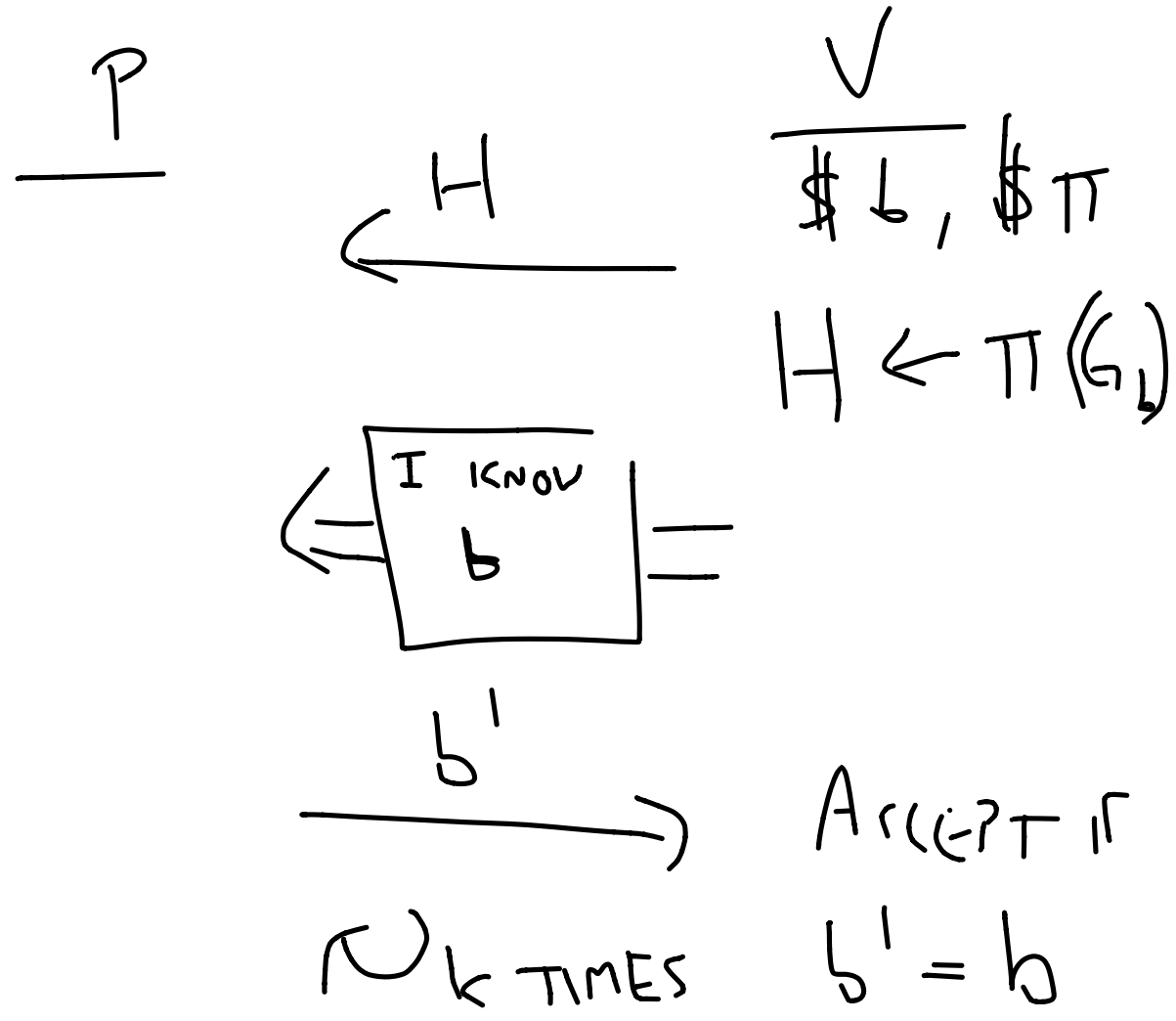
ZK FOR GNI

IDEA:



ZK FOR GNI

$G_0 \not\sim G_1$

P

V

$\$ \pi_0, \pi_1$

$\$ b$

IF $b = 0$:

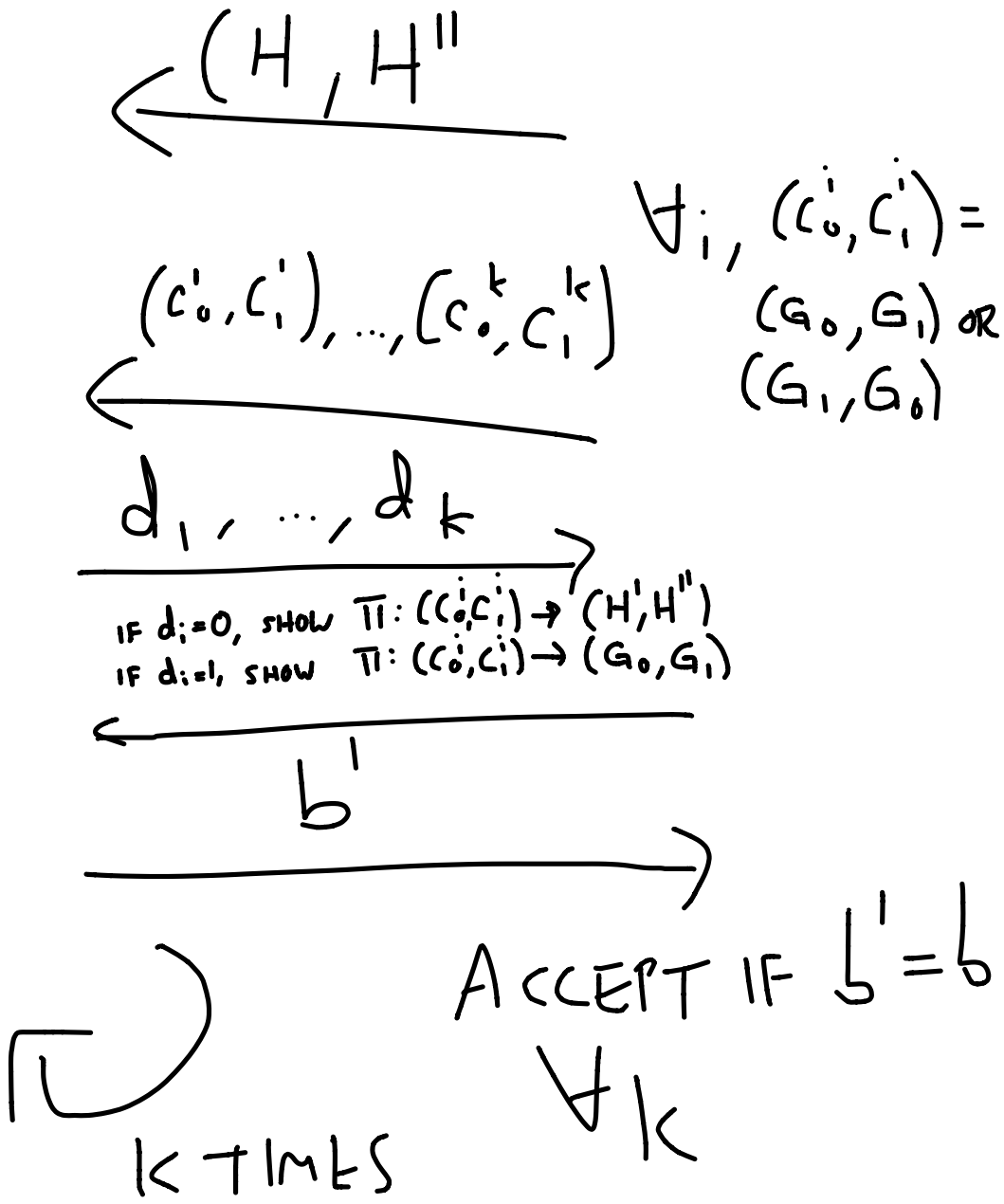
$(H', H'') =$

(H_0, H_1)

IF $b = 1$

$(H', H'') =$

(H_1, H_0)


(H, H'')
∀i, (C_0^i, C_1^i) =
(G_0, G_1) OR
(G_1, G_0)
(C_0^1, C_1^1), ..., (C_0^k, C_1^k)
d_1, ..., d_k
IF d_i=0, SHOW Π: (C_0^i, C_1^i) → (H', H'')
IF d_i=1, SHOW Π: (C_0^i, C_1^i) → (G_0, G_1)
b'
ACCEPT IF b'=b
∀k
k TIMES

WHY ZK?

S_v ASKS FOR

$\Pi : (C_0', C_1') \to (H', H'')$

RESETS, & ASKS FOR

$\Pi' : (C_0', C_1') \to (G_0, G_1)$

BY SENDING $\overline{d_1}$.

THIS GIVES

$\Pi'^{-1} \circ \Pi' : (H', H'') \to (G_0, G_1)$

+ REVEALS b TO S_v

WHO THEN SENDS $b' = b$.

COMPLETENESS

IF P KNOWS $G_0 \neq G_1$,

KNOWS IF $(H', H'') =$

(G_0, G_1) OR (G_1, G_0)

& ALWAYS GETS $b' = b$

SOUNDNESS:

IF P^* DOESN'T KNOW $G_0 \nsim G_1$, CAN ONLY GUESS b' W/ PROB. $\frac{1}{2}$

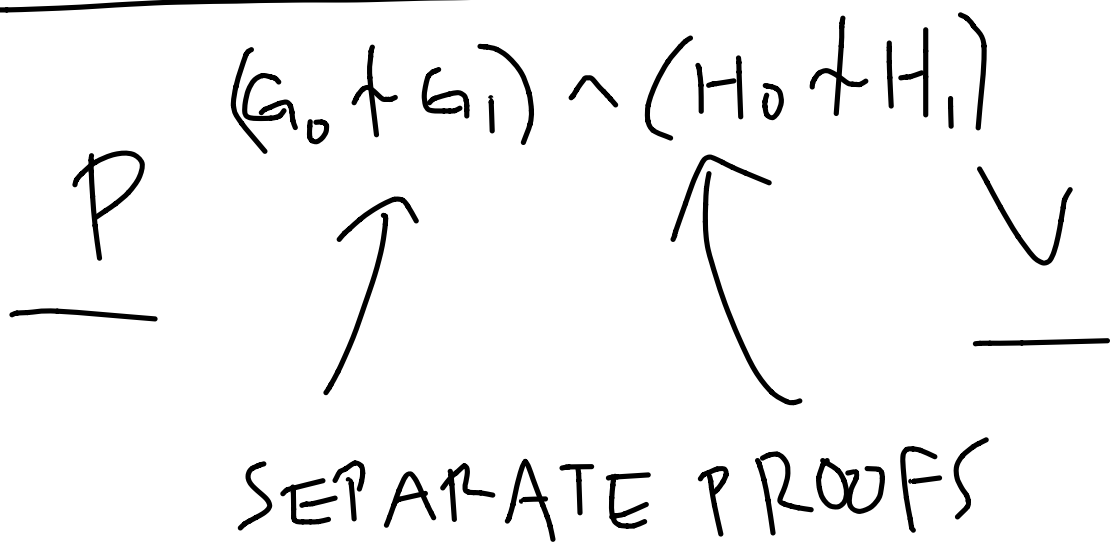
AFTER k TRIALS,

$$\Pr[\text{ACCEPT}] = \frac{1}{2^k}$$

CAN REPEAT IN PARALLEL!

