PROBABILISTIC PROOF SYSTEMS

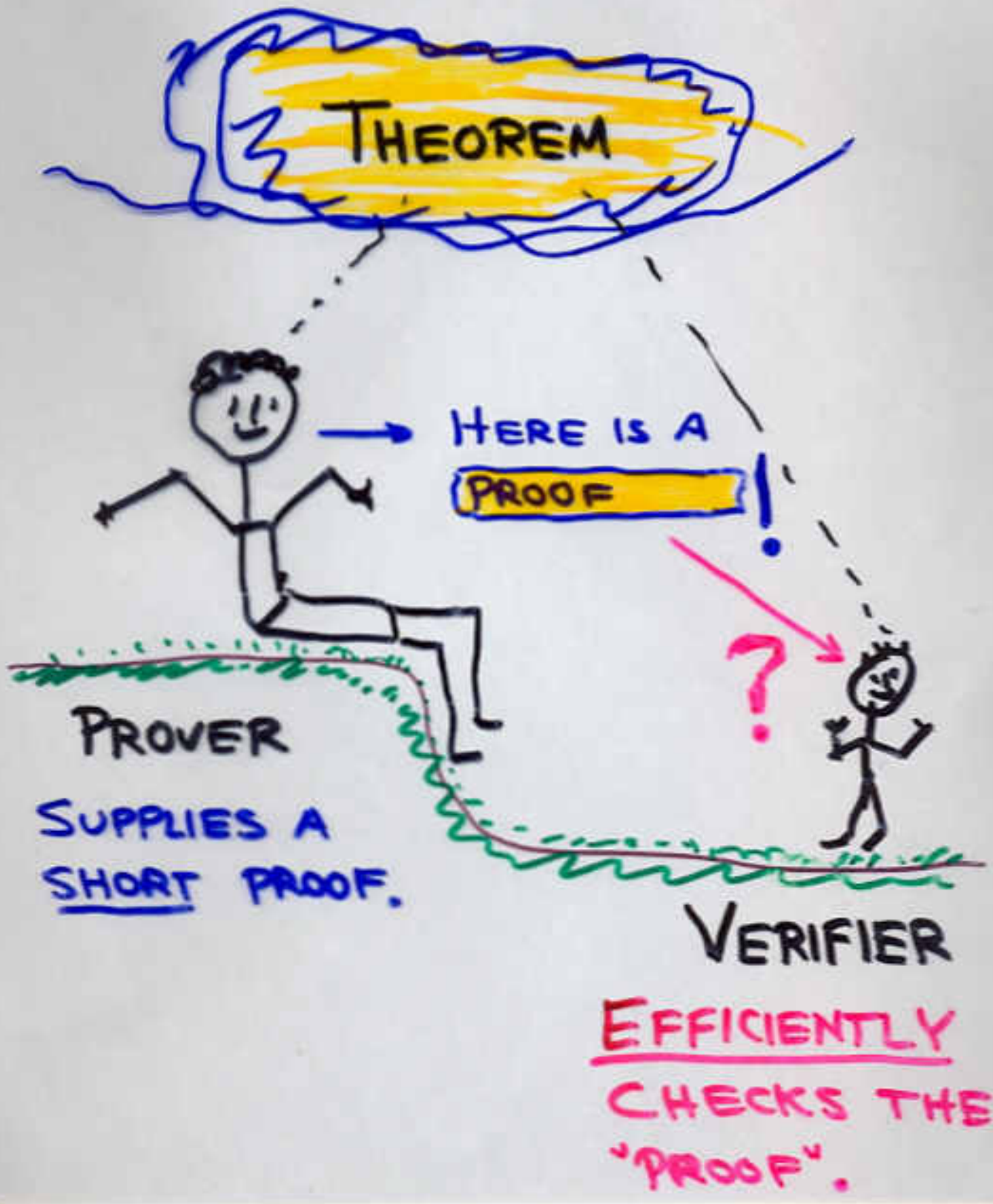
(AN EXPOSITION)

