Guest Code

Translation Cache

vPC →

Guest Code
`mov     ebx, eax`
`cli`
`and     ebx, ~0xfff`
`mov     ebx, cr3`
`sti`
`ret`

Translation Cache	
`mov     ebx, eax`	← **start**
`call    HANDLE_CLI`	
`and     ebx, ~0xfff`	
`mov     [CO_ARG], ebx`	
`call    HANDLE_CR3`	⟷
`call    HANDLE_STI`	⟷
`jmp     HANDLE_RET`	⟷