NOT SEQUENTIAL.

PROVING "OR" & "AND"



SEPARATE PROOFS

WHAT ABOUT OR?

DOESN'T WANT TO REVEAL WHICH DISJUNCTS ARE TRUE.

(G_0, G_1) V (H_0, H_1)

P — V

RUN BOTH IN PARALLEL W/ SAME RANDOM BIT b.

IF T GETS $b' = b$, MUST KNOW G_0 & G_1 OR H_0 & H_1.

WHAT ABOUT

$(G_0 \sim G_1) \vee (H_0 \sim H_1)$?

P

b_1, b_2

π_1, π_2

V

b

$C_0 = \pi_1(G_{b_1})$

$C_1 = \pi_1(G_{1-b_1})$

$D_0 = \pi_2(H_{b_2})$

$D_1 = \pi_2(H_{1-b_2})$

$(C_0, C_1), (D_0, D_1)$

SHOW ME $b_1 \oplus b_2 = b$

IF $G_0 \neq G_1$ & $H_0 \neq H_1$,
b_1 & b_2 UNIQUELY DEFINED,
50% CHANCE P CAN'T
MAKE $b_1 \oplus b_2 = b$

OTHERWISE, P CAN CHOOSE
VALUE OF EITHER b_1 OR
b_2 FREELY & CAN ALWAYS
REVEAL $b_1 \oplus b_2 = b$.

ZK FOR ALL OF NP

REMINDER:

GRAPH 3-COLORING

IS NP-COMPLETE

IF WE PROVE G IS

3 COLORABLE IN ZK

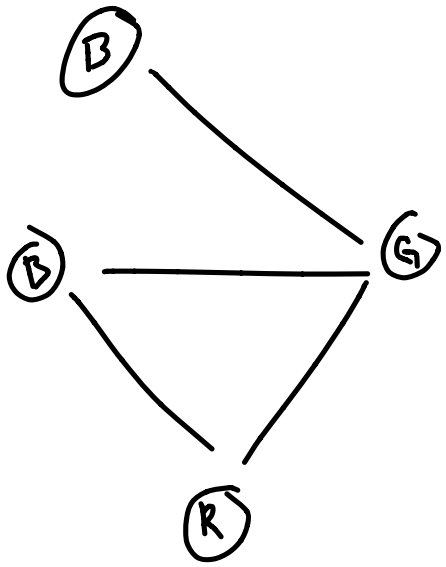
CAN PROVE ANY NP

STATEMENT IN NP

THM [GMW]

ASSUMING A COMMITMENT SCHEME, ∃ A ZK PROOF FOR ALL OF NP.

$G =$



IDEA: P PERMUTES COLORS, COMMITS TO COLOR OF EVERY NODE.

V ASKS FOR OPENING OF NODES ON A RANDOM EDGE.

ACCEPT IF NODES ARE DIFFERENT COLORS FOR ALL k TRIALS W/ FRESH RANDOM PERMUTATION.

COMPLETENESS:

TRIVIAL

SOUNDNESS:

$$\Pr[\text{CAUGHT}] \geq \frac{1}{|\mathcal{C}|}$$

IN EACH TRIAL

$\Pr[\text{ACCEPT FALSE STATEMENT}]$

= CONSTANT FOR $|\mathcal{C}|$ TRIALS.

FOR $|\mathcal{C}| \cdot k$ TRIALS, NEGLIGIBLE IN k

Zero Knowledge:

S_V knows ahead of time which edge V will ask for, just commit different colors on that edge.

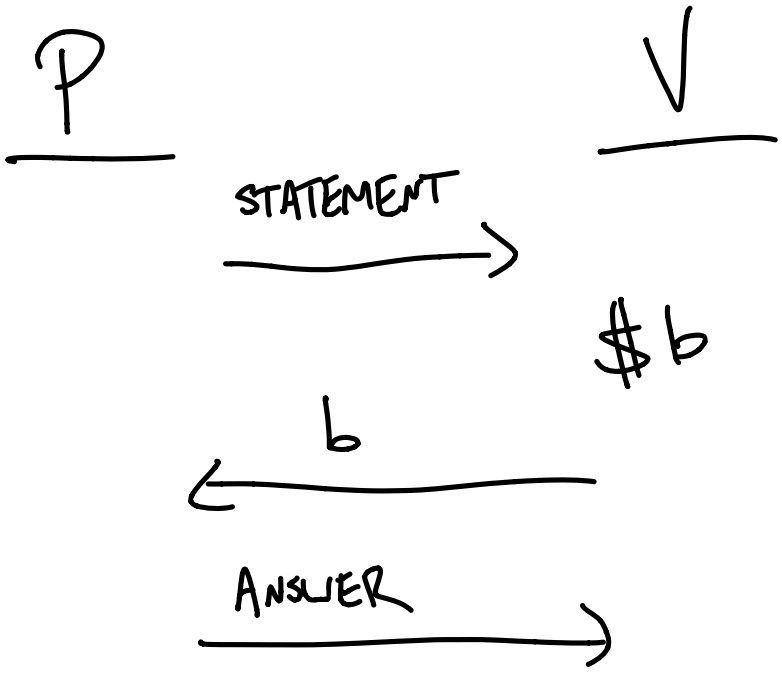
For V^*, reset if guess wrong edge

Argument Vs. Proof

Proof: P_{∞}, V_{ppt}

Arg: P_{ppt}, V_{∞}

BLUM'S PROTOCOL (SIGMA PROTOCOL)

