$\mathcal{ZKP}$ $\mathfrak{ZKP}$

$\mathcal{ZKP}$

What is it

Kurt Pan

05/21/23

What is a *Proof/Argument*

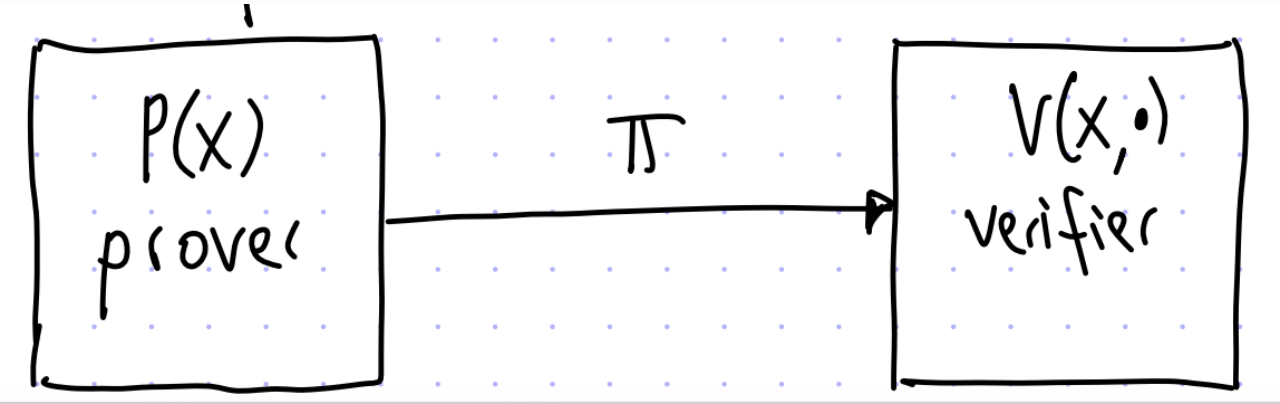
> A proof is whatever convinces me.

- *Statement* is `True`
- *Computation* is `Correct`

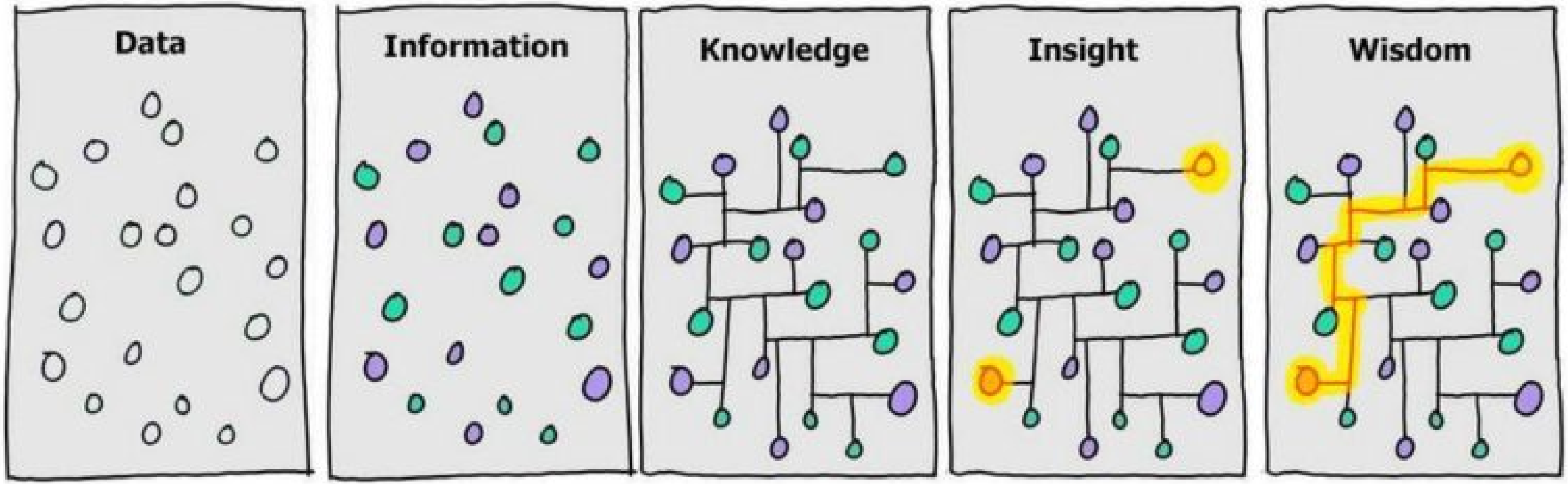
Proof System

- specified by a PPT verification algorithm $\mathcal{V}$
- 真的假不了 （**Completeness**）
- 假的真不了 （**Soundness**）

Mathematical Proofs = $\mathcal{NP}$



What is *Knowledge*


Data
Information
Knowledge
Insight
Wisdom

- **Data** is represented by a series of random dots that could mean something – or nothing.
- **Information**, which is where meaning or relationship is applied to the raw material. For the elimination of uncertainty.
- **Knowledge** is gained when we are *able* to memorise the information. As we gain knowledge we begin to make sense of things and draw connections between different pieces of information. However, it's at the 'Insight' level where data becomes seriously useful.
- **Wisdom** – the ability to use insight to facilitate informed decision making.
- 从「大数据」到「人工智慧」必然要经过「零知识」时代

R.I.P 陈皓！

> 有一个观点，数据是没有用的，只有把数据关联起来才有意义。**数据关联了以后，才叫信息**，我们不是做数据，我们是做信息。**信息里面找到因果关系，我们才能有知识**，比如说因为这个所以那个，这叫知识；有了知识以后，才能导出公式，我们才能通过公式去完成一些事情。所有做科学实验都是走这条路的，不断地做实验、拿数据，在数据里面把它标注好，关联起来，然后找信息，从信息里面找因果关系，从因果关系里看看能不能推出一些公式。大概就是这么一个逻辑。

