Zero Knowledge Proofs

$\text{View}_V^P(G_0, G_1) =$

$(R, b, R(G_b), b', \text{output})$

$P \quad (G_0, G_1) \quad V$

$\not\cong$

samples random relabelling $R : [n] \to [n]$

random bit b

$\xleftarrow{\quad R(G_b) \quad}$

if $G_0 \cong G_1$ $\xrightarrow{\quad \perp \quad}$ rejects

else,

if $R(G_b) \stackrel{?}{=} G_0$, $b' = 0$

if $R(G_b) \stackrel{?}{=} G_1$, $b' = 1$ $\xrightarrow{\quad b' \quad}$ accepts iff $b = b'$

$P \quad x \quad V(r)$

output (acc/rej)

$\underbrace{\mathrm{View}_V^P(x)}$: (randomness r, messages, output)

RV over V's randomness r and any P's randomness

Honest-Verifier Perfect Zero Knowledge (strong)

(P,V) is HVPZK if $\exists$ PPT simulator S s.t.

$\forall x \in L$: $S(x)$ is identically distributed to $\mathrm{View}_V^P(x)$

$\hookrightarrow (r', m', o')$

Simulator $S(G_0, G_1)$:

1. Generate R, b, and $R(G_b)$ according to V

2. Set $b' = b$

3. Output $(R, b, R(G_b), b', \text{accept})$ $\quad \therefore$ PZK

Alternative HVPZK:

$\exists$ PPT $S: \forall x: S(x, (x \in L)) \equiv \text{View}_V^P(x)$

If $\text{View}_V^P(x) = \bot$ when $x \notin L$: Alt. HVPZK = HVPZK

Perfect Zero Knowledge

(P,V) is PZK if $\forall$ PPT V^* $\exists$ PPT S_{V^*}:

$\boxed{PZK \subseteq AM \cap coAM}$

$\forall x \in L$:

- $\Pr[S_{V^*}(x) = \perp] \leq 1/2$
- Conditioned on $S_{V^*}(x) \neq \perp$, dists of $S_{V^*}(x)$ is identical to $View^P_{V^*}(x)$

Graph Isomorphism:

P (G_0, G_1) V

Comp: perfect

Snd: error $\frac{1}{2}$

ZK: perfect?

Samples random relabelling R

random bit b

$$\xrightarrow{H = R(G_b)}$$

random bit b'

$$\xleftarrow{b'}$$

find relabelling R' s.t. $R'(G_{b'}) = H$

$$\xrightarrow{R'}$$

Check $R'(G_{b'}) = H$

Given V^* Simulator S_{V^*}: Given $G_0 \equiv G_1$

1. Generate R, b, $H = R(G_b)$
2. Compute $b' \leftarrow V^*(H; r)$ (r sampled by S_{V^*})
3. If $b' = b$, set $R' = R$, output $(r, H, b', R',$ output of $V^*)$

Same as $\mathrm{View}^P_{V^*}(G_0, G_1)$

$(r, H, b, R, V^*(H, b, R; r))$

4. If $b' \neq b$, output $\perp$

$\hookrightarrow$ happens w.p. $\leq \frac{1}{2}$

Computational Indistinguishability

$D = \{D_\lambda\}_{\lambda \in \mathbb{N}}$, each D_λ over $\{0,1\}^{\ell(\lambda)}$

$\{D_{0\lambda}\}$ $\{D_{1\lambda}\}$

$\boxed{D_0 \approx_C D_1}$ if $\forall$ PPT A $\forall c \in \mathbb{N}$ $\exists \lambda_c \in \mathbb{N}$

$$\forall \lambda > \lambda_c : \left| \Pr_{x \leftarrow D_{0\lambda}}[A(1^\lambda, x) = 1] - \Pr_{x \leftarrow D_{1\lambda}}[A(1^\lambda, x) = 1] \right| \le \frac{1}{\lambda^c}$$

$$\mathrm{Adv}_A^{D_0, D_1}(\lambda) = o\left(\frac{1}{\mathrm{poly}(\lambda)}\right)$$

Computational Zero Knowledge:

(P,V) is CZK if $\forall$ PPT V^* $\exists$ PPT S_{V^*} s.t.

