Lecture 5

Lecturer: Jonathan Katz *Scribe(s): Andrew Miller*

1 Oblivious Transfer Cont.

1.1 Pre-processing Oblivious Transfer

For the pre-processing OT protocol, one round of OT is used to establish keys. Thereafter, an arbitrary number of OT's over different messages can be performed for using these keys.

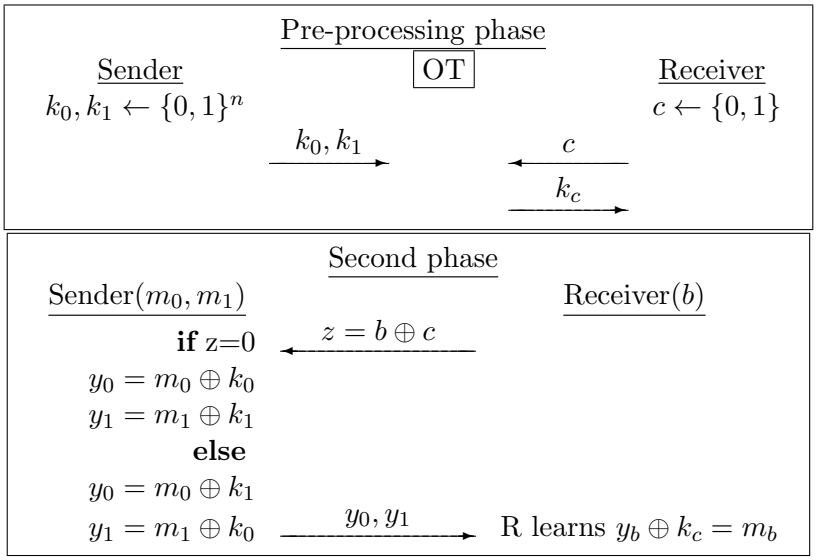


Figure 1: Protocol for Pre-processing OT

1.2 OT Extension

An OT extension protocol turns k OTs on m-bit strings into m OTs on n-bit strings, where k is the security parameter.

