COS433/Math 473: Cryptography

Mark Zhandry

Princeton University

Spring 2020

Announcements

HW7 Due SUNDAY
Project 3/HW 8 due May 12th

Final Exam Details

Slightly longer than homework, but slightly shorter questions

Pick any **48 hour** period during the dates **May 13 – May 21**

- Will send out more comprehensive instructions

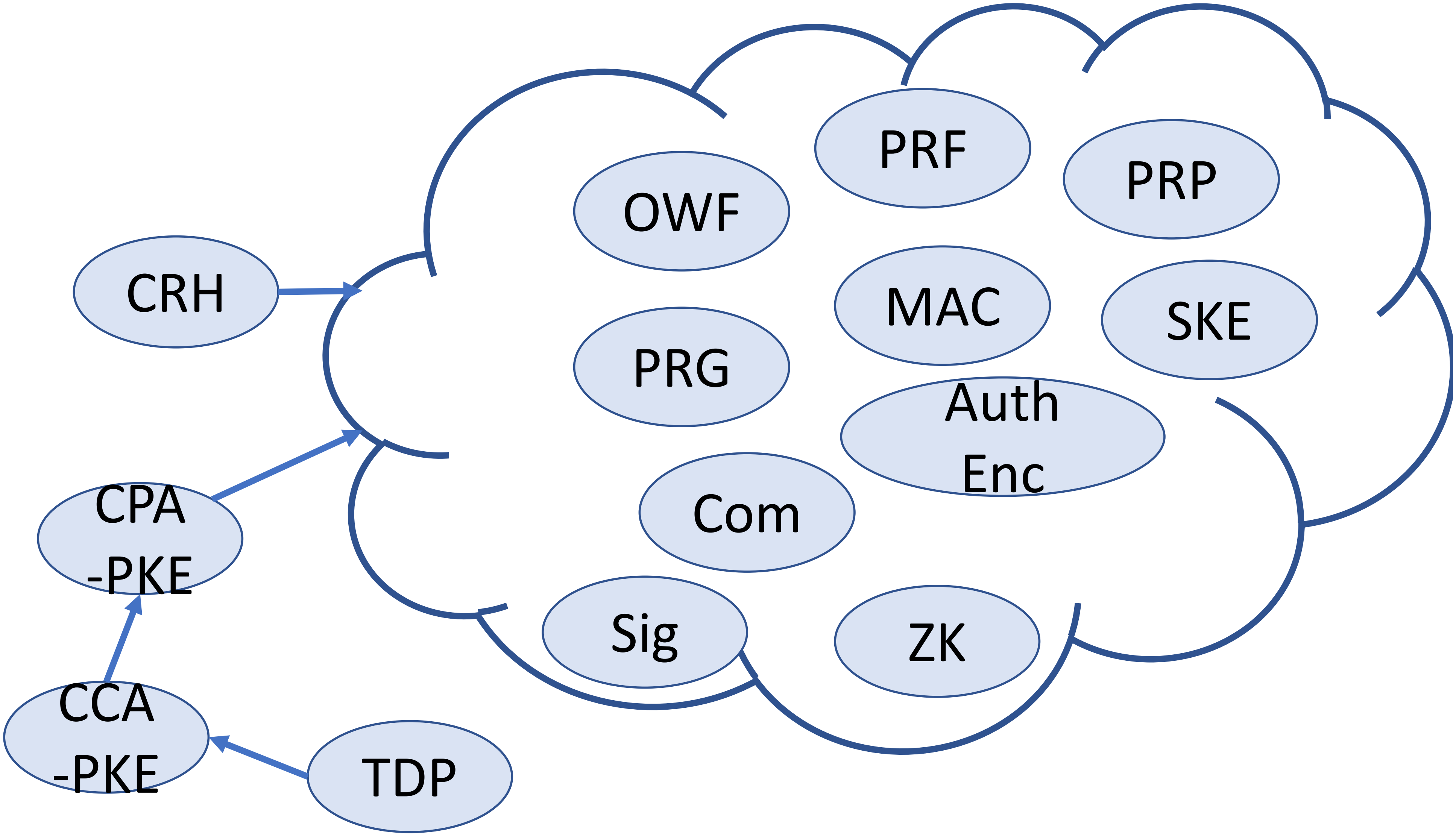
Individual, but open notes/slides/internet…

Example exams on course webpage

Previously on COS 433…

Crypto from Minimal Assumptions

What's Known



CRH
CPA
-PKE
CCA
-PKE
TDP
OWF
PRF
PRP
MAC
SKE
PRG
Auth
Enc
Com
Sig
ZK

Generally Believed That…

Cannot construct PKE from OWF

Cannot construct CRH from OWF

Cannot construct PKE from CRH

Cannot construct CRH from PKE

Black Box Separations

How do we argue that you cannot build, say, PKE from collision resistance?

- We generally believe both exist!

Observation: most natural constructions treat underlying objects as black boxes (don’t look at code, just input/output)

Maybe we can rule out such natural constructions

Black Box Separations

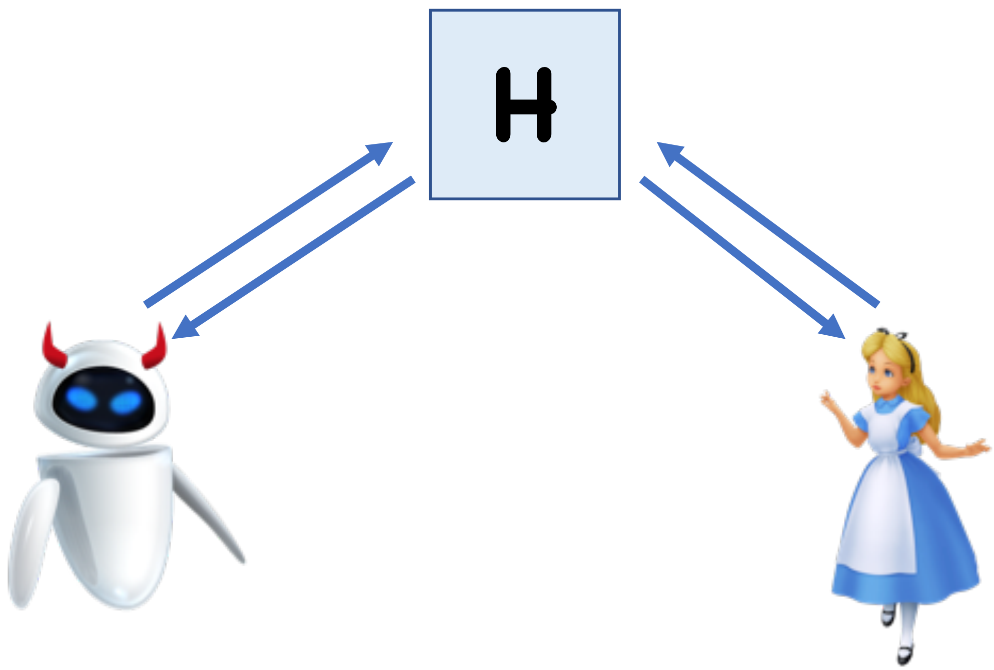
Present a world where collision resistance exists, but PKE does not

Hopefully, natural (black box) constructions make sense in this world

- Can construct PRGs, PRFs, PRPs, Auth-Enc, etc

Separating PKE from OWF

Random oracle model:



