTINGUISHABILITY and SZK ARGUMENTS for NP

ALON ROSEN **IDC HERZLIYA**

fact FOUNDATIONS & APPLICATIONS of CRYPTOGRAPHIC THEORY

BIU WINTER SCHOOL | February 2019

Statistical Zero-Knowledge

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

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

$$\mathrm{PZK} \quad \subseteq \quad \mathrm{SZK} \quad \subseteq \quad \mathrm{CZK}$$

Recall: If $\mathrm{NP} \subseteq SZK$ then the polynomial-time hierarchy collapses to the second level

Possible relaxations:

- Computational indistinguishability (previous lectures)
- Computational soundness (now)

Interactive Argument Systems

Definition [BCC'86]: An interactive argument system for L is a PPT algorithm V and a function P such that $\forall x$:

Completeness: If $x \in L$, then $Pr[(P,V) \text{ accepts } x] = 1$

Computational soundness: If $x \notin L$, then $\forall PPT\ P^*$

$$Pr[(P^*,V) \text{ accepts } x] \leq neg(n)$$

- Computational soundness is typically based on a cryptographic assumption (e.g. CRH)
- Hardness of breaking the assumption is parametrized by security parameter n
- Independent parallel repetitions do not necessarily reduce the soundness error [BIN'97]

CZK Proofs vs SZK Arguments

CZK Proofs

- **Soundness is unconditional (undisputable)**
- **Secrecy is computational - suitable when secrets are ephemeral and "environment" is not too powerful**

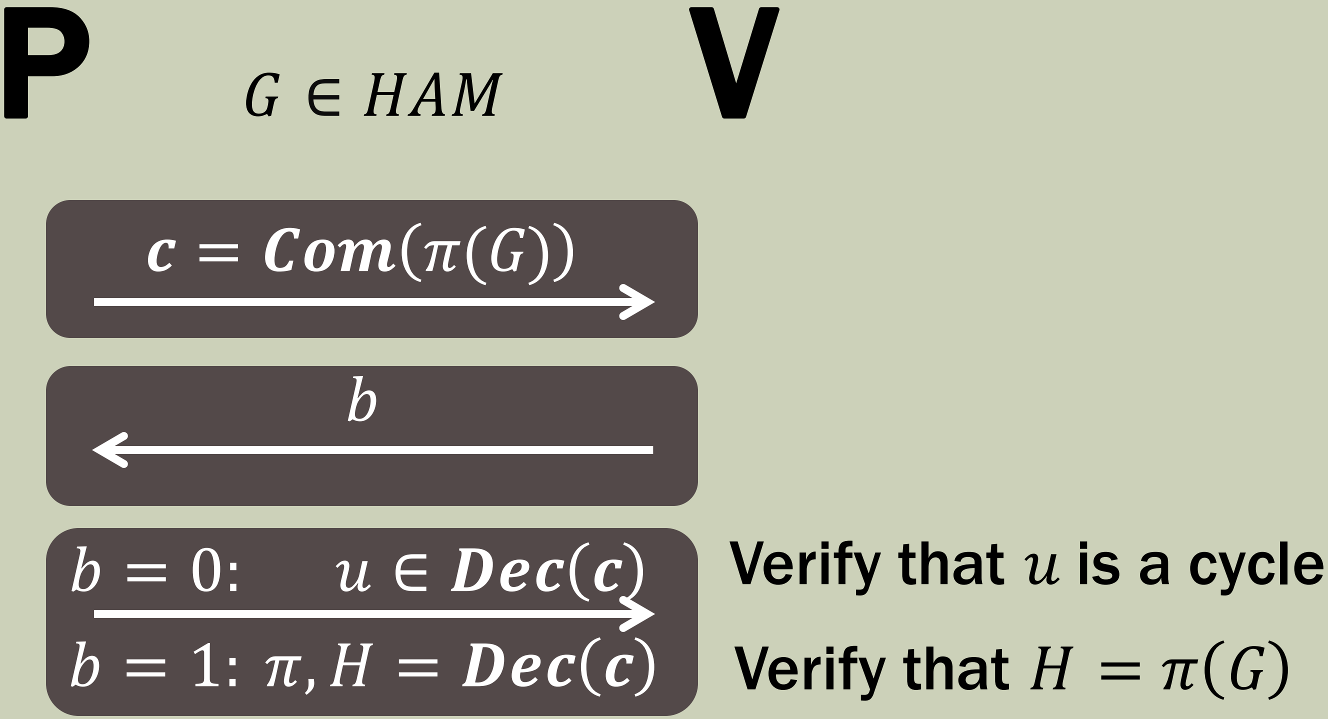
SZK Arguments

- **Secrecy is unconditional (everlasting)**
- **Soundness is computational – suitable when prover is a weak device and no much time for preprocessing**

$\mathrm{NP} \subseteq \mathit{S}\mathrm{ZK}$ **arguments**

Statistical ZK argument for HAM

Theorem: If statistically-hiding commitments exist then there exists an SZK argument for HAM



P $G \in HAM$ **V**

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

$$\xleftarrow{b}$$

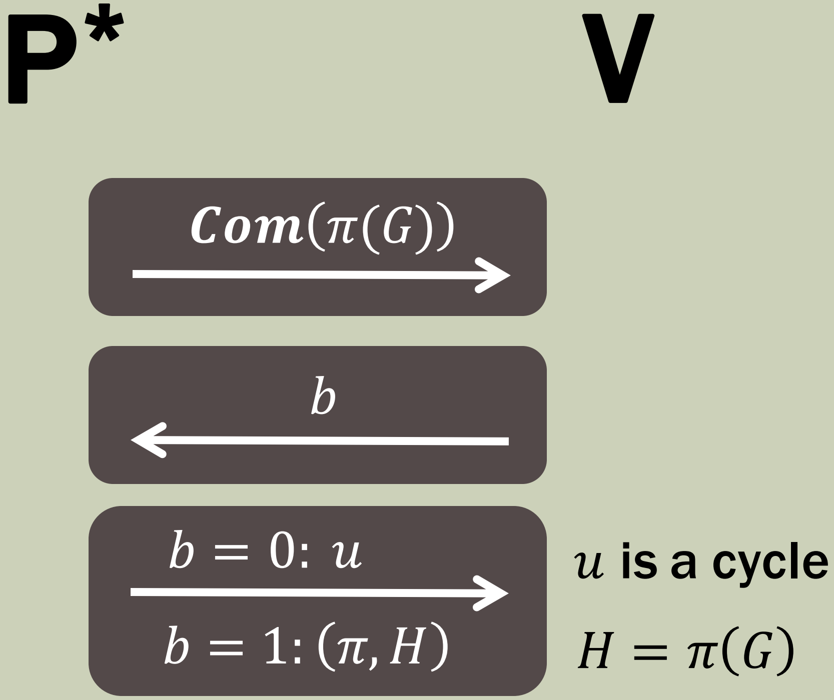
$b = 0$: $u \in \boldsymbol{Dec}(\boldsymbol{c})$ Verify that u is a cycle

$$\longrightarrow$$

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

Computational Soundness

Claim: If $(\boldsymbol{Com}, \boldsymbol{Dec})$ is computationally binding then (P, V) is an interactive argument for HAM



