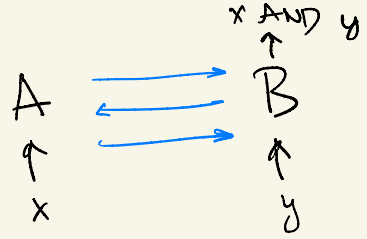
ZERO-KNOWLEDGE PROOFS



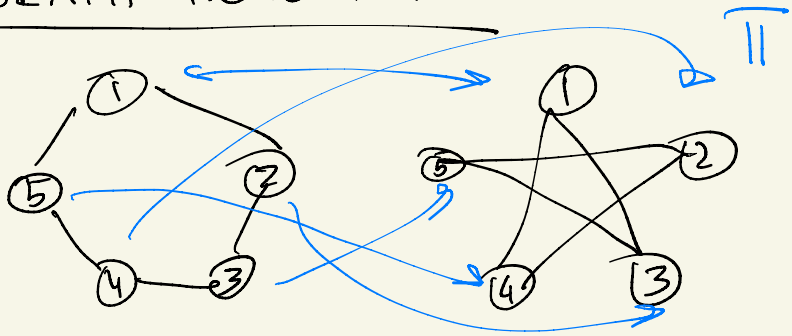
A, B HONEST BUT CURIOUS

$C = Enc(PK, x)$

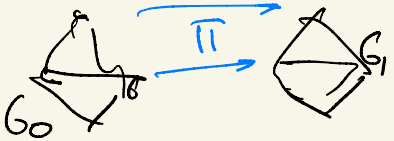
PROOF THAT C IS AN Enc OF x UNDER PK.

PROOFS THAT REVEAL NOTHING EXCEPT THAT CLAIM IS TRUE.

GRAPH ISOMORPHISM



IS A BIJECTION π BETWEEN VERTICES THAT PRESERVES THE EDGES.



Alice

"I KNOW π"

Bob

GRAPH ISOMORPHISM PROTOCOL

Alice KNOWS π S.T. $\pi(G_0) = G_1$.

1. Alice CHOOSE A RANDOM PERMUTATION ρ OF VERTICES AND SENDS $\rho(G_0) = G$ TO Bob.
2. Bob SENDS A RANDOM BIT b.
3. IF $b=0$, Alice REVEALS ρ
   IF $b=1$, Alice REVEALS $\rho \circ \pi$. } ϕ
4. Bob CHECKS THAT $\phi(G_b) = G$.

$b=0$: $G = \rho(G_0)$ ✓

$b=1$: $G = \rho(\pi(G_0)) = \rho(G_1)$.

Claim IF G_0, G_1 NOT ISOMORPHIC THEN Alice CANNOT HANDLE BOTH CHALLENGES.

Proof. SUPPOSE SHE COULD.

$\rightarrow G \simeq G_0$ AND $G \simeq G_1 \rightarrow G_0 \simeq G_1$.

BOB'S VIEW IS (G, b, ϕ) $\phi(G_b) = G$.

RANDOM RANDOM

HE CAN SIMULATE BY CHOOSING b, ϕ AT RANDOM AND SETTING $G = \phi(G_b)$.

IN PARTICULAR, NO INFO LEAKED ABOUT π.

TWO TYPES OF STATEMENTS

① "G_0, G_1 ARE ISOMORPHIC" PROOF OF FACT

② "I KNOW AN ISOMORPHISM π" PROOF OF KNOWLEDGE

PROOF RELATION $R(x, \pi)$

statement proof.

