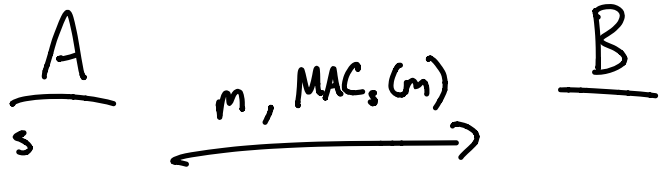
MACs: Message Authentication Codes



Eavesdropper cannot authenticate $m' \neq m$ without secret s.

Idea: $s = a, b$ coefficients of line $y = ax + b$

$$MAC_s(m) = a \cdot m + b$$

If E sees only one MAC, has only one evaluation point. Cannot know a, b except by guessing with probability $\frac{1}{|F|}$, where F is the field.

WEAKNESS: $S = a, b$ ONLY GOOD FOR 1 MESSAGE.

IF REUSED, ALL SECURITY BROKEN.

STRENGTH: INFORMATION - THEORETIC SECURITY

GENERALIZED NOTION: PAIRWISE INDEPENDENCE

GIVEN $h(x)$, $h(y)$ LOOKS RANDOM

IN PRACTICE, CAN GENERATE $S = a, b$ FROM A PRG

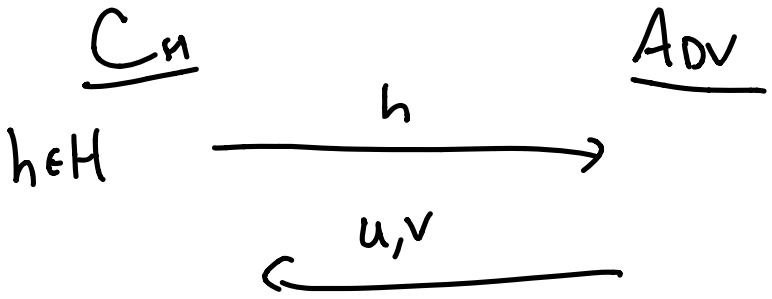
AND GET MANY KEYS EFFICIENTLY.

IS THERE A NOTION BETWEEN

PAIRWISE INDEPENDENCE AND COLLISION RESISTANCE?

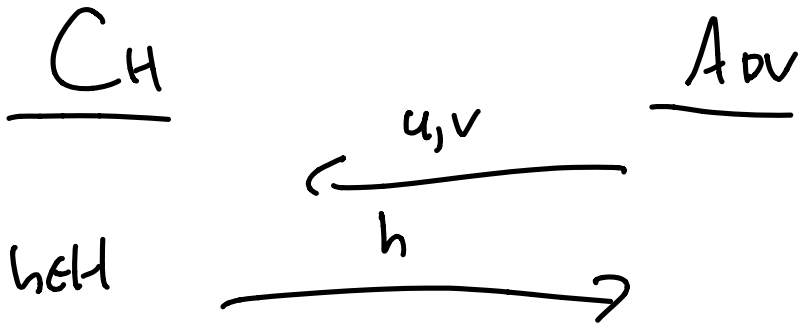
REMINDER: COLLISION RESISTANT HASH

H IS COLLISION RESISTANT HASH FUNCTION FAMILY IF, $Pr[\text{ADV WINS}]$ IS NEGLIGIBLE



ADV WINS IF $h(u) = h(v)$

WHAT IF ADV CHOOSES u, v FIRST?



ADV WINS IF $h(u) = h(v)$

THIS IS PRECISELY PAIRWISE INDEPENDENCE

IDEA:

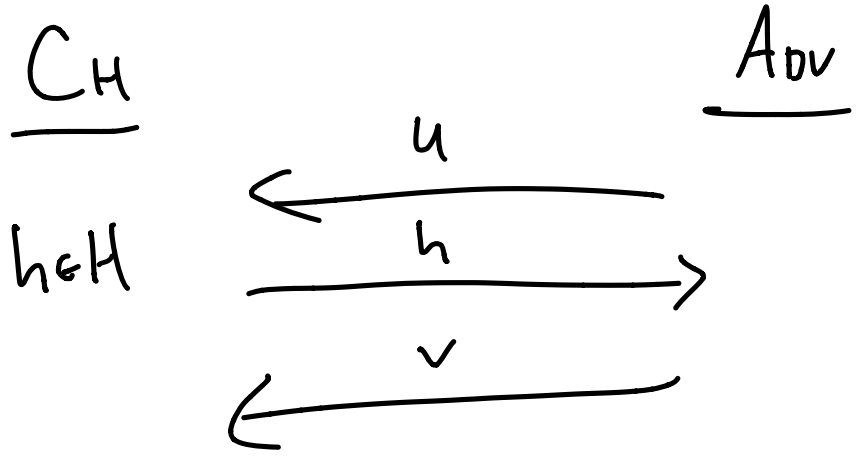
ADV CHOOSES TWO RANDOM X VALUES,

CH CHOOSES A RANDOM LINE $y = ax + b$.

ADV WINS IF $au + b = av + b \pmod n$

WITH PROBABILITY $> \frac{1}{n}$ ← FIELD SIZE

WHAT ABOUT IN BETWEEN?



IF $\Pr[h(u) = h(v)] < \frac{1}{|H|}$, THIS IS CALLED

UNIVERSAL ONE-WAY HASH FUNCTION

THIS IS A WEAKER NOTION THAN COLLISION-RESISTANCE, AND WE CAN BUILD UOWH FROM OWFs.

☆ Let's build digital signatures from UOWH instead!

Reminder: Lamport's 1-time Signatures

$sk =$

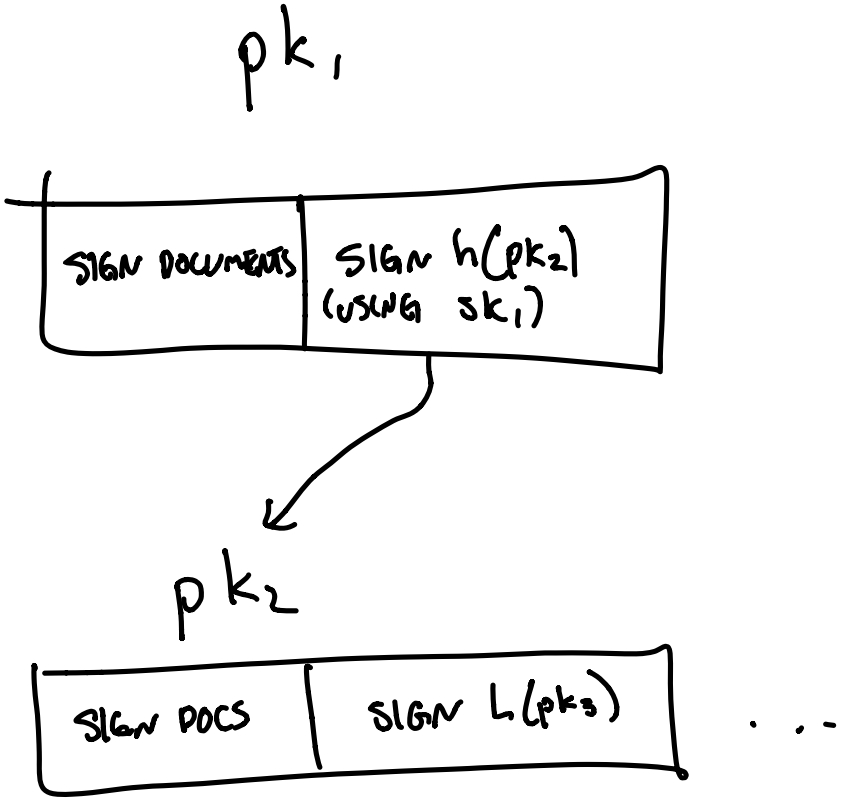
x_1	x_3	x_5
x_2	x_4	x_6

$pk =$

$f(x_1)$	$f(x_3)$	$f(x_5)$
$f(x_2)$	$f(x_4)$	$f(x_6)$

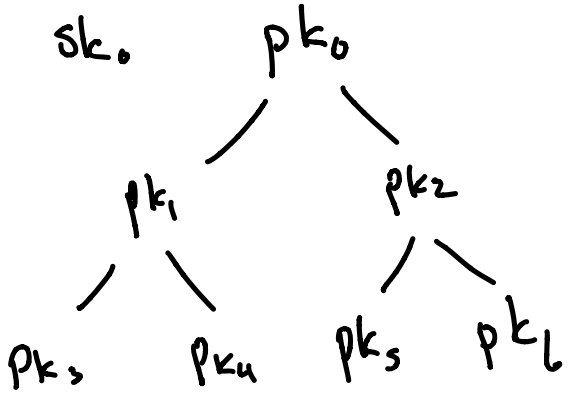
$Sig(D = 001) = x_1 \; x_3 \; x_6$

WHEN WE RUN OUT OF ROOM IN OUR sk, NEED TO PUBLISH NEW pk, sk PAIR AND SIGN IT WITH OLD pk SO EVERYONE KNOWS BOTH pk_1 & pk_2 BELONG TO SAME PERSON.