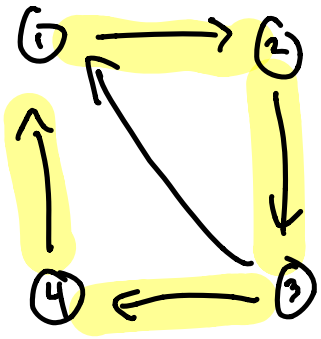


IF $x \notin L$, V REJECTS W/ PROBABILITY $\frac{1}{2}$

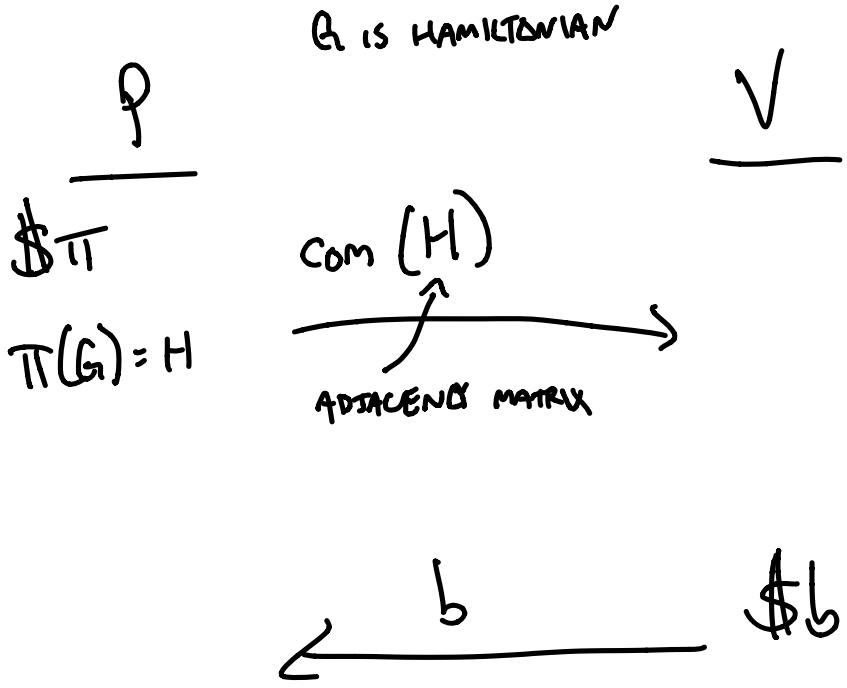
IDEA: $L = \{$ GRAPHS G W/ HAMILTONIAN CYCLE $\}$

NOTE: L IS NP-COMPLETE

INTUITION: G, $|G|=n$ HAMILTONIAN IFF ADJACENCY MATRIX HAS n ENTRIES SUCH THAT EACH IS IN DIFFERENT ROW/COLUMN & EACH IS EQUAL TO 1.



	1	2	3	4
1	0	1	0	0
2	0	0	1	0
3	1	0	0	1
4	1	0	0	0



IF $b=0$, SEND π, OPEN EVERYTHING

IF $b=1$, OPEN ONLY CYCLE EDGES IN H

COMPLETENESS: TRIVIAL

SOUNDNESS: IF G NOT HAMILTONIAN, P EITHER SENDS HAMILTONIAN $H \neq \pi(G)$ (CAUGHT IF $b=0$) OR SENDS NON-HAMILTONIAN $H = \pi(G)$ (CAUGHT IF $b=1$)

ZERO KNOWLEDGE: IF S_V KNOWS b IN ADVANCE, CAN EITHER SEND HAMILTONIAN $H \neq \pi(G)$ WHEN $b=1$ OR NON-HAMILTONIAN $H = \pi(G)$ WHEN $b=0$.

WHY IS ZK IMPORTANT?

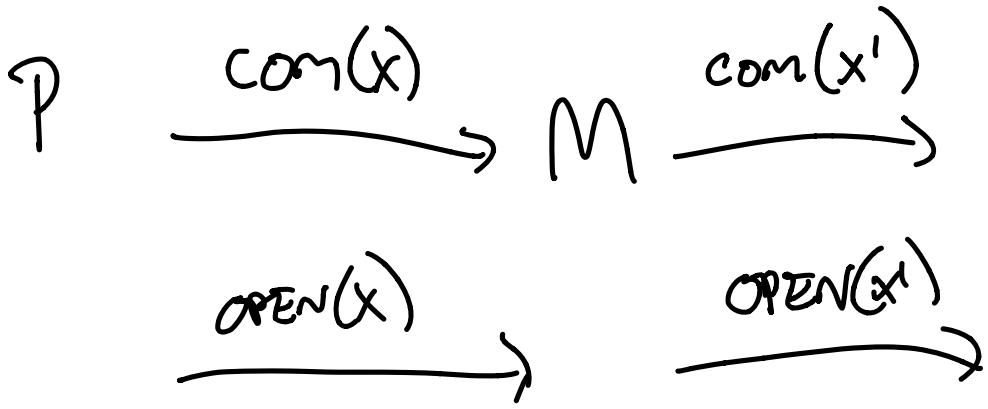
EXAMPLE (a): NON-MALLEABLE COMMITMENTS

IDEA: WHAT IF YOU CAN CREATE

$COM(X')$ FROM $COM(X)$

WITHOUT OPENING $COM(X)$?

