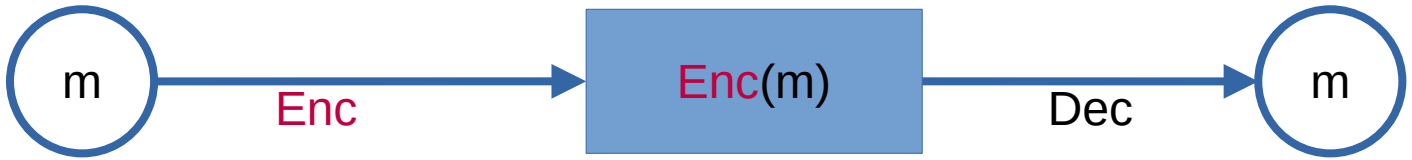
Fully Homomorphic Encryption: definitional issues and open problems

Daniele Micciancio
(UC San Diego)

[May 2022]

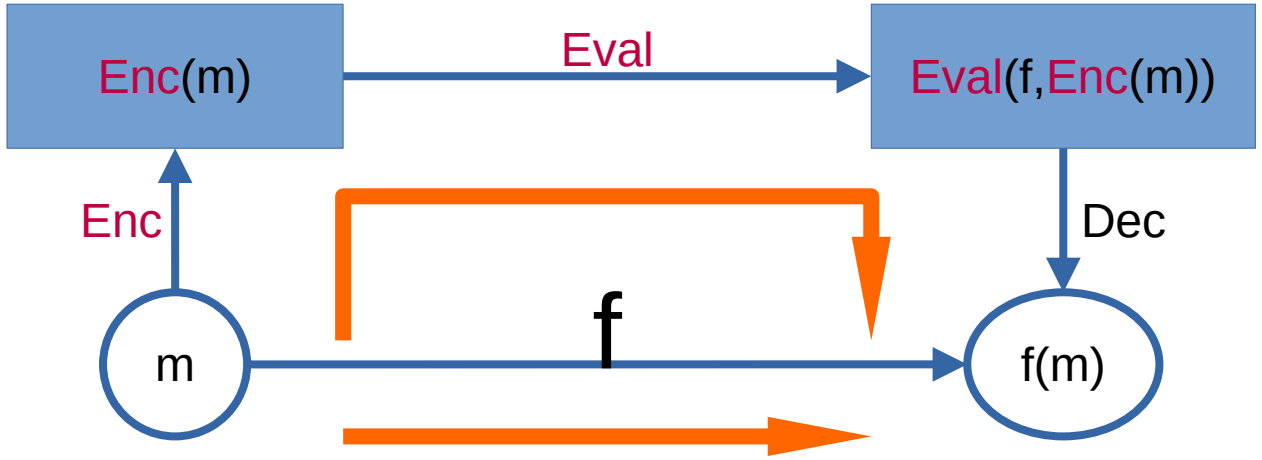
Encryption Scheme

- Syntax: (Gen,Enc,Dec)
- Correctness:
  - (pk,sk) ← Gen
  - $Dec_{sk}(Enc_{pk}(m)) = m$



Fully Homomorphic Encryption

- FHE Scheme: (Gen,Enc,Dec,Eval)
  - (pk,sk) ← Gen
  - $Dec_{sk}(Eval_{pk}(f,Enc_{pk}(m)) = f(m)$

