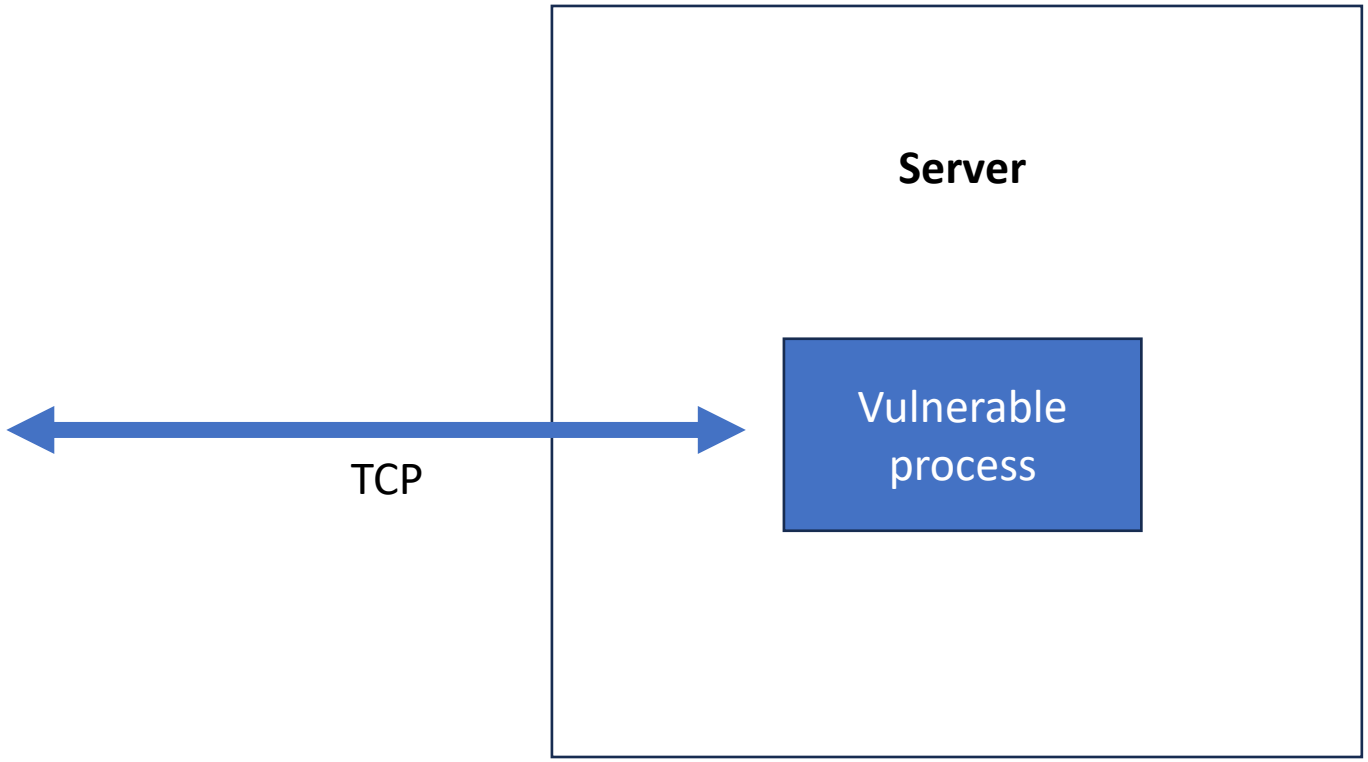
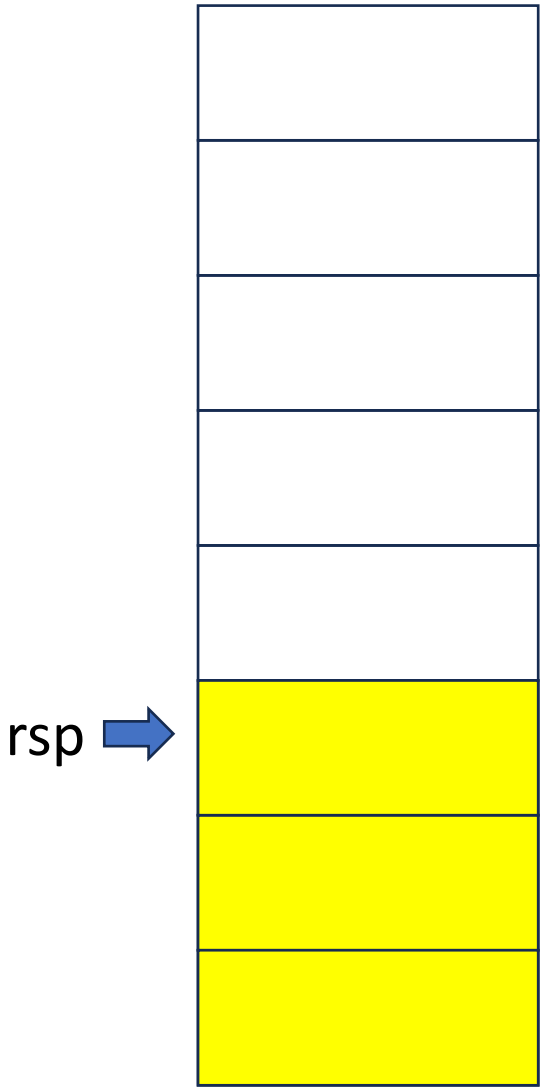
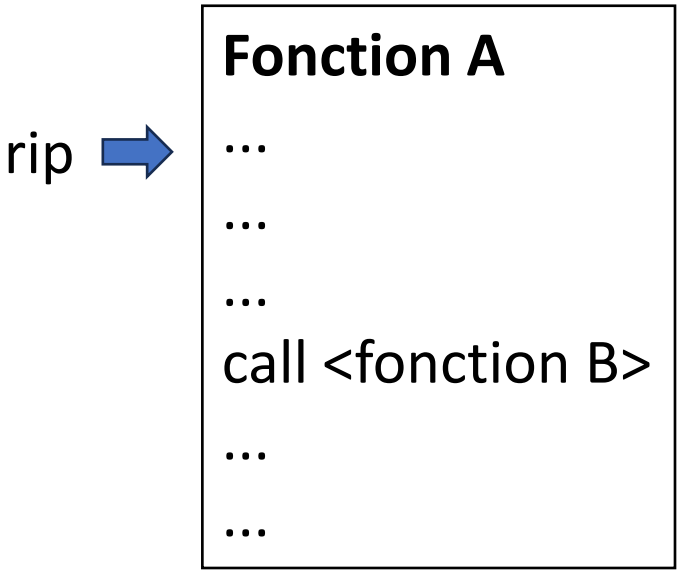
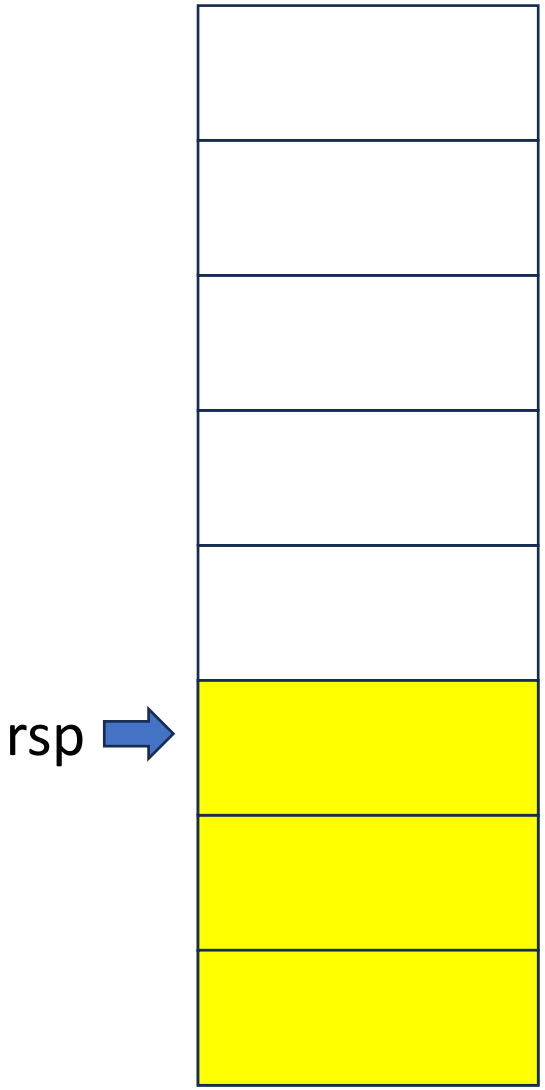
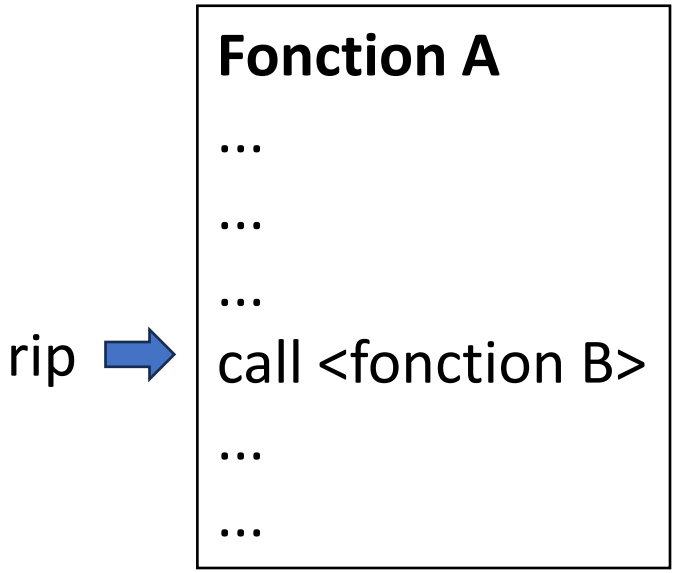

HACKER

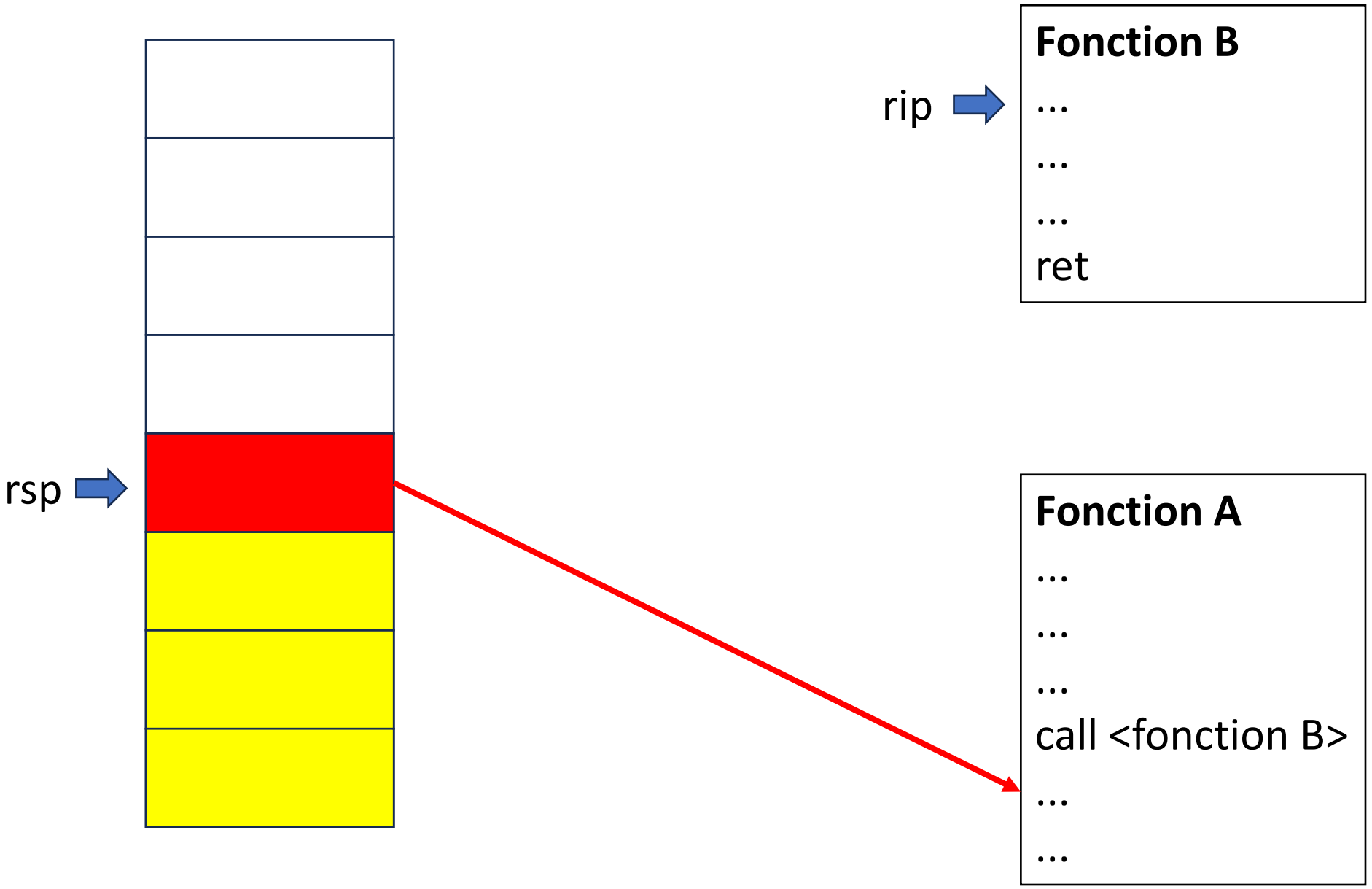

Server
Vulnerable process
TCP

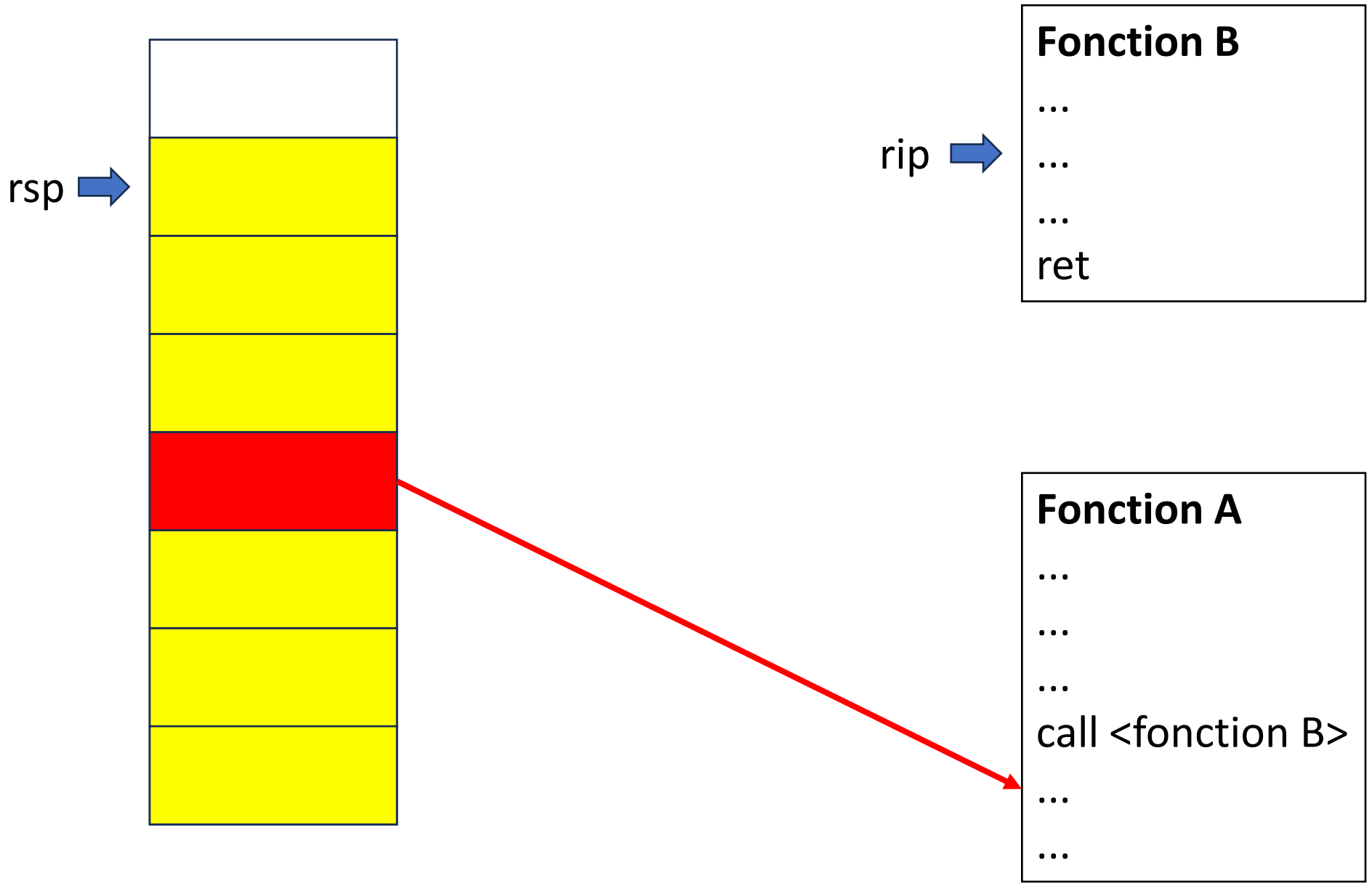

rsp

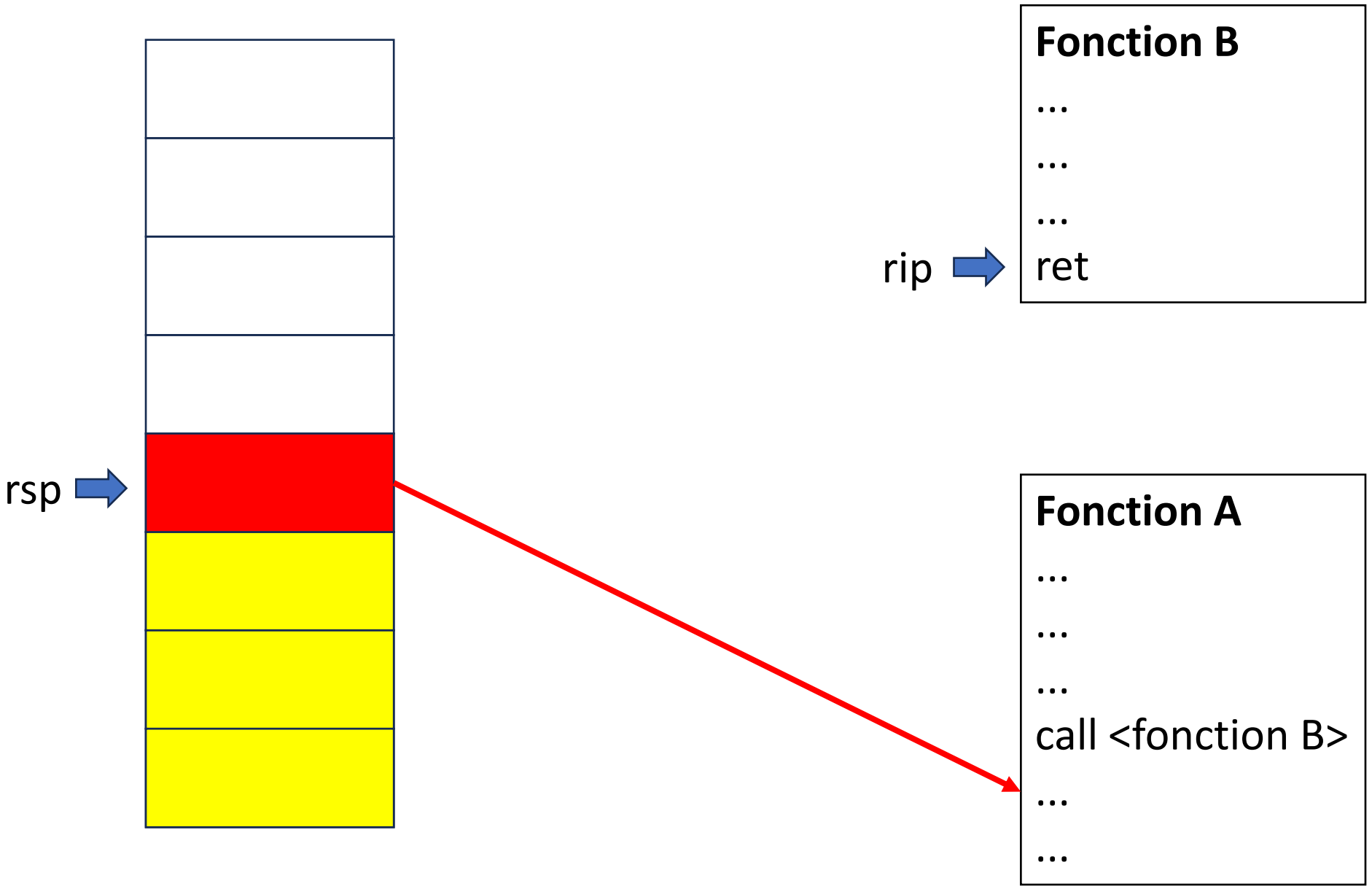

rip
Fonction A
...
...
...
call <fonction B>
...
...

