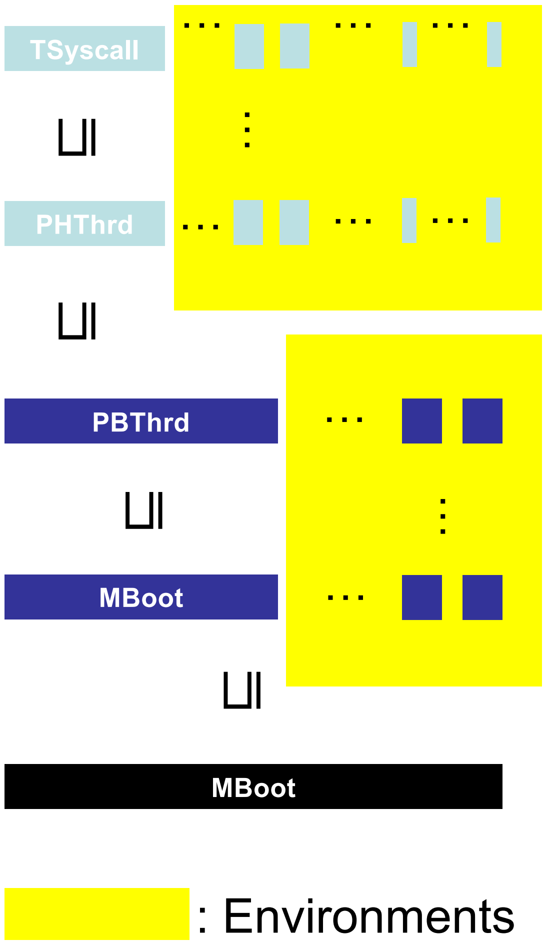
(2) Section 5.2

(3) Section 5.3

(1) Section 5.1

(4) Section 5.4

CertiKOS Structure



Theorems

$$\llbracket \mathbf{Tsyscall}[tid, \varepsilon'_{\mathrm{thrd}}]\langle \mathbf{Ctxt} \rangle \rrbracket_{\mathrm{mach}_{\mathrm{HAsm}}}$$

$$\sqsupseteq$$

$$\llbracket \mathbf{PHThrd}[tid, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\mathrm{mach}_{\mathrm{HAsm}}}$$

$$\sqsupseteq$$

$$\left\llbracket \mathbf{PBThrd}\left[cid, \varepsilon'_{\mathrm{cpu}}\right]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rangle \right\rrbracket_{\mathrm{mach}_{\mathrm{LAsm}}}$$

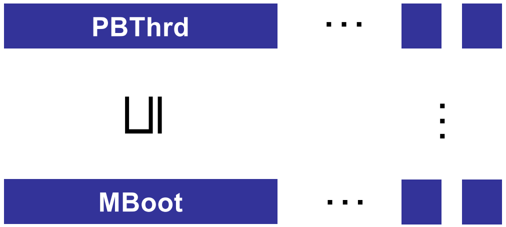
$$\sqsupseteq$$

$$\left\llbracket \mathbf{MBoot}\left[cid, \varepsilon_{\mathrm{cpu}}\right]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rangle \right\rrbracket_{\mathrm{mach}_{\mathrm{LAsm}}}$$

$$\sqsupseteq$$

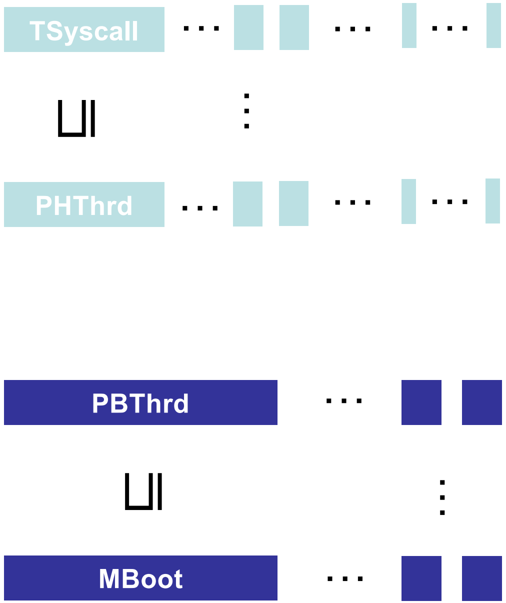
$$\llbracket \mathbf{MBoot}\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rangle \rrbracket_{\mathrm{mach}_{\mathrm{x86}}}$$