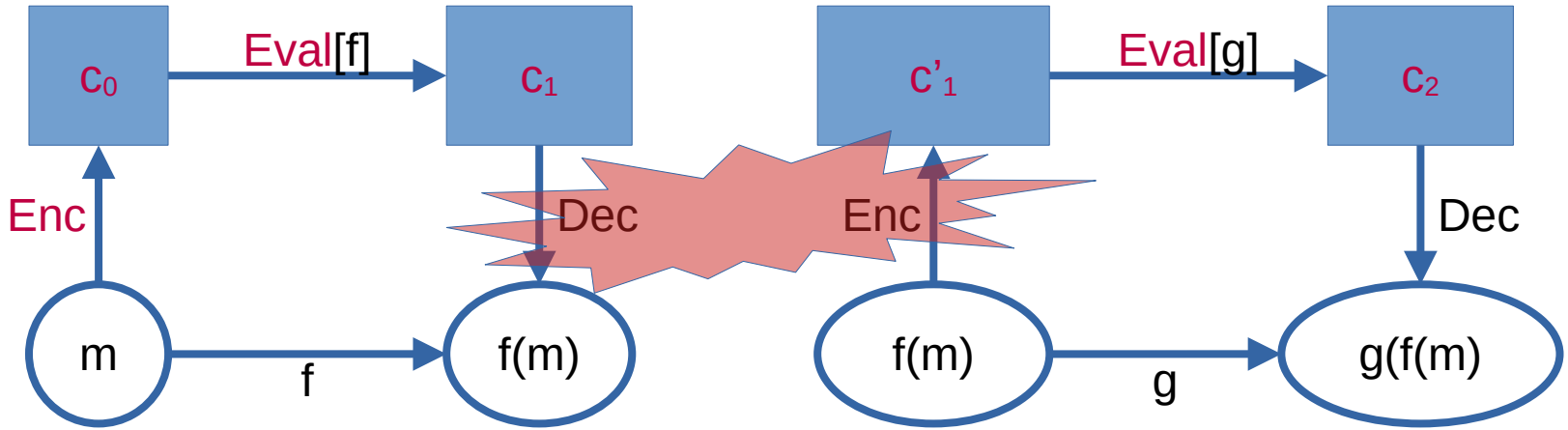


Composition

- Perform two computations in sequence:
  - Input : m → f(m) → g(f(m)) : output
  - c_0 = Enc(m)
  - c_1 = Eval(f,c_0)
  - c_2 = Eval(g,c_1)
- Question: Dec(c_2) = g(f(m)) ?
- Answer: not necessarily

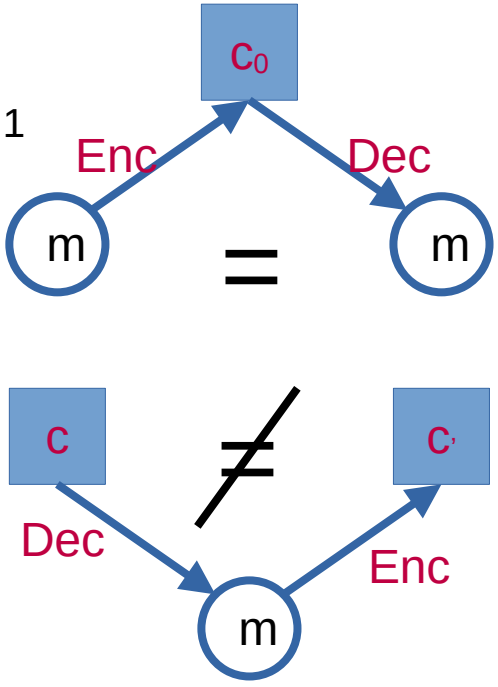
The Problem with Composition

- c_0 = Enc(m)
- c_1 = Eval(f,c_0)
- c_2 = Eval(g,c_1)