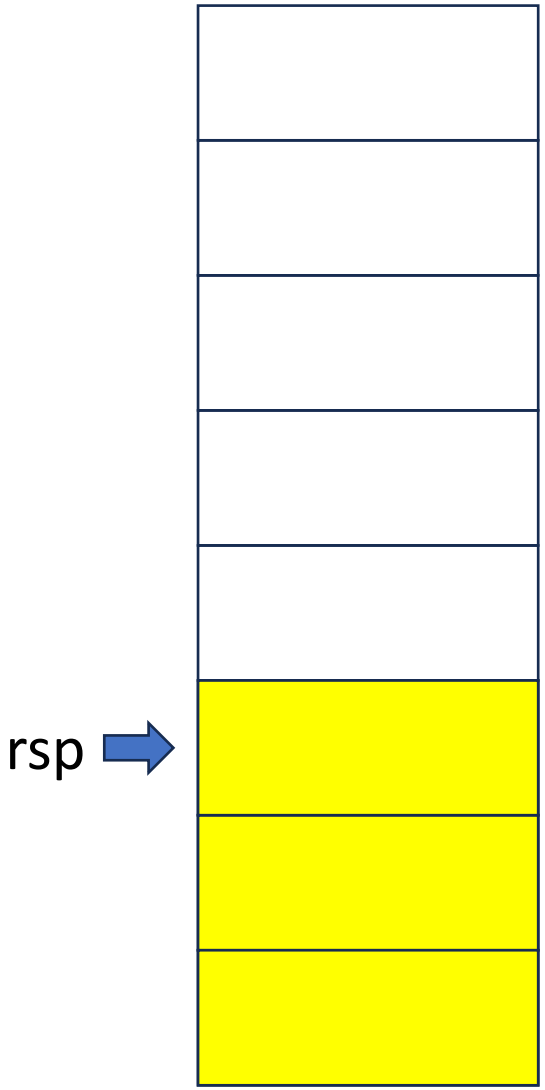

rsp


Fonction A
...
...
...
rip
call <fonction B>
...
...


rip
Fonction B
...
...
...
ret
rsp
Fonction A
...
...
...
call <fonction B>
...
...


rsp
rip
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...


Fonction B
...
...
...
ret
rip
rsp
Fonction A
...
...
...
call <fonction B>
...
...



Fonction B

...

...

...

ret

Fonction A

...

...

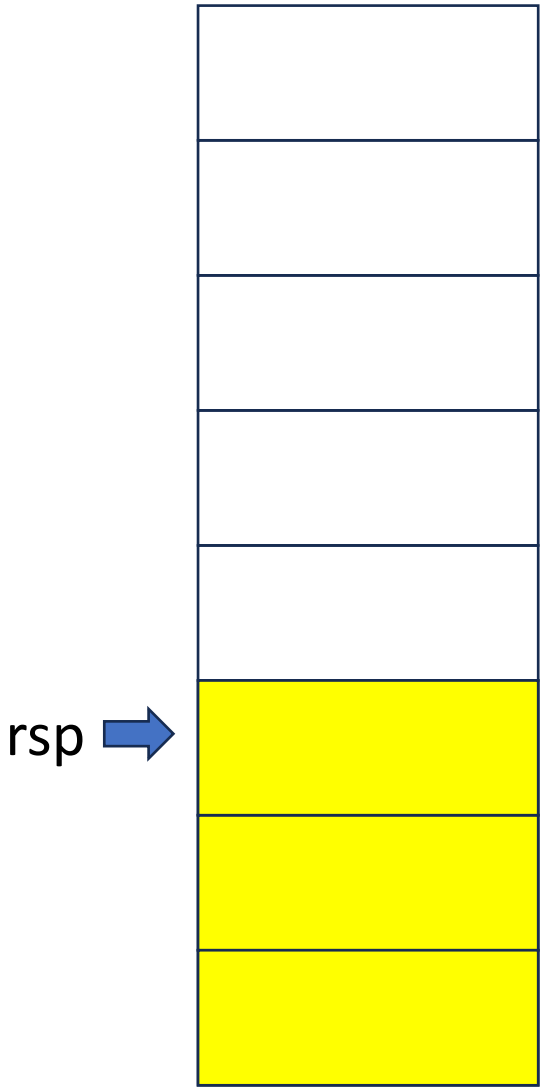
...

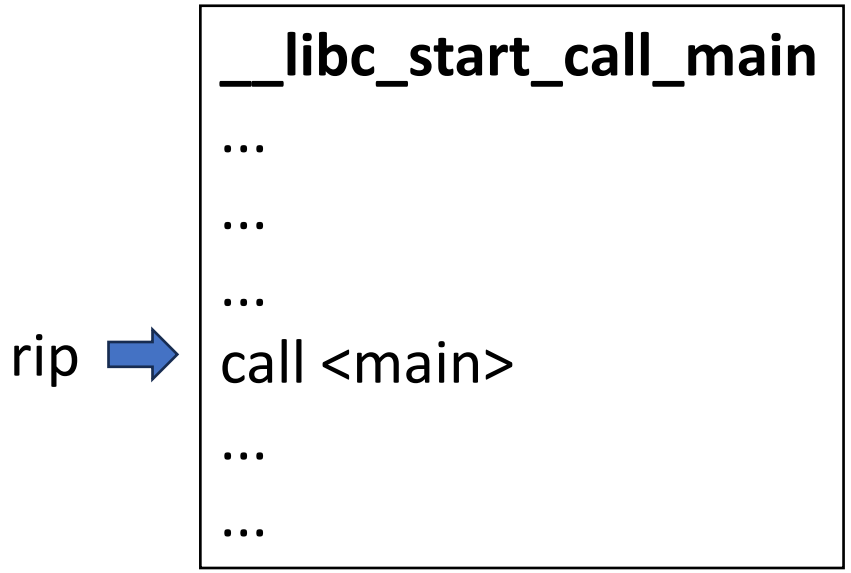
call <fonction B>

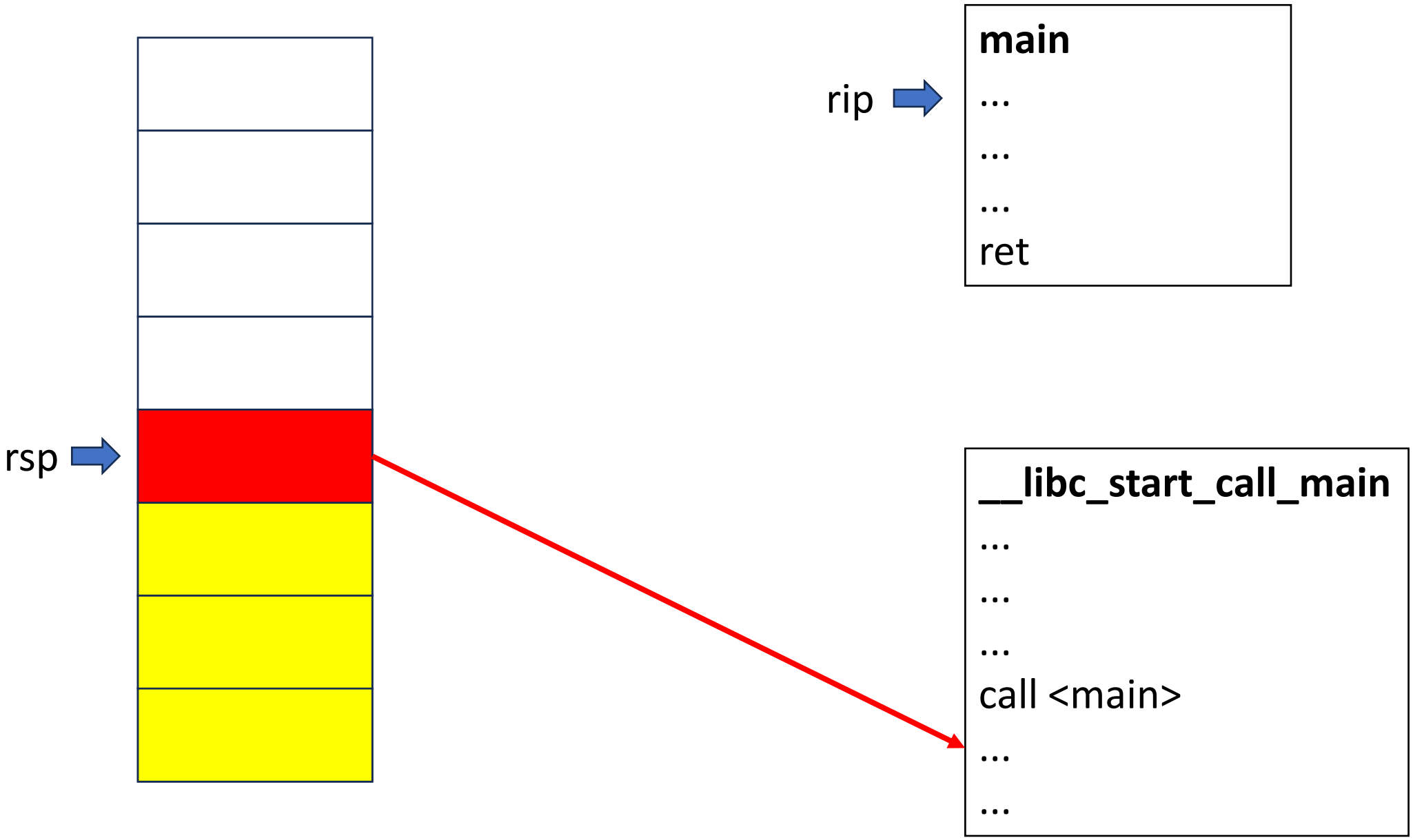
rip

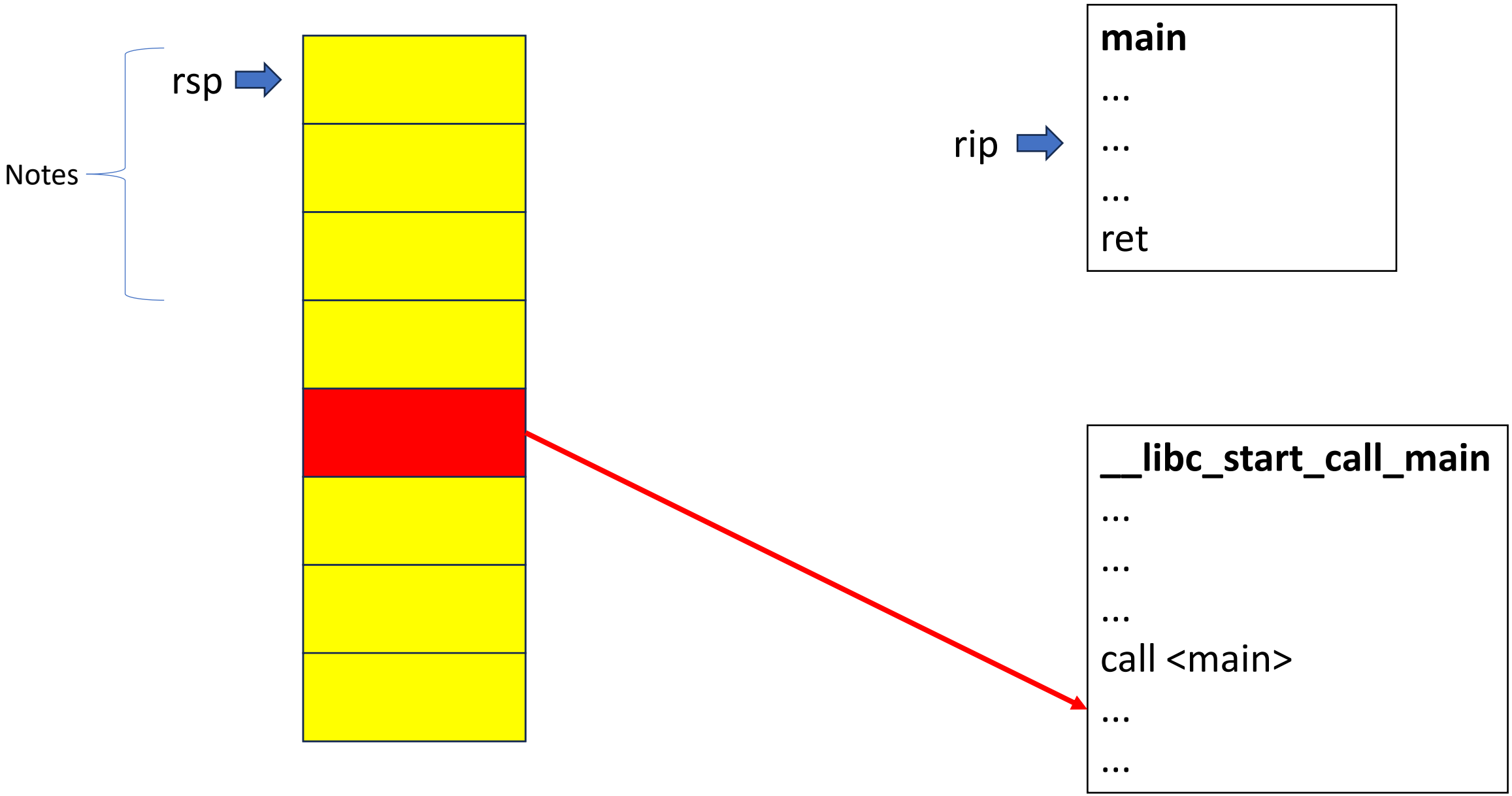
...

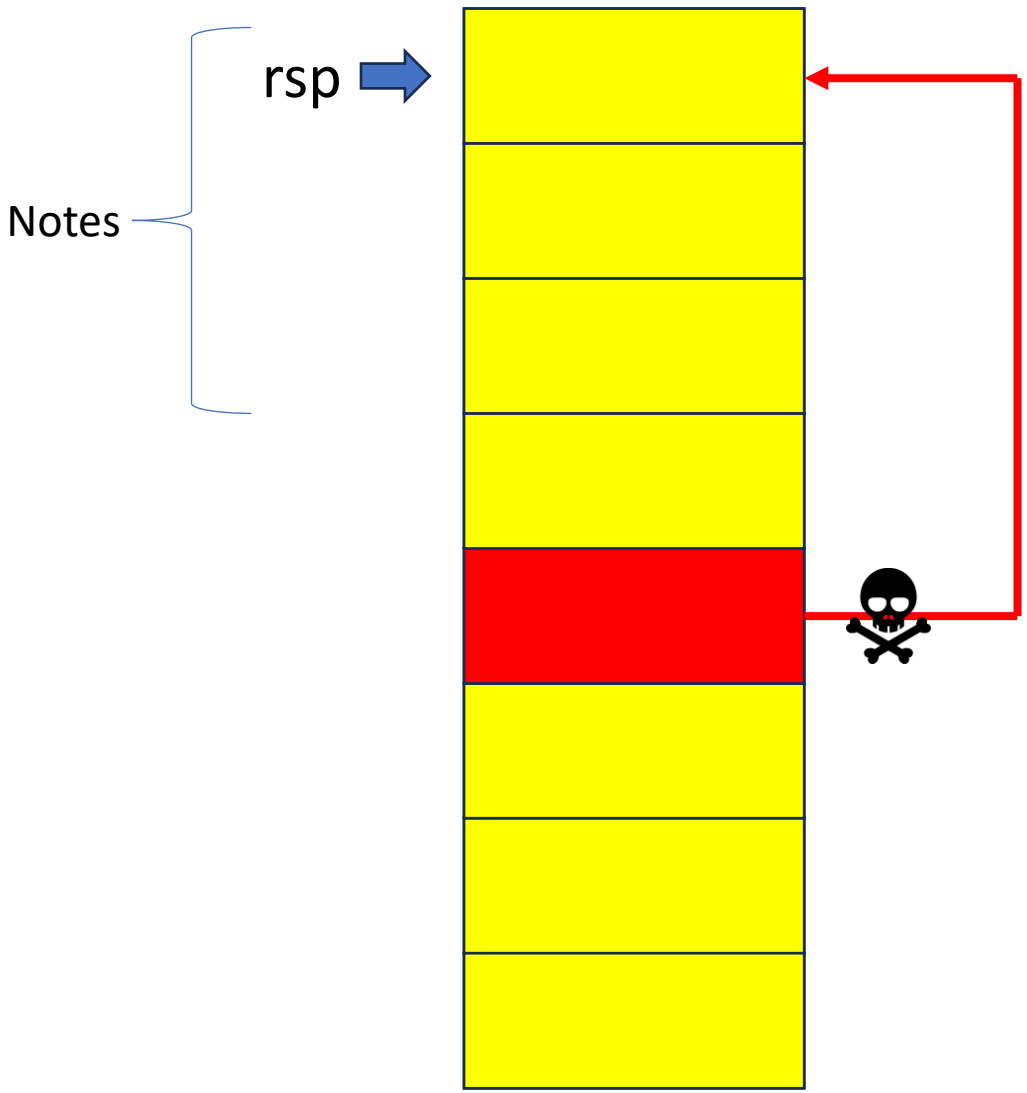
...


rsp


__libc_start_call_main
...
...
...
rip
call <main>
...
...


rip
main
...
...
...
ret
rsp
__libc_start_call_main
...
...
...
call <main>
...
...


rsp
Notes
rip
main
...
...
...
ret
__libc_start_call_main
...
...
...
call <main>
...
...