Knowledge is Power

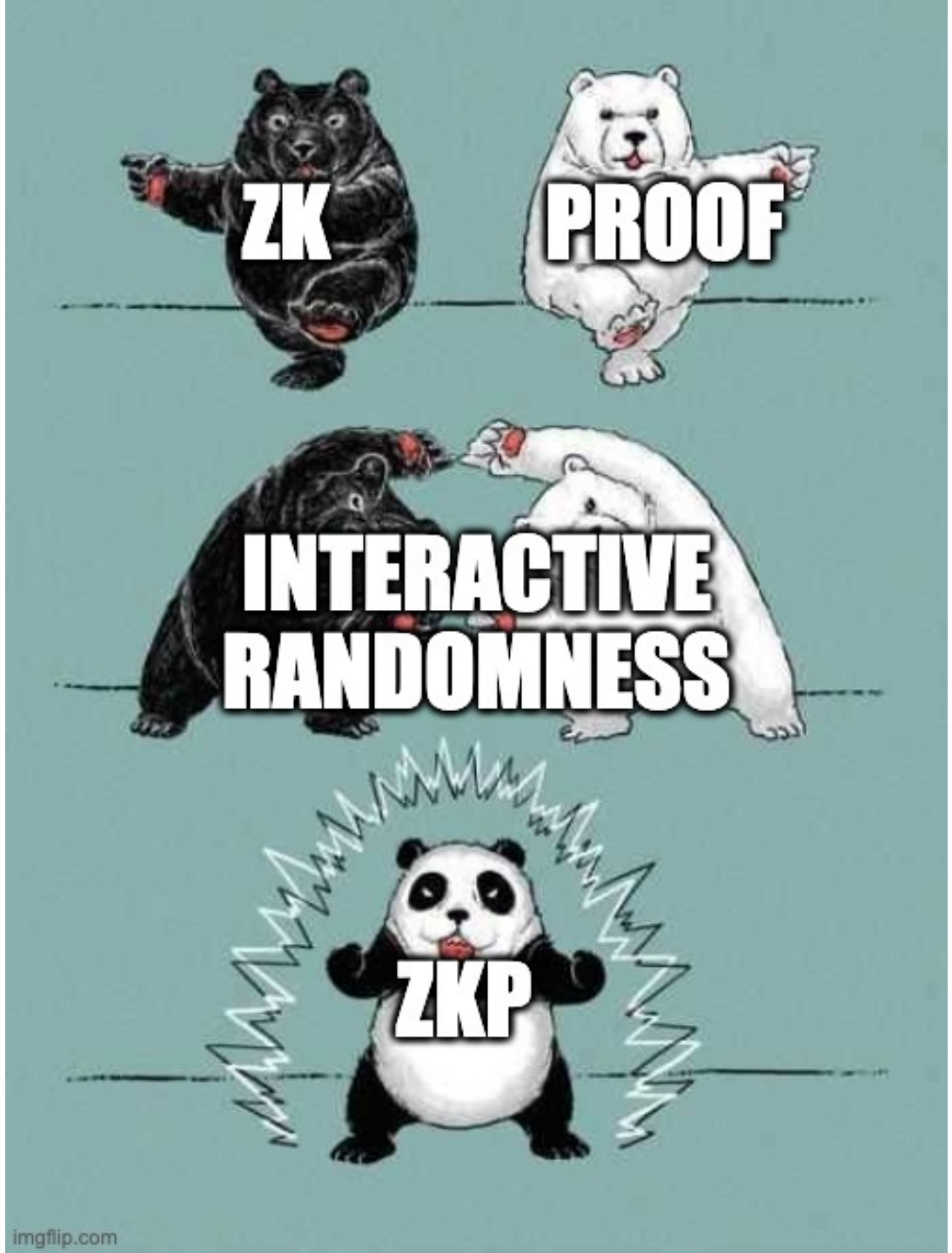
- 语言$\mathcal{L}$/关系$\mathcal{R}$

  $x \in \mathcal{L}$

$$C(\mathrm{x}, w) = 1$$

witness w

What is *Zere-Knowledge Proof*?


ZK
PROOF
INTERACTIVE
RANDOMNESS
ZKP
imgflip.com

一个不增加任何计算能力（知识）
但却可以使我想信的东西（证明）

A proof that reveals no more *information* (or knowledge)
than the validity of the statement it supports.

“听君一席话，
如听一席话。”