P*

V

$\boldsymbol{Com}(\pi(G))$ $\longrightarrow$

b $\longleftarrow$

$b = 0$: u $\longrightarrow$ $b = 1$: (π, H)

u is a cycle

$H = \pi(G)$

Computational soundness:

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

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

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

Case 2: u not consistent with (π, H)

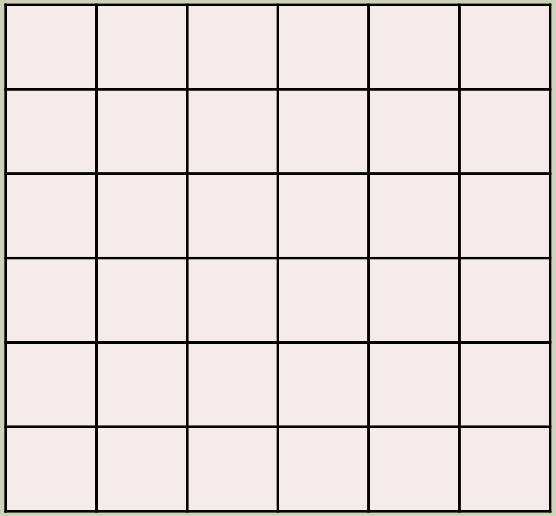
↓

$PPT\ P^*$ breaks binding of $\boldsymbol{Com}$

Statistical ZK

$\underline{S^{V^*}(G)|\ b\ =\ 0}$

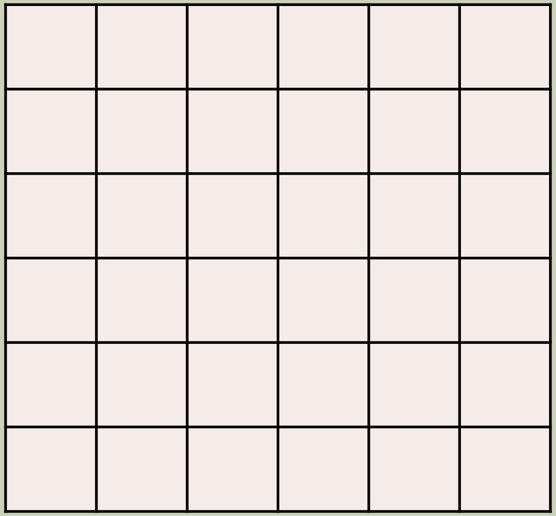
$\boldsymbol{c} = Com(G_0)$



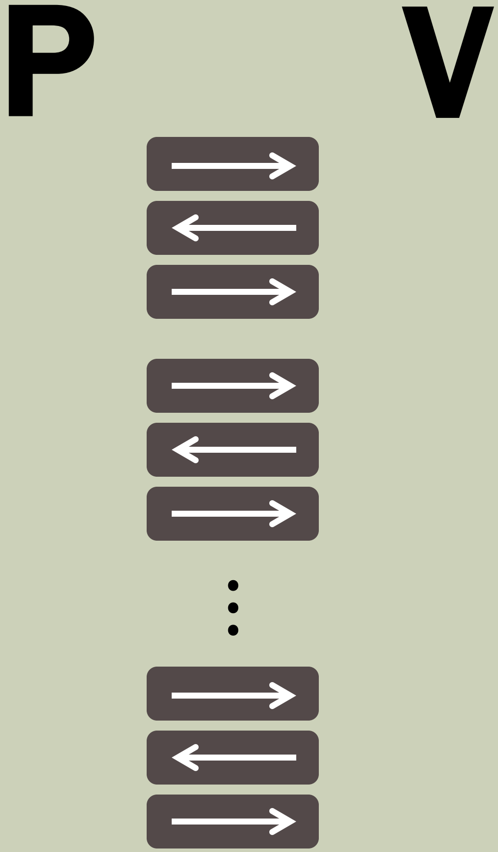
$\cong_s$

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

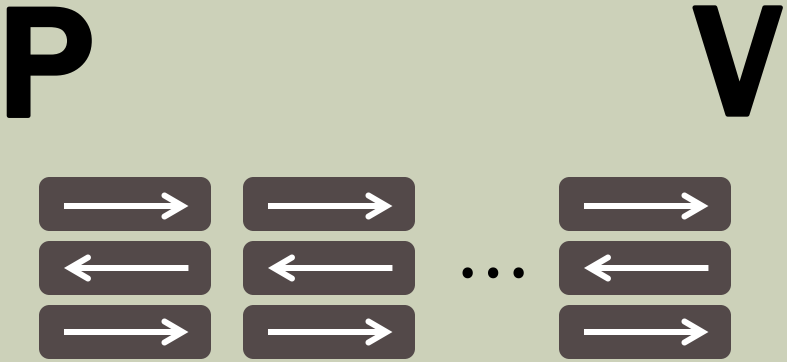
$\boldsymbol{c} = Com(G_1)$



Amplifying soundness



- Negligible soundness
- High round complexity
- ZK



- Negligible soundness
- Low round complexity
- ZK?

Witness Indistinguishability

The Goal

Goal: construct argument for every $L \in \mathrm{NP}$

- in statistical ZK
- with negligible soundness
- and a constant number of rounds

Main tool: witness indistinguishability

Witness-Indistinguishability

An extremely useful (and meaningful) relaxation of ZK

The interaction does not reveal which of the NP-witnesses for $x \in L$ was used in the proof

Witness-indistinguishable: $\forall w_1, w_2$

$$(P(w_1), V^*)(x) \cong_c (P(w_2), V^*)(x)$$

Witness independent: $\forall w_1, w_2$

$$(P(w_1), V^*)(x) \cong_s (P(w_2), V^*)(x)$$

Defined with respect to some NP-relation R_L

NP -Witnesses and NP -Relations

$L \in \mathrm{NP}$ if $\exists$poly-time recognizable relation R_L so that

$$x \in L \Leftrightarrow \exists w,\ (x, w) \in R_L$$

Define the "set of NP-witnesses for $x \in L$"

$$R_L(x) = \{w \mid (x, w) \in R_L\}$$

$$= \{w \mid V(x, w) = \text{ACCEPT}\}$$

- $R_L(x)$ is fully determined by R_L (equivalently, by V)
- $L \in \mathrm{NP}$ can have many different NP-relations R_L

Witness-Indistinguishability

Definition [FS'90]: (P,V) is **witness indistinguishable** wrt NP-relation R_L if $\forall PPT\ V^*\ \forall x \in L\ \forall w_1, w_2 \in R_L(x)$

$$(P(w_1), V^*)(x) \cong_c (P(w_2), V^*)(x)$$

- **Holds trivially (and hence no security guarantee) if there is a unique witness w for $x \in L$**
- **Interesting (and useful) whenever more than one w**
- **Holds even if w_1, w_2 are public and known**

- **Every ZK proof/argument is also WI**
- **WI is closed under parallel/concurrent composition**

An Equivalent Definition

Unbounded simulation: $\forall PPT\ V^* \ \exists S \ \forall x \in L$

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

Claim: (P, V) **has unbounded simulation iff it is** WI

Proof:

$(\Rightarrow)$ $(P(w_1), V^*)(x) \cong_c S(x) \ \cong_c (P(w_2), V^*)(x)$

$(\Leftarrow)$ **Exercise**

ZK implies WI

Claim: If (P, V) is ZK then it is also WI

Proof: $(P(w_1), V^*)(x) \cong_c S(x) \cong_c (P(w_2), V^*)(x)$

Corollary: If statistically-binding commitments exist then every $L \in \mathrm{NP}$ has a witness-indistinguishable proof

