Sequential Composition
- Modular Composition
  - Hybrid world execution, $\text{Hybrid}_{\pi,A}^{F_1,\ldots,F_m}(k, x, z)$
  - Security of hybrid world protocol
  - Composition theorem
- Parallel Composition? arbitrary (concurrent) composition?

Hybrid world

$\text{Hybrid-world protocol } \Pi \text{ evaluating } F \text{ is secure if for all ppt } A, \exists \text{ ppt } S \text{ s.t.}$

$\text{Hybrid}_{\pi,A}^{F_1,\ldots,F_m}(k, x, z) \approx \text{Ideal}_{F_1,S}(k, x, z)$
Theorem

If \( g_1, \ldots, g_m \) are secure protocols for computing \( F_1, \ldots, F_m \), and if \( \Pi \) is a secure protocol for computing \( F \) in the \((F_1, \ldots, F_m)\)-hybrid world, then the composed protocol \( \Pi_{g_1, \ldots, g_m} \) is a secure protocol for \( F \).

Parallel vs. Concurrent Composition?

Say \( \Pi_1, \Pi_2 \) are secure protocols computing \( f_1, f_2 \), resp.

\[
\begin{array}{c}
\Pi_1 \\
\downarrow \\
\Pi_2 \\
\end{array}
\]

Note: Concurrent composition in semi-honest case holds
Oblivious transfer (OT)

- OT from DH
- extending the domain
  (From 1-of-2 OT to 1-of-N OT)

1-out-of-N oblivious transfer

\[ \text{OT} \]

\[ \pi_i(x_1, \ldots, x_N) \quad i \]

Semi-honest OT:

Let (Gen, Enc, Dec) be a CPA-secure encryption scheme.

\[ \pi_i(x_1, \ldots, x_N) \]

\[ \pi_2(i) \quad i \in \{1, \ldots, N\} \]

\[ (pk_i, sk_i) \leftarrow \text{Gen}(1^x) \]

Sample N-1 other keys

\[ \{pk_1, \ldots, pk_{i-1}, pk_{i+1}, \ldots, pk_N\} \leftarrow \text{Sample}\text{Key}(1^x) \]

\[ \text{Enc}_{pk_i}(x_i), \ldots, \text{Enc}_{pk_N}(x_N) \]

\[ x_i = \text{Dec}_{sk_i}(C_i) \]
Theorem:
The above securely computes OT. (Assumptions to be specified during the proof.)

Proof:

- $P_1$ Corrupted. Assume public keys generated by $SampleKey$ are identically distributed to public keys generated by $Gen$.

Then construct the following adversary $S$:

\[ S(x_1, ..., x_N) \]

\[ P_2 (i) \]

$pk_1, ..., pk_N \leftarrow Sample_i (1^k)$

Output $P_i(pk_1, ..., pk_N)$

- $P_2$ Corrupted.
Need to prove that for all $x_i, x_j, i$,

real: $(c_i, s_i, \text{Enc}_{pk_i}(x_i), \text{Enc}_{pk_{i-1}}(s_i))$ where $pk_i \leftarrow \text{Gen}(1^k, r_i)$

$pk_{i-1} \leftarrow \text{Samp}(1^k, s_i)$

ideal: $(c_i, s_i, \text{Enc}_{pk_i}(x_i), \text{Enc}_{pk_{i-1}}(0))$

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

\[
A(pk)
\]

output $\ell(x_{i-1}, 0)$, and get back ciphertext $c_{i-1}$

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

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

$s_{i-1} \leftarrow \text{SampRand}(pk) \parallel pk \leftarrow \text{SampleKey}(1^k, s_{i-1})$

output $D(c_i, s_{i-1}, c_i, c_{i-1})$

Need assumption on $\text{SampRand}$:

$(c_i, \text{SampleKey}(1^k, r_i)) \approx (\text{SampRand}(1^k), \text{Gen}(1^k))$