EXAMPLE: AUCTIONING



IF $X' = X+1$, M ALWAYS OUTBIDS P

SOLUTION: WHEN COMMITTING TO X, PROVE IN ZK THAT I KNOW VALUE X.

REQUIRES PROOF OF KNOWLEDGE

AN IP IS A PROOF OF KNOWLEDGE

THAT $X \in L$ IF AN EXTRACTOR $E \in PPT$

WHICH, GIVEN ACCESS TO THE CODE

OF P, CAN OUTPUT THE WITNESS

W TO THE FACT THAT $X \in L$.

EXAMPLE (b): HONEST-BUT-CURIOUS → MALICIOUS SECURITY

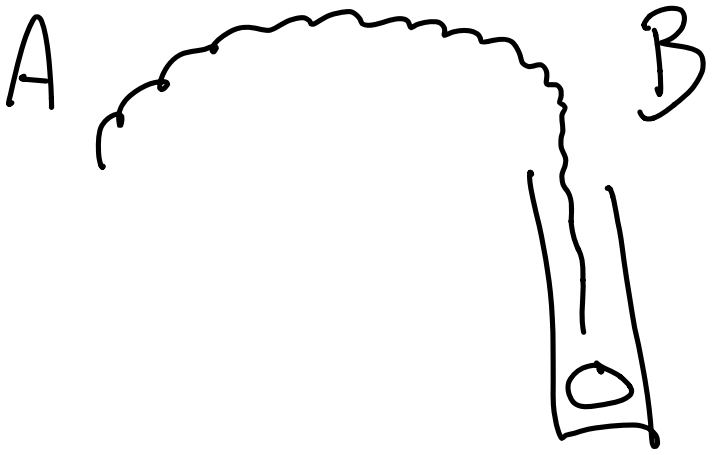
IDEA: SUPPOSE PROTOCOL IS SECURE AS LONG AS ALL PLAYERS BEHAVE ACCORDING TO THE PROTOCOL.

CAN GET MALICIOUS SECURITY BY MAKING PLAYERS PROVE IN ZK THAT THEY ARE ACTING ACCORDING TO PROTOCOL SPECIFICATION.

PROBLEM: HOW DO WE KNOW MALICIOUS P_i IS USING RANDOM RANDOMNESS?

SOLUTION: COIN FLIP INTO THE WELL

PICTURE:



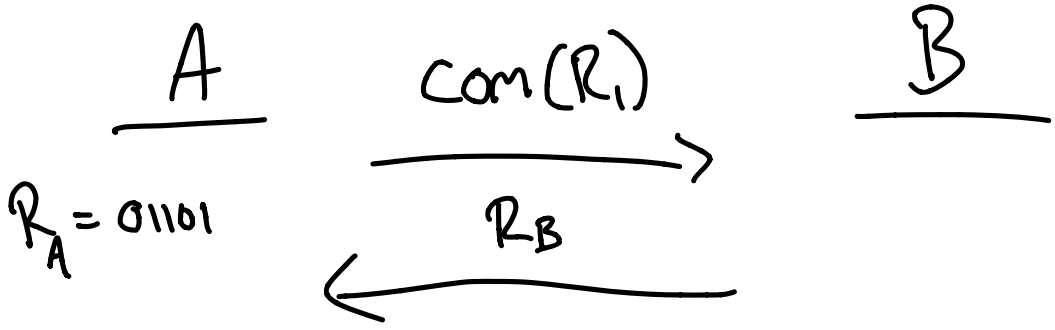
ALICE FLIPS, BOB SEES RESULTING COIN.

How does this help?