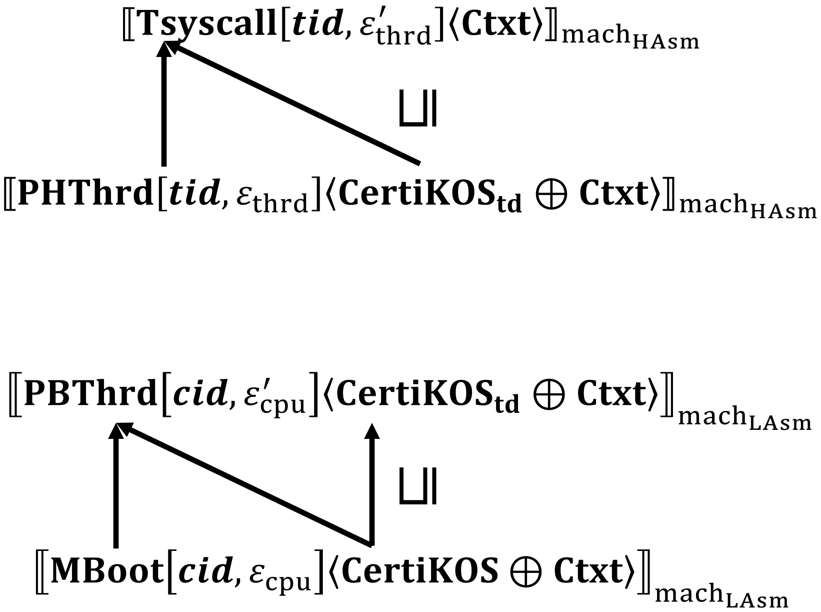
(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



$$\begin{tikzcd}
\llbracket \mathbf{PBThrd}[\boldsymbol{cid}, \varepsilon'_{\mathrm{cpu}}]\langle \mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}\rangle \rrbracket_{\mathrm{mach_{LAsm}}} \\
\llbracket \mathbf{MBoot}[\boldsymbol{cid}, \varepsilon_{\mathrm{cpu}}]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle \rrbracket_{\mathrm{mach_{LAsm}}} \arrow[u, "\sqsubseteq"']
\end{tikzcd}$$

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS_{cpu}} \oplus \mathbf{CertiKOS_{td}}$)





$[\![\mathbf{Tsyscall}[\boldsymbol{tid}, \varepsilon'_{\mathrm{thrd}}]\langle\mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$

$\sqsubseteq$

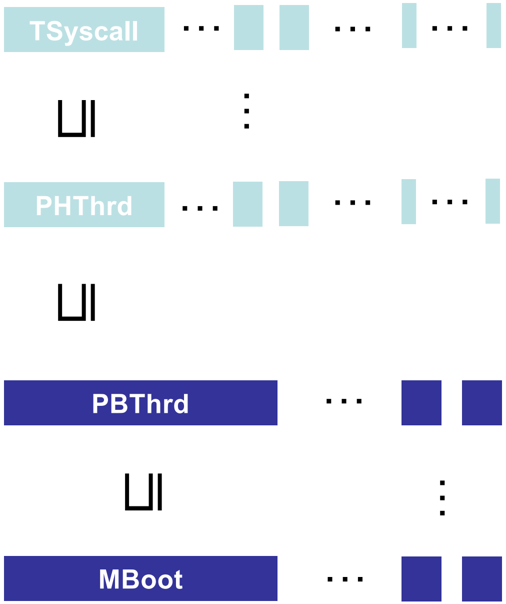
$[\![\mathbf{PHThrd}[\boldsymbol{tid}, \varepsilon_{\mathrm{thrd}}]\langle\mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$

$[\![\mathbf{PBThrd}[\boldsymbol{cid}, \varepsilon'_{\mathrm{cpu}}]\langle\mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$

$\sqsubseteq$

$[\![\mathbf{MBoot}[\boldsymbol{cid}, \varepsilon_{\mathrm{cpu}}]\langle\mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



