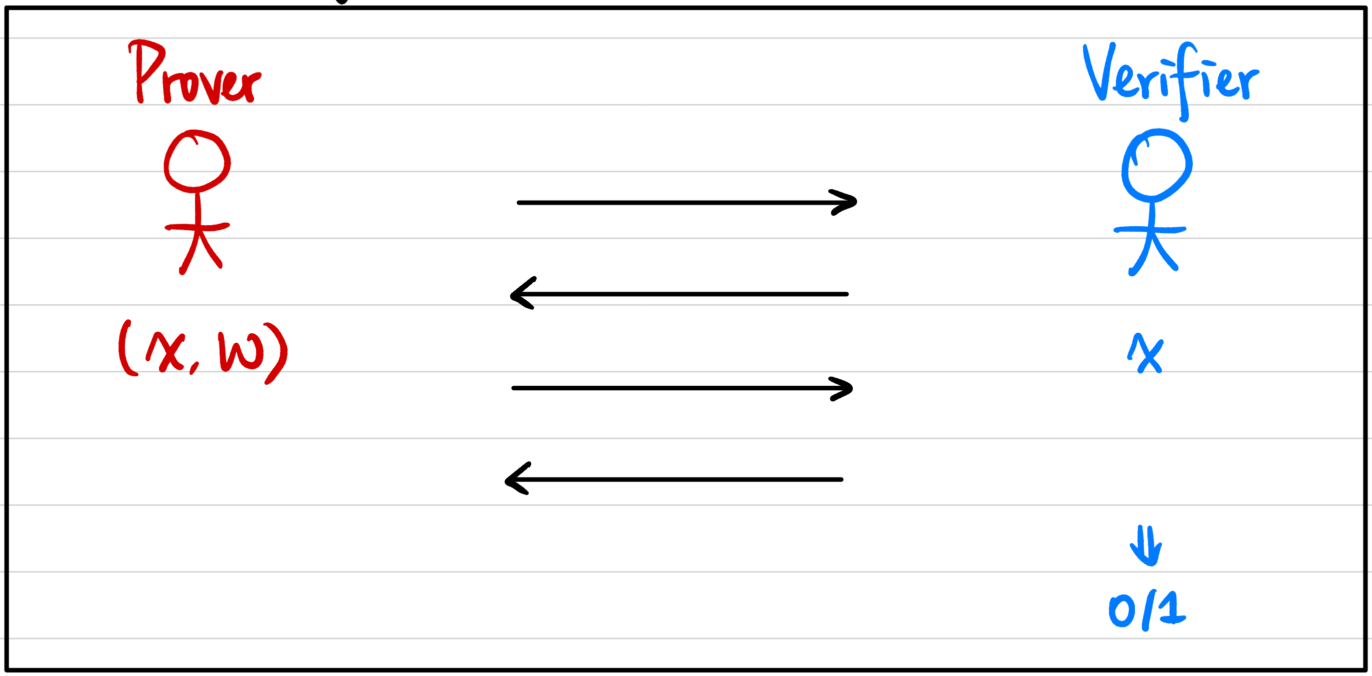
CSCI 1510

- Perfect ZKP for Diffie-Hellman Tuples (continued)
- Commitment Schemes
- ZKP for All NP

Zero-Knowledge Proof (ZKP)

