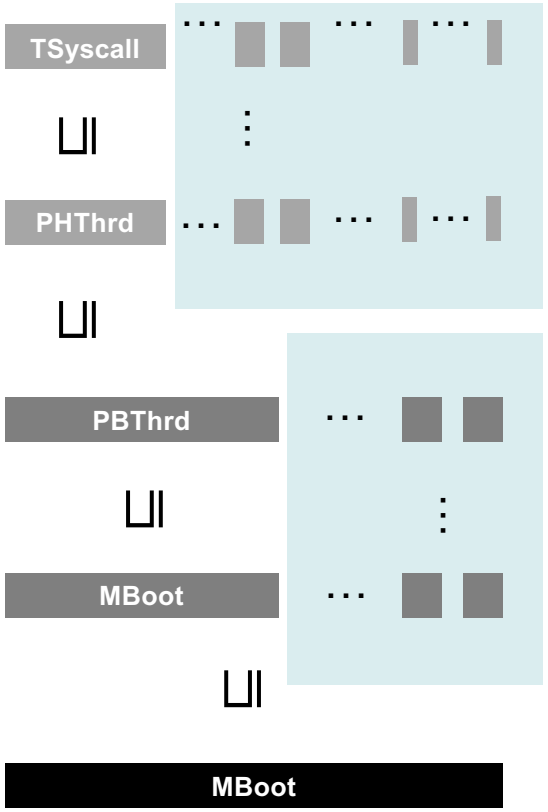
(2) Section 5.2

(3) Section 5.3

(1) Section 5.1

(4) Section 5.4

CertiKOS Structure



CertiKOS Theorems

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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

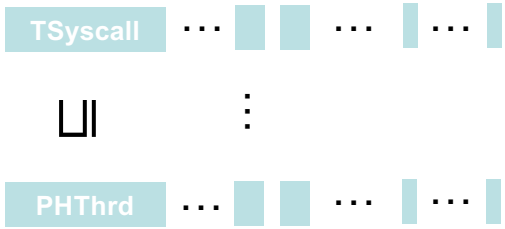
$$[\![\mathbf{MBoot}\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{x86}}}$$

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

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

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

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



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

$$\sqcup\!|$$

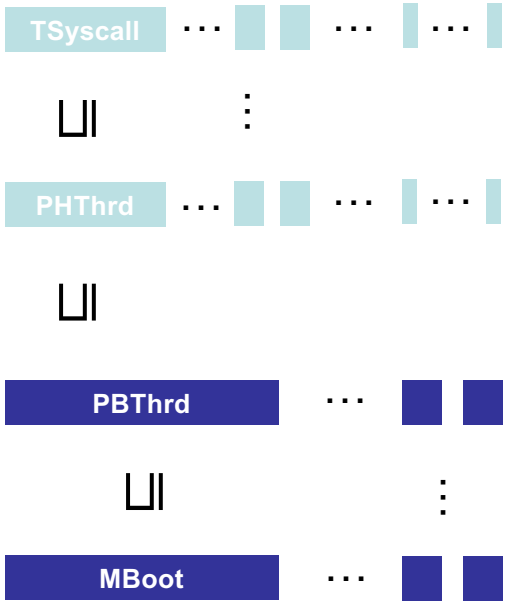
$$[\![\mathbf{PHThrd}[\boldsymbol{tid}, \varepsilon_{\mathrm{thrd}}]\langle \mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{HAsm}}}$$

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

$$\sqcup\!|$$

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

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



(2)

(3)

(1)

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

$$\sqcup\!|$$

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

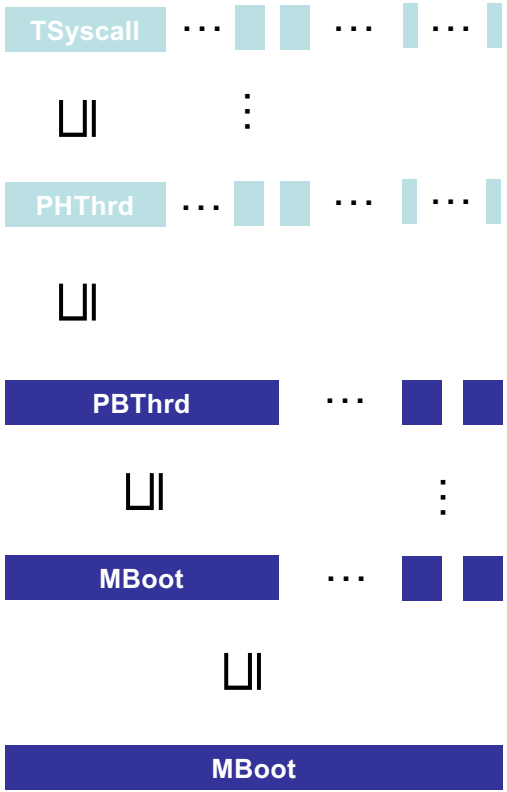
$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