by

ODED GOLDREICH
WEIZMANN INSTITUTE
ISRAEL

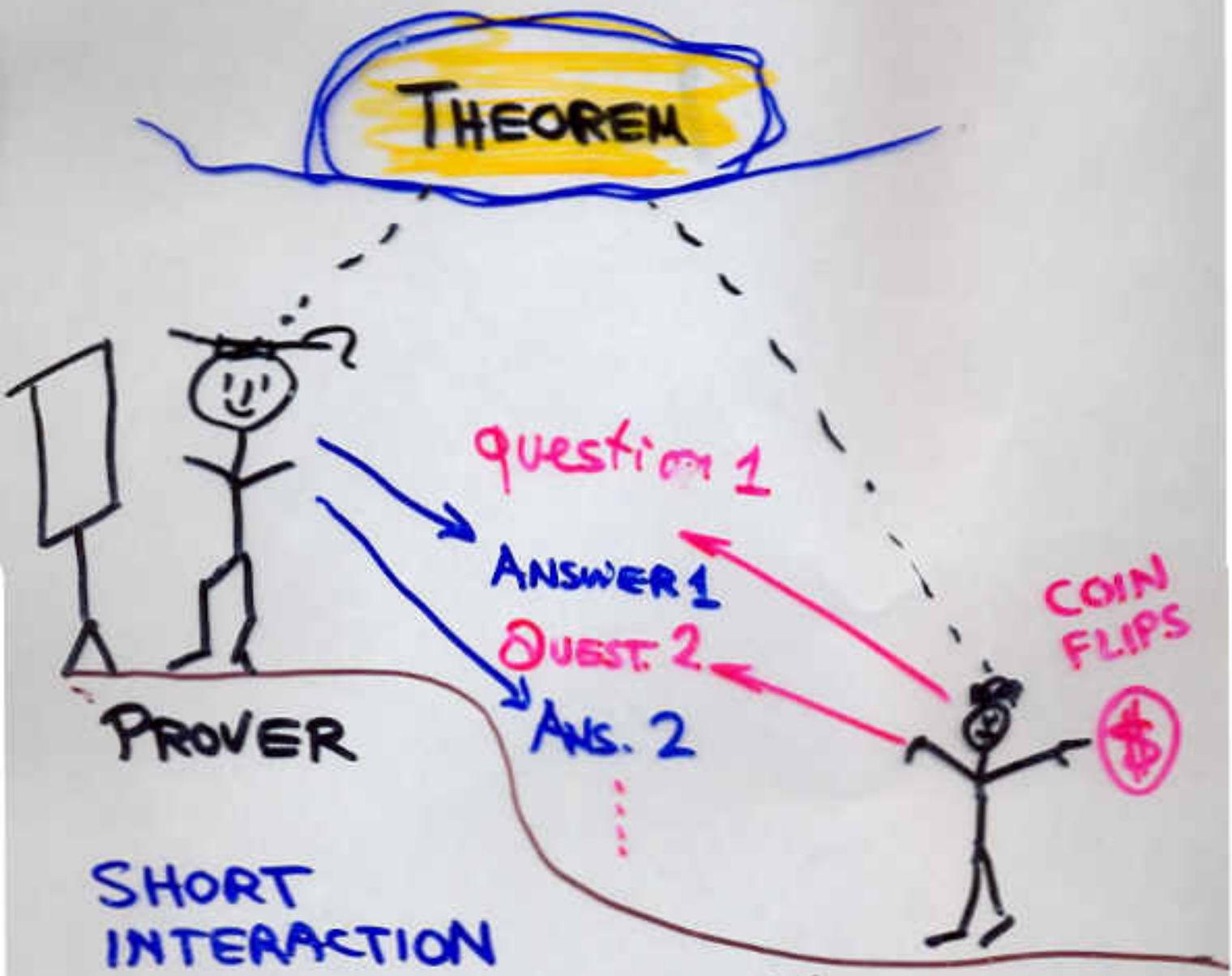
What is a proof?

- TRADITIONAL APPROACH:



↑ completeness & soundness

INTERACTIVE PROOFS [GMR]



- EFFICIENT GENERATION OF QUESTIONS.
- EFFICIENT CHECKING.

completeness & soundness

IP – Completeness & Soundness

Completeness

≙ the prover can convince the verifier to accept any valid claim, with probability 1.