Computation power is unlimited, but number of calls to random oracle is polynomial

Separating PKE from OWF

In ROM, despite unlimited computational power, CRHF functions exist

- $F(x) = H(x)$
- Best collision finder is birthday attack → exponential queries

Possible to show PKE does NOT exist in ROM

- In fact, not even public key distribution exists
- Idea: adversary can use unlimited computational power to narrow down search to just a few secret keys without making any oracle queries

Black Box Separations

Of course, our pretend world isn't real

However, it shows a barrier for commonly used proof techniques

- Similar to "relativization" for complexity theory

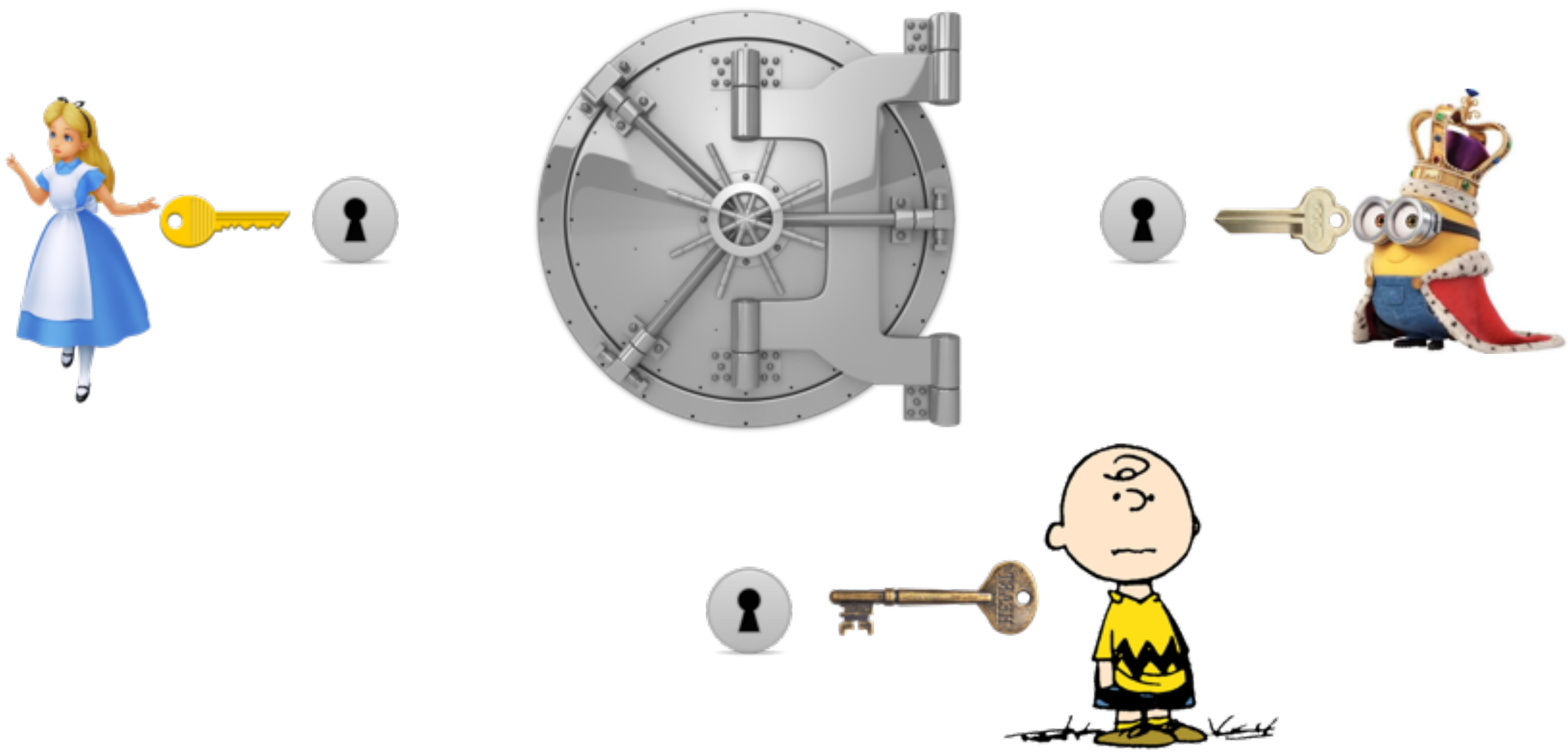
Non-black box techniques are known and used, but relatively rare

Beyond COS 433

Secret Sharing

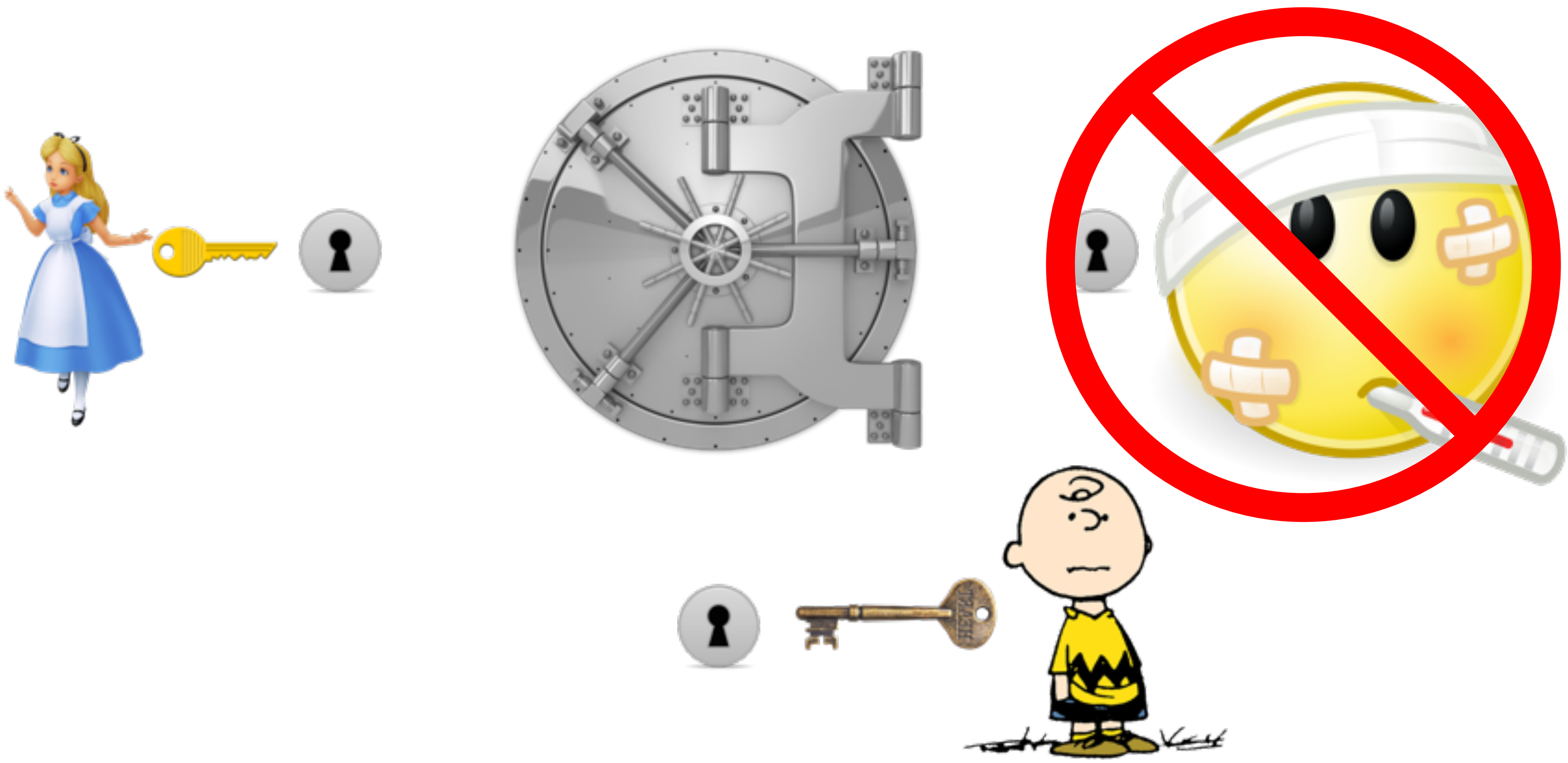
Vault should only open if both Alice and Bob are present

