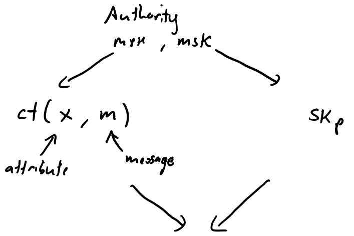
# Functional Encryption (FE)

Tuesday, October 6, 2020 11:44 AM

Recall ABE:



- learn m if $P(x) = \text{true}$ (functionality)
- otherwise m hidden (security; w/ collusion)
- always learn x

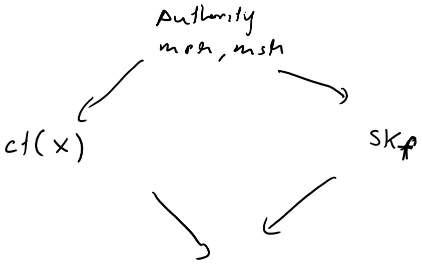
---

Predicate enc (PE)

only learn x if $P(x) = \text{true}$

---

Functional Enc (FE)



- functionality: learn $f(x)$
- security: nothing else

---

ABE $\quad x = (x', m) \quad\quad f(x): \; (x', m)$ if $P(x') = \text{true}$

PE $\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ ~~$x'$~~ $\bot$ otherwise

---

ABE/PE/FE: can exchange $f, x$.

FE security (non-adaptive)

adv chooses $\{f_i\}_{i\in[n]}, \{x_j\}_{j\in[\ell]}$

- Simulation:

$$\begin{bmatrix} mpk \\ sk_{f_1}, \ldots, sk_{f_n} \\ ct(x_1), \ldots, ct(x_\ell) \end{bmatrix} \approx Sim\left(\{f_i\}_{i\in[n]}, \{f_i(x_j)\}_{i,j}\right)$$

$$\left( \begin{matrix} sk_{f_1}, \dots, sk_{f_n} \\ ct(x_1), \dots, ct(x_\ell) \end{matrix} \right) \approx Sim\left( \{f_i\}_{i \in [n]}, \{f_i(x_j)\}_{i,j} \right)$$

unachievable! think of $f_i(x_j) = PRF(x_j, i)$

- Ind Security: Adv chooses $\{f_i\}_{i \in [n]}, x_0, x_1$ s.t. $f_i(x_0) = f_i(x_1) \quad \forall i$

$$(mpk, \{sk_{f_i}\}, ct(x_0)) \approx (mpk, \{sk_{f_i}\}, ct(x_1))$$

$\Longleftarrow$ ind. obfuscation

## no-collusion FE

- adv sees single secret key $sk_f$.

→ symmetric-key no-collusion simulation sec FE : need msk to encrypt (CPA-attack security)

$\Uparrow$

garbled circuits

$$\{K_{i,b}\}_{i \in [n], b \in \{0,1\}}$$

$$\begin{tikzcd} C \arrow[r, "\text{``garble''}"] & \tilde{C} \arrow[dr] & \\ & & C(x) \\ x \arrow[r, "\text{``garble''}"] & \tilde{x} = \{K_{i,x_i}\} \arrow[ur] & \end{tikzcd}$$

security: $(\tilde{C}, \tilde{x}) \approx Sim(C(x))$

Garbled circuits ⇒ Sym. Key FE

$ct(C) = \tilde{C}$

$SK_x = \tilde{X}$

No collusion (one-key), many ctext simulation secure.

Garbled circuits + PKE ⇒ PK FE

$$mpk = \begin{bmatrix} pk_{1,0} & \cdots & , & pk_{n,0} \\ pk_{1,1} & \cdots & & pk_{n,1} \end{bmatrix}$$

$$msk = \begin{bmatrix} sk_{1,0} & & sk_{n,0} \\ sk_{1,1} & - - - & sk_{n,1} \end{bmatrix}$$

$SK_x = \{SK_{i,x_i}\}$

$ct(C) = \tilde{C}, \quad Enc(pk_{i,b}, \quad K_{i,b})$