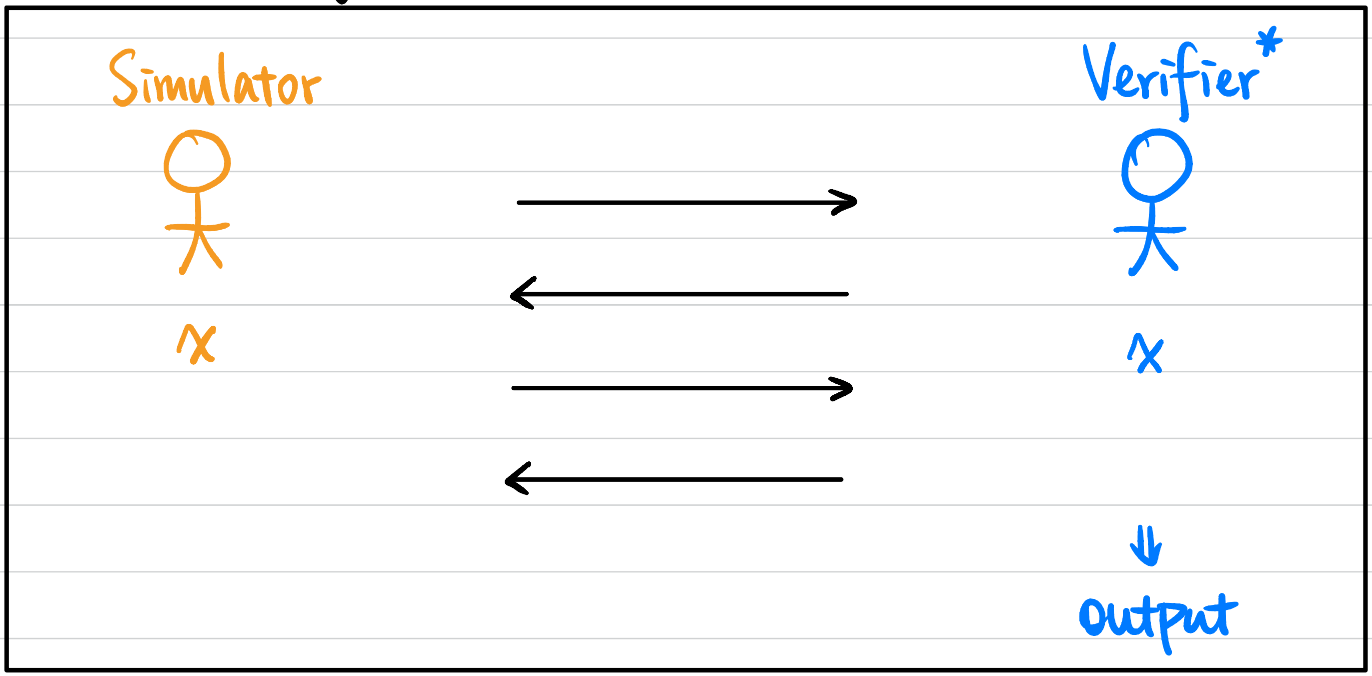


Let (P, V) be a pair of PPT interactive machines. (P, V) is a zero-knowledge proof system for a language L with associated relation R_L if

- **Completeness:** $\forall (x, w) \in R_L$, $\Pr[\, P(x,w) \longleftrightarrow V(x) \text{ outputs } 1 \,] = 1$.
- **Soundness:** $\forall x \notin L$, $\forall$ (PPT) P^*, $\Pr[\, P^*(x) \longleftrightarrow V(x) \text{ outputs } 1 \,] \leq \mathrm{negl}(n)$.

  argument
- **Zero-Knowledge?**

Zero-Knowledge Proof (ZKP)



- **Zero-Knowledge:** $\forall$PPT V^*, $\exists$PPT S s.t. $\forall (x,w) \in R_L$,

$$\mathrm{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \simeq S(x)$$

perfect / statistical / computational

$\equiv$ $\quad \overset{s}{\approx}$ $\quad \overset{c}{\approx}$

Perfect ZKP for Diffie-Hellman Tuples

Input: Cyclic group G of order q, generator g, $\underset{g^a}{\overset{\shortparallel}{h}}$, $\underset{g^b}{\overset{\shortparallel}{u}}$, $\underset{g^{ab}}{\overset{\shortparallel}{v}}$

Witness: b

Statement: $\exists\, b \in \mathbb{Z}_q$ s.t. $u = g^b \wedge v = h^b$

Prover (b)		**Verifier**
$r \xleftarrow{\$} \mathbb{Z}_q$		
	$\xrightarrow{A := g^r,\ B := h^r}$	
		$\sigma \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{\ \sigma\ }$	
	$\xrightarrow{s := \sigma \cdot b + r \bmod q}$	
		Verify $g^s = A \cdot u^\sigma$, $h^s = B \cdot v^\sigma$

Completeness?