P_1 chooses P_2 randomness,

P_2 chooses P_1 randomness

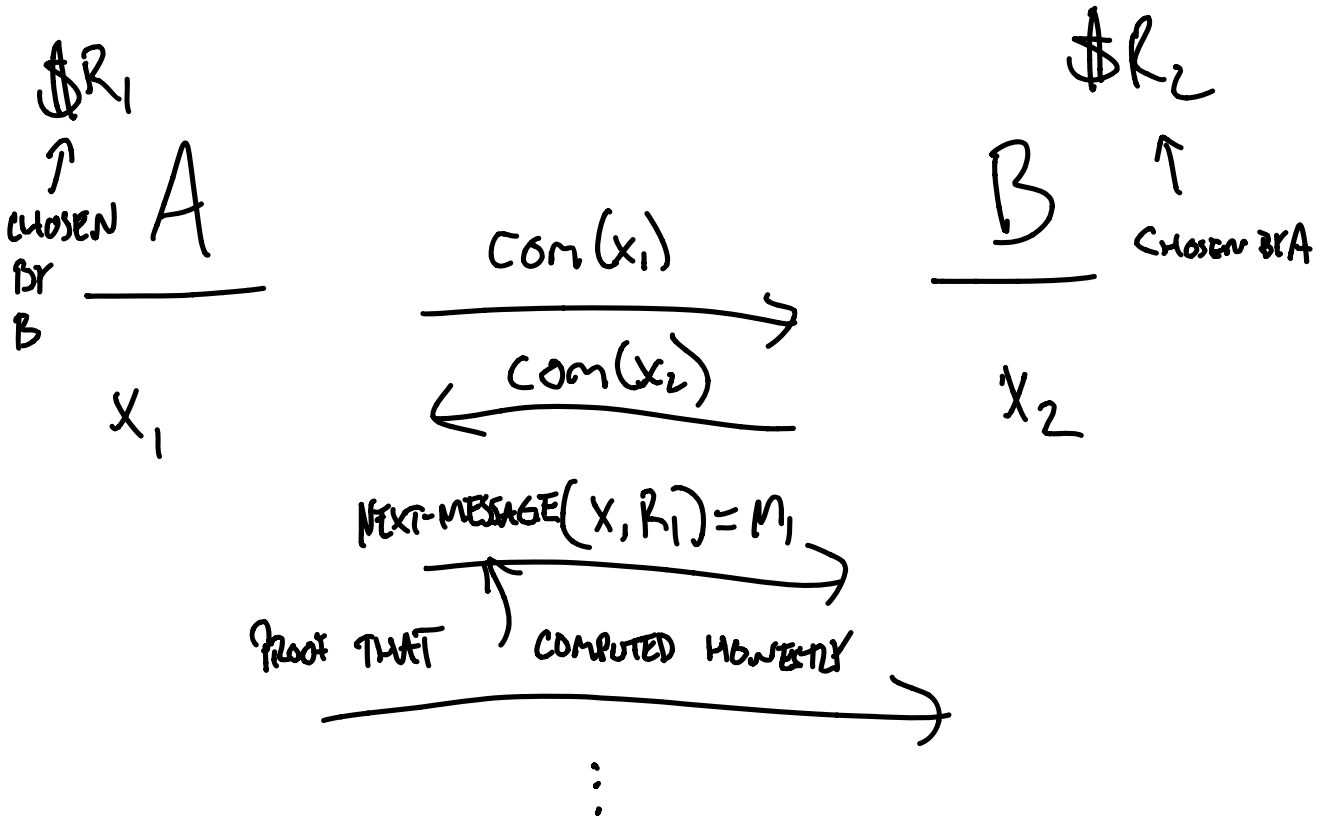
Protocol: B flips coin into A's well



A's randomness

$R_1 = R_A \oplus R_B$

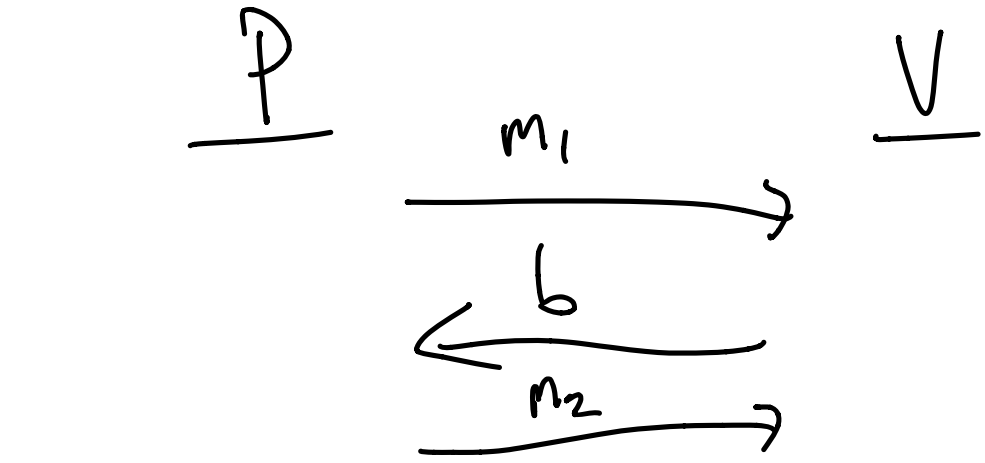
HBC → MALICIOUS SECURITY:



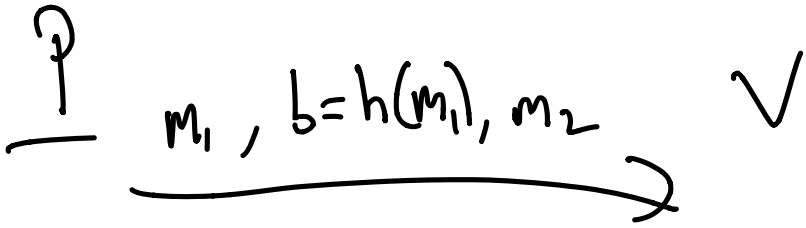
EXAMPLE (3): IDENTIFICATION

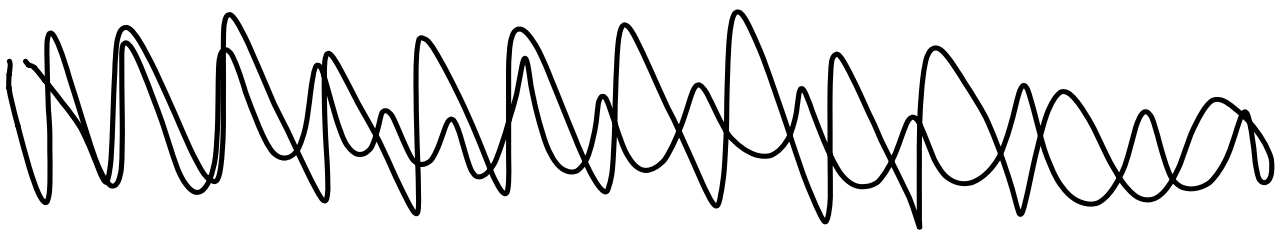
COROLLARY: FIAT-SHAMIR HEURISTIC

SUPPOSE ALL OF V'S MESSAGES IN PROTOCOL ARE JUST RANDOM BITS (AKA SIGMA PROTOCOL). THEN WE CAN MAKE PROTOCOL NON-INTERACTIVE BY HAVING PROVER COMPUTE BITS OF V USING HASH FUNCTION!


P
V
m_1
b
m_2


FIAT-SHAMIR

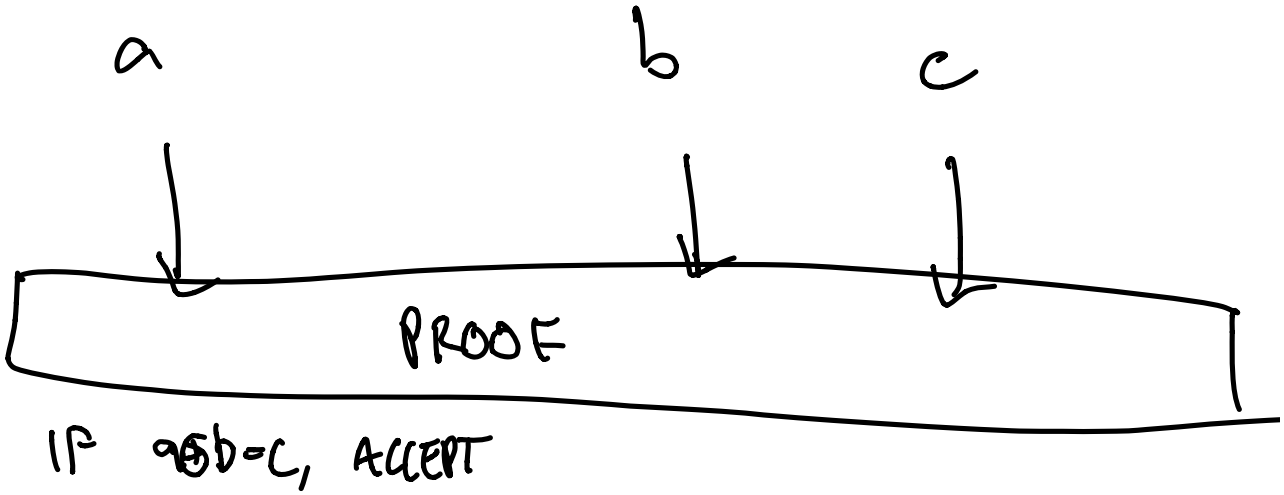

P
$m_1, b = h(m_1), m_2$
V



PROBABILISTICALLY CHECKABLE PROOFS

IDEA: PUBLISH LONG PROOF.

VERIFIER CONVINCED BY ONLY CHECKING A FEW RANDOM BITS OF THE PROOF.