CREATES LINKED LIST OF pk_s TO KEEP SIGNING DOCUMENTS. NOW, WE NEVER RUN OUT OF ROOM IN sk!

CAN SHORTEN VERIFICATION BY BUILDING A TREE INSTEAD OF A LIST.



SIGN $h(pk_1, pk_2)$ WITH pk_0, sk_0

CAN ALSO USE PRG TO GENERATE SECRET KEYS.

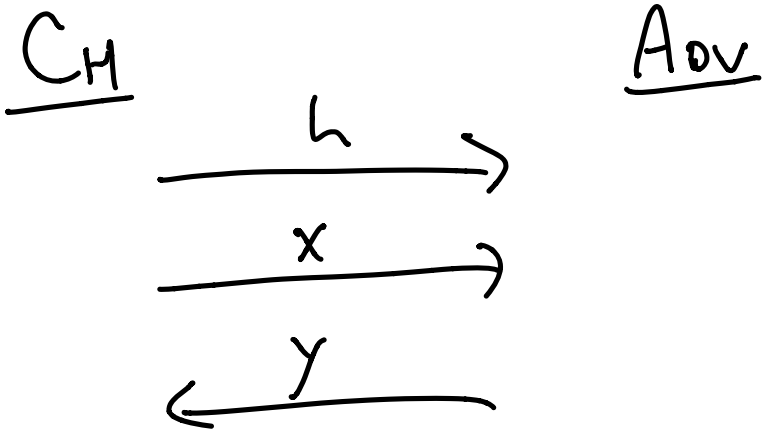
BUT: NEEDS COLLISION-RESISTANT HASH FUNCTION SO THAT FORGING SIG(h(D)) IS AS HARD AS FORGING SIG(D). OTHERWISE, ADV COULD PUBLISH FAKE pk^* AND LINK IT TO MY PERSONAL pk. IDENTITY THEFT!

CAN WE MAKE IT WORK WITH UNIVERSAL 1-WAY HASH FUNCTION INSTEAD? THEN WE DON'T NEED TRAPDOORS, JUST 1WF

IDEA: pk_0 IS PUBLIC.

SO ADVERSARY CAN'T COME UP WITH A RANDOM COLLISION.

MUST FIND COLLISION ON SPECIFICALLY pk_0.



ADV MUST FIND y S.T. $h(y) = h(x)$

THIS IS PRECISELY UWH

BUT WHERE u IS CHOSEN BY CH!

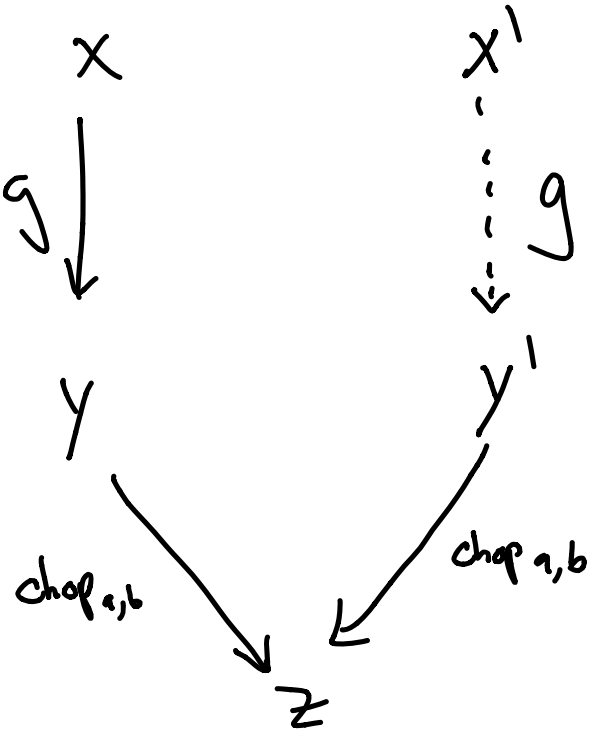
HOW TO BUILD U1WHF

FROM 1WP?

LET $g : (n+1)$ BITS $\to (n+1)$ BITS BE 1WP

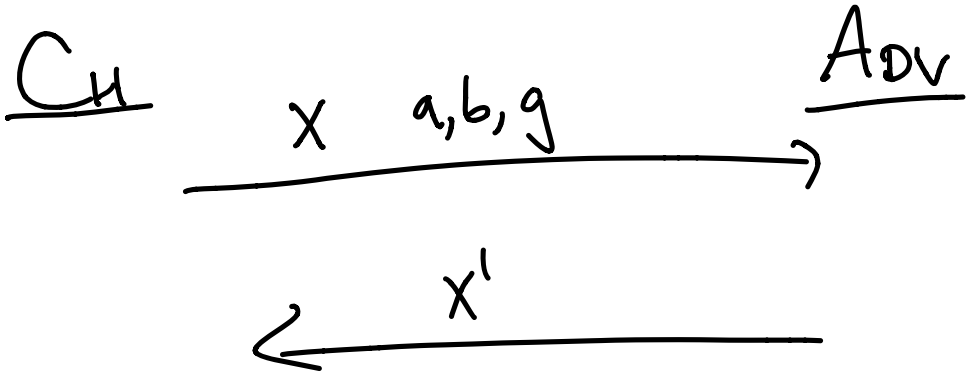
DEFINE $\text{Chop}_{a,b}(y) = \underbrace{ay+b}_{\text{DELETE LAST BIT}}$

$$UwH_{g,a,b} := chop_{a,b}(g(x))$$



2 TO 1 BECAUSE chop IS 2 TO 1 + g IS 1 TO 1

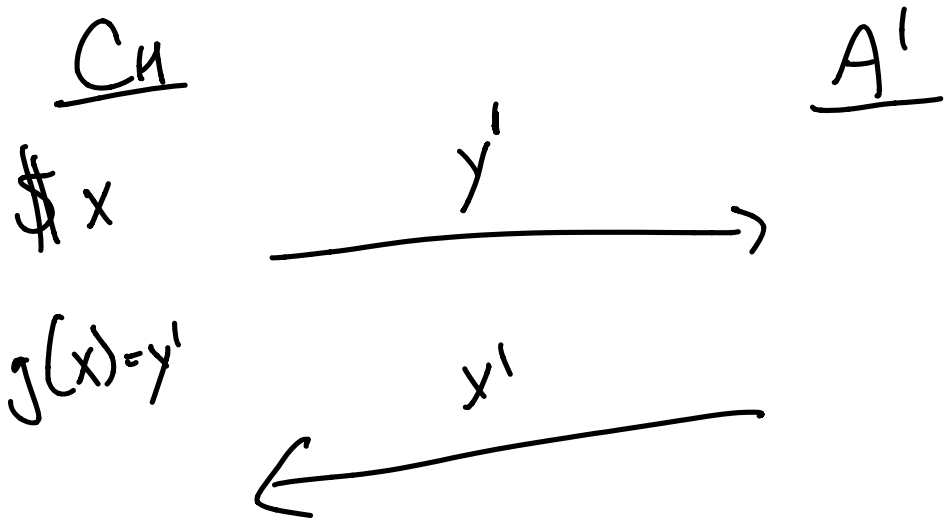
WHY IS THIS UNIVERSAL 1-WAY?



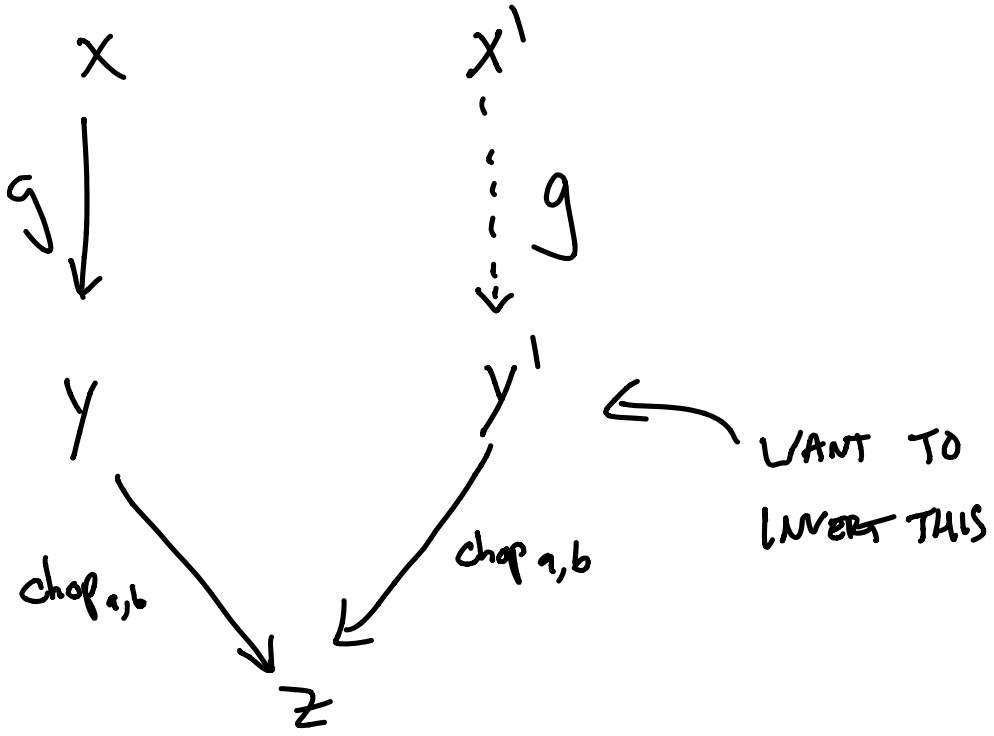
ADV WINS IF $chop_{a,b}(g(x)) = chop_{a,b}(g(x'))$

GIVEN AN ADV WHO WINS THIS GAME, WE CAN USE ADV TO CONSTRUCT A' WHO INVERTS THE OWP g.