Proof: (P, V) for HAM is CZK and so, by claim above, it is also witness-indistinguishable

Analogously,

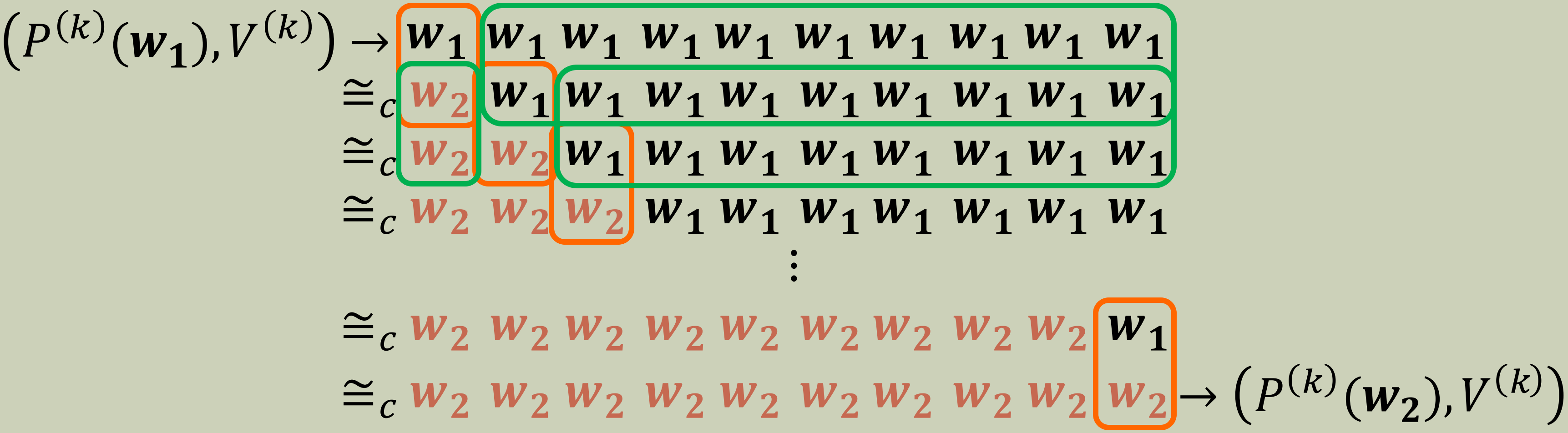
Corollary: If statistically-hiding commitments exist then every $L \in \mathrm{NP}$ has a witness-independent argument

WI is Closed under Parallel Composition

Let $\left(P^{(k)},V^{(k)}\right)$ denote k parallel executions of (P,V)

Theorem: If (P,V) is WI then $\left(P^{(k)},V^{(k)}\right)$ is also WI

Hybrid argument (w_1, w_2 are known):



$$\left(P^{(k)}(\mathbf{w_1}),V^{(k)}\right) \rightarrow \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}$$

$$\cong_c \mathbf{w_2}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}$$

$$\cong_c \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}$$

$$\cong_c \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}\ \mathbf{w_1}$$

$$\vdots$$

$$\cong_c \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_1}$$

$$\cong_c \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2}\ \mathbf{w_2} \rightarrow \left(P^{(k)}(\mathbf{w_2}),V^{(k)}\right)$$

CONSTANT-ROUND WI FOR NP

Theorem: Assuming non-interactive statistically-binding commitments, every $L \in \mathrm{NP}$ has a 3-round witness-indistinguishable *proof* with soundness error 2^{-k}

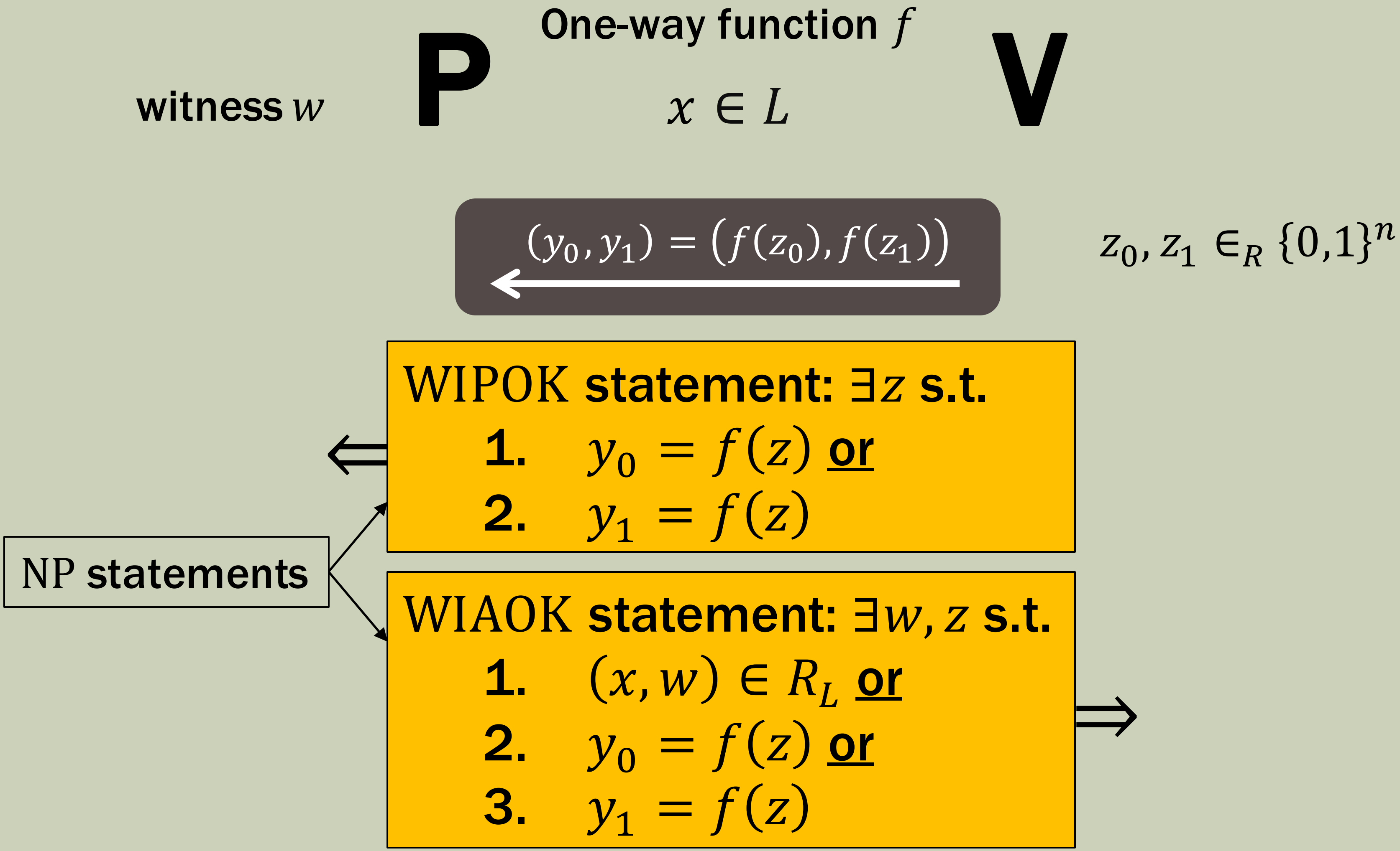
Theorem: Assuming 2-round statistically-hiding commitments, every $L \in \mathrm{NP}$ has a 4-round witness-independent *argument* with soundness error $exp(-O(k))$