Soundness

≙ there is no way to fool the verifier to accept an invalid claim, with probability OVER 1/2.*

*) Can be reduced by repetitions.

(Prob. over verifier's coin tosses.)

RED

GREEN

EXAMPLE: (GRAPH) NON-ISOMORPHISM

SET OF OBJECTS W/ RELATION

PROVER **VERIFIER**

TO WHICH IS R ISOMORPHIC?

RANDOMLY PERMUTE

$\alpha \in \{1,2\}$

CHECKS: IS α = CHOSEN?

- REPEAT TO INCREASE "STATISTICAL EVIDENCE"

ALSO: SVM for full (IP)

THE POWER OF INTERACTIVE PROOFS

IT IS EASY TO PROVE
THAT SOMETHING EXISTS.

⟶ JUST SHOW IT !

HOW CAN YOU PROVE THAT
SOMETHING DOES NOT EXIST ?

ANS: USE an interactive proof!

RANDOMNESS is essential

"IP w.o RAND" → NP


ZK

+ motivate ZK in full

HOW MUCH KNOWLEDGE IS REVEALED VIA A PROOF?

EXAMPLE:

PROVER — VERIFIER

SENDS → ISOMORPHISM →

CHECKS.

- CAN WE CONVINCE THE VERIFIER WITHOUT YIELDING AN ISOMORPHISM?

- MINIMIZE THE KNOWLEDGE GAINED BY THE VERIFIER IS THE ESSENCE OF CRYPTOGRAPHIC PROTOCOLS.

ZERO-KNOWLEDGE [GMR]