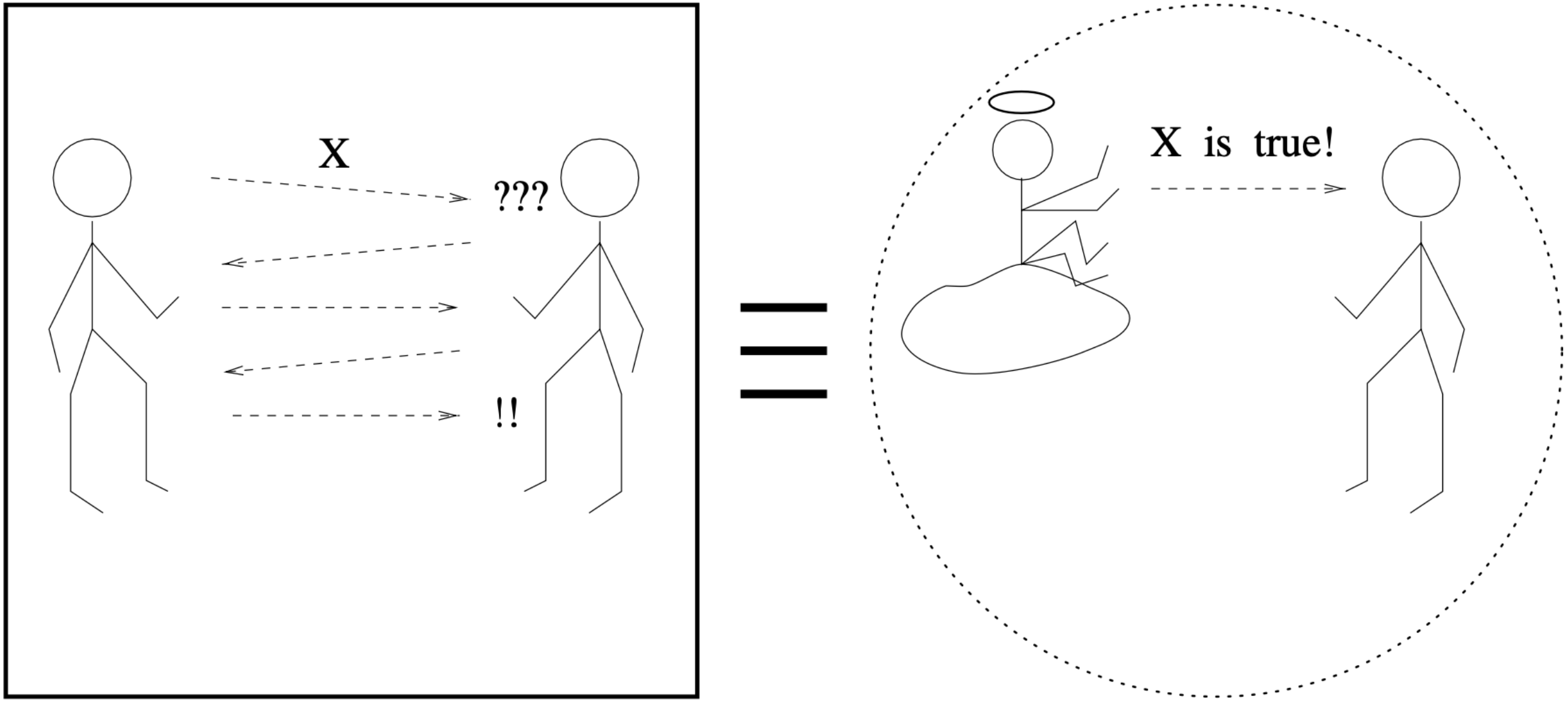


Figure 4.1: Zero-knowledge proofs: an illustration.

Simulator

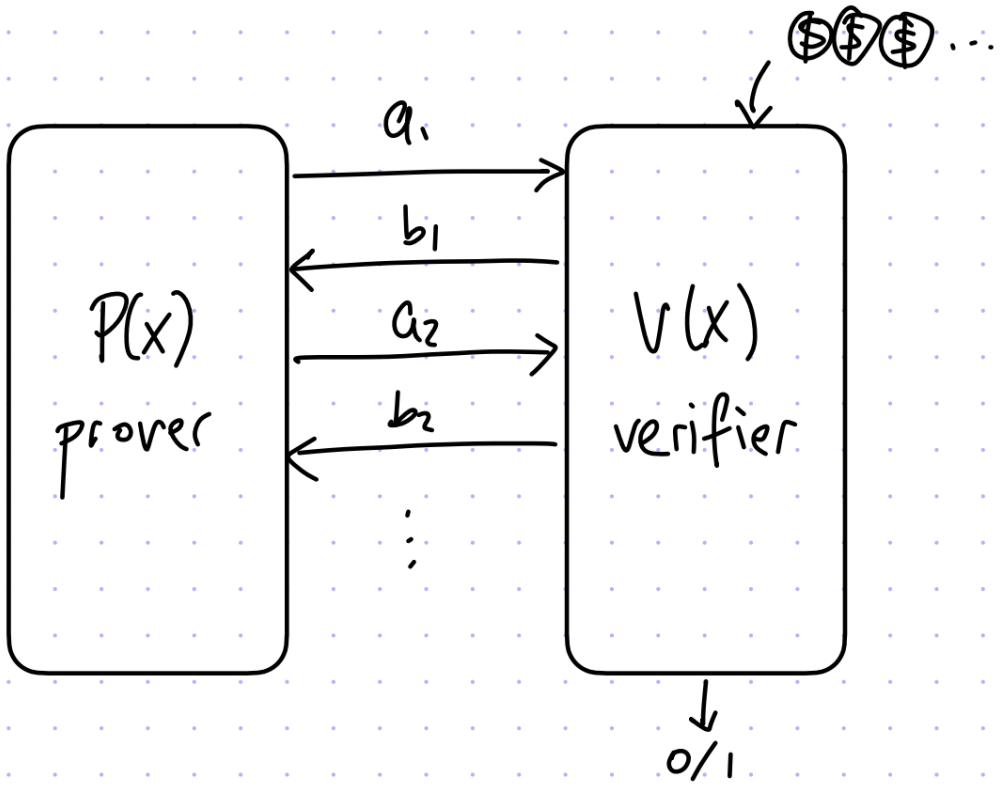
- $\langle P, V^* \rangle (x)$ (i.e., the output of the interactive machine V^* after interacting with the interactive machine P on common input x)
- $S^*(x)$ (i.e., the output of machine S^* on input x)

“潘老师认识到零知识证明和计算复杂性理论在密码学中的重要性并且知道我们在这方面可能会遇到问题。零知识证明可用来构造安全的密码认证协议，计算复杂性理论可用来评估密码难题的破解难度。那时候**复旦大学的朱洪老师是零知识证明的专家，潘老师便把他请来给我们作报告。**”

--王小云

What are *IP/MIP/PCP/IOP*

Interactive Proofs



randomness \ interaction	Y	N
Y	IP	MA
N	NP	NP

believed to equal NP (it does if strong PRGs exist)

