COS 433/Math 473: Cryptography

Mark Zhandry

Princeton University

Fall 2020

Announcements

HW6 Due today

PR2 Due Dec 5

Final Exam Details

Slightly longer than homework, but slightly shorter questions

Pick any **36 hour** period during the dates **Dec 9 – 14**

- Intended to be a 3 hour exam
- Will send out more comprehensive instructions

Individual, but open notes/slides/internet…

Example exams on course webpage

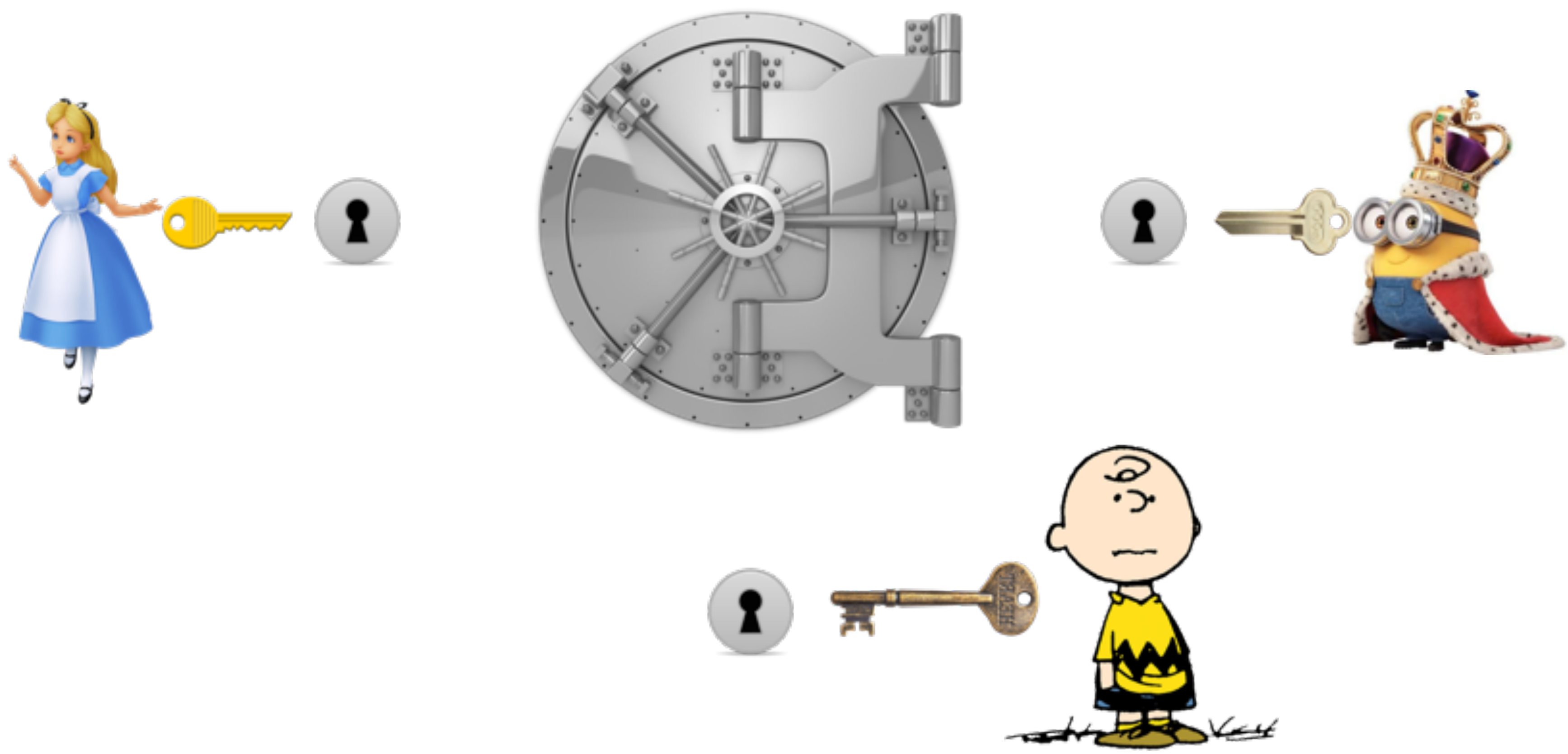
Today

Secret sharing
Beyond COS 433

Secret Sharing

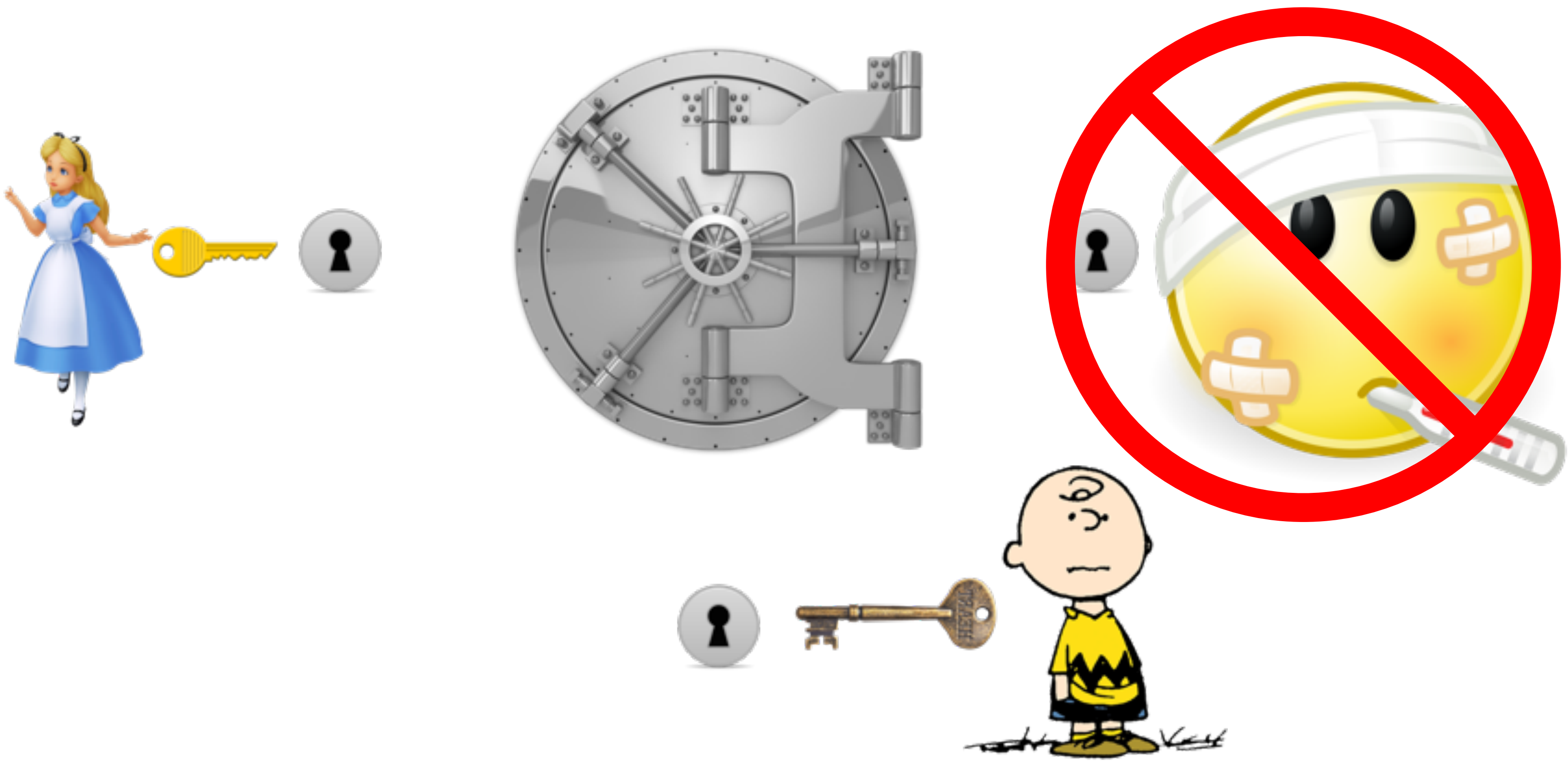
Vault should only open if both Alice and Bob are present