WHATEVER

A (not necessarily honest) VERIFIER

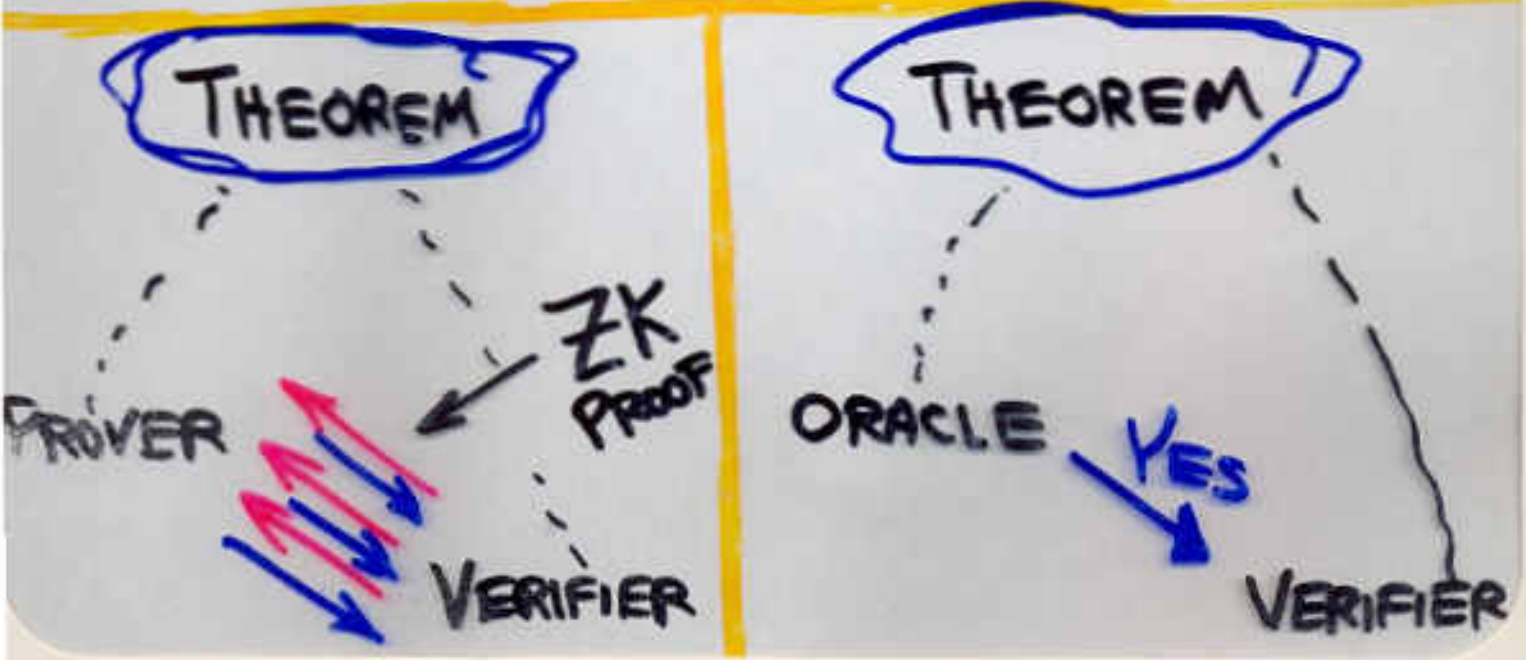
CAN EFFICIENTLY COMPUTE

AFTER INTERACTING WITH THE PROVER

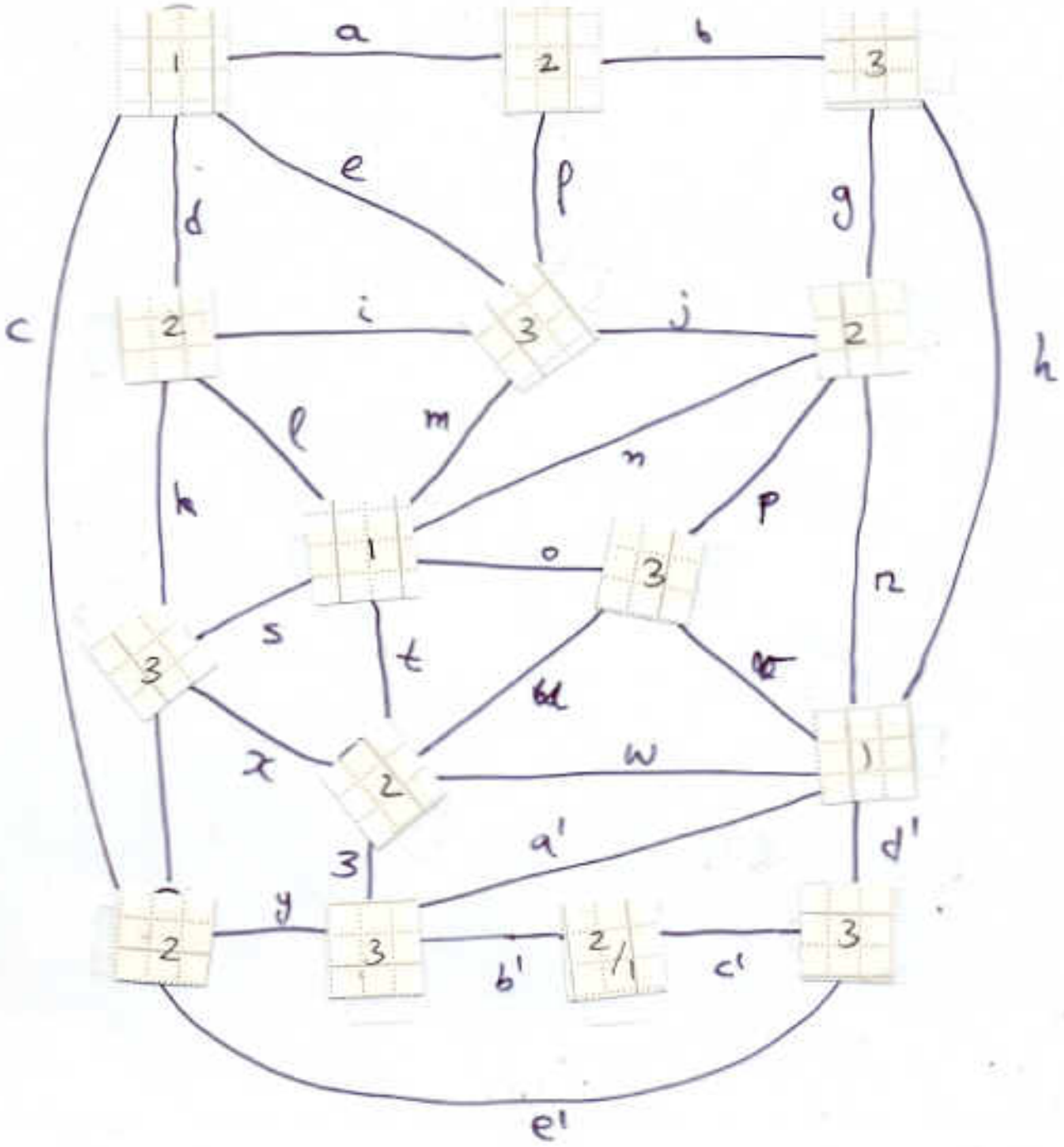
HE (i.e. the verifier) CAN ALSO

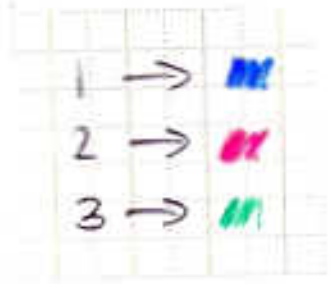
EFFICIENTLY COMPUTE BY HIMSELF

(assuming that the theorem is valid).



