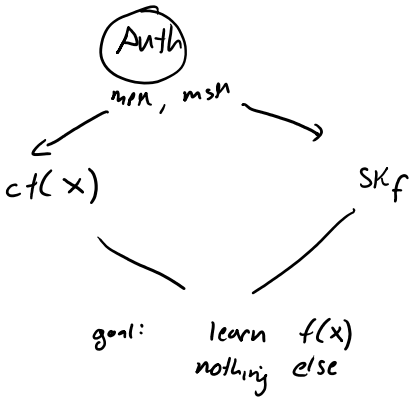
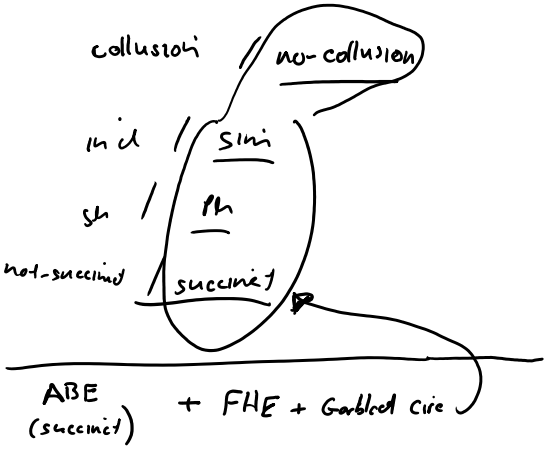
Functional Enc II

Thursday, October 8, 2020 11:22 AM





$(FE.mpk, FE.msk) = (ABE.mpk, ABE.msk)$

$FE.Enc_{mpk}(x)$:
- $\cdot$ $sk \leftarrow \$$, $\{K_{i,b}\} \leftarrow GC.Keys$
- $\hat{x} = FHE.Enc_{sk}(x)$
- $\{ABE.Enc((\hat{x}, i, b), K_{i,b})\}_{i=1,\dots n,\ b=0,1}$
- $\tilde{C} = Garble(FHE.Dec_{sk}(\cdot))$

$FE.SK_f = ABE.SK_g$

$g(\hat{x}, i, b)$: { $x^* = FHE.Eval(f, \hat{x})$
output "true" if $x^*_i = b$ }

learn $\{K_{i,x^*_i}\}$ // garbled input for x^*

Proof of security:

Proof of security:

- Hybrid 0: mpk, sk_f, $FE.ct(x) = (\hat{x}, ABE.ct(\hat{z}, i, s \ldots), \tilde{C})$

ABE ≈

- Hybrid 1: for all i, if $x_i^* \neq b$, "remove $k_{i,z}$"

GC ≈

- Hybrid 2: switch $(\tilde{C}, \tilde{x}^* = \{k_{i,x_i^*}\})$ to $GC.Sim(f(x))$

FHE ≈

- Hybrid 3: switch $\hat{x}$ to encryption of 0.

↑

Sim