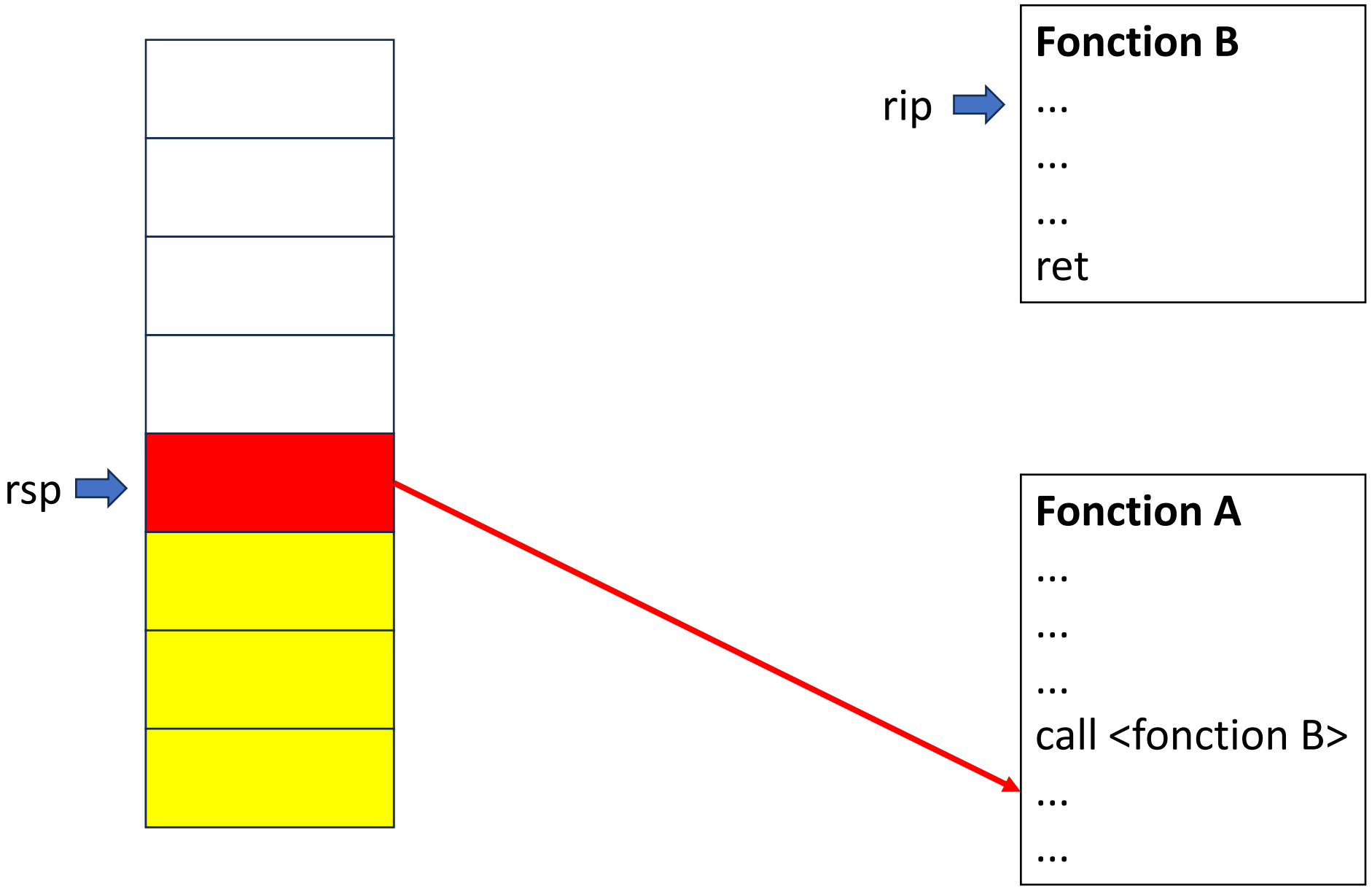


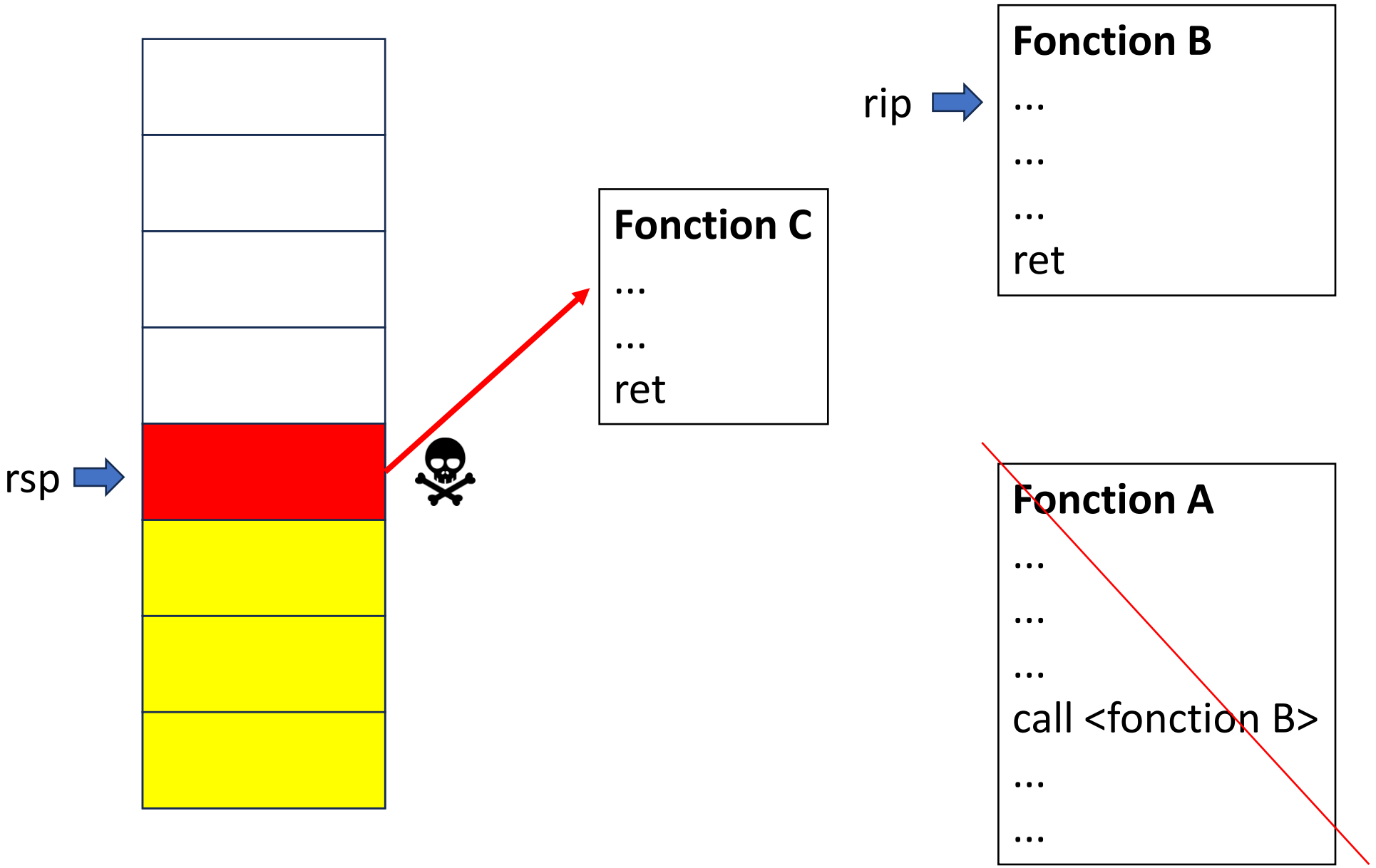
rip

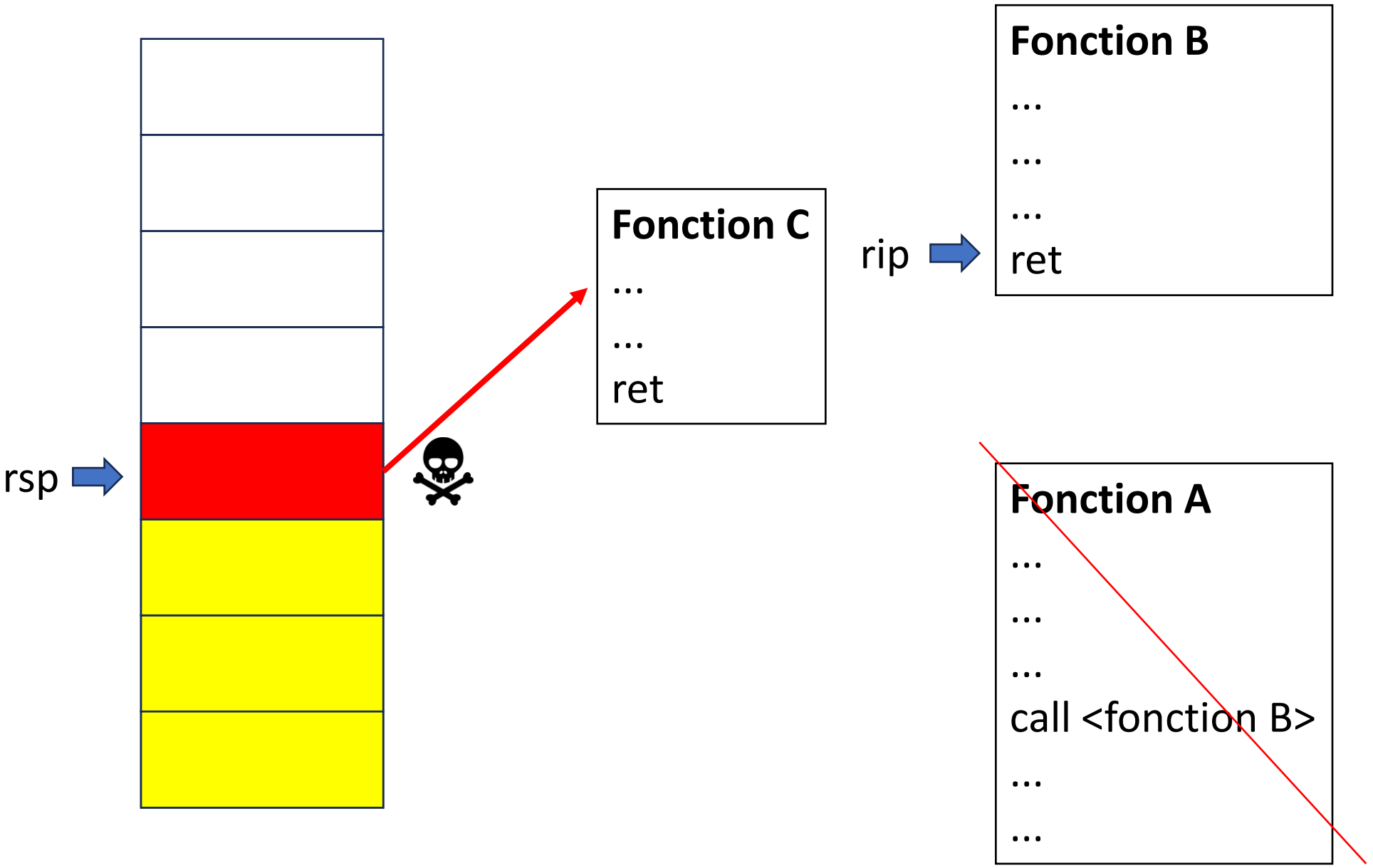
main
…
…
…
ret

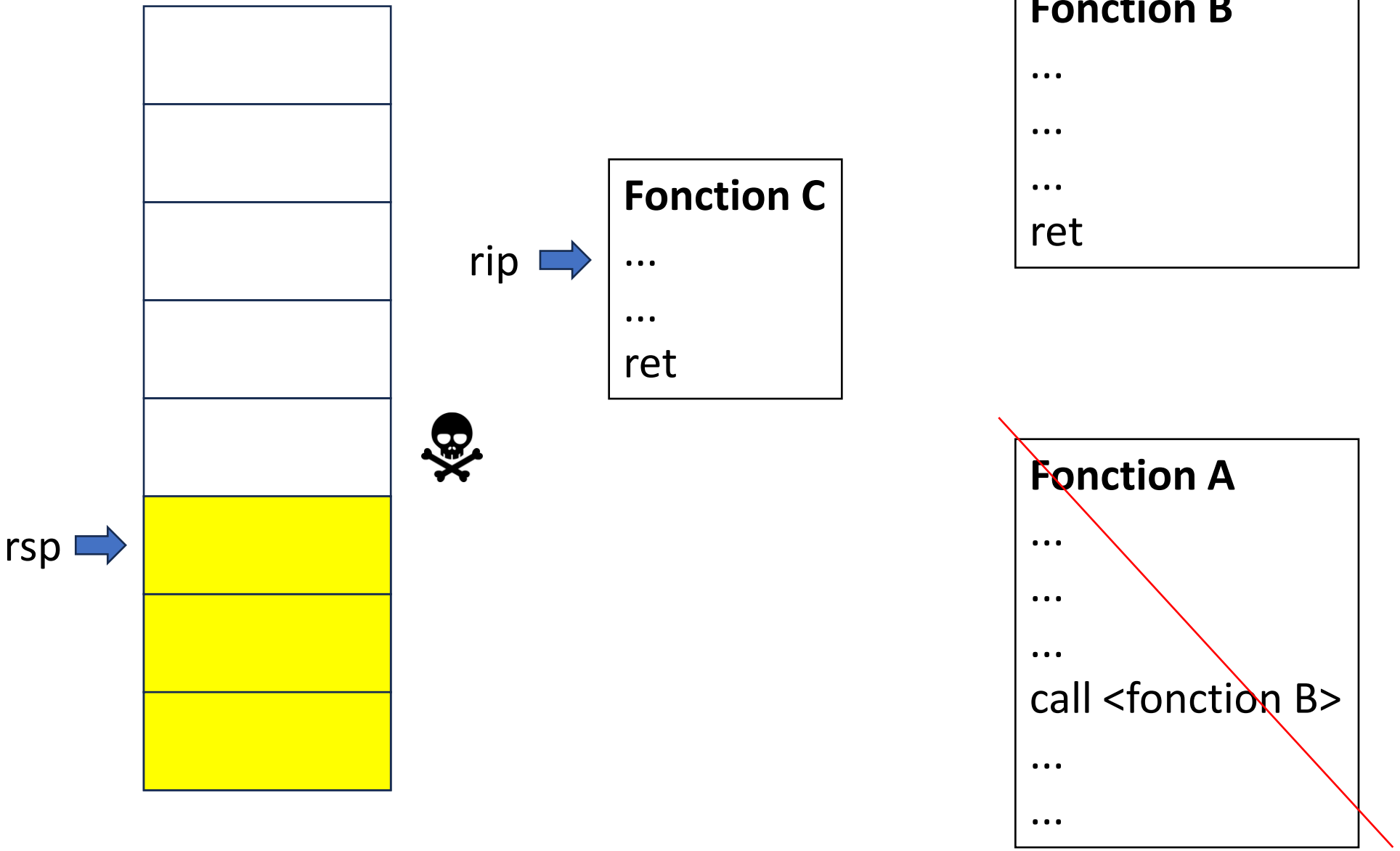
__libc_start_call_main
…
…
…
call <main>
…
…

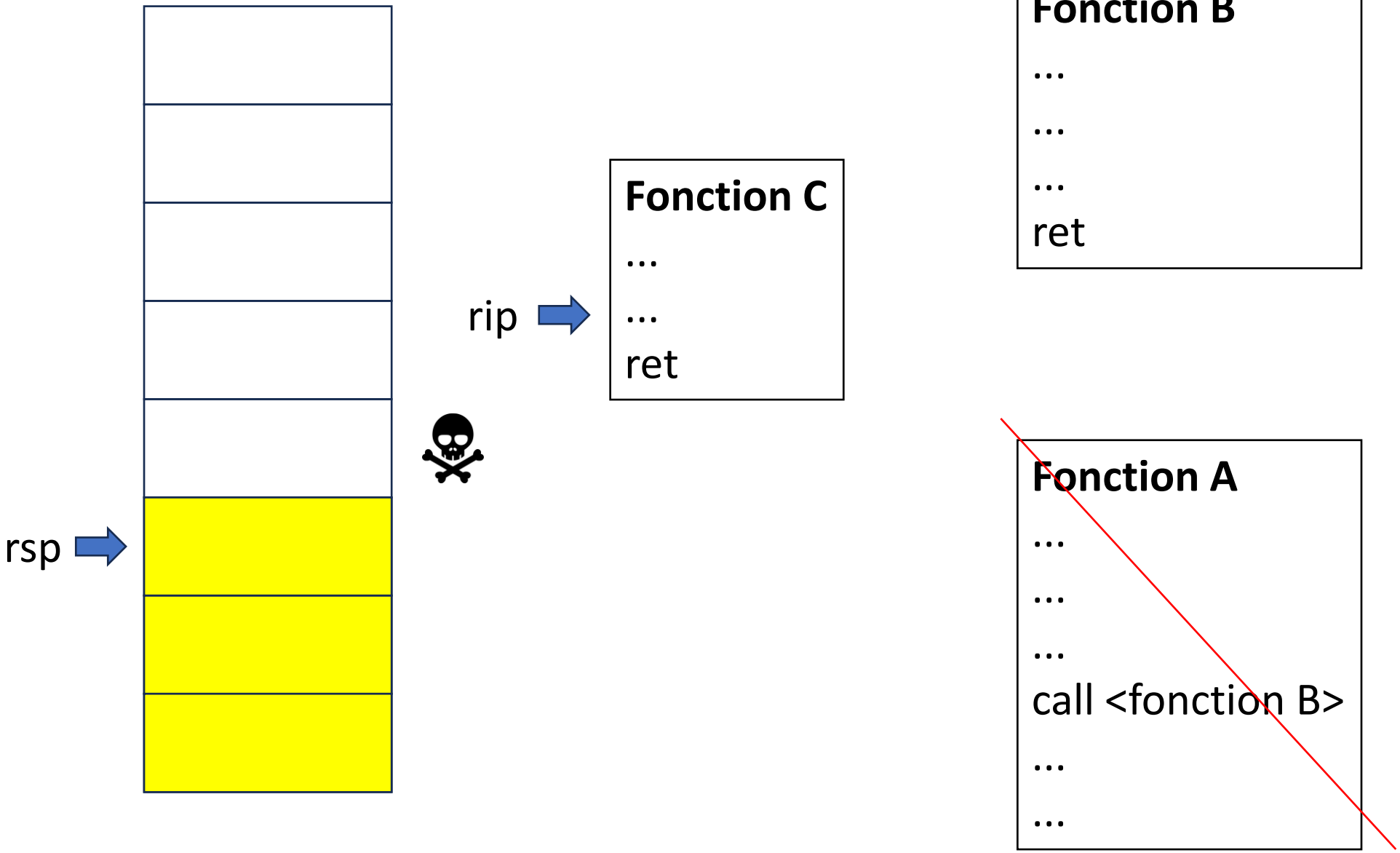

CODE
CODE EVERYWHERE
imgflip.com

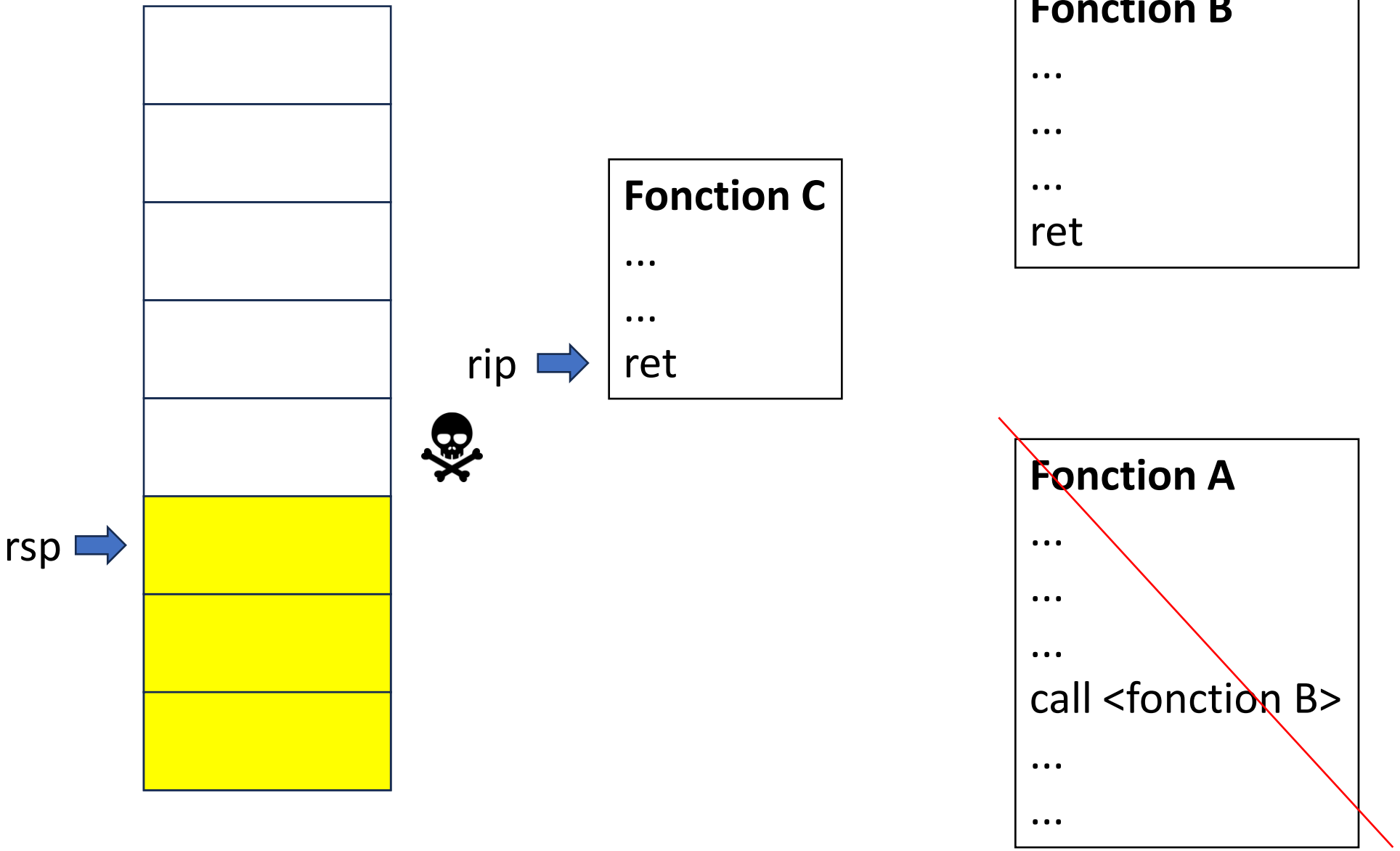

rip
Fonction B
...
...
...
ret
rsp
Fonction A
...
...
...
call <fonction B>
...
...