COVER




1 →
2 →
3 →

Quasi ZK (in full)

THE POWER OF ZERO-KNOWLEDGE

IT IS EASY TO PROVE THAT SOMETHING EXISTS:

— Just show it!

HOW DO YOU PROVE THAT SOMETHING EXISTS WITHOUT SHOWING IT?

(& SHOWING NOTHING WHICH THE VERIFIER COULD NOT GENERATE BY ITSELF!)

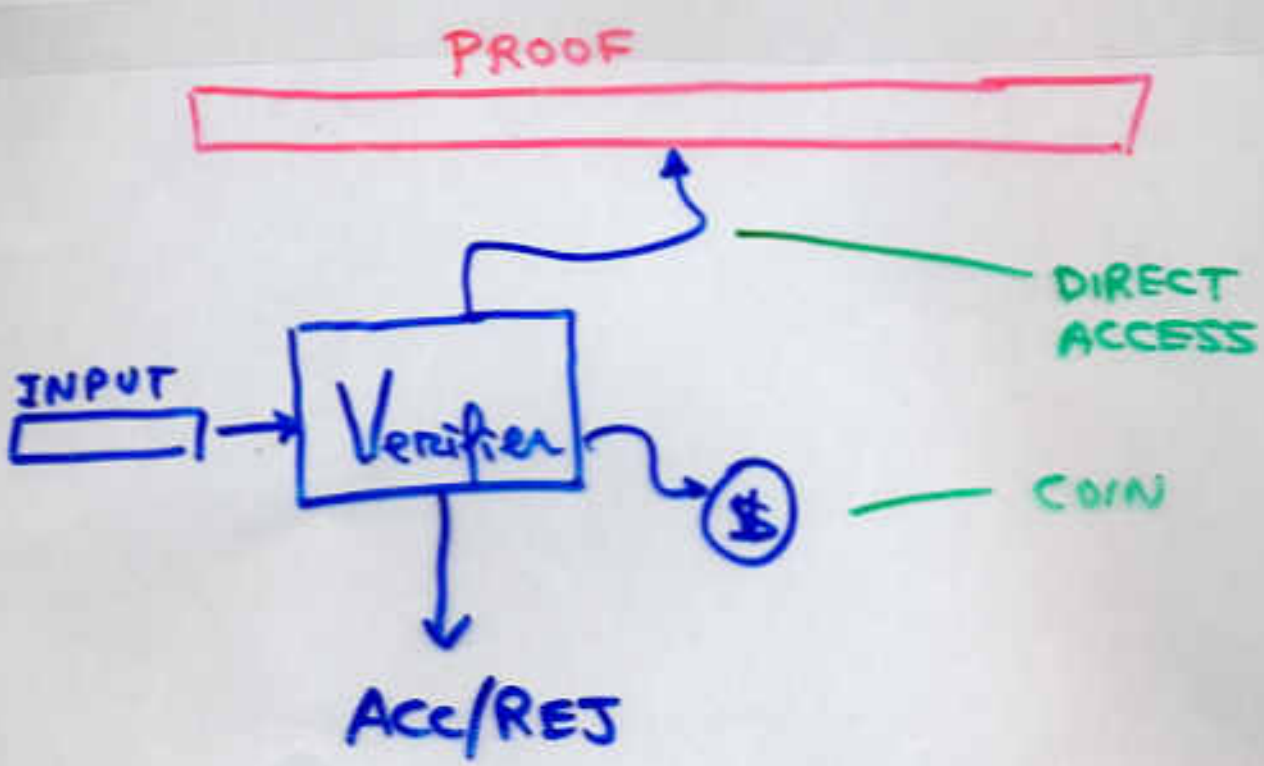
— use Zero-Knowledge proofs!