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

Beyond Thresholds

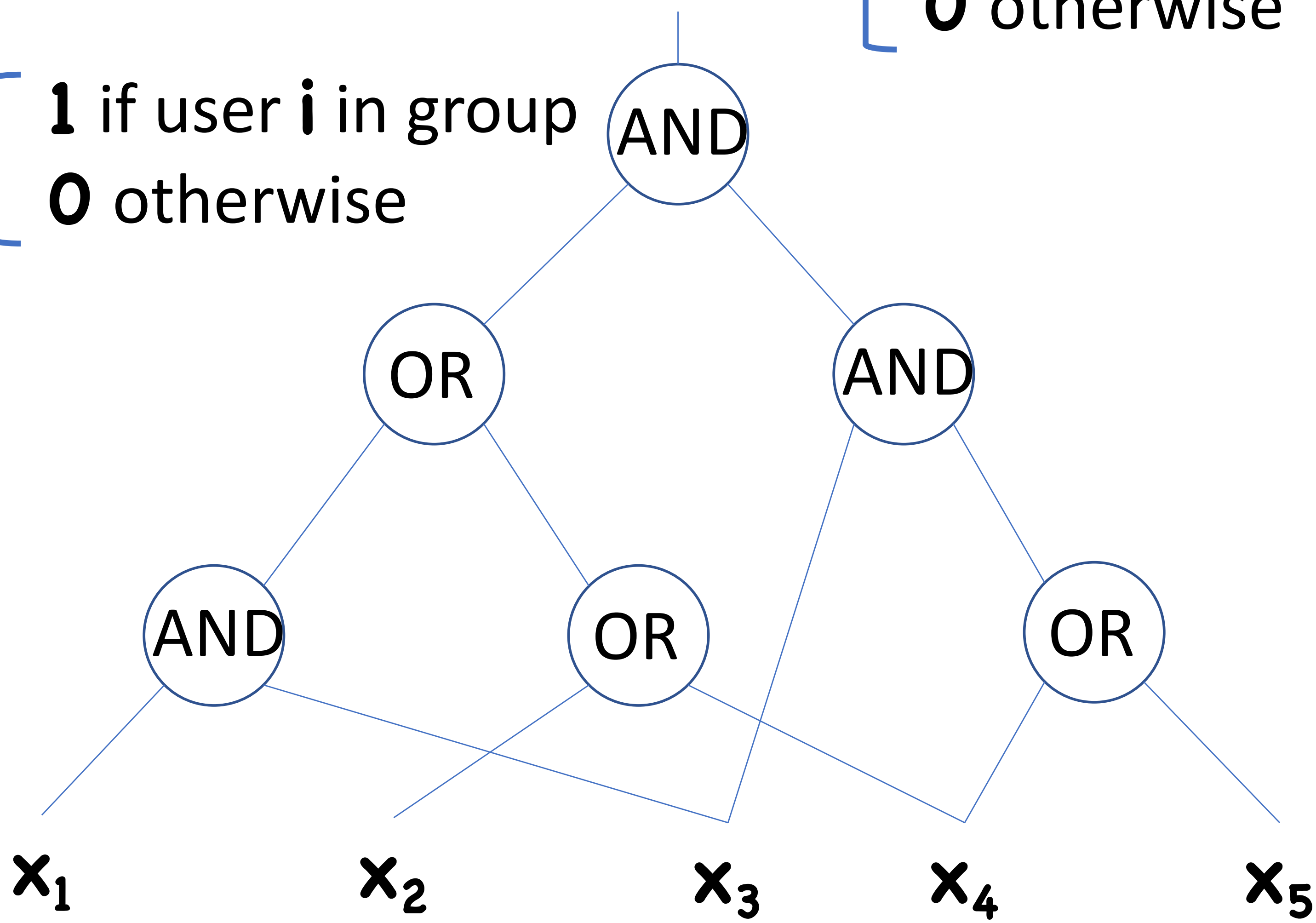
Can do secret sharing for a variety of access structures

- Any monotone formula
- Assuming secret key encryption, any monotone circuit

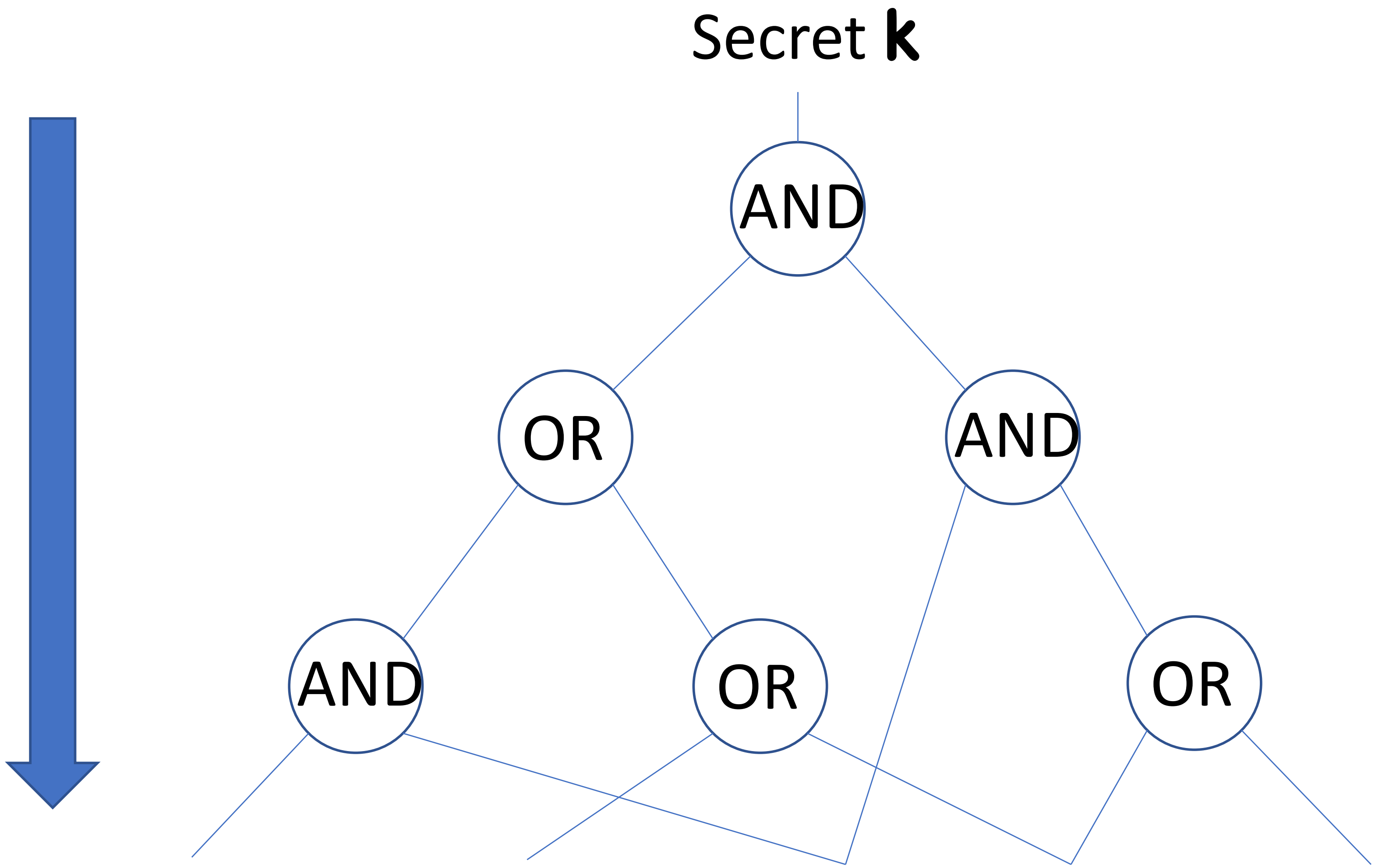
Secret Sharing for Formula

$$\mathbf{out} = \begin{cases} \mathbf{1} & \text{if group authorized} \\ \mathbf{0} & \text{otherwise} \end{cases}$$

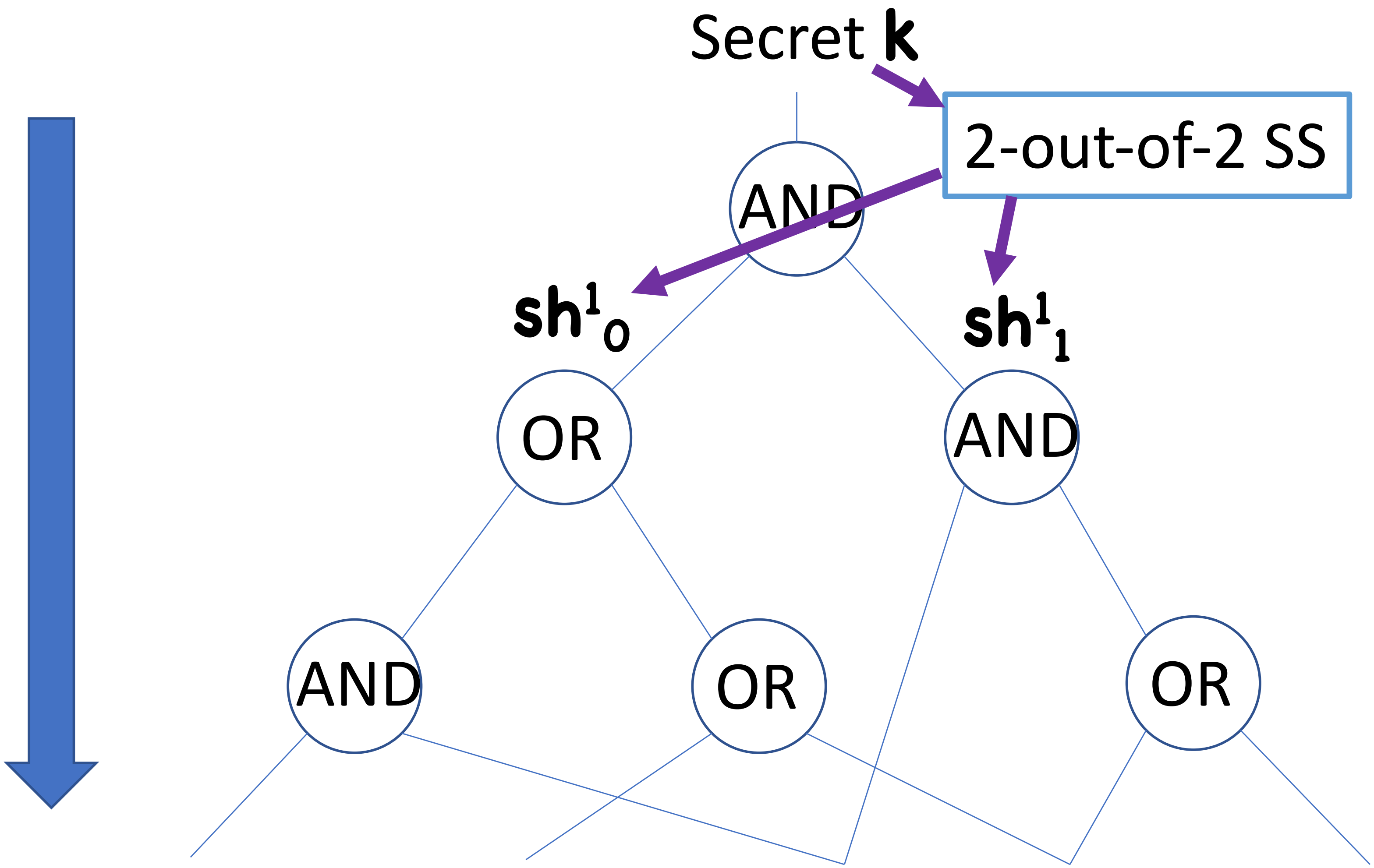
$$x_i = \begin{cases} \mathbf{1} & \text{if user } \mathbf{i} \text{ in group} \\ \mathbf{0} & \text{otherwise} \end{cases}$$