If $\sigma = 0 \Rightarrow s = r \Rightarrow g^s = A \quad h^s = B$

If $\sigma = 1 \Rightarrow s = b + r \Rightarrow g^s = A \cdot u \quad h^s = B \cdot v$

Soundness?

$$\underset{\substack{\| \\ g^a}}{(g,\ h},\ \underset{\substack{\| \\ g^b}}{u},\ \underset{\substack{\| \\ g^c}}{\overset{=h^{b'}}{v}}) \notin L \qquad b \neq b'$$

$$\forall x \notin L,\ \forall P^*,\quad \Pr[P^*(x) \longleftrightarrow V(x) \text{ outputs } 1] \leq \mathrm{negl}(n)$$

Prover*: $r \xleftarrow{\$} \mathbb{Z}_q$

Verifier

- Prover* → Verifier: $A := g^r,\ B := h^{r'}$
- Verifier: $\sigma \xleftarrow{\$} \{0,1\}$
- Verifier → Prover*: σ
- Prover* → Verifier: s (~~$S := \sigma \cdot b + r \bmod q$~~)
- Verify $g^s = A \cdot u^\sigma$, $h^s = B \cdot v^\sigma$

n times

Soundness error 2^{-n}.

$$g^s = A \cdot u^\sigma \Leftrightarrow g^s = g^r \cdot (g^b)^\sigma = g^{r+b\cdot\sigma} \Leftrightarrow s = r + b\cdot\sigma \mod q$$

$$h^s = B \cdot v^\sigma \Leftrightarrow h^s = h^{r'} \cdot (h^{b'})^\sigma = h^{r'+b'\cdot\sigma} \Leftrightarrow s = r' + b'\cdot\sigma \mod q$$

$$r - r' = (b - b')\cdot\sigma$$

If $r = r'$ ⇒ caught by V if $\sigma = 1$

If $r \neq r'$ ⇒ caught by V if $\sigma = 0$.

Zero-Knowledge?

$\forall$ PPT V^*, $\exists$ PPT S s.t. $\forall (x, w) \in R_L$,

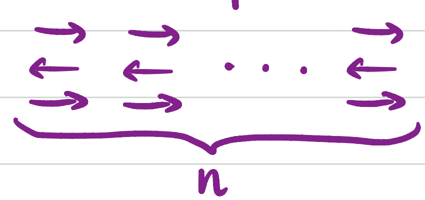
$$\text{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \equiv S(x)$$

Simulator		**Verifier***
$s \xleftarrow{\$} \mathbb{Z}_q$	
$\sigma' \xleftarrow{\$} \{0,1\}$	
$A := g^s / u^{\sigma'}$	
$B := h^s / v^{\sigma'}$	
$\xrightarrow{\quad A,\ B \quad}$
$\xleftarrow{\quad \sigma \quad}$
If $\sigma = \sigma'$, send back s	
Otherwise rewind	
$\xrightarrow{\quad s \quad}$

$\Pr[\sigma \neq \sigma'] = \frac{1}{2}$

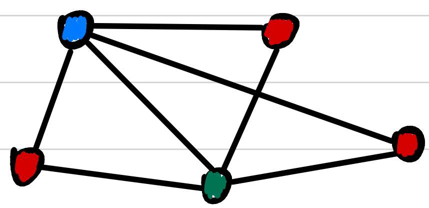
Rewind n times $\Rightarrow$ failure prob. 2^{-n}.

Parallel Repetition:



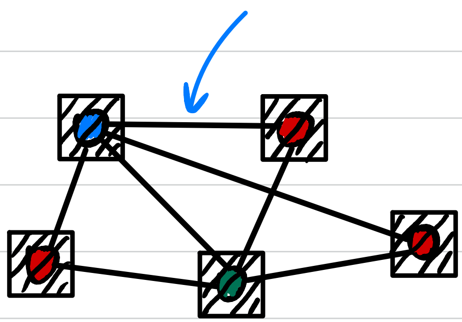
NOT ZK!

ZKP for Graph 3-Coloring (All NP)



NP language $L = \{ G : G \text{ has 3-Coloring} \}$

NP relation $R_L = \{ (G, \text{3COL}) \}$



$\pi : \{ \bullet \ \bullet \ \bullet \} \to \{ \bullet \ \bullet \ \bullet \}$

Commitment Scheme

Sender | **Receiver**

$m \in \{0,1\}$

Commit:

$r \xleftarrow{\$} \{0,1\}^n$

$c := Com(m;r) \quad \xrightarrow{\quad c \quad}$

Decommit:

$\xrightarrow{\quad (m,r) \quad}$

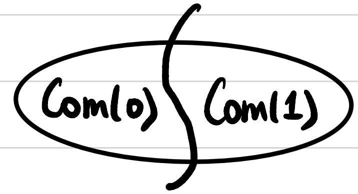
Verify:

$c = Com(m;r)$

Commitment Scheme

Def A non-interactive perfectly binding commitment scheme is a PPT algorithm Com statisfying:

- Perfectly Binding: $\forall r, s \in \{0,1\}^n$, $Com(0; r) \neq Com(1; s)$



- Computationally Hiding: $Com(0; U_n) \overset{c}{\approx} Com(1; U_n)$

A decommitment of a commitment value c is (b, r) s.t. $c = Com(b; r)$.

Computationally Binding: $\forall$PPT $\mathcal{A}$ can't find $r, s \in \{0,1\}^n$ s.t. $Com(0; r) = Com(1; s)$

Perfectly Hiding: $Com(0; U_n) \equiv Com(1; U_n)$

Can a commitment scheme be both perfectly binding & perfectly hiding? No!

Perfectly Binding Commitment Scheme

Assume one-way permutations exist.

Let $f: \{0,1\}^n \to \{0,1\}^n$ be a OWP and $hc: \{0,1\}^n \to \{0,1\}$ be a hard-core predicate of f.

$$Com(b; r) := (f(r),\ hc(r) \oplus b)$$

- Perfectly Binding?

$\forall r, s \in \{0,1\}^n$, $Com(0; r) = (f(r), hc(r) \oplus 0)$ $\qquad r \neq s \Rightarrow f(r) \neq f(s)$

$Com(1; s) = (f(s), hc(s) \oplus 1)$ $\qquad r = s \Rightarrow hc(r) \oplus 0 \neq hc(s) \oplus 1$.

- Computationally Hiding?

$$(f(r),\ \underset{\substack{\uparrow \\ \text{Computationally indistinguishable from random}}}{hc(r)} \oplus b)$$

ZKP for Graph 3-Coloring

Input: $G = (V, E)$

Witness: $\phi : V \to \{0,1,2\}$

Given a perfectly binding commitment scheme Com.

Soundness?

$G \notin L$, by perfect binding of Com,

$$\Pr[P^* \text{ not caught}] \le \left(1 - \frac{1}{|E|}\right)^{n \cdot |E|} \approx e^{-n}$$

Prover		Verifier
Randomly sample $\pi : \{0,1,2\} \to \{0,1,2\}$		
$\forall v \in V$, $r_v \xleftarrow{\$} \{0,1\}^n$, $C_v := \mathrm{Com}(\pi(\phi(v)); r_v)$		
	$\xrightarrow{\{C_v\}_{v \in V}}$	
		Randomly pick an edge $(u,v) \in E$
	$\xleftarrow{(u,v)}$	
Reveal decommitments of C_u & C_v		
	$\xrightarrow[\beta = \pi(\phi(v)),\ r_v]{\alpha = \pi(\phi(u)),\ r_u}$	Verify: $C_u = \mathrm{Com}(\alpha; r_u)$ $C_v = \mathrm{Com}(\beta; r_v)$ $\alpha, \beta \in \{0,1,2\}$, $\alpha \neq \beta$

$n \cdot |E|$ times

Completeness?

Zero-Knowledge?

$\forall$ PPT V^*, $\exists$ PPT S s.t. $\forall (x, w) \in R_L$,

$$\mathrm{Output}_{V^*}[P(x,w) \longleftrightarrow V^*(x)] \overset{c}{\approx} S(x)$$

Simulator | **Verifier***

$(u', v') \overset{\$}{\leftarrow} E$

$\alpha, \beta \overset{\$}{\leftarrow} \{0,1,2\}$ s.t. $\alpha \neq \beta$

$r_{u'} \overset{\$}{\leftarrow} \{0,1\}^n$ $\quad c_{u'} := \mathrm{Com}(\alpha; r_{u'})$

$r_{v'} \overset{\$}{\leftarrow} \{0,1\}^n$ $\quad c_{v'} := \mathrm{Com}(\beta; r_{v'})$

$\forall v \in V \setminus \{u', v'\}$:

$\quad r_v \overset{\$}{\leftarrow} \{0,1\}^n$, $c_v := \mathrm{Com}(0; r_v)$

Simulator $\xrightarrow{\{c_v\}_{v \in V}}$ Verifier*

Simulator $\xleftarrow{(u,v)}$ Verifier*

If $(u,v) = (u', v')$:

Reveal decommitments of c_u & c_v $\quad \xrightarrow[\beta,\ r_v]{\alpha,\ r_u}$

Otherwise rewind