AGAIN RANDOMNESS IS essential

"ZK W.O. RAND" ⇝ BPP


P
C
P

PROBABILISTICALLY CHECKABLE PROOFS (PCP)



(SYSTEM FOR $S \subseteq \text{Prob}^*$)

COMPLETENESS

$$x \in S \rightarrow \exists \pi \quad \text{Prob}[V^{\pi}(x)=1] = 1$$

SOUNDNESS

$$x \notin S \rightarrow \forall \pi \quad \text{Prob}[V^{\pi}(x)=1] \leq 1/2$$

IMPORTANT: #QUERIES, PROOF LENGTH, ~~#COIN TOSSES~~

LENGTH

PCP (cont.)

$PCP[r(\cdot), q(\cdot)]$ ← class having PCP systems of such RND & Q. complex

- $r(\cdot)$ → **RANDOM.** Complexity
- $q(\cdot)$ → **QUERY** Complexity

THM: $NP = PCP[\log, O(1)]$, with $O(1) = 3$

CONNECT. to APPROX.

V (a verifier of such PCP)

YIELDS NATURAL OPT. PROBLEMS

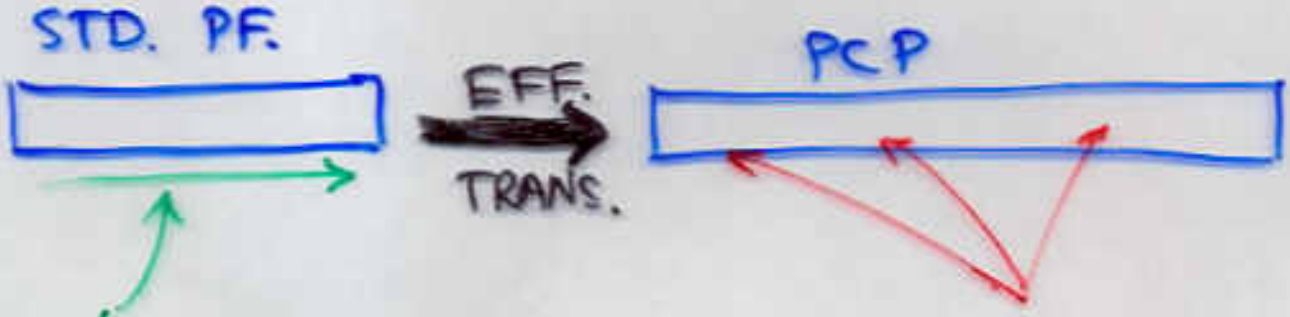
$$\nu(x) \triangleq \max_{\pi} \{ Prob[V^{\pi}(x) = 1] \}$$

$x \in S \Rightarrow \nu(x) = 1$

$x \notin S \Rightarrow \nu(x) \leq 1/2$

PCP (cont.)

We can EFFICIENTLY TRANSFORM STANDARD PROOFS TO PROB. CHECK. ONES!



must read all of it to get convinced

CAN BE VERIFIED PROBABILISTICALLY (W. ERR. PROB. $\approx 1/2$) BY MAKING 3 QUERIES!

CAN REDUCE THE ERR. PROB. to 2^{-k} BY MAKING $\approx k$ QUERIES (RATHER THAN $\approx 3k$)

PCP length = poly(std. PF length)

sum-up PCP (full).

THE POWER OF PCP

IT IS EASY TO VERIFY A PROOF
BY EXAMINING ALL OF IT.

BUT CAN YOU VERIFY A PROOF
BY LOOKING AT A TINY PORTION OF IT?
(SAY AT 10 BITS?)

Yes! PROBABILISTICALLY