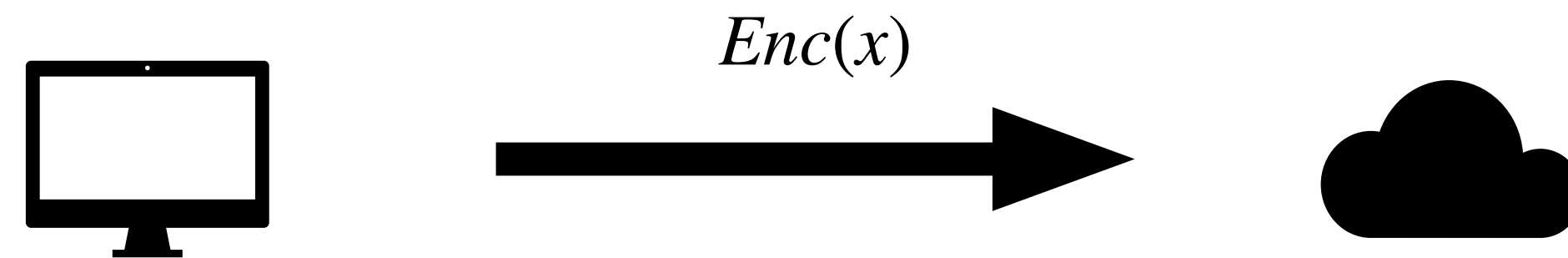
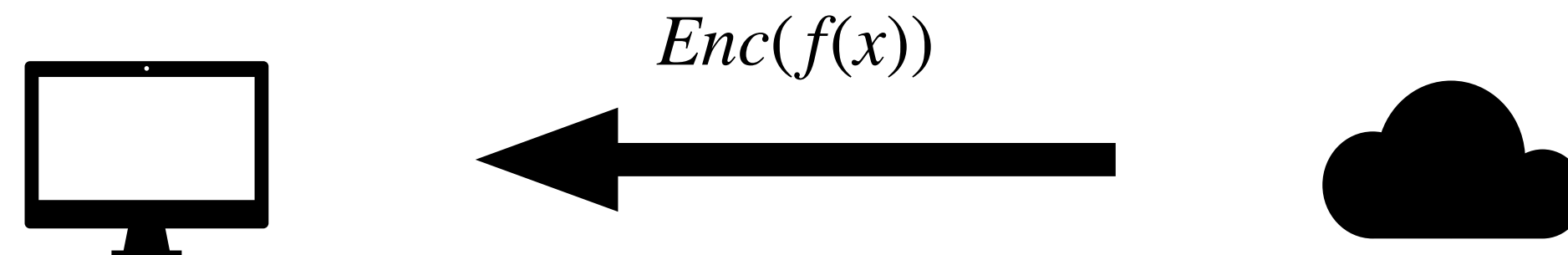


# Calcul privé

## Chiffrement homomorphe



$$f(Enc(x)) = Enc(f(x))$$



# TFHE

## Fast Fully Homomorphic Encryption over the Torus

- Schéma de chiffrement complètement homomorphe
- Implémenté par la librairie TFHE-rs 🦀
- Primitives cryptographiques:
  - Blind Arithmetic
  - Blind Comparison
  - Blind Function Evaluation