

Zero Knowledge Proofs (ZKP)

- Interactive Proofs
- Zero Knowledge & Simul
- Interactive Digital Signatures
- Non-interactive ZKP
- Succinctness etc. [ZERONARKS]

Definition of a Proof

Proof \equiv string c

Class PP

\exists poly-time TM M s.t. $\forall w \in L \Rightarrow M(w) = \text{accept}$
 $\forall w \notin L \Rightarrow M(w) = \text{reject}$ } poly time
 deciders

then $L \in P$

Class NP

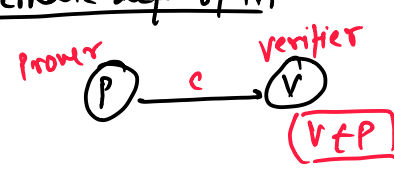
\exists poly-time TM M s.t.
 $\forall w \in L \exists c \text{ s.t. } M(w, c) = \text{accept}$
 $\forall w \notin L \nexists c \text{ s.t. } M(w, c) = \text{accept}$ } poly time
 verifiers
 $(c \text{ is called certificate})$

we now allow margin of error
 this gives us BPP

Class BPP

\exists PPTM M s.t.
 $\forall w \in L P[M(w) = \text{accept}] \geq 2/3$
 $\forall w \notin L P[M(w) = \text{reject}] \geq 2/3$

Alternate def of NP



$\forall w \in L \exists P \text{ s.t. } (P \rightarrow V) \text{ accepts}$
 $\forall w \notin L \forall P^* P^* \rightarrow V \text{ reject}$

Class BPPNP

$\forall w \in L \exists P P[(P \rightarrow V) = \text{accept}] \geq K$
 $\forall w \notin L \forall P^* P[(P^* \rightarrow V) = \text{accept}] \leq K'$ ($K < K'$)

for now Prover-Verifier communication is one-way
 if Verifier can communicate with Prover we get IP

IP = PSPACE = NPSpace

PSPACE should be \supset NP
 not yet proven
 more powerful than NP ($\because IP \geq \text{co-NP}$)

Intuition

Consider a Game

winning strategy

$\exists m_1 \forall m_2 \exists m_3 \forall m_4 \dots f(m) = 1$
 your moves app moves
 TQBF Problem

hard to get a certificate (need to give entire decision)
 \neq NP (not proven yet)

easy to solve using interaction (just play a game with V)

(needs more strategy: Arithmetic) [convert Boolean formula to arithmetic formula]

ZKP

completeness: $\forall w \in L \exists P P[(P \rightarrow V) = \text{accept}] \geq K$

soundness: $\forall w \notin L \forall P^* P[(P^* \rightarrow V) = \text{accept}] \leq K'$ ($K > K'$)

Zero Knowledge: \exists PPTM S that 'simulates' interaction with P
 V does not get any certificate

$NP \leq ZKP$

verifier interacting with P

verifier interacting with S

Proof

Consider an NP Problem

say, Graph 3-coloring (NP-complete)

Input: Graph $G = (V, E)$

Output: Yes if G is 3-colorable (tripartite)

- Prover permutes the 3 colors (R, G, B) and generates another valid 3-coloring of G
- \forall nodes, send a locked box containing the color values



- Verifiers asks for keys of the boxes of endpoints of any random edge in G
 $(i, j) \in E \forall i, j \in V$ requested

- if $C_i = C_j \rightarrow \text{accept}$
 $C_i \neq C_j \rightarrow \text{reject}$

Completeness

if coloring is valid; color of endpoints will always be different

$\therefore \text{Pr}[(P \rightarrow V) = \text{accept}] = 1$

Soundness

$\text{Pr}[(P^* \rightarrow V) = \text{accept}] = 1 - \frac{1}{|E|} < 1$

P^* can cheat by adding another color; but will be caught with non-zero prob.

Zero-Knowledge

for $(i, j) \in E$ if valid 3-coloring exists

(C_i, C_j) will be unequal

can be $(R, G), (R, B), (B, R), (B, G), (G, R), (G, B)$
 with equal prob.

simulator S creates $(R, G), (R, B), (B, R), (B, G), (G, R), (G, B)$
 with equal prob.

$\therefore S$ & P are indistinguishable to V

How to make boxes? Use Bit commitment

so that there is guarantee that color inside box isn't changed when giving keys
 Use commit phase & reveal phase

Digital Signatures are non-interactive Zero Knowledge Proof.

Prover sends signature to verifier

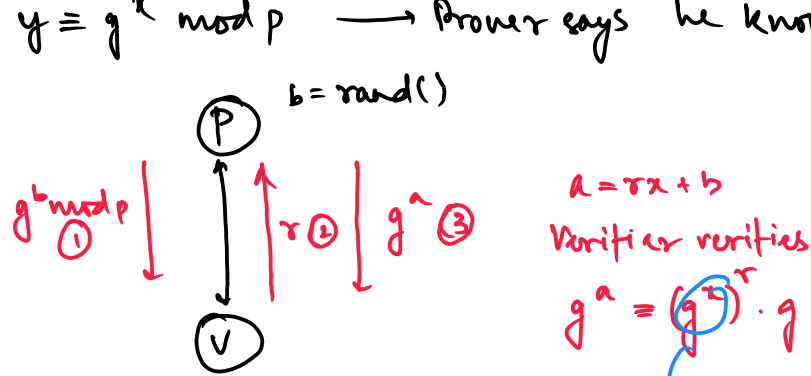
Verifier can verify Prover is the author of the message without knowing the message

Interactive Digital Signatures \rightarrow not impractical

Shamir's problem

ZKP for DLP

$y = g^x \text{ mod } p \rightarrow$ Prover says he knows x



Here system is Interactive

(V is sending back r)

Use Fiat-Shamir Heuristic

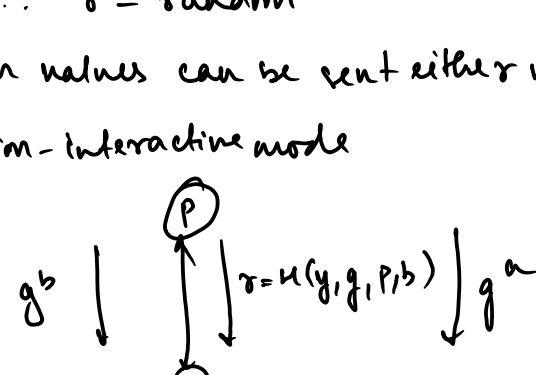
$H(y, g, p, b) = r$

Hashes are equivalent to random oracle

$\therefore r = \text{random}$

random values can be sent either way

\therefore non-interactive mode



non-interactive (only Prover sending) \equiv Digital signature

Succinctness

since hash-and-sign paradigm allows large messages to have small digital signature. we define succinctness as the amount of compression of a proof (non-interactive)