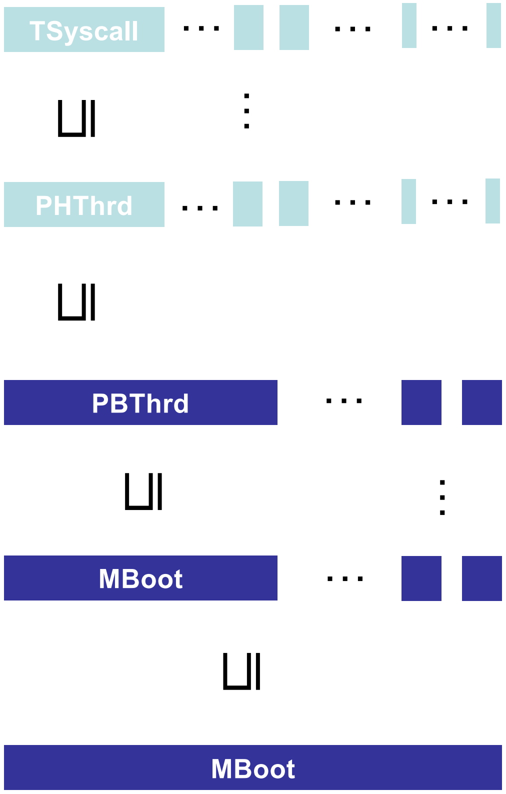
$$\begin{gathered}
[\![\mathbf{Tsyscall}[\boldsymbol{tid}, \varepsilon'_{\mathrm{thrd}}]\langle \mathbf{Ctxt} \rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}} \\
\rotatebox{90}{$\sqsubseteq$} \\
[\![\mathbf{PHThrd}[\boldsymbol{tid}, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}} \\
\rotatebox{90}{$\sqsubseteq$} \\
[\![\mathbf{PBThrd}[\boldsymbol{cid}, \varepsilon'_{\mathrm{cpu}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}} \\
\rotatebox{90}{$\sqsubseteq$} \\
[\![\mathbf{MBoot}[\boldsymbol{cid}, \varepsilon_{\mathrm{cpu}}]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}
\end{gathered}$$

(2)

(3)

(1)

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



$$[\![\mathbf{Tsyscall}[tid, \varepsilon'_{\mathrm{thrd}}]\langle \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$$

(2) $\sqsubseteq$

$$[\![\mathbf{PHThrd}[tid, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$$

(3) $\sqsubseteq$

$$[\![\mathbf{PBThrd}[cid, \varepsilon'_{\mathrm{cpu}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

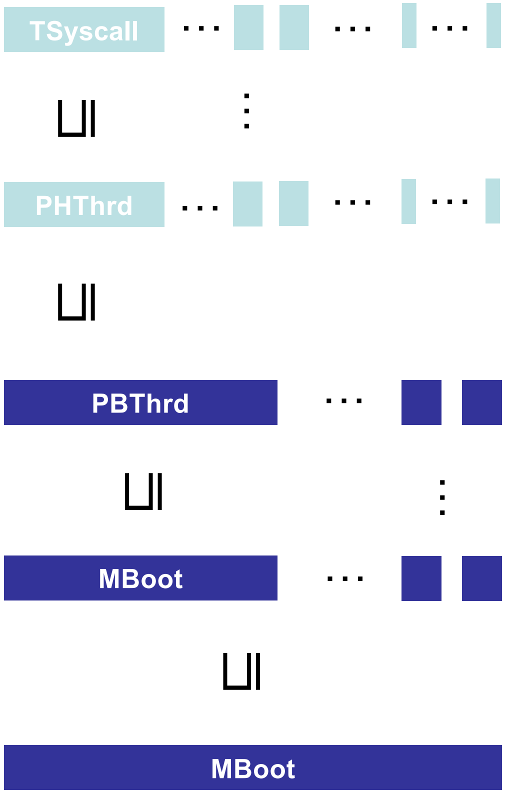
(1) $\sqsubseteq$

$$[\![\mathbf{MBoot}[cid, \varepsilon_{\mathrm{cpu}}]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