THAT IS,



A' wins if $g(x') = y'$



CHOOSE $x, COMPUTE $g(x) = y$.

CHOOSE RANDOM z AND FIND a, b

S.T. $\text{chop}_{a,b}(y) = z = \text{chop}_{a,b}(y')$. THAT IS,

$ay + b = z\,0$ AND $ay' + b = z\,1$

2 VARIABLES a, b, 2 EQUATIONS, JUST SOLVE.

THEN, GIVE UWH ADV X, Z

AND IT WILL SPIT OUT X', SUCCESSFULLY INVERTING Y'.

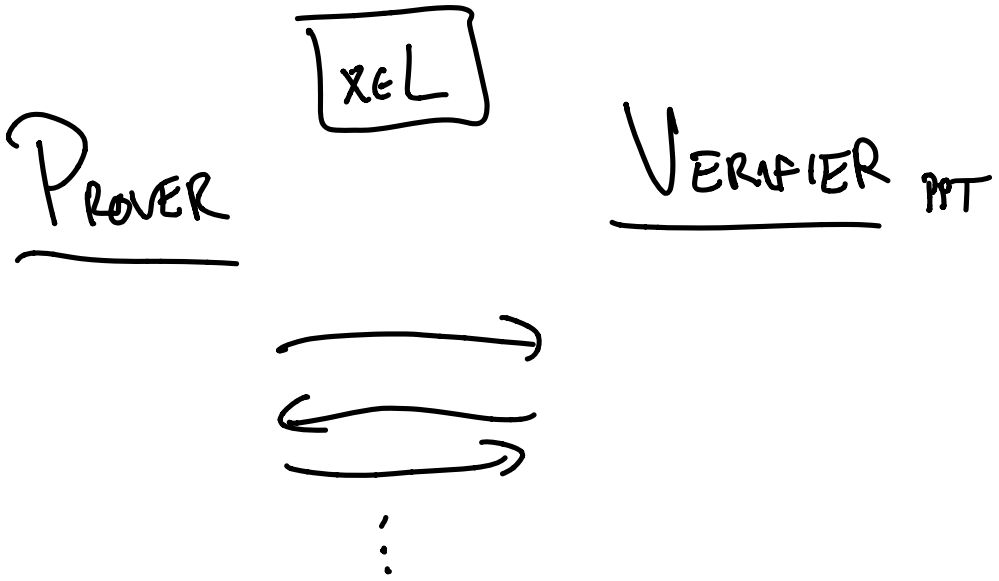
CAN DO THIS POLYNOMIALLY-MANY TIMES IN SUCCESSION TO GET UWH: $\text{poly}(n) \to n$

Zero Knowledge Proofs

Idea: Prove knowledge that a particular statement is true without revealing how you know the statement is true.

Example: Proving I can tell difference between Coca-Cola & Pepsi by passing blind taste test 10 times in a row.

BACKGROUND: INTERACTIVE PROOFS



L HAS AN IP IF:

① COMPLETENESS

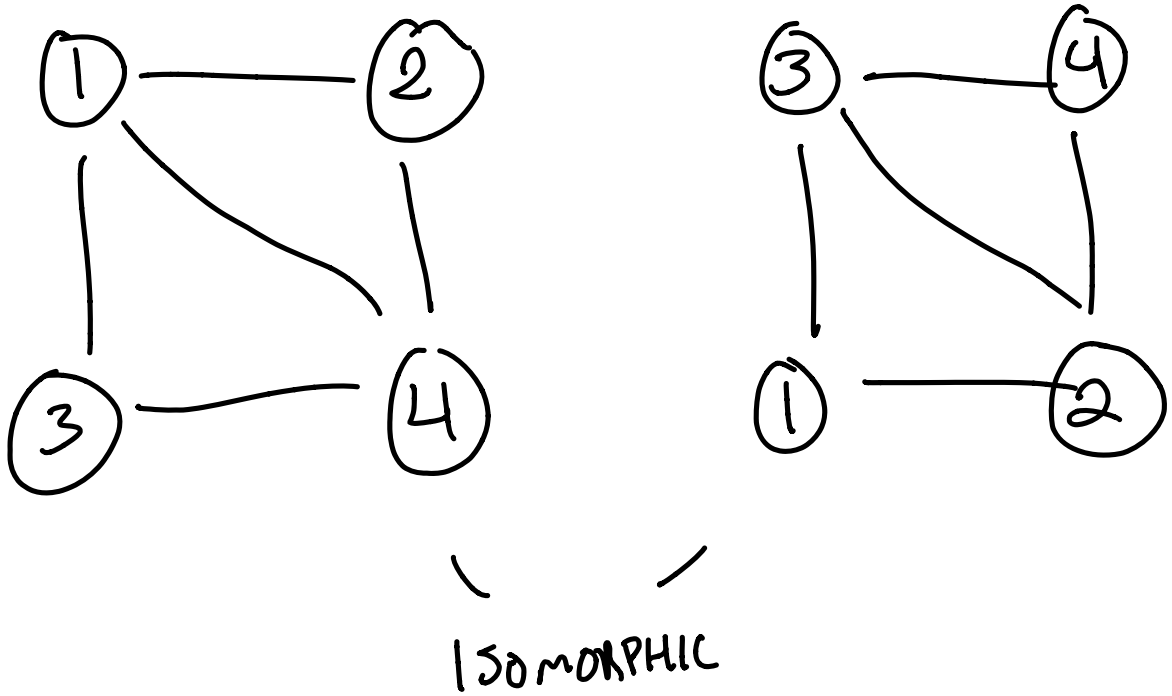
IF P IS HONEST, HAS STRATEGY TO CONVINCE V

② SOUNDNESS

IF DISHONEST P^* CANNOT CONVINCE V EXCEPT W/ NEGLIGIBLE PROBABILITY

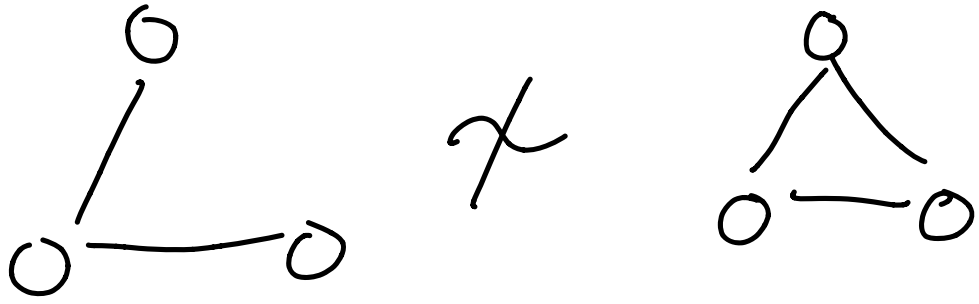
AMAZINGLY, WE CAN PROVE THINGS INTERACTIVELY WHICH CANNOT BE PROVEN OTHERWISE!

