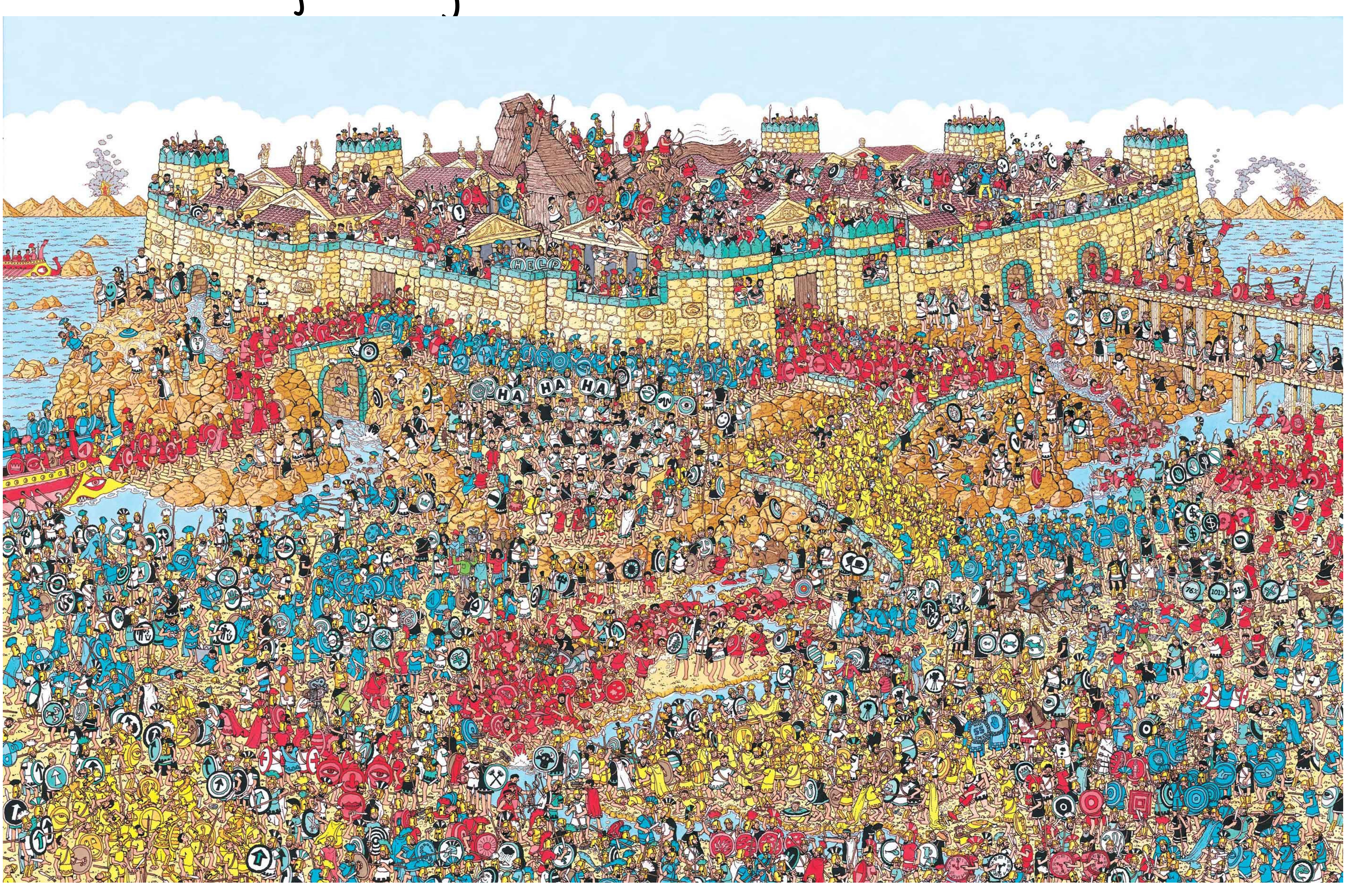
# Zero-knowledge proofs and secure computation

3/8/21 12:05 AM

## Administrivia.

- Final Exam.
  - A few questions. covering everything.
  - Open book. no discussions
  - Allow multiple submissions. Last day: 3/16 (Tue)