(4) $\sqsubseteq$

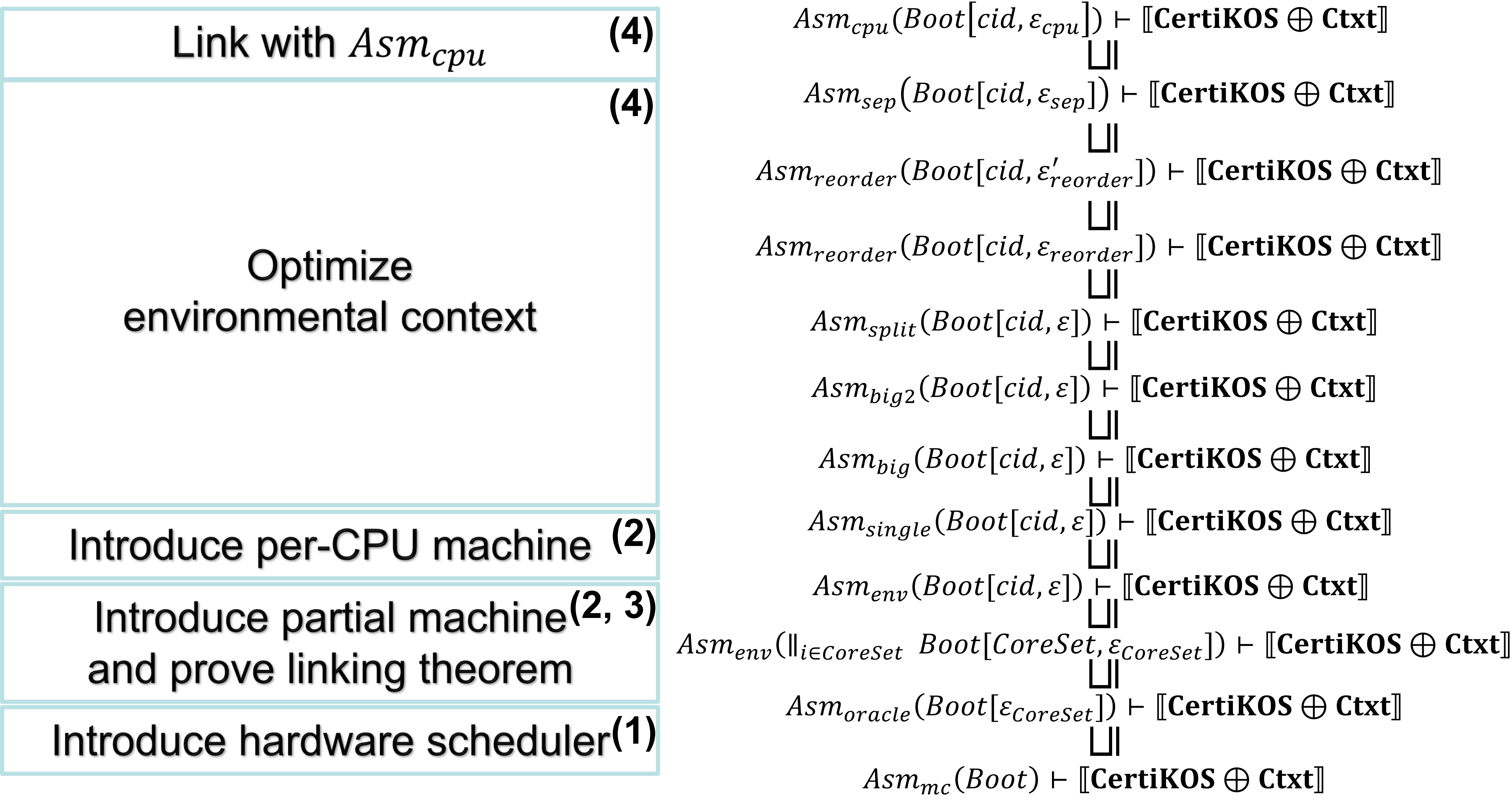
$$[\![\mathbf{MBoot}\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{x86}}}$$

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



$$\begin{array}{cc}
 & \llbracket \mathbf{Tsyscall}[\mathit{tid}, \varepsilon'_{\mathrm{thrd}}]\langle \mathbf{Ctxt}\rangle \rrbracket_{\mathrm{mach}_{\mathrm{HAsm}}} \\
(2) & \rotatebox{90}{$\sqsubseteq$} \\
 & \llbracket \mathbf{PHThrd}[\mathit{tid}, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle \rrbracket_{\mathrm{mach}_{\mathrm{HAsm}}} \\
(3) & \rotatebox{90}{$\sqsubseteq$} \\
 & \Big\llbracket \mathbf{PBThrd}\big[\mathit{cid}, \varepsilon'_{\mathrm{cpu}}\big]\langle \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt}\rangle \Big\rrbracket_{\mathrm{mach}_{\mathrm{LAsm}}} \\
(1) & \rotatebox{90}{$\sqsubseteq$} \\
 & \Big\llbracket \mathbf{MBoot}\big[\mathit{cid}, \varepsilon_{\mathrm{cpu}}\big]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle \Big\rrbracket_{\mathrm{mach}_{\mathrm{LAsm}}} \\
(4) & \rotatebox{90}{$\sqsubseteq$} \\
 & \llbracket \mathbf{MBoot}\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle \rrbracket_{\mathrm{mach}_{\mathrm{x86}}}
\end{array}$$