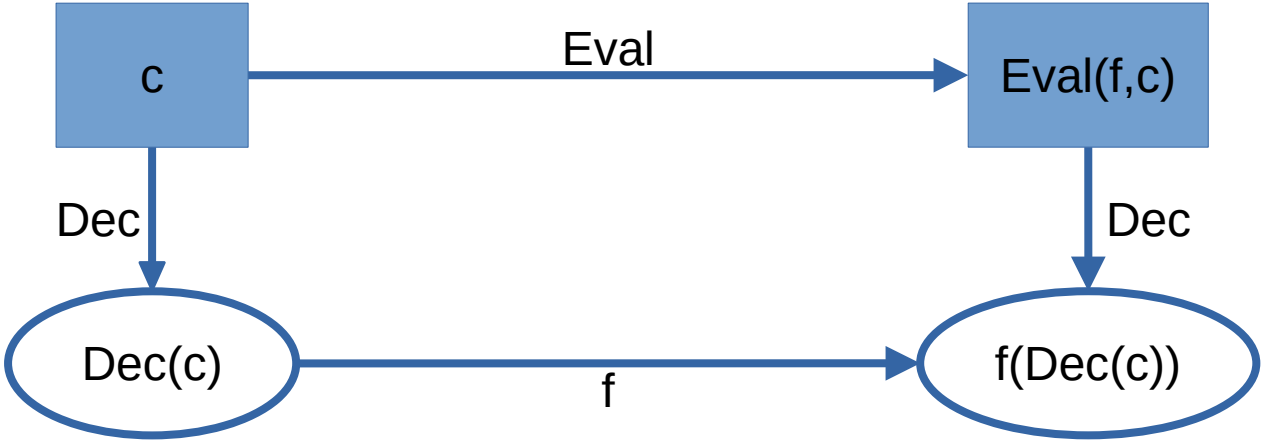
Correctness of Encryption

- Property 1: $c_1 = Enc(m_1)$
- Property 2: $Dec(c_1) = m_1$
- Correctness of encryption: $Dec(Enc(m_1)) = m_1$
  - (Property 1) implies (Property 2)
- But the converse may not be true
  - (Property 2) does not imply (Property 1)
  - $Enc(Dec(c_1))$ is not in general equal to c_1



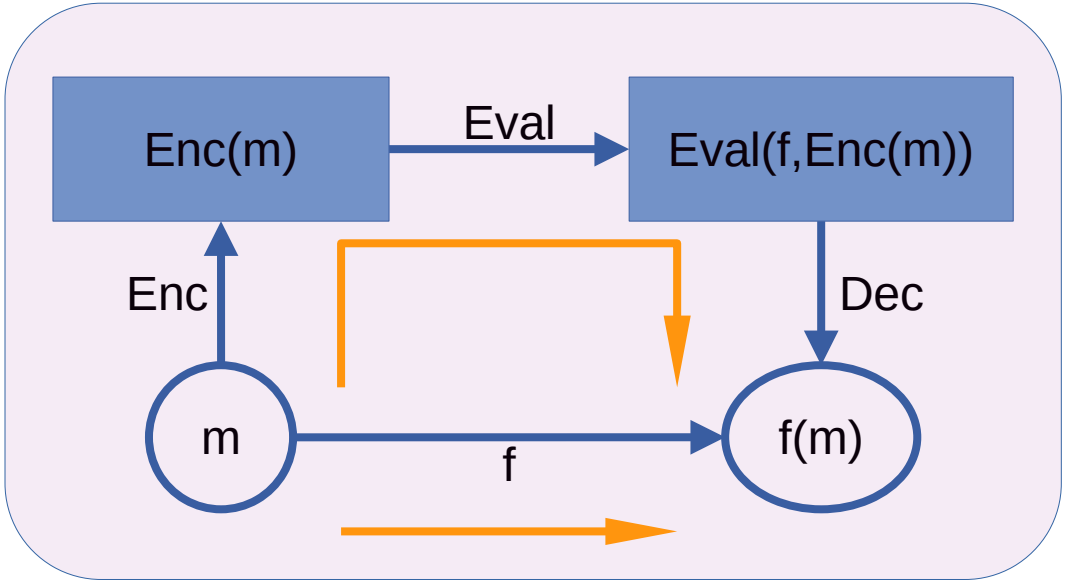
Fully Composable HE

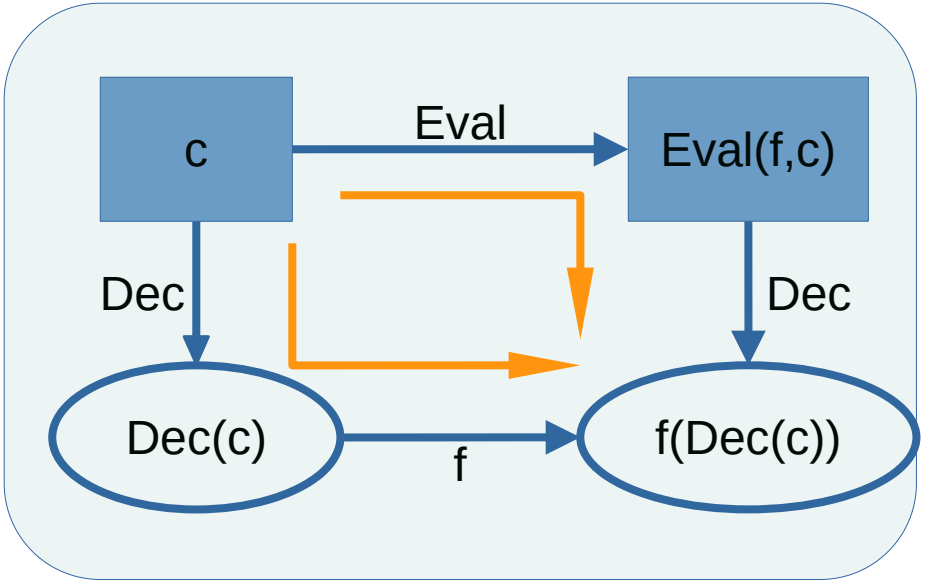
- FHE Scheme: (Gen,Enc,Dec,Eval)
- A new correctness property:
  - Dec(Eval(f,c)) = f(Dec(c))