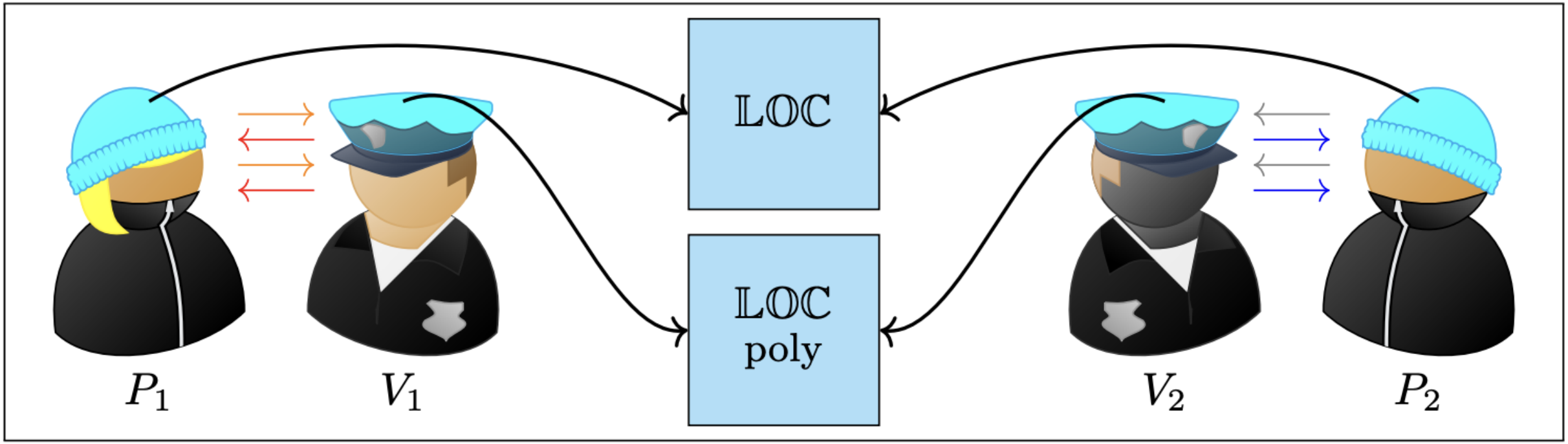
(unbounded) honest prover, (efficient) honest verifier

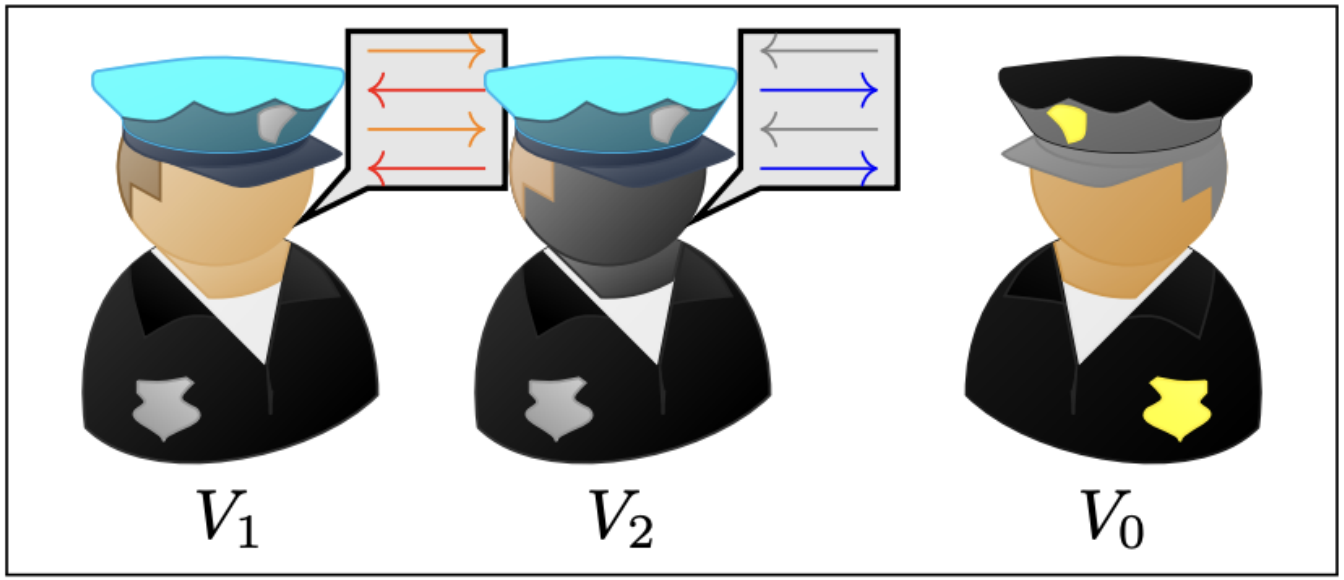
An interactive proof for L is a pair (P, V) s.t.

(1) completeness: $\forall x \in L \quad \Pr_r\left[\langle P(x), V(x;r)\rangle = 1\right] = 1$

(2) soundness: $\forall x \notin L \; \forall \tilde{P} \quad \Pr_r\left[\langle \tilde{P}, V(x;r)\rangle = 1\right] \leq 1/2$

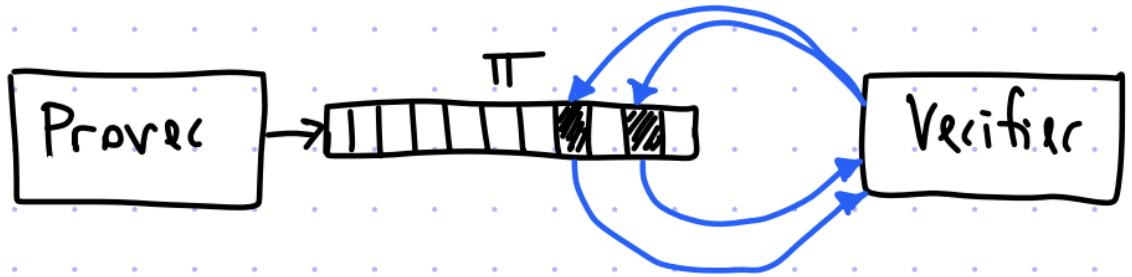
any noticeable gap suffices for definition