EXAMPLE: GRAPH NON-ISOMORPHISM

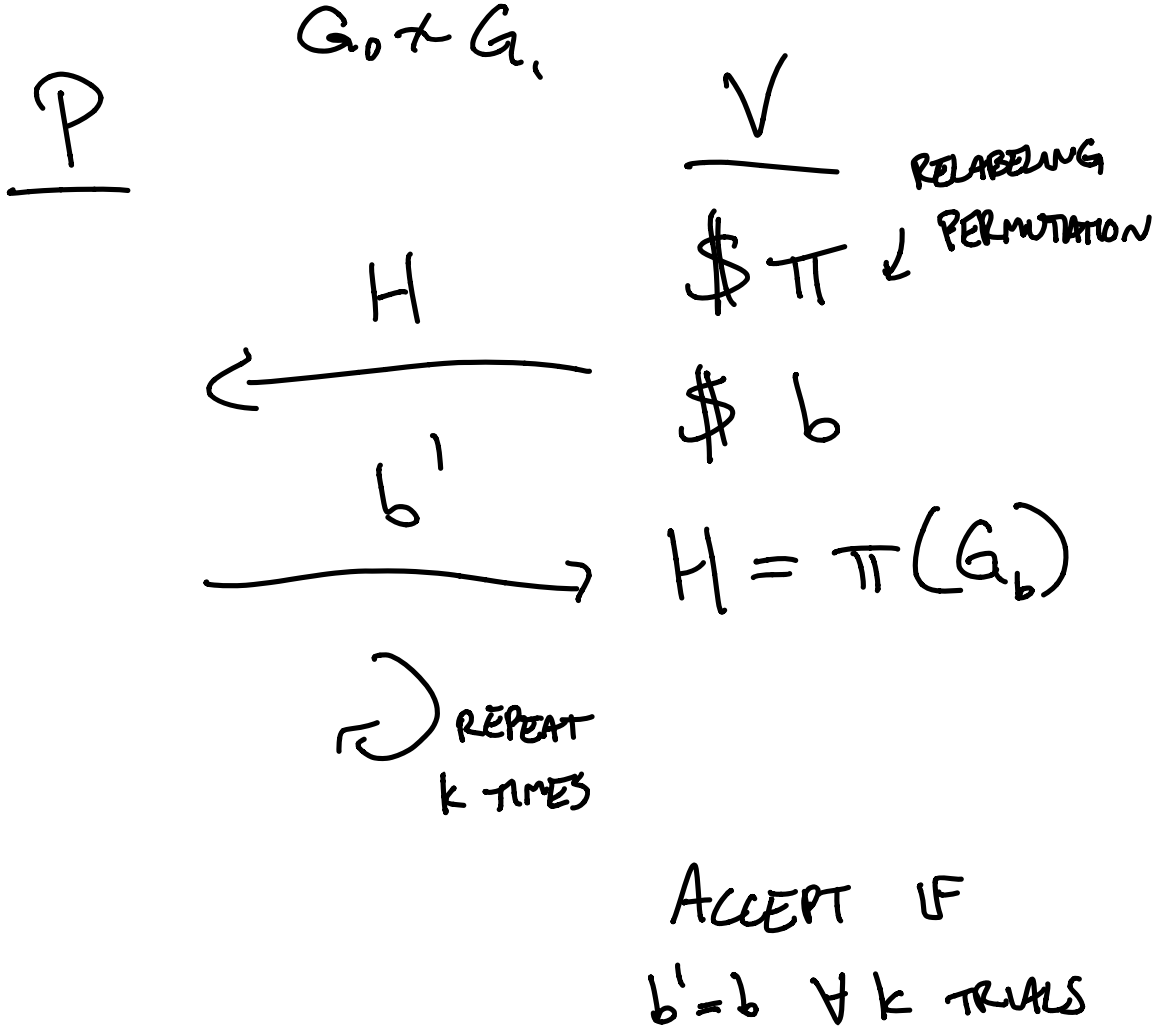


$G_0 \sim G_1$ IF WE CAN RELABEL NODES SUCH THAT EDGE STRUCTURE IS PRESERVED.

$G_0 \not\sim G_1$ IF NO SUCH RELABELING EXISTS. MUCH HARDER PROBLEM.



DONT KNOW HOW TO PROVE $G_0 \not\cong G_1$ CLASSICALLY, BUT WE CAN DO IT INTERACTIVELY!



ACCEPT IF $b' = b$ $\forall$ k TRIALS

COMPLETENESS: IF P KNOWS HOW TO DISTINGUISH G_0 FROM G_1, CAN TELL IF $H \sim G_0$ OR $H \sim G_1$ AND BE CORRECT EVERY TIME.

SOUNDNESS: IF $G_0 \sim G_1$, H HIDES b INFORMATION-THEORETICALLY.

$$Pr[b = b'] = \frac{1}{2} \quad \text{EACH TIME.}$$

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

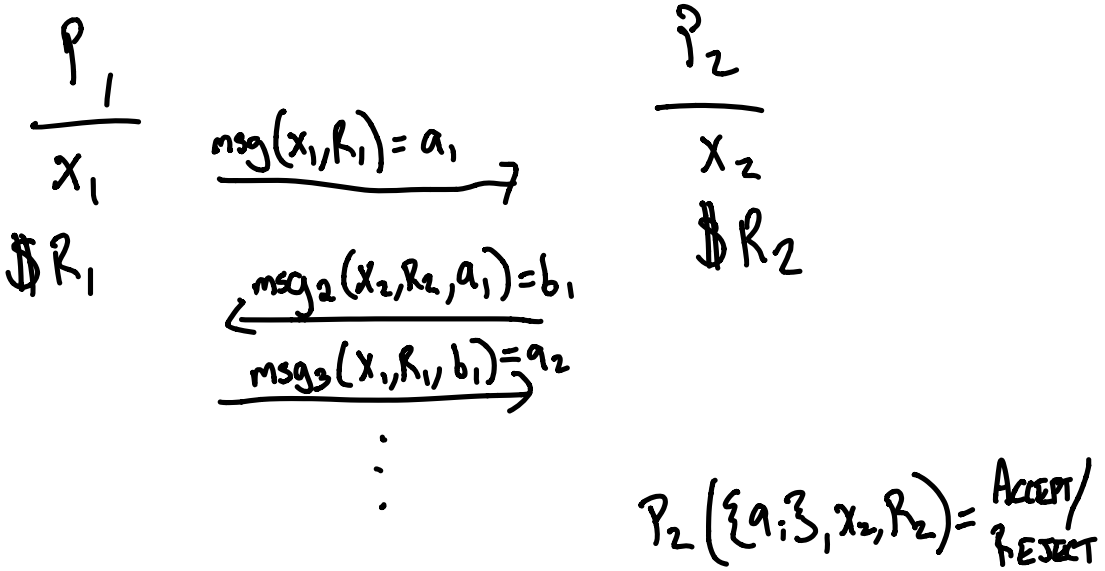
[SHAMIR] $\exists$ IP FOR ANY LANGUAGE $L \in$ PSPACE. BEYOND EVEN NP-COMPLETE PROBLEMS.

MIDTERM: MONDAY MAY 2nd

CLOSED NOTE, CLOSED BOOK

INTERACTIVE PROTOCOL REMINDER:

MESSAGES COMPUTED BY "NEXT MESSAGE" FUNCTIONS



IP = SET OF LANGUAGES L WITH (PERFECT) COMPLETENESS / (COMPUTATIONAL) SOUNDNESS

EXAMPLES: GRAPH ISOMORPHISM (GI)

GRAPH NON-ISOMORPHISM (GNI)

P, V BOTH KNOW COMMON INPUT $x = (G_0, G_1)$

P WANTS TO CONVINCE V THAT $x \in GI$ (OR $x \in GNI$)

PERFECT COMPLETENESS:

$$\forall\ x \in L \quad P_R\left[P \leftrightarrow V(x),\ V \text{ ACCEPTS}\right] = 1$$

COMPUTATIONAL COMPLETENESS:

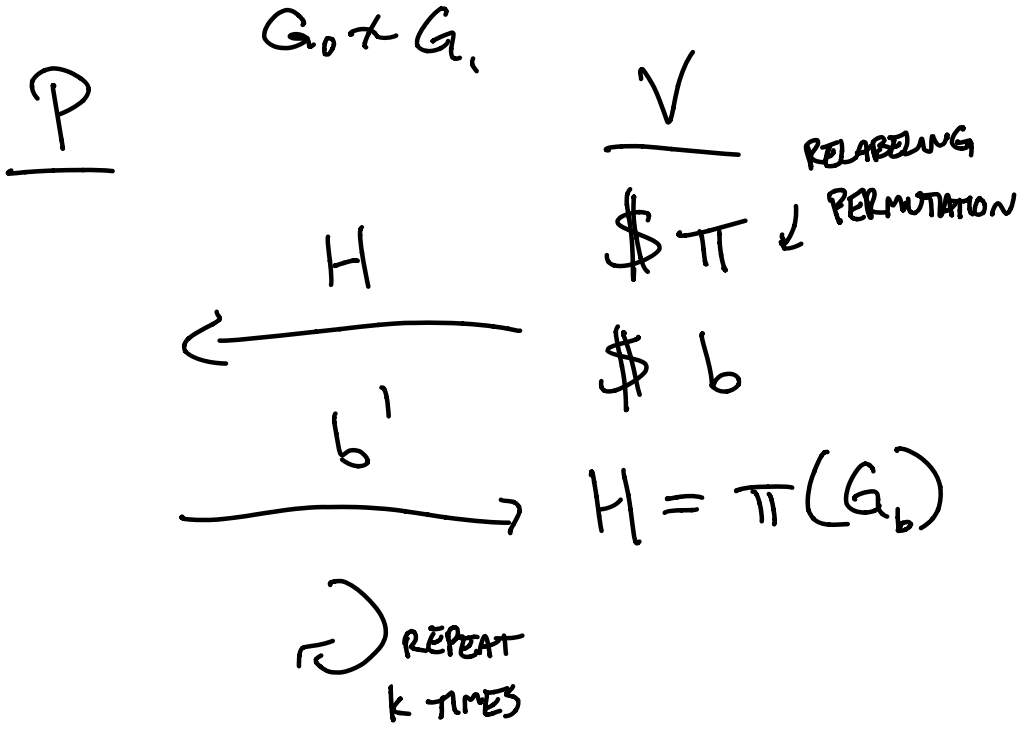
$$\forall\ x \in L \quad P_R\left[P \leftrightarrow V(x),\ V \text{ ACCEPTS}\right] > \frac{2}{3}$$