Comparing the two definitions

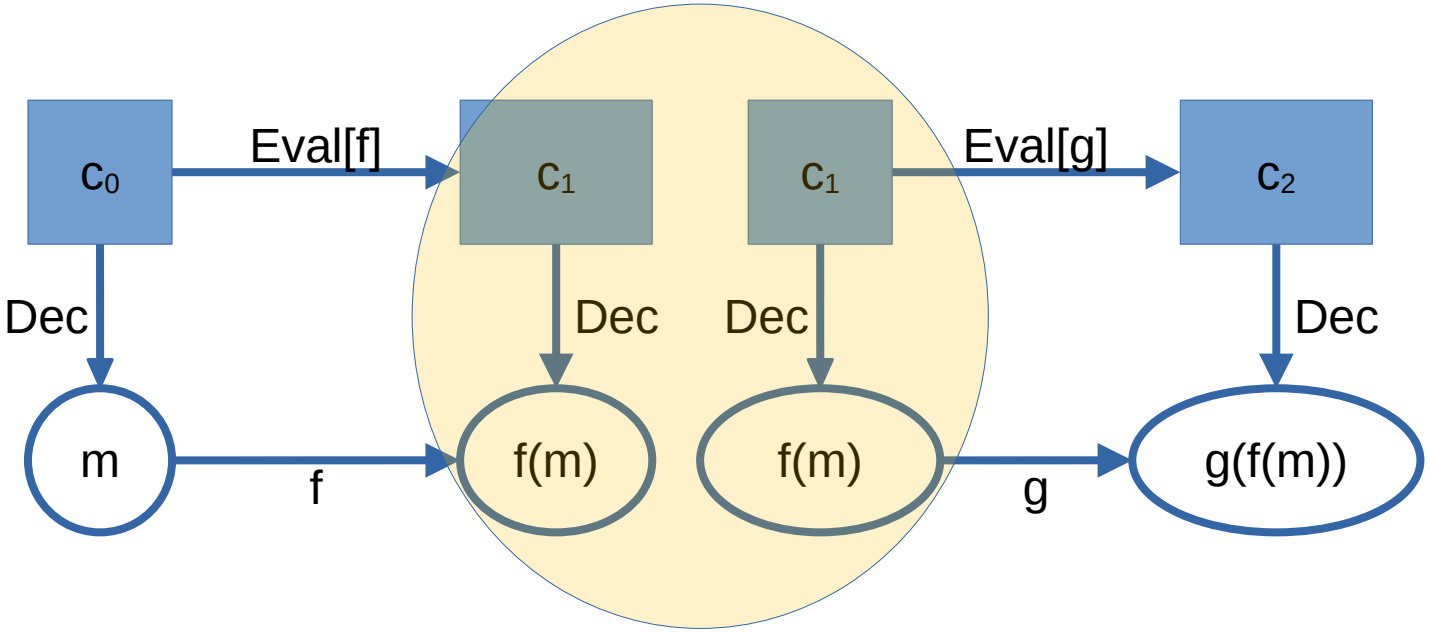
- FHE: Dec(Eval(f,Enc(m))) = f(m)
- CFHE: Dec(Eval(f,c)) = f(Dec(c))





Composition

- $c_0 = Enc(m)$; $c_1 = Eval(f,c_0)$; $c_2 = Eval(g,c_1)$
- $Dec(c_2) = g(f(m))$!



