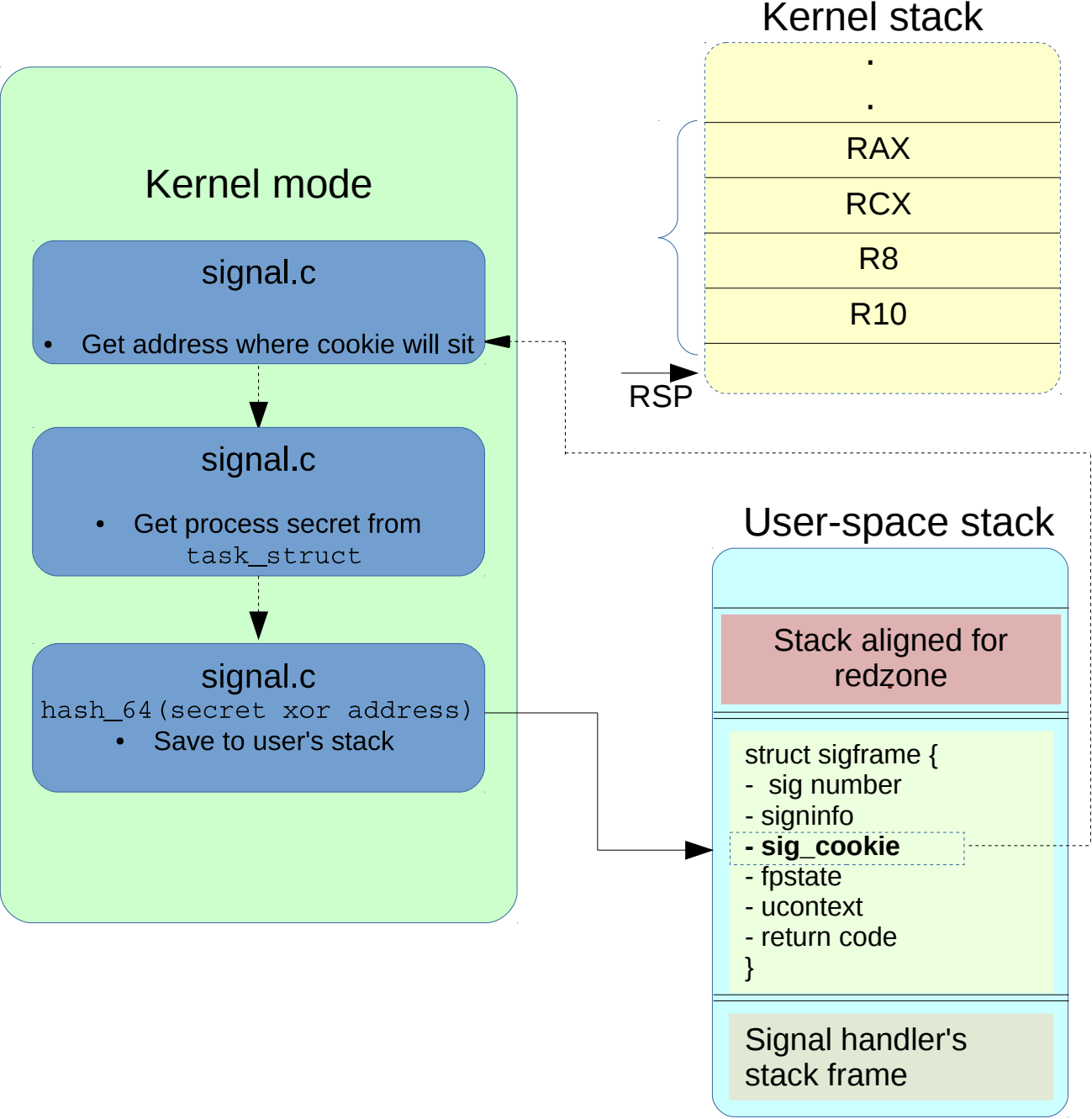
Kernel stack
.
.
RAX
RCX
R8
R10
RSP
Kernel mode
signal.c
• Get address where cookie will sit
signal.c
• Get process secret from task_struct
signal.c
hash_64(secret xor address)
• Save to user's stack
User-space stack
Stack aligned for redzone
struct sigframe {
- sig number
- signinfo
- sig_cookie
- fpstate
- ucontext
- return code
}
Signal handler's stack frame