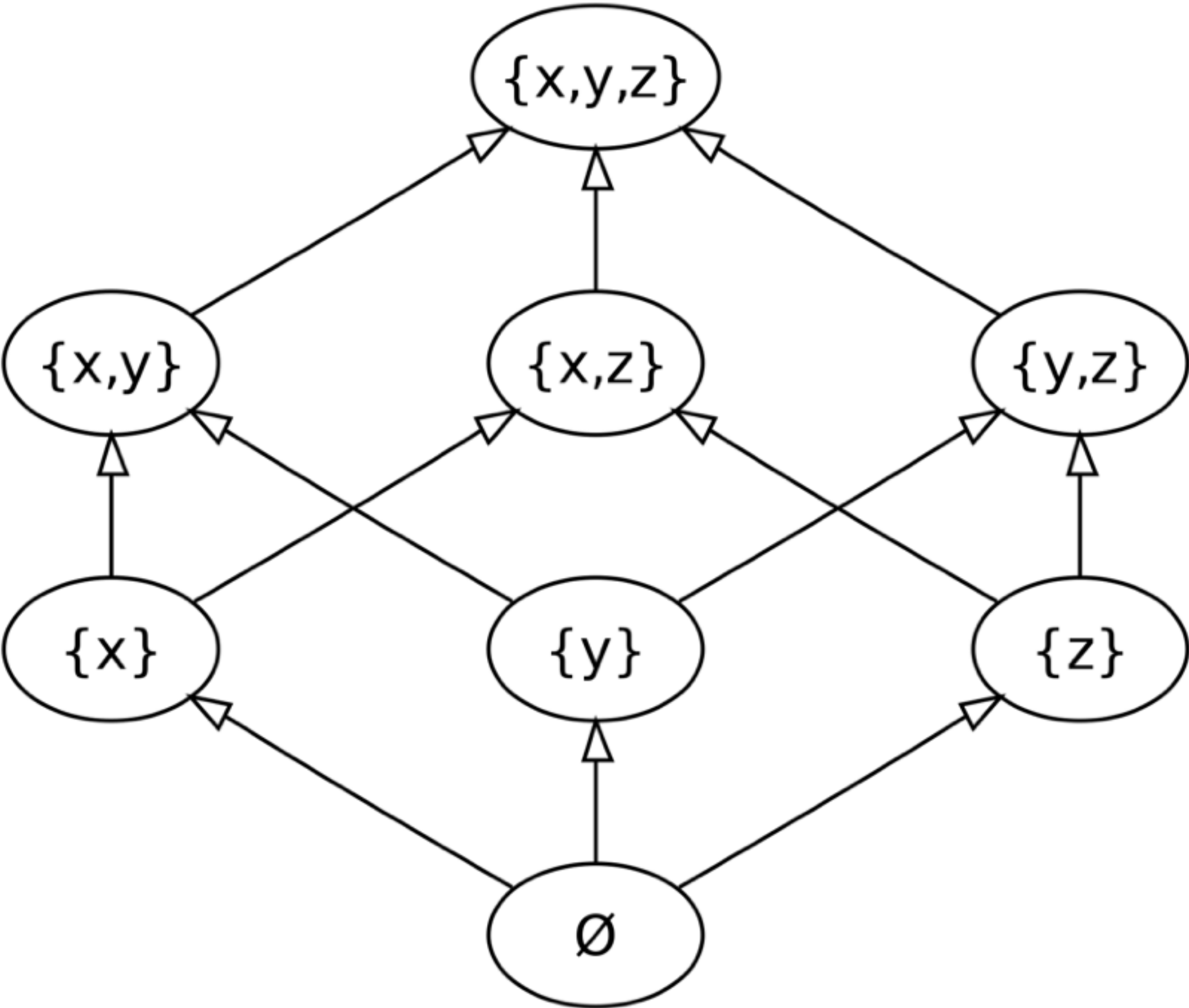


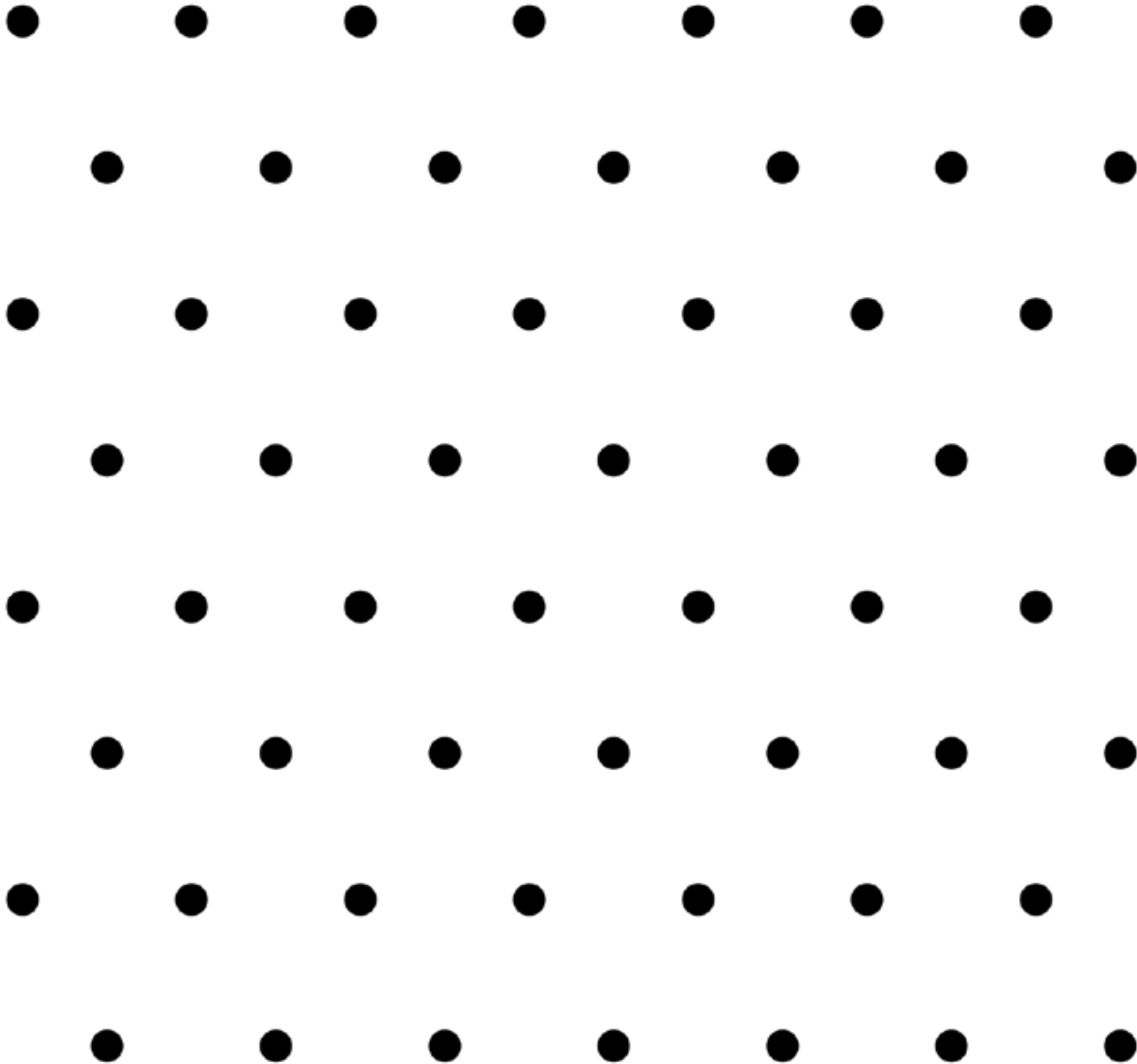
Lattice?

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 d'exposé

- Crypto moderne 🔥
- Réseaux Euclidiens et problème du vecteur le plus court 🖐️
- Problème d'apprentissage avec erreurs 📖
 - Schéma à clé secrète 🙈
 - Schéma à clé publique 📢
- Problème d'apprentissage avec erreurs dans les anneaux 💍
 - Schéma de signature 🖋️
 - Schéma d'établissement de clé 💀