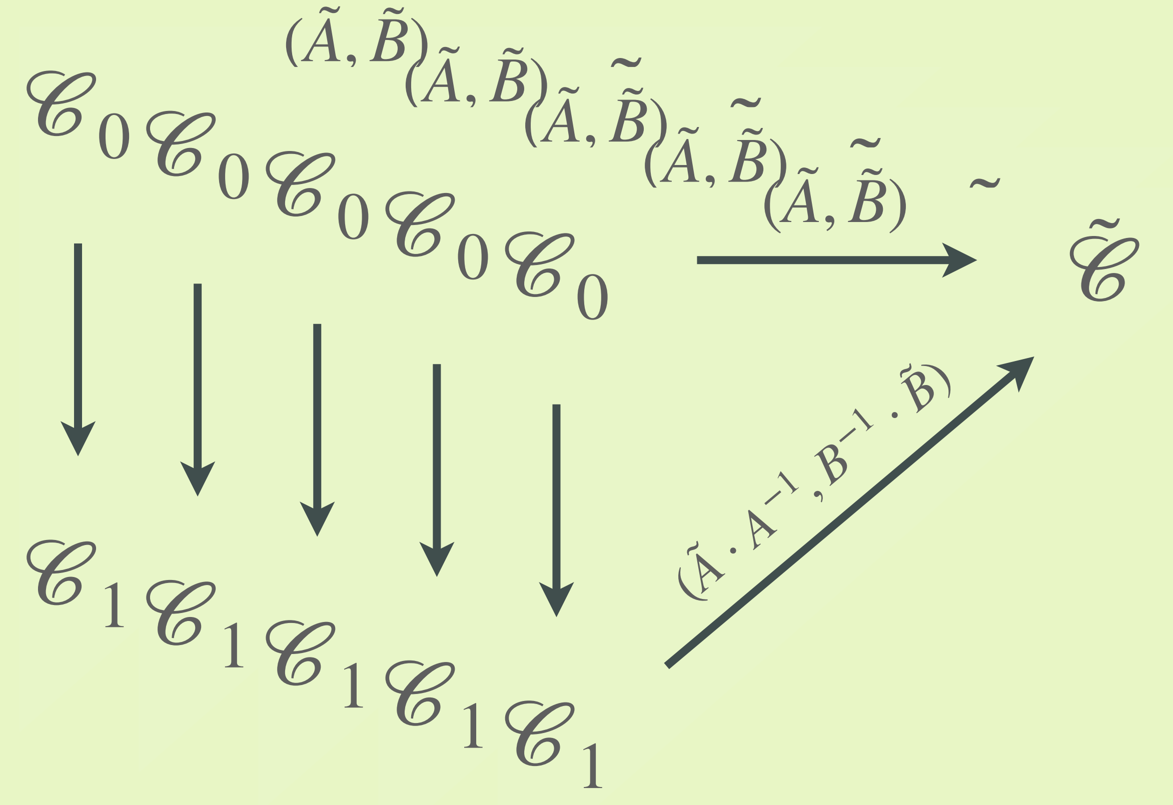
2

From MCE to MEDS

naive approach

$$\begin{tikzcd}
\mathscr{C}_0 \arrow[r, "(\tilde{A},\tilde{B})"] \arrow[d, "(A,B)"'] & \tilde{\mathscr{C}} \\
\mathscr{C}_1 \arrow[ur, "(\tilde{A}\cdot A^{-1},B^{-1}\cdot\tilde{B})"] &
\end{tikzcd}$$

repeat t times



1 [1]

multiple pk

$$\begin{tikzcd}
 & \mathscr{C}_0 \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathscr{C}_1 \;\cdots & \mathscr{C}_i & \cdots\; \mathscr{C}_s
\end{tikzcd}$$

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

2 [2]

fix weight

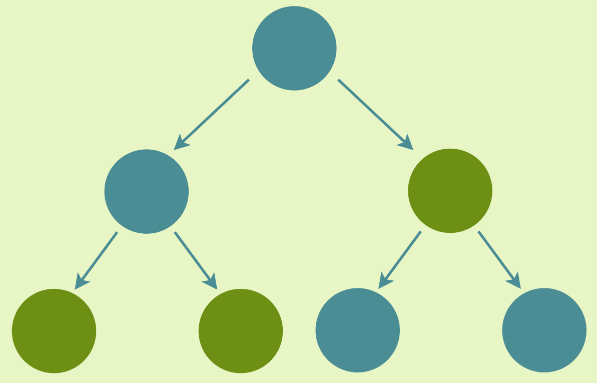
- generate $\mathscr{C}_0 \rightarrow \tilde{\mathscr{C}}$ from seed
- respond to $b = 0$ with seed
- response much cheaper!

adjust probability so that
$b = 0$ appears more

3 [2]

seed tree

instead of sending t seeds, send tree



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

4 [3,4]

compression

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

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

Hint: this does not break MCE!

[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.

[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