- The protocols are in fact proofs of knowledge
- We will use them to construct
  - a **5**-round SZK argument (of knowledge) for NP
  - a constant-round identification scheme

both with soundness error $exp(-O(k))$

Constant-Round $\mathcal{SZK}$ Arguments for $\mathcal{NP}$

Statistical ZK argument for NP [FS'90]



One-way function f

witness w **P** $x \in L$ **V**

$(y_0, y_1) = (f(z_0), f(z_1))$ ←

$z_0, z_1 \in_R \{0,1\}^n$

$\Leftarrow$ WIPOK **statement:** $\exists z$ **s.t.**

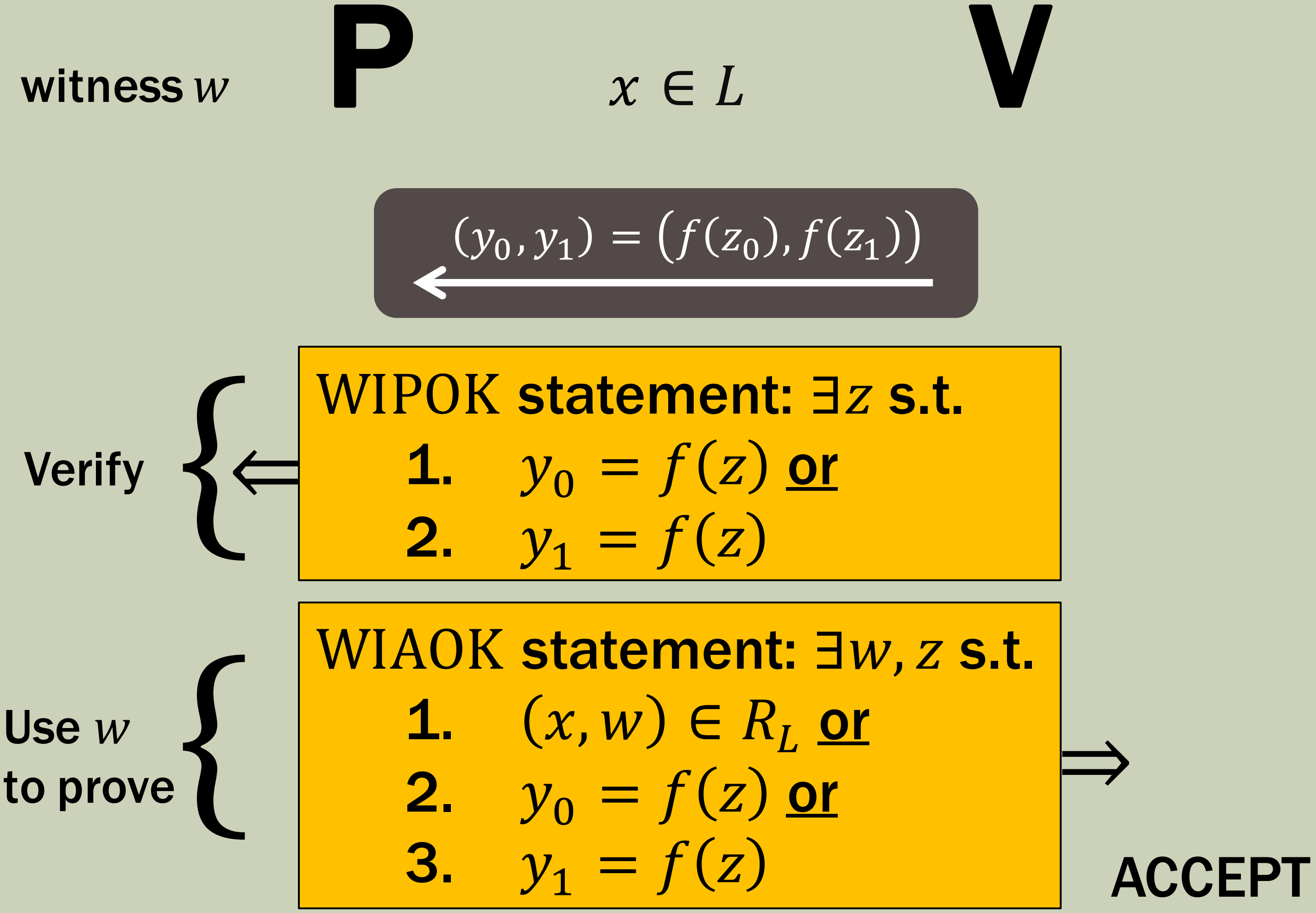
1. $y_0 = f(z)$ **or**
2. $y_1 = f(z)$

NP **statements**

WIAOK **statement:** $\exists w, z$ **s.t.** $\Rightarrow$

1. $(x, w) \in R_L$ **or**
2. $y_0 = f(z)$ **or**
3. $y_1 = f(z)$

Completeness



witness w **P** $x \in L$ **V**

$(y_0, y_1) = \big(f(z_0), f(z_1)\big)$

Verify { ⟸

WIPOK **statement:** $\exists z$ **s.t.**

1. $y_0 = f(z)$ **or**
2. $y_1 = f(z)$

Use w to prove {

WIAOK **statement:** $\exists w, z$ **s.t.**

1. $(x, w) \in R_L$ **or**
2. $y_0 = f(z)$ **or**
3. $y_1 = f(z)$

⟹ **ACCEPT**

Soundness/POK

P* $x \notin L$ **V**

Given to V:

$y_b = f(\boldsymbol{z_b})$

Sampled by V:

$y_{1-b} = f(z_{1-b})$

$\xleftarrow{(y_0, y_1) = (f(z_0), f(z_1))}$

WIPOK **statement:** $\exists z$ **s.t.**

1. $y_0 = f(z)$ **or**
2. $y_1 = f(z)$

Cannot guess b $\Leftarrow$ WIPOK statement

Use z_{1-b} **to prove**

WIAOK **statement:** $\exists w, z$ **s.t.**

1. $\xcancel{(x, w) \in R_L}$ **or**
2. $y_0 = f(z)$ **or**
3. $y_1 = f(z)$

$\Rightarrow$ **Extract** z_{ext}

$\downarrow$

$y_0 = f(z_{\text{ext}})$ **or**
$y_1 = f(z_{\text{ext}})$

SOUNDNESS/POK

Claim: If POK is witness indistinguishable then $\forall PPT\ P^*$

$$Pr_b[f(z_{\text{ext}}) = y_b] \approx 1/2$$

Exercise: otherwise P^* distinguishes between

$$(V(z_b), P^*)(y_0, y_1) \text{ and } (V(z_{1-b}), P^*)(y_0, y_1)$$

- If $f(z_{\text{ext}}) = y_b$ then z_{ext} is a preimage of $y_b = f(\boldsymbol{z_b})$
- So if P^* cheats w.p. ε we invert y_b w.p. $\approx \varepsilon/2$
- Thus, if f is one-way, P^* makes V accept $x \notin L$ with $neg(n)$ probability

