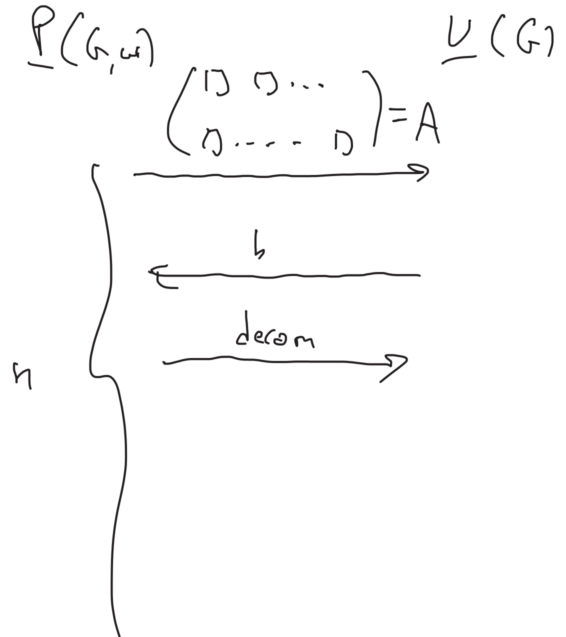
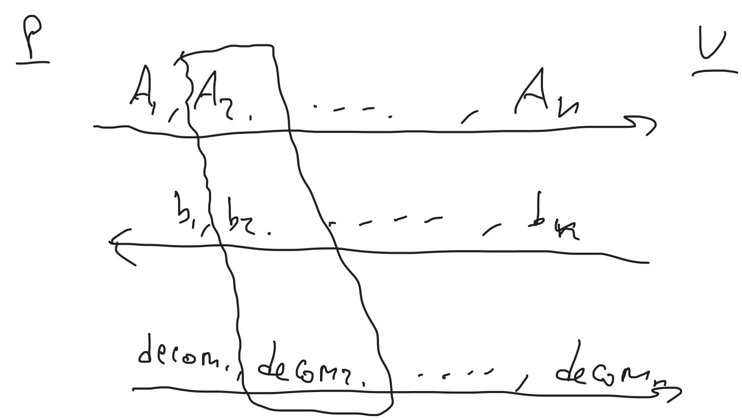
- Scribes?
- lecture recording

- 3-round WI-PoK
- Goldreich-Kahan protocol
- Feige-Shamir protocol



parallel repetition:



We do not know how to prove it ZK.
It is a PoK

KE(G)

- run an honest interaction w/ P^*; let challenge be $\vec{b}$
- if interaction fails, stop
- otherwise, set $\vec{b}'' = 0^n$ and do:
    - $\vec{b}' \leftarrow \{0,1\}^n$
    - if $P^*(\vec{b}')$ succeeds & $\vec{b}' \neq \vec{b}$, break
    - if $P^*(\vec{b}'')$ succeeds & $\vec{b}'' \neq \vec{b}$, break
    - if $\vec{b}'' = 1^n$, break

- increment "$\tilde{b}$"
- Given two successful executions for distinct challenges, compute w

---

Let ε denote the prob. that P^* succeeds

Claim

If $\varepsilon > 1/2^n$ then KE computes a witness w/ prob. ε

Claim

KE runs in expected polynomial time

Proof

$\Pr[\text{KE enters the loop}] = \varepsilon$

if $\varepsilon = k/2^n$, $k > 1$

Expected # of iterations $= \frac{k}{2^n} \cdot \frac{2^n}{k-1} \leq 2$

if $\varepsilon = 1/2^n$

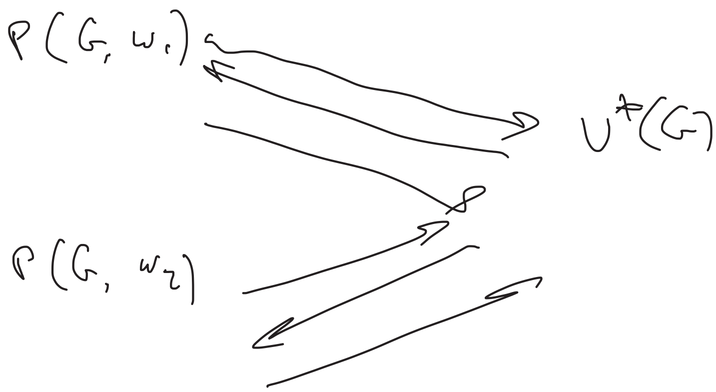
Expected # of iterations $= \frac{1}{2^n} \cdot 2^n = 1$ $\boxed{\checkmark}$

