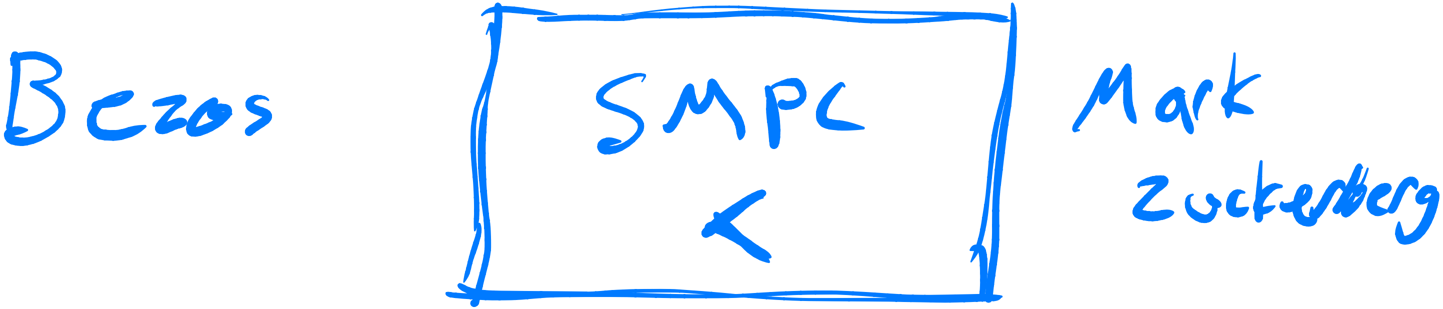
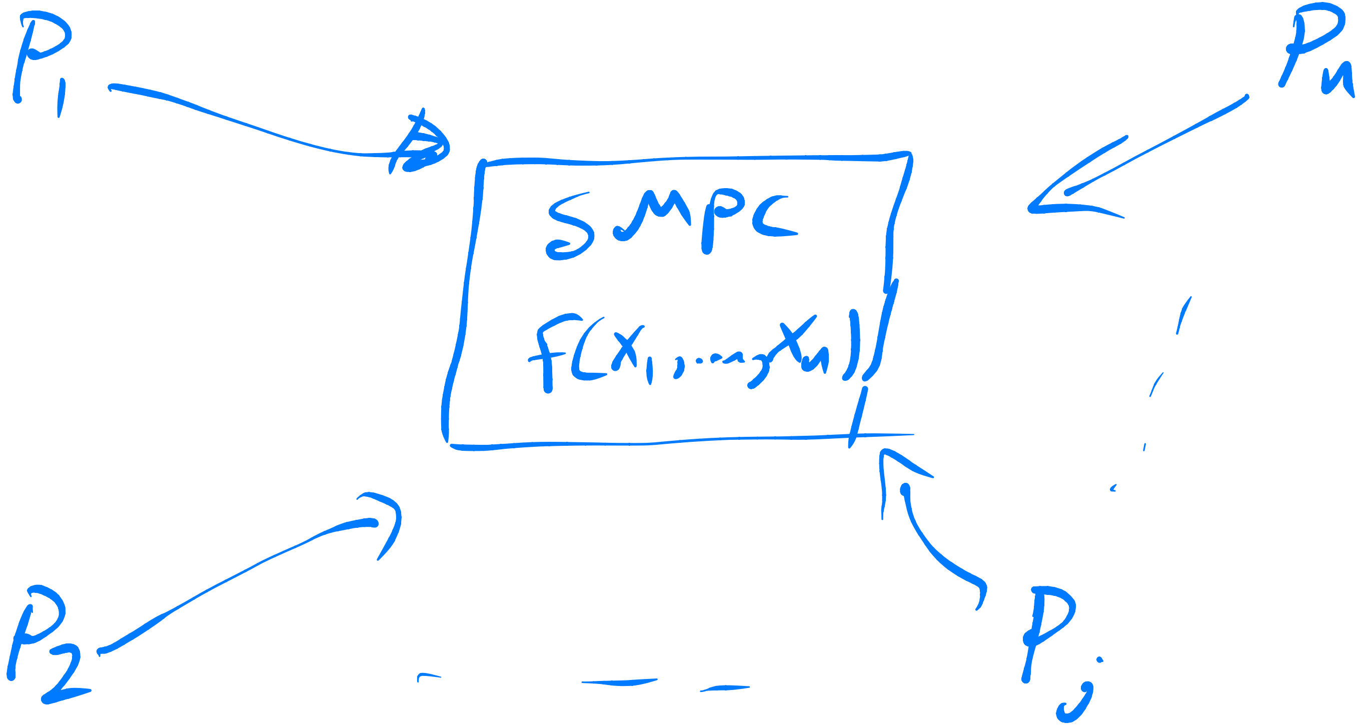
- secure multi-party computation
- secret sharing

Secure multi-party computation

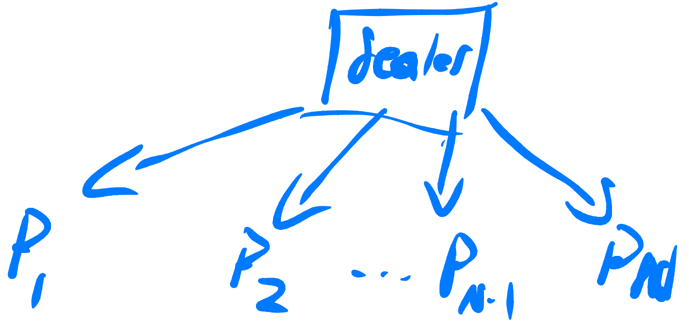
Yao's millionaire problem




P_1
P_n
SMPC
$f(x_1,\ldots,x_n)$
P_2
P_j

Secret Sharing

- "split" secret across parties



"split" secret

Property: $K < N$, any K can't reconstruct

$K+1$ can reconstruct