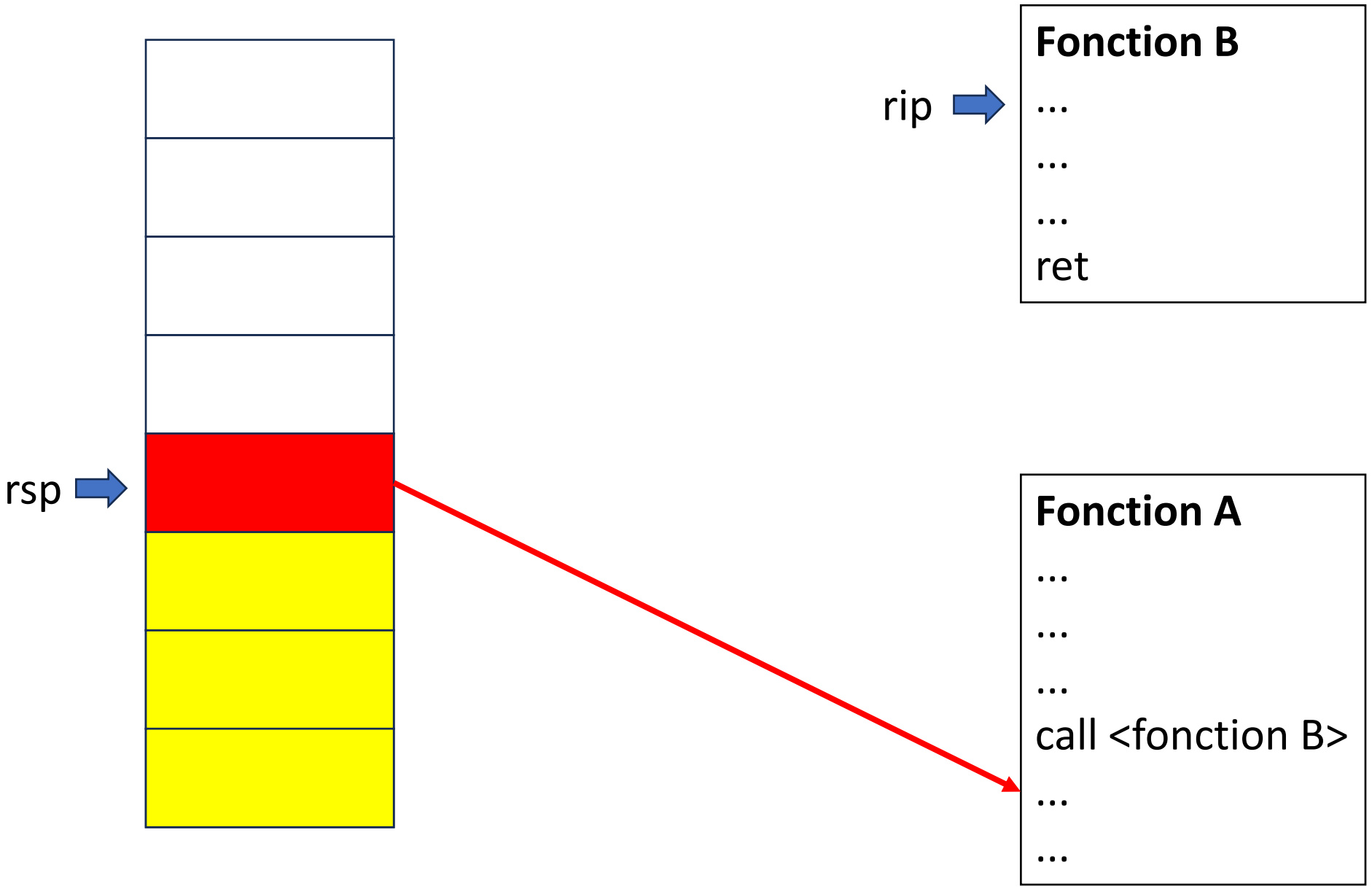

rsp
Fonction C
...
...
ret
rip
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

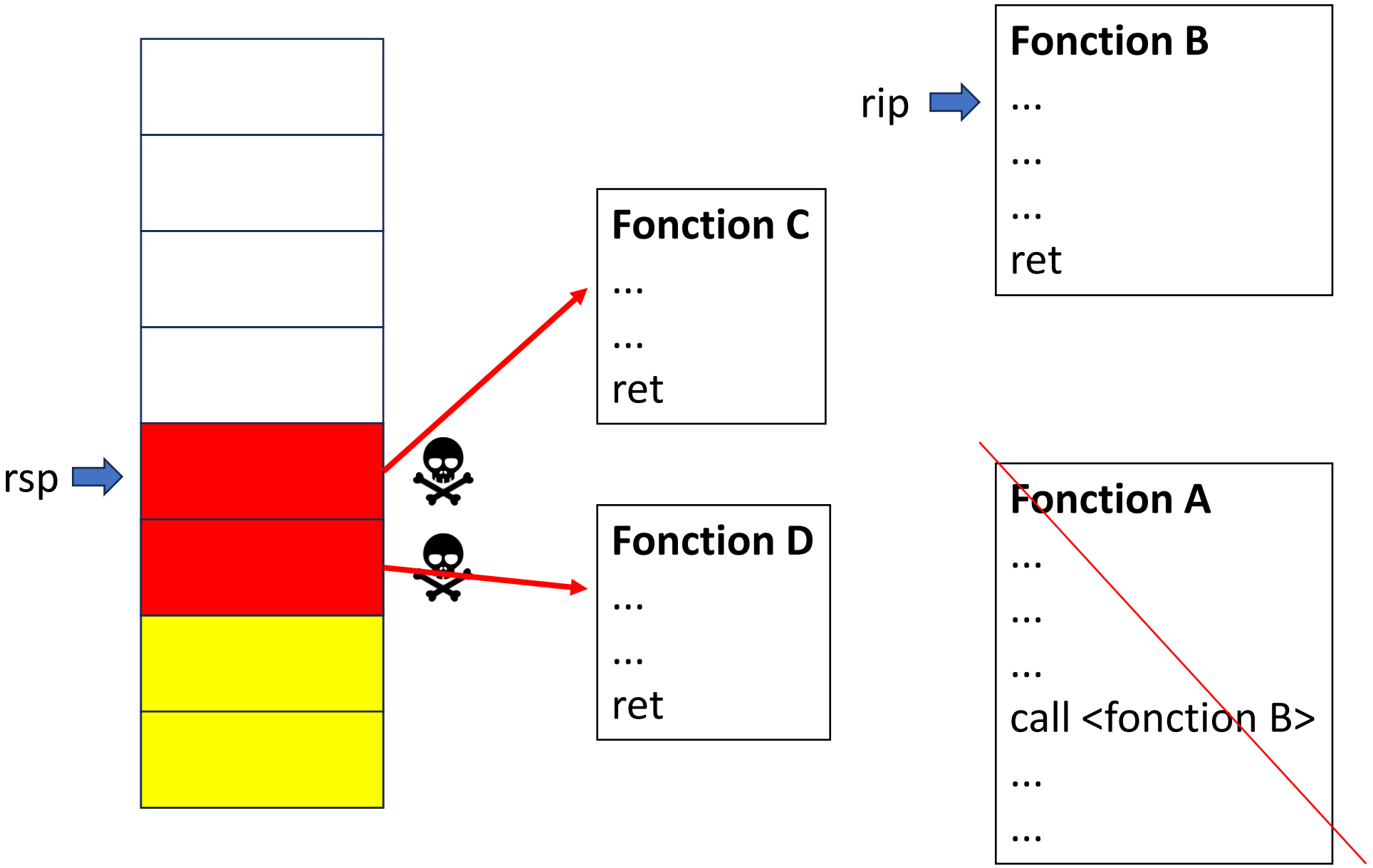

rsp
Fonction C
...
...
ret
rip
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

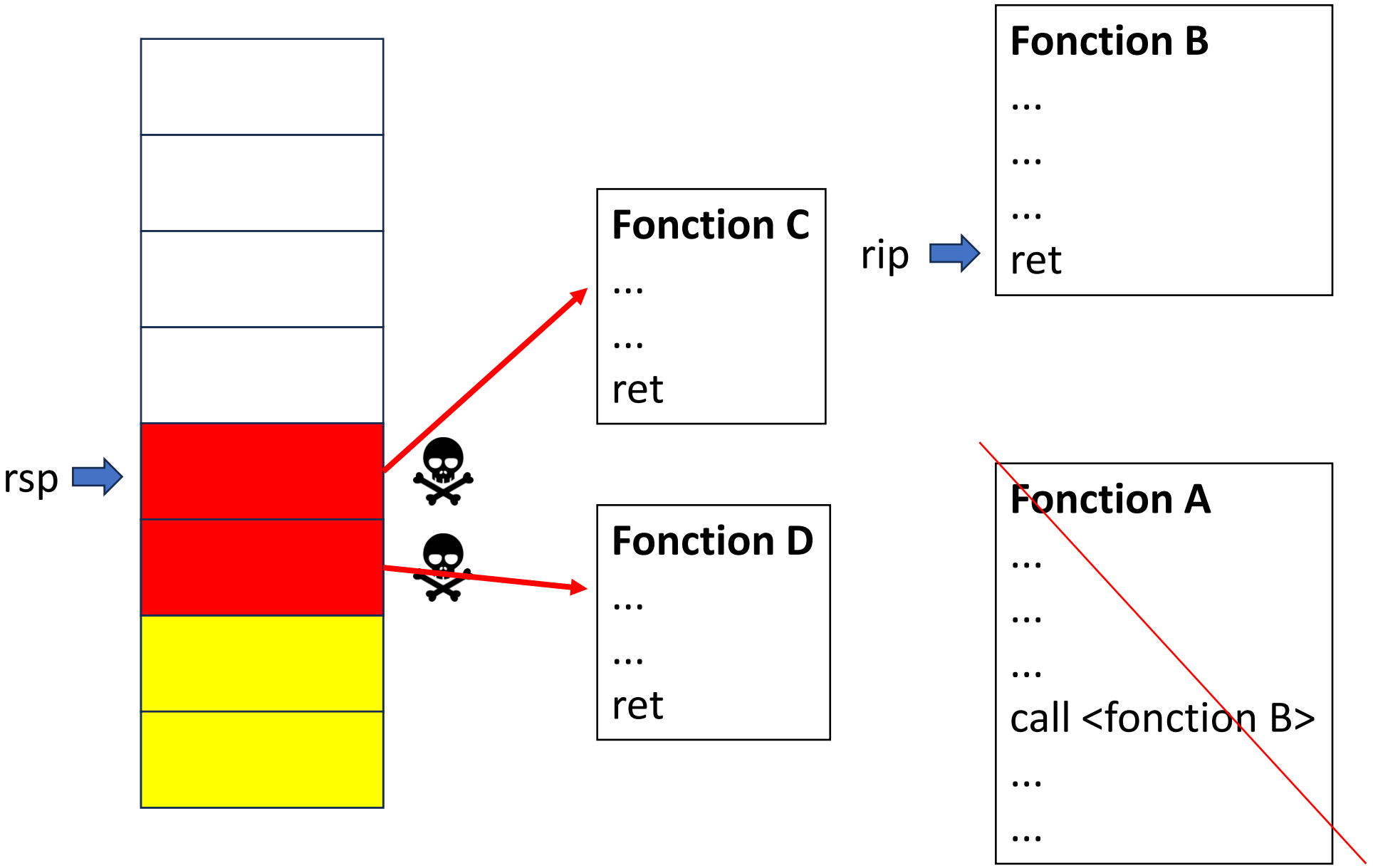

rsp
rip
Fonction C
...
...
ret
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

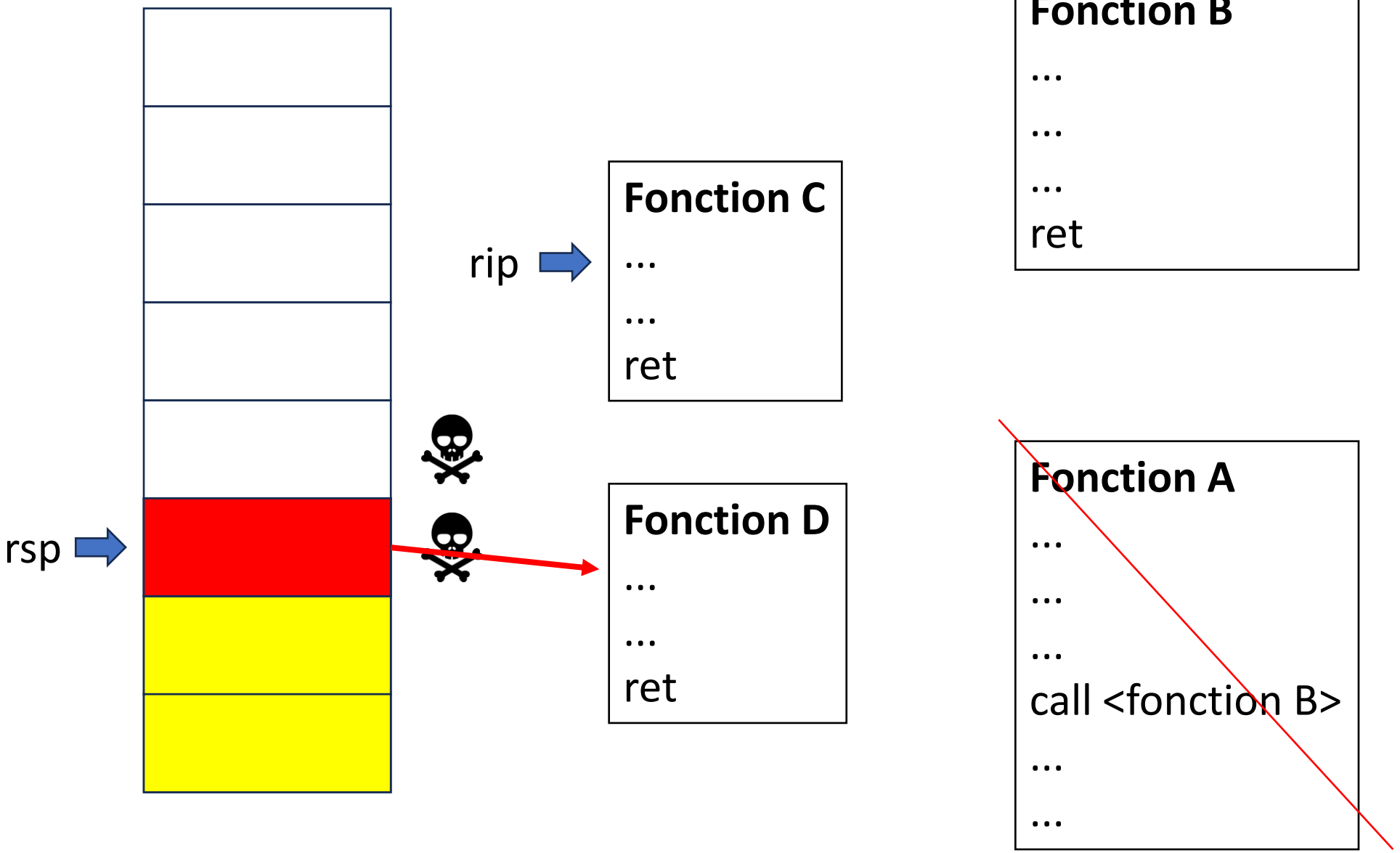

Fonction B
...
...
...
ret
rip
Fonction C
...
...
ret
rsp
Fonction A
...
...
...
call <fonction B>
...
...

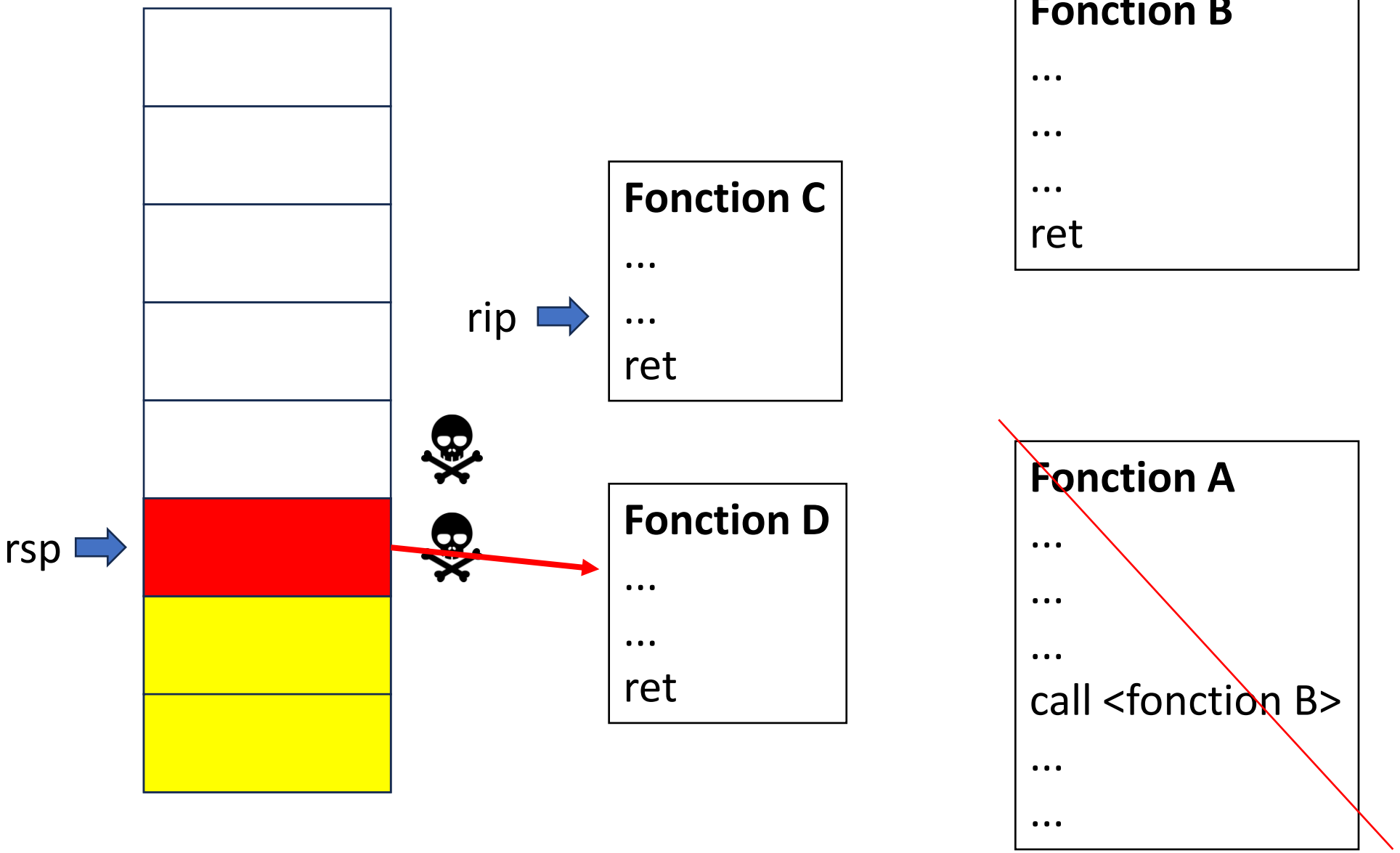

rsp
rip
Fonction C
...
...
ret
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

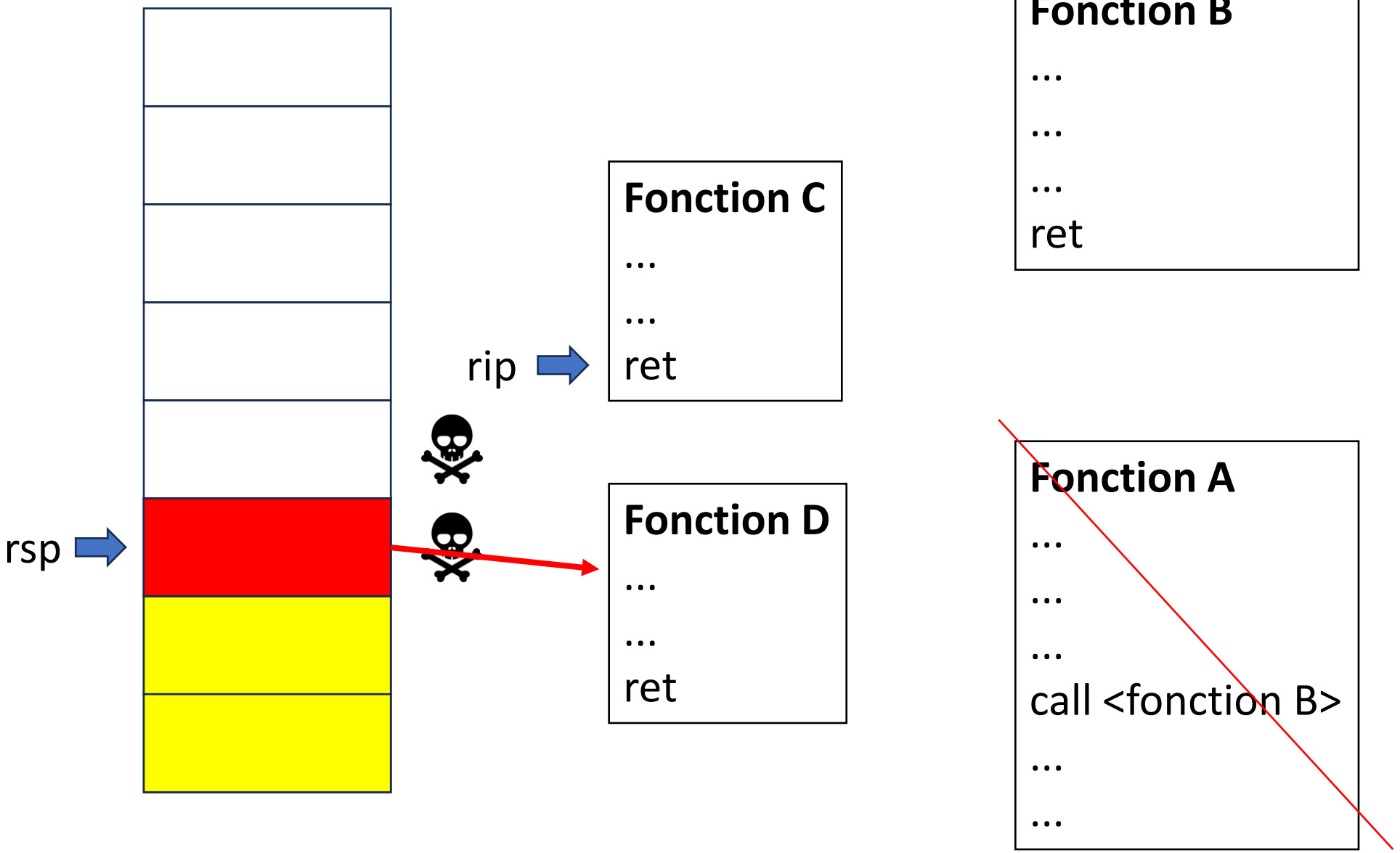

rip
Fonction B
...
...
...
ret
rsp
Fonction A
...
...
...
call <fonction B>
...
...