$\Rightarrow$ this is a PoK

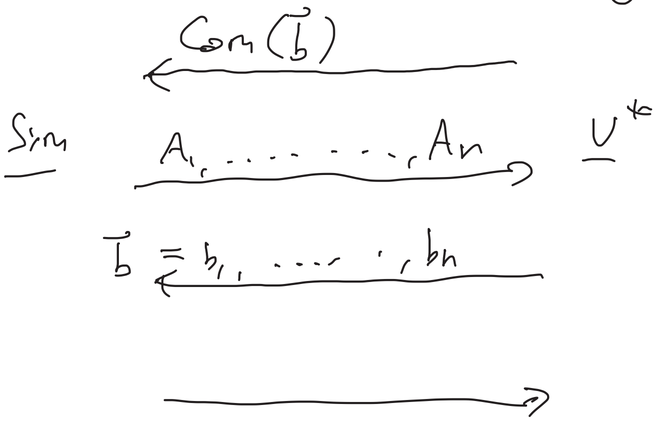
Witness indistinguishability (WI)

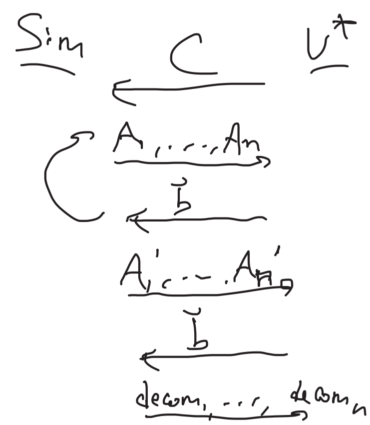
- Cheating V^* cannot distinguish which of two possible witnesses P is using

$ZK \Rightarrow WI$

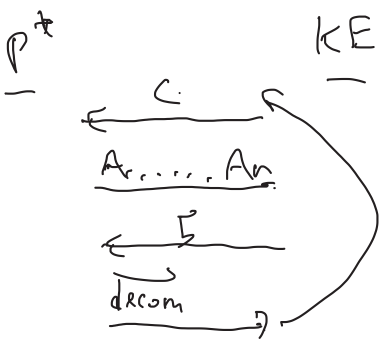


Goldreich-Kahan





Goldreich-Kahan protocol is ZK



Goldreich-Kahan is not known to be a PoK

Feige-Shamir

$x \in L$ for some $L \in NP$

$P(x, w)$

V

$x_1, x_2 \leftarrow \{0,1\}^n$

$y_1 = f(x_1)$, $y_2 = f(x_2)$

f is a one-way function

$\xleftarrow{y_1, y_2}$

WI-PoK : $\exists\, b, x_b$ s.t. $f(x_b) = y_b$

WI-PoK :

$L_2 : x \in L \vee (\exists\, b, x_b \text{ s.t. } y_b = f(x_b))$

Sim

V^*

ZK

$\xleftarrow{y_1, y_2}$

PoK

run KE, extract b, x_b

run WI-PoK WI using b, x_b

PoK

P^*

KE

$\xleftarrow{y_1, y_2}$

$x_1, x_2 \leftarrow \{0,1\}^n$

$y_1 = f(x_1)$, $y_2 = f(x_2)$

WI-PoK

WI-PoK

- run KE' to extract a witness w
- output w

$\Pr[\text{KE outputs a witness for } L_2] = \Pr(P^* \text{ succeeds}) = \varepsilon$

$\Pr(\text{KE outputs a witness then } x \in L) = \varepsilon_1$

$\Pr(\text{KE outputs } x_1 : f(x_1) = y_1) = \varepsilon_2$

$\Pr(\text{KE outputs } x_2 : f(x_2) = y_2) = \varepsilon_3$

these are negligible

Assume toward contradiction that KE' extracts a preimage of y_1 w.h.p.

$\underline{P^*}$ $\underline{KE}(y_1)$

y_1, y_2

$x_2 \leftarrow \{0,1\}^n$

$y_2 = f(x_2)$

WI-PoK

WI-PoK KE' extracts a preimage of $\cancel{y}_1$

$\underline{P^*}$ $\underline{KE}$

y_1, y_2

WI-PoK using x_1

WI-PoK using x_1

run KE', get x_1

$\underline{P^*}$ $\underline{KE}$

y_1, y_2

WI-PoK using x_2

WI-PoK using x_2

run KE', get x_1

$\mathcal{E}_2'$