PROPERTIES OF SCHEDULER

① integrity-preserving.

$$\text{if} \quad \alpha_c(t_s) = t_s' \quad \text{then} \quad \forall t \in t_s'.\ t \in t_s$$

that is the scheduler does not modify tasks

② for TSNI: eventual progress

$$\text{if } |t_s| > 1 \text{ then } \alpha_{step}(\alpha_{step}(t_s)) \neq \alpha_{step}(t_s)$$

③ non-interfering

=> can't make decision on high data when less sensitive threads exist. However, it's ok to use public information to schedule public/secret threads.

how to accomodate for this?

① modify configurations to track label on the current label:

$$\langle \Sigma, \ell \rangle^{i}_{\iota @ \ell'} \longleftarrow \text{label on } \ell$$

- 1st thread label on CL is $\bot$
- modify I-Sandbox:

$$\frac{t_{new} = \langle \Sigma', \ell \rangle^{i'}_{\ell @ \ell} \quad \ldots\ldots}{\Sigma; \langle \Sigma, E[\text{sandbox } e]_I \rangle^{i}_{\ell @ \ell'}, \ldots \xhookrightarrow{\alpha} \Sigma'; \alpha_{sandbox}(t_1, \ldots, t_{new})}$$

- define erasure for threadpools (only for scheduler thm)

$$\mathcal{E}_{\ell_A}\left(\langle \Sigma', e \rangle^{i'}_{\ell @ \ell'}\right) = \begin{cases} \langle \bullet \rangle^{i'} & \text{if } \ell' \not\sqsubseteq \ell_A \\ \langle \underset{\substack{\uparrow \\ \text{apply } \mathcal{E}_{\ell_A} \text{ homomorphically}}}{\Sigma'}, e \rangle^{i'}_{\ell @ \ell'} & \text{otherwise} \end{cases}$$

Def with this in place we say that scheduler $\alpha_c : ts \to ts$ is non-interferent if $\mathcal{E}_\ell(ts_1) = \mathcal{E}_\ell(ts_2)$

$\alpha_c(ts_1) = ts_1'$, $\alpha_c(ts_2) = ts_2'$

and $\mathcal{E}_\ell(ts_1') = \mathcal{E}_\ell(ts_2')$

where $\ell = \sqcap$ label on label of all task in ts