DTTF/NB479: Dszquphsbqiz Day 31

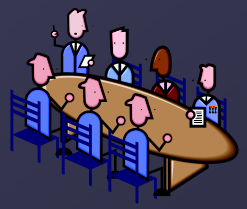
- Announcements:
  - SHA due Tuesday
  - Last exam Thursday
  - Available for project questions this week
  - You will evaluate each other's presentations during 10th week.
- Questions?

- Secret sharing

What is *secret splitting*?

- I have a secret M I want to share
- To figure it out, you'll need **teamwork**.

- Simple: use a sum
  - Pick large n > M
  - Pick a random r, 0≤ r ≤ n-1
  - To share between two people:
    - Alice r, M-r (mod n)
    - They can work together to sum
  - Generalize to k people:
    - r_1, r_2, …r_{k-1}, and $M - \sum_1^{k-1} r_i$ (all mod n)



There are many applications of secret splitting and secret sharing

1. Inheritances
2. Military
3. Government
4. Information security

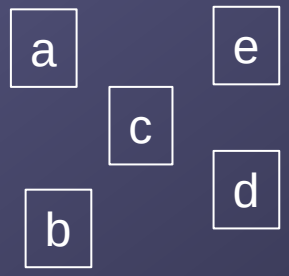
What if I wanted a **subset** of the people to be able to reconstruct the secret?

Secret splitting is trivial

Secret *sharing* is not!

(t,w)-threshold schemes require *t* people from a set of *w* to compute the secret

- Knowing t or more pieces makes M easily computable
- t–1 or fewer pieces leaves M **completely undetermined**
- If (3,5) threshold scheme:
  - {a,d,e} can figure out secret
  - {c,e} cannot
  - {a,b,c,d} is redundant

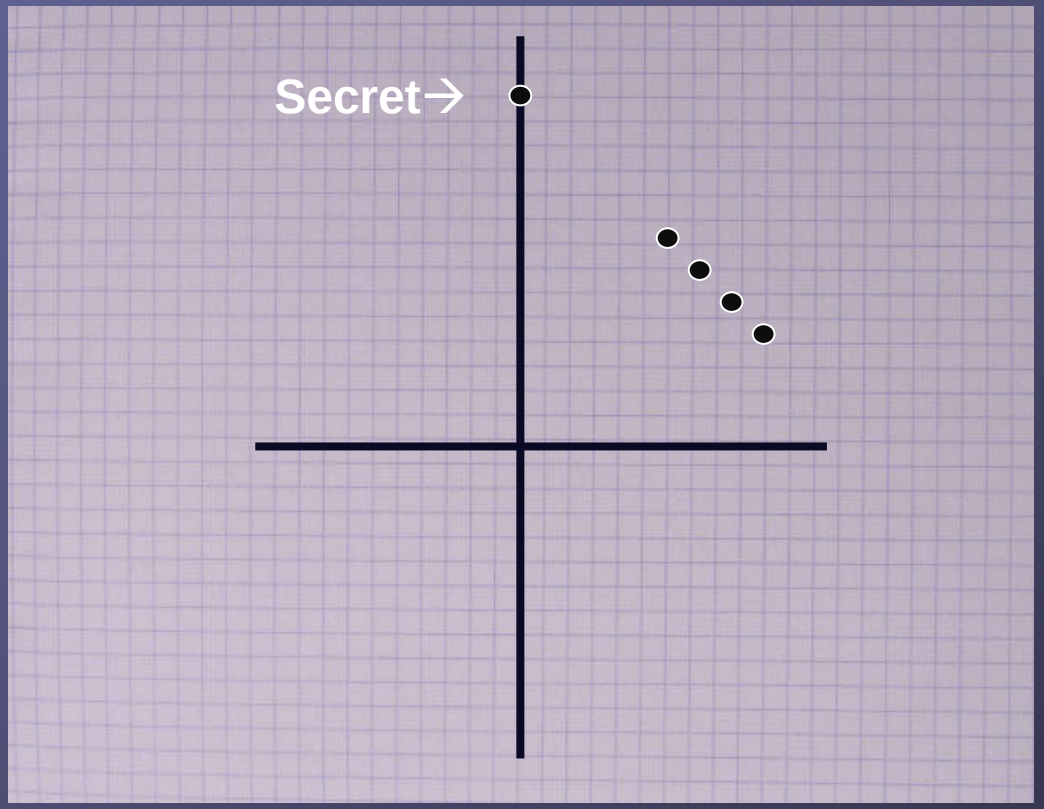


- Secret splitting (all participants required) is just a special case:
  - Let t = w

Idea: we can use curve fitting to reconstruct a function, and thus a message

The y-intercept of the line encodes the secret!