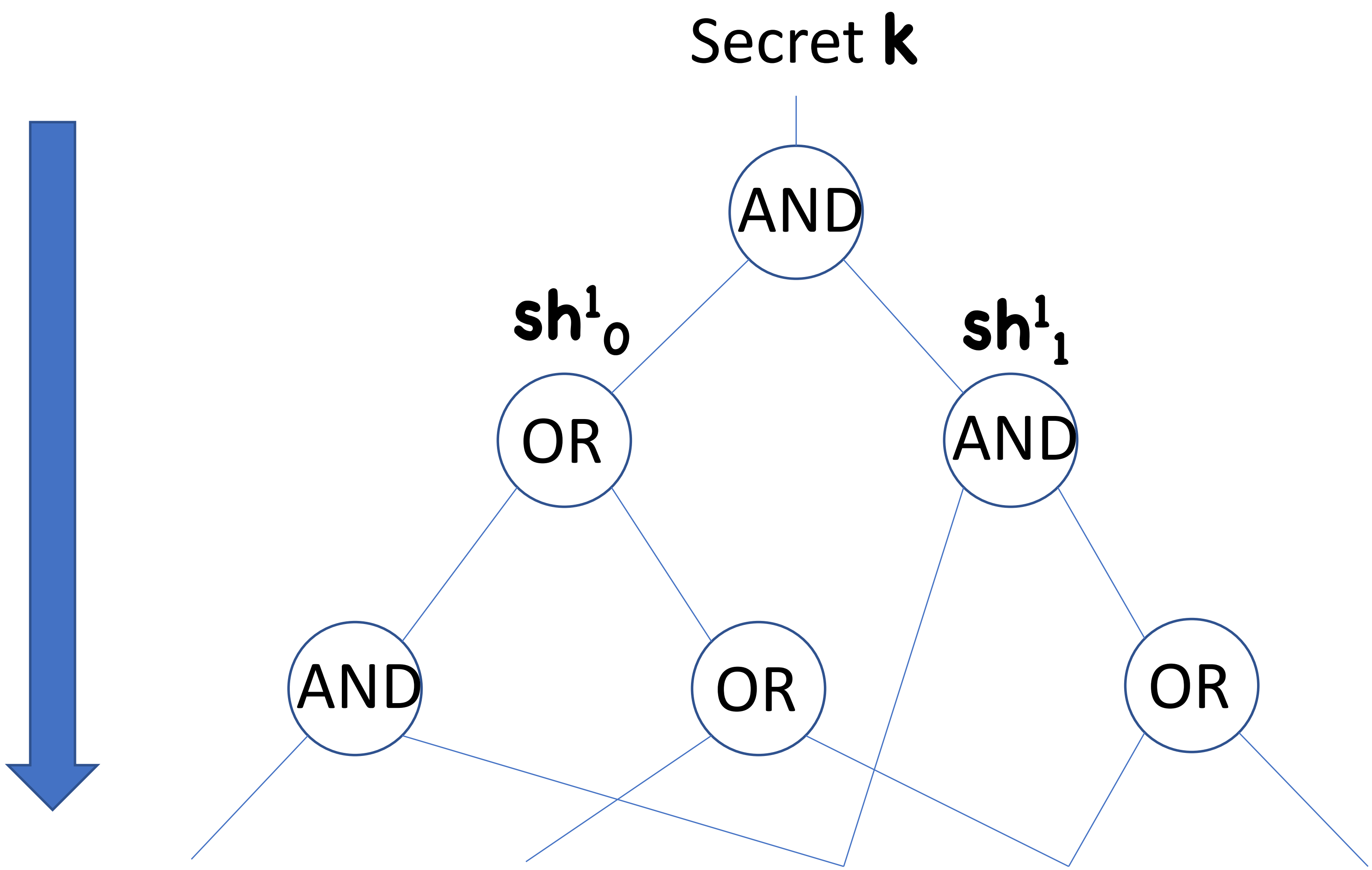
Secret Sharing for Formula



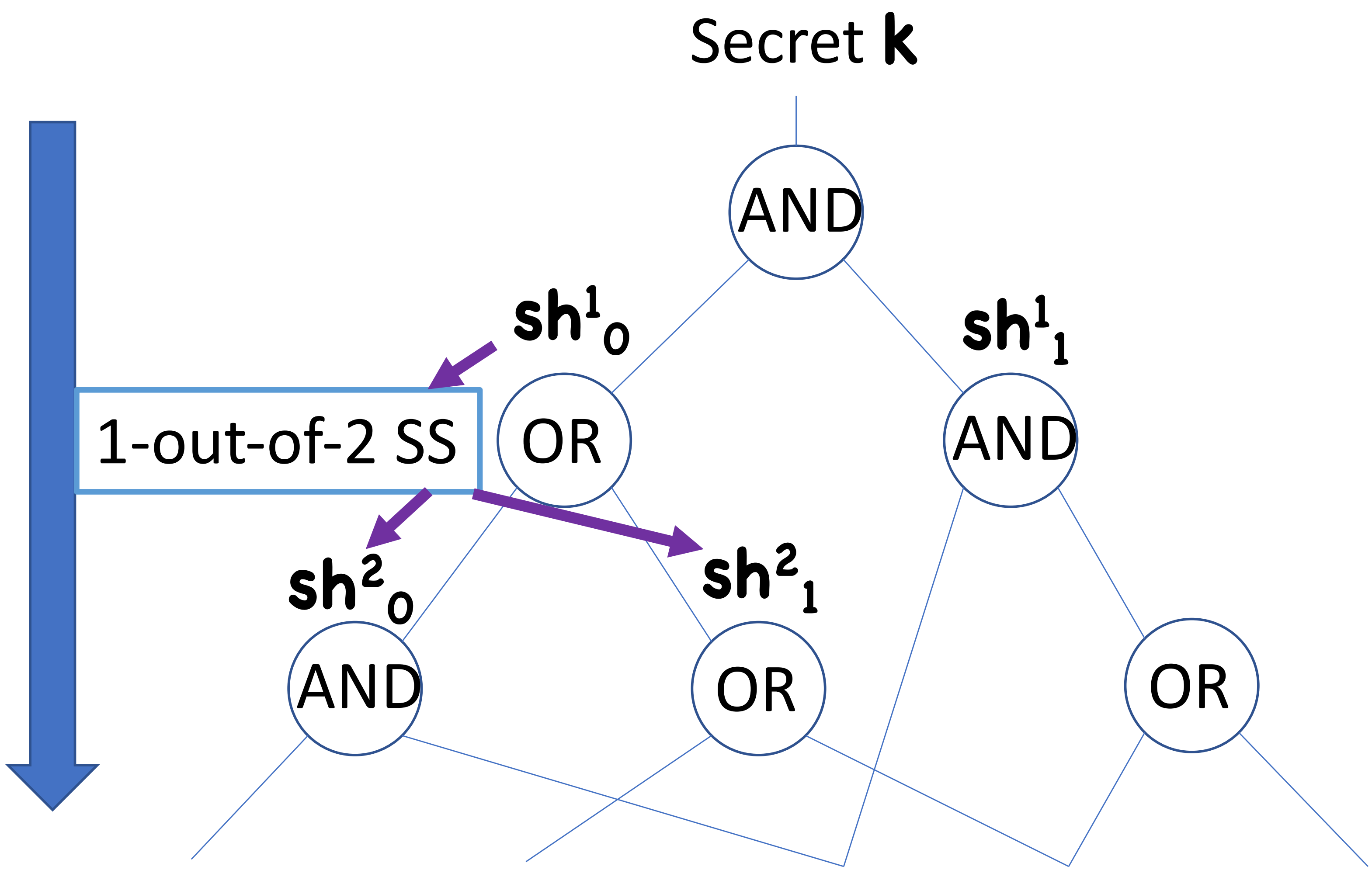
Secret Sharing for Formula



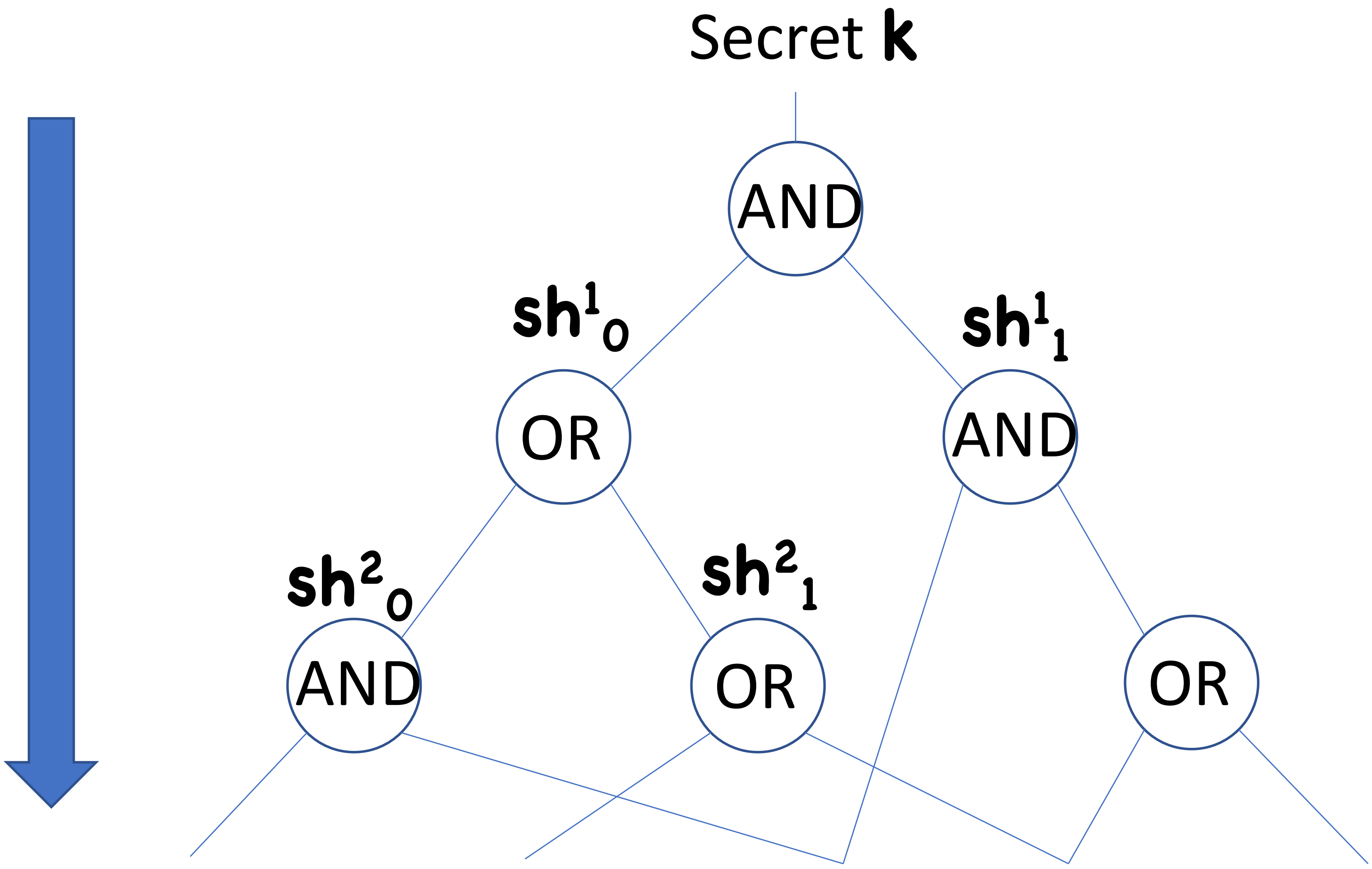
Secret Sharing for Formula



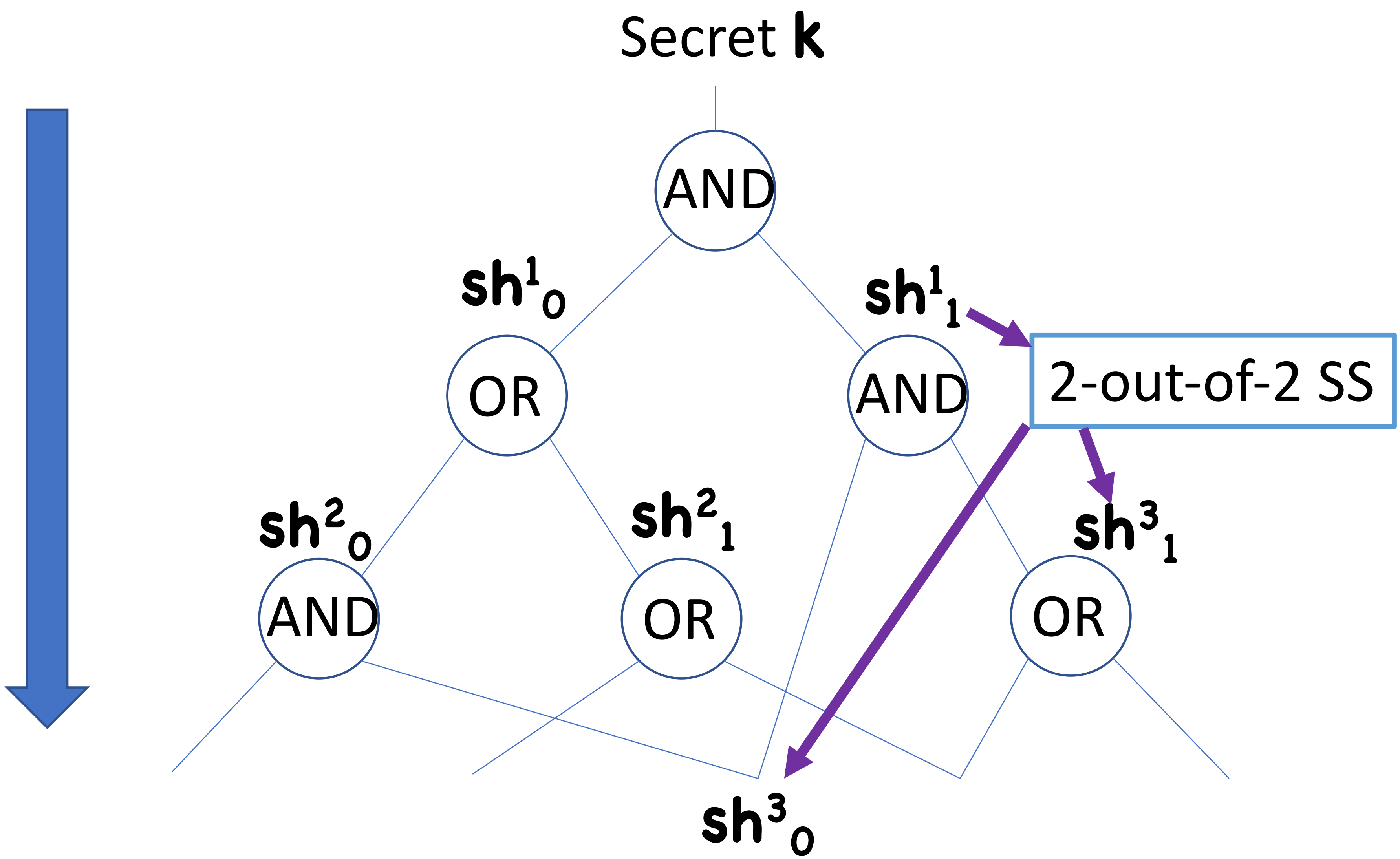
Secret Sharing for Formula



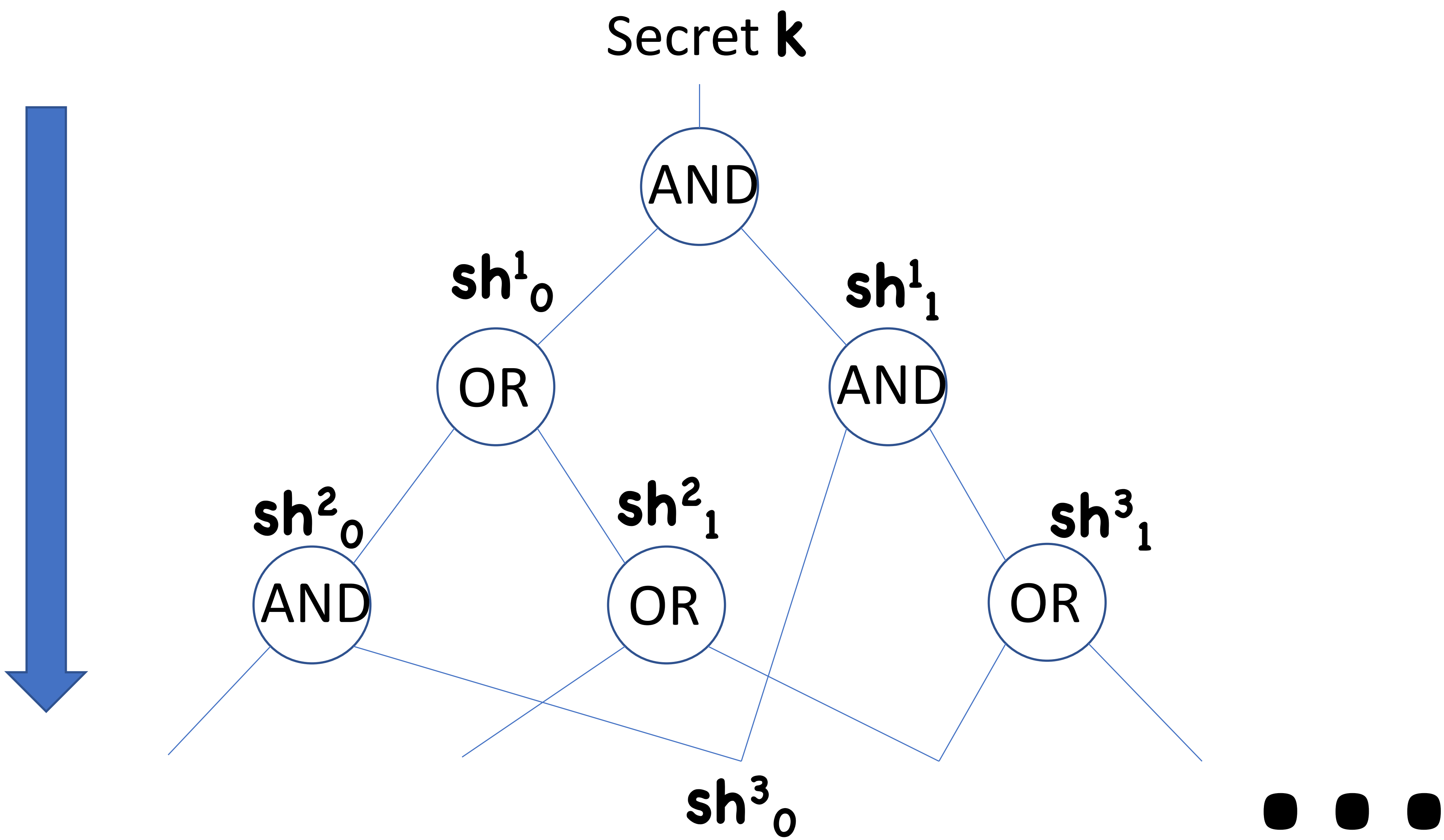
Secret Sharing for Formula



Secret Sharing for Formula