$x = (G_0, G_1)$, π ISOMORPHISM $G_0 \to G_1$

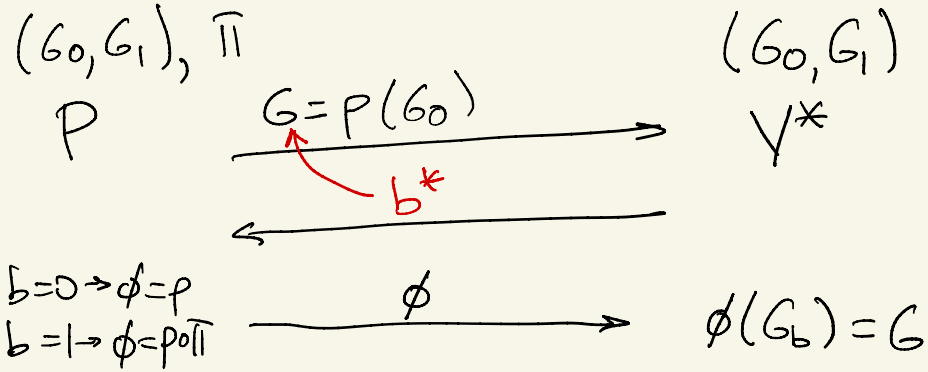
$((G_0, G_1), \pi) \in R$ IF $\forall x, y$: x, y EDGE IN G_0 $\Leftrightarrow$ $\pi(x), \pi(y)$ EDGE IN G_1.

PROOF SYSTEM FOR R IS A PROTOCOL BETWEEN $P(x, \pi)$ AND $V(x)$:

- COMPLETENESS: IF $(x, \pi) \in R$ THEN $V(x)$ ACCEPTS WITH PROB. 1
- SOUNDNESS: IF $(x, \pi) \notin R$ FOR ALL π THEN $V(x)$ REJECTS ANY P^* WITH PROBABILITY $\geq 1/2$.

(P,V) IS HONEST-VERIFIER ZERO-KNOWLEDGE IF $\exists$ Sim S.T. $\forall (x,\Pi) \in R$ THE VIEW OF V UPON INTERACTING WITH $P(x,\Pi)$ IS INDISTINGUISHABLE FROM $Sim(x)$.

G1 SIMULATOR IS $(\infty, 0)$-HVZK.



A CHEATING V^* COULD CHOOSE HIS CHALLENGE b^* TO DEPEND ON G $(b^* = b^*(G))$

(P,V) IS (S,ε)-ZERO-KNOWLEDGE IF FOR EVERY V^* OF SIZE $\leq t$ AND EVERY $(x,\Pi) \in R$ THERE IS A SIMULATOR Sim S.T. $Sim(x)$ OUTPUTS A RV THAT IS (S,ε)-INDIST'LE FROM $(V^*(x) \longleftrightarrow P(x,\Pi))$.

SIMULATION OVERHEAD $oh(t)$ = EXTRA AMOUNT OF WORK Sim HAS TO DO.

Sim FOR G1:

- RANDOMLY GUESS V^* CHALLENGE b.
- SIMULATE 1ST PROVER MESSAGE $G = \phi(G_b)$
- IF V^* RESPONSE $b^* = b$, OUTPUT ϕ.

① $Sim(G_0, G_1)$ LOOKS LIKE $P(x, \pi) \leftrightarrow V^*(x)$

② $P(b^* = b)$ IS REASONABLE

view $|b^* = b$: G, b, ϕ S.T. $\phi(G_b) = G$

↑ RANDOM

IDENTICAL TO SIMULATED VIEW.

$G = \phi(G_0)$ w/p 1/2, $\phi(G_1)$ w/p 1/2 → V^*

b^* ←

IDENTICALLY DISTRIBUTED → IND. OF b → $P(b^* = b) = \frac{1}{2}$.

$oh(t)$: CONSISTS OF SAMPLING ϕ, b AND COMPUTING $\phi(G_b)$ → $O(n^2 + n \log n)$ EFFICIENT

n = # VERTICES

$1/2 \to 1/2^{100}$ → REPEAT 100 TIMES

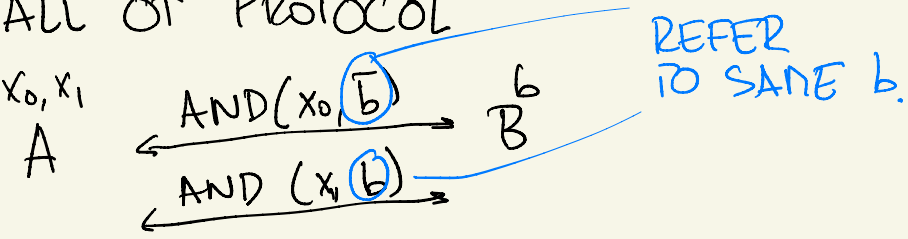
EG. ZKP STATEMENT $\exists X, Y$ S.T. $h = g^X, h' = g^Y, h'' = g^{XY}$