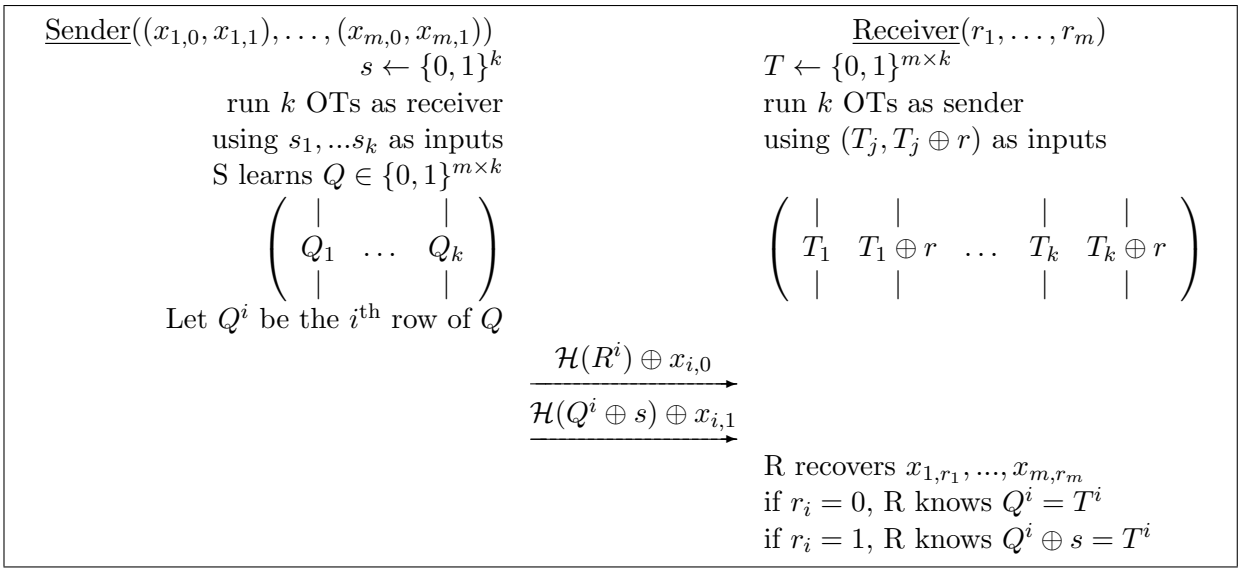


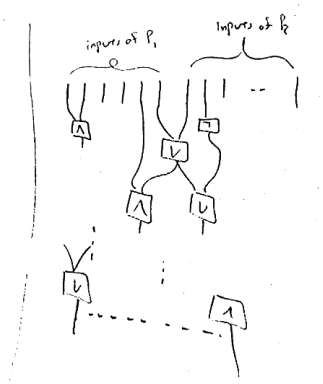
Figure 2: Protocol for OT extension

1.2.1 Assumption on Randomness of the Hash Function

For arbitrary $T^1, ..., T^m$ and s, the hash function outputs, $\mathcal{H}(s \oplus T^1), \mathcal{H}(s \oplus T^2), ..., \mathcal{H}(s \oplus T^m)$, should be indistinguishable from uniform random, even given $T^1, ..., T^m$.

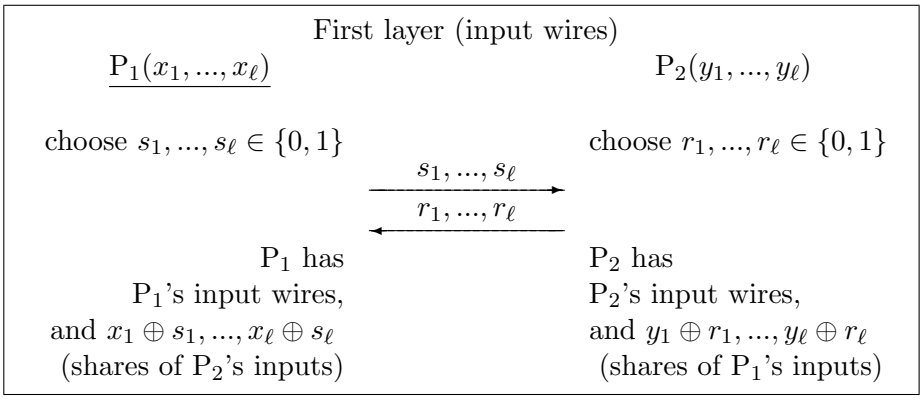
1.3 GMW (Goldreich-Micali,Wigderson) Approach to semi-honest two-party computation

Secure computation of arbitrary circuits from OT. Assume we have a Boolean circuit with 2ℓ inputs, the first half are from P_1, the second half are from P_2. The gates may have arbitrary fan-in and fan-out. At the bottom we have some number of output gates, and both parties learn all the outputs.



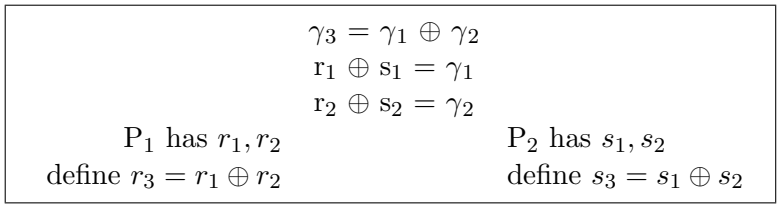
The approach is to have 2-out-of-2 secret sharing for every wire value. The protocol proceeds layer by layer, beginning with the input layer.

1.3.1 Input Layer



1.3.2 XOR Gate

No communications are required for an XOR gate - each party can construct the shares of the output using their existing shares of the inputs.



1.3.3 NOT Gate

NOT gates are easy - just agree that one player (e.g., P_1) flips the bit.

1.3.4 AND Gate

Each AND gate requires an invocation of OT.

$\gamma_3 = \gamma_1 \wedge \gamma_2$
$\mathrm{r}_1 \oplus \mathrm{s}_1 = \gamma_1$
$\mathrm{r}_2 \oplus \mathrm{s}_2 = \gamma_2$

P_1 has r_1, r_2
choose $r_3 \xleftarrow{\$} \{0,1\}$
this is P_1's share of γ_3

P_2 has s_1, s_2
use 1-out-of-4 OT to select appropriate row from table

s_1	s_2	s_3
0	0	$(\mathrm{r}_1 \wedge \mathrm{r}_2) \oplus \mathrm{r}_3$
0	1	$(r_1 \wedge \neg r_2) \oplus r_3$
1	0	$(\neg r_1 \wedge r_2) \oplus r_3$
1	1	$(\neg r_1 \wedge \neg r_2) \oplus r_3$