

C: $m, Enc, Dec, f()$

S: $Eval$

1 C encrypts his
message m , $Enc(m)$



2 C sends $Enc(m)$ to store

3 C queries, $f()$

5 S returns $Enc(f(m))$



4 S
evaluates
 $f()$ homo-
morphically

6 C computes
 $Dec(Enc(f(m))) = f(m)$,
and recovers $f(m)$