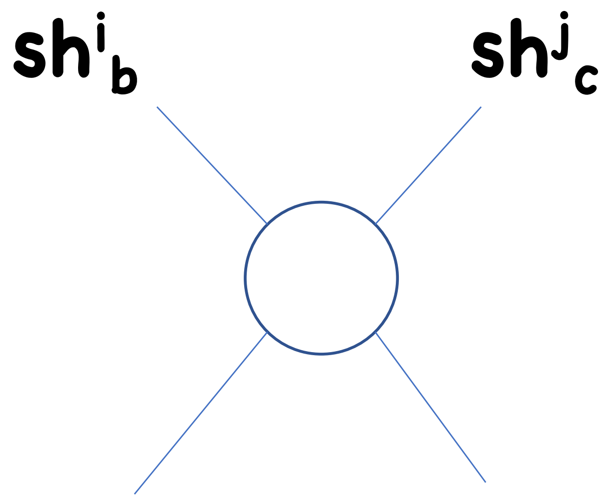


Secret Sharing for Formula



Secret Sharing for Circuits

Obstacle: fan-out

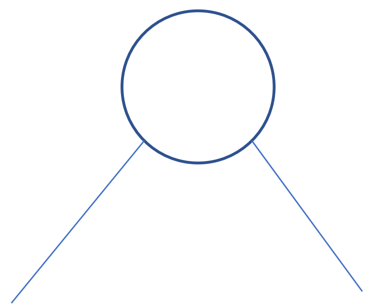


Must secret share $(\mathbf{sh}^i_b, \mathbf{sh}^j_c)$

Problem: share sizes grow exponentially with depth

Solution: Encrypt shares

- Choose new key $\mathbf{k^r}$ for each node $\mathbf{r}$
- Release $\mathbf{Enc(k^r\ ,\ (sh^i_b,\ sh^j_c)\ )}$ to everyone

