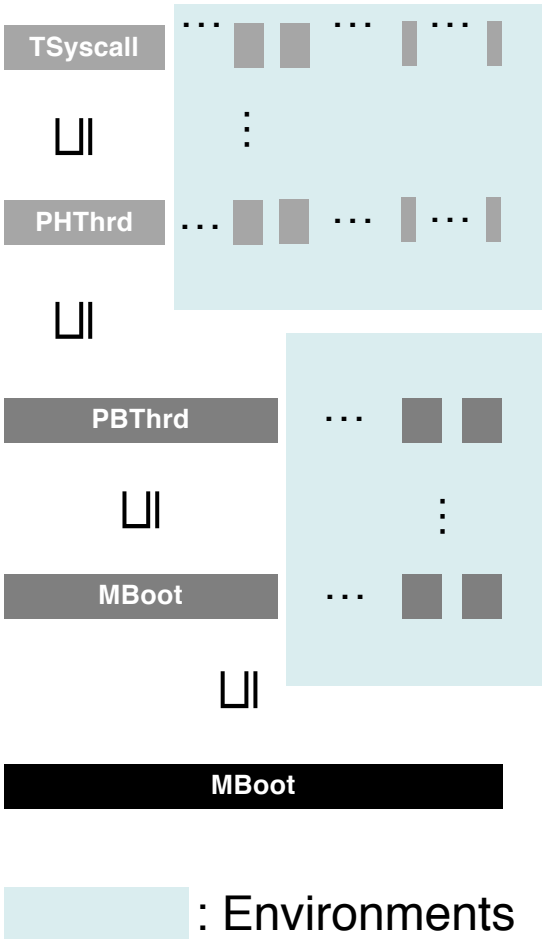
(2) Section 5.2

(3) Section 5.3

(1) Section 5.1

(4) Section 5.4

## CertiKOS Structure




## CertiKOS Theorems

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

$$\sqcup\!|$$

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

$$\sqcup\!|$$

