# Thoughts on Parallelizable Hashing

## #1 Preference for degree growing with length

- Can't predict who will hash it again
- Fixed degree is simpler, but more suitable with interactivity

## #2 Interleaving of whole block(s)

- Atomic "absorbing of one block"
- Keeps serial fallback implementations simpler

## #3 How to deal with a security proof of $\mathcal{T}^{\mathsf{SHA2}}$ ?

- Indifferentiability of $\mathcal{T}^{\mathcal{F}}$ from indiff. of $\mathcal{F}$
- Use $\mathcal{F} = \mathsf{HMAC}_{K=0}^{\mathsf{SHA2}}$ ?

## #4 Wish for something simple and clean