Here is a (2,4) scheme:

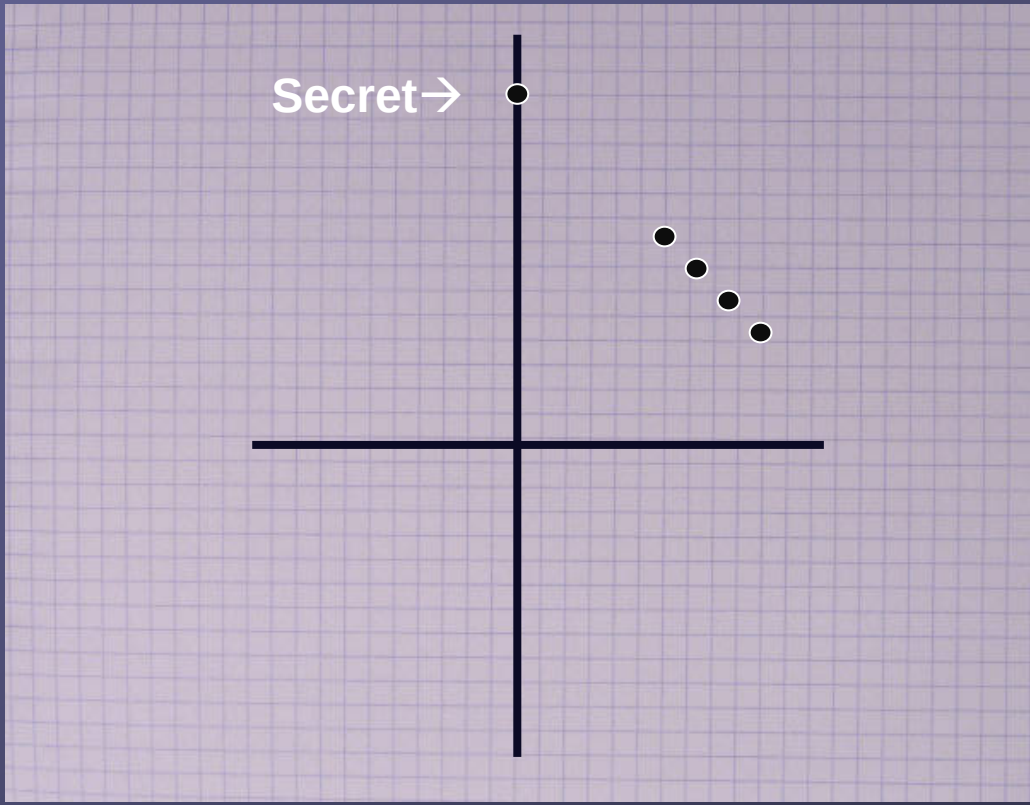


Your quiz question is an example of a (2,3) scheme

The Shamir threshold scheme uses curve-fitting with higher dimensions

The y-intercept of the line encodes the secret!