PROOF X, Y

ZERO-KNOWLEDGE PROOFS FOR ANY FACT

COMMITMENTS

RECALL OT PROTOCOL

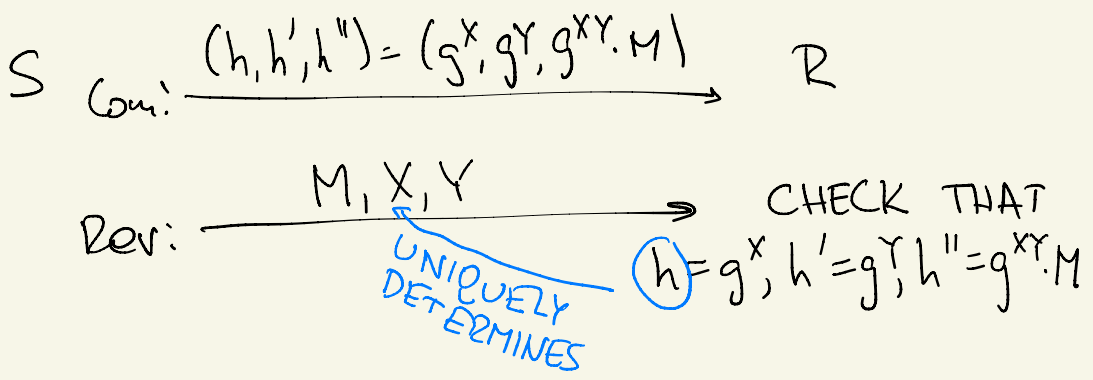


COMMITMENT SCHEME IS A 2-PHASE PROTOCOL BETWEEN SENDER AND RECEIVER

COMMITMENT S $\xrightarrow{C = \text{Com}(M)}$ R

DISCLOSURE $\xrightarrow{M}$

PROOF THAT M IS "DETERMINED" BY C



HIDING: COMMITMENTS ARE (S, ε)-SIMULATABLE WITHOUT KNOWING M.

BINDING: NO S^* OF SIZE $\leq s$ CAN DECOMMIT TO TWO DIFFERENT $M \neq M'$ WITH PROB. $> \varepsilon$

(Com, Rec) IS $(\infty, 0)$ - BINDING

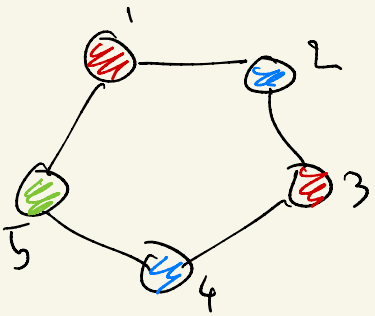
HIDING: Sim OUTPUTS IND. RANDOM $(h, h', h'') \sim (g^x, g^y, g^R)$

ASSUME (S, ε)-DDH, (g^x, g^y, g^R) $(S - t_X, \varepsilon)$ - IND. FROM $(g^x, g^y, g^{xy} \cdot M)$.

UNIVERSAL STATEMENTS

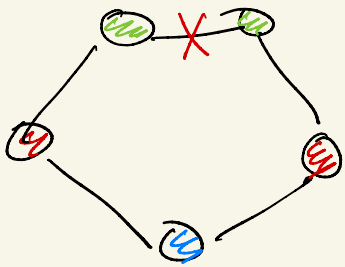
A 3-COLORING OF A GRAPH G IS AN ASSIGNMENT OF COLORS {R,G,B} TO VERTICES SO THAT NO EDGE HAS BOTH ENDPOINTS OF SAME COLOR.

G IS 3-COLORABLE IF THERE EXISTS A VALID 3-COLORING.

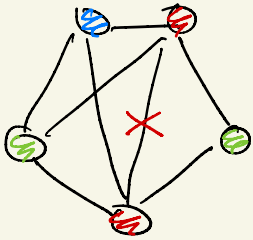


VALID 3-COL

π = RBRBG



NOT VALID



NOT VALID

NOT 3-COLORABLE

3COL PROOF RELATION

(G, π) : π IS A VALID 3COL OF G.

