Quickie proposal:
What are hash trees and why you should care
Algo \[ \text{Titlu} \]
1. Hash functions
2. Hash trees
3. Authenticated data structures
Hash functions

one-way
pre-image attack

second pre-image attack
collision attack

- ∐ → 0
- □ →

birthday paradox

23 people

≥ 50%
Hash trees
Hash chains
Authenticated log
naive a.k.a. blockchain

... → O → O → O → O → O → ...

D D D
Authenticated logs

tree-based

...
Authenticated Map

key $\Rightarrow$ value

hash(key) $\Rightarrow$ value
Authenticated Map
with modification
hīshti a.k.a.
auth. log-backed map

state 1
state 2