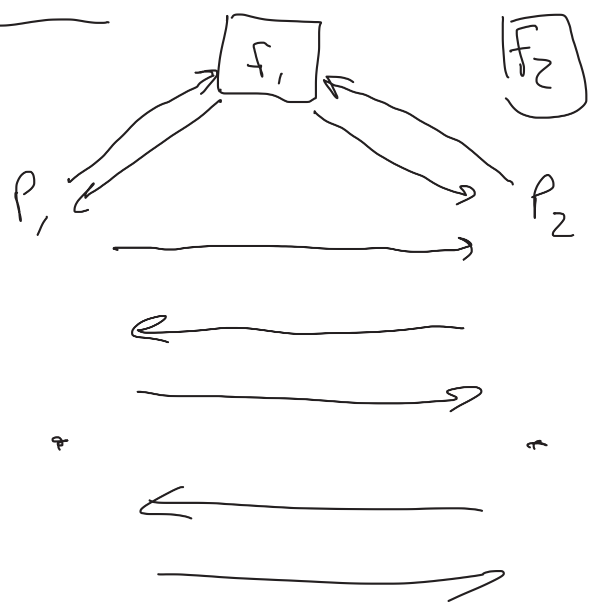
- Sequential Composition
- Modular Composition
  - hybrid-world execution, $\mathrm{Hybrid}^{f_1,\ldots,f_m}_{\Pi,A}(\kappa, \vec{x}, z)$
  - Security of hybrid-world protocol
  - Composition theorem
- parallel composition? arbitrary (concurrent) composition?

<u>hybrid world</u>



hybrid-world protocol Π evaluating f is secure if for all PPT A, $\exists$ PPT S s.t.

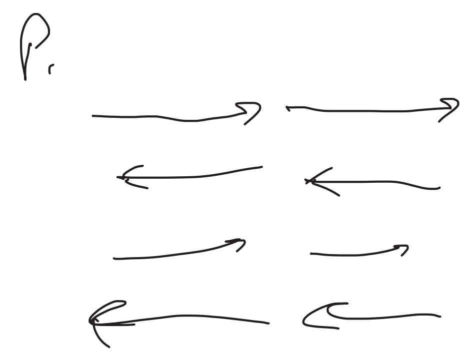
$$\mathrm{Hybrid}^{f_1,\ldots,f_m}_{\Pi,A}(\kappa, \vec{x}, z) \approx \mathrm{Ideal}_{f,S}(\kappa, \vec{x}, z)$$

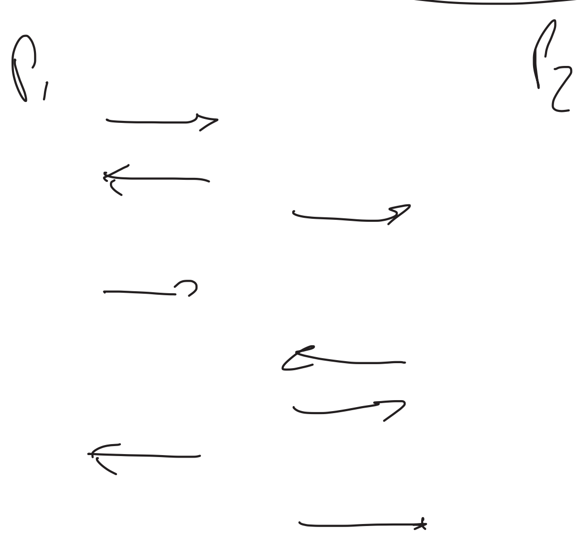
Theorem:

If $\rho_1, \dots, \rho_m$ are secure protocols for computing $F_1, \dots, F_m$, and if Π is a secure protocol for computing F in the $(F_1, \dots, F_m)$-hybrid world, then the composed protocol $\Pi^{\rho_1, \dots, \rho_m}$ is a secure protocol for F.

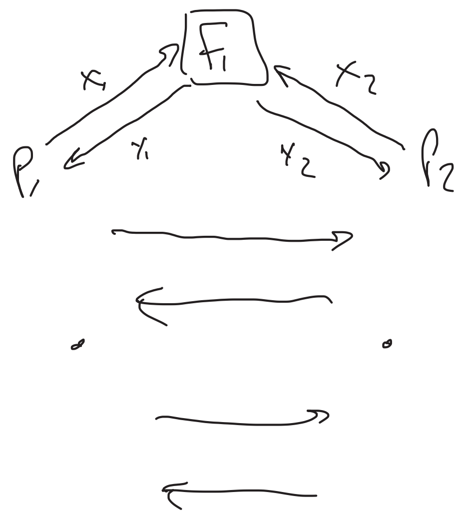
Parallel & Concurrent composition?

Say Π_1, Π_2 are secure protocols computing F_1, F_2, resp..