CFHE implies FHE

- FHE: Dec(Eval(f,Enc(m))) = f(m)
- CFHE: Dec(Eval(f,c)) = f(Dec(c))
- Let c = Enc(m). Then

Dec(Eval(f,Enc(m))

= Dec(Eval(f,c)) [definition of c]

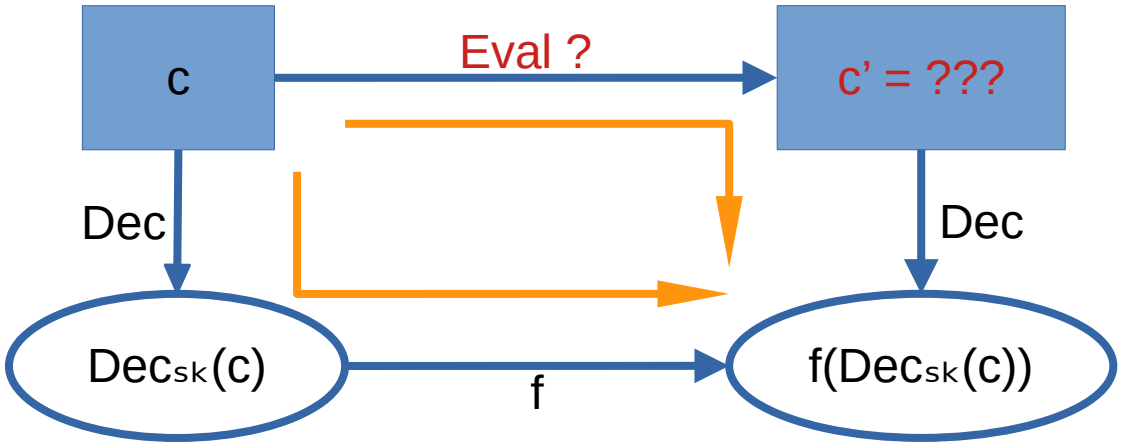
= f(Dec(c)) [CFHE]

= f(Dec(Enc(m)) [definition of c]

= f(m) [correctness of decryption]

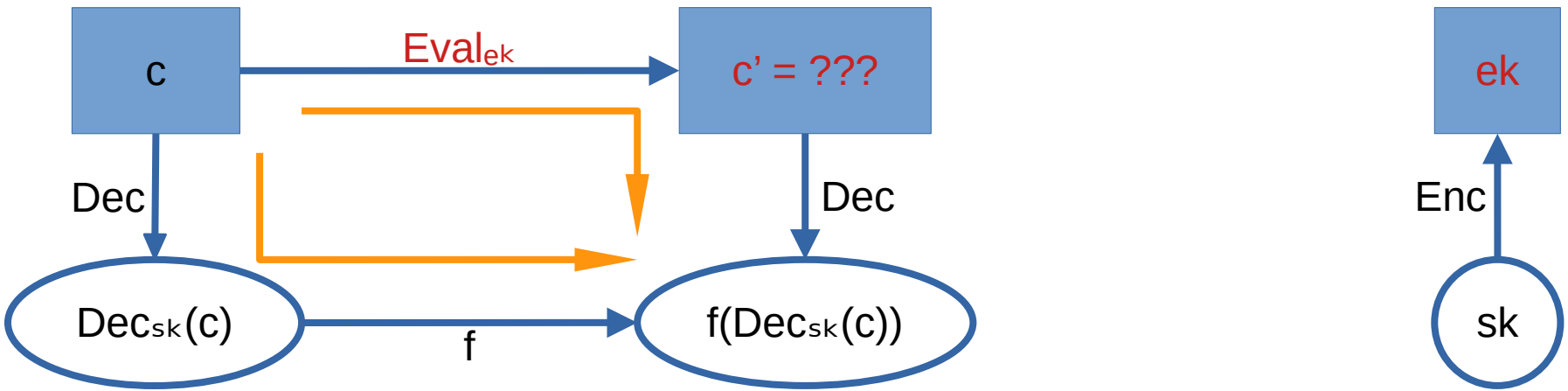
Bootstrapping revisited

- **Theorem:** FHE+circular security => CFHE
  - Given FHE(Gen,Enc,Dec,Eval)
  - Build CFHE(Gen,Enc,Dec,Eval)
  - Goal: $Dec_{sk}(c') = f(Dec_{sk}(c))$