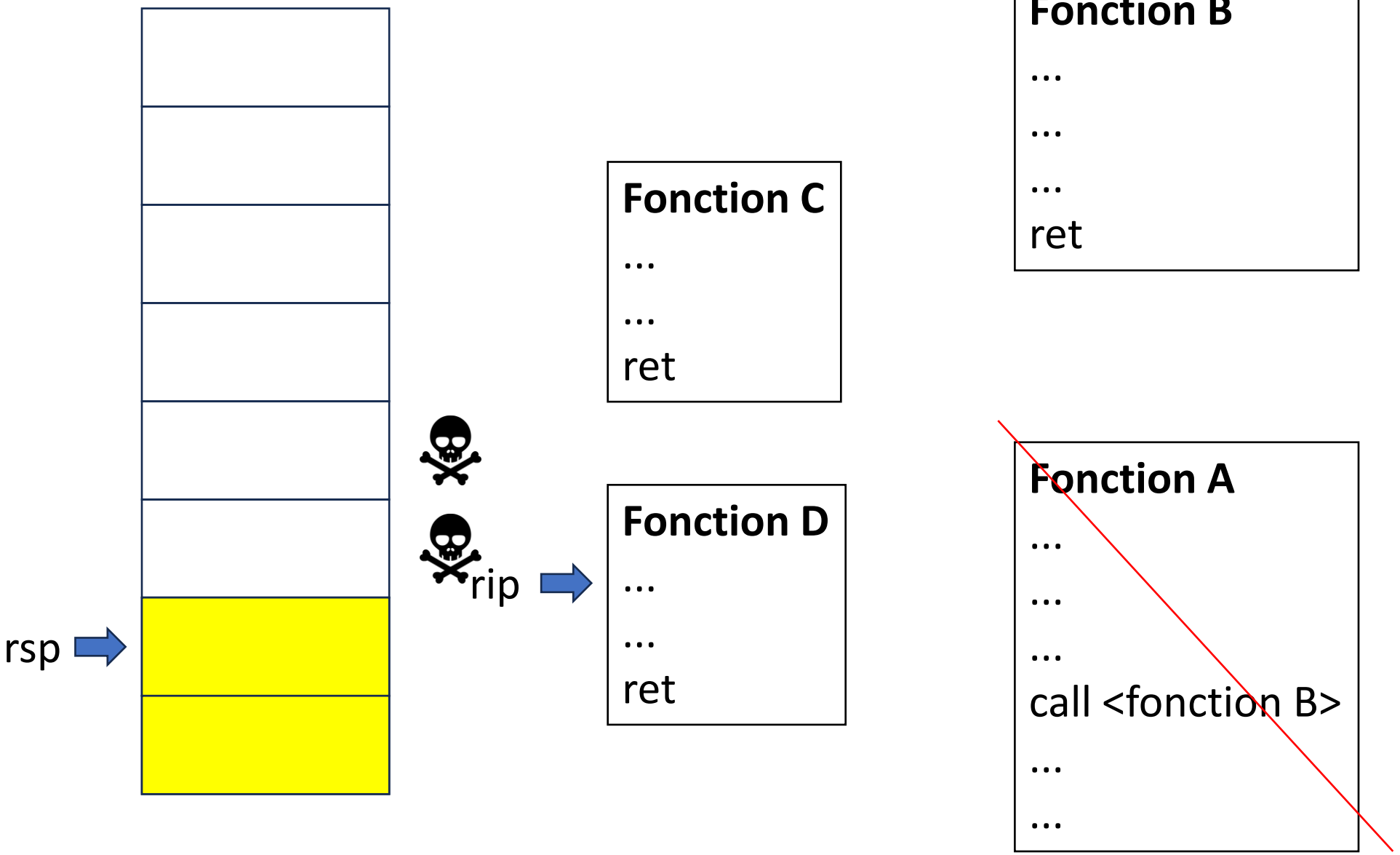

rip
Fonction B
...
...
...
ret
Fonction C
...
...
ret
rsp
Fonction D
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

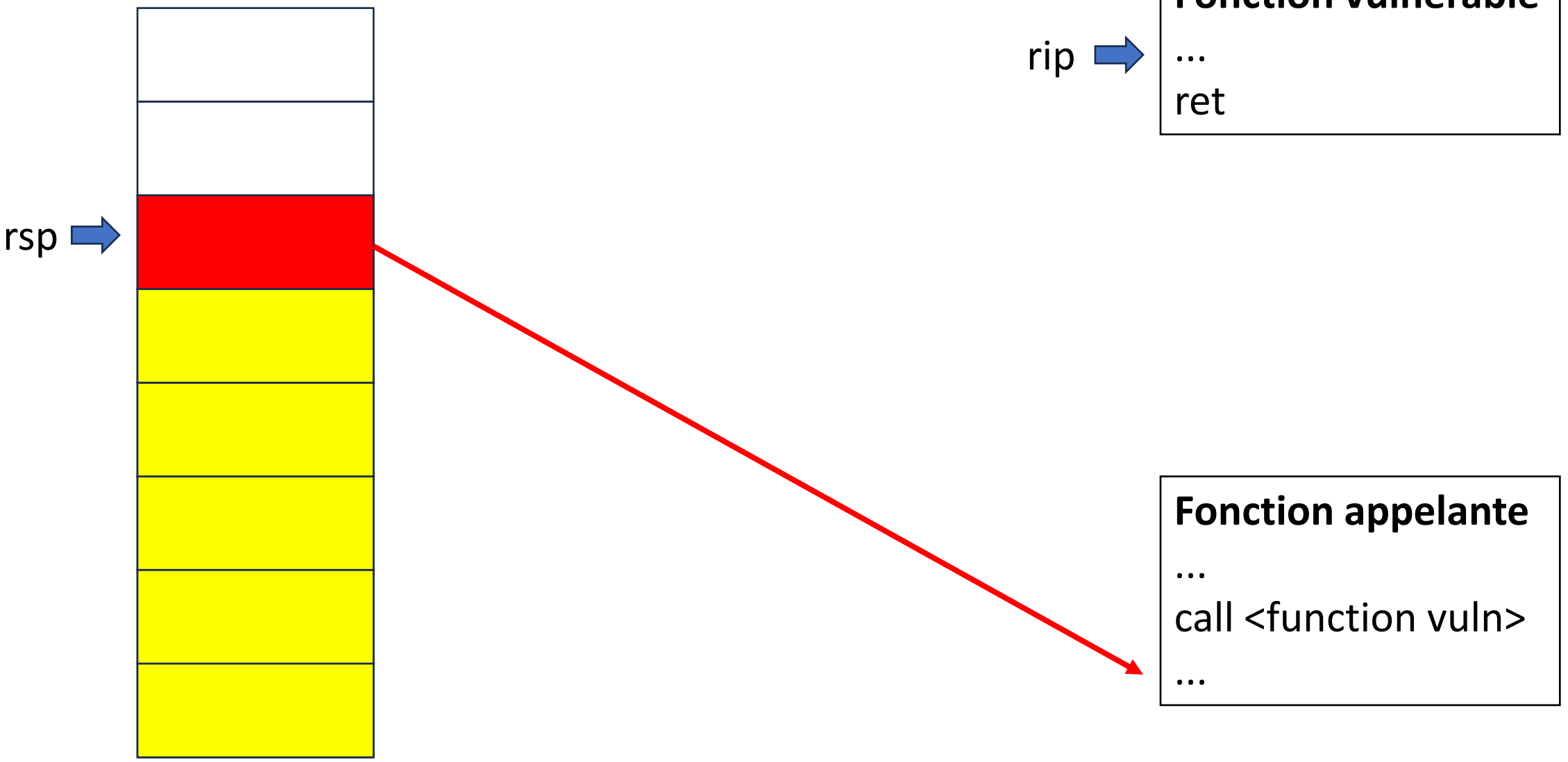

rsp
Fonction C
...
...
ret
Fonction D
...
...
ret
rip
Fonction B
...
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...

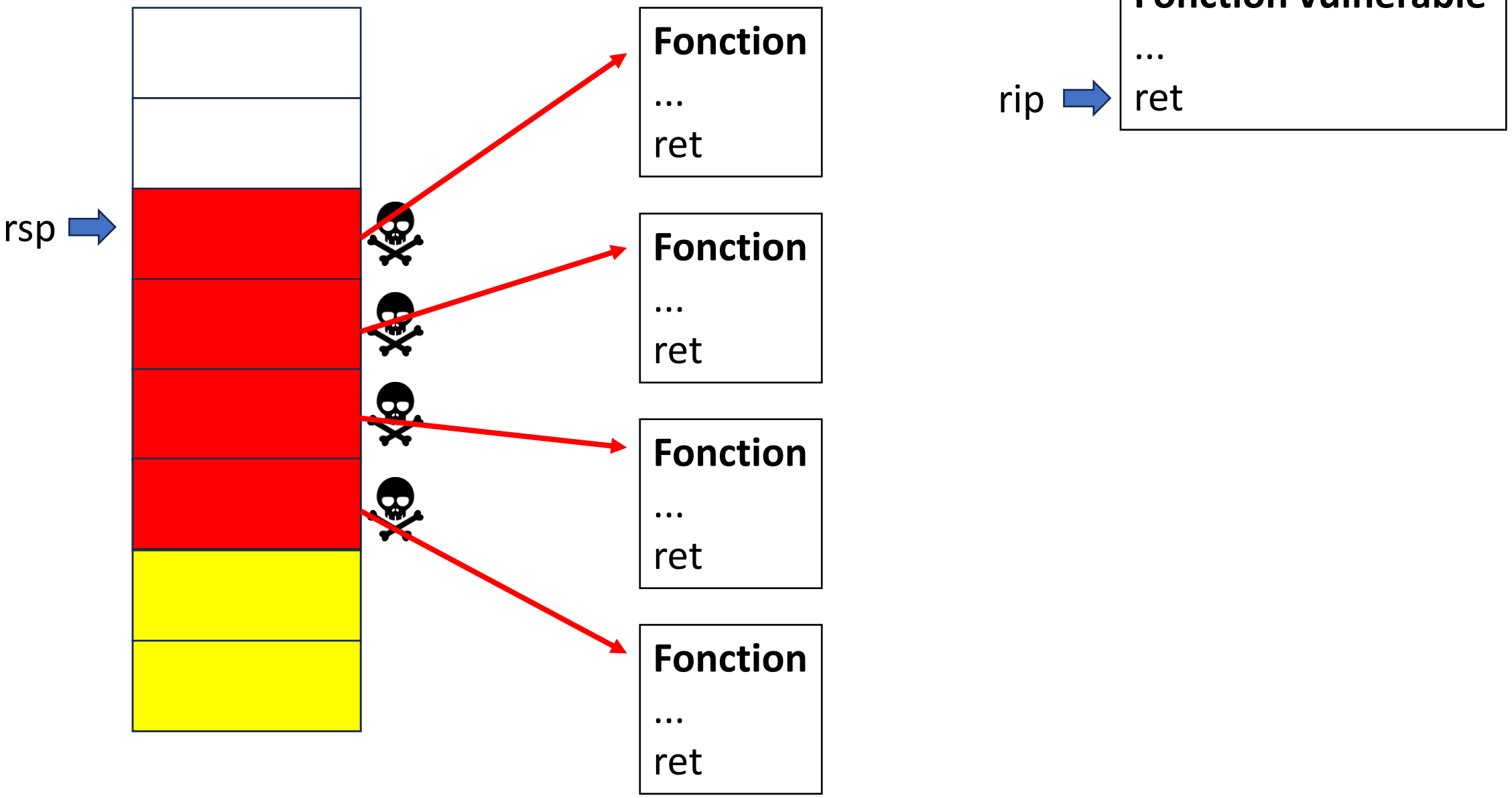

Fonction B
...
...
...
ret
rip
Fonction C
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...
rsp
Fonction D
...
...
ret

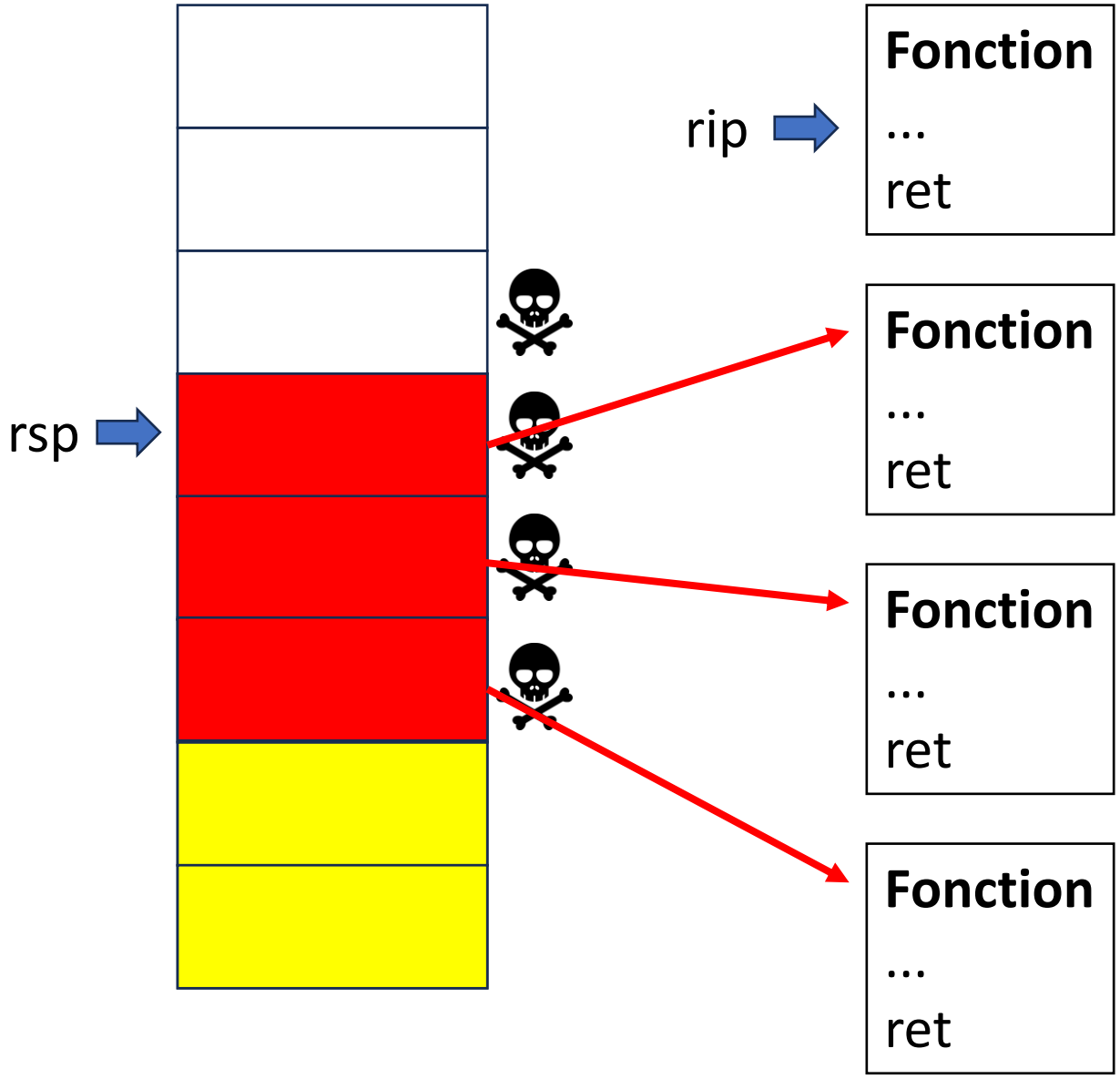

Fonction B
...
...
...
ret
Fonction C
...
...
ret
rip
rsp
Fonction D
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...


Fonction B
...
...
...
ret
Fonction C
...
...
ret
rip
Fonction D
...
...
ret
rsp
Fonction A
...
...
...
call <fonction B>
...
...


Fonction B
...
...
...
ret
Fonction C
...
...
ret
Fonction D
...
...
ret
Fonction A
...
...
...
call <fonction B>
...
...
rip
rsp


rip
Fonction vulnérable
...
ret
rsp
Fonction appelante
...
call <function vuln>
...

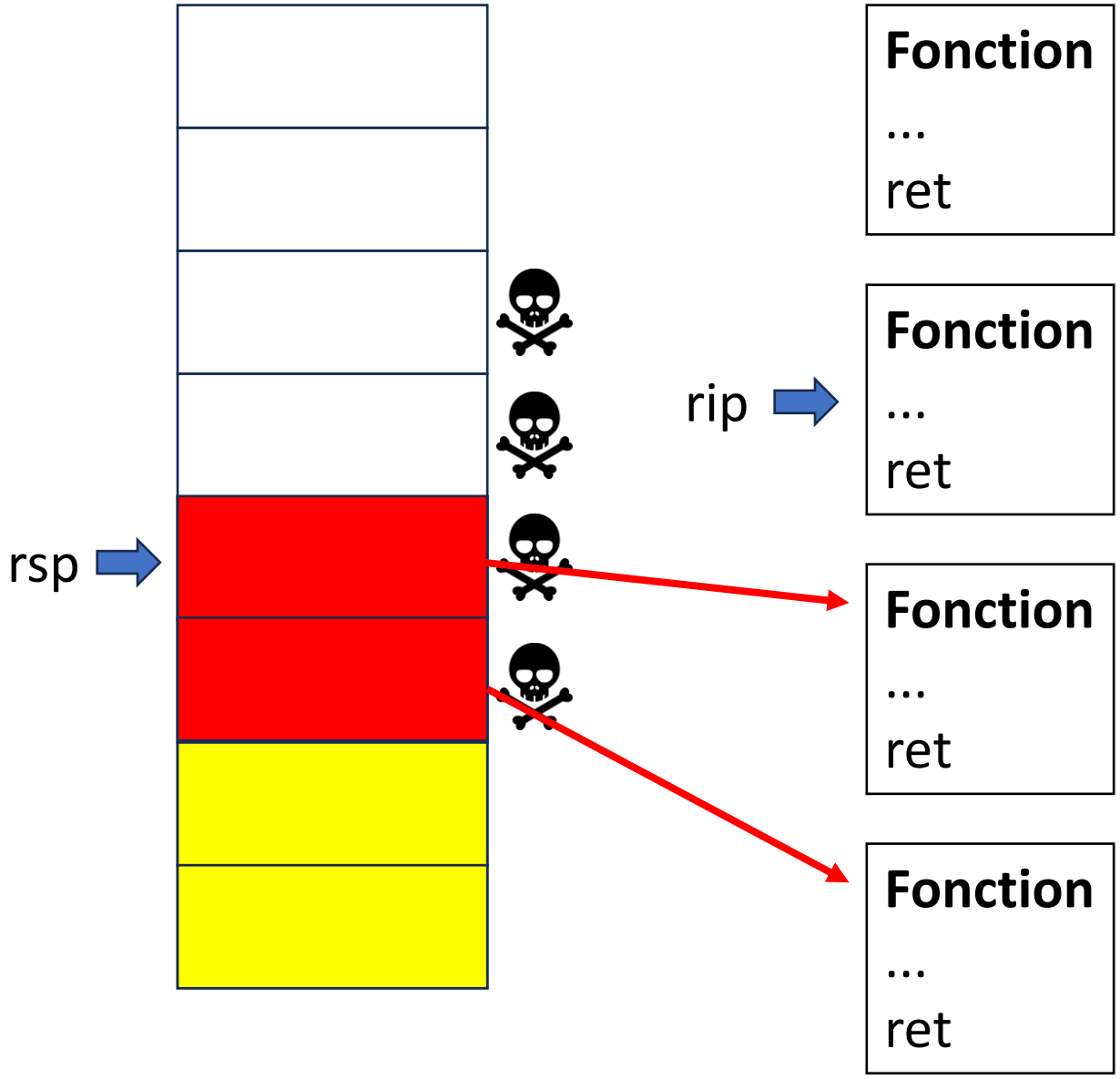

rsp
Fonction
...
ret
Fonction
...
ret
Fonction
...
ret
Fonction
...
ret
rip
Fonction vulnérable
...
ret



Fonction vulnérable

...