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

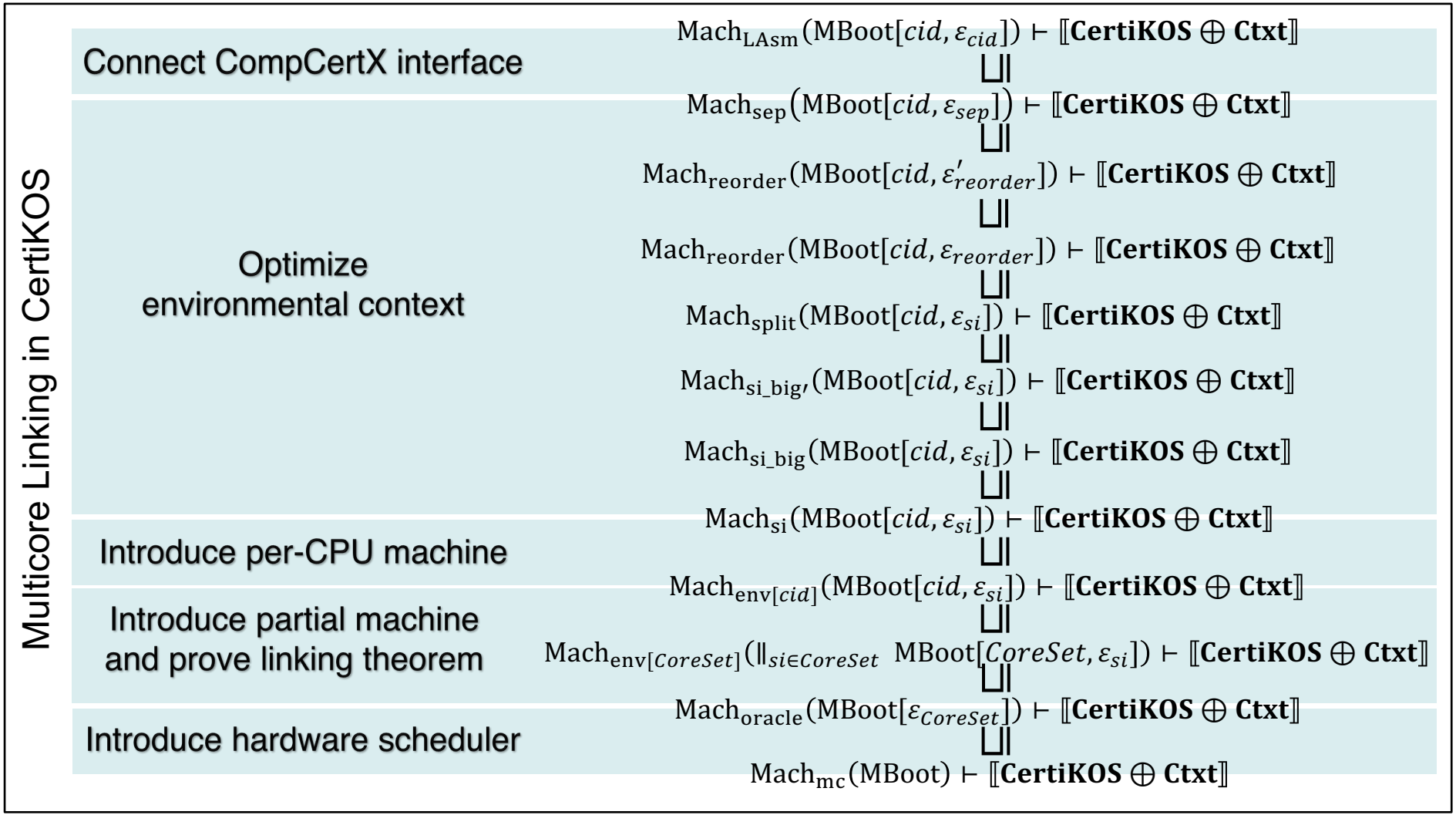
$$\sqcup\!|$$

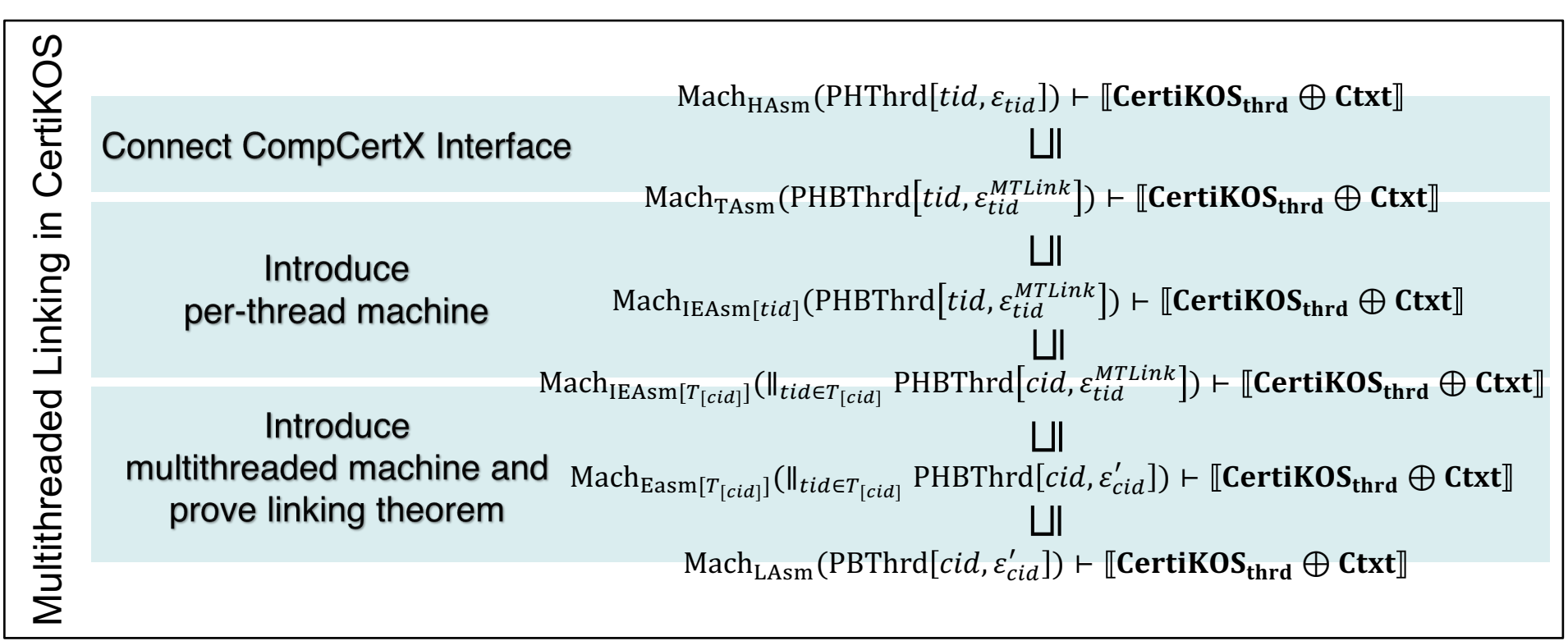
$$[\![\mathbf{MBoot}[cid, \varepsilon_{cid}]\langle \mathbf{CertiKOS} \oplus \mathbf{Ctxt}\rangle]\!]_{\mathrm{mach}_{\mathrm{LAsm}}}$$