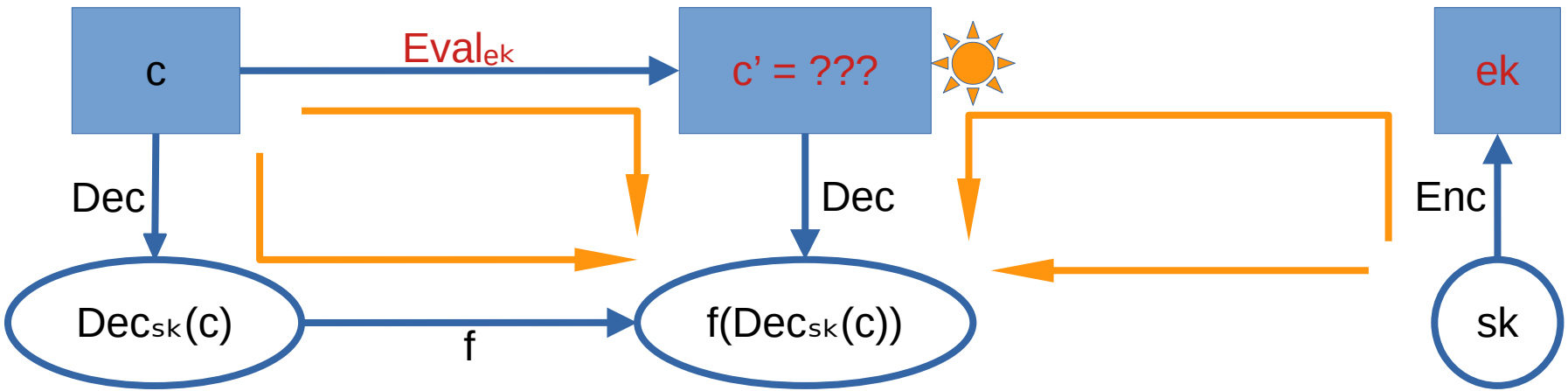
Bootstrapping revisited

- **Theorem:** FHE+circular security => CFHE
  - Gen: ek = Enc(sk)



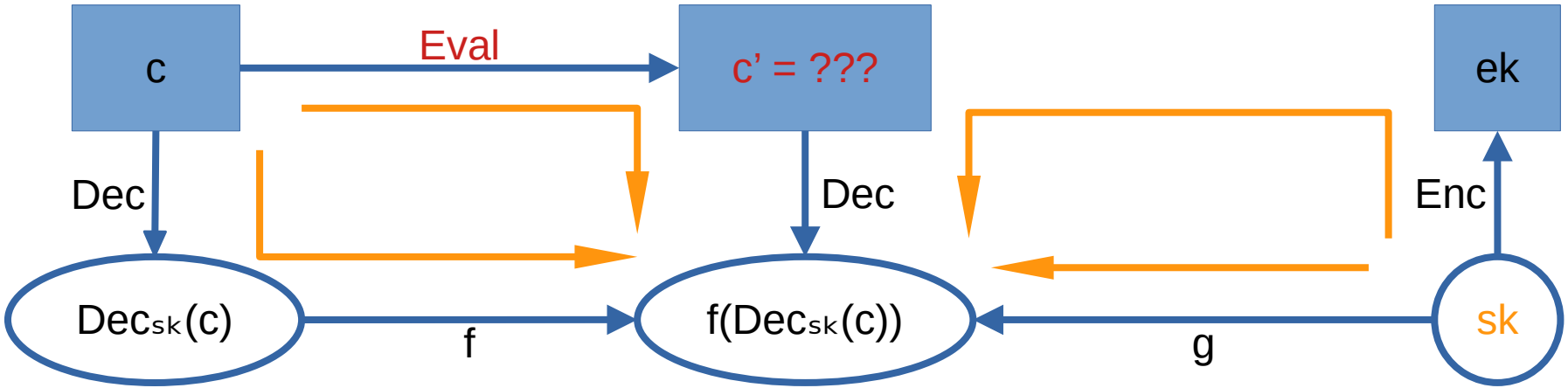
Bootstrapping revisited

- **Theorem:** FHE+circular security => CFHE
  - Gen: ek = Enc(sk)



Bootstrapping revisited

- **Theorem:** FHE+circular security => CFHE
  - Gen: ek = Enc(sk)
  - g(sk) = f(Dec_{sk}(c))



Bootstrapping revisited

- **Theorem:** FHE+circular security => CFHE
  - Gen: ek = Enc(sk)
  - g(sk) = f(Dec_{sk}(c))
  - $Eval_{ek}$(f,c) = c' = Eval(g,ek)