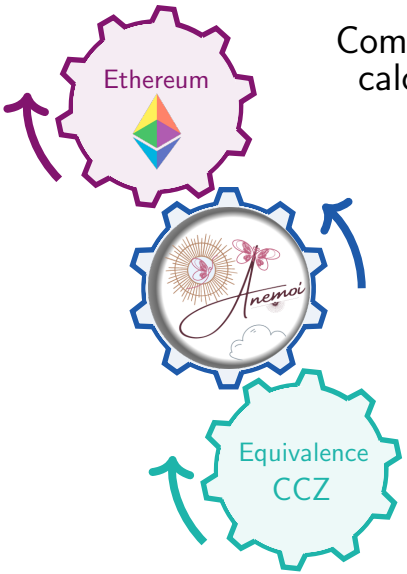

Comment prouver **efficacement** l'exactitude d'un calcul sans en dévoiler la moindre information ?

dans $\mathbb{Z}/p\mathbb{Z}$, p grand entier premier

Evaluation de la sécurité.

Cryptanalyse

- ☞ *Attaque théorique* [BCP22]
- ☞ *Attaques pratiques* [BBLP22]

Conception

- ☞ *Notre design* [BBC+22]

Amélioration de la conception.