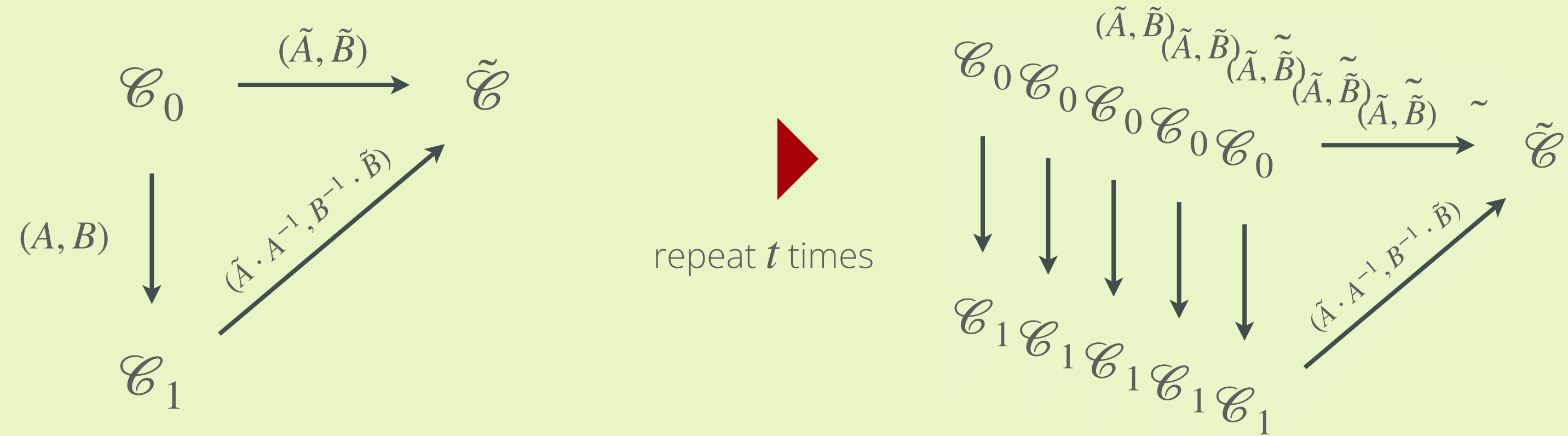




From MCE to MEDS

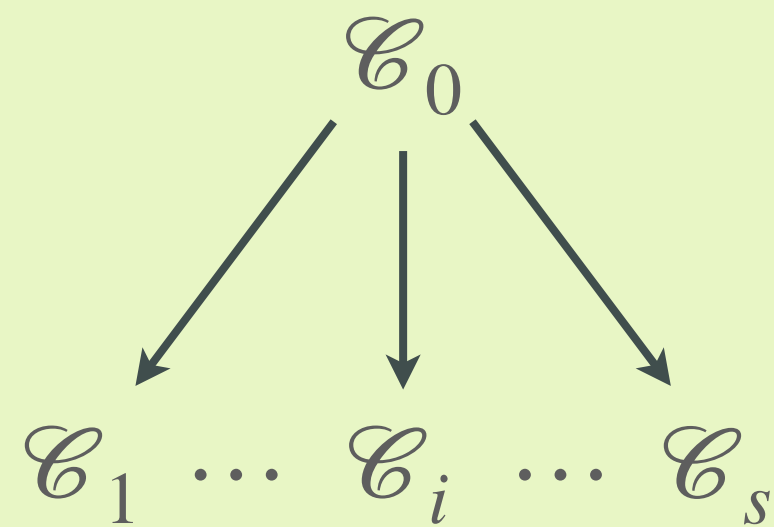
naive approach



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!



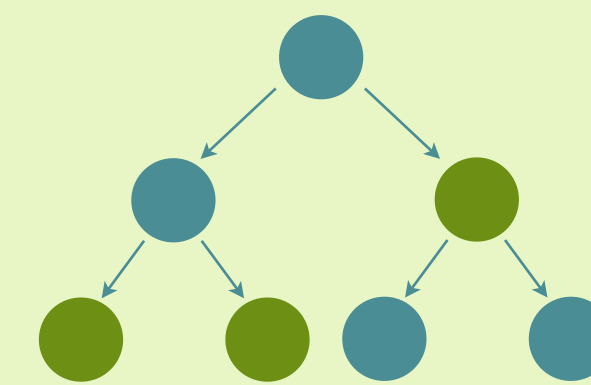
adjust probability so that
 $b = 0$ appears more

3

seed tree

[2]

instead of sending t seeds, send tree



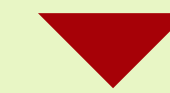
to reveal nodes N_1, \dots, N_w , communicate
 N_1, \dots, N_w and for the $t - w$ remaining
nodes only appropriate parent nodes

4

compression

[3,4]

instead of generating A_i, B_i from seed
and computing $\mathcal{C}_i = A_i \cdot \mathcal{C}_0 \cdot B_i$



generate part of \mathcal{C}_i from seed.
compute appropriate A_i, B_i
and rest of \mathcal{C}_i

Hint: this does not break MCE!

[3] J. Ding, M-S Chen, A. Petzoldt, D. Schmidt, B-Y. Yang, M. Kannwischer, and J. Patarin. Rainbow. NIST 2020.

[4] W. Beullens, M-S. Chen, S-H. Hung, M. Kannwischer, B. Peng, C-J. Shih, and B-Y. Yang. Oil and Vinegar: Modern parameters and implementations.

Performance of MEDS