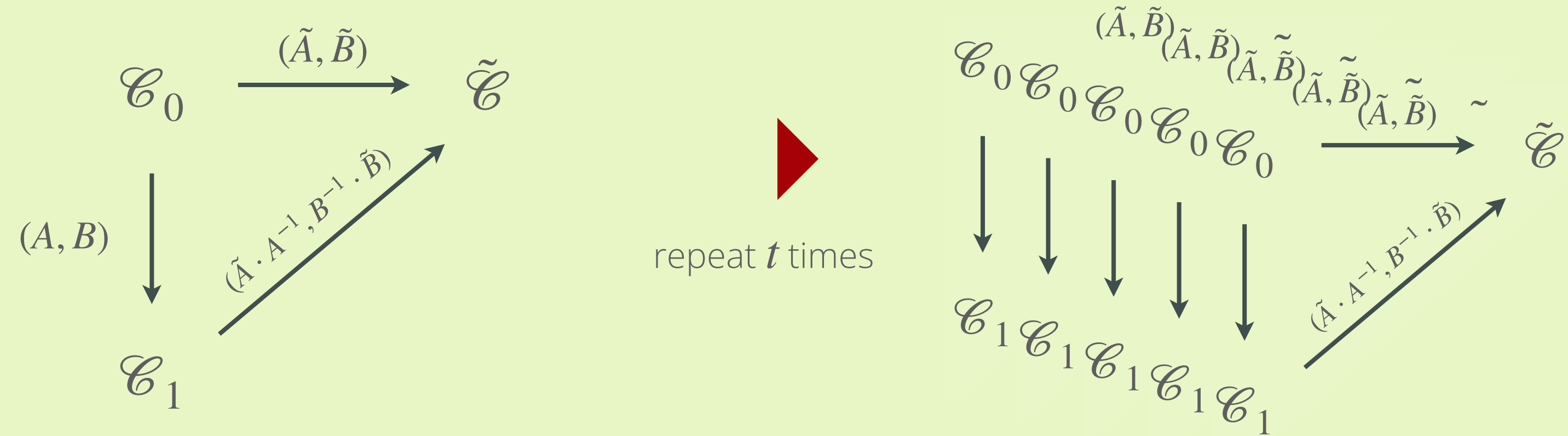




**From MCE
to MEDS**

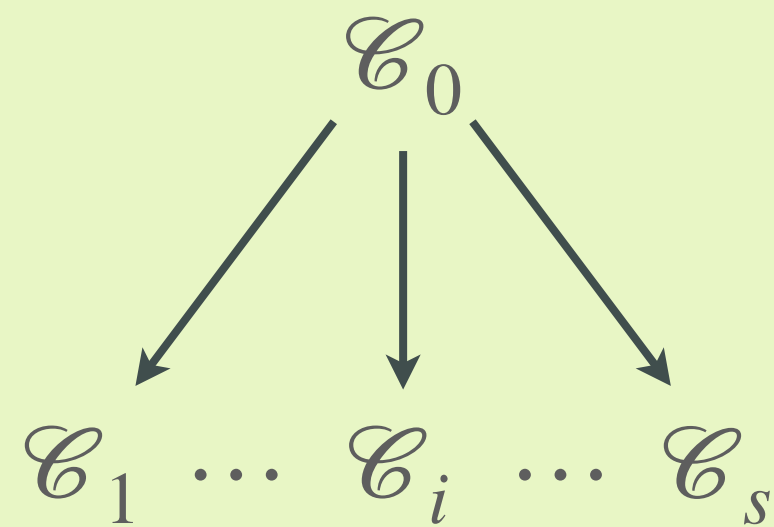
naive approach



1

[1]

multiple pk



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

2

[2]

fix weight

- generate $\mathcal{C}_0 \rightarrow \tilde{\mathcal{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