ZERO-KNOWLEDGE

Simulator S $x \in L$ **V***

$$\xleftarrow{(y_0, y_1) = \left(f(z_0), f(z_1)\right)}$$

Extract z $\Leftarrow$

WIPOK **statement: $\exists z$ s.t.**

1. $y_0 = f(z)$ **or**
2. $y_1 = f(z)$

Use z
to prove

WIAOK **statement: $\exists w, z$ s.t.**

1. $(x, w) \in R_L$ **or**
2. $y_0 = f(z)$ **or**
3. $y_1 = f(z)$

$\Rightarrow$ Cannot
distinguish
if 1,2 or 3

Zero-Knowledge

Claim: If AOK is witness independent then $\forall PPT\ V^*$

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

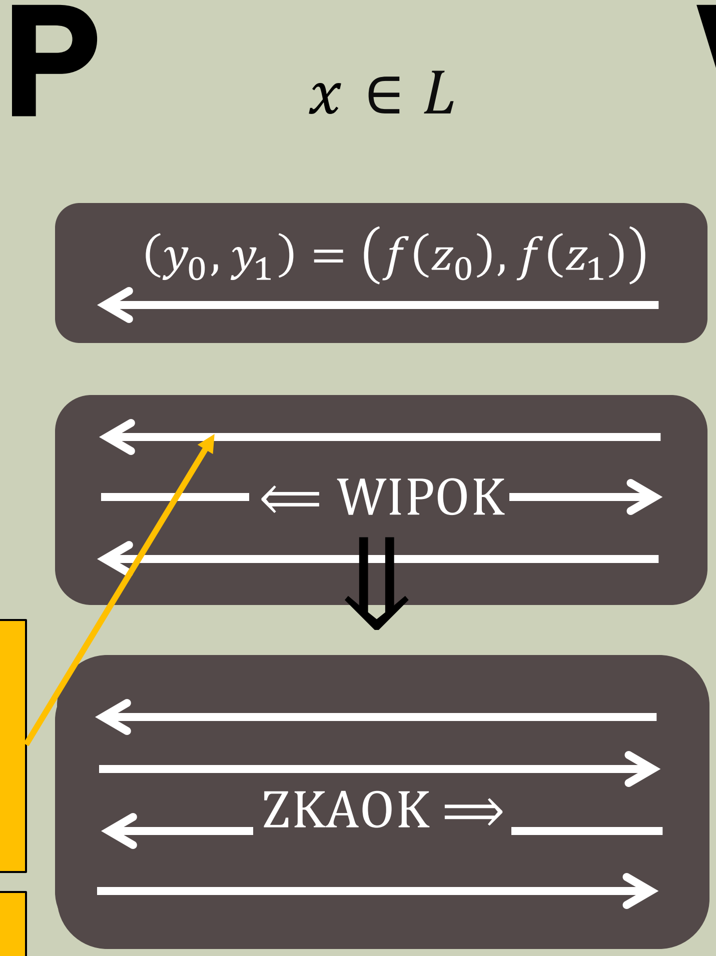
Exercise: otherwise build $\widehat{V}^*$ for AOK using V^* and then distinguish between

$$\left(P(w), \widehat{V}^*\right)(x, y_0, y_1) \text{ and } \left(P(z), \widehat{V}^*\right)(x, y_0, y_1)$$

Hint: $\widehat{V}^*$ relays WIPOK messages between V^* and P

Corollary: If 2-round statistically-hiding commitments exist then every $L \in \mathrm{NP}$ has a constant-round SZK argument

Towards 4-rounds?



An issue: in simulation can set 2nd message of WIAOK only after z_b is extracted from WIPOK

In order to get 4-rounds more ideas are required [FS’89, BJY’97]

Trapdoor commitments:

$$\boldsymbol{Com}_{g,h}(m,r) = h^r \cdot g^m$$

If $\log_g h$ is known, can decommit to any (m', r')

$+$

Witness hiding: infeasible for V^* to output witness following the interaction

Summary so far

Defined:

- **Interactive arguments**
- **Statistically-hiding commitments**
- **Witness indistinguishability/independence**

Saw:

- $\mathrm{NP} \subseteq \mathit{S}\mathrm{ZK}$ **arguments**
- ZK **implies** WI **(and hence** $\mathrm{NP} \subseteq \mathrm{WI}$**)**
- WI **composes (and hence negligible error)**
- $\mathrm{NP} \subseteq \mathit{S}\mathrm{ZK}$ **in constant number of rounds**