Computational Soundness:

$\forall x \notin L, \forall P^*$

$$\Pr[P^* \leftrightarrow V(x), V \text{ accepts}] < \frac{1}{3}$$

IP for GNI:



ACCEPT IF $b' = b$ $\forall$ k TRIALS

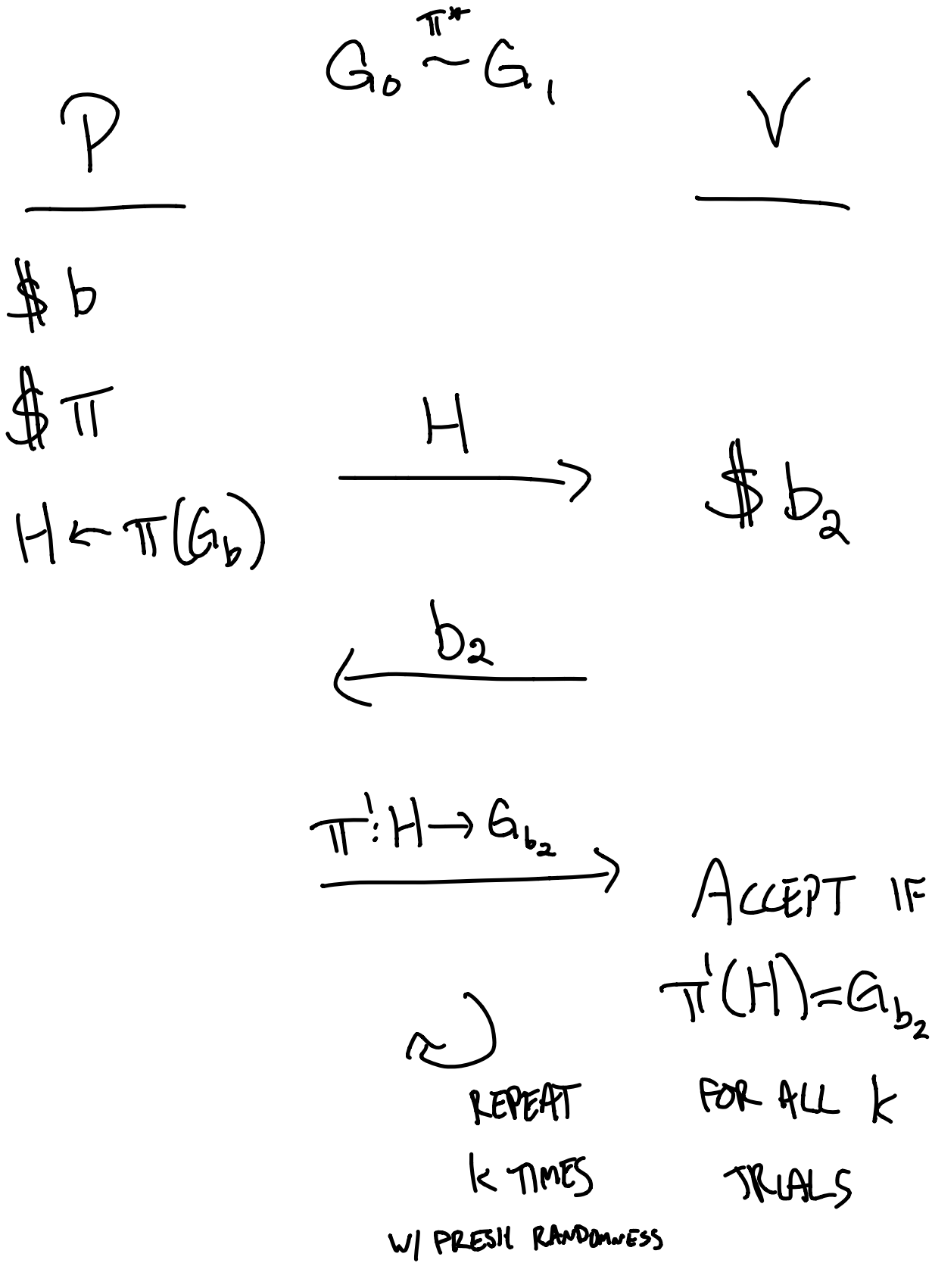
WHAT ABOUT PROVING $G_0 \sim G_1$?

CLASSICAL PROOF: $P \xrightarrow{\pi : G_0 \to G_1} V$

V VERIFIES THAT $\pi(G_0) = G_1$

BUT: THIS REVEALS THE INFORMATION $\pi : G_0 \to G_1$

WHAT IF P WANTS TO CONVINCE V WITHOUT REVEALING π?


$G_0 \overset{\pi^*}{\sim} G_1$
P
V
$b
$\pi
$H \leftarrow \pi(G_b)$
H
b_2
$\pi' : H \to G_{b_2}$
ACCEPT IF
$\pi'(H) = G_{b_2}$
REPEAT
k TIMES
W/ FRESH RANDOMNESS
FOR ALL k
TRIALS

COMPLETENESS: IF $G_0 \sim G_1$, THEN

(PERFECT) $H \sim G_0$ AND $H \sim G_1$,

SO P CAN CONSTRUCT

$\pi' : H \longrightarrow G_{b_2}$ EVEN IF $b \neq b_2$

VIA $\pi' = \pi(\pi^*(G_b))$

SOUNDNESS: IF $G_0 \not\sim G_1$, THEN

P CAN ONLY CONSTRUCT

π' IF $b = b_2$. THEN,

$P_R[V \text{ ACCEPTS}] = \frac{1}{2^k}$

INTUITIVELY, THIS HIDES PERMUTATION $\pi^*: G_0 \to G_1$. HOW DO WE FORMALIZE THIS NOTION?

INTUITION: IP IS ZERO-KNOWLEDGE

IF ALL MESSAGES FROM PROVER COULD HAVE BEEN SIMULATED BY VERIFIER WHO DOESN'T KNOW PRIVATE INFORMATION KNOWN BY P.

DEF IP FOR L IS ZERO-KNOWLEDGE

IF $\forall x \in L$, $\forall V^* \in PPT$, $\exists S_{V^*} \in PPT$

SUCH THAT

$$S_{V^*}(x) \cong [P \leftrightarrow V^*(x)]$$

WHY V^* INSTEAD OF V? BECAUSE

V MIGHT CHEAT AND DEVIATE FROM PROTOCOL

TO TRY TO LEARN SECRET INFO. WANT

TO DEFEND AGAINST THIS.

How to define S_V for GI?

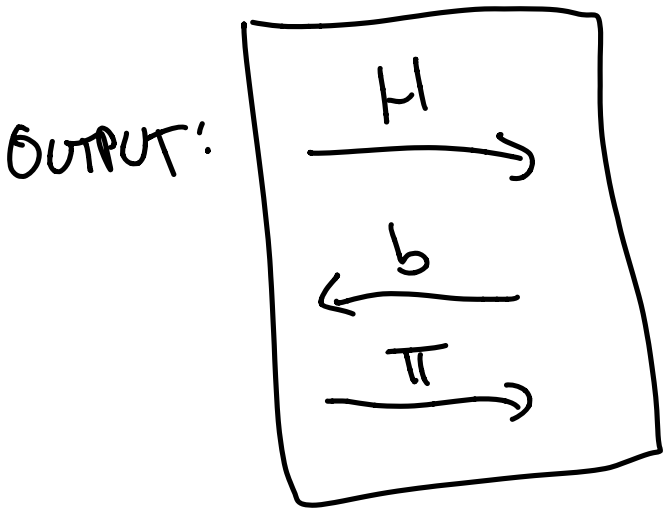
(Honest Verifier)

S_V

$\$ \; b$

$\$ \; \pi$

$H \leftarrow \pi(G_b)$



SAME DISTRIBUTION AS ORIGINAL PROTOCOL!

IN ORIGINAL PROTOCOL, P MUST PICK H BEFORE KNOWING b. BUT S_V CAN PICK H AFTER PICKING b, ALLOWING S_V TO ALWAYS ANSWER CORRECTLY.

WHAT IF V^* COMPUTES b FROM $h(H)$, USING COLLISION-RESISTANT HASH FUNCTION?