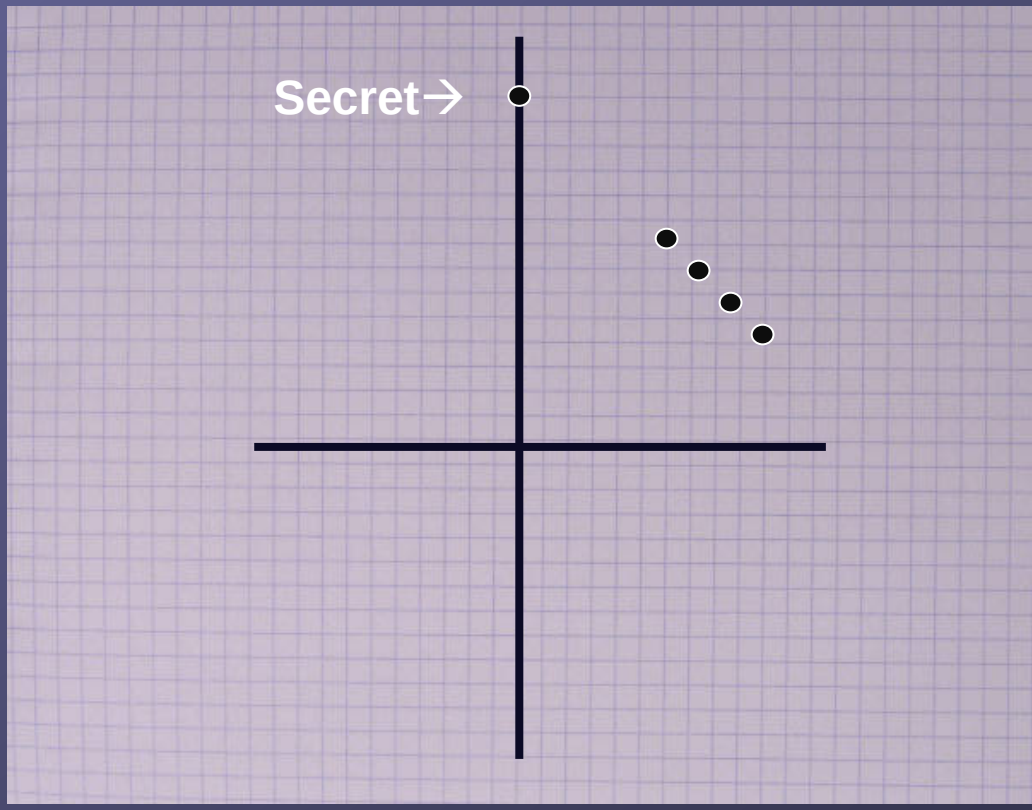
Derivation on board



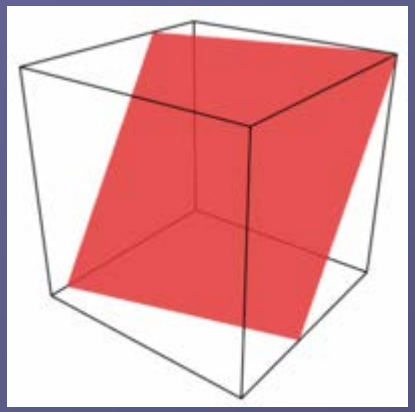
Extensions to Shamir

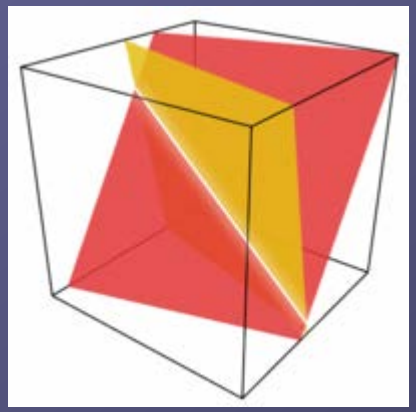
Multiple shares

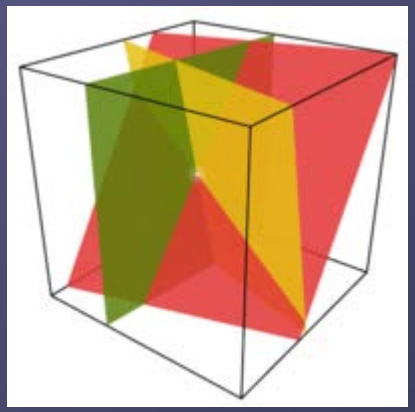
Multiple groups of people



In the Blakely scheme, we represent the secret as the y-coordinate of the intersection of hyperplanes



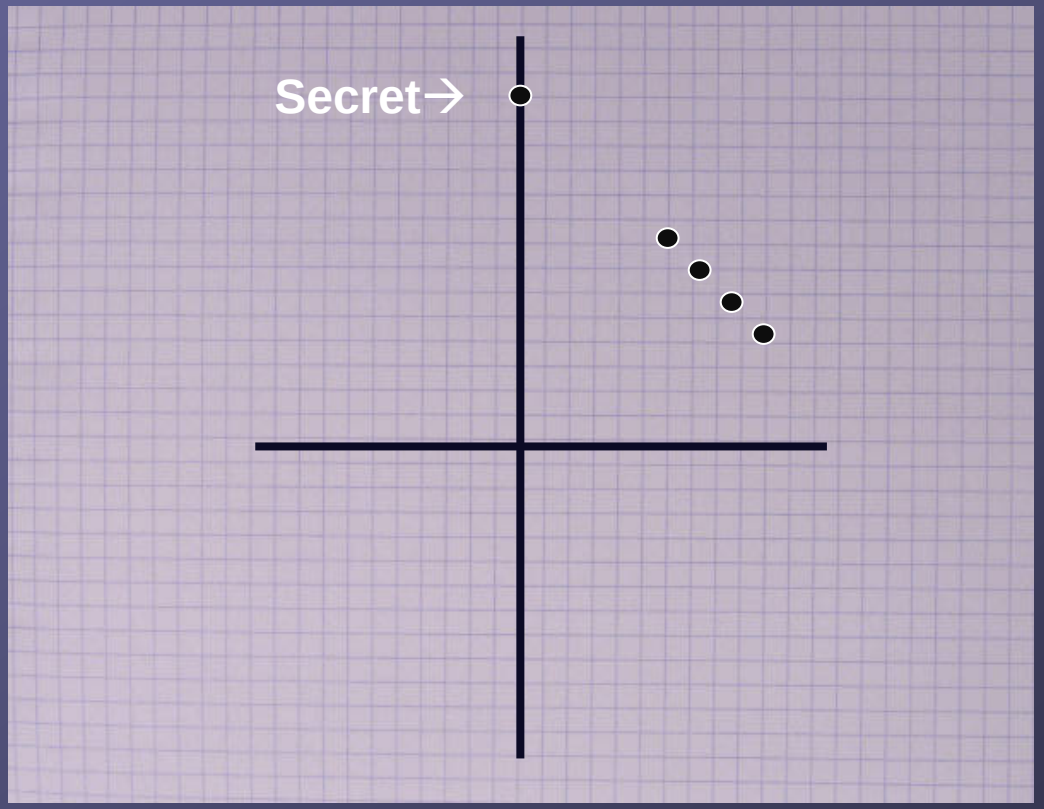




http://en.wikipedia.org/wiki/Secret_sharing

Back to Shamir

The y-intercept of the line encodes the secret!



Your quiz question is an example of a (4, 6) scheme

Project workday tomorrow: quiz due at 2:00 pm.