LOC
LOC
poly
P_1
V_1
V_2
P_2


V_1
V_2
V_0

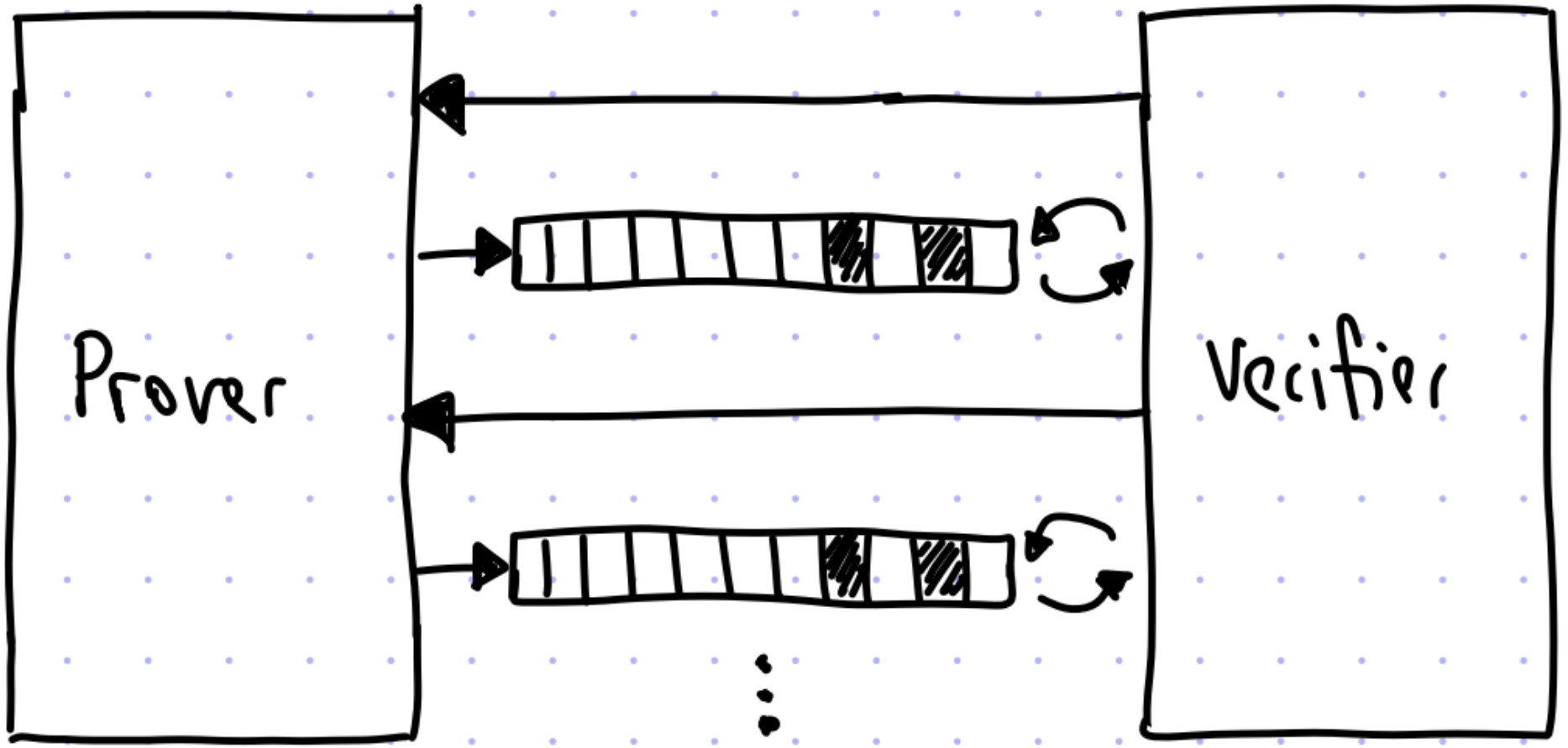
PCP represents proofs where the polynomial-time verifier has two new resources:

① randomness, and ② oracle access to proof



Interactive Oracle Proof (IOP)

add randomness, interaction, and oracle access to proof



- $\mathcal{IP} = \mathcal{PSPACE}$
- $\mathcal{MIP} = \mathcal{NEXP}$
- $\mathcal{MIP}^* = \mathcal{RE}$
- $\mathbf{NP} = \mathbf{PCP}[\mathrm{O}(\log n), \mathrm{O}(1)]$

What are

PZK/SZK/CZK/HVZK/WI/WH

$$\left\{\left\langle P, V^{*}\right\rangle(x)\right\}_{x \in L}$$

$$\sim$$

$$\left\{S^{*}(x)\right\}_{x \in L}$$

- WI: don't know which witness is used

$$\left\{\left\langle P\left(w_x^1\right), V^*(z)\right\rangle(x)\right\}_{x\in L, z\in\{0,1\}^*}$$

$$\left\{\left\langle P\left(w_x^2\right), V^*(z)\right\rangle(x)\right\}_{x\in L, z\in\{0,1\}^*}$$

- WH: difficult to reverse the witness

$$\Pr\left[\left\langle P\left(Y_n\right), V^*(z)\right\rangle\left(X_n\right) \in R_L\left(X_n\right)\right] < \frac{1}{p(n)}$$

What are

Argument/KS/SE/UC

> **arguments** permit the existence of “proofs” of incorrect statements, so long as those “proofs” require exorbitant computational power to find

- i.g. soundness for computational bounded prover (**Computational soundness**)

Knowledge Soundness (Proof of Knowledge)

- Not only the witness exist, but also I "know" it.

> The password of this account *exists*, but I did not know it.

