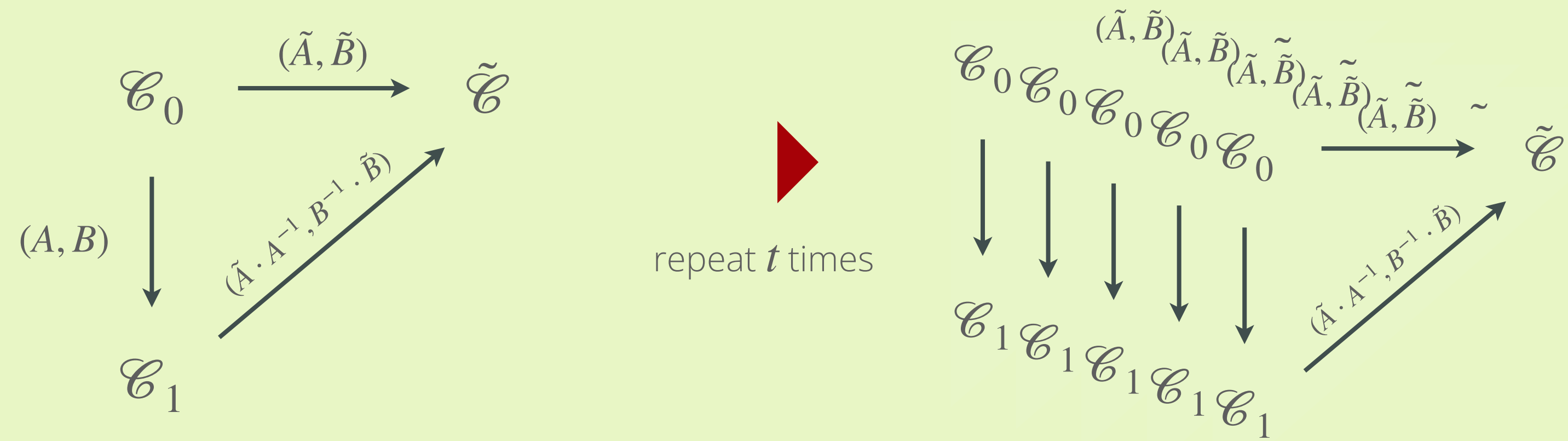




From MCE  
to MEDS

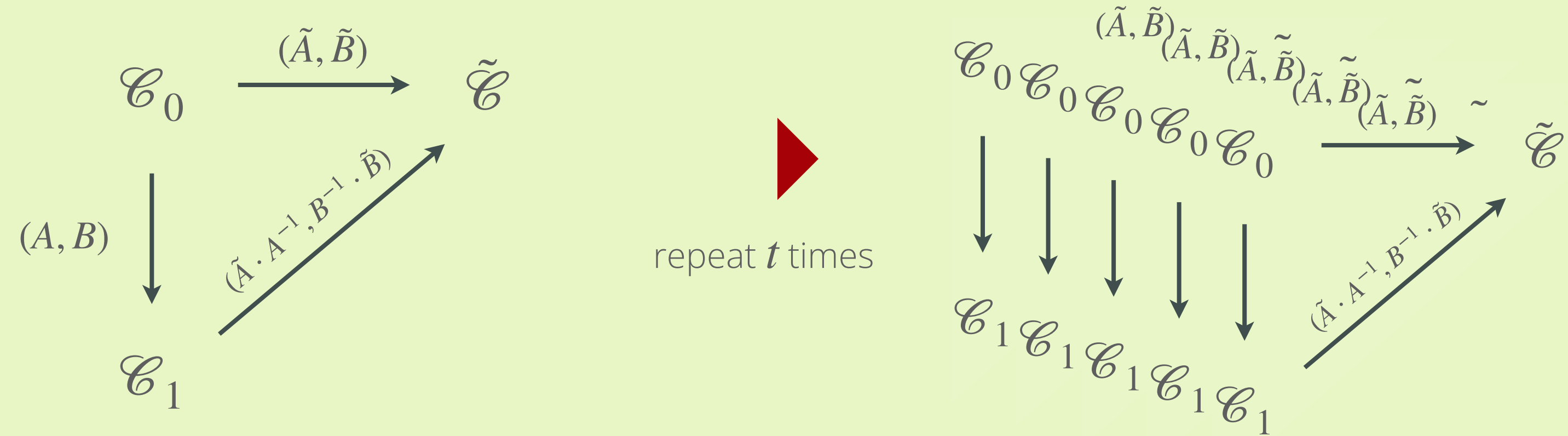
naive approach



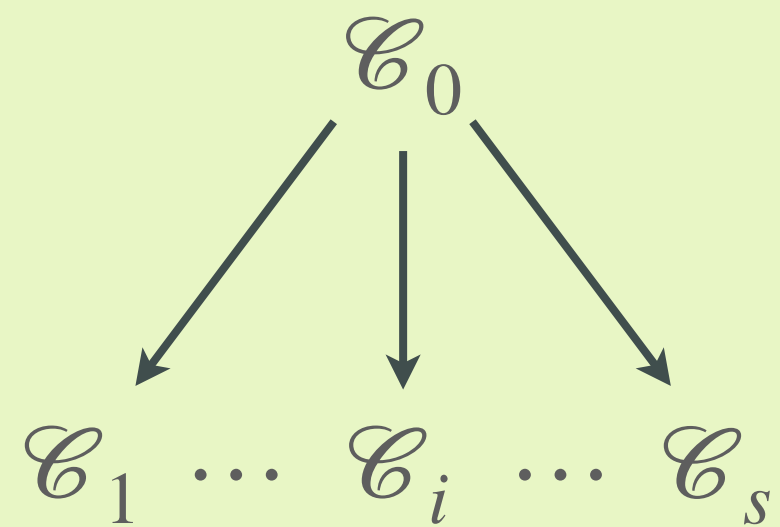


**From MCE  
to MEDS**

**naive approach**



**multiple pk**



provide  $s$  public keys,  $b \in \{0, \dots, s\}$   
response is isometry  $\mathcal{C}_b \rightarrow \tilde{\mathcal{C}}$