Secret Sharing



Vault should only open if Alice, Bob, and Charlie are all present

Secret Sharing



Vault should only open if any two of
Alice, Bob, and Charlie are present

n-out-of-**n** Secret Sharing

Share secret **k** so that can only reconstruct secret if all **n** users get together

Ideas?

t-out-of-n Secret Sharing

Let p be a prime $> n$, $\geq \#(k)$

Share(k,t,n):

- Choose a random polynomial P of degree $t-1$ where $P(0) = k$
- $sh_i = P(i)$

Recon($(sh_i)_{i \in S}$): use shares to interpolate P, then evaluate on 0

t-out-of-**n** Secret Sharing

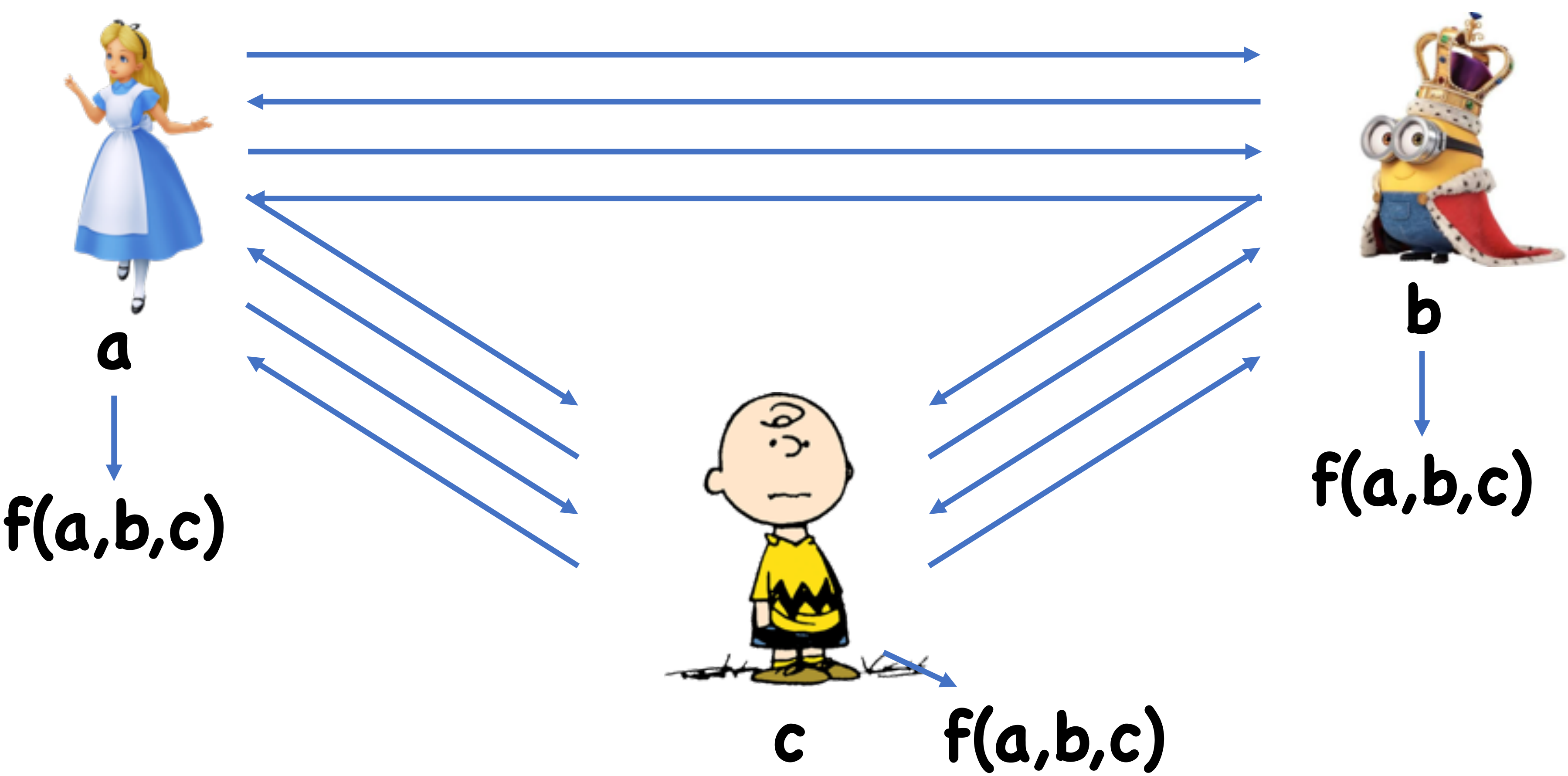
Correctness:

- **t** input/outputs (shares) are enough to interpolate a degree **t-1** polynomial

Security:

- Given just **t-1** inputs/outputs, **P(0)** is equally likely to be any value

Multiparty Computation



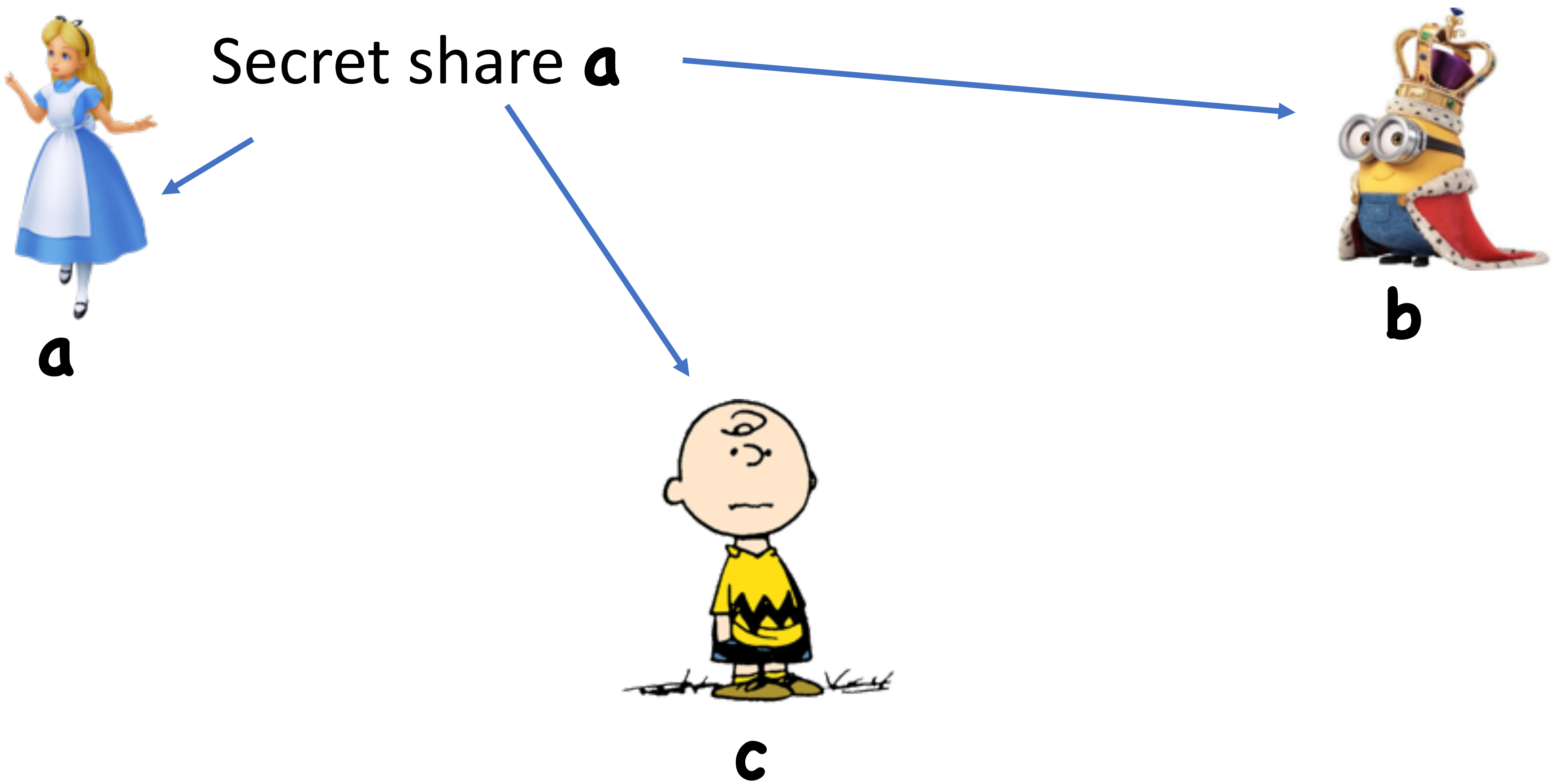
Multiparty Computation

Observation 1: t-out-of-n secret sharing is additively homomorphic:

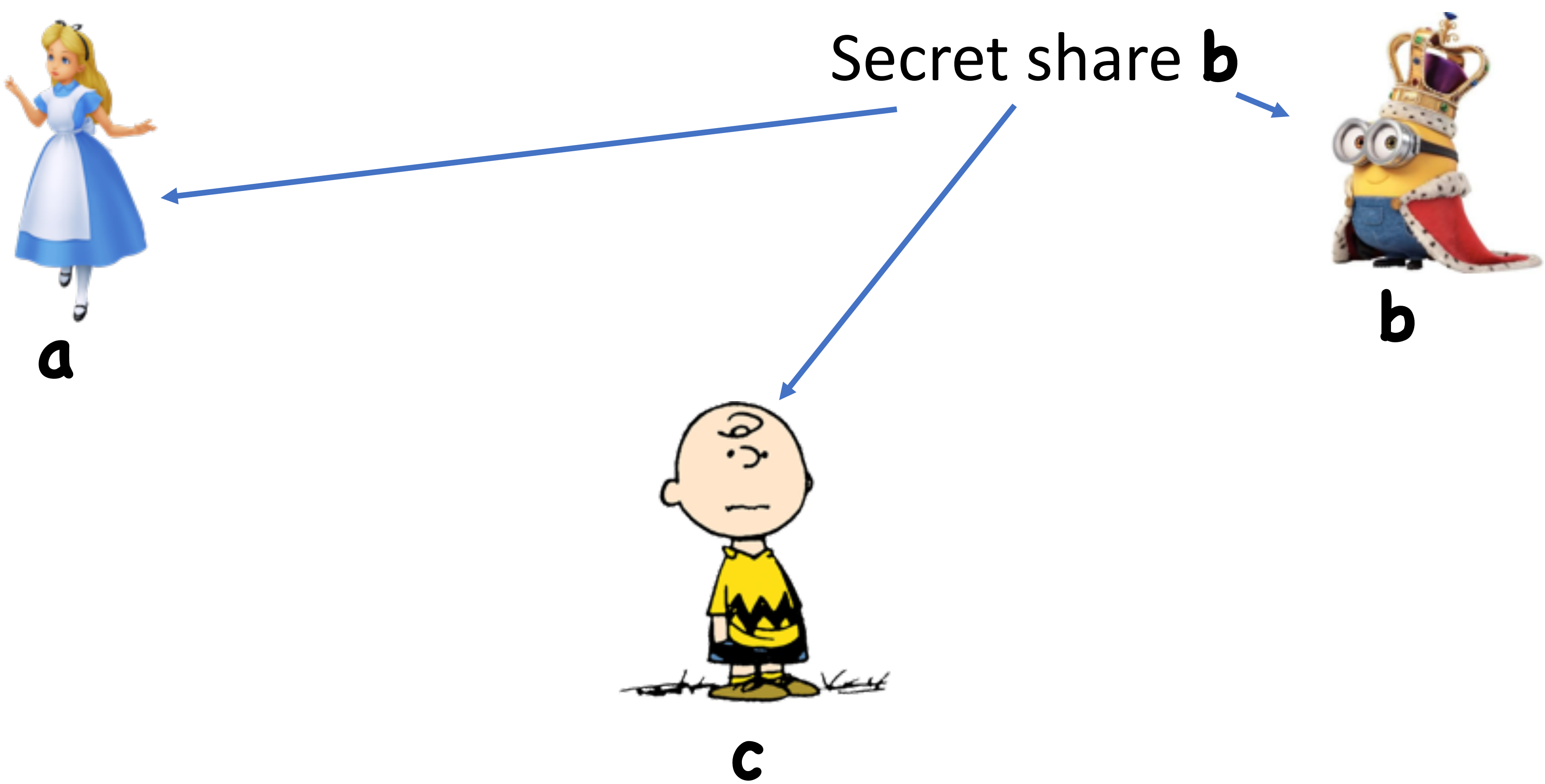
Given shares sh_1 of x_1 and sh_2 of x_2, $r \times sh_1 + s \times sh_2$ is a share of $r \times x_1 + s \times x_2$

- $sh_1 = P_1(i)$, $sh_2 = P_2(i)$, so
$$r \times sh_1 + s \times sh_2 = (r \times P_1 + s \times P_2)(i)$$
- $r \times P_1 + s \times P_2$ has same degree

