Zero-knowledge proofs: prelims

- Intuition
- Languages, relations, witnesses
- ZKP syntax
- ZKP security

Intuition

Coke vs. Pepsi - same or different?

1. Buy coke/pepsi from b
2. Give to distinguisher
3. Distinguisher guesses bit
4. Amplify

Interactive proof - prove truth of statement to verifier. Zero-knowledge: hide the "why"

Relations, languages, witnesses

A Language — set of bit strings: $L \subseteq \{0,1\}^*$

usually share some property: e.g. 3-colorable graphs

An (NP) relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$

given det. polytime $W(\cdot,\cdot) : 0/1$

statement x, witness w

$$R = \{(x,w) : W(x,w) = 1\}$$

$$L_R = \{x : \exists w \text{ s.t. } W(x,w) = 1\}$$

E.g. graph x, witness w

ZKP Syntax

A ZKP for a language L w/ w.c. W has two randomized ITMs (P, V)

- P unbounded, V ppt
- $P(x, w) \leftrightarrow V(x)$ ← outputs 0/1
- Sending witness satisfies func: V can run W
- non-interactive: one msg $P \to V$
  Preprocessing: create/setup based on L
  Succinct: low communication, low V comp.