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



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

(2)

$$\sqcup\!|$$

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

(3)

$$\sqcup\!|$$

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

(1)

$$\sqcup\!|$$

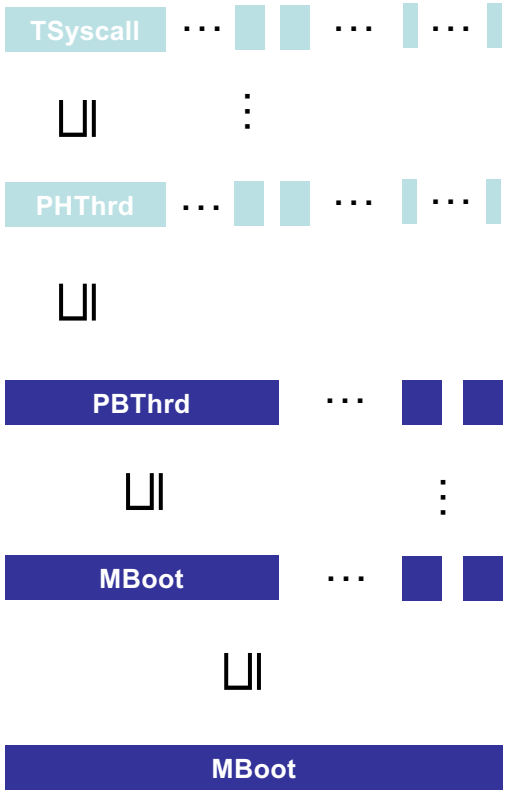
$$[\![\mathbf{MBoot}[\boldsymbol{cid}, \varepsilon_{\mathrm{cpu}}]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

(4)

$$\sqcup\!|$$

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

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



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

(2)

$$\sqcup\!|$$

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

(3)

$$\sqcup\!|$$

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

(1)

$$\sqcup\!|$$

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

(4)

$$\sqcup\!|$$

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

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

Link with Asm_{cpu} **(4)**

(4)

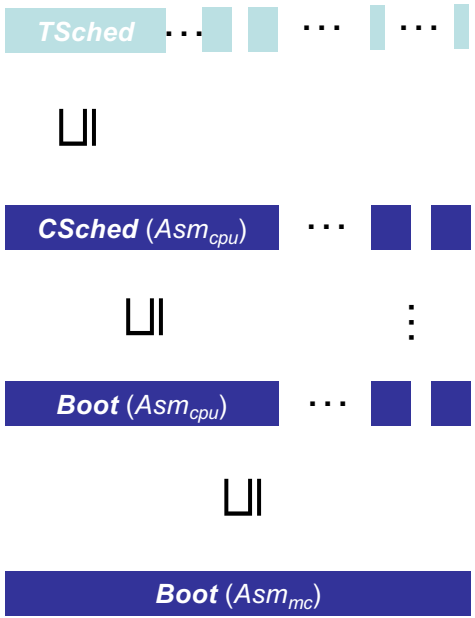
Optimize
environmental context

Introduce per-CPU machine **(2)**

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

Introduce hardware scheduler **(1)**

$$Asm_{cpu}(Boot[cid, \varepsilon_{cpu}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{sep}(Boot[cid, \varepsilon_{sep}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{reorder}(Boot[cid, \varepsilon'_{reorder}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{reorder}(Boot[cid, \varepsilon_{reorder}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{split}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{big2}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{big}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{single}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{env}(Boot[cid, \varepsilon]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{env}(\|_{i \in CoreSet}\ Boot[CoreSet, \varepsilon_{CoreSet}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{oracle}(Boot[\varepsilon_{CoreSet}]) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$
$$\sqcup\!|$$
$$Asm_{mc}(Boot) \vdash [\![\textbf{CertiKOS} \oplus \textbf{Ctxt}]\!]$$



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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

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

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)**

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

$$\sqcup|$$

$$IAsm_{thrd}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_T^{zip}]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqcup|$$

$$IAsm_{mt}(PHBThread[tid, \varepsilon'_{cpu}, \varepsilon_T]) \vdash [\![\mathbf{CertiKOS_{td}} \oplus \mathbf{Ctxt}]\!]$$

$$\sqcup|$$

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

$$\sqcup|$$

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

$$\sqcup|$$

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