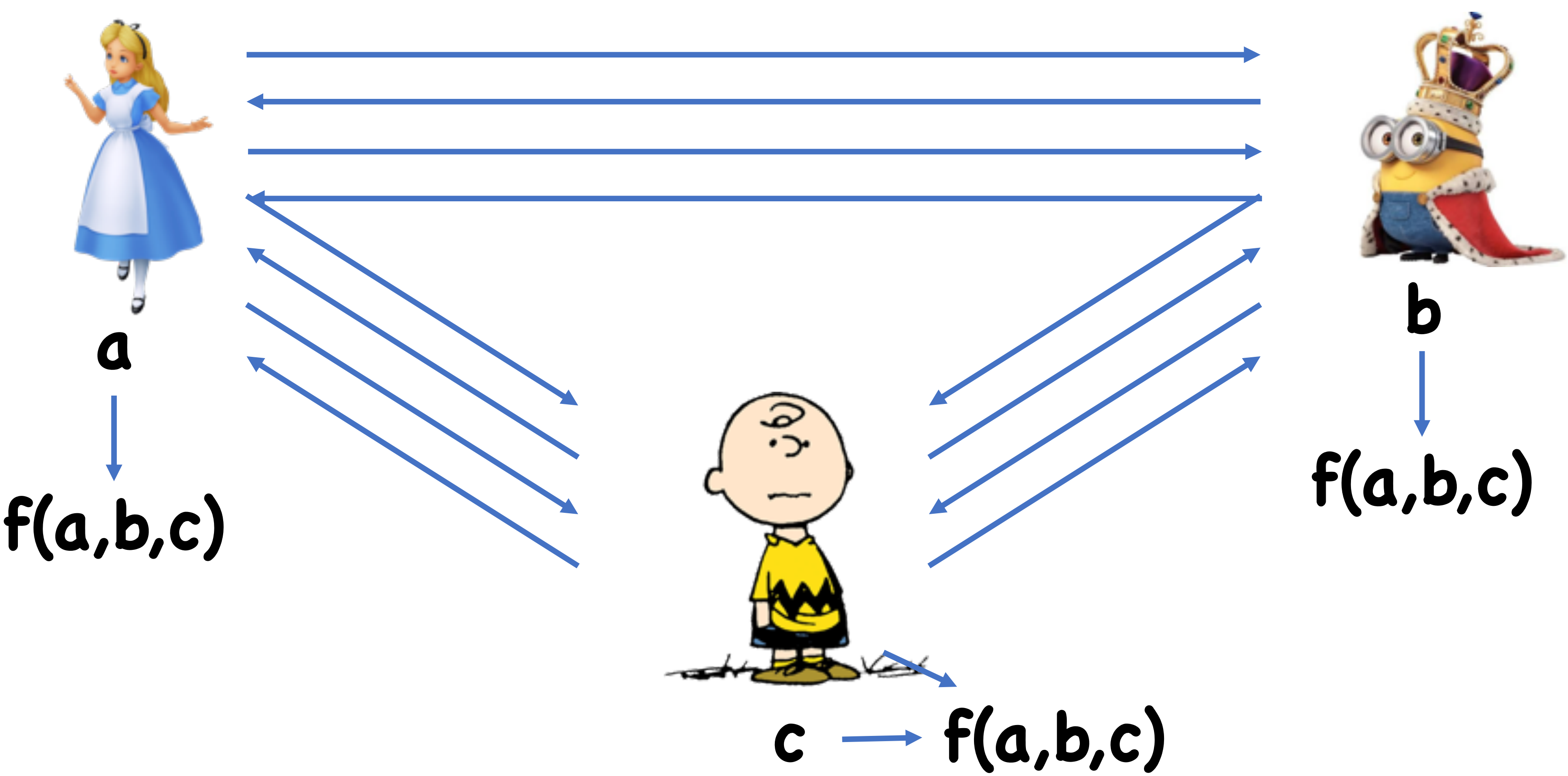


Secret share $\mathbf{k^r}$ to children

Using computationally secure (secret key) encryption, $\mathbf{k^r}$ stays independent of depth

Beyond COS 433

Multiparty Computation



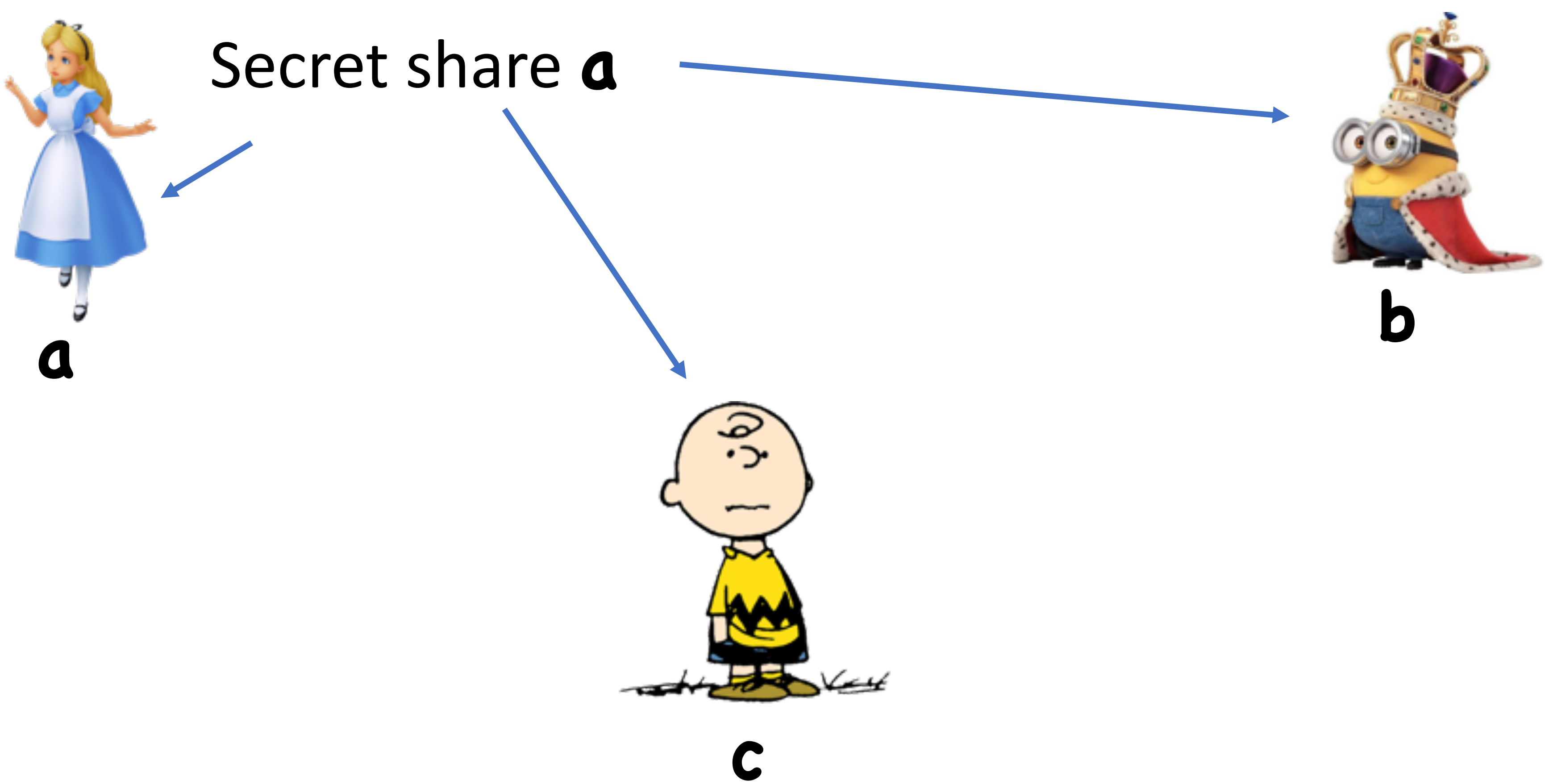
Multiparty Computation

Observation 1: $\mathbf{t}$-out-of-$\mathbf{n}$ secret sharing is additively homomorphic:

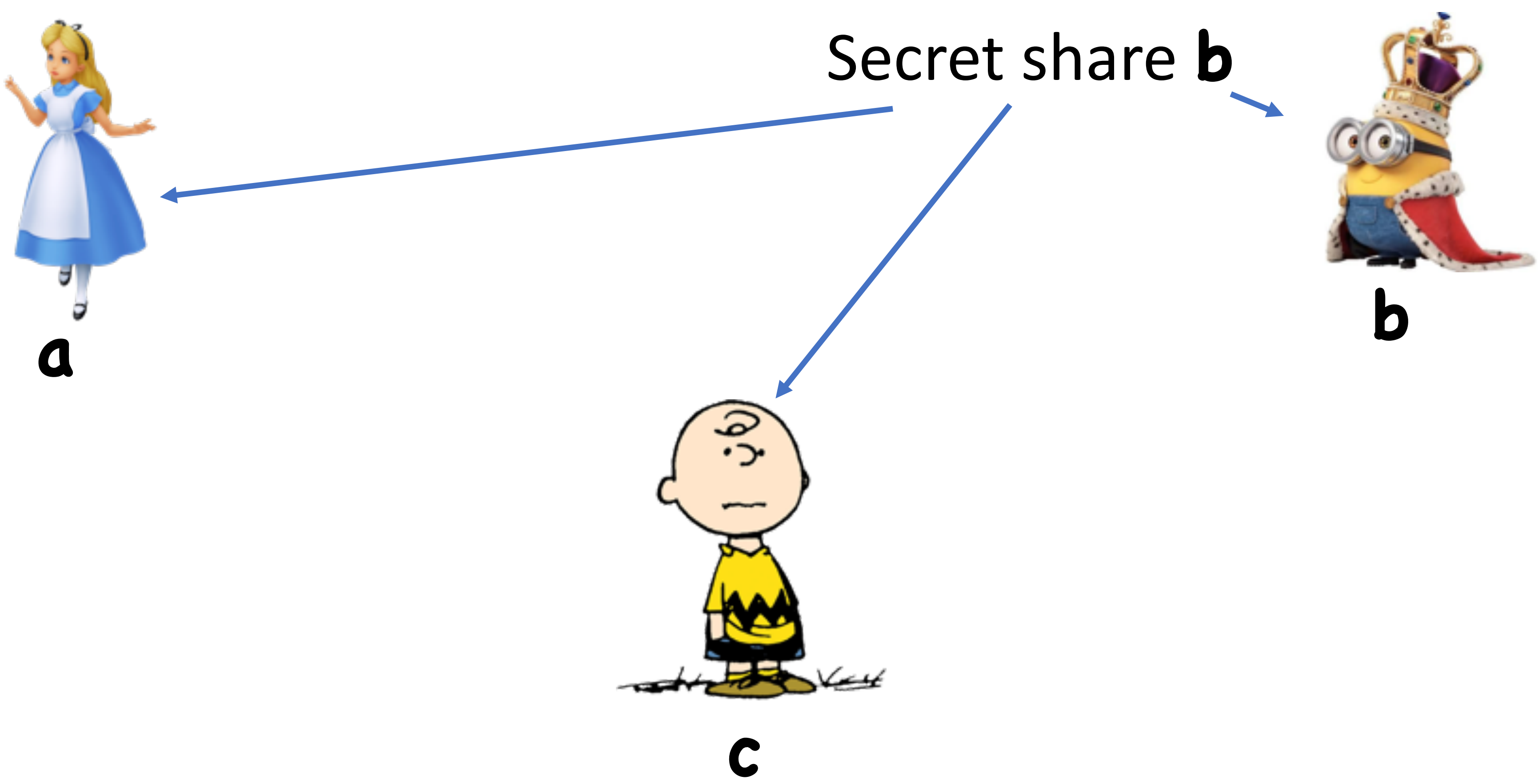
Given shares $\mathbf{sh_1}$ of $\mathbf{x_1}$ and $\mathbf{sh_2}$ of $\mathbf{x_2}$, $\mathbf{r\times sh_1+s\times sh_2}$ is a share of $\mathbf{r\times x_1+s\times x_2}$

