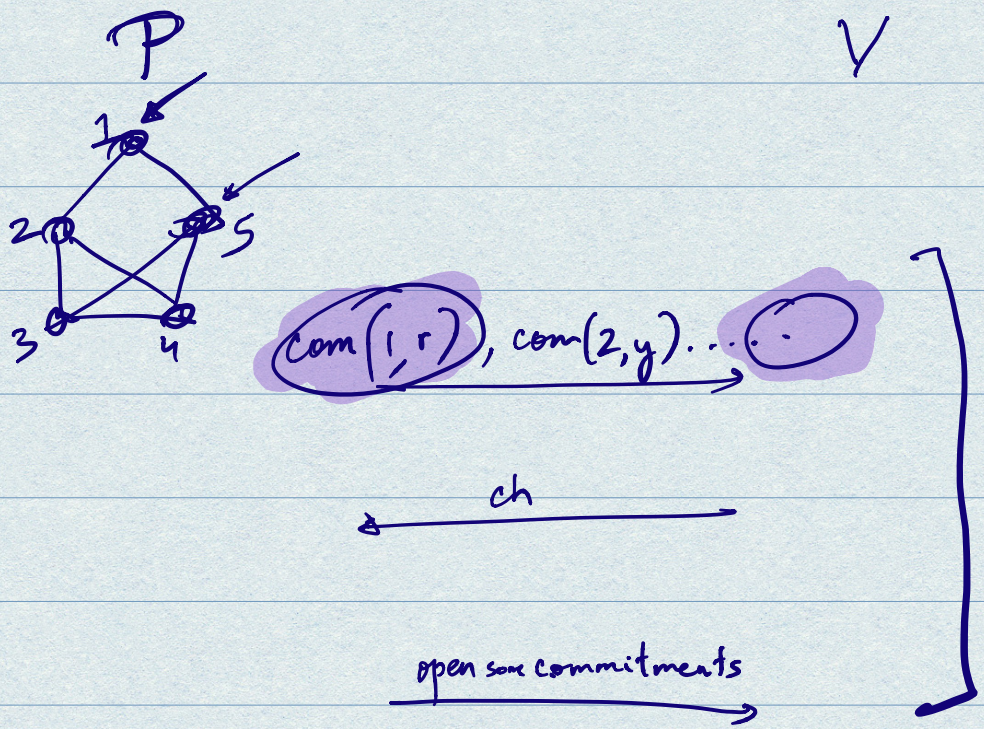
RECAP : ZERO-KNOWLEDGE



Sound against unbounded P

ZK against PPT V

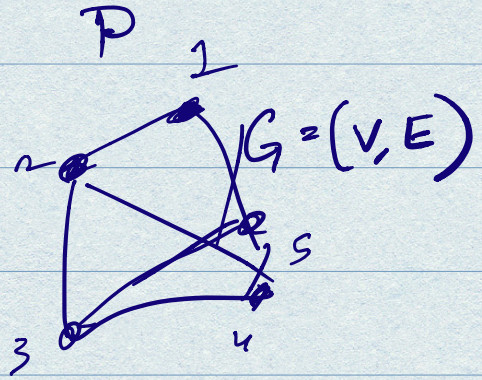
What if : Sound against PPT P

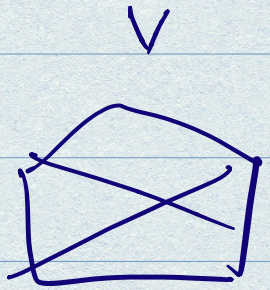
ZK against unbounded V

CRHF ⇒ commitment ; binding against PPT committers

hiding against unbounded receivers.

Graph Hamiltonicity





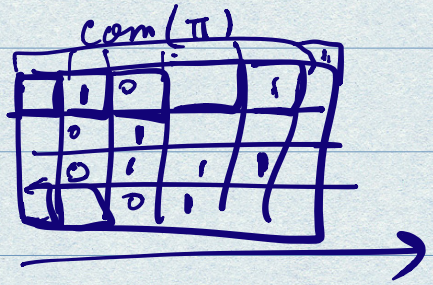
Goal: prove that G has a Hamiltonian cycle.

P knows $H \subseteq E$ V.

"witness"

$\pi \leftarrow Perm\{1 \ldots 5\}$

$G' = \pi(G)$: maps $i \in V$ to $\pi(i) \in V'$,
$(i,j) \in E$ to $\pi(i), \pi(j) \in E'$.