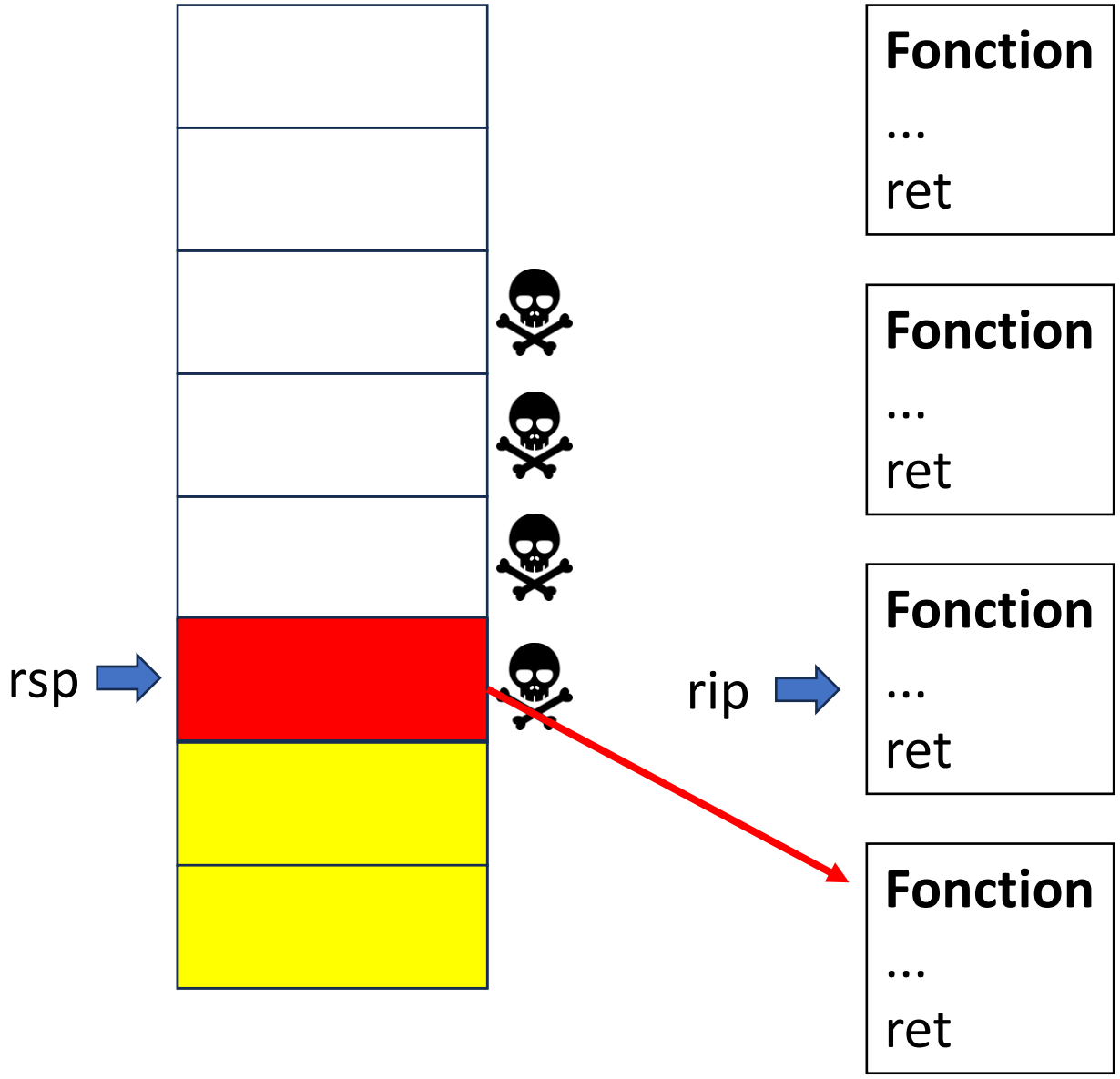
ret



Fonction vulnérable

...

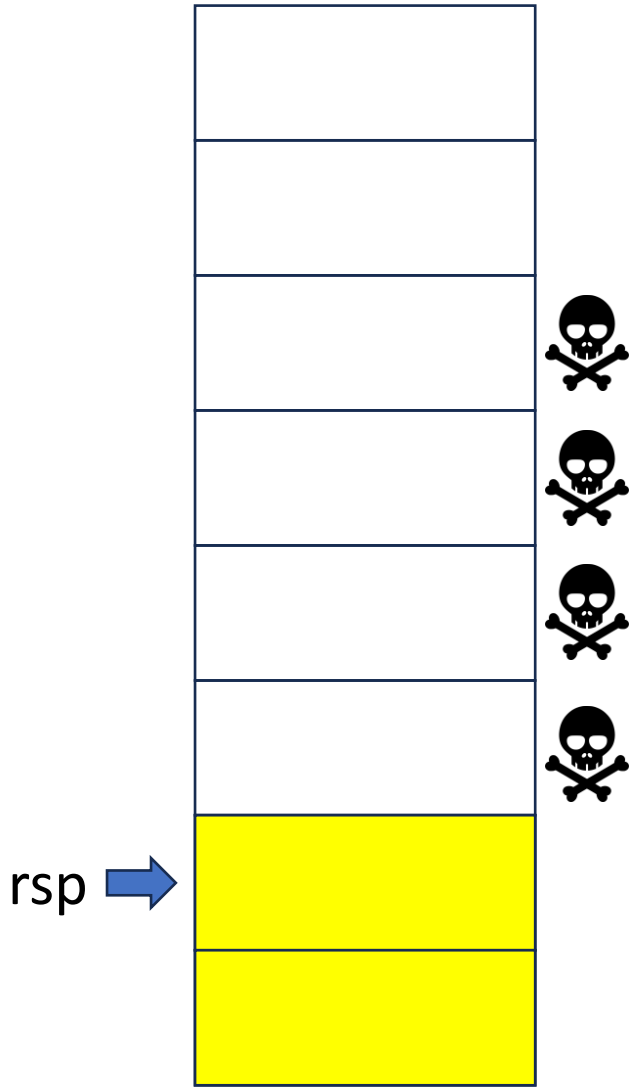
ret



Fonction vulnérable

...

ret



Fonction
...
ret

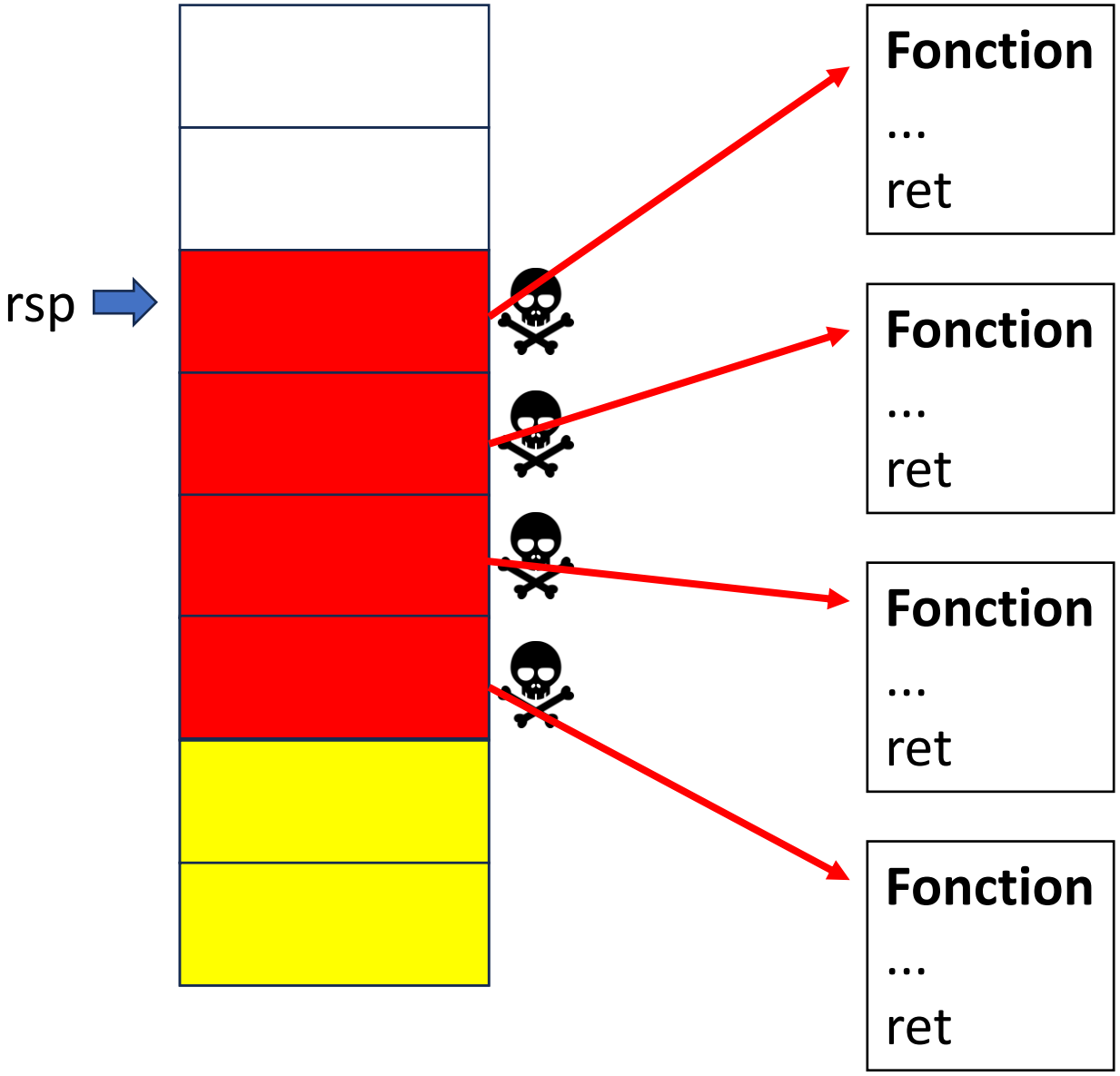
Fonction
...
ret

Fonction
...
ret

rip

Fonction
...
ret

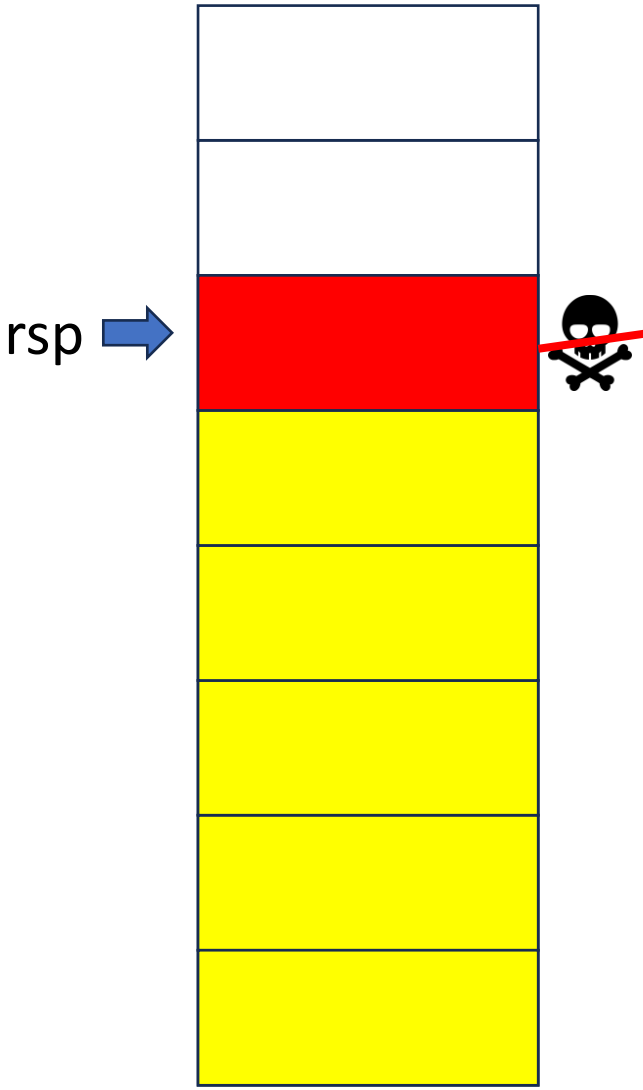
Fonction vulnérable
...
ret



rip

Fonction vulnérable
...
ret

Arg 1	Rdi	???
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???



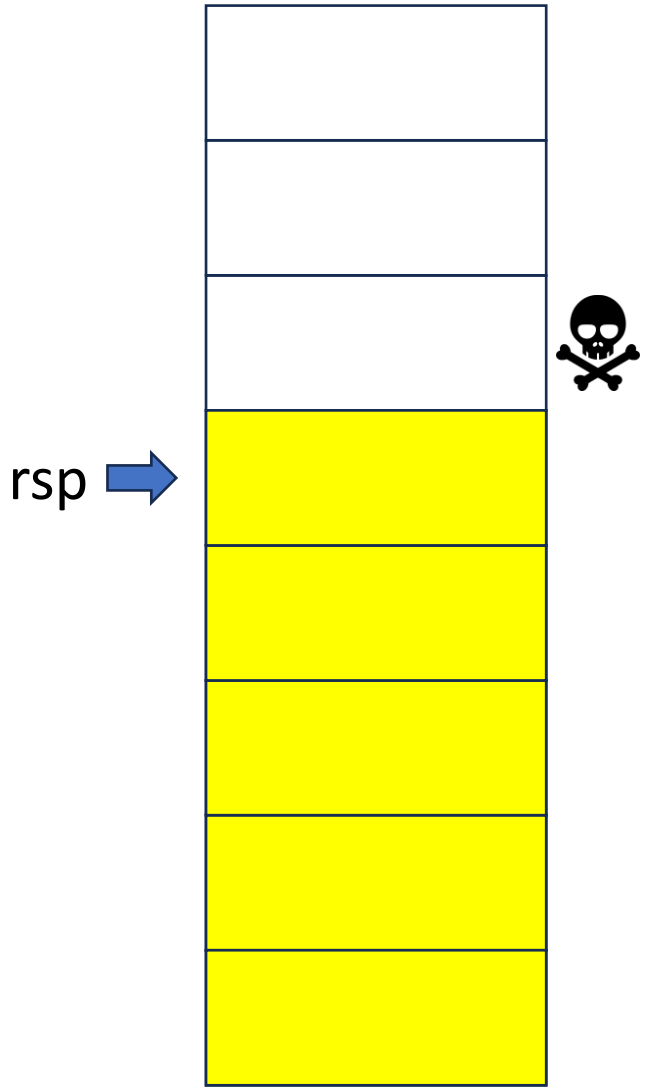
pop rdi
ret

rip

Fonction vulnérable

...
ret

Arg 1	Rdi	???
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???



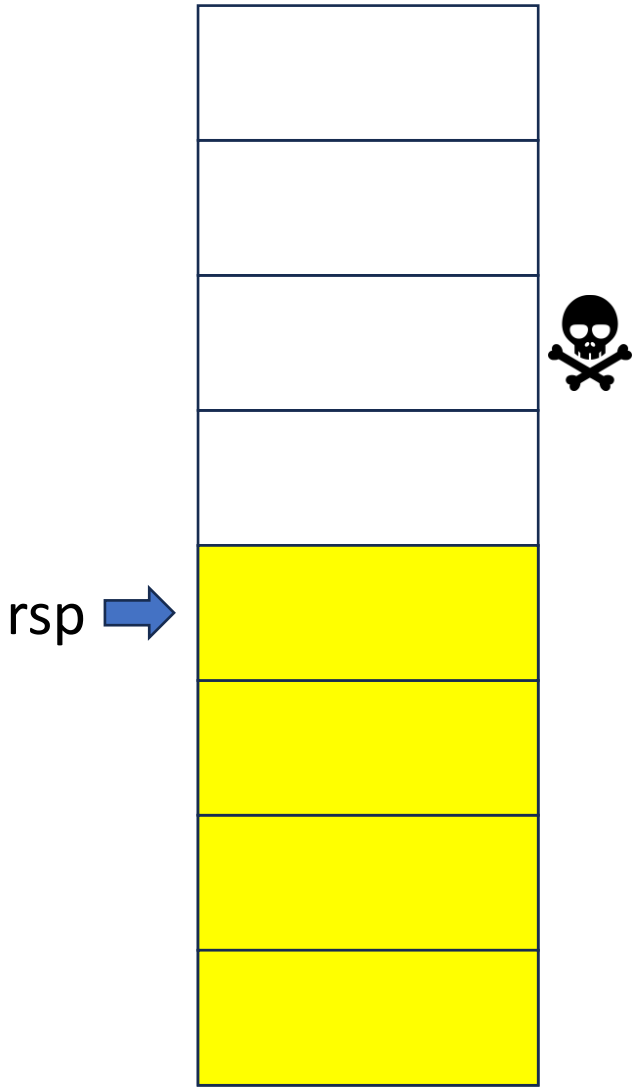
rip

pop rdi
ret

Fonction vulnérable

...
ret

Arg 1	Rdi	???
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???



rip

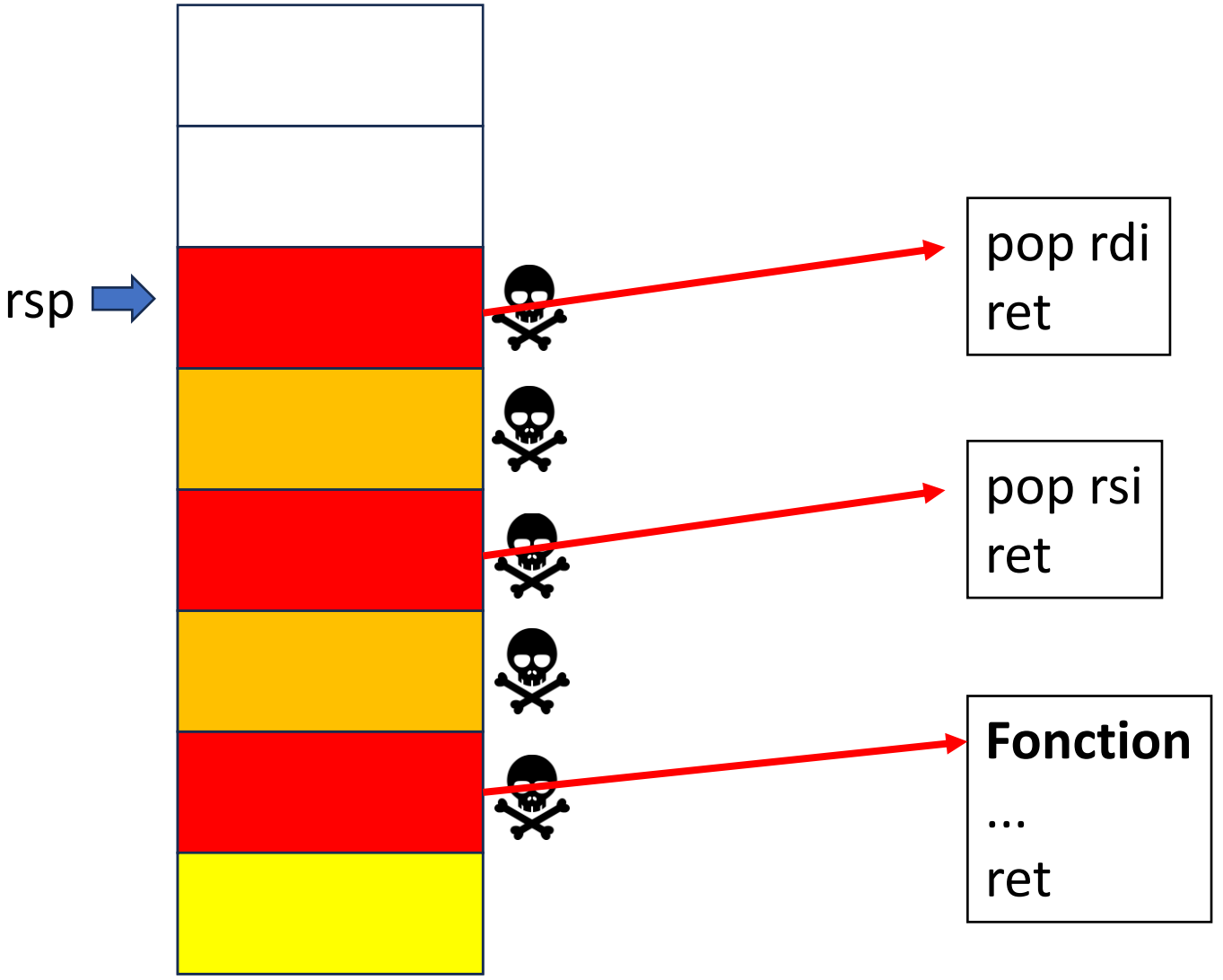
pop rdi
ret

Fonction vulnérable

...
ret

Arg 1	Rdi	
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???


rip
Fonction vulnérable
...
ret
rsp
Fonction appelante
...
call <function vuln>
...