## Zero-knowledge Proofs.



An interactive proof (P.V) for L is zero-knowledge if

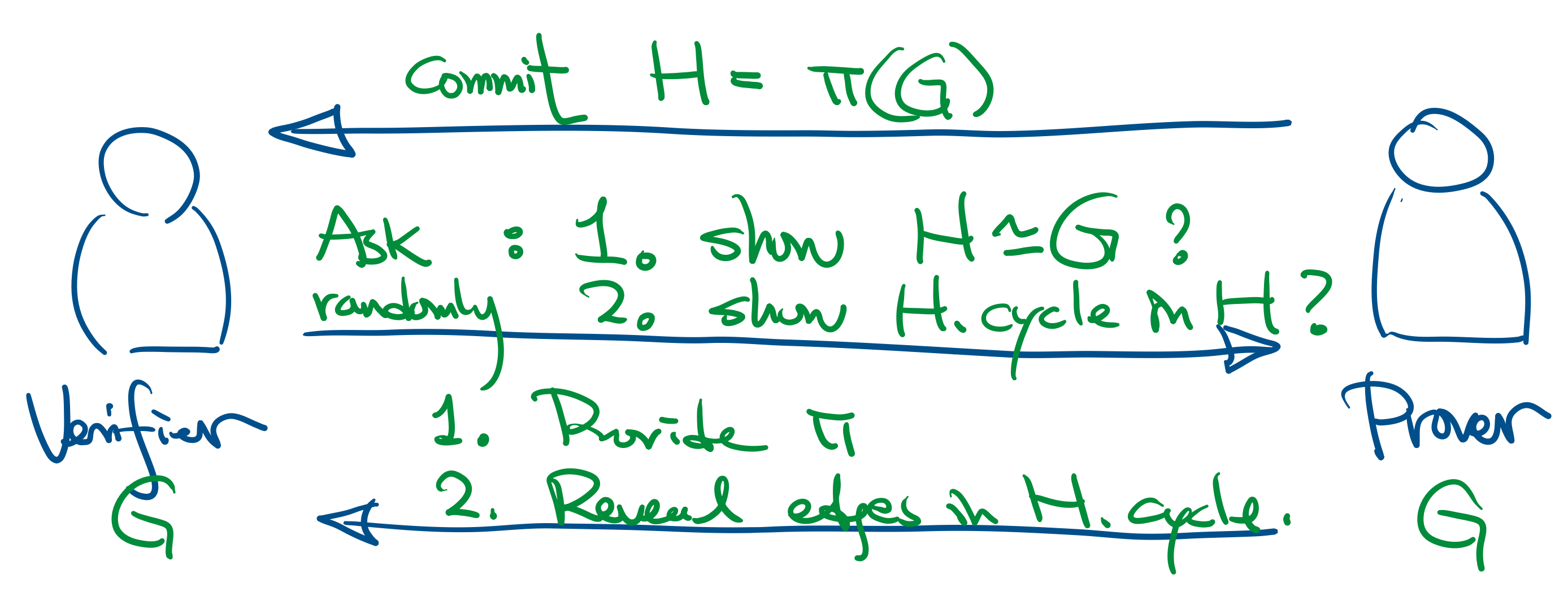
- [complete] honest V convinced w.h.p. by honest P.
- [sound] crooked $\tilde{P}$ fail to convince honest V.
- [zero-knowledge] no malicious $\tilde{V}$ learns anything beyond the statement is true.

Computationally indistinguishable.

Q. What problems have ZK proofs?

Thm HAMCYCLE has CZK proof. [M. Blum'86]

Pf.



Commit $H = \pi(G)$
Ask randomly: 1. show $H \simeq G$? 2. show H.cycle in H?
1. Provide $\pi$
2. Reveal edges in H.cycle.
Verifier
G
Prover
G

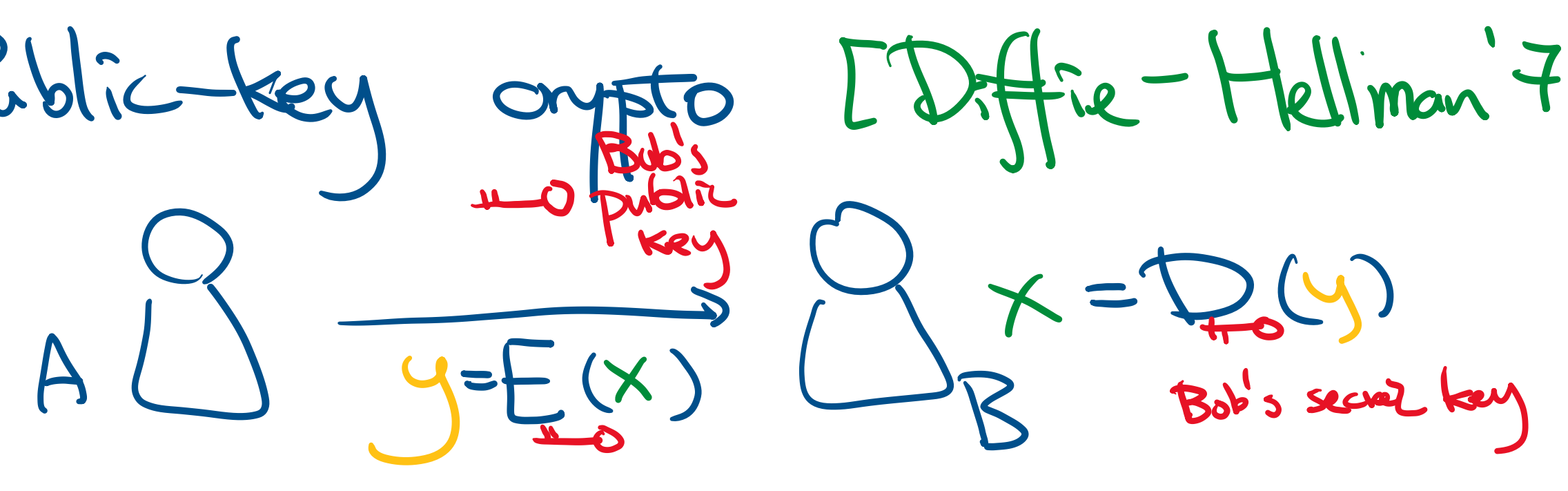
- [complete] Prover knows H.cycle in G ⇒ in H.
- [sound] If G has no H.cycle. but $\tilde{P}$ fakes it. Commit fake $\tilde{H} \neq G$.
- [ZK] Every round $\hat{V}$ learns either
  - $H \simeq G$. (but not H.cycle in H)
  - H has H.cycle. (but not $\pi$)