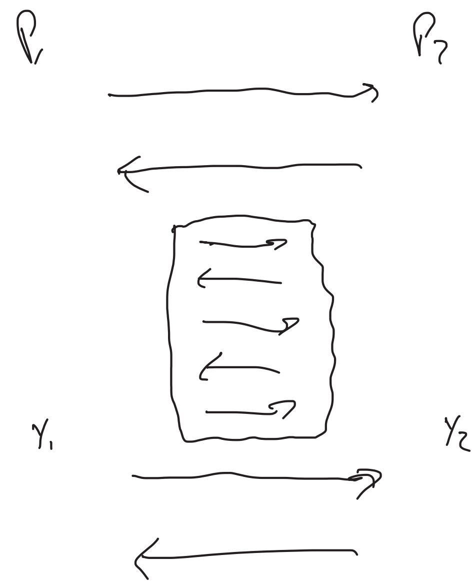




Note: Concurrent composition in semi-honest case holds hybrid world

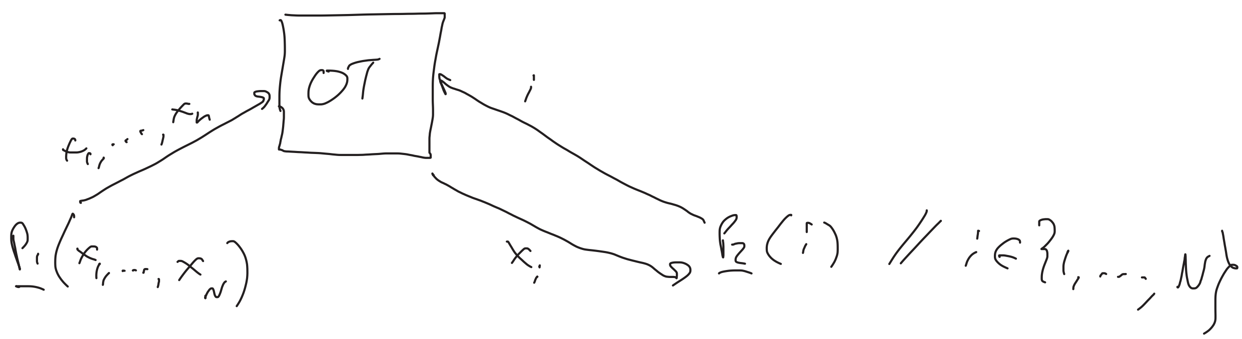


real-world



- Oblivious transfer (OT)
  - OT from DDH
  - extending the domain
  - (from 1-of-2 OT to 1-of-N OT)

1-out-of-N oblivious transfer



<u>Semi-honest OT:</u>

Let $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ be a CPA-secure public-key encryption scheme.

<u>$P_1(x_1, \dots, x_n)$</u>

<u>$P_2(i)$</u>

$(pk_i, sk_i) \leftarrow \mathrm{Gen}(1^k)$

sample $N-1$ other keys

$pk_1, \dots, pk_{i-1}, pk_{i+1}, \dots, pk_N \leftarrow$ <u>Sampkey</u>(1^k)

$\xleftarrow{pk_1, \dots, pk_N}$

$\xrightarrow{\mathrm{Enc}_{pk_1}(x_1), \dots, \mathrm{Enc}_{pk_N}(x_N)}$

$x_i = \mathrm{Dec}_{sk_i}(c_i)$

Theorem:

The above securely computes OT (in semi-honest model). (Assumptions to be specified during the proof.)

Proof

- P_1 corrupted. Assume public keys generated by SampKey are identically distributed to public keys generated by Gen. Then construct the following adversary S:

$$\underline{S(x_1, \dots, x_N)} \xrightarrow{x_1, \dots, x_N} \boxed{OT} \qquad \underline{P_2}\,(i)$$

$$pk_1, \dots, pk_N \leftarrow \text{SampKey}(1^k)$$

$$\text{output } P_1(\underline{pk_1, \dots, pk_N})$$

- P_2 corrupted.

$$\underline{P_1} \xrightarrow{x_1, x_2} \boxed{OT} \xleftarrow{i} \underline{S}(i), \qquad \boxed{OT} \xrightarrow{x_i} \underline{S}(i)$$

$$(pk_i, sk_i) \leftarrow \text{Gen}(1^k; r_i)$$

$$pk_{3-i} \leftarrow \text{SampGen}(1^k, r_{3-i})$$

$$c_i \leftarrow \text{Enc}_{pk_i}(x_i)$$

$$c_{3-i} \leftarrow \text{Enc}_{pk_{3-i}}(0 \cdots 0)$$

$$\text{Output } (r_1, r_2, c_1, c_2, i)$$

Need to prove that for all x_1, x_2, i,

real: $\left(r_i, r_{3-i}, \mathrm{Enc}_{pk_i}(x_i), \mathrm{Enc}_{pk_{3-i}}(x_{3-i})\right)$ where $pk_i \leftarrow \mathrm{Gen}(1^k; r_i)$

$pk_{3-i} \leftarrow \mathrm{Samp}(1^k; r_{3-i})$

$\approx$?

ideal: $\left(r_i, r_{3-i}, \mathrm{Enc}_{pk_i}(x_i), \mathrm{Enc}_{pk_{3-i}}(0)\right)$ "

Assume toward a contradiction that some efficient distinguisher D can distinguish these distributions, construct adversary A breaking CPA-security of encryption

$\underline{A(pk)}$

output $\underline{(x_{3-i}, 0)}$, and get back ciphertext c_{3-i}

$pk_i \leftarrow \mathrm{Gen}(1^k; r_i)$

$c_i \leftarrow \mathrm{Enc}_{pk_i}(x_i)$

$r_{3-i} \leftarrow \mathrm{SampRand}(pk)$ // $pk \leftarrow \mathrm{SampKey}(1^k; r_{3-i})$

output $D(\underline{r_i, r_{3-i}, c_i, c_{3-i}})$

Need assumption on SampRand:

$$(r, \mathrm{SampKey}(1^k; r)) \approx (\mathrm{SampRand}(\cdot), \mathrm{Gen}(1^k))$$