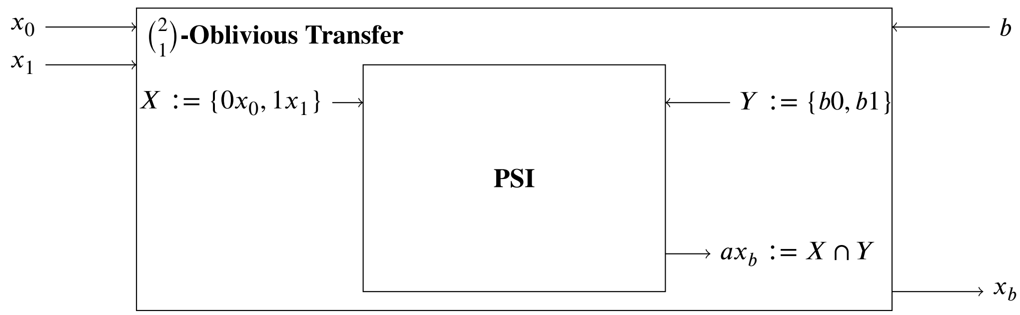
7.1 Oblivious Transfer from Private Set Intersection

We can create the following scheme, for the given problem:

S
$x_0 \leftarrow \{0,1\}$
$x_1 \leftarrow \{0,1\}$

R
$b \leftarrow \{0,1\}$



With this procedure we get the following truth table:

x_0	x_1	b	$0x_0$	$1x_1$	$b0$	$b1$	$ax_b := X \cap Y$	x_b
0	0	0	00	10	00	01	00	0
0	0	1	00	10	10	11	10	0
0	1	0	00	11	00	01	00	0
0	1	1	00	11	10	11	11	1
1	0	0	01	10	00	01	01	1
1	0	1	01	10	10	11	10	0
1	1	0	01	11	00	01	01	1
1	1	1	01	11	10	11	11	1

7.2 Private Set Intersection from Additively Homomorphic Encryption

7.2.1 A learns if $P(y) = 0$

Following the solution for a PSI algorithm for semi-honest adversaries by FREEDMAN, NISSIM and PINKAS, we can create the following protocol (REMIND: $P(y) = \prod_{x \in X}(x - y) = \sum_{i=0}^{n} \alpha_i \cdot y^i$):

A(X)		**B(y)**
Encrypt all coefficients of $P(y)$		
For $i = 0$ to n:		
$c_i = \text{AM-ENC}(pk, \alpha_i)$	$\xrightarrow{c_0,\ldots,c_n}$	$r \leftarrow \mathbb{GF}(q)$
		For $i = 0$ to n:
		$c'_i = (c_i)^{y^i}$
		$c = \prod c'_i \quad (= P(y))$
		$\hat{c} = c^r \quad (= r \cdot P(y))$
$m = \text{AM-DEC}(sk, c_y)$	$\xleftarrow{c_y}$	$c_y = \hat{c} \cdot \text{AM-ENC}(pk, y) \quad (r \cdot P(y) + y)$
Return $m \overset{?}{\in} X$		

7.2.2 A learns if $X \bigcap Y$

$\mathbb{B}$ will know execute its part for all $y \in Y$ and send $c_{y_1}, ..., c_{y_m}$ to $\mathbb{A}$, for which $\mathbb{A}$ can check whether these are valid encryptions of $x \in X$ and therefore part of the set:

A(X)		**B(Y)**
Again compute all c_i encryptions of $P(y)$		
For $i = 0$ to n:		
$\quad c_i \;=\; \text{AM-ENC}\ (pk, \alpha_i)$	$\xrightarrow{c_0,\dots,c_n}$	$r \leftarrow \mathbb{GF}(q)$
		For $i = 0$ to m:
		$\quad c_{y_i}$ is the encryption of $r \cdot P(y_i) + y_i$ as before
$C_y = \bigcup c_{y_i}$	$\xleftarrow{c_{y_i},\dots,c_{y_m}}$	
$S = \{\}$		
For each $c_y \in C_y$:		
$\quad m = \text{AM-DEC}()sk, c_y$		
$\quad$ If $m \in X$:		
$\qquad S = S \cup \{m\}$		
Return S		

7.3 Secure 2-way AND using Oblivious Transfer

We can create the following scheme, for the given problem:

$\underline{\mathbb{A}}$
$x \leftarrow \{0, 1\}$

$\underline{\mathbb{B}}$
$y \leftarrow \{0, 1\}$

$x_0 = 0 \longrightarrow$
$x_1 = x \longrightarrow$

$\binom{2}{1}$**-Oblivious Transfer**

$\longleftarrow y$

x_0	x_1	y	x_y
0	0	0	$x_0 = 0$
0	1	0	$x_0 = 0$
0	0	1	$x_1 = 0$
0	1	1	$x_1 = 1$

$\longrightarrow x_y = x \wedge y$

$\xleftarrow{\quad x_b \quad}$

In this OTS y will be the index of which x_i, will be returned by the OTS, so if $y = 0$ the value of x_0 will be returned, the sender $\mathbb{A}$, will input $x_0 = 0$ and $x_0 = x$, where x is the chosen value from $\mathbb{A}$. This will lead to an output-behaviour of an AND-Operator.
In the end $\mathbb{B}$ sends the returned value from the OTS to $\mathbb{A}$.