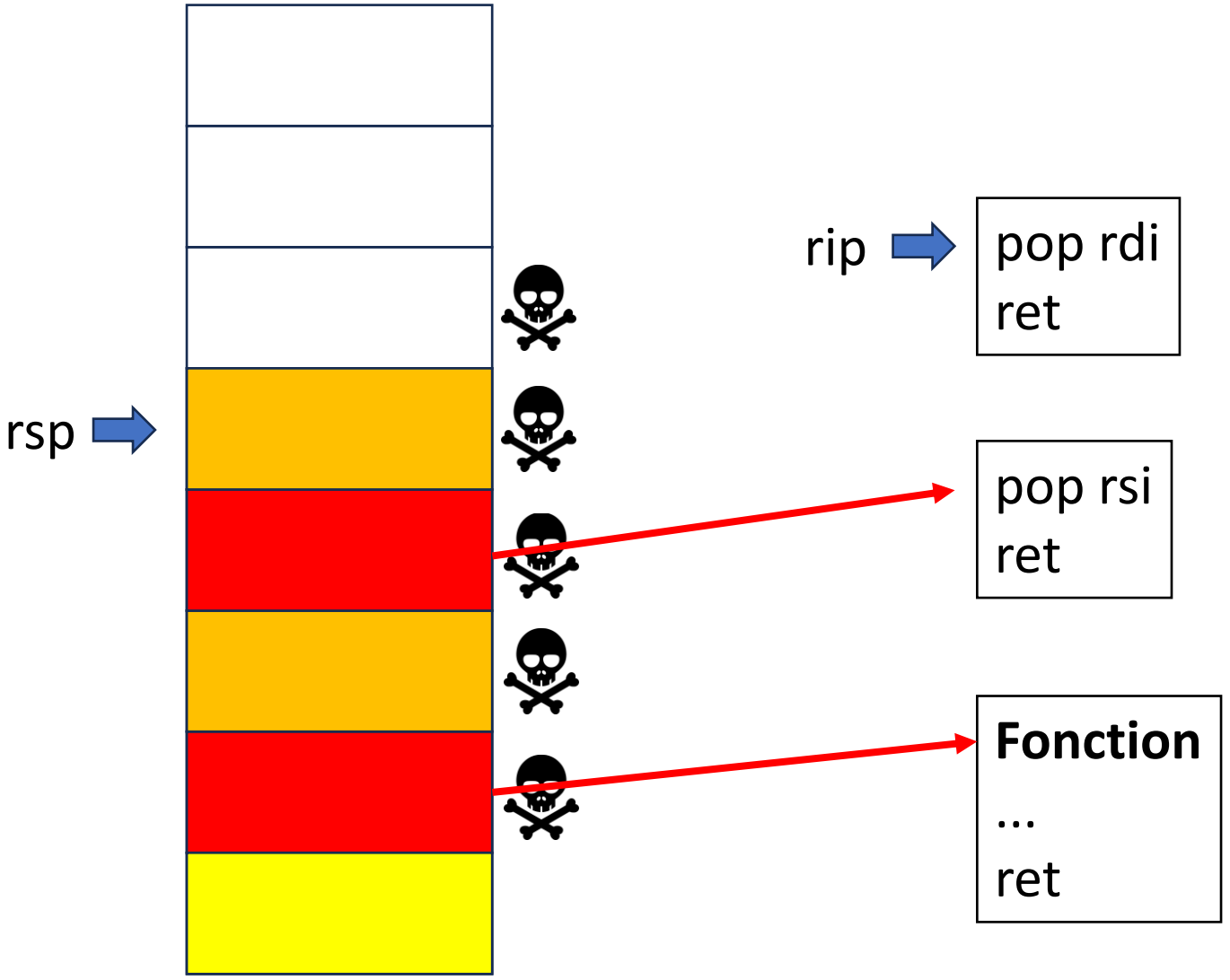
rip

Fonction vulnérable

...

ret

Arg 1	Rdi	???
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???

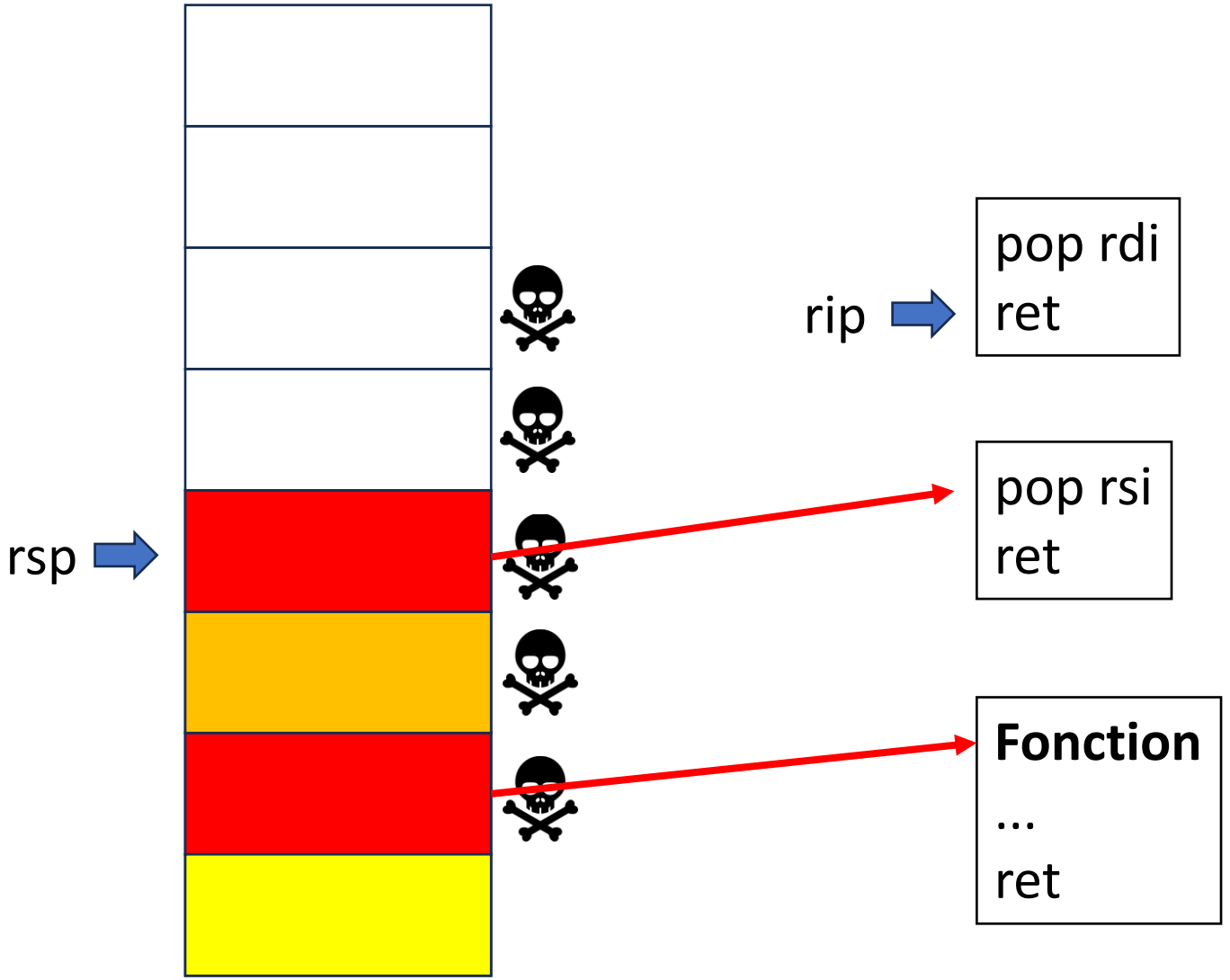


Fonction vulnérable

...

ret

Arg 1	Rdi	???
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???

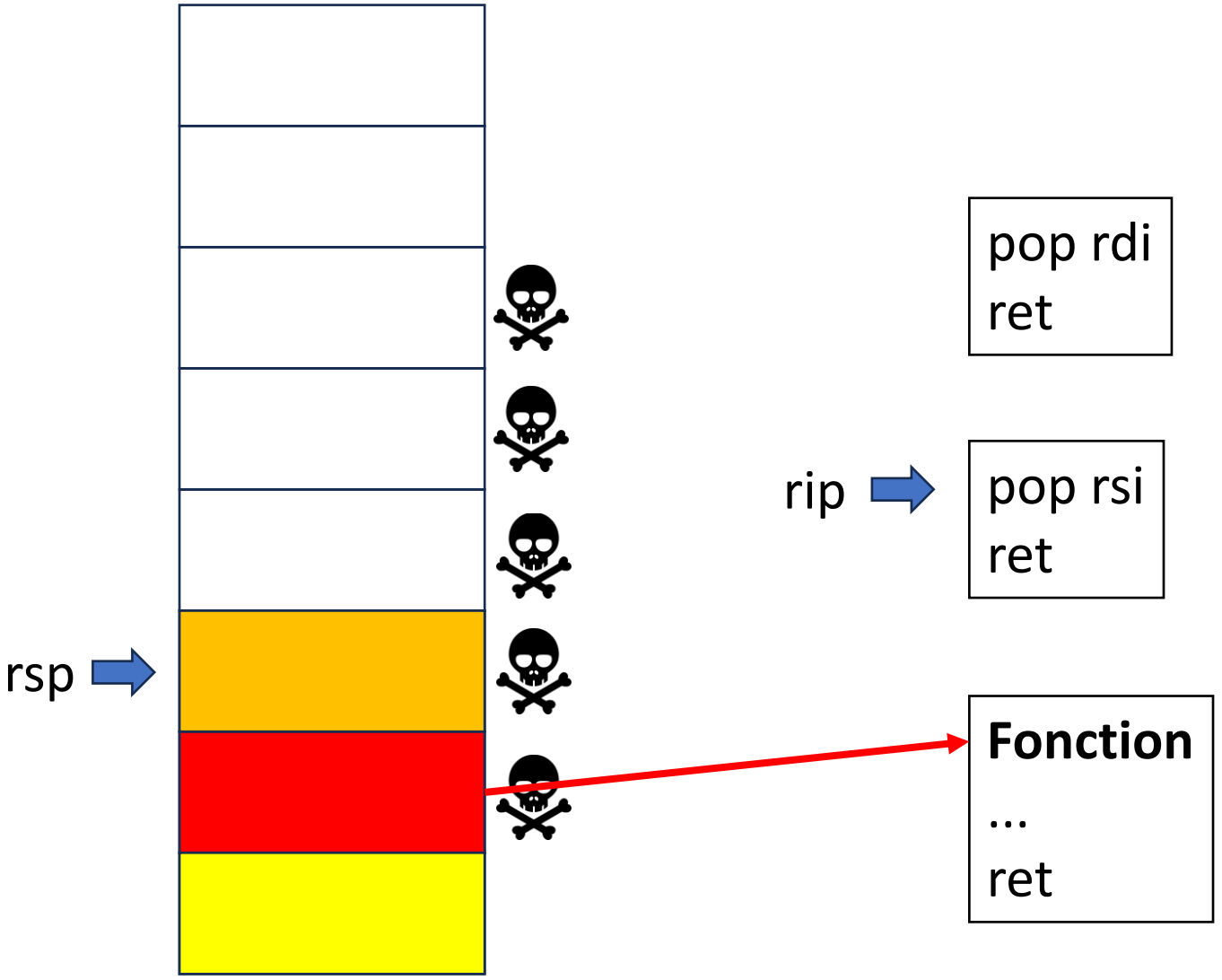


Fonction vulnérable

...

ret

Arg 1	Rdi	
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???

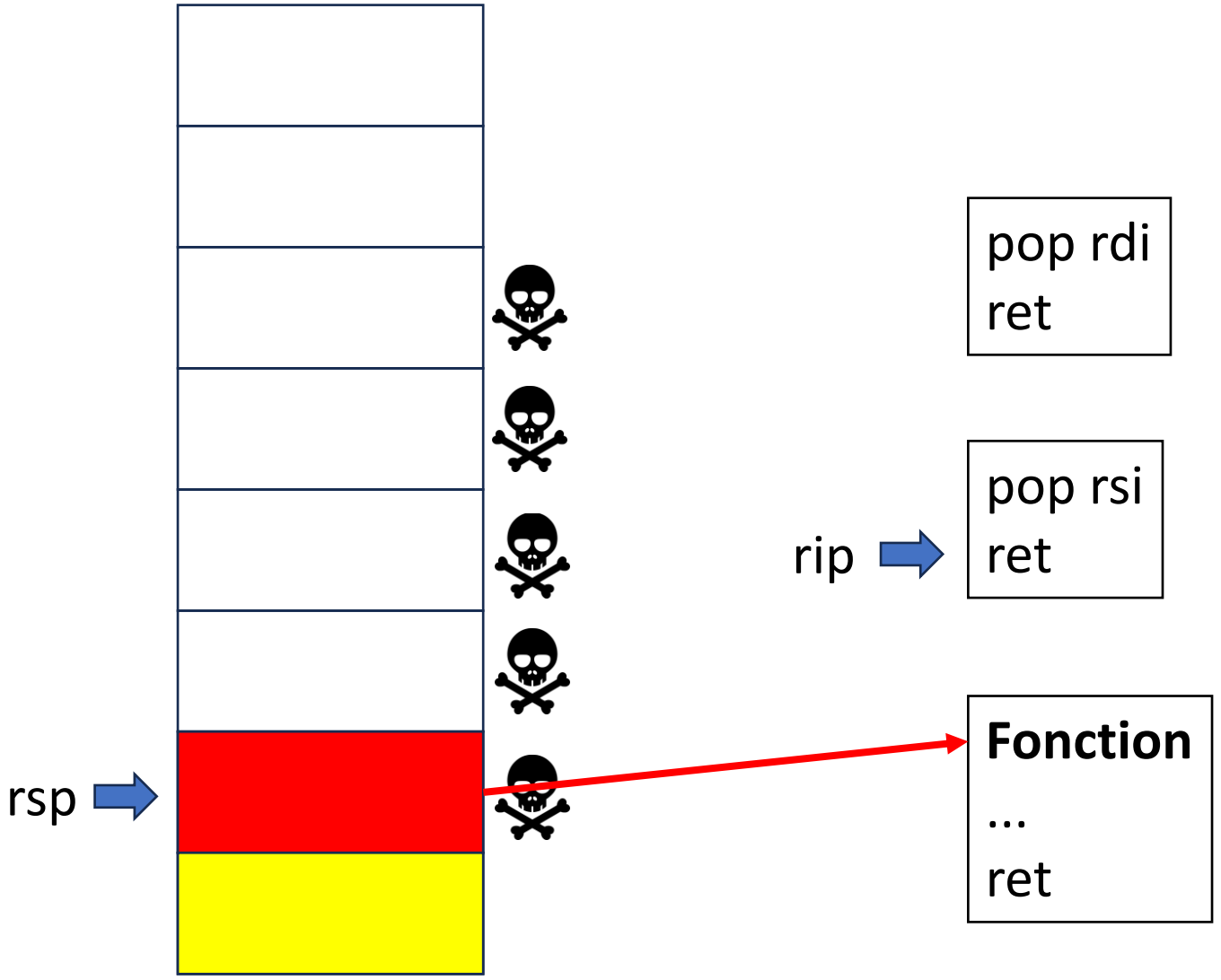


Fonction vulnérable

...

ret

Arg 1	Rdi	
Arg 2	Rsi	???
Arg 3	Rdx	???
Arg 4	Rcx	???


rsp
rip
pop rdi
ret
pop rsi
ret
Fonction
...
ret
Fonction vulnérable
...
ret
Arg 1
Rdi
Arg 2
Rsi
Arg 3
Rdx
???
Arg 4
Rcx
???

Fonction vulnérable

...

