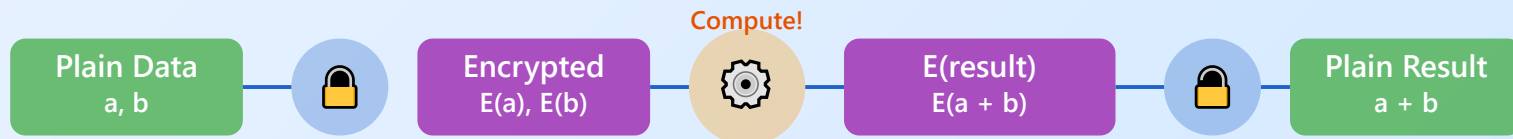


Homomorphic Encryption



How It Works

Mathematical Property:

$$E(3) + E(5) = E(8) \quad E(a) \oplus E(b) = E(a \oplus b)$$

Operation on encrypted data = Encryption of operated data

Types

Partial HE

Only addition OR
multiplication

Somewhat HE

Limited number of
operations

Fully HE ★

Arbitrary
computations



Security



100-1000x slowdown

Performance

