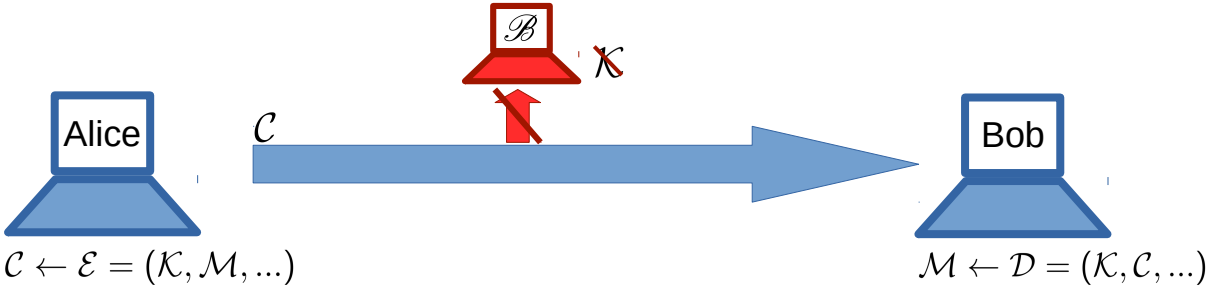
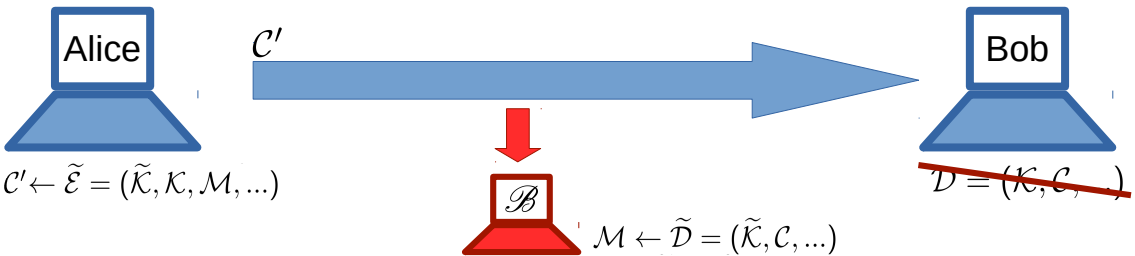

Alice
$\mathcal{B}$
$\mathcal{K}$
$\mathcal{C}$
Bob
$\mathcal{C} \leftarrow \mathcal{E} = (\mathcal{K}, \mathcal{M}, ...)$
$\mathcal{M} \leftarrow \mathcal{D} = (\mathcal{K}, \mathcal{C}, ...)$


Alice
$\mathcal{C}'$
Bob
$\mathcal{C}' \leftarrow \widetilde{\mathcal{E}} = (\widetilde{\mathcal{K}}, \mathcal{K}, \mathcal{M}, ...)$
$\mathcal{B}$
$\mathcal{D} = (\mathcal{K}, \mathcal{C}, ...)$
$\mathcal{M} \leftarrow \widetilde{\mathcal{D}} = (\widetilde{\mathcal{K}}, \mathcal{C}, ...)$