# LECTURE 16

## Last class - Summary.

We SAW:

$X \in NP$, $L \in NP$
↳ Karp reduction → 3-col

Assuming the existence of commitments, there exist ZK proofs for the language of all 3-colorable Graphs

[The ZK proofs satisfy Completeness, Soundness, ZK.]

Proof of knowledge

Interaction was important

com(colors)
challenge
open colors

Sequential repetition reduced soundness error

Sequential repetition was ZK.

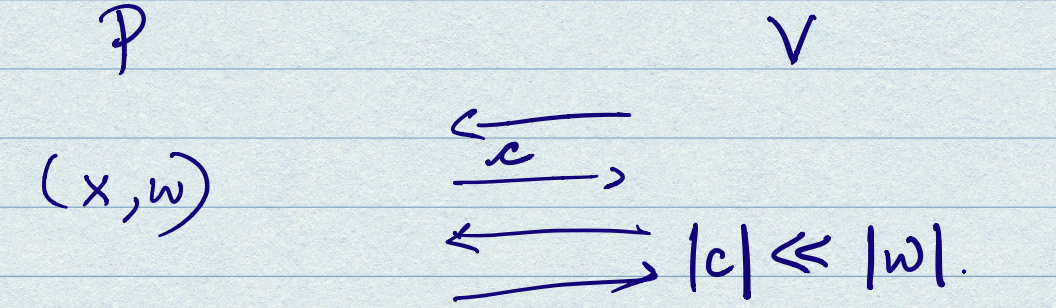
parallel repetion was sound, but not ZK

H.W.1 Notation $c_1 = Enc(b_1)$, $c_2 = Enc(b_2)$, $c_3 = Enc(b_1 \oplus b_2)$

$\bigoplus_{i \text{ s.t. } x_i = 1} b_i$ = XOR of the $b_i$'s $\forall i$ where $x_i = 1$

# ASIDE. SNARK.

- Succinct Non-interactive Argument of Knowledge.




* Completeness
* Soundness
* Succinctness replaces ZK.

## ZK-SNARKS.

Zero knowledge SNARKs

"Proof of Knowledge".

Soundness : (Roughly)

If $V$ accepts $\Rightarrow x \in L$.

PoK :

If $V$ accepts $\Rightarrow$

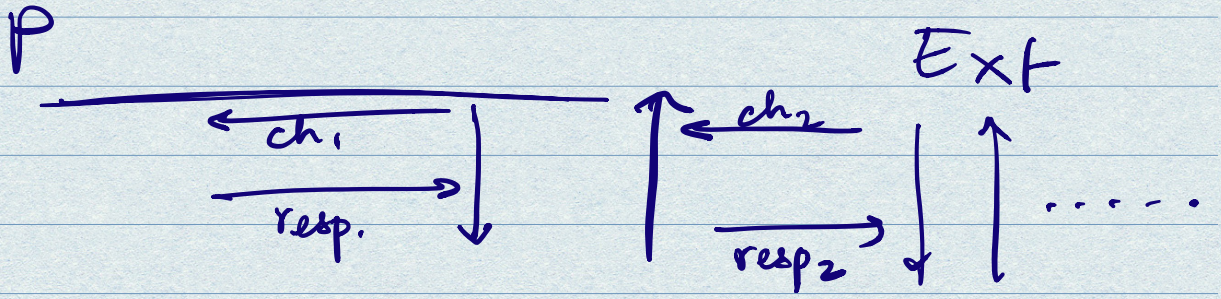
Prover "knows" some secret

(eg., NP witness $w$ s.t. $R_L(x, w) = 1$)

**Definition** [Proof of Knowledge].

An interactive proof $\langle P, V \rangle$ for NP language $L$ and relation $R_L$ is a Proof-of-knowledge with error $\varepsilon$, if $\exists$ PPT Ext

$$\Pr\left[R_L(x, w) = 1 \;\middle|\; \text{Ext}^{P^*}(x) = w\right] \geq \Pr\left[V\left(\langle P^*, V \rangle\right) = 1\right] - \varepsilon$$




---

# LATTICE - BASED ZK Proofs of Knowledge

## "Schnorr - like" ZK PoKs

P

V

A, y

A, y

"short" x s.t. $Ax = y$

Sample r

$z = Ar$ →

← $c$

$x' = cx + r$ →

CHECK:

$Ax' = cy + z$.

$= cAx + Ar$

P V

A, y A, y

"short" x s.t. Ax = y

Sample r

$z = Ar$ →

← $c$

$x' = cx + r$ →

CHECK:

$Ax' = cy + z$.

$= c(Ax) + z$

x' is short.

V

"Proof of knowledge" of $x$ s.t. $Ax = cy$

P

$z$ →

← $c_1$

$x_1$ →

$Ax_1 = cy + z$

← $c_2$

$x_2$ →

$Ax_2 = c_2 y + z$

$Ax_1 = c_1 y + z$

(and) $Ax_2 = c_2 y + z$

$A(x_1 - x_2) = (c_1 - c_2) y \Rightarrow$ $x = x_1 - x_2$, $c = c_1 - c_2$

$Ax = cy$

Kawachi, Tanaka, Xagawa '08

## Stern-like protocols.

P V

A, y Ay

"short" x s.t.

$Ax = y$

Constraint: #0s in x = #1s in x

$\pi : \{0,1\}^n \to \{0,1\}^n$

$c_1 = com(\pi, Ar)$

$c_2 = com(\pi(r))$

$c_3 = com(\pi(x + r))$

→

choose 2 out of 3 com

←

decommit the chosen commitments

→

V does the following:

If $c_1$, $c_2$ are opened

V obtains $\pi$, $\pi(r)$, $Ar$

recover $r$ ↑ $A$

If $c_2$, $c_3$ are opened

V obtains $\pi(x+r)$, $\pi(r)$

$\pi(x+r) - \pi(r) = \pi(x)$ ← $x$

If $c_1$, $c_3$ are opened

V obtains $\pi$, $\pi(x+r)$, $Ar$.

$x+r$ → $A$, $Ax$

check if $A(x+r) = y + Ar$

---

Suppose $\exists$ P that for a fixed set of commitments $c_1, c_2, c_3$.

has $Pr[V \text{ accepts}] > \frac{2}{3} + \Delta$

Then $Pr[\text{Ext outputs witness}] > \text{poly}(\Delta)$