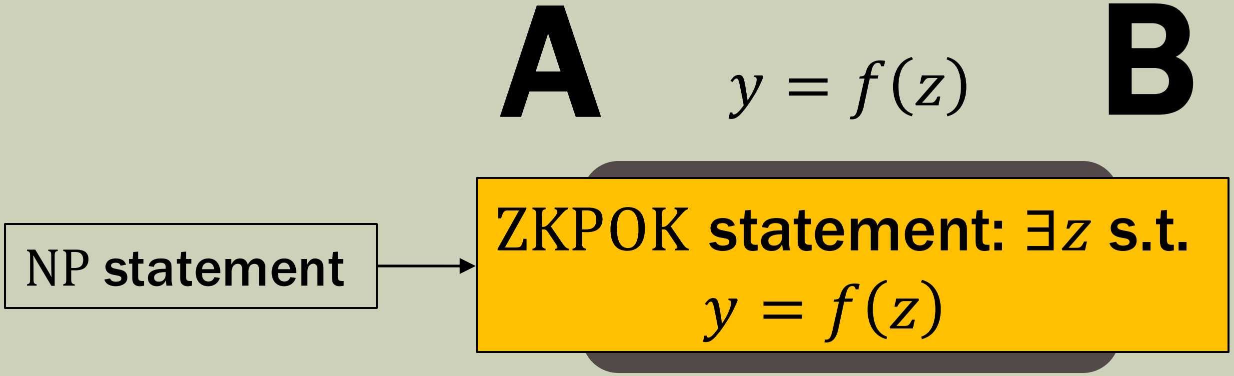
Witness Hiding

Identification using a ZKPOK

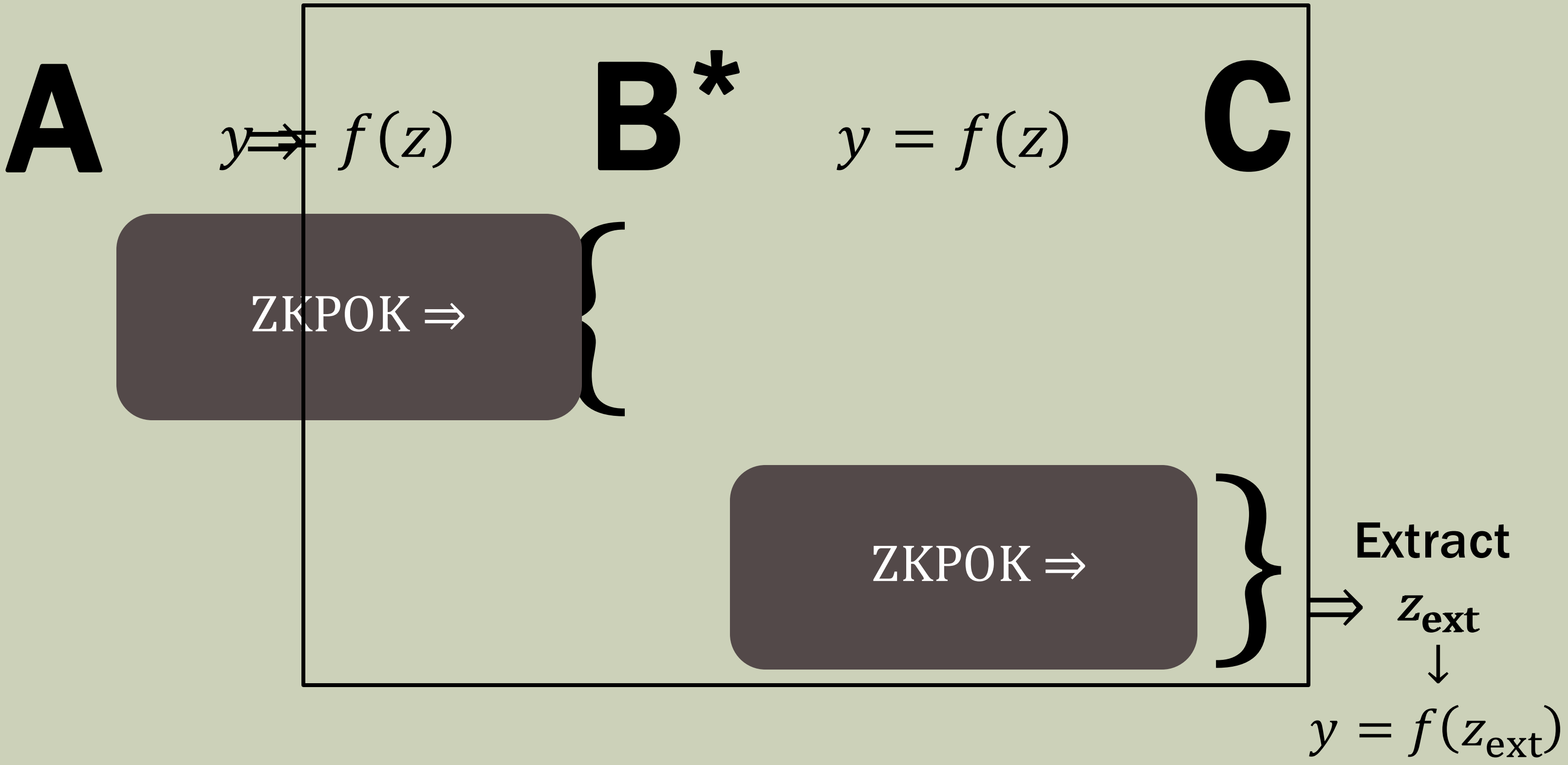
Setup phase (f is a one-way function):

$Gen(1^n)$: Alice picks $z \in_R \{0,1\}^n$ and publishes $y = f(z)$

Identification phase:



Bob cannot impersonate Alice



A

$y \Rightarrow f(z)$

B^*

$y = f(z)$

C

ZKPOK ⇒

ZKPOK ⇒

Extract

$\Rightarrow z_{\mathbf{ext}}$

$\downarrow$

$y = f(z_{\mathrm{ext}})$

- **Use constant-round** ZKPOK **with** $neg(n)$ **error**
- **<u>Observation</u>: “witness hiding” is sufficient**

Identification using a WHPOK

Setup phase:

$Gen(1^n)$: **Alice picks** $z_0, z_1 \in_R \{0,1\}^n$ **and publishes**

$$(y_0, y_1) = \left(f(z_0), f(z_1)\right)$$

Identification phase:

A (y_0, y_1) **B**

WIPOK **statement:** $\exists z$ **s.t.**

1. $y_0 = f(z)$ **or**
2. $y_1 = f(z)$

We already saw: if proof is WI **and** f **is a OWF then a** $PPT\ B^*$ **cannot output** z **following the interaction**

Witness Hiding

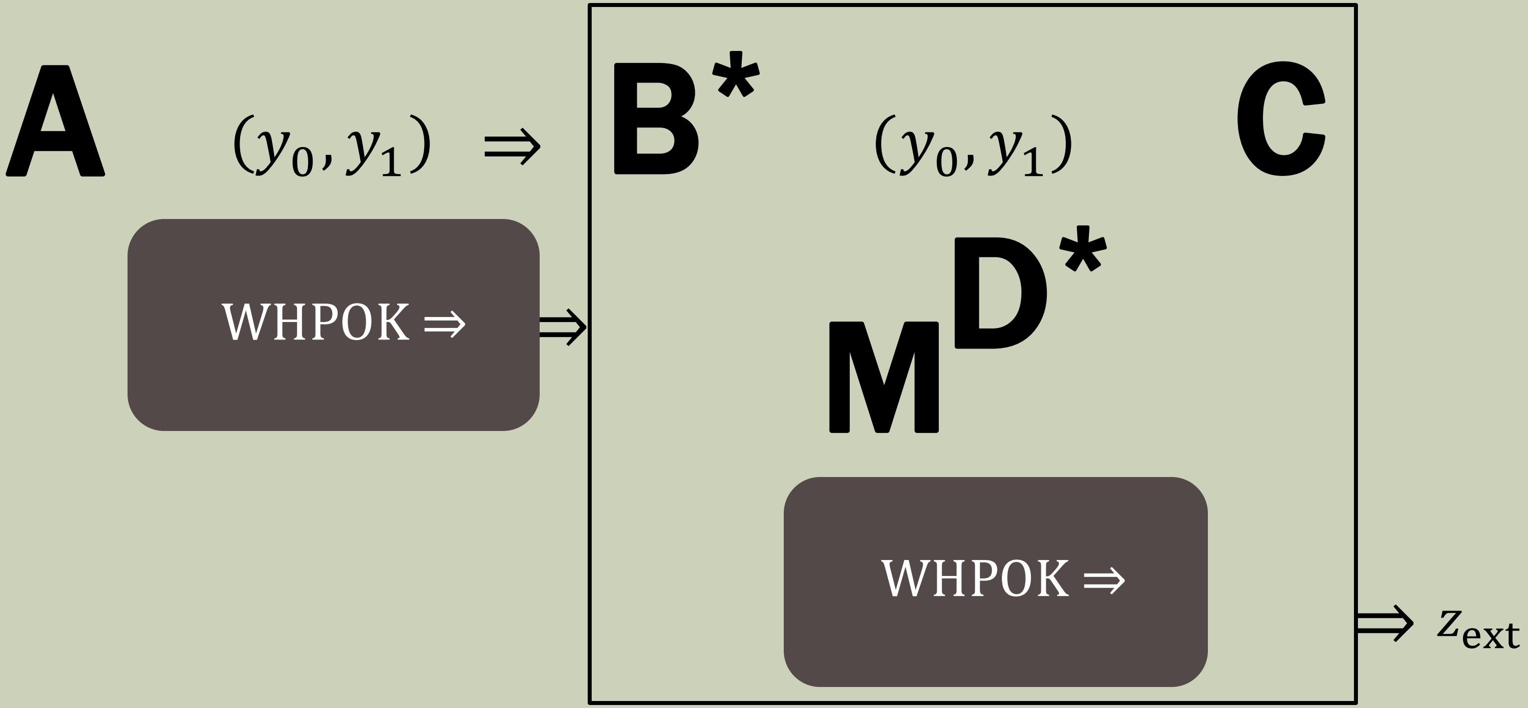
- If V^* can output a witness $w \in R_L(x)$ following the interaction with P he could have done so without it
- WH is implied by ZK but does not necessarily imply ZK
- Defined with respect to an instance generator Gen for R_L