ret

pop rdi

ret

pop rsi

ret

rip

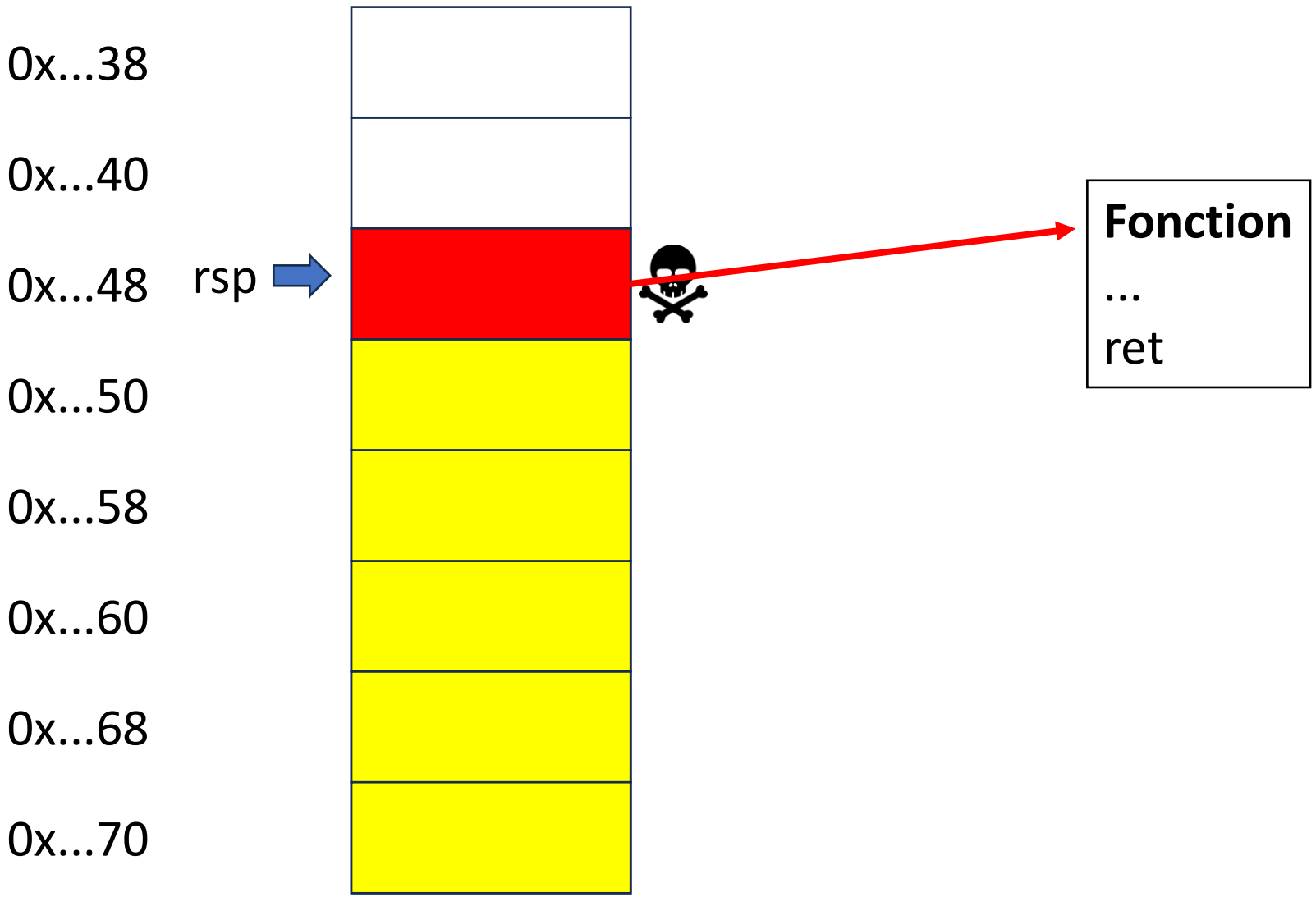
Fonction

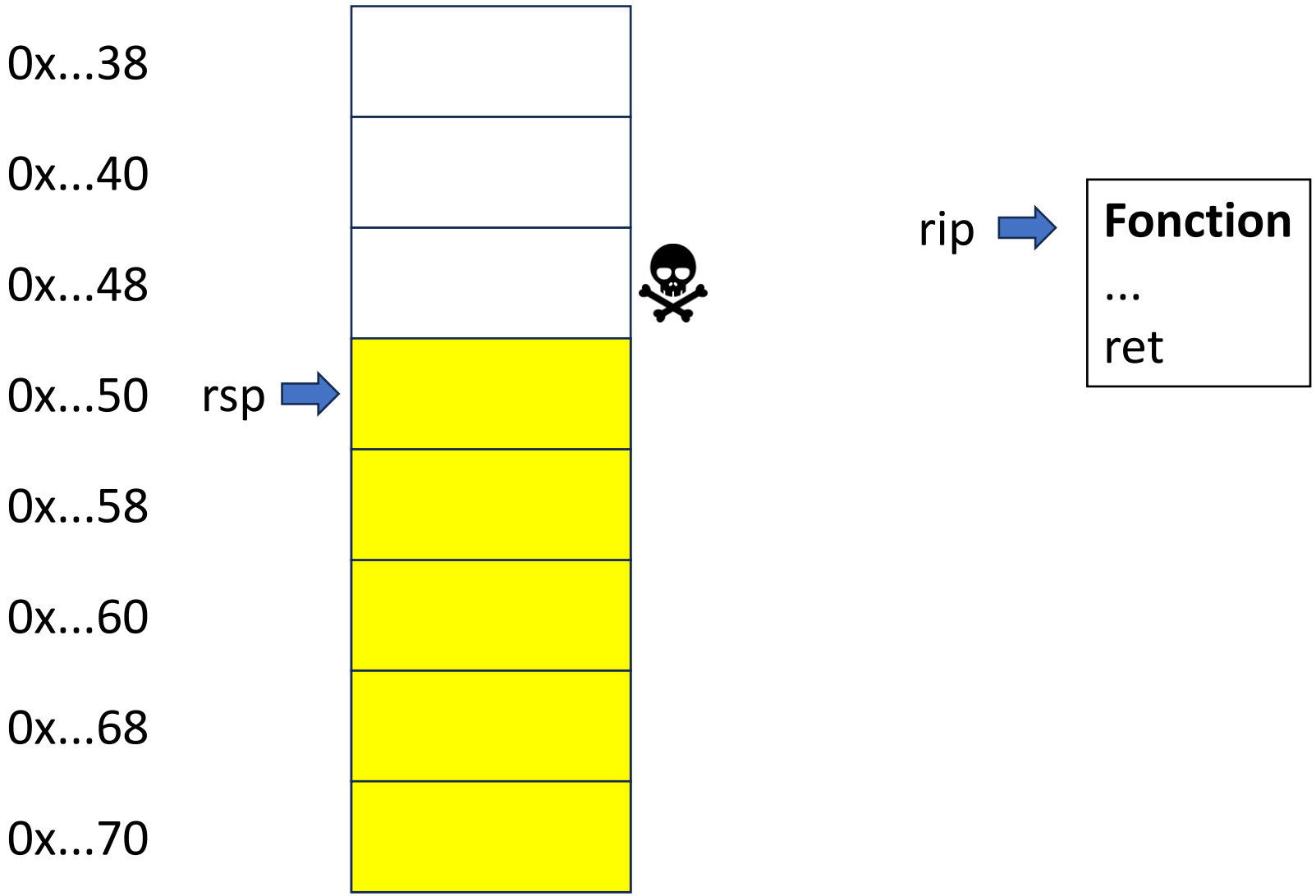
...

ret

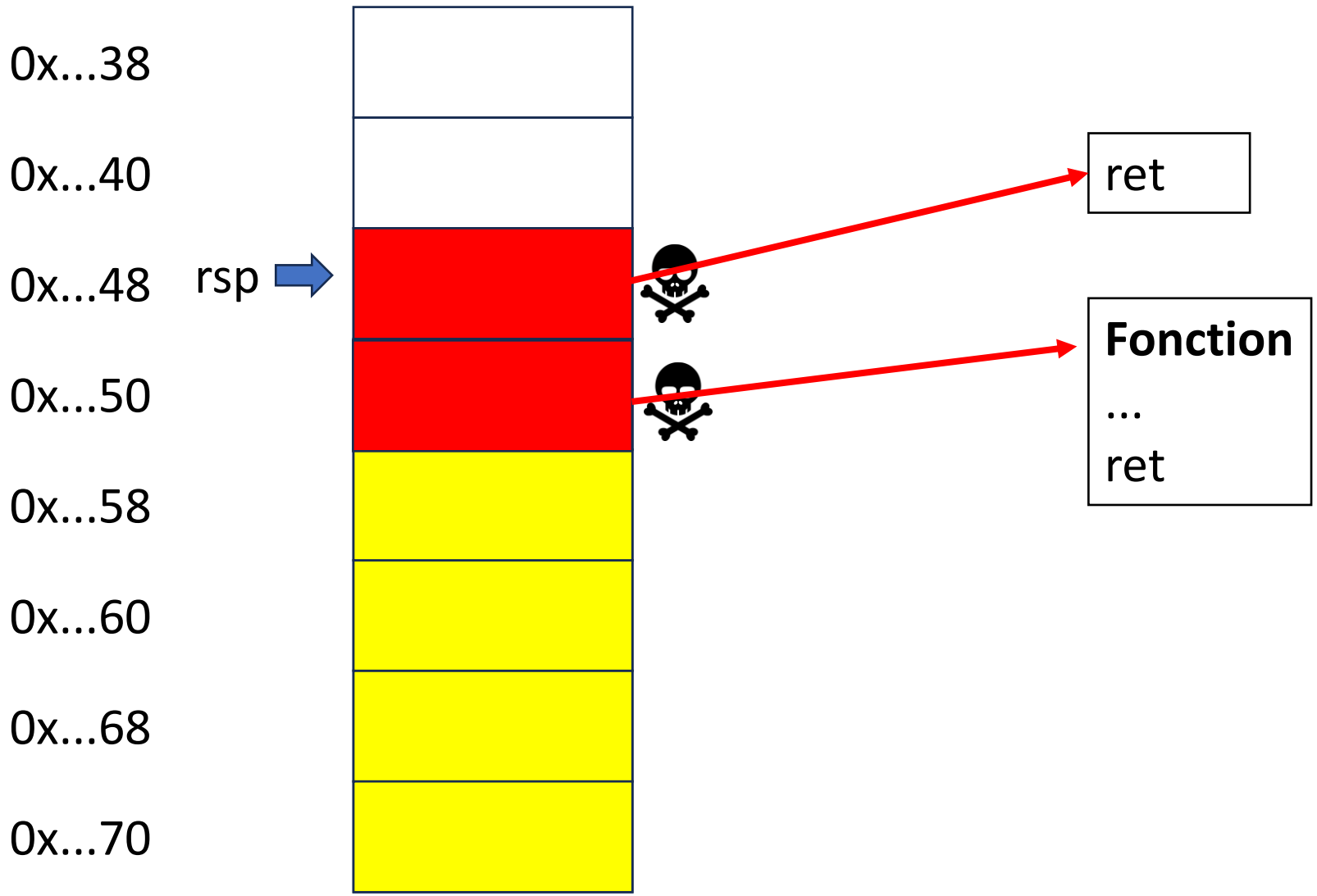
Arg 1	Rdi	
Arg 2	Rsi	
Arg 3	Rdx	???
Arg 4	Rcx	???

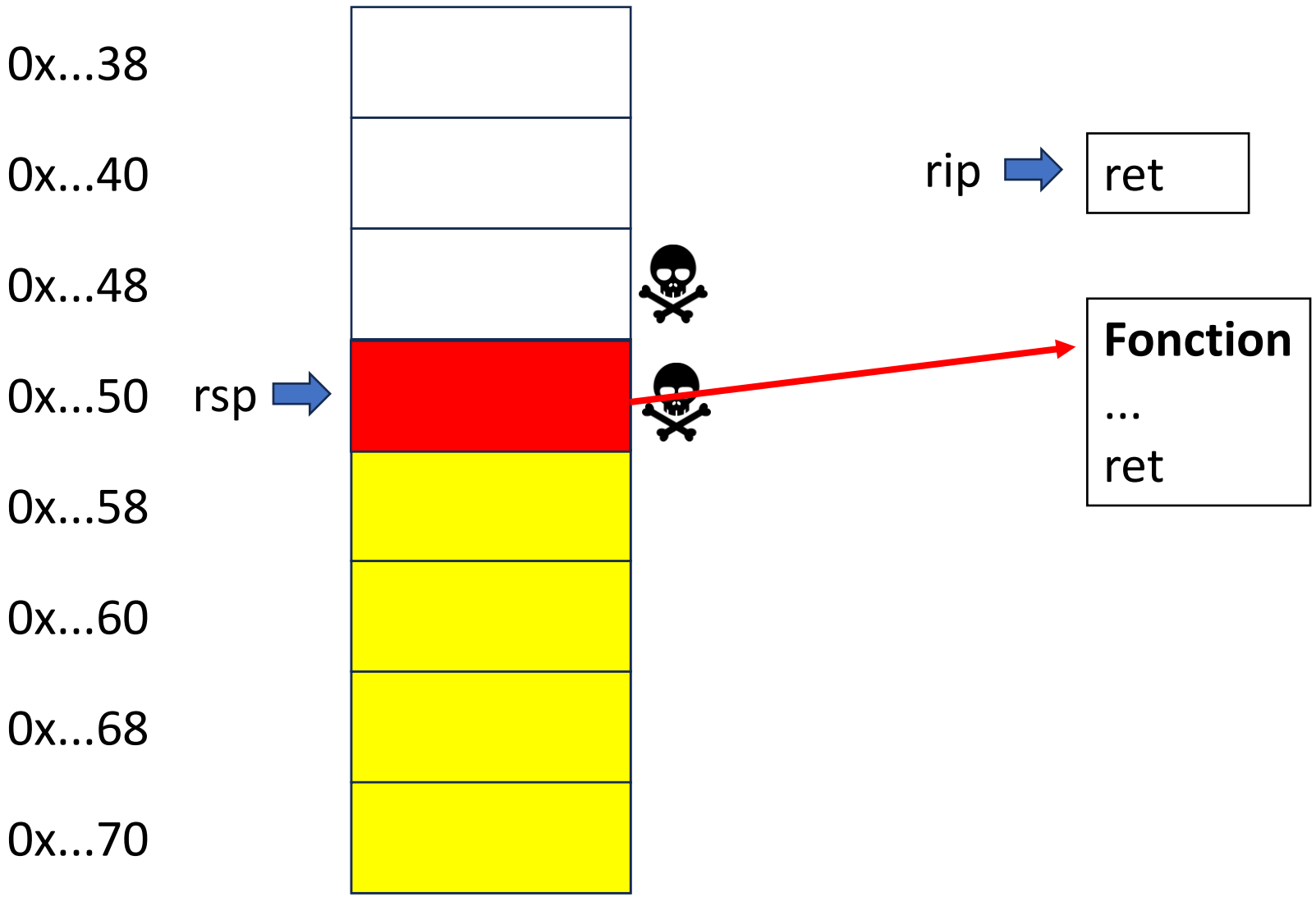

0x...38
0x...40
rsp
0x...48
0x...50
0x...58
0x...60
0x...68
0x...70

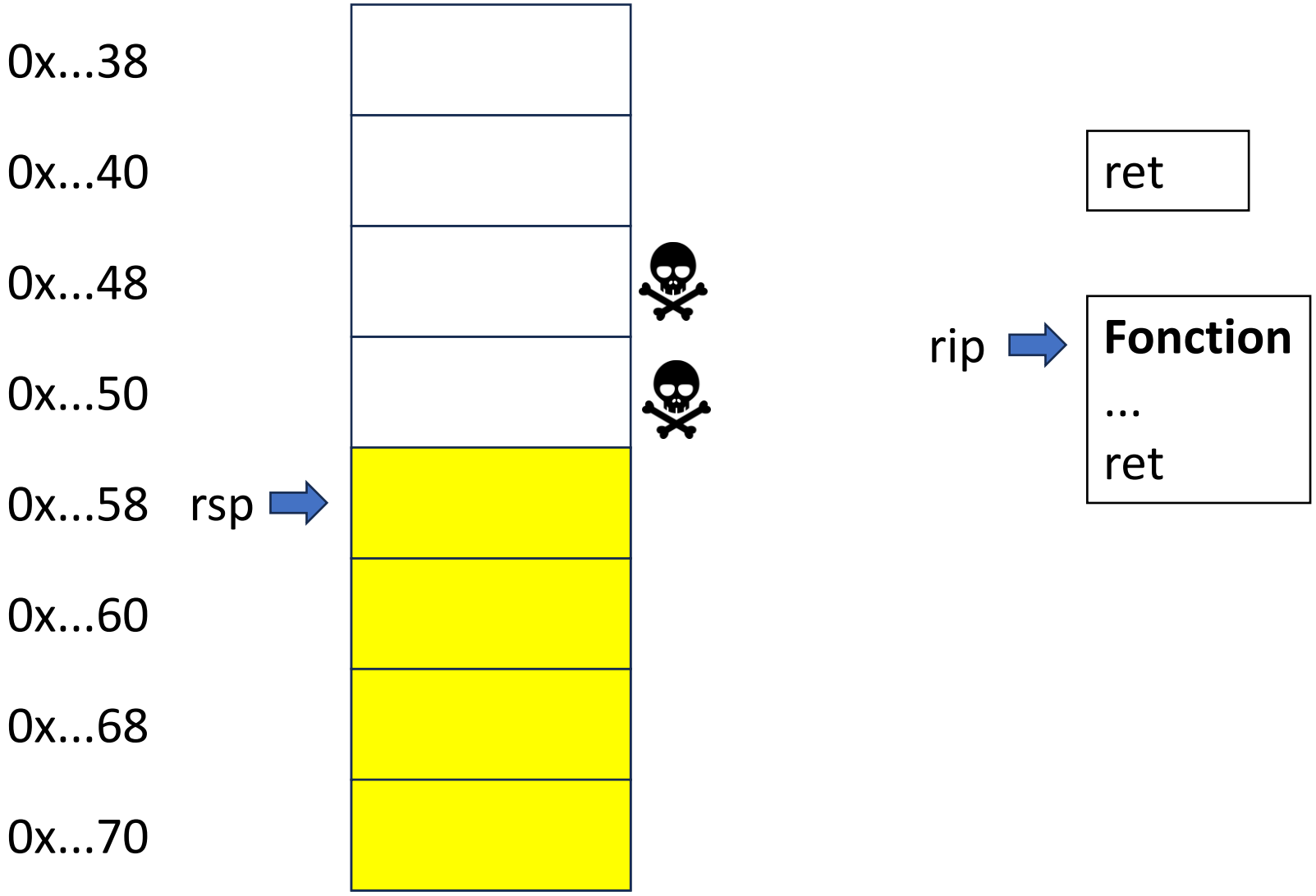

0x...38
0x...40
rsp
0x...48
0x...50
0x...58
0x...60
0x...68
0x...70
Fonction
...
ret


0x...38
0x...40
0x...48
0x...50
rsp
0x...58
0x...60
0x...68
0x...70
rip
Fonction
...
ret

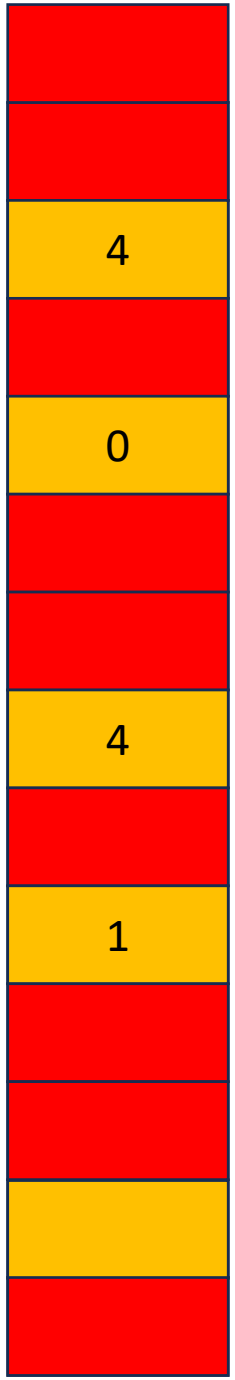

0x...38
0x...40
rsp
0x...48
0x...50
0x...58
0x...60
0x...68
0x...70


0x...38
0x...40
0x...48
0x...50
0x...58
0x...60
0x...68
0x...70
rsp
ret
Fonction
...
ret


0x...38
0x...40
0x...48
0x...50
0x...58
0x...60
0x...68
0x...70
rsp
rip
ret
Fonction
...
ret


0x...38
0x...40
0x...48
0x...50
0x...58
rsp
0x...60
0x...68
0x...70
ret
rip
Fonction
...
ret

```
dup2(4, 0);
dup2(4, 1);
system(“/bin/sh”);
```



ret

pop rdi
ret

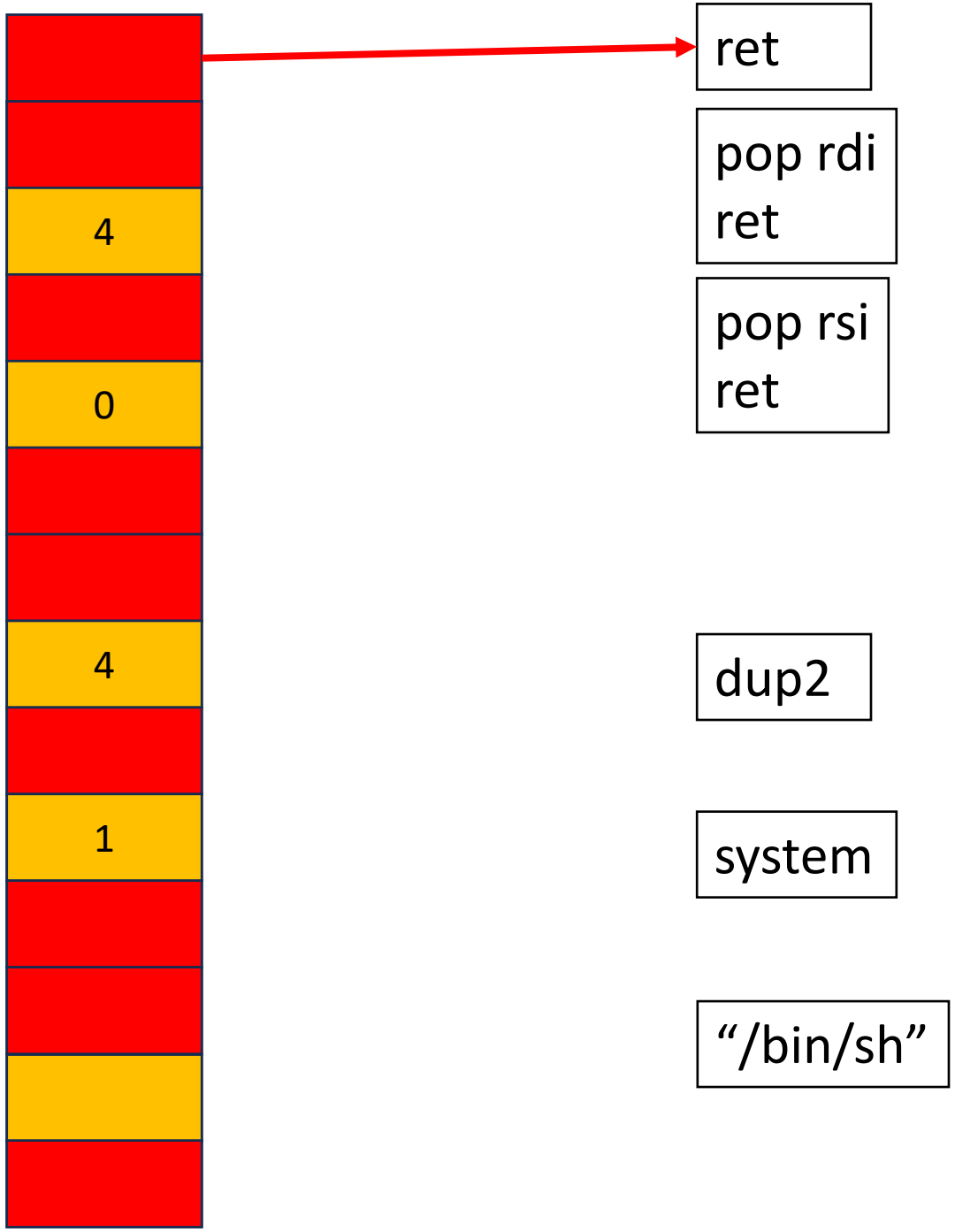
pop rsi
ret

dup2