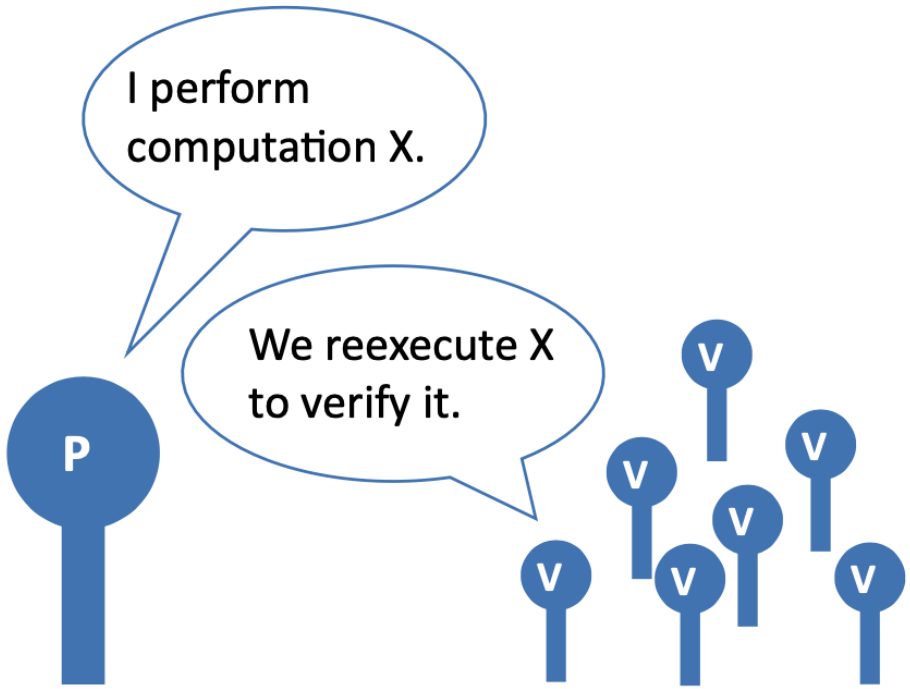
- SE/UC

What is *Non-Interactive*

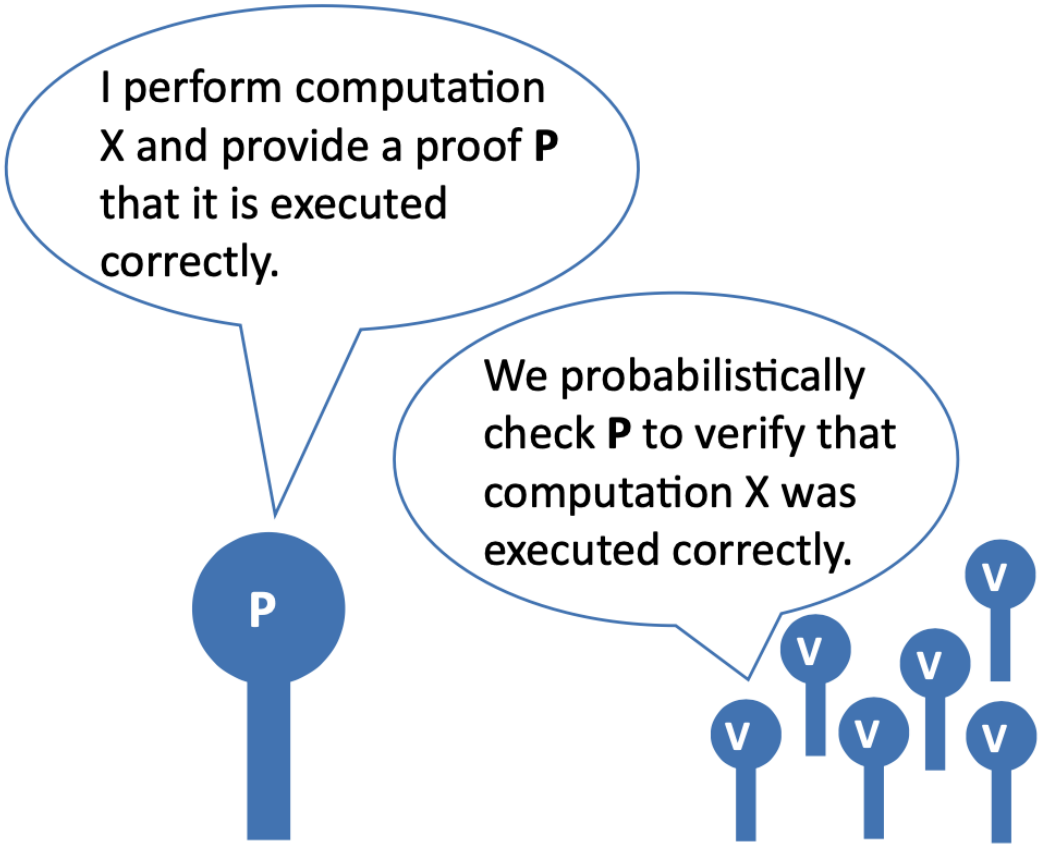
- Not "No Interaction"
- consists of a single message from $\mathcal{P}$ to $\mathcal{V}$
- designated verifier/ publicly verifiable
- Fiat-Shamir Transformation: $c = H(\mathrm{Trans})$
- public coin vs privite coin
- NIZK/ Signature

What is *Succinctness*

Reexecution vs Using a Proof



A. Multiple reexecution



B. Using a proof

What is *Trusted Setup/Ceremony*

- An algorithm that determines a protocol's public parameters using information that must remain secret to ensure the protocol's security.
- Maybe a MPC protocol
- CRS model: no NIZK in plain model beyond $\mathcal{BPP}$
- Circuit-specific/Universal/Updated/Transparent
- Vitalik: How do trusted setups work?
- KZG Ceremony: https://ceremony.ethereum.org/

What is *Polynomial Commitment*

- in the first phase, a Prover commits to a polynomial p by emitting a public commitment; in the second phase the Verifier chooses a value x, and the Prover produces a value y and convinces the Verifier that $y = p(x)$.
- KZG/IPA/FRI/Ligero/Brakedown/Orion...

