IND-CPA^D

New security notion for ~~approximate~~ LWE-based? Fully Homomorphic Encryption

Félix Larose-Gervais, April 2025

Agenda

Presentation plan

- Crypto refreshers
  - Definitions and security notions
  - LWE and the importance of the noise
- IND-CPA^{D}
  - Definitions
  - Attacks on toy schemes