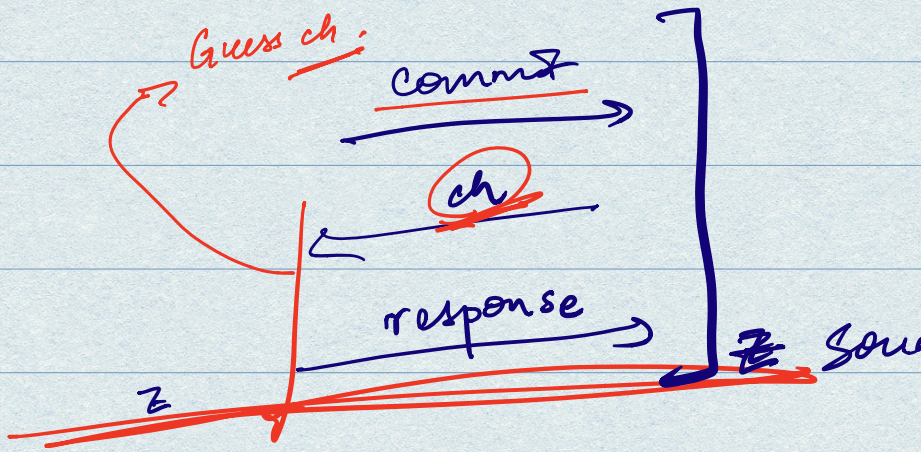


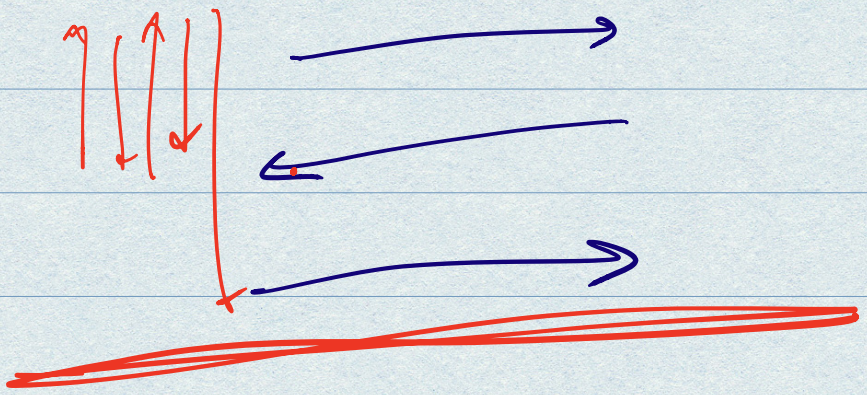
ch ∈ {0, 1}

if ch = 0, open all cells, open π

if ch = 1, open π(H).

This is a PoK.





Definition of ZK:

Def. 1

$\exists$ PPT Sim s.t. $\forall V^*$, $\forall x \in L$, $\forall z$,

$$View_{V^*}\left[P(x), V^*(x,z)\right] \approx_c \boxed{View_{V^*}\langle Sim^{V^*}(x,z)\rangle}$$

$$\left[Sim(V^*, x)\right]$$

Any protocol satisfying Def 1 will compose sequentially s.t. the resulting protocol also satisfies Def 1.

Parallel Composition

ZK is not known to compose in parallel.

$\alpha = [\text{com}(\ ), \text{com}(\ ), \ldots]$

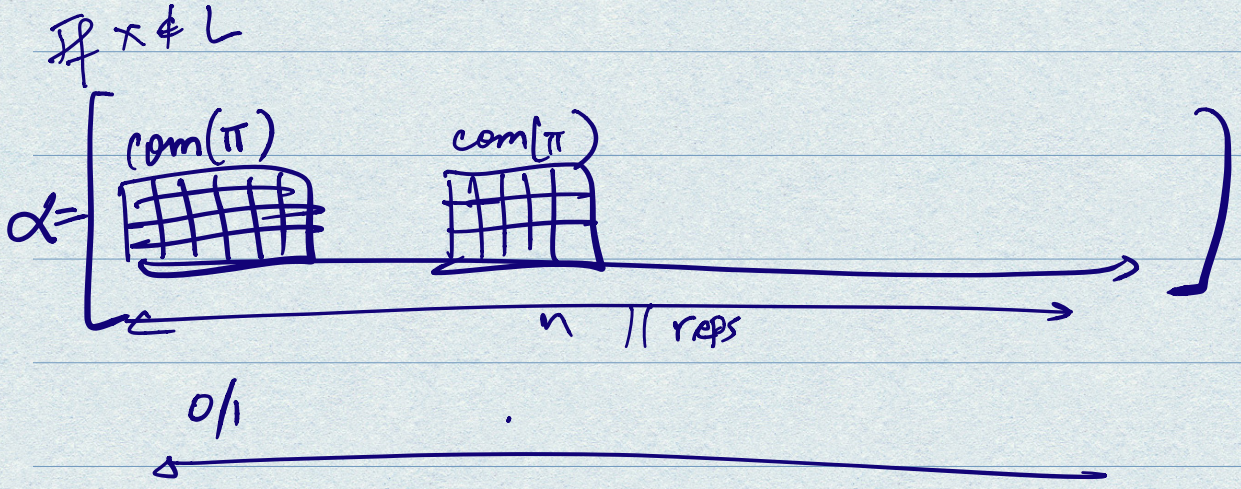
$ch \in \{0,1\}^n$

$resp_1, resp_2, \ldots$

non-interactive ⇓

P computes $ch = H(\alpha)$.

H can be implemented via a special type of hashing.



If $x \notin L$,

∀ prover commitments, $\exists \leq 1$ challenge on which V accepts. All other $2^n - 1$ challenges, P gets caught.

"BAD" challenge

Build H s.t. P cannot find α s.t. $H(\alpha) = BAD(\alpha)$.

Non-interactive ZK from LWE.
(with setup).

4 round ZK : known

2 rounds impossible without setup

3 rounds (?).

Weak ZK possible in 2 rounds [FHE]

$\exists$ Sim s.t. $\forall$ PPT V, $\forall x \in L$, $\forall z$, $\forall$ PPT $\mathcal{D}$,

$$\left| \Pr[\mathcal{D}=1 \mid \langle \quad \rangle] - \Pr[\mathcal{D}=1 \mid \mathrm{Sim}(V, \mathcal{D})] \right| = \mathrm{negl}.$$