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

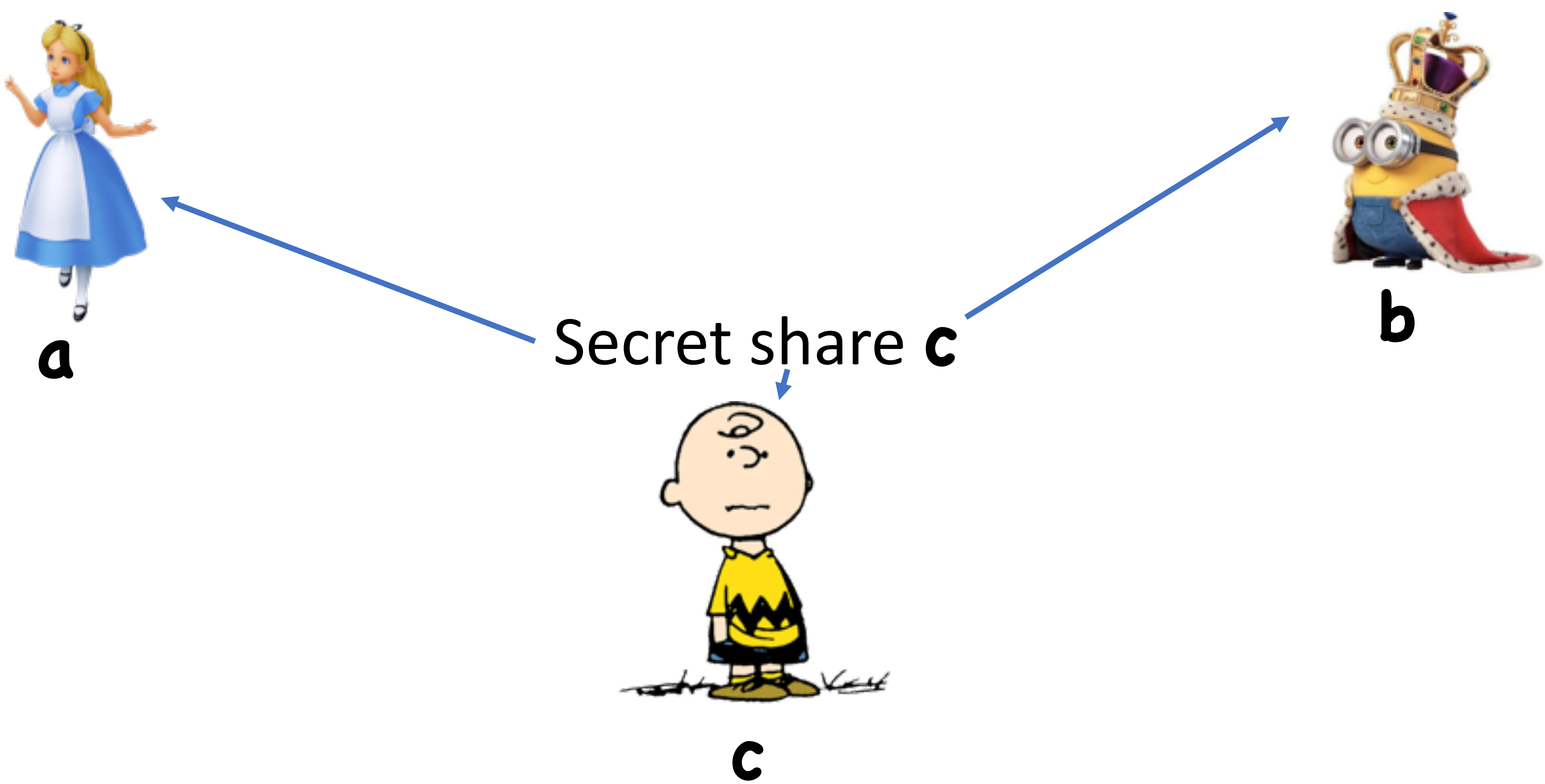
MPC for linear $\mathbf{f}$



MPC for linear **f**



MPC for linear **f**



MPC for linear **f**

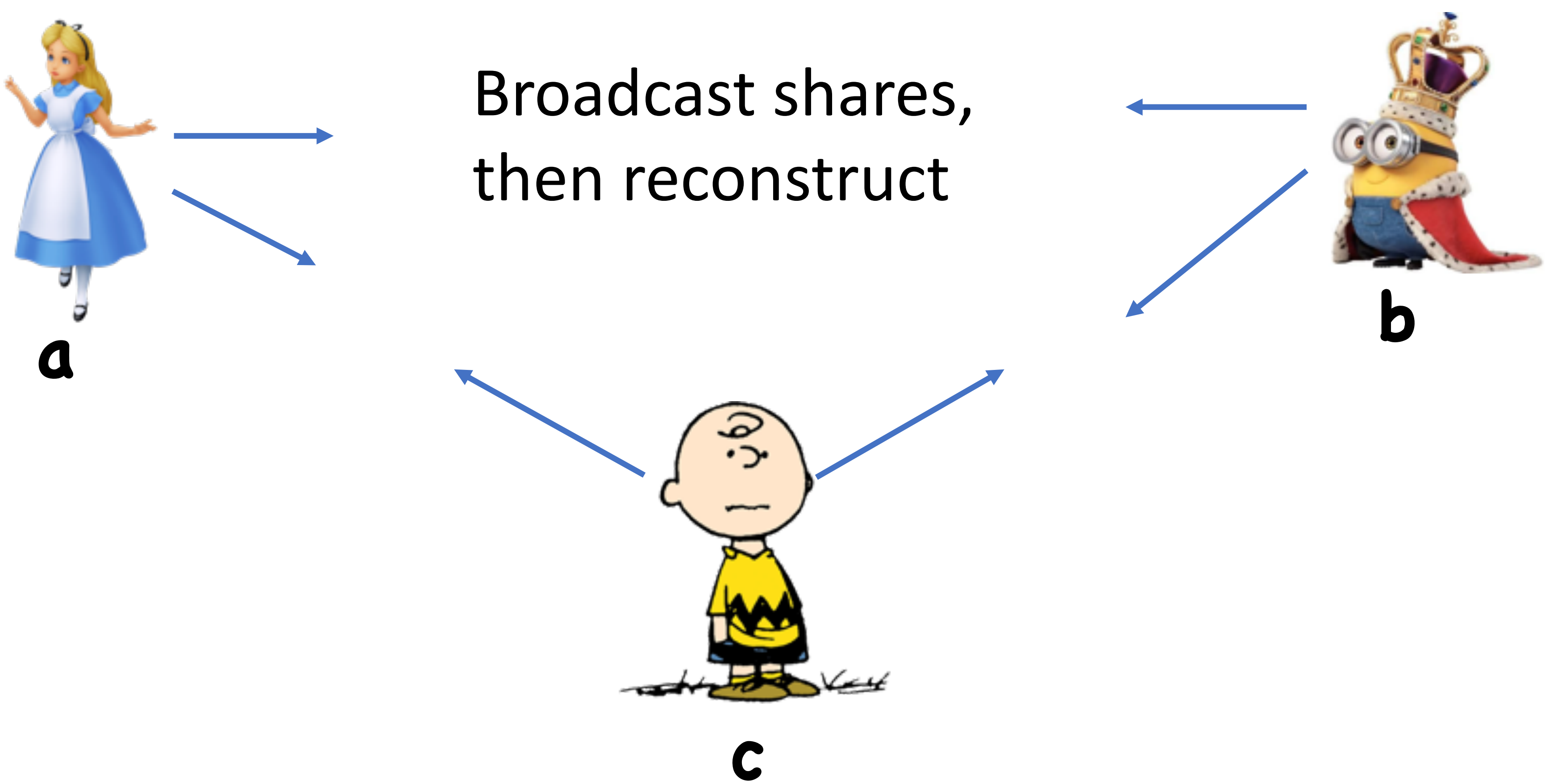
a

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

b

c

MPC for linear **f**



MPC for General f

Observation 2: t-out-of-n Secret Sharing is sort of multiplicatively homomorphic

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

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

Idea: can do multiplications locally, and then some additional interaction to get degree back to d

MPC for General f

To maintain correctness, need threshold to stay at most n

- But multiplying doubles threshold, so need $t \leq n/2$
- Thus 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 $n-1$

MPC for Malicious Adversaries

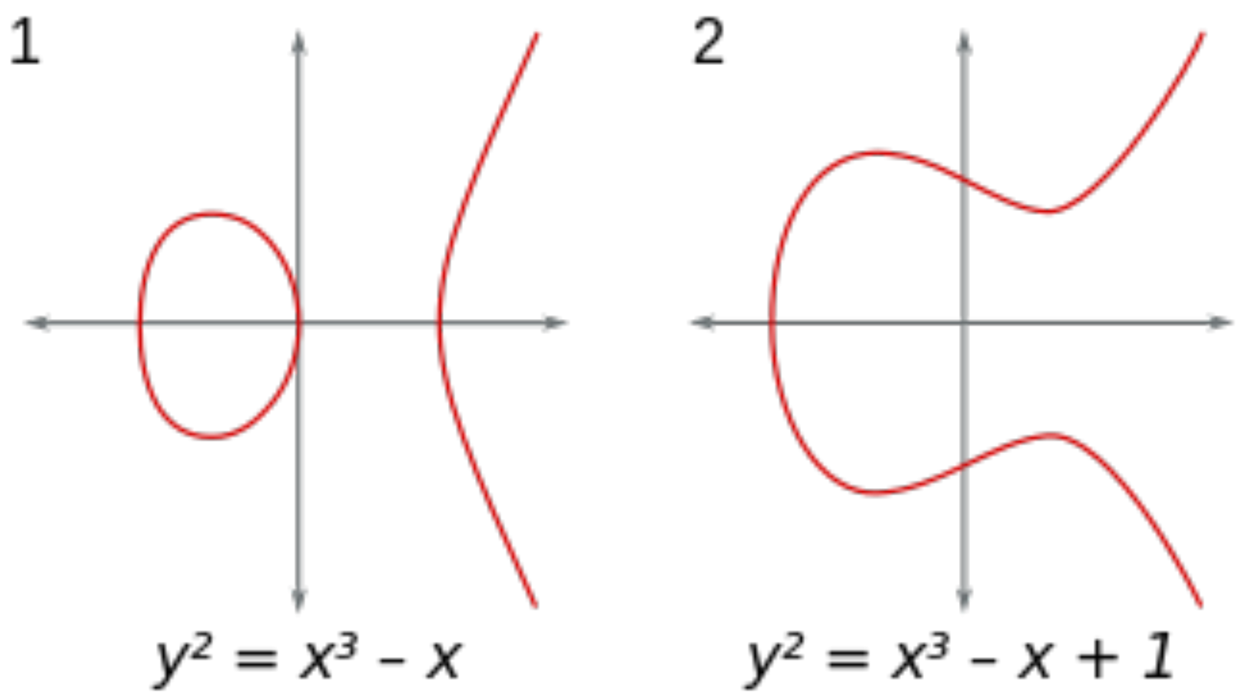
So far, everything assumes players act honestly, and just want to learn each other's inputs

But what if honest players deviate from protocol?

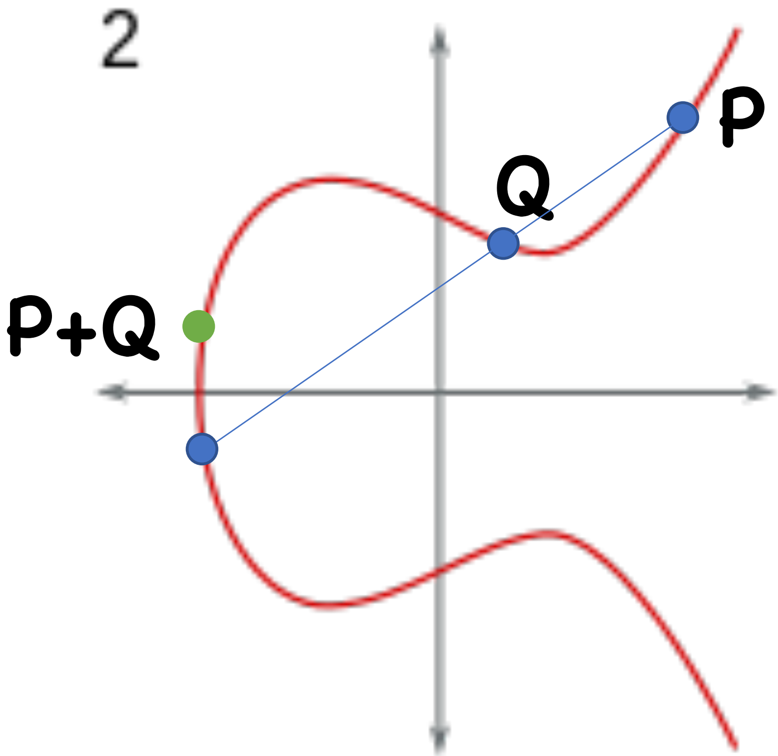
Idea: use ZK proofs to prove that you followed protocol without revealing your inputs