(where $\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}$)



Link with Asm_{cpu} (4)

Optimize environmental context (4)

Introduce per-CPU machine (2)

Introduce partial machine and prove linking theorem (2, 3)

Introduce hardware scheduler (1)

$$Asm_{cpu}(Boot[cid, \varepsilon_{cpu}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{sep}(Boot[cid, \varepsilon_{sep}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{reorder}(Boot[cid, \varepsilon'_{reorder}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{reorder}(Boot[cid, \varepsilon_{reorder}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{split}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{big2}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{big}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{single}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{env}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

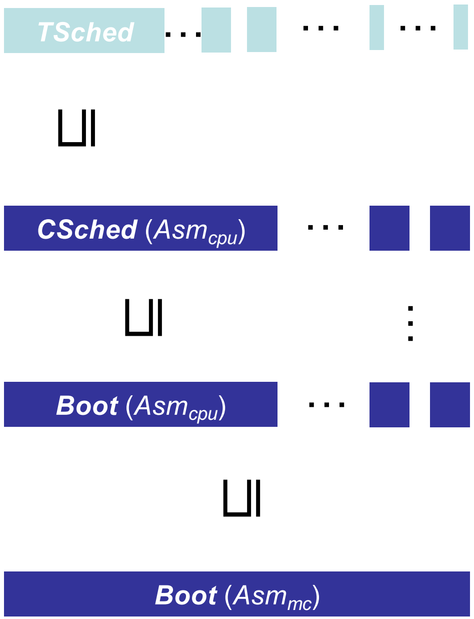
$$Asm_{env}(\|_{i \in CoreSet} \; Boot[CoreSet, \varepsilon_{CoreSet}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{oracle}(Boot[\varepsilon_{CoreSet}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$

$$\sqcup\!|$$

$$Asm_{mc}(Boot) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$



$$\mathit{Asm}_{thrd}(\mathit{TSched}[tid, \varepsilon'_{cpu}, \varepsilon_{thrd}]) \vdash \llbracket \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rrbracket$$

$$\sqsubseteq$$

$$\mathit{Asm}_{cpu}(\mathit{CSched}[cid, \varepsilon'_{cpu}]) \vdash \llbracket \mathbf{CertiKOS}_{\mathbf{td}} \oplus \mathbf{Ctxt} \rrbracket$$

$$\sqsubseteq$$

$$\mathit{Asm}_{cpu}(\mathit{Boot}[cid, \varepsilon_{ccpu}]) \vdash \llbracket \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rrbracket$$

$$\sqsubseteq$$

$$\mathit{Asm}_{mc}(\mathit{Boot}) \vdash \llbracket \mathbf{CertiKOS} \oplus \mathbf{Ctxt} \rrbracket$$

$$(\text{where } \boxed{\mathbf{CertiKOS} \coloneqq \mathbf{CertiKOS}_{\mathbf{cpu}} \oplus \mathbf{CertiKOS}_{\mathbf{td}}})$$

Link per-CPU machine compiler with per-thread machine (5)

Introduce per-thread machine (1, 2, 3)

Introduce multithreaded machine and prove linking theorem (1, 2, 3, 4)

$$Asm_{thrd}(PHThread[tid, \varepsilon'_{cpu}, \varepsilon_{thrd}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$IAsm_{thrd}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_{T}^{zip}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$IAsm_{mt}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_{T}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$IAsm_{mt}(\|_{ti \in TSet}\ PHBThread[cid, \varepsilon'_{cpu}\ ]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$Asm_{mt}(\|_{ti \in TSet}\ PHBThread[cid, \varepsilon'_{cpu}\ ]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqsubseteq$$

$$Asm_{cpu}(PBThread[cid, \varepsilon'_{cpu}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$