What is *Arithmetization*

- The process of turning *a generic statement or question* into *a set of equation* to be verified or solved.

> I am twice older than my youngest sibling

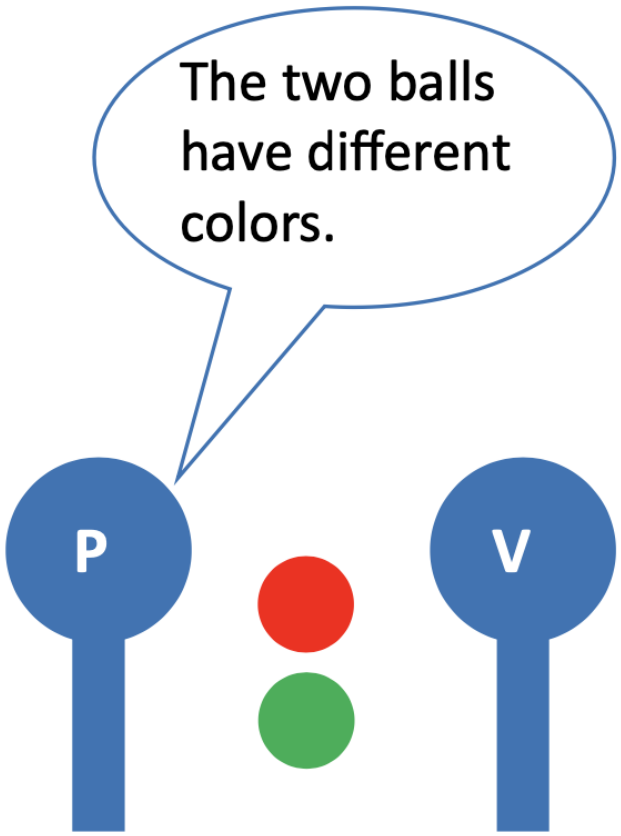
$$x = 2 * \min\left(a_1, a_2, \ldots, a_n\right)$$

- Boolean Circuits/Arithmetic Circuits
- R1CS/QAP/Plonkish/AIR/CCS
- Front-end: Circom/Cairo/Noir/Leo…

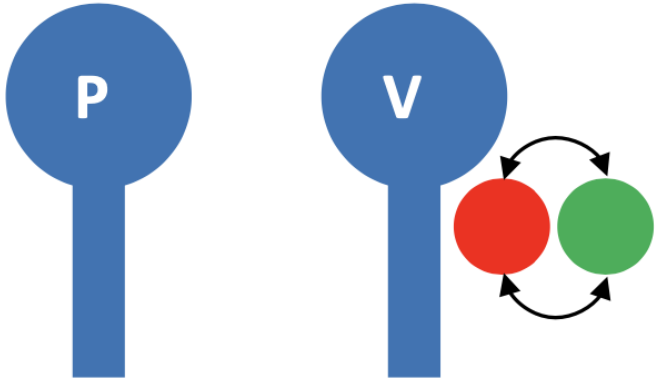
Some Examples

1. Coke Vs. Pepsi

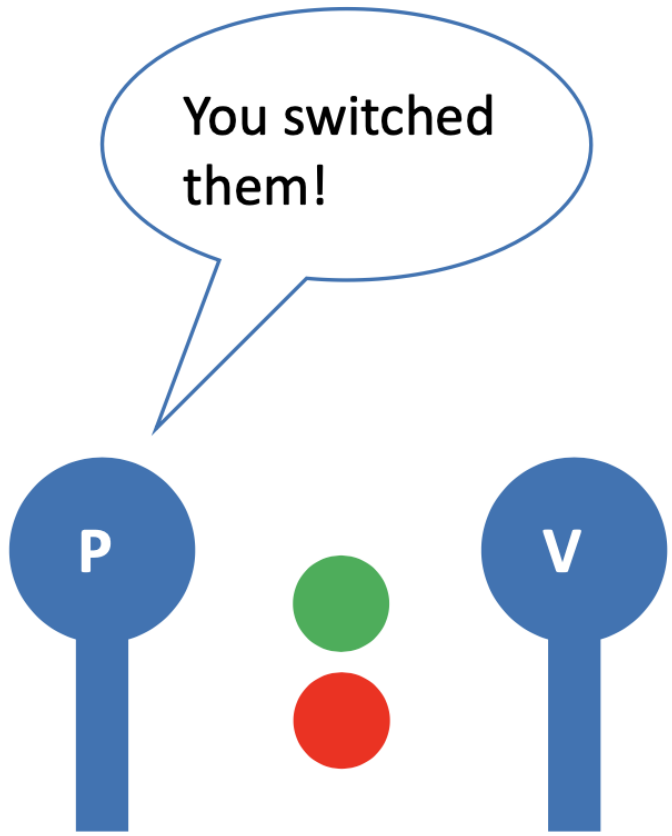

Coca-Cola
Pepsi



A. Statement



B. Shuffling



C. Verification

- Recall: Knowledge
- transfer of trust
- $coNP$
- Soundness error $\epsilon_s = \frac{1}{2^n}$
- Private coin
- Designated verifier

2.Where's Waldo


LE CHÂTEAU DES VAMPIRES
CHARLIE ET LE MAGE BLANCHEBARBE FONT HALTE AU CHÂTEAU DES VAMPIRES, DANS LEQUEL BEAUCOUP D'AUTRES CHARLIE SE SONT DÉJÀ AVENTURÉS. PARTOUT CE NE SONT QUE CLIQUETIS D'OS (L'OS DE OUAF EST CELUI QUI EST LE PLUS PROCHE DE SA QUEUE), RICANEMENTS DIABOLIQUES, RÉPUGNANTS GARGOUILLIS. CHARLIE S'EMPARE DU SIXIÈME PARCHEMIN AUSSI VITE QU'IL LE PEUT ET POURSUIT SON VOYAGE.

