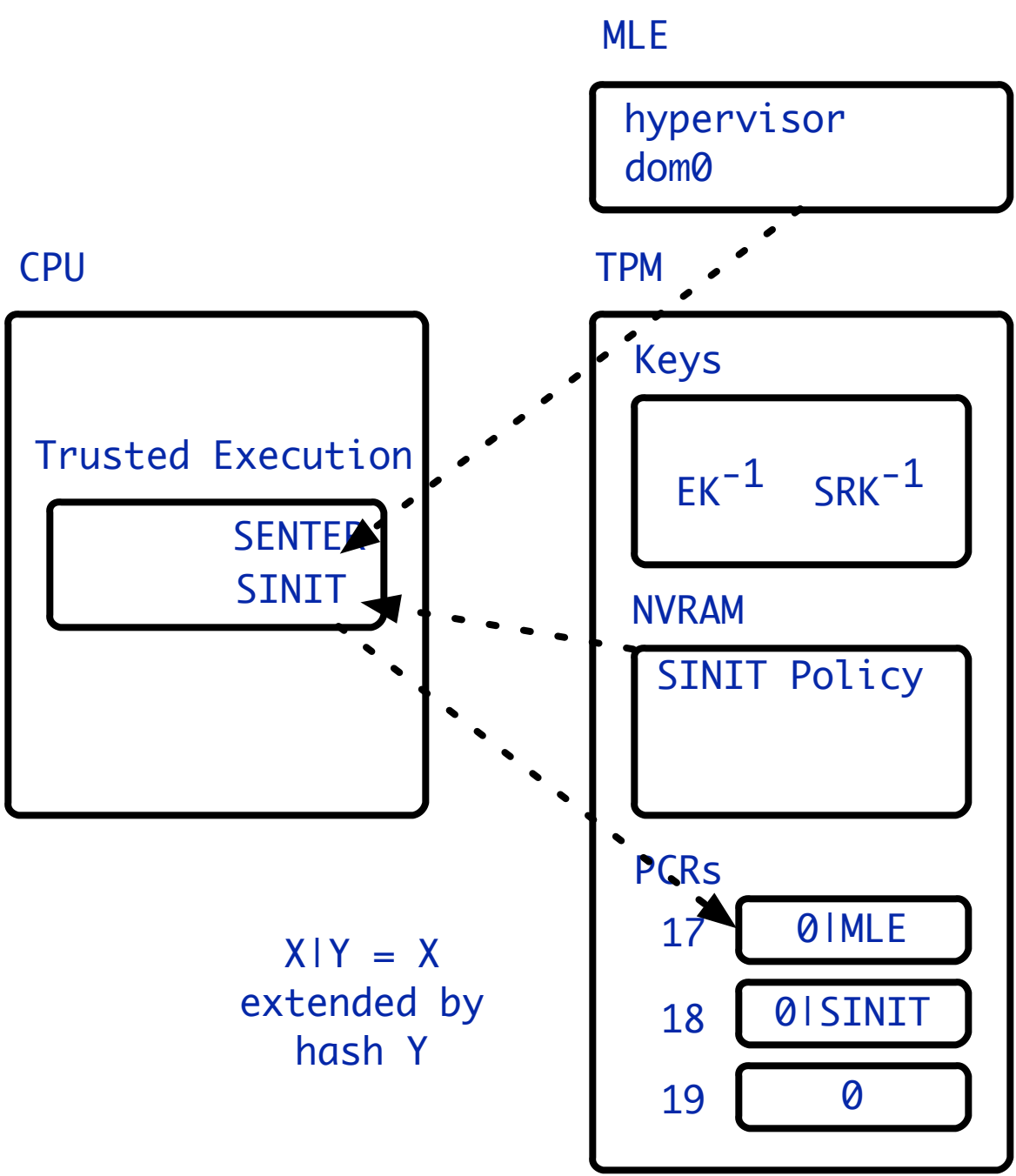
MLE
hypervisor
dom0
CPU
TPM
Trusted Execution
SENTER
SINIT
Keys
EK-1 SRK-1
NVRAM
SINIT Policy
PCRs
17
0|MLE
18
0|SINIT
19
0
X|Y = X
extended by
hash Y