Definition [FS'90]: (P, V) is witness hiding with respect to (Gen, R_L) if $\exists PPT\ M\ \forall PPT\ V^*$

$$Pr[(P(w), V^*)(x) \in R_L(x)] \leq Pr\left[M^{V^*}(x) \in R_L(x)\right] + neg(n)$$

Claim: If an NP-statement $x \in L$ has two independent witnesses then any WI protocol for $x \in L$ is also WH

Bob cannot impersonate Alice



- D^* **interacts with A and outputs a witness** z_{ext} **for** (y_0, y_1)
- **By witness hiding,** $M^{D^*}(y_0, y_1)$ **outputs a witness for** (y_0, y_1)
- **<u>Exercise</u>: use** M^{D^*} **to invert the one-way function** f

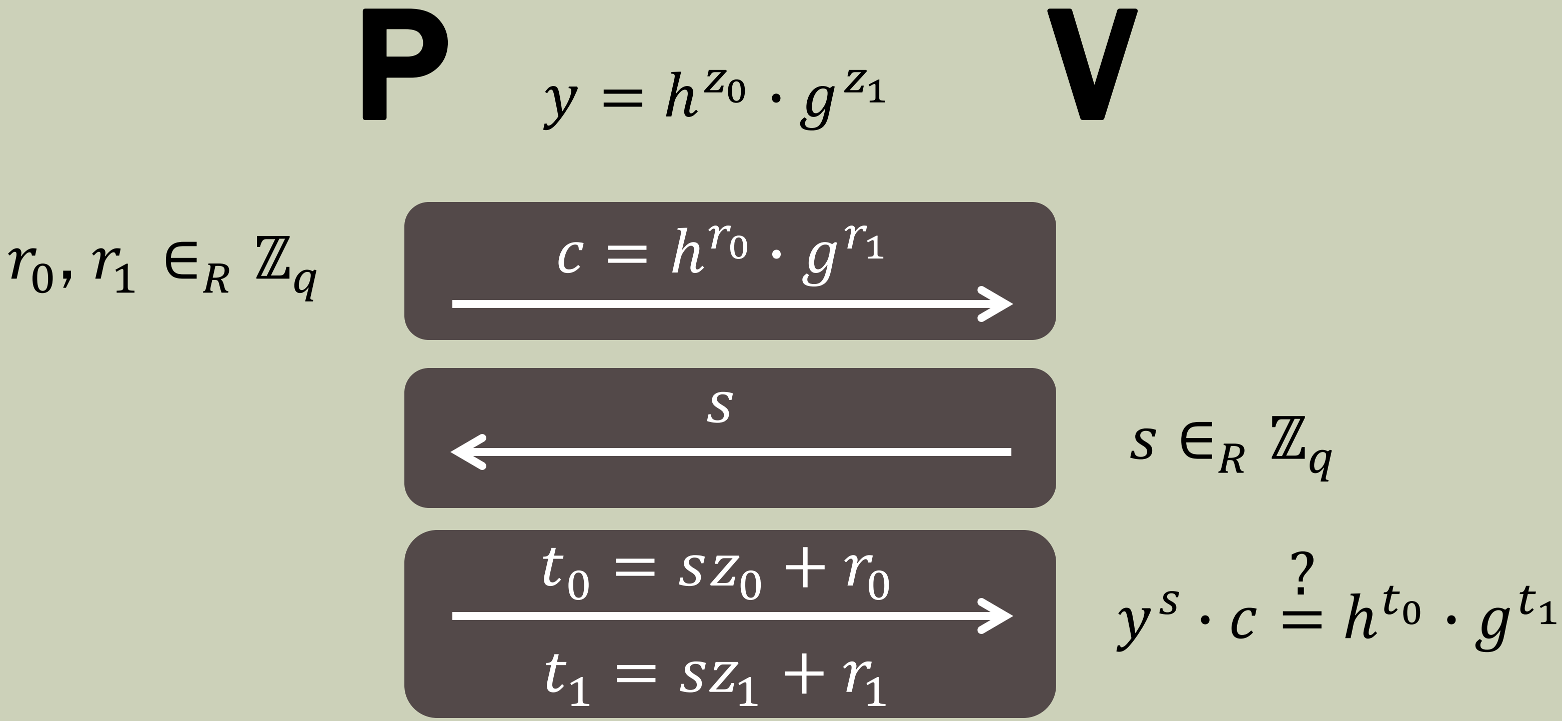
The Fiat-Shamir Identification Scheme

- Repeat the QR_N protocol k times in parallel
- Single execution is ZK and so is WI
- Single execution is WI and so k executions are WI
- k executions are WI with multiple independent witnesses and so are WH with error 2^{-k}
- This gives an identification scheme based on the hardness of finding a square root of

$$x = w^2 \ mod \ N$$

- Recent [CCHLRRW'19, PS'19]: k parallel repetitions of QR_N protocol are not ZK (under plain LWE)

Okamoto's protocol



P $y = h^{z_0} \cdot g^{z_1}$ **V**

$r_0, r_1 \in_R \mathbb{Z}_q$ $\xrightarrow{c = h^{r_0} \cdot g^{r_1}}$

$\xleftarrow{s}$ $s \in_R \mathbb{Z}_q$

$\xrightarrow[t_1 = sz_1 + r_1]{t_0 = sz_0 + r_0}$ $y^s \cdot c \overset{?}{=} h^{t_0} \cdot g^{t_1}$

- **witness independent with soundness error** $1/q$
- **<u>and</u> each** y **has** q **witnesses** $(z_0, z_1) \in \mathbb{Z}_q^2$
- **so the protocol is witness hiding**

Summary

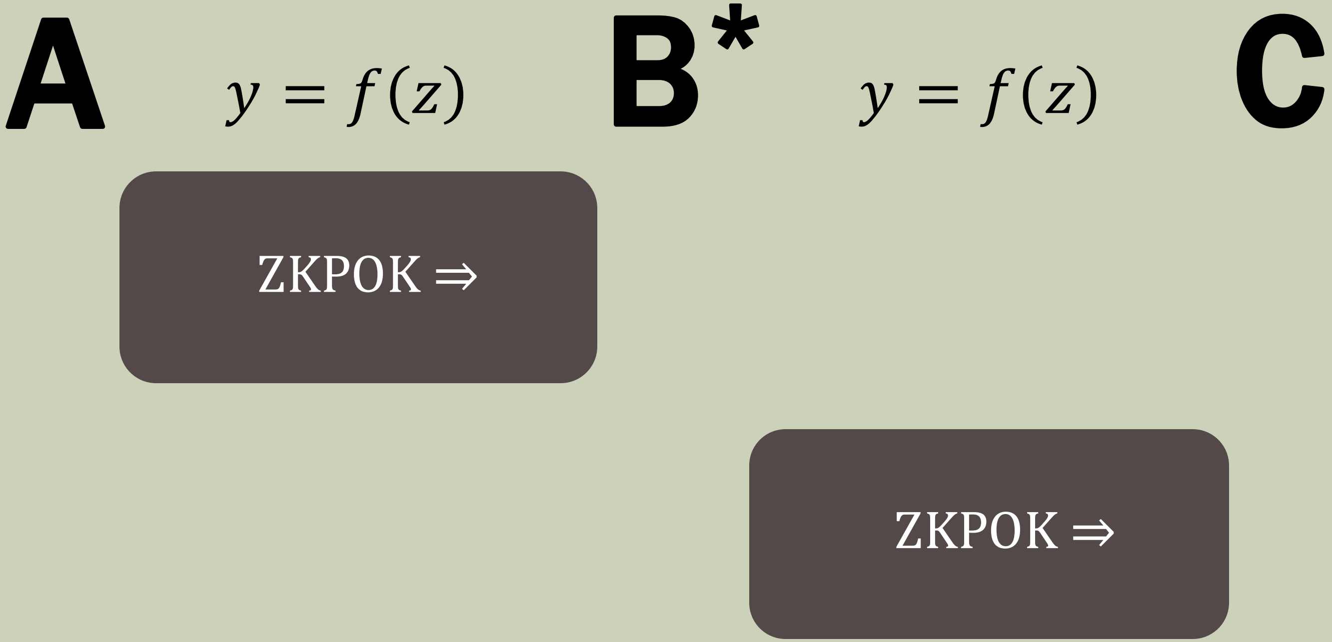
Defined:

  - Interactive arguments
  - Statistically-hiding commitments
  - Witness indistinguishability/independence
  - Witness hiding

- Saw:
  - $\mathrm{NP} \subseteq \mathcal{SZK}$ arguments
  - ZK implies WI and WI composes
  - $\mathrm{NP} \subseteq \mathcal{SZK}$ in constant number of rounds
  - Identification schemes via ZK and via WH

Food for Thought

Man-in-the-middle Attacker



A $y = f(z)$ **B*** $y = f(z)$ **C**

$\mathrm{ZKPOK} \Rightarrow$

$\mathrm{ZKPOK} \Rightarrow$

- **What if both ZKPOKs take place at the same time?**
- **Both proof of security <u>and</u> real-life security fail**
- **Must address man-in-the-middle explicitly**

Zero Knowledge vs WI and WH

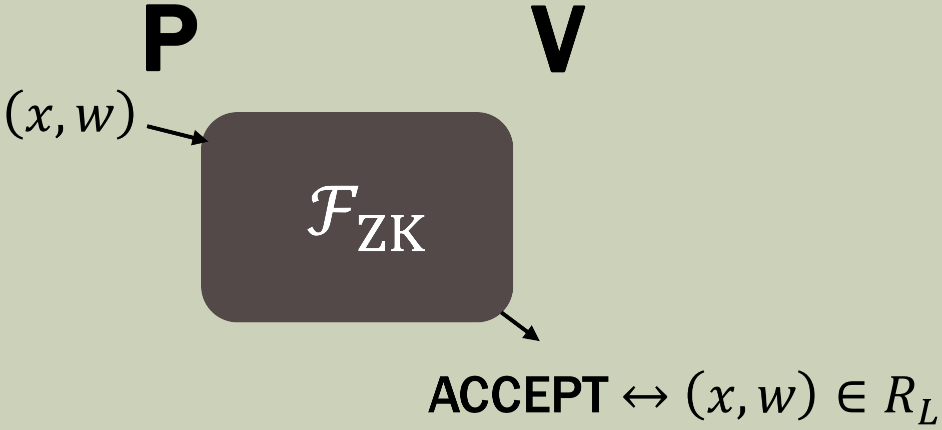
Encryption:

semantic security ↔ indistinguishability of encryptions

Protocols:

witness indistinguishability ← zero knowledge

- Unlike WH both ZK and WI compose
- ZK leaks nothing → modular protocol design
- ZKPOK functionality:



P

V

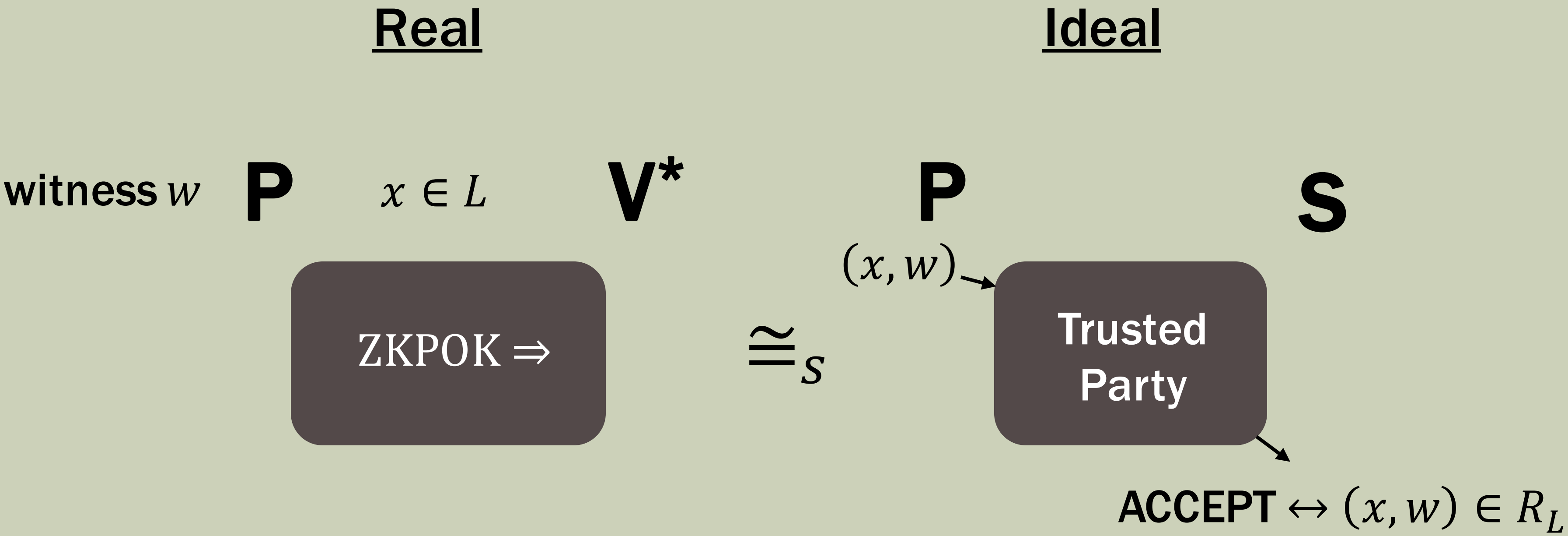
(x, w)

$\mathcal{F}_{\mathrm{ZK}}$

ACCEPT ↔ $(x, w) \in R_L$

ZK via Real/Ideal Paradigm

Real/ideal paradigm: ∀Real $PPT\ V^*$ ∃Ideal $PPT\ S$



Real

Ideal

witness w **P** $x \in L$ **V***

ZKPOK ⇒

$\cong_S$

P **S**

(x, w)

Trusted Party

ACCEPT $\leftrightarrow (x, w) \in R_L$

- **Special case of two-party computation**
- V **has no input (binary output) and** P **has no output**

History

Uriel Feige

Adi Shamir

Amos Fiat

Gilles Brassard

David Chaum

Claude Crépeau

Mihir Bellare

Russell Impagliazzo

Tatsuaki Okamoto

The End

Questions?