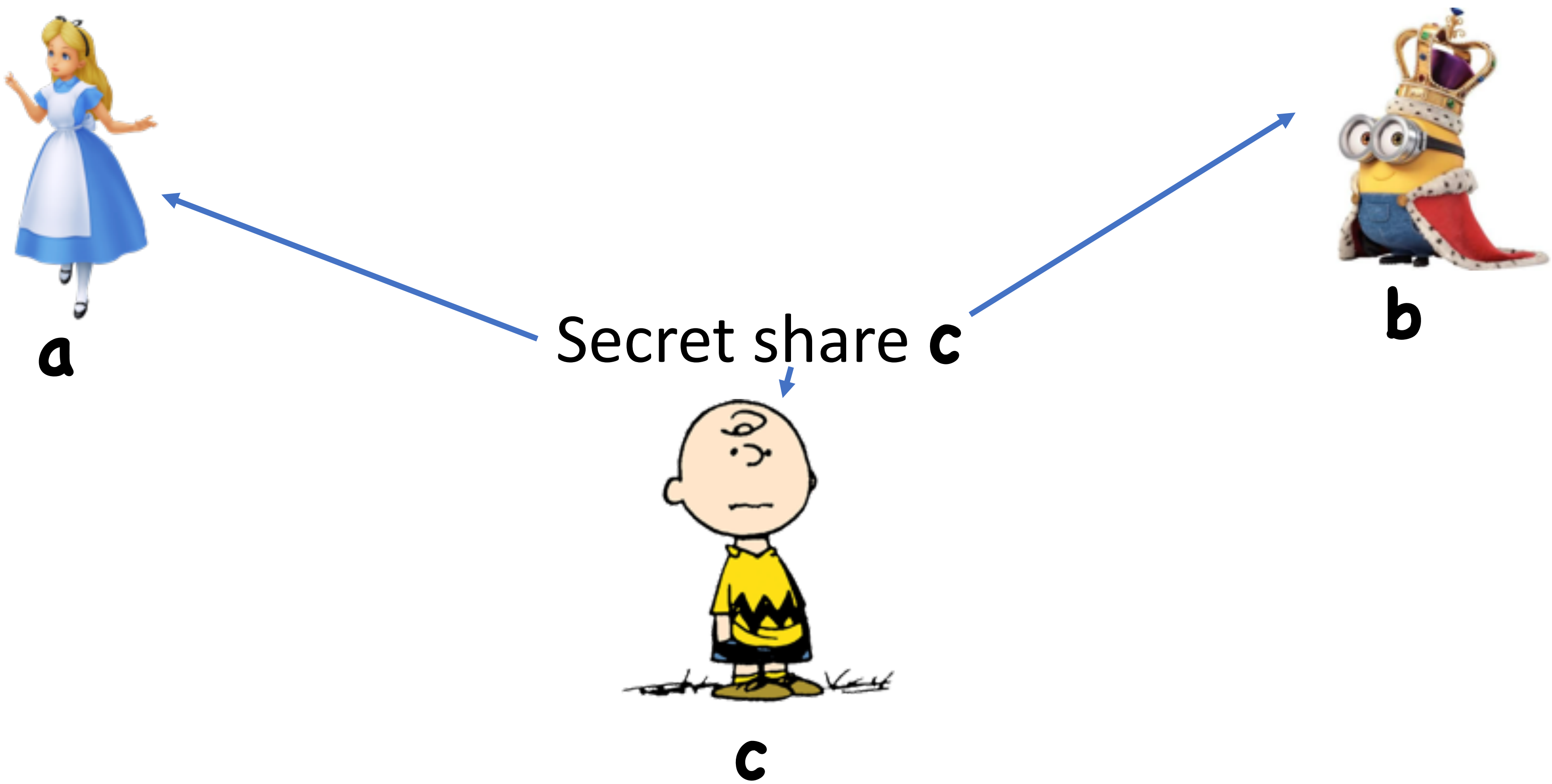
MPC for linear **f**



MPC for linear **f**



MPC for linear **f**



MPC for linear **f**

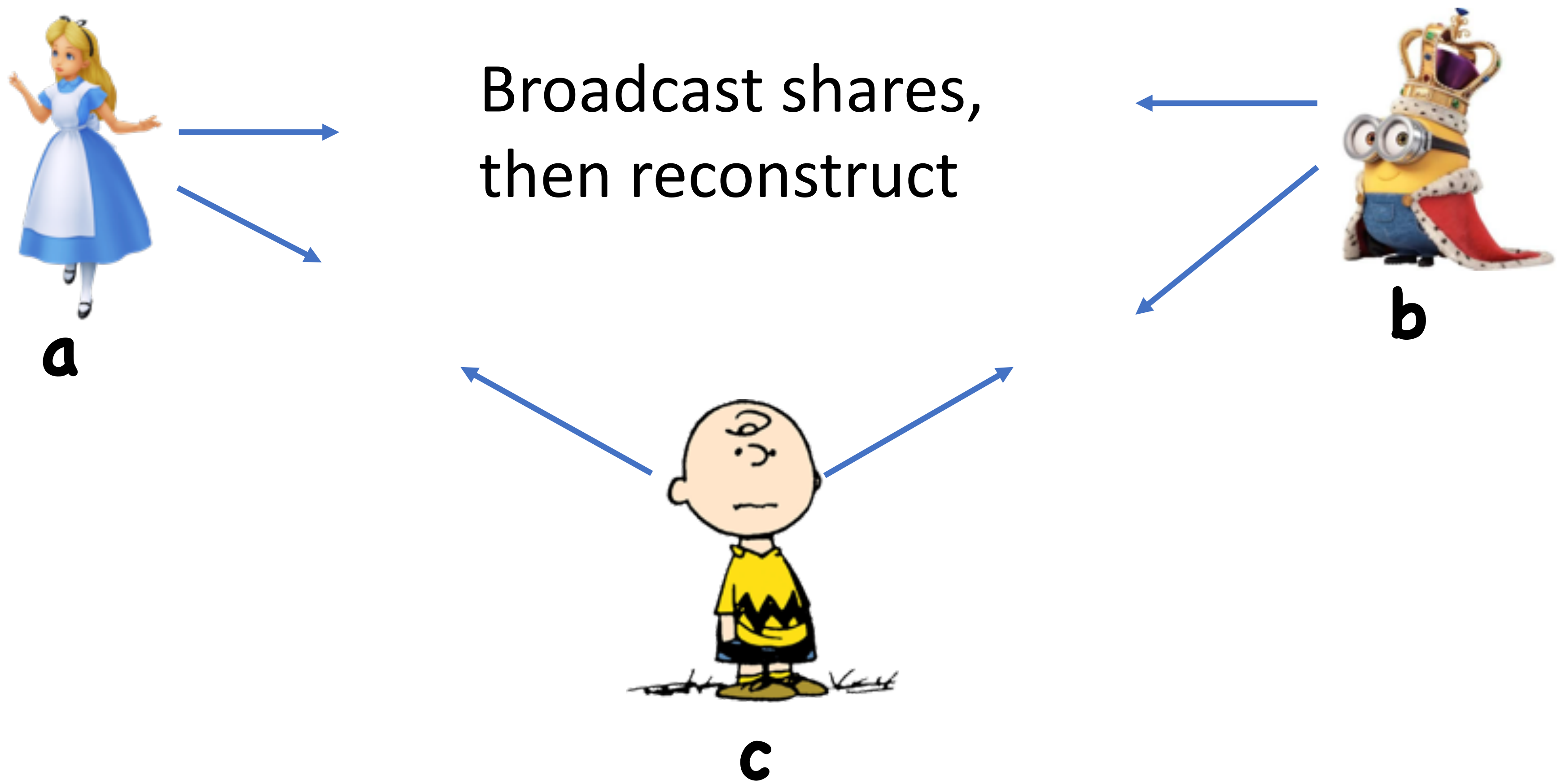
a

Locally compute
shares of **f(a,b,c)**

b

c

MPC for linear **f**



MPC for General $\mathbf{f}$

Observation 2: $\mathbf{t}$-out-of-$\mathbf{n}$ Secret Sharing is sort of multiplicatively homomorphic