S_{V^*} CANNOT CHOOSE b FIRST ANYMORE!

BECAUSE WITH PROBABILITY $\frac{1}{2}$, $h(\pi(G_b)) \neq b$.

HOW DO WE BUILD S_{V^*} FOR ARBITRARY V^*?

IDEA: USE NEXT MESSAGE FUNCTION OF V^*

$$b_2 = MSG_{1,v^*}(R, H)$$

LET'S EXPERIMENT WITH THIS FUNCTION!

INTUITION: HOW TO MAKE A YOUTUBE VIDEO CLAIMING TO PREDICT A COIN FLIP?

JUST DO 100 TAKES AND ONLY KEEP THE TAKES WHERE I'M CORRECT!

S_{V^*}

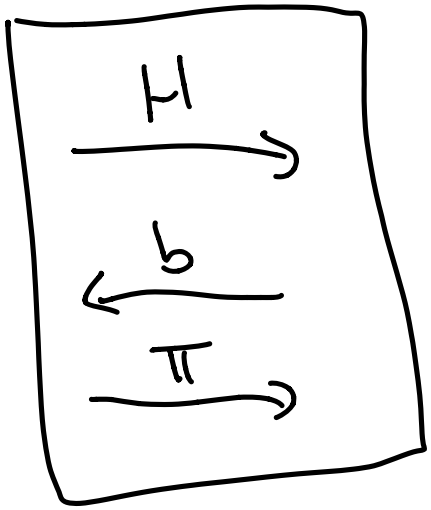
$\$ b$

$\$ \pi$

$H \leftarrow \pi(G, b)$

IF $b = MSG_{1,V^*}(R, H)$:

OUTPUT:



OTHERWISE: RESTART V^* AND TRY AGAIN W/ FRESH b, π

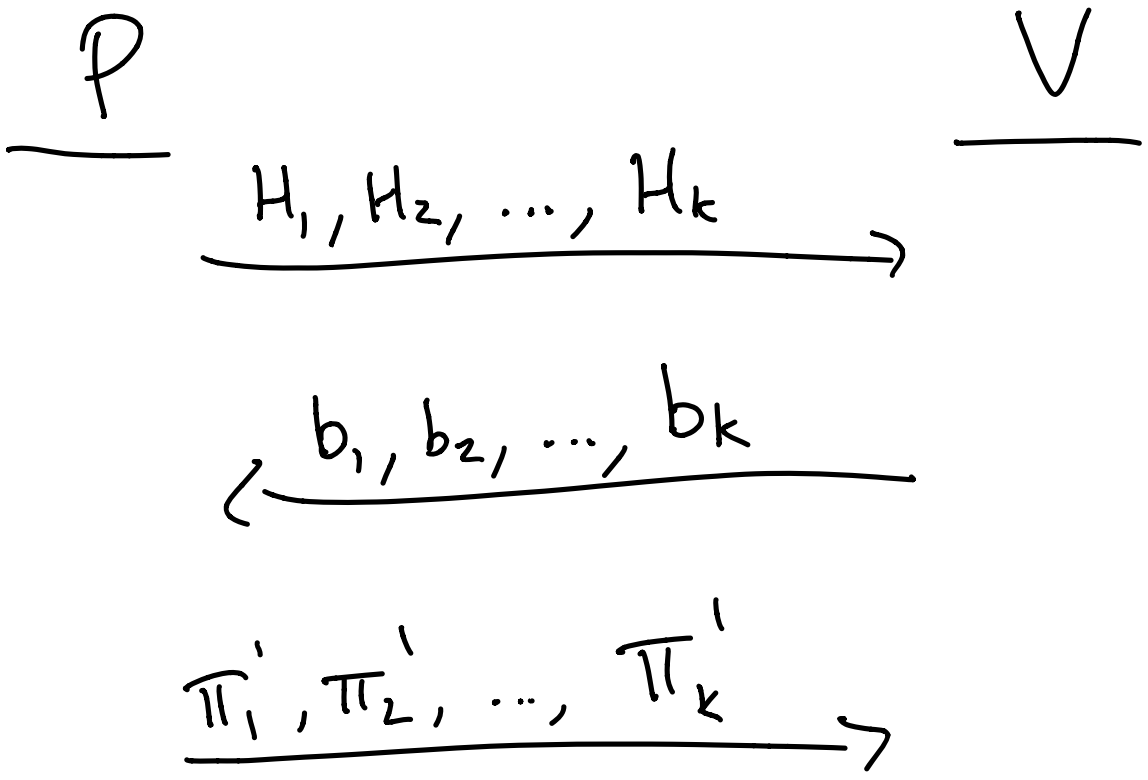
THIS WILL PRODUCE THE CORRECT TRANSCRIPT AFTER 2k TRIALS ON AVERAGE.

EFFICIENCY QUESTION:

PERFORMING k TRIALS SEQUENTIALLY INTRODUCES A LOT OF LATENCY.

E.g. 3ms PER ROUND OF COMMUNICATION.

CAN WE COLLAPSE TO JUST 3 ROUNDS?



SOUNDNESS $= 1 - \frac{1}{2^k}$ ✓

COMPLETENESS $= 1$ ✓

WHAT ABOUT ZERO-KNOWLEDGE?

FOR HONEST V, NO PROBLEM. CAN USE ORIGINAL STRATEGY WITHOUT RESETTING.

BUT IF V^* DOES $b_1, b_2, \ldots, b_k = h(H_1, \ldots, H_k)$

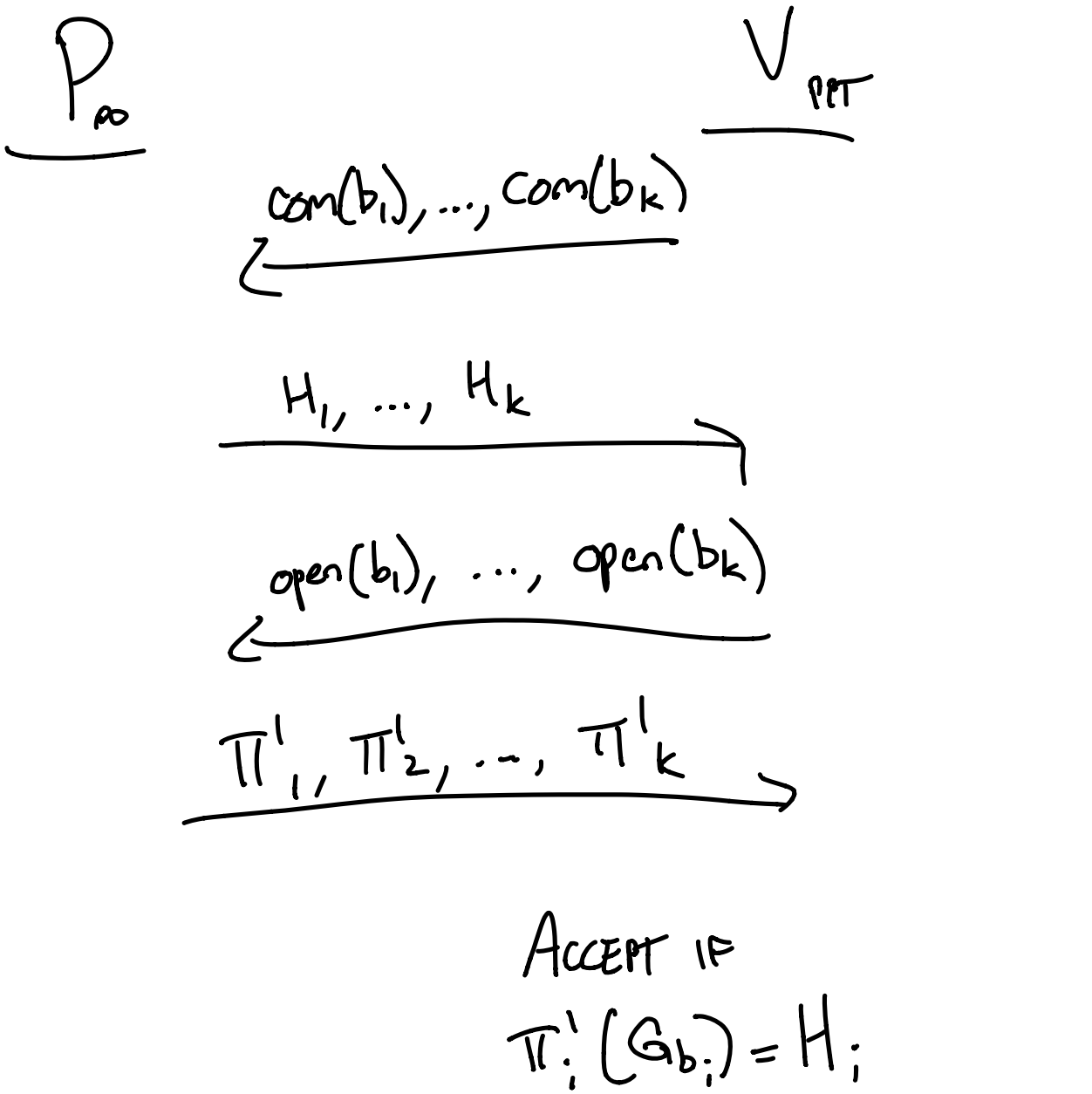
HAVE TO RESTART FROM SCRATCH

EVERY TIME OUR GUESS IS WRONG.

