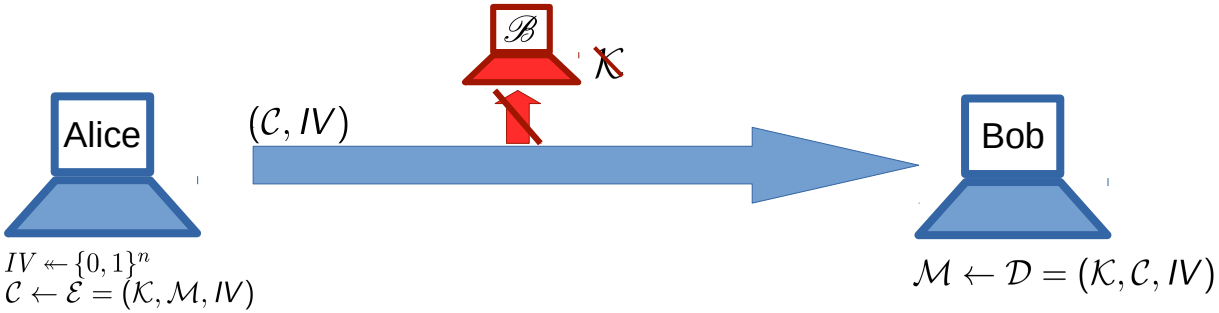
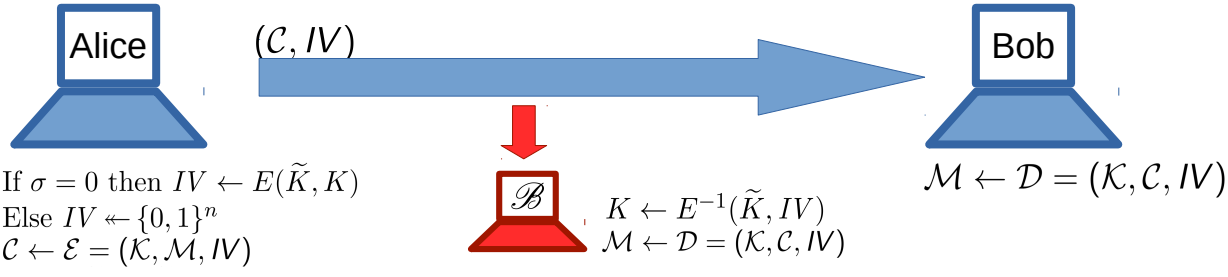

$\mathscr{B}$
K
Alice
(C, IV)
Bob
$IV \twoheadleftarrow \{0,1\}^n$
$C \leftarrow \mathcal{E} = (K, M, IV)$
$M \leftarrow \mathcal{D} = (K, C, IV)$


Alice
(C, IV)
Bob
If $\sigma = 0$ then $IV \leftarrow E(\widetilde{K}, K)$
Else $IV \twoheadleftarrow \{0,1\}^n$
$C \leftarrow \mathcal{E} = (K, M, IV)$
$\mathscr{B}$
$K \leftarrow E^{-1}(\widetilde{K}, IV)$
$M \leftarrow \mathcal{D} = (K, C, IV)$