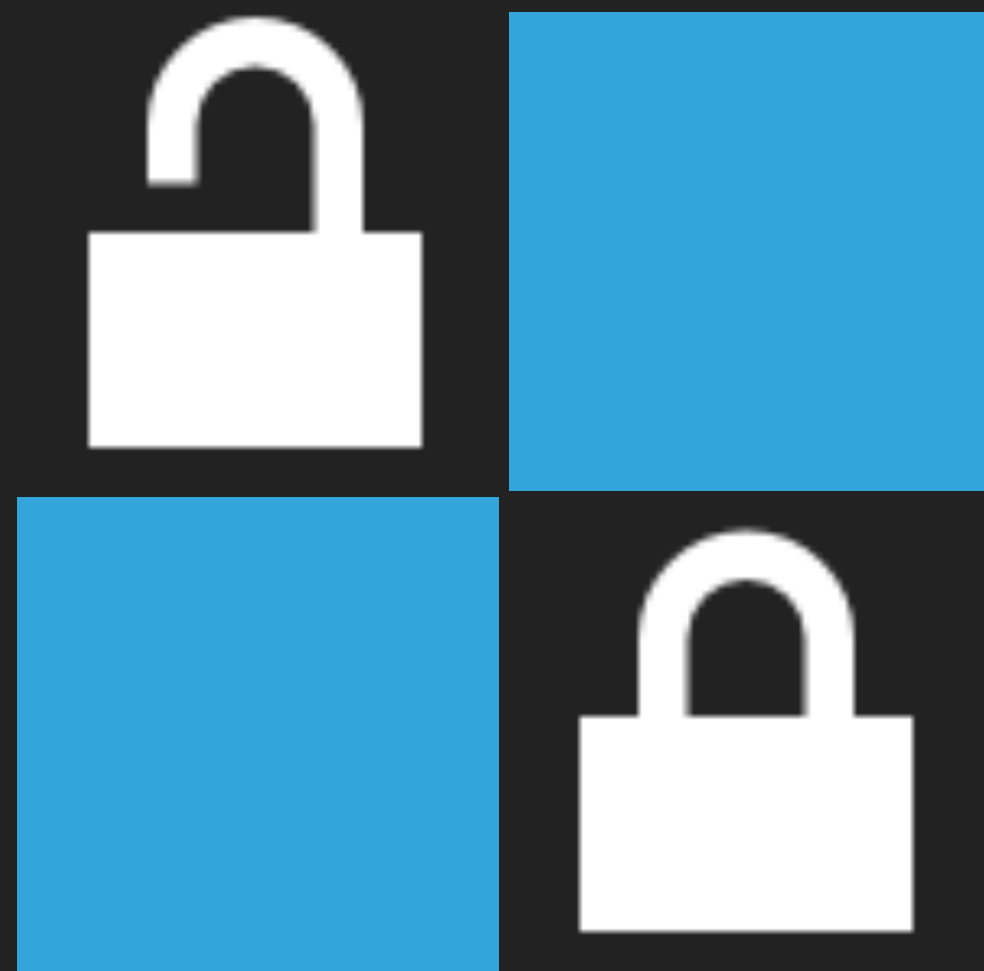


HOW TO SOLVE THE POST QUANTUM PROBLEM?

- ▶ Post quantum will come - likely in the next 5-15 years. Or much earlier (see link below)
- ▶ AES256 and other symmetric algorithms likely still secure (but key length greatly reduced: bit length/2)
- ▶ We have **no** quantum safe asymmetric algorithms
- ▶ **Solution: Crypto Agility!** Design everything in ways that allow algorithms to be replaced (as shown throughout the slides)



- ☒ Data treatment ...
- ☒ Use existing ...
- ☒ ...

PATTERNS

CRYPTO CHECKLIST