S_{V^*} WOULD NEED EXPONENTIALLY LONG

TO CONSTRUCT PROPER TRANSCRIPT.

5-ROUND ZKP FOR GI



ACCEPT IF

$\pi'_i(G_{b_i}) = H_i$

INTUITION: V^* CANNOT CHANGE MIND ABOUT b_i, SO CANNOT CHOOSE THEM BASED ON H

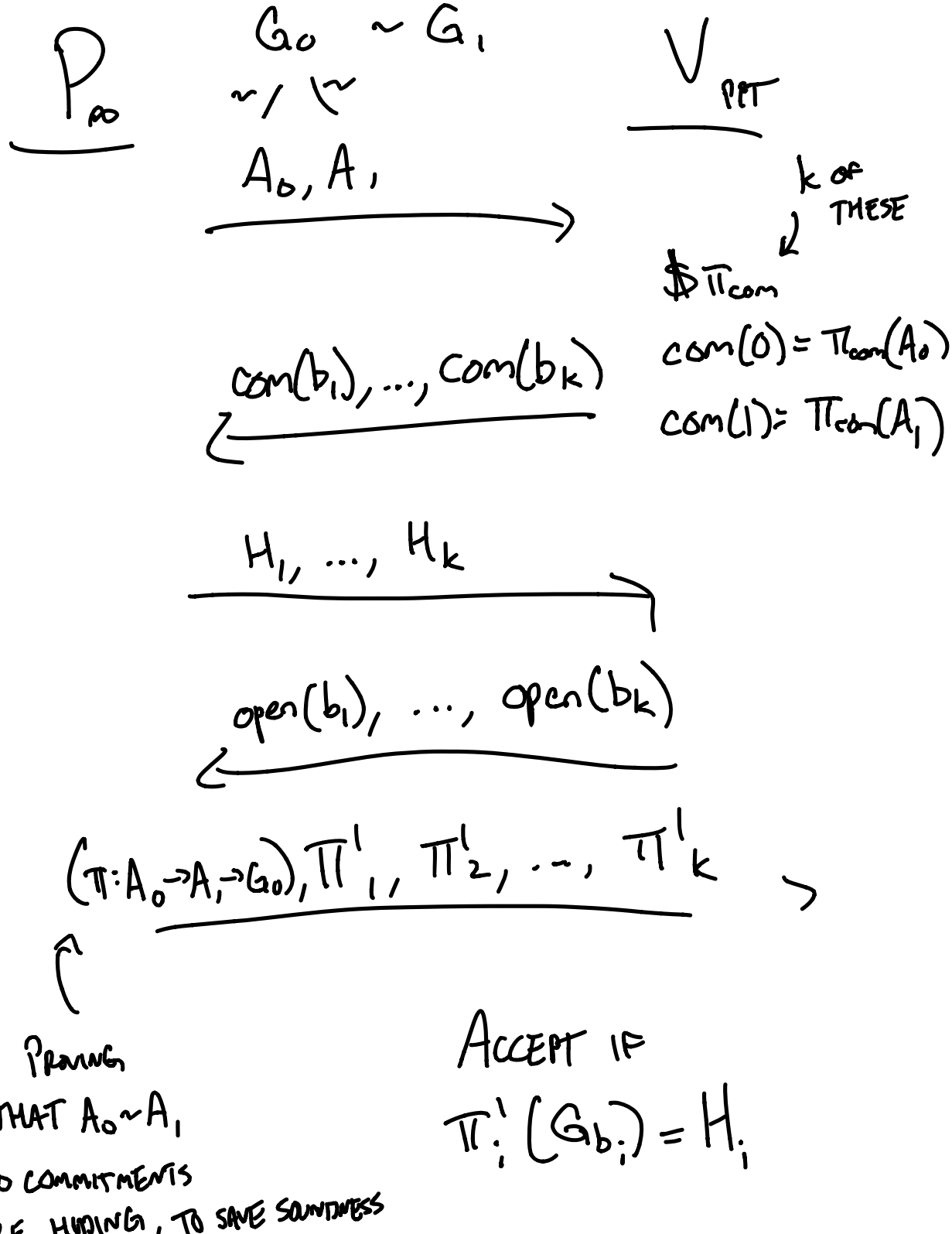
S_{V^*} RUNS FIRST 3 ROUNDS WITH V^*, LEARNS $b_1, \ldots, b_k$, RESTARTS V^*, AND CHOOSES $H_i = \pi_i(b_i)$, AND SENDS $H_1, \ldots, H_k$ AND THEN $\pi_1, \ldots, \pi_k$.

BUT HOW DO WE COMMIT A BIT TO AN INFINITELY POWERFUL PROVER?

IDEA: PROVER GIVES $A_0 \sim G_0$ AND $A_1 \sim G_0$. VERIFIER COMPUTES

$$com(0) = \Pi_{com}(A_0)$$
$$com(1) = \Pi_{com}(A_1)$$

FOR $\$$ Π_{com}


P_∞
$G_0 \sim G_1$
$\sim / \not\sim$
V_{PPT}
A_0, A_1
k OF THESE
$\$ \pi_{com}$
$com(0) = \pi_{com}(A_0)$
$com(1) = \pi_{com}(A_1)$
$com(b_1), \ldots, com(b_k)$
$H_1, \ldots, H_k$
$open(b_1), \ldots, open(b_k)$
$(\pi : A_0 \to A_1 \to G_0), \pi'_1, \pi'_2, \ldots, \pi'_k$
PROVING THAT $A_0 \sim A_1$ SO COMMITMENTS ARE HIDING, TO SAVE SOUNDNESS
ACCEPT IF $\pi'_i(G_{b_i}) = H_i$

IF V^* FINDS $\pi : A_0 \to A_1$,

V^* CAN CHANGE MIND ON COMMITMENTS

BUT IF $G_0 \sim G_1$, THEN

SUCH A V^* CAN FIND AN ISOMORPHISM

BETWEEN $G_0 \sim G_1$ IF A_1 COMES

FROM G_1 INSTEAD OF G_0.

SO S_{V^*} CAN RUN FIRST 4

ROUNDS BUT WITH $A_0 \sim G_0$ + $A_1 \sim G_1$,

EXTRACT PERMUTATION FROM $G_0 \sim G_1$,

RESET, AND COMPLETE PROTOCOL HONESTLY KNOWING THE ISOMORPHISM.

THUS: EITHER V^* CANNOT CHANGE COMMITMENTS, IN WHICH CASE WE RUN FIRST 4 ROUNDS TO EXTRACT b_i & CONSTRUCT SPECIAL H_i WHICH WE CAN PROVIDE $\Pi_i'(G_{b_i} \to H_i)$