$$\sqcup\!|$$

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

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


Multicore Linking in CertiKOS
Connect CompCertX interface
Optimize
environmental context
Introduce per-CPU machine
Introduce partial machine
and prove linking theorem
Introduce hardware scheduler
$\mathrm{Mach}_{\mathrm{LAsm}}(\mathrm{MBoot}[cid, \varepsilon_{cid}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{sep}}(\mathrm{MBoot}[cid, \varepsilon_{sep}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{reorder}}(\mathrm{MBoot}[cid, \varepsilon'_{reorder}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{reorder}}(\mathrm{MBoot}[cid, \varepsilon_{reorder}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{split}}(\mathrm{MBoot}[cid, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{si\_big'}}(\mathrm{MBoot}[cid, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{si\_big}}(\mathrm{MBoot}[cid, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{si}}(\mathrm{MBoot}[cid, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{env}[cid]}(\mathrm{MBoot}[cid, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{env}[CoreSet]}(\|_{si \in CoreSet}\ \mathrm{MBoot}[CoreSet, \varepsilon_{si}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{oracle}}(\mathrm{MBoot}[\varepsilon_{CoreSet}]) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$
$\sqsubseteq$
$\mathrm{Mach}_{\mathrm{mc}}(\mathrm{MBoot}) \vdash [\![\mathbf{CertiKOS} \oplus \mathbf{Ctxt}]\!]$


Multithreaded Linking in CertiKOS
Connect CompCertX Interface
Introduce per-thread machine
Introduce multithreaded machine and prove linking theorem
$\mathrm{Mach}_{\mathrm{HAsm}}(\mathrm{PHThrd}[tid, \varepsilon_{tid}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$
$\sqcup\!|$
$\mathrm{Mach}_{\mathrm{TAsm}}(\mathrm{PHBThrd}[tid, \varepsilon_{tid}^{MTLink}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$
$\sqcup\!|$
$\mathrm{Mach}_{\mathrm{IEAsm}[tid]}(\mathrm{PHBThrd}[tid, \varepsilon_{tid}^{MTLink}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$
$\sqcup\!|$
$\mathrm{Mach}_{\mathrm{IEAsm}[T_{[cid]}]}(\|_{tid \in T_{[cid]}} \mathrm{PHBThrd}[cid, \varepsilon_{tid}^{MTLink}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$
$\sqcup\!|$
$\mathrm{Mach}_{\mathrm{Easm}[T_{[cid]}]}(\|_{tid \in T_{[cid]}} \mathrm{PHBThrd}[cid, \varepsilon'_{cid}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$
$\sqcup\!|$
$\mathrm{Mach}_{\mathrm{LAsm}}(\mathrm{PBThrd}[cid, \varepsilon'_{cid}]) \vdash [\![\mathbf{CertiKOS_{thrd}} \oplus \mathbf{Ctxt}]\!]$