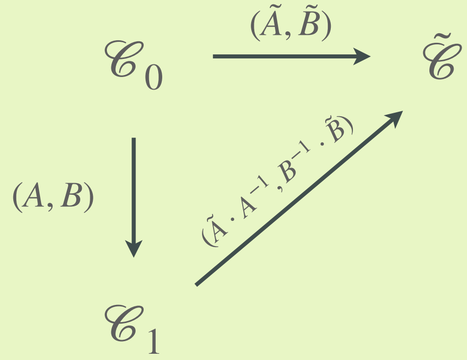
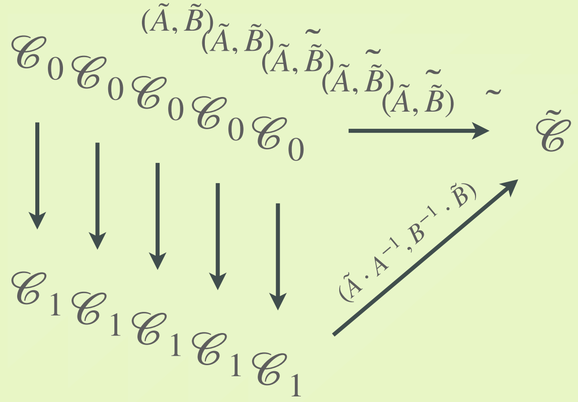
From MCE to MEDS

naive approach

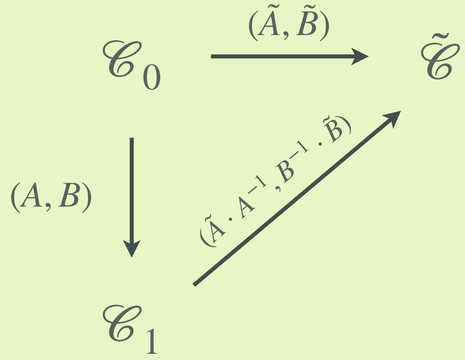


repeat t times

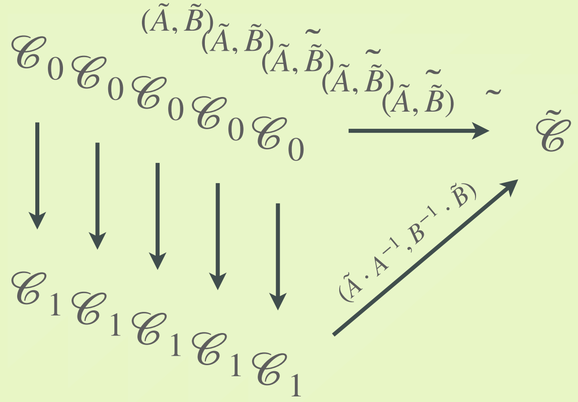


From MCE to MEDS

naive approach



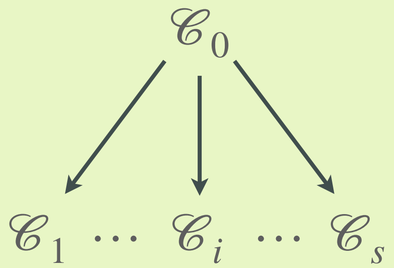
repeat t times



1

[1]

multiple pk



provide s public keys, $b \in \{0,\ldots,s\}$
response is isometry $\mathscr{C}_b \to \tilde{\mathscr{C}}$

[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 Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. ASIACRYPT 2020.