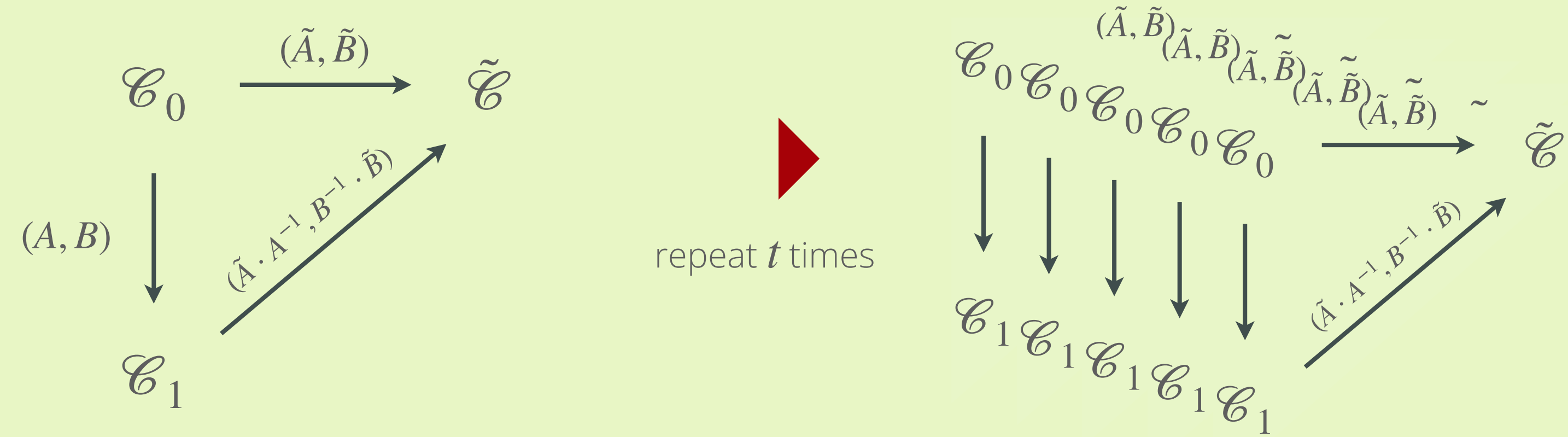


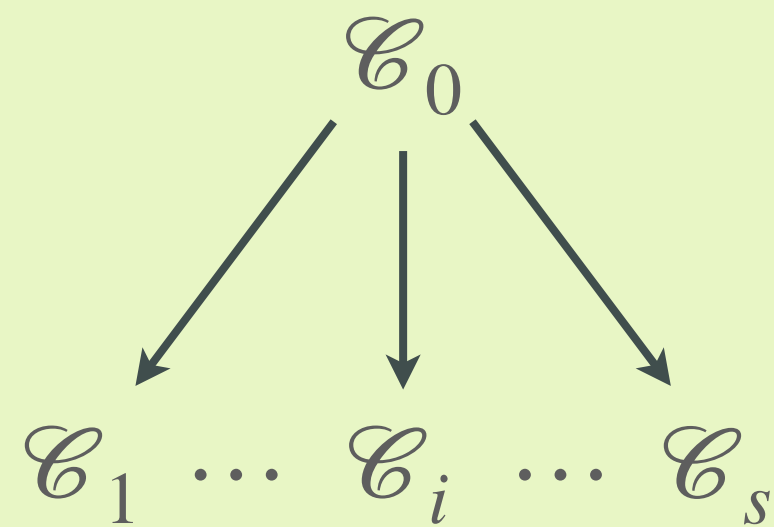


**From MCE
to MEDS**

naive approach



multiple pk



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

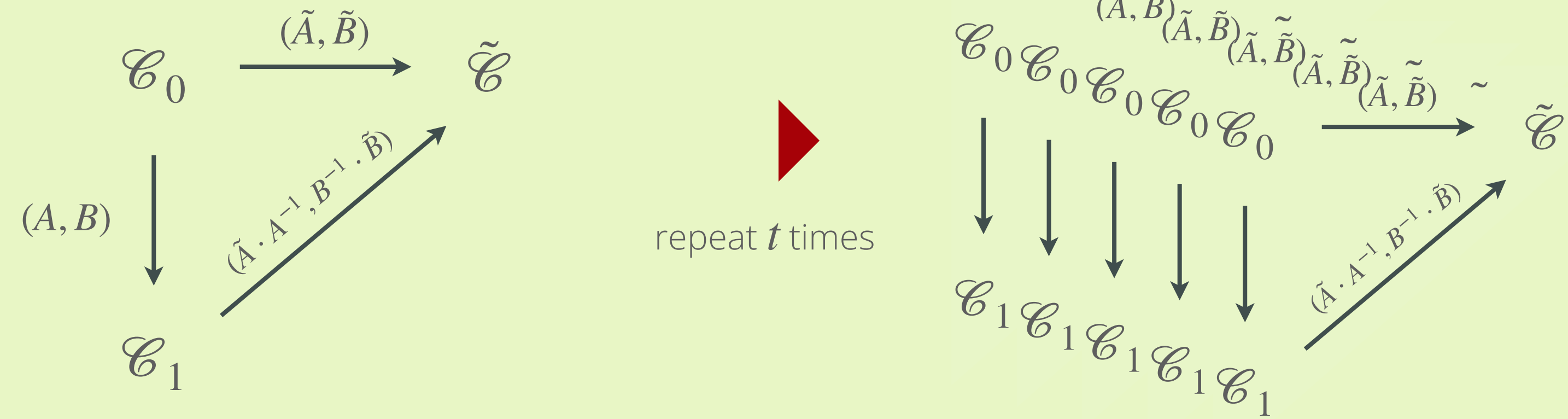
[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.

[2] W. Beullens, S. Katsumata, and F. Pintore. Calamari and Falafel: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.



From MCE to MEDS

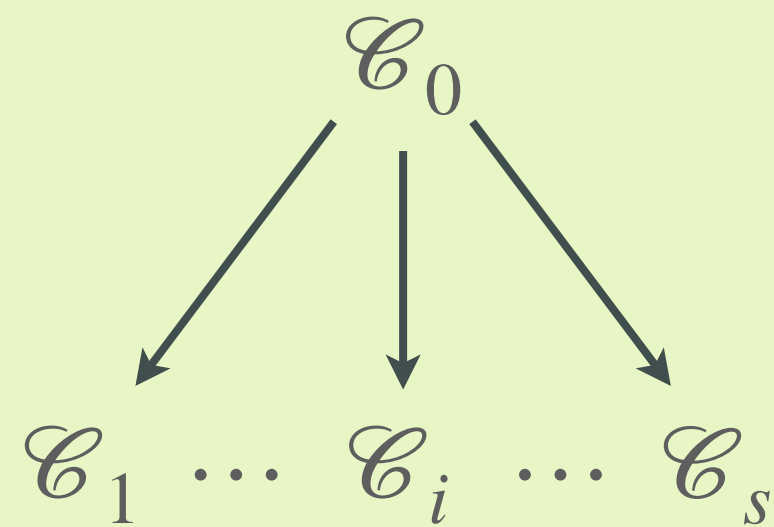
naive approach



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

[1] L. De Feo and S. D. Galbraith. SeaSign: Compact isogeny signatures from class group actions. EUROCRYPT 2019.

[2] W. Beullens, S. Katsumata, and F. Pintore. Calamari and Falafel: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.