EXAMPLE: CAN TRANSLATE 3-SAT FORMULA

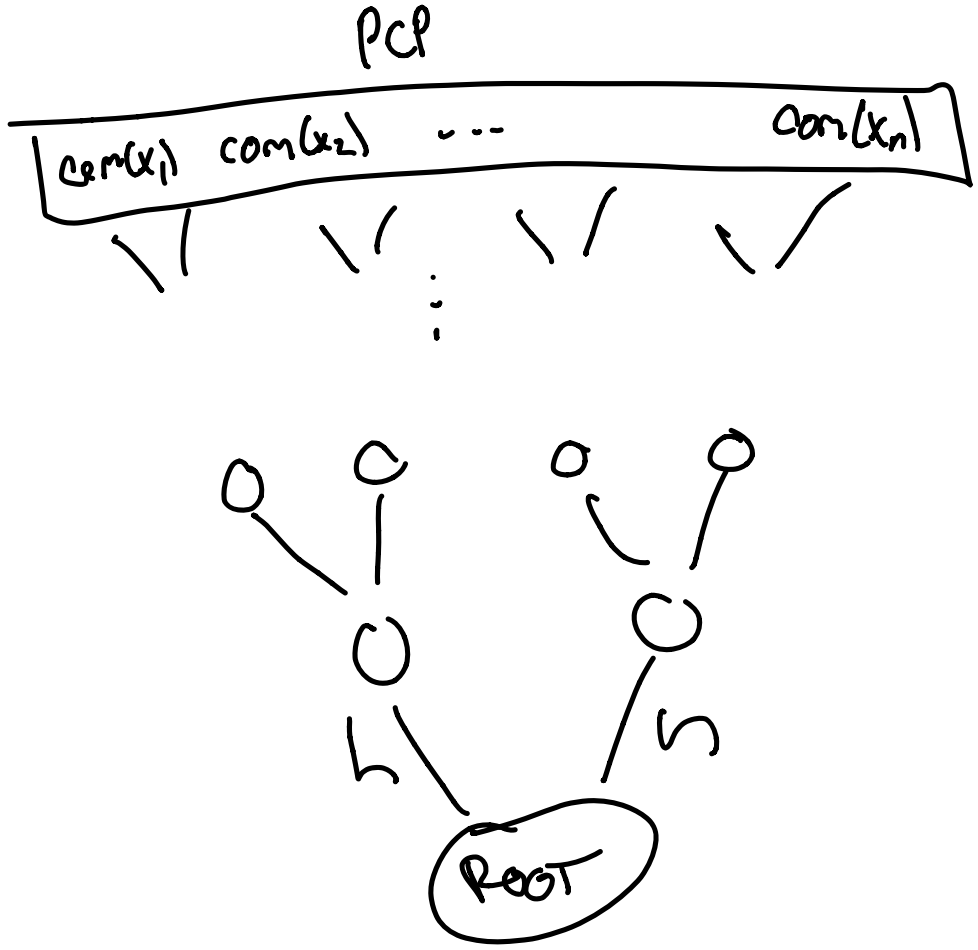
$\Phi \rightarrow \Phi'$ SUCH THAT

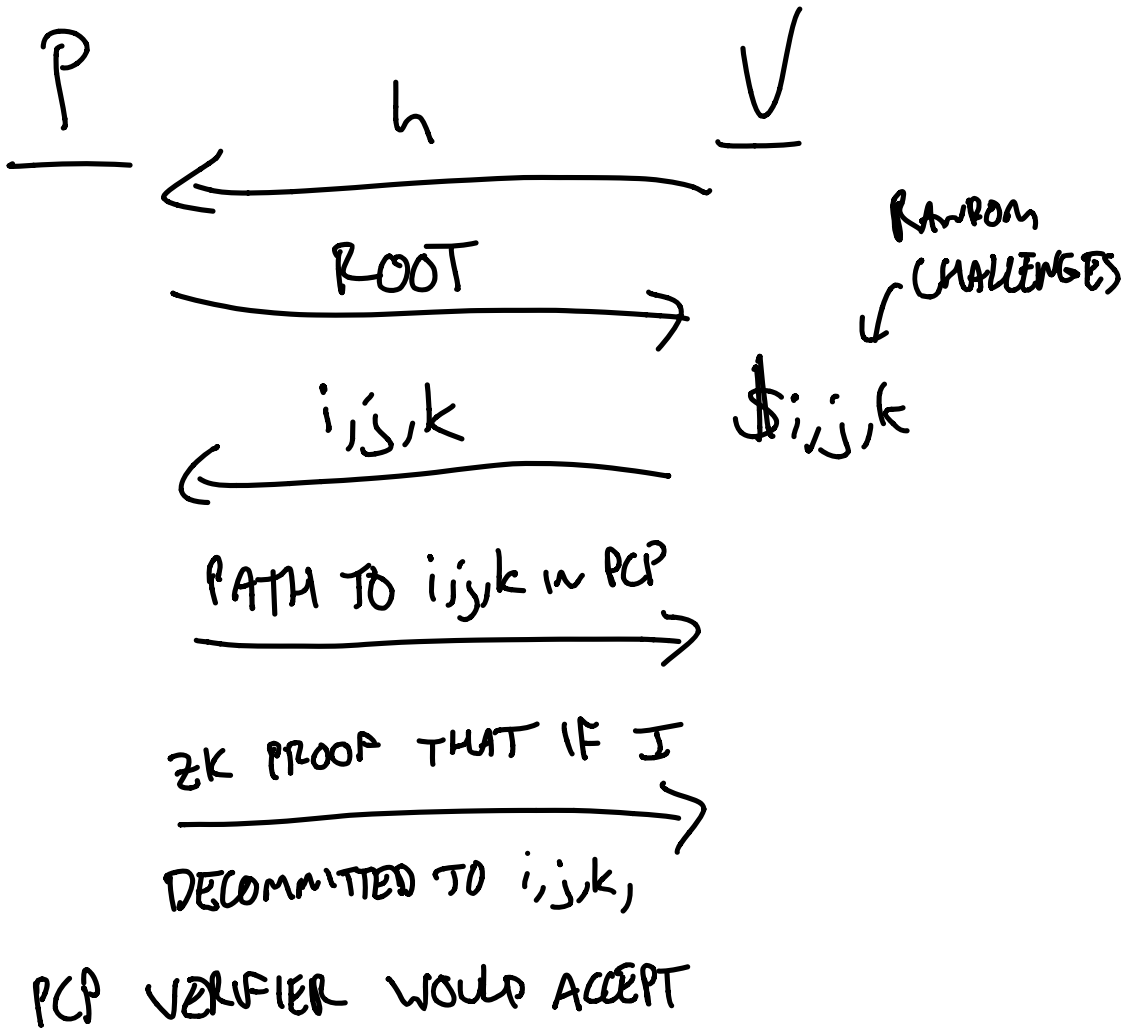
- Φ SATISFIABLE $\Rightarrow$ Φ' SATISFIABLE
- Φ NOT SATISFIABLE $\Rightarrow$ >90% OF CLAUSES IN Φ' MUST BE UNSATISFIABLE

PCP = SATISFYING ASSIGNMENT FOR Φ'

V CHECKS A FEW RANDOM CLAUSES, CHECKS IF TRUE, & ACCEPTS IF ALL TRUE.

IN PRACTICE, DON'T WANT TO SEND GIANT PCP, SO WE USE MERKLE HASH TREE





MAIN TAKEAWAY: PROOF IS COMPACT EVEN WHEN STATEMENT IS HUGE.