Given shares $\mathbf{sh_1}$ of $\mathbf{x_1}$ and $\mathbf{sh_2}$ of $\mathbf{x_2}$, $\mathbf{sh_1 \times sh_2}$ is a share of $\mathbf{x_1 \times x_2}$, but with a different threshold

- $\mathbf{sh_1 = P_1(i)}$, $\mathbf{sh_2 = P_2(i)}$, so
$$\mathbf{sh_1 \times sh_2 = (P_1 \times P_2)(i)}$$
- $\mathbf{P_1 \times P_2}$ has degree $\mathbf{2d}$

Idea: can do multiplications locally, and then some additional interaction to get degree back to $\mathbf{d}$

MPC for General f

To maintain correctness, need threshold to stay at most n

- But multiplying doubles threshold, so need $t \leq n/2$
- This means scheme broken if adversary corrupts n/2 users.
- Known to be optimal for "information-theoretic" MPC

Using crypto (e.g. one-way functions), can get threshold all the way up to n

MPC for Malicious Adversaries

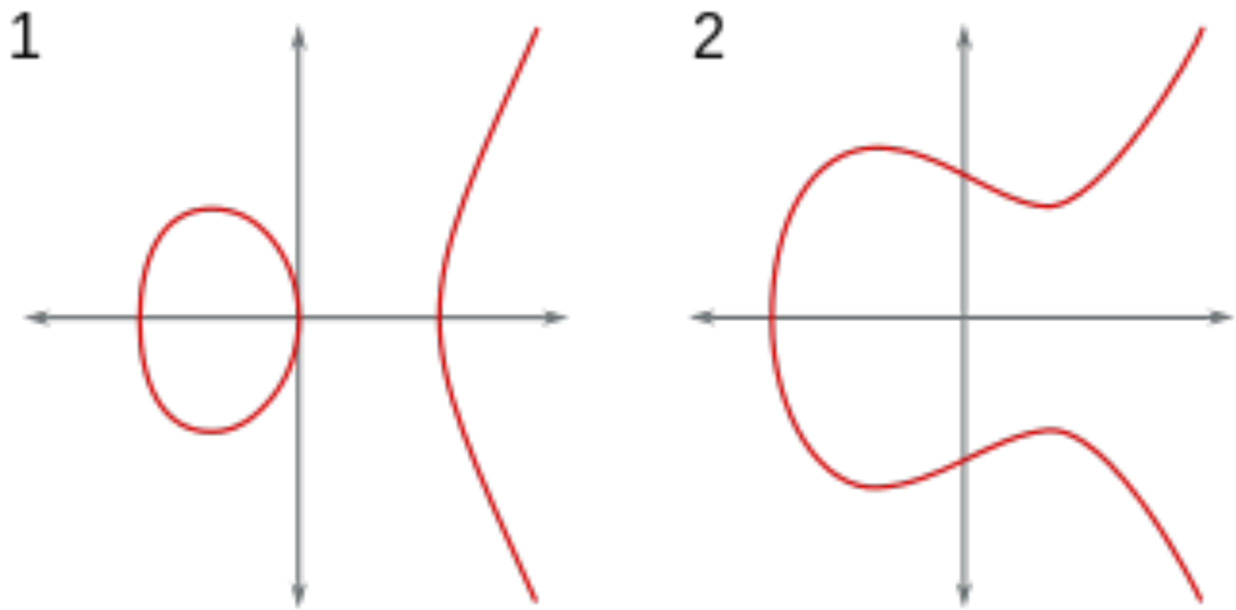
So far, everything assumes players act honestly, and just want to learn each other's inputs

But what if honest players deviate from protocol?

Idea: use ZK proofs to prove that you followed protocol without revealing your inputs

