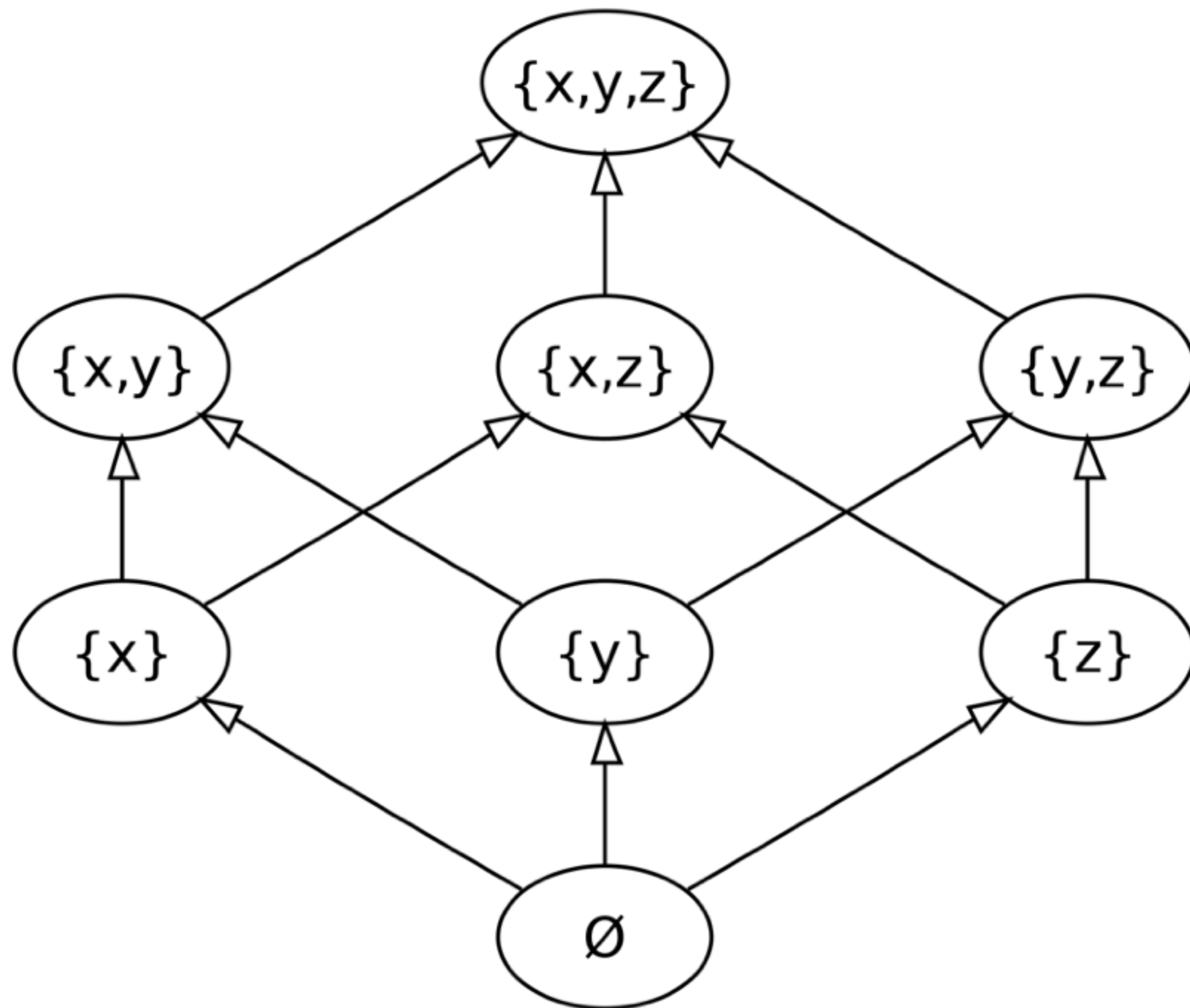


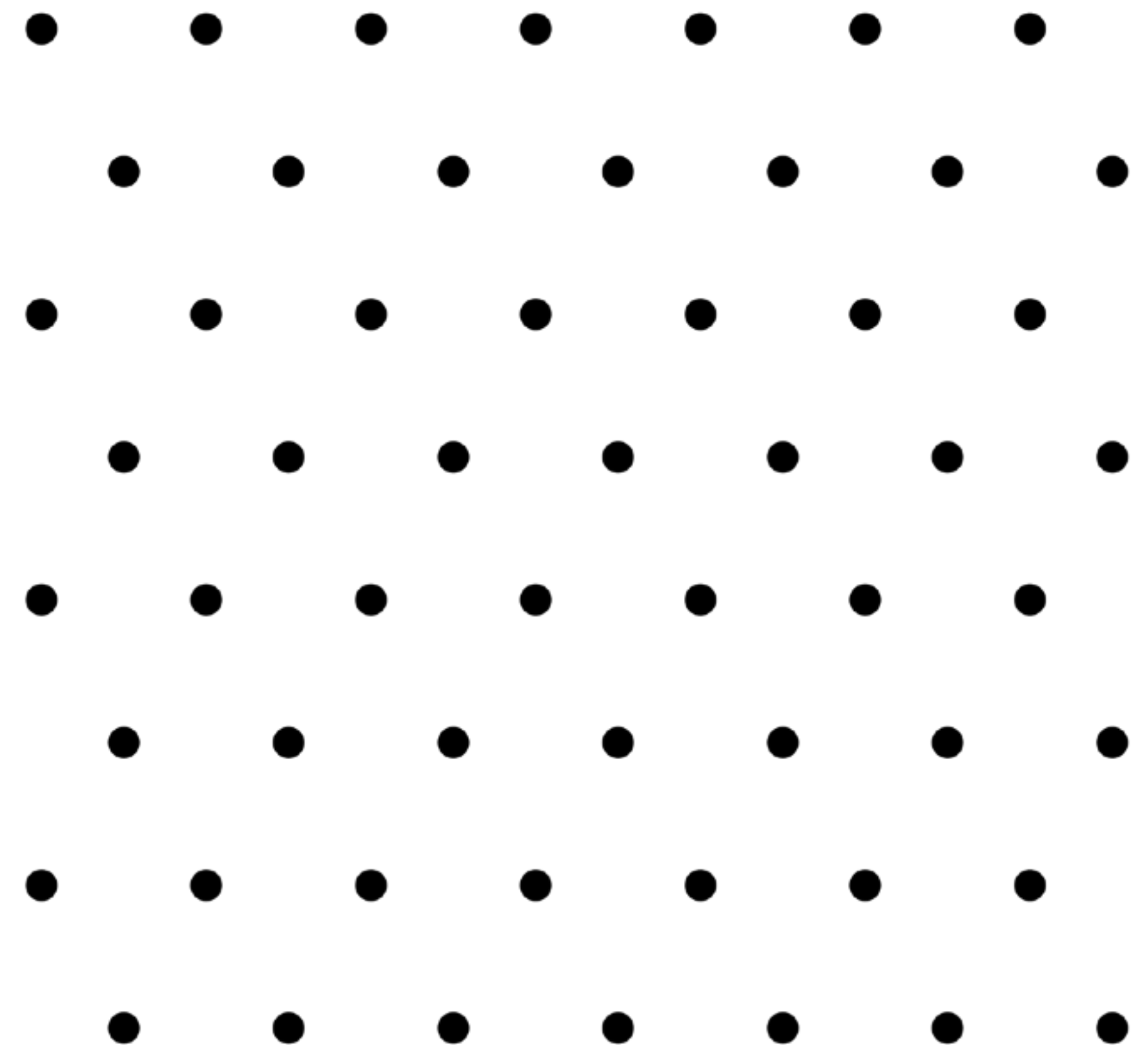
# Lattice?

Treillis ❌



[https://en.wikipedia.org/wiki/Lattice\\_\(order\)](https://en.wikipedia.org/wiki/Lattice_(order))

Réseaux ✅



[https://en.wikipedia.org/wiki/Lattice\\_\(group\)](https://en.wikipedia.org/wiki/Lattice_(group))

# Agenda

## Plan de l'exposé

- Cryptographie moderne et ses problèmes:
  - Chiffrement asymétrique (RSA)
  - Échange de clé (DH)
- Piste de solution: les réseaux Euclidiens
  - Problème du vecteur le plus court (SVP)
  - Algorithme d'approximation efficace (LLL)
- Exemple d'application: le problème d'apprentissage avec erreurs (LWE)