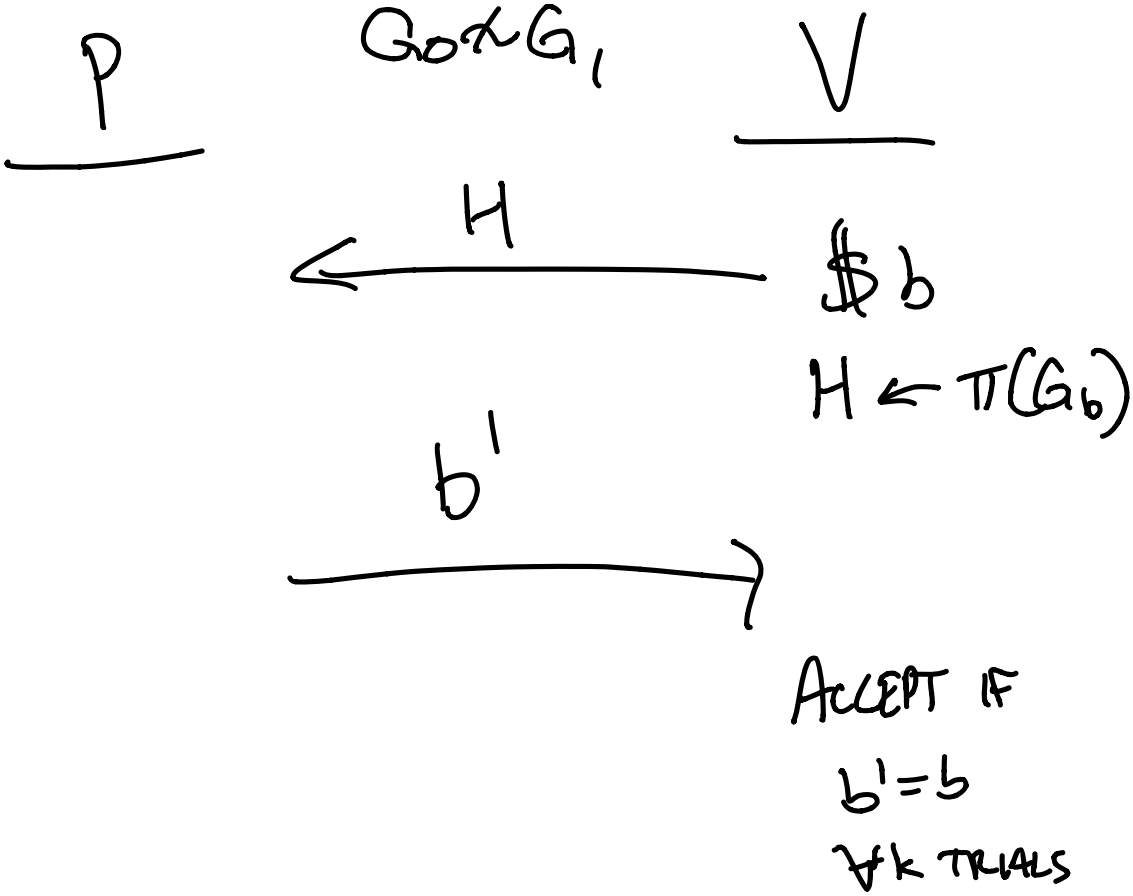
OR

V^* CHANGES COMMITMENTS & PROVIDES $\Pi^*: G_0 \to G_1$, S_{V^*} EXTRACTS & PLAYS HONESTLY.

Now, back to GNI.

How can we construct ZKP?

Is this ZK?

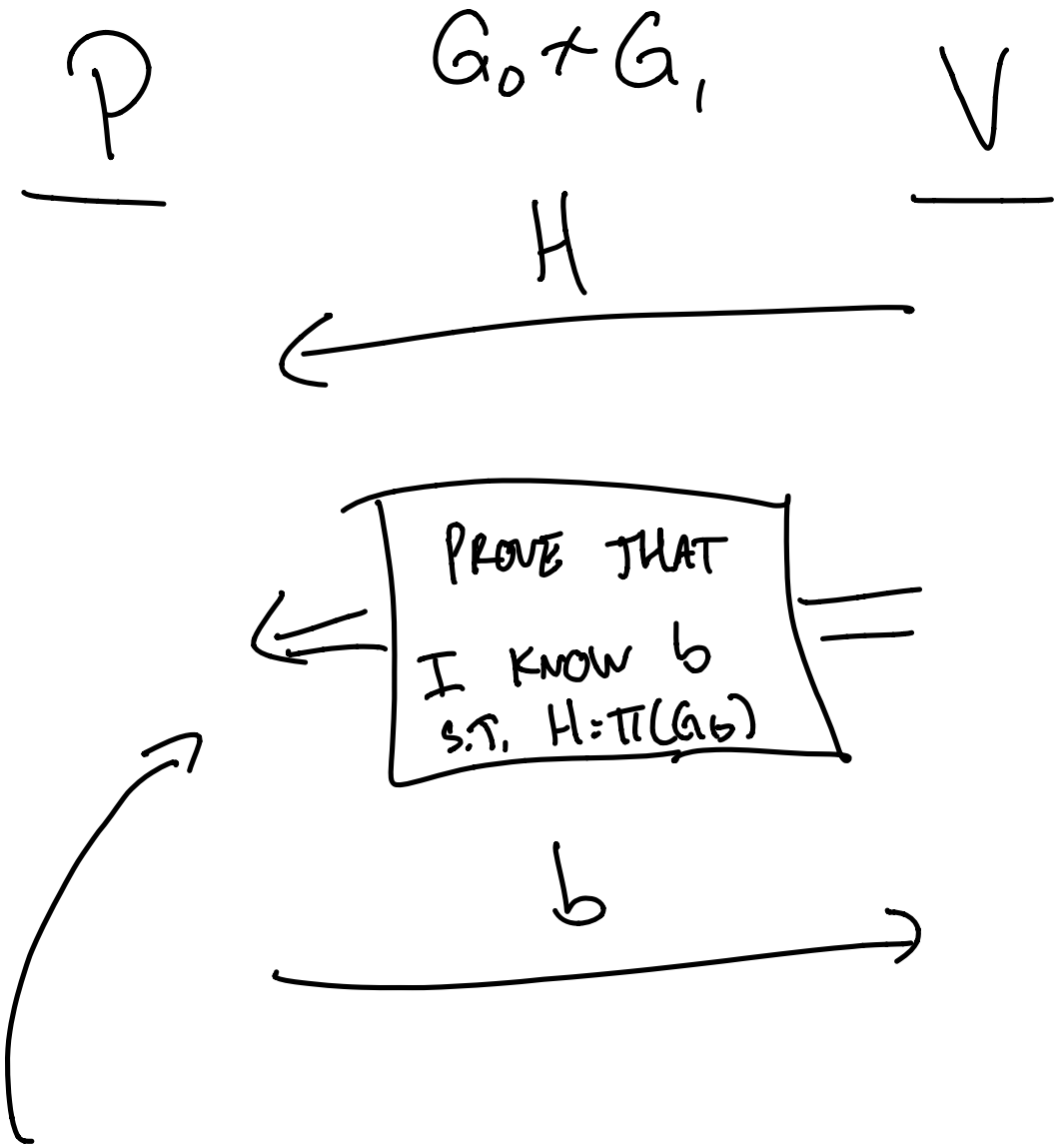


PROBLEM: WHAT IF V FINDS H SOMEWHERE?

DOESN'T COMPUTE $H \sim \pi(G_b)$.

THEN V LEARNS WHETHER $H \sim G_0$ OR $H \sim G_1$. NOT ZK FOR V^*.

MUST HAVE V PROVE THAT V ALREADY KNOWS THE ANSWER b!

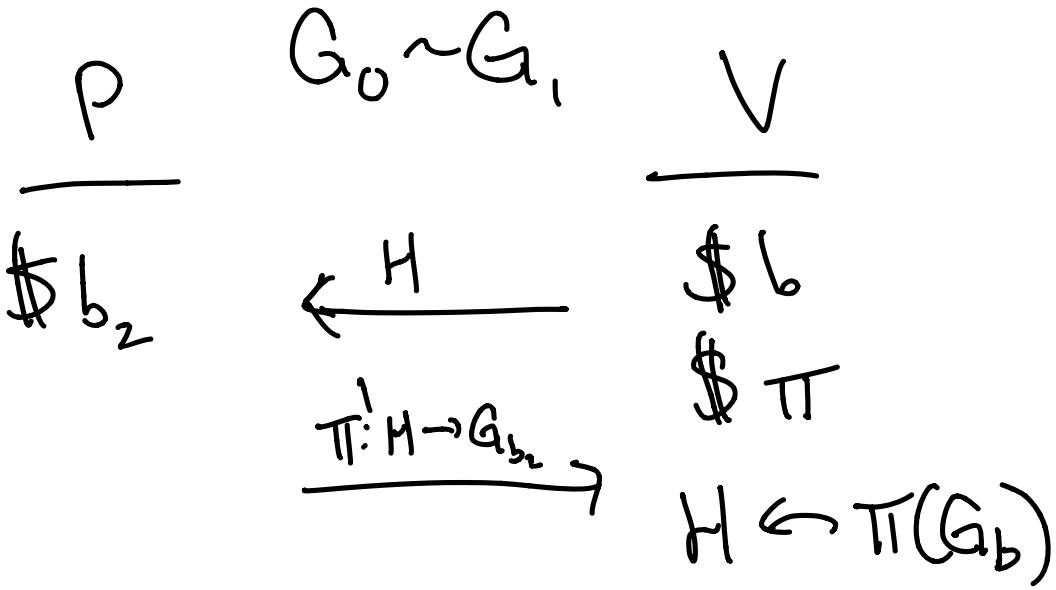


CALLED PROOF OF KNOWLEDGE.

WILL COVER THIS NEXT TIME.

THERE'S A PROBLEM WITH OUR ZK DEFINITION...

EXAMPLE:



REPEAT k TIMES, ACCEPT IF $b \neq b_2$ FOR SOME TRIAL

CLEARLY NOT ZK:

IF $b \neq b_2$,

$$\pi'(\pi(G_b)) = G_{b_2},$$

SO $\pi' \circ \pi$ IS $\pi^* : G_0 \to G_1$!

BUT: V CAN SIMULATE THIS TRANSCRIPT!

THE PROBLEM IS SIMULATOR NEEDS TO ALSO SIMULATE RANDOMNESS OF V.

IF WE INCLUDE V's RANDOMNESS,

S_V CANNOT PROPERLY SIMULATE,

BECAUSE π REQUIRES FINDING

$\pi^* : G_0 \to G$, WHICH IS ASSUMED

TO BE HARD.