COMPLETE PROOF RELATION

EG. $A \leftarrow (h, h', h'') \rightarrow B$

(h, h', h''): STATEMENT

(X, Y): PROOF

$h = g^X, h' = g^Y, h'' = g^{XY}$: RELATION

CONVERT

Π: COLORING

G: GRAPH

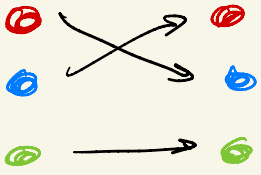
Π IS A 3COL OF G

- IF (X,Y) ARE DDH EXPONENTS $h = g^X, h' = g^Y, h'' = g^{XY}$ THEN Π IS A 3COL OF G.
- IF (h, h', h'') IS NOT A DDH TRIPLE THEN G IS NOT 3-COLORABLE.

GOLDREICH-MICALI-WIGDERSON PROTOCOL

$P(G, \Pi)$ $\qquad$ $V(G)$

RANDOMLY PERMUTE COLORS



$C_1 = Com(\Pi_1), \ldots, C_n = Com(\Pi_n)$ $\rightarrow$

$\leftarrow$ RANDOM EDGE (u, v) IN G

DISCLOSES Π_u, Π_v $\rightarrow$ (RANDOM DISTINCT COLORS)

ACCEPT IF $\Pi_u \neq \Pi_v$
AND DISCLOSURES VALIDATE

COMPLETENESS: $V(G)$ ACCEPTS $P(G,\pi)$ WITH PROB. 1 IF π IS A 3COL OF G.

SOUNDNESS: G NOT 3-COLORABLE $\rightarrow$ P^*'S COMMITMENT MUST CONTAIN PAIR (u^*, v^*) S.T. C_{u^*} AND C_{v^*} DECOMMIT TO SAME COLOR $\rightarrow (u,v) = (u^*, v^*)$ W/P $\geq \frac{1}{m}$

SO $P(P^* \text{ PASSES}) \leq 1 - 1/m$.

REPEAT mk TIMES $\rightarrow (1 - 1/m)^{mk} \leq e^{-k}$.

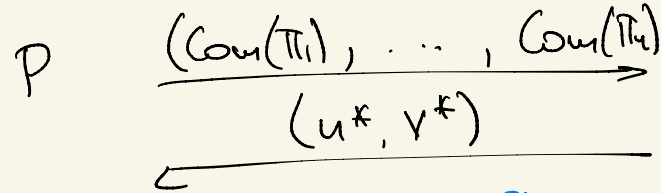
ZERO KNOWLEDGE

MODEL: V OBSERVES ONLY TWO RANDOM DISTINCT COLORS

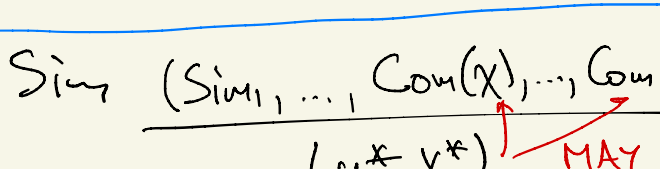
- ISSUE 1: Com IS NOT PERFECTLY HIDING
- ISSUE 2: V^* CAN CHOOSE (u^*, v^*) AS A FUNCTION OF $(C_1, \ldots, C_n)$.

Simulator for V^*:

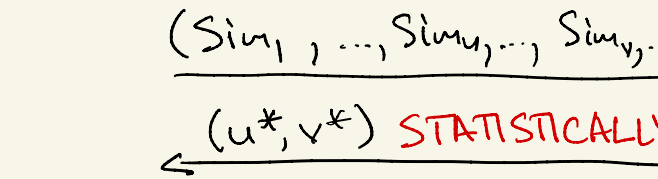
- Guess (u, v) at random
- Simulate commitments except for (u, v) where $C_u = \mathrm{Com}(\chi)$, $C_v = \mathrm{Com}(\chi')$ for two random distinct colors.
- If $u^* = u$ and $v^* = v$, output (V^*'s randomness, $C_1, \ldots, C_n, \chi, \chi'$).
- If not, repeat.



$(\leq \ldots, (n-2)\ell)$-IND



$(\leq \ldots, 2\ell)$-IND



$$P[(u^*, v^*) = (u, v)] = \frac{1}{n} \longrightarrow P[(u^*, v^*) = (u, v)] \geq \frac{1}{n} - 2\varepsilon$$

IN SIMULATED INTERACTION