Overall picture:

Alice

Agree on $f$

Bob

$x \rightarrow$ protocol for $f$ $\rightarrow y$

$f(x, y)$

Security (informal): Bob learns nothing except $f(x, y)$.
Alice learns nothing.

For a formal definition, see the universal composable framework paper (Canetti 2000).

Protocol

1. Alice proposes an "encrypted circuit" for $f$, and sends it to Bob. She convinces Bob that the circuit is correct.

2. Alice and Bob run on OT protocol s.t. Bob learns the keys corresponding to his $y$.

3. Alice sends Bob the keys corresponding to her $x$. She convinces Bob they are correct.

4. Bob evaluates the encrypted circuit and outputs $f(x, y)$.

Building block: cryptosystem that requires two keys. You should learn nothing with only one key.
Encrypted AND gate:

\[
\begin{array}{c|c|c|c}
0 & 0 & 0 & \text{Enc}\left(\left(K_1^0, K_2^0\right), K_3^0\right) \\
0 & 1 & 0 & \text{Enc}\left(\left(K_1^0, K_2^1\right), K_3^0\right) \\
1 & 0 & 0 & \text{Enc}\left(\left(K_1^1, K_2^0\right), K_3^0\right) \\
1 & 1 & 1 & \text{Enc}\left(\left(K_1^1, K_2^1\right), K_3^1\right) \\
\end{array}
\]

randomly permute

Revised Protocol

1. Alice sends \((C_1, C_2, C_3, C_4)\) to Bob.

2. Bob learns \(K_2^0\) via OT.

3. Bob learns \(K_1^x\).

4. Bob decrypts the ciphertext corresponding to row \(x\ y\). He outputs the result, \(\text{AND}(x,y)\).

To encrypt the whole circuit, Alice picks keys for every wire \(i\), \((K_i^0, K_i^1)\). Let the \(j^{th}\) gate have truth table \((t_{00}, t_{01}, t_{10}, t_{11})\). Take input wires \(W_{j,0}\) and \(W_{j,1}\), and output wire \(W_{j,3}\). The \(j^{th}\) encrypted gate is:

\[
\begin{align*}
t_{00} & \Rightarrow \text{Enc}\left(\left(K_{W_{j,0}}^0, K_{W_{j,1}}^0\right), K_{W_{j,3}}^0\right) \\
t_{01} & \Rightarrow \text{Enc}\left(\left(K_{W_{j,0}}^0, K_{W_{j,1}}^1\right), K_{W_{j,3}}^0\right) \\
t_{10} & \Rightarrow \text{Enc}\left(\left(K_{W_{j,0}}^1, K_{W_{j,1}}^0\right), K_{W_{j,3}}^1\right) \\
t_{11} & \Rightarrow \text{Enc}\left(\left(K_{W_{j,0}}^1, K_{W_{j,1}}^1\right), K_{W_{j,3}}^1\right)
\end{align*}
\]
Another type of secure 2PC for set intersection:

Alice
\[ A = \{ a_1, a_2, \ldots, a_k \} \]

Bob
\[ \{ b \} = B \]

\[ C = A \cap B \]

Alice picks a polynomial \( p_A \) s.t. \( p_A(a_i) = 0 \quad \forall i \)
\[ p_A(x) \neq 0 \quad \forall x \text{ s.t. } x \neq a_i \quad \forall i \]

(modulo a large enough \( q \))

Let \( p_A(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_k x^k \). Use additively homomorphic encryption, so \( \widehat{x} \oplus \widehat{y} = \widehat{x+y} \), where boxes denote encryption.

Alice
\[ d_0, d_1, \ldots, d_k \]

Bob

Compute \( d_i b \) via repeated doubling.

\[ d_0 + d_1 b + d_2 b^2 + \ldots + d_k b^k \]

which is \( p_A(b) \).

Pick a random \( r \).

\[ p_A(b) \cdot r \]

\[ p_A(b) \cdot r \equiv 0 \]