Elliptic Curves

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



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

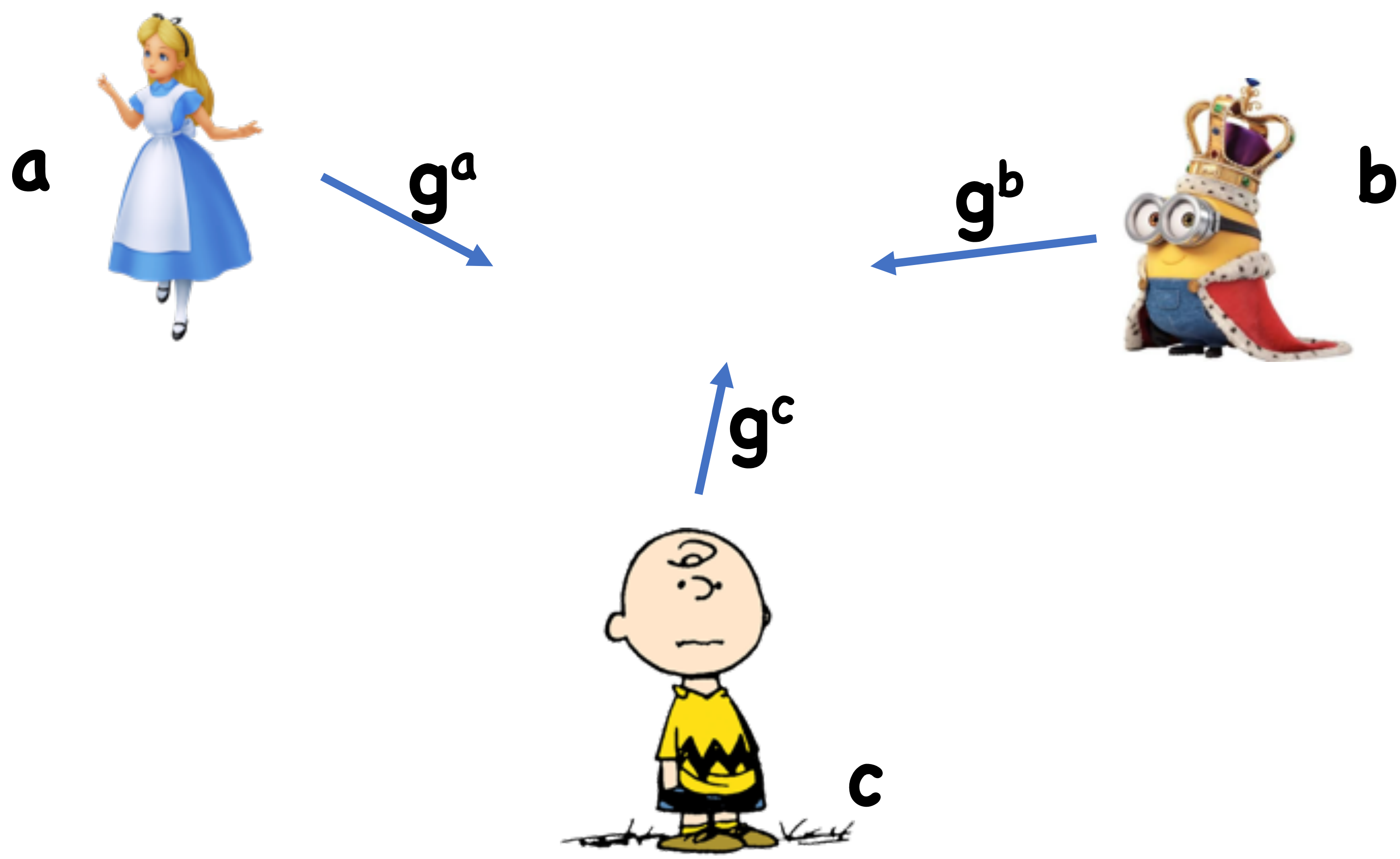
Bilinear Maps

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

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

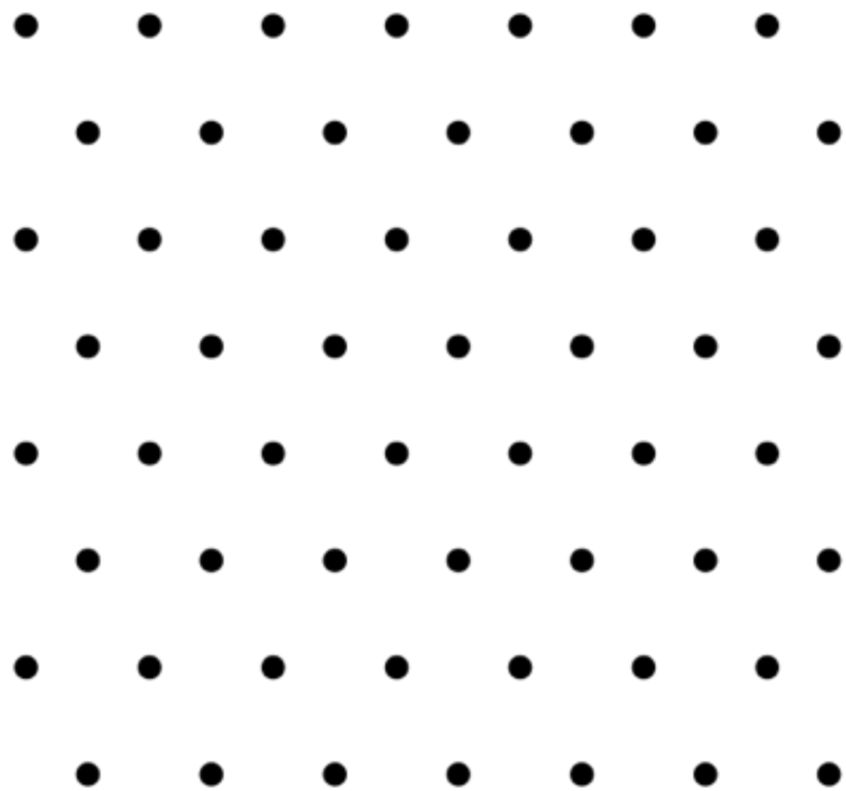
Many more applications than bilinear maps:

- $\mathbf{n+1}$ party non-interactive key exchange
- Obfuscation
- …

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

- Recently, constructions based on other math

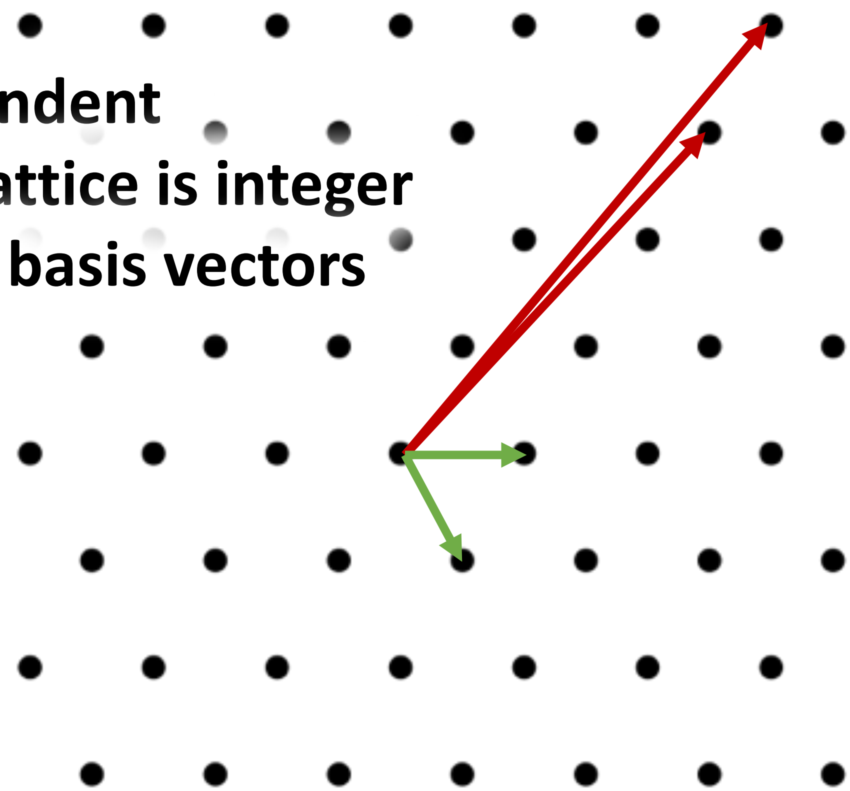
Lattices



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

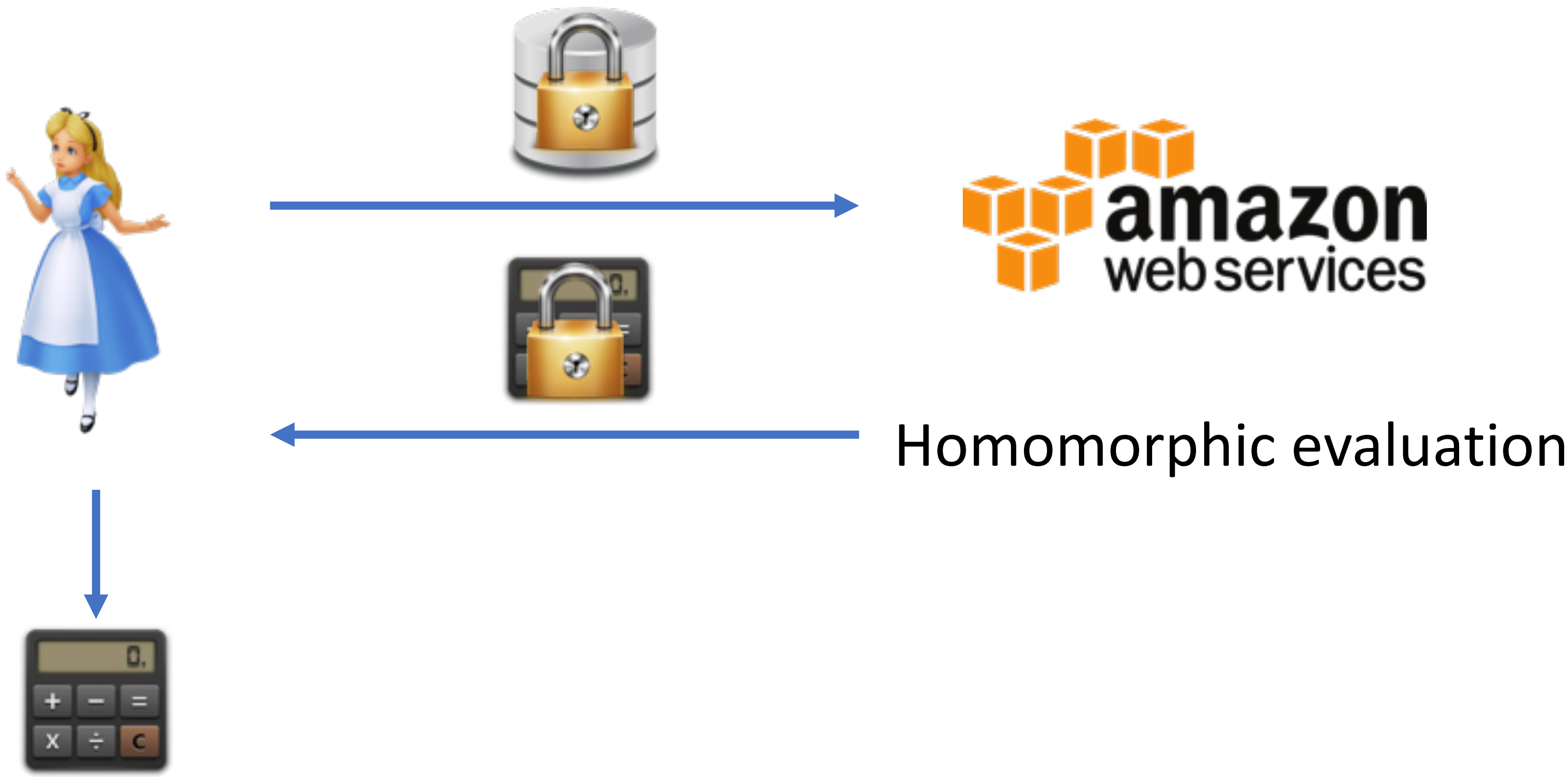
Delegation

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 (or something else) instead

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

COS 533 (Spring 2021)

Advanced crypto

Will cover many of these topics

- Various math tools used for crypto
- Advanced cryptosystems
- More theory
- Some cryptanalysis

Undergrads welcome