  $\hat{V}$ can simulate P:

  Pretend to be P.
  - Choose randomly: 1. choose $\pi$. $H = \pi(G)$ 2. $H = K_n$.
  - $\boxed{\text{Commit}}$ H.
  - Answer questions w/ $\pi$, or H-cycle.

## Application. Secure computation.

- Public-key crypto [Diffie-Hellman'76, RSA'77]

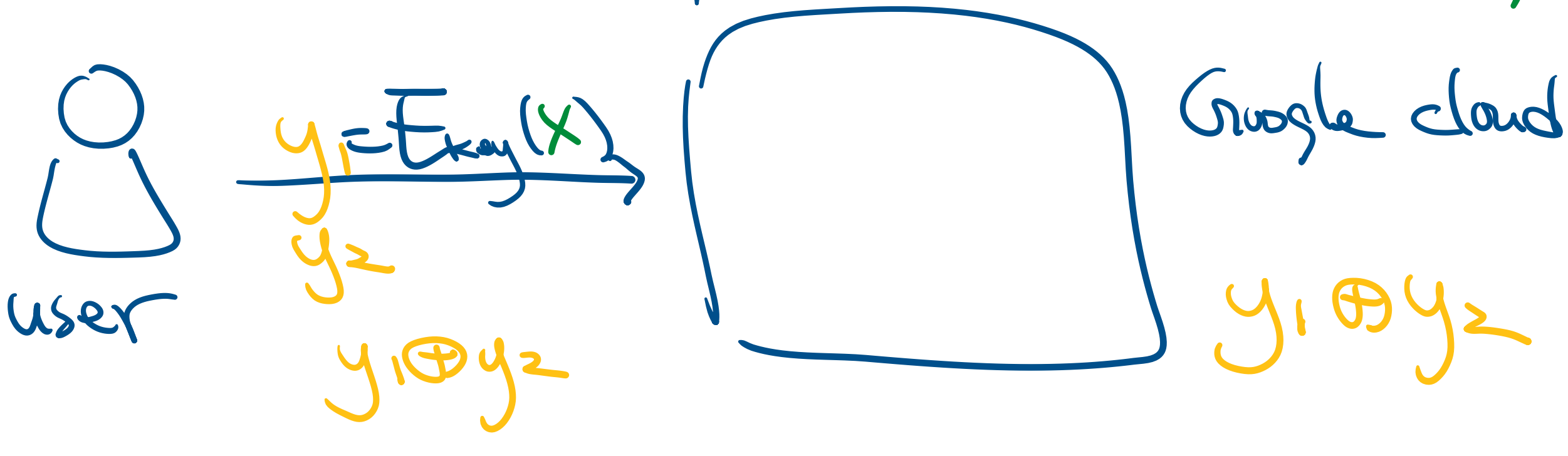


- Secret sharing [Shamir-Blakley'79]

  $P(x) = a_0 + a_1 x + a_2 x^2$ $P(0)$

  pirates & treasure box.
- Multi-party secure computation. [Yao'82]

  millionaire problem.
- Fully homomorphic encryption scheme. [Gentry'09]



Which world do we live in? [Impagliazzo'95]

- Algorithmica: P=NP and actually practical.
- Heuristica: P≠NP but efficient on avg/in practice
- Pessiland: NP problems hard on avg. no PRG.
- Cryptomania: ∃PRG. secure computation.

Q. Does undiscovered/under-utilized physic laws change which world we are in?

- Quantum.
- Time travel