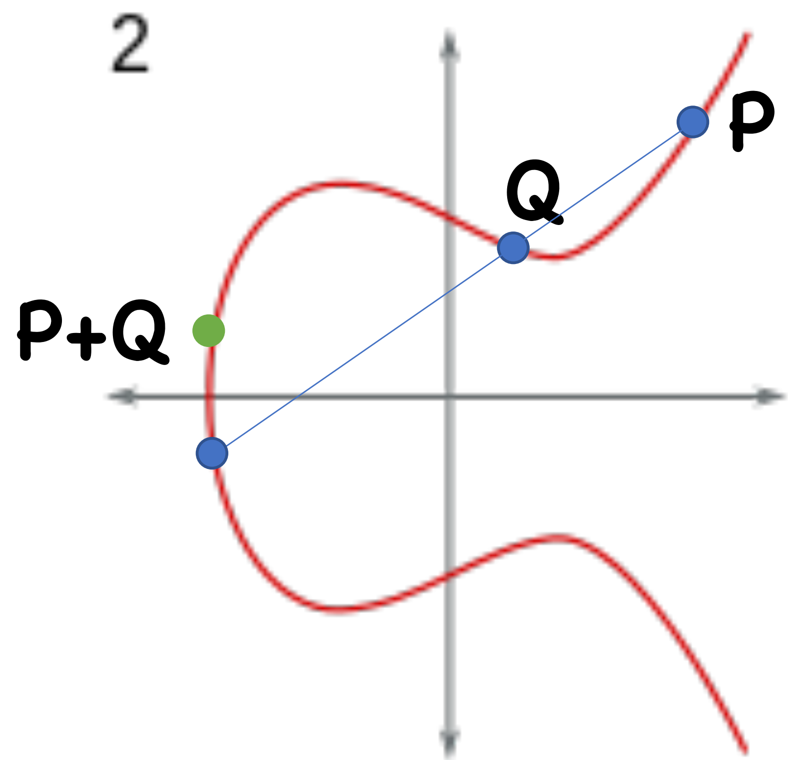
Elliptic Curves

$$y^2 = a\,x^3 + b\,x^2 + c\,x + d$$



$y^2 = x^3 - x$ $\qquad$ $y^2 = x^3 - x + 1$

Group Law on ECs



ECs for Crypto

Consider EC over finite field

Set of solutions form a group

Dlog in group appears hard

- Given $aP = (P+P+\ldots+P)$, find a
- Can use in crypto applications

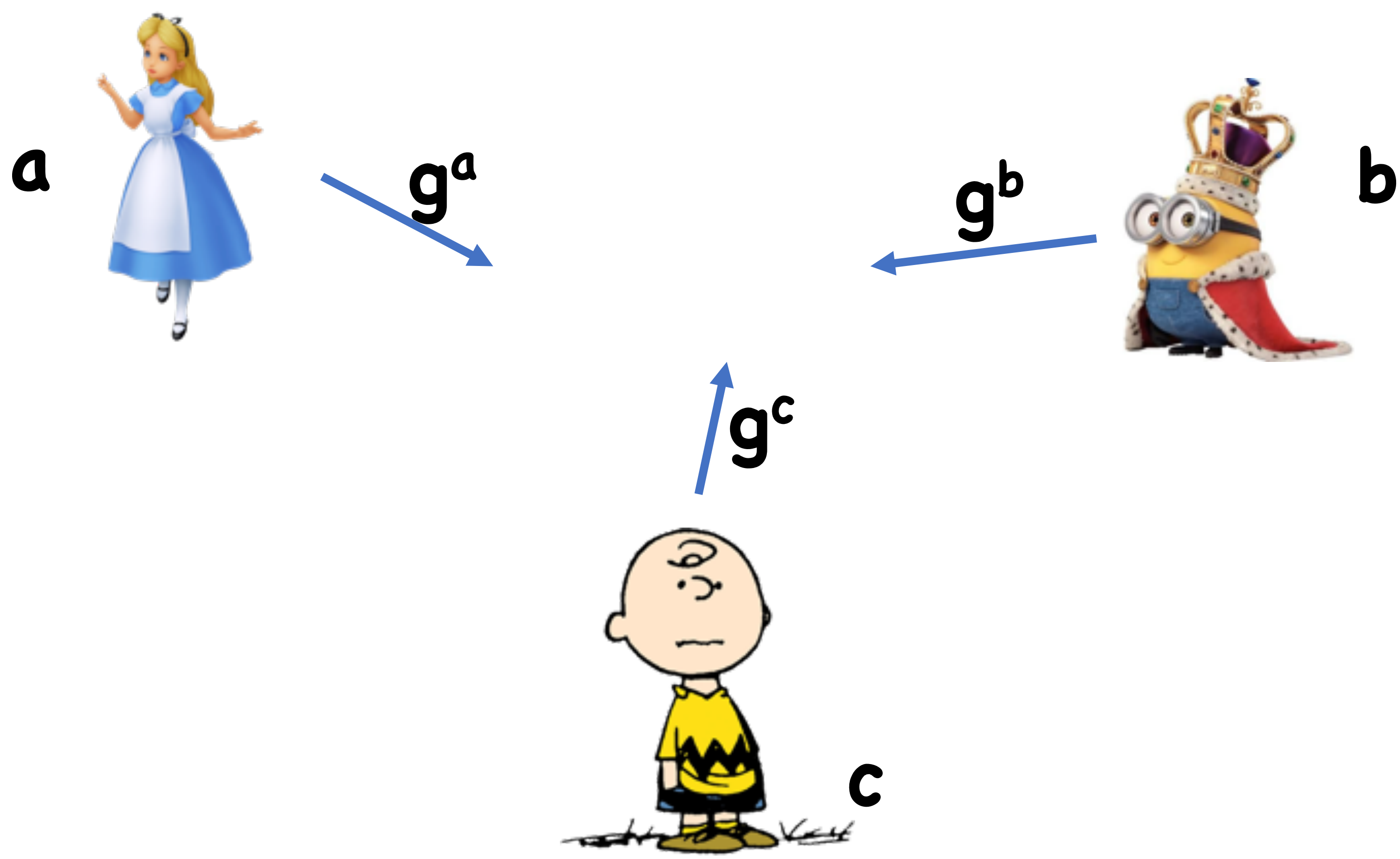
Bilinear Maps

On some Elliptic curves, additional useful structure

Map $\mathbf{e:G\times G\rightarrow G_2}$

- $\mathbf{e(g^a\ ,g^b) = e(g,g)^{ab}}$

3-party Key Exchange



Shared key = $\mathbf{e(g,g)^{abc}}$

Bilinear Maps

Extremely powerful tool, many applications beyond those in COS 433

- 3 party *non-interactive* key exchange
- Identity-based encryption (your public key is just your email address)
- Broadcast encryption (encrypt to arbitrary sets of users more efficiently than simply encrypting to each user)
- Traitor tracing (identify traitor who leaked secret key)

Multilinear Maps

Map $\mathbf{e{:}G^n \rightarrow G_2}$

- $\mathbf{e(g^a\ ,g^b,\ \ldots) = e(g,g,\ldots)^{ab\ldots}}$

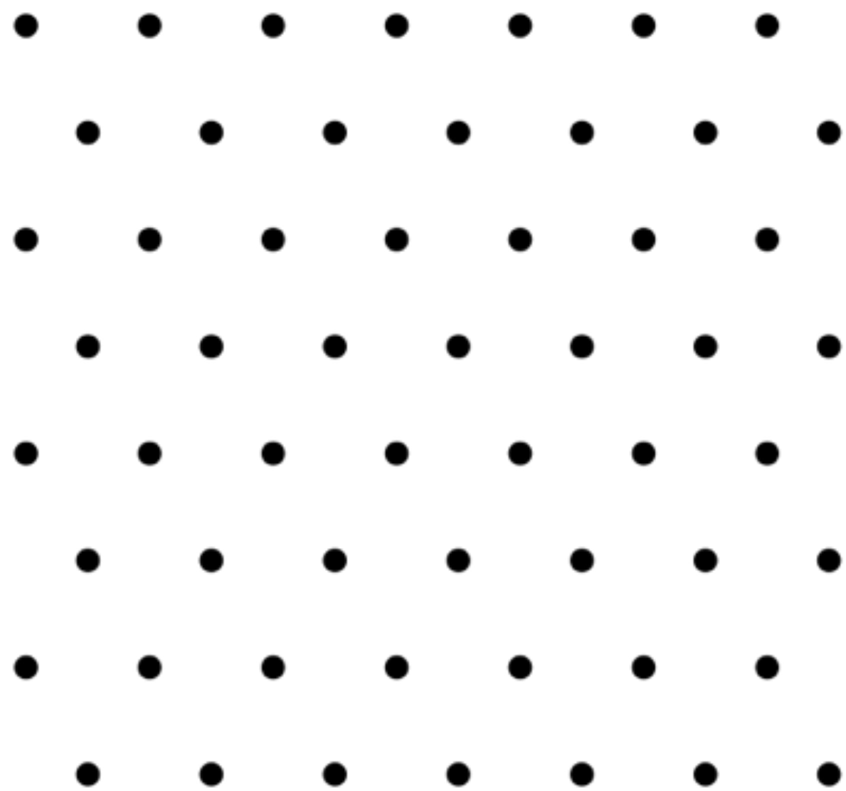
Many more applications that bilinear maps:

- n+1 party non-interactive key exchange
- Obfuscation
- …

Unfortunately, don't know how to construct from elliptic curves

- Recently, constructions based on other math

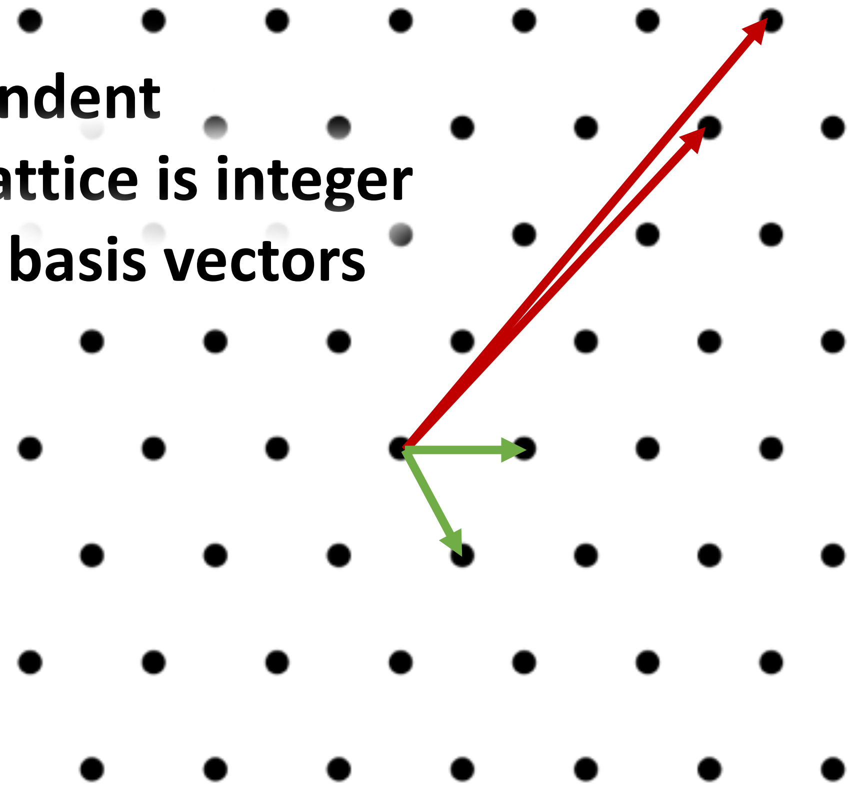
Lattices



Lattices

Basis:

- **Linearly independent**
- **Every point in lattice is integer combination of basis vectors**



Lattices

Hard problems in (high dimensional) lattices:

- Given a basis, find the shortest vector in the lattice
- Given a basis an a point not in the lattice, find the closest lattice point

Can base much crypto on approximation versions of these problems

- Basically everything we've seen in COS433, then some

Fully Homomorphic Encryption

Additively/multiplicatively homomorphic encryption:

Basic ElGamal:

$$\mathbf{Enc(pk, x)} \otimes \mathbf{Enc(pk, y)} = \mathbf{Enc(pk, x{\times}y)}$$

ElGamal where plaintext put in exponent:

$$\mathbf{Enc(pk, x)} \oplus \mathbf{Enc(pk, y)} = \mathbf{Enc(pk, x+y)}$$

What if you could do both simultaneously?

- Arbitrary computations on encrypted data
- Known from lattices

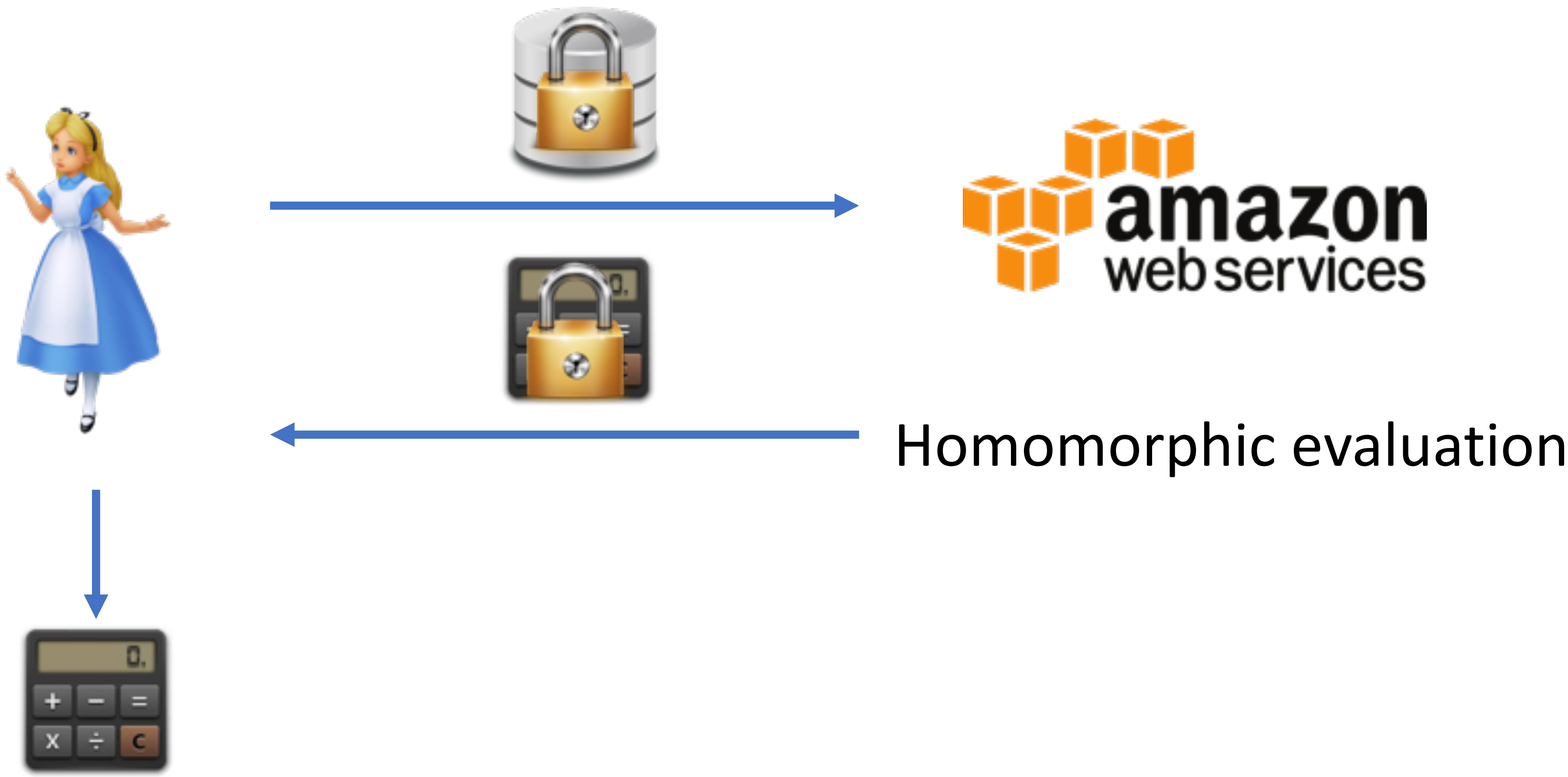
Delegation

Doesn’t want Amazon to learn sensitive data

Delegation

Now, Alice wants Amazon to run expensive computation on data

Delegation



Quantum Computing

Computers that take advantage of quantum physics

Turns out, good at solving certain problems
- Dlog in any group ($\mathbb{Z}_p^*$, ECs)
- Factor integers

Also can speed up brute force search:
- Invert functions in time $2^{n/2}$
- Find collisions in time $2^{n/3}$

Quantum Computing

To protect against quantum attacks, must:

- Must increase key size
  - 256 bits for one-way functions
  - 384 bits for collision resistance
- Must not use DDH/Factoring
  - Lattices instead

Quantum computers still at least a few years away, but coming

COS 533 – Advanced Crypto

Plan to teach Spring 2021

Will cover many of these topics

Undergrads welcome

Announcements

HW7 Due SUNDAY

Project 3/HW 8 due May 12^{th}