

For each α , choose random $x_v \in \mathbb{Q}[Z_2^k]$