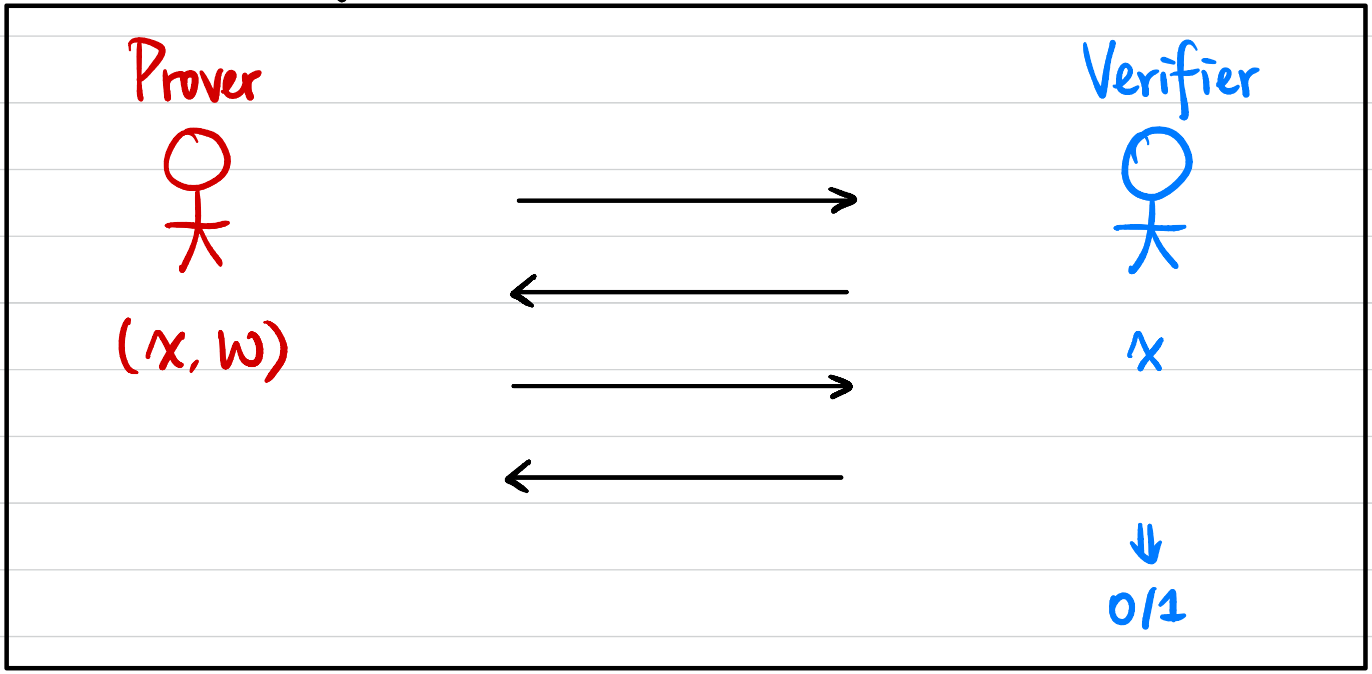
CSCI 1510

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

Zero-Knowledge Proof (ZKP)



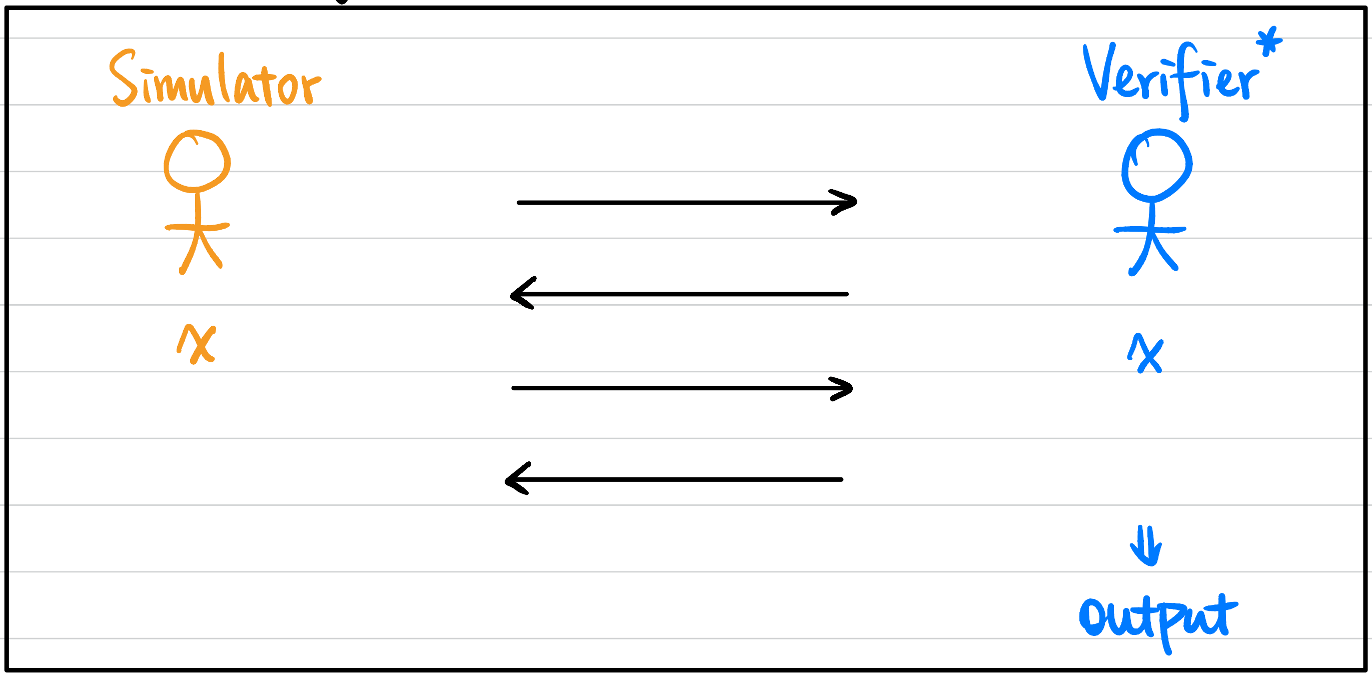
Let (P, V) be a pair of PPT interactive machines. (P, V) is a zero-knowledge proof system for a language L with associated relation R_L if

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

  argument

- **Zero-Knowledge?**

Zero-Knowledge Proof (ZKP)



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

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

perfect / statistical / computational

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

Perfect ZKP for Diffie-Hellman Tuples

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

Witness: b

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

Prover		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 $g^s = u^\sigma \cdot A$
		$h^s = v^\sigma \cdot B$

n

Completeness?

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

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

Soundness?

$(g, h, u, v) \notin L$ $\qquad v = h^{b'} \qquad b' \neq b$

$h = g^a, \quad u = g^b, \quad v = g^c$

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

Prover*

$r \xleftarrow{\$} \mathbb{Z}_q$

A, B

$\xrightarrow{\cancel{A := g^r, \ B := h^r}}$

Verifier

$\sigma \xleftarrow{\$} \{0, 1\}$

$\xleftarrow{\ \sigma\ }$

s

$\xrightarrow{\cancel{s := \sigma \cdot b + r \mod q}}$

n

Verify $g^s = u^\sigma \cdot A$

$h^s = v^\sigma \cdot B$

$$g^s = u^\sigma \cdot A \iff g^s = (g^b)^\sigma \cdot A \iff (g^s)^a = (g^b)^{\sigma \cdot a} \cdot A^a \iff h^s = h^{b \cdot \sigma} \cdot A^a$$

$$h^s = v^\sigma \cdot B \iff h^s = (h^{b'})^\sigma \cdot B$$

$$\Pr[g^s = u^\sigma \cdot A \ \wedge \ h^s = v^\sigma \cdot B] = \Pr[h^{b \cdot \sigma} \cdot A^a = h^{b' \cdot \sigma} \cdot B] = \Pr[h^{(b - b') \cdot \sigma} = B / A^a]$$

$$\leq \tfrac{1}{2}$$

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***

$\sigma' \xleftarrow{\$} \{0,1\}$

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

$A := g^s / u^{\sigma'}$

$B := h^s / v^{\sigma'}$

$$\xrightarrow{\quad A,\ B \quad}$$

$$\xleftarrow{\quad \sigma \quad}$$

If $\sigma = \sigma'$, send back s

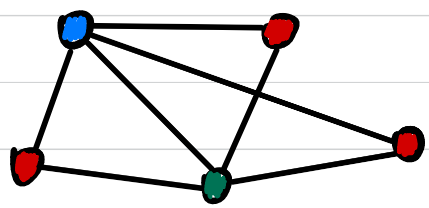
Otherwise rewind

$$\xrightarrow{\quad s \quad}$$

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

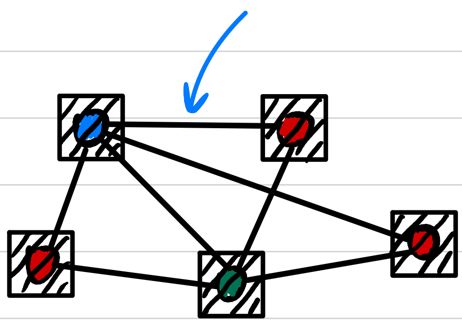
Rewind n times $\Rightarrow$ failure prob. 2^{-n}.

ZKP for Graph 3-Coloring (All NP)



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

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



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

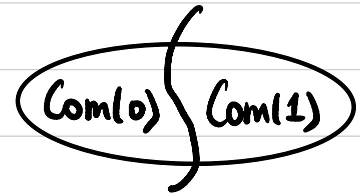
Commitment Scheme

Sender		Receiver
$m \in \{0,1\}$		
Commit:		
$r \xleftarrow{\$} \{0,1\}^n$		
$c := \mathrm{Com}(m; r)$	$\xrightarrow{\quad c \quad}$	
Decommit:	$\xrightarrow{\quad (m,r) \quad}$	Verify:
		$c = \mathrm{Com}(m; r)$

Commitment Scheme

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

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



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

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

Computationally Binding: $\forall$ PPT A, $\Pr[A \text{ outputs } r, s \in \{0,1\}^n \text{ s.t. } \mathrm{Com}(0; r) = \mathrm{Com}(1; s)] \leq \mathrm{negl}(n)$

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

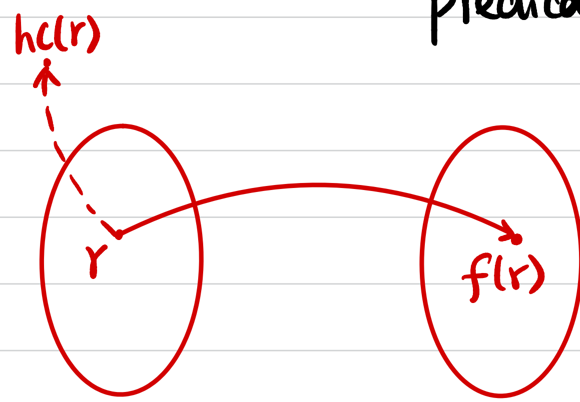
Can a commitment scheme be both perfectly binding & perfectly hiding? No!

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?

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

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

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

- Computationally Hiding?

  $Com(0; U_n) \overset{c}{\approx} Com(1; U_n)$

  $(f(r), hc(r) \oplus b)$

  $\uparrow$

  Computationally indistinguishable from random

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,

$\Pr[P^* \text{ be caught}] \geq \frac{1}{|E|}$

$\Pr[V \text{ outputs } 1] \leq \left(1 - \frac{1}{|E|}\right)^{n \cdot |E|} \approx \left(\frac{1}{e}\right)^n$

Prover | **Verifier**

Prover: Randomly sample $\pi: \{0,1,2\} \to \{0,1,2\}$

Prover: $\forall v \in V$, $r_v \xleftarrow{\$} \{0,1\}^n$, $C_v := \mathrm{Com}(\pi(\phi(v)); r_v)$

Prover → Verifier: $\{C_v\}_{v \in V}$

Verifier: Randomly pick an edge $(u,v) \in E$

Verifier → Prover: (u,v)

Prover: Reveal decommitments of C_u & C_v

Prover → Verifier: $\alpha = \pi(\phi(u))$, r_u; $\beta = \pi(\phi(v))$, r_v

Verifier: Verify: $C_u = \mathrm{Com}(\alpha; r_u)$

$C_v = \mathrm{Com}(\beta; r_v)$

$\alpha, \beta \in \{0,1,2\}$, $\alpha \neq \beta$

$k = n \cdot |E|$

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***

$(u', v') \xleftarrow{\$} E$

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

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

$r_{v'} \xleftarrow{\$} \{0,1\}^n$ $\quad C_{v'} := \mathrm{Com}(\beta, r_{v'})$

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

$\quad r_v \xleftarrow{\$} \{0,1\}^n$, $\quad C_v := \mathrm{Com}(0; r_v)$

$\xrightarrow{\{C_v\}_{v \in V}}$

$\xleftarrow{(u,v)}$

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

$\quad$ Reveal decommitments of C_u & C_v

Otherwise rewind

$\xrightarrow[\beta,\ r_v]{\alpha,\ r_u}$

$\Pr[(u,v) = (u', v')] = \frac{1}{|E|}$ $\qquad$ Rewind $n \cdot |E|$ times $\Rightarrow$ failure prob. e^{-n}.