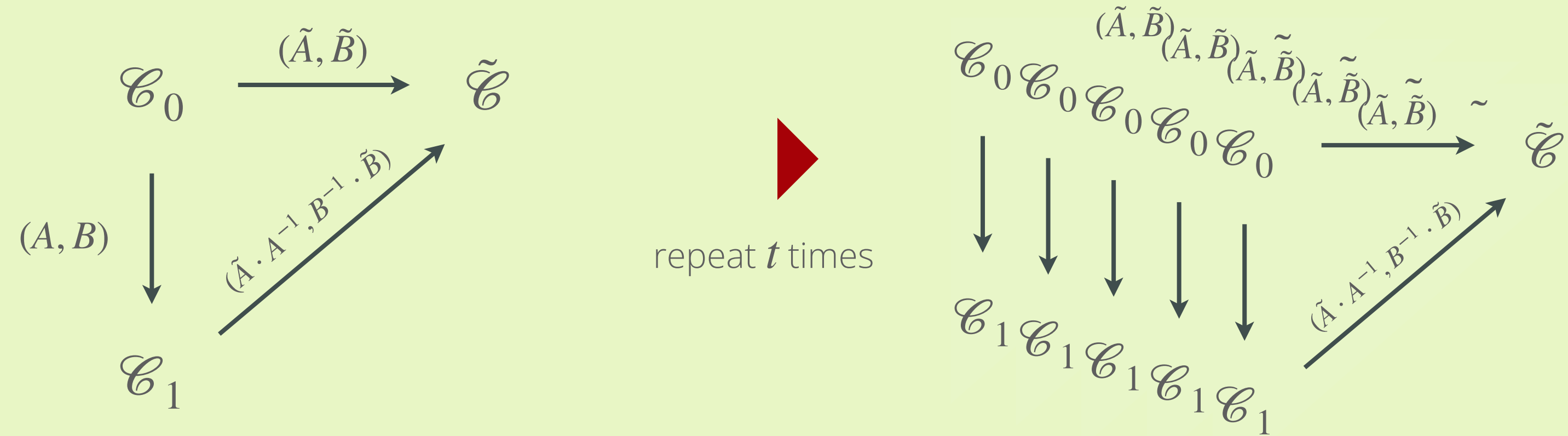


adjust probability so that
 $b = 0$ appears more



**From MCE
to MEDS**

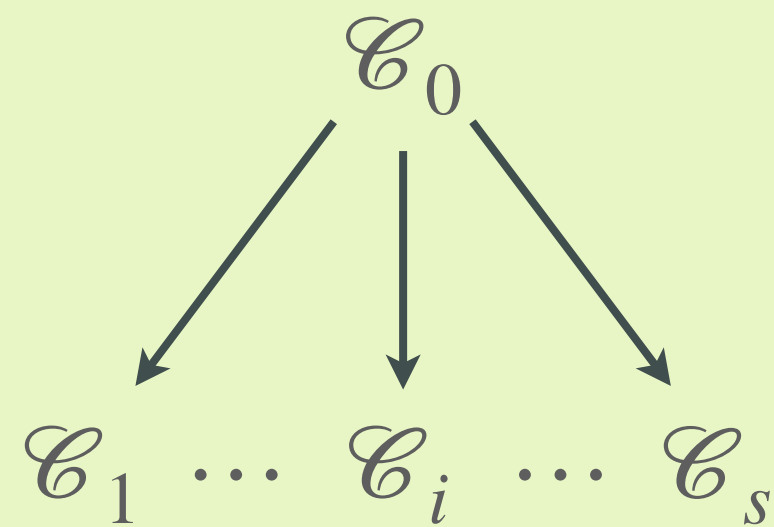
naive approach



1

multiple pk

[1]



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

2

fix weight

[2]

- generate $\mathcal{C}_0 \rightarrow \tilde{\mathcal{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!



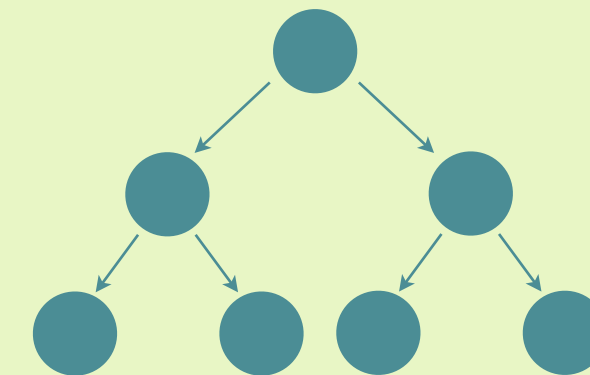
adjust probability so that
 $b = 0$ appears more

3

seed tree

[2]

instead of sending t seeds, send tree



to reveal nodes N_1, \dots, N_w , communicate
 N_1, \dots, N_w and for the $t - w$ remaining
nodes only appropriate parent nodes