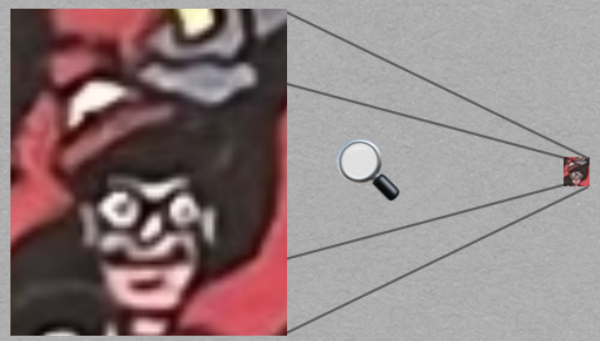
M

N

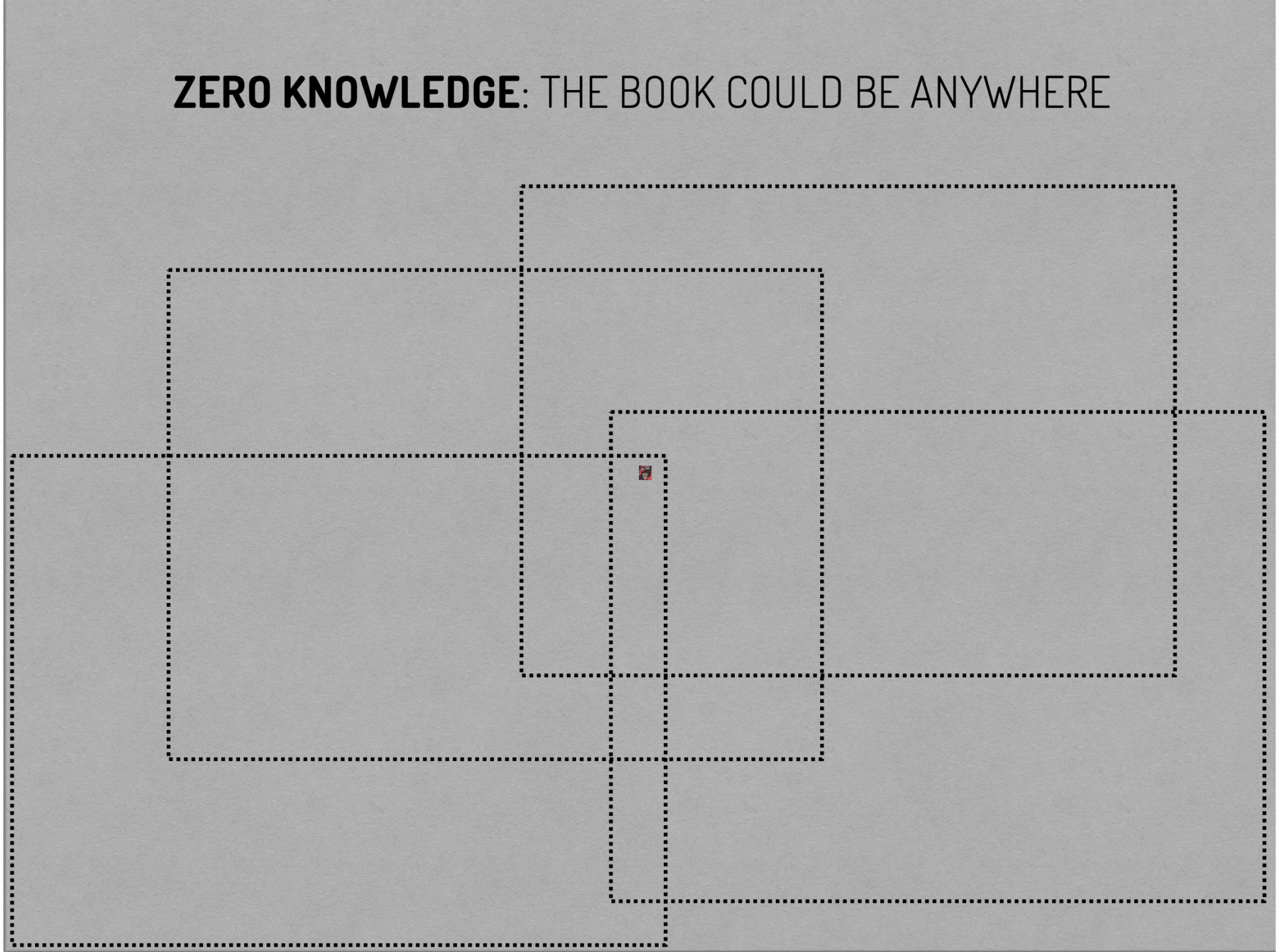
2N

2M

SOUNDNESS: THE VERIFIER CAN SEE WALDO FOR THEMSELVES!



ZERO KNOWLEDGE: THE BOOK COULD BE ANYWHERE



- non-interactive
- proof of knowledge
- ceremony

Other Examples

- Alibaba's Cave/Sudoku
- GI/QR/GNI/QNR/G3C/Hamilton/Schnorr
- Oded Goldreich

Application of ZKP

- Blockchain(Rollups/zkEVM/Private Cryptocurrencies)
- zkDocs: Zero-knowledge Information Sharing (Age > 18)
- Zordle: ZK Wordle
- Using ZK Proofs to Fight Disinformation
- A zero-knowledge protocol for nuclear warhead verification
- Identification/Voting/PET/Copyright Protection etc.

Thanks

(I hope this talk is NOT Zero-Knowledge for you :))

Kurt Pan's Awesome Zero-Knowledge Proofs (2022):
https://site.kurtpan.pro/ktpzkp22.html