$\forall x \in L$: $\quad S_{V^*}(x) \approx_c \mathrm{View}_{V^*}^{P}(x)$

$$\big\{S_{V^*}(x, 1^\lambda)\big\}_{\lambda \in \mathbb{N}} \qquad \big\{\mathrm{View}_{V^*(1^\lambda)}^{P(1^\lambda)}(x)\big\}_{\lambda \in \mathbb{N}}$$

$\boxed{NP \subseteq CZK}$

under comp. assumptions

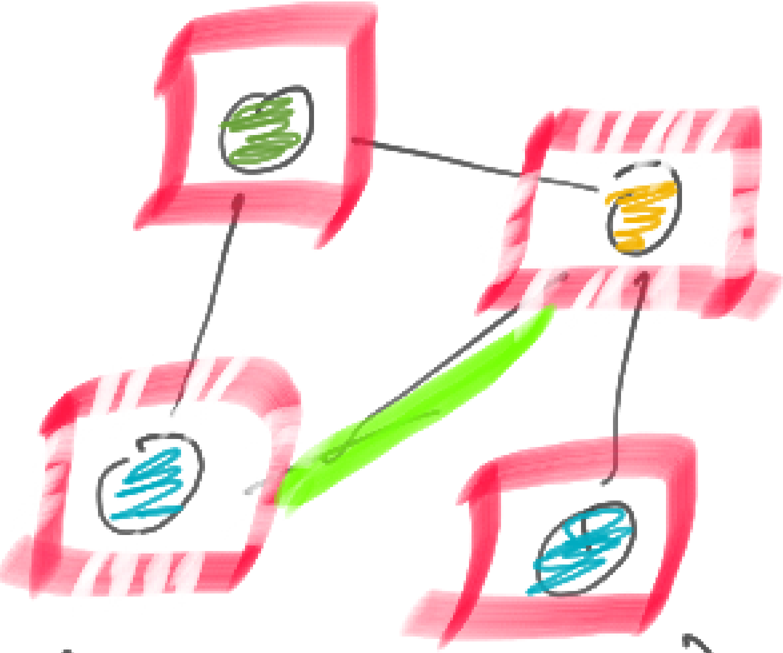
$IP \subseteq CZK$

under same assumptions

CZK for 3-Colouring (which is NP-complete)

$\{G : G \text{ is 3-colourable}\}$ → colouring of every $v \in V$ with 3 colours s.t. for any edge (u,v), colour of $u \neq$ colour of v

P | G | V



(random 3-colouring)
Valid

(commitment) →

← Open e

keys to boxes for e →

Picks random edge e

Check colours are different and among (blue, yellow, green)

Commitments:

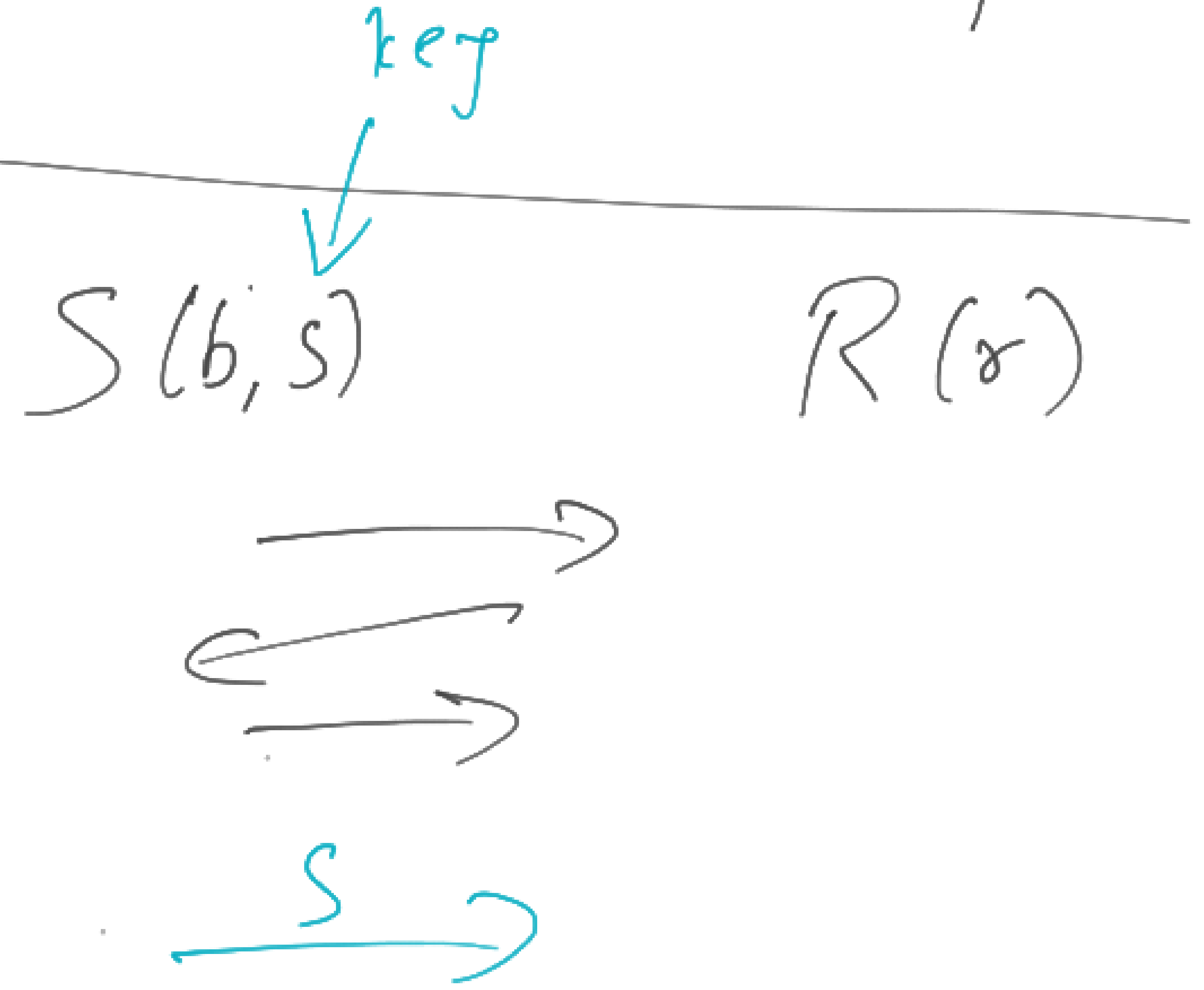
A protocol between poly-time Sender S and poly-time Receiver R

- Sender uses randomness s, R uses r, both get sec. param. 1^λ
- Sender gets secret bit b
- $\mathrm{View}^{S(1^\lambda, b, s)}_{R(1^\lambda, r)}$ ← locked box
  - should hide b if not given s

Hiding

- $\exists$ unique b for which $\exists s$ consistent with the view

Binding



Protocol bet. $S(1^\lambda, b, s)$ and $R(1^\lambda, r)$

computational
Hiding:

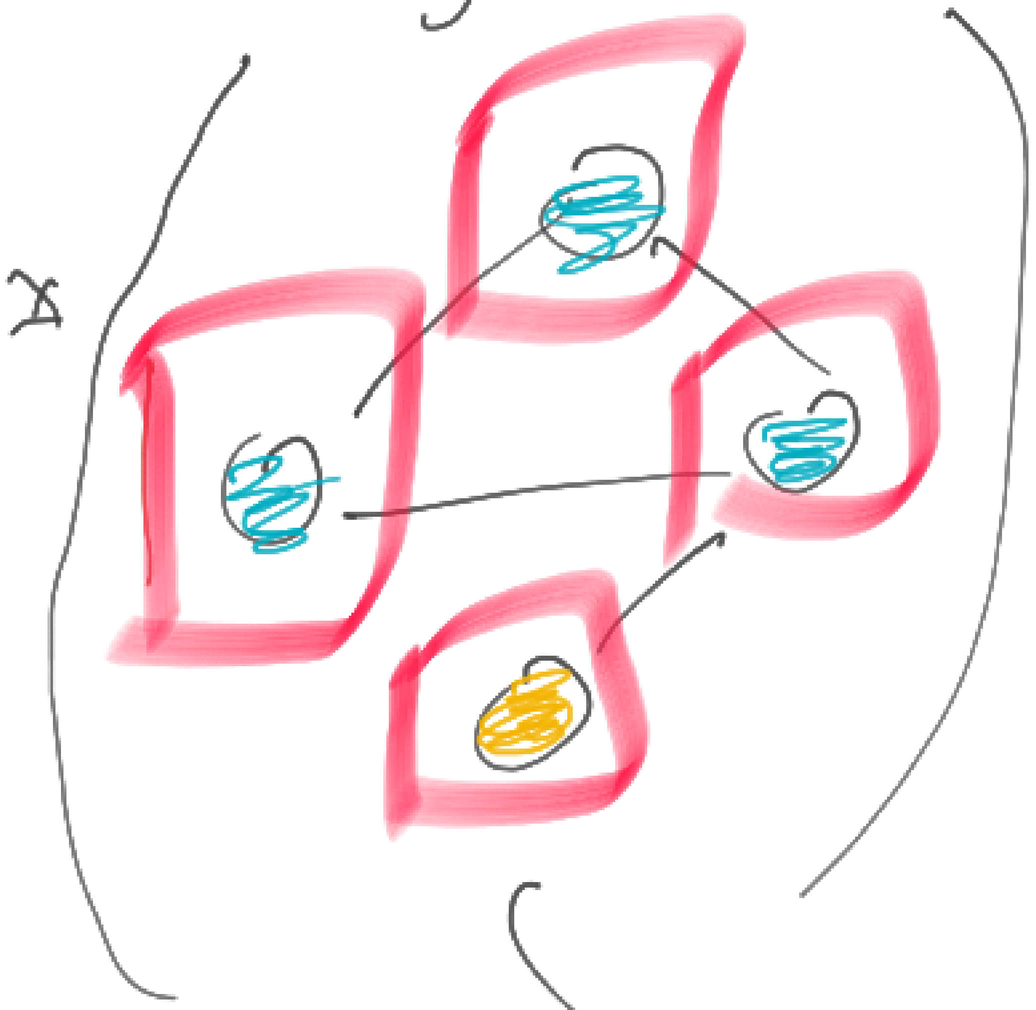
$$\mathrm{View}_{R(1^\lambda,\cdot)}^{S(1^\lambda,0,\cdot)} \approx_c \mathrm{View}_{R(1^\lambda,\cdot)}^{S(1^\lambda,1,\cdot)}$$

Statistical
Binding: for all except negl.(λ) frac. of r, $\forall s_0, s_1$

$\mathrm{View}_{R(1^\lambda,r)}^{S(1^\lambda,0,s_0)}$ and $\mathrm{View}_{R(1^\lambda,r)}^{S(1^\lambda,1,s_1)}$ are disjoint

Simulator:

1. Coloring of G in which one edge is properly colored

2. V^*  $\longrightarrow e$.

3. If e is properly colored. If not, output $\perp$.

4. If it is open the commitments, give to V^*

5. Output $(r_{V^*}, , e, \text{output})$

PRG $G: \{0,1\}^n \longrightarrow \{0,1\}^{3n}$

$G(x) \approx_c X$

$x \leftarrow \{0,1\}^n \qquad X \leftarrow \{0,1\}^{3n}$

$S(b, s \in \{0,1\}^n) \qquad R(r \in \{0,1\}^{3n})$

$\xleftarrow{\quad r \quad}$

$\xrightarrow{G(s) \oplus (b \cdot r)}$

Hiding:

$(r, G(s))$

$\approx_c$

(r, U_{3n})

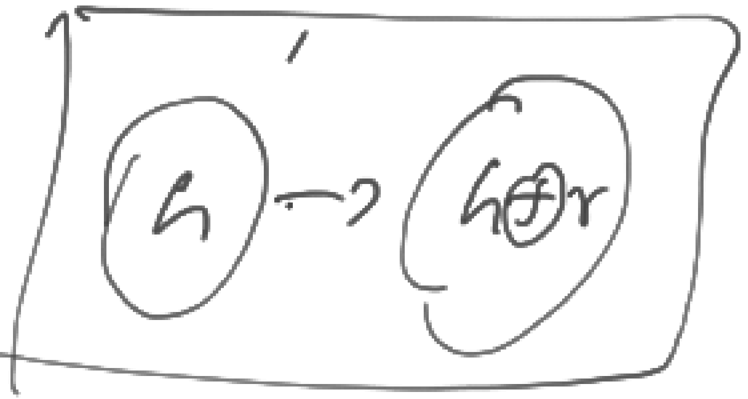
$\approx_c \quad (r, G(s) \oplus r)$

Binding:

$(r, G(s))$

$=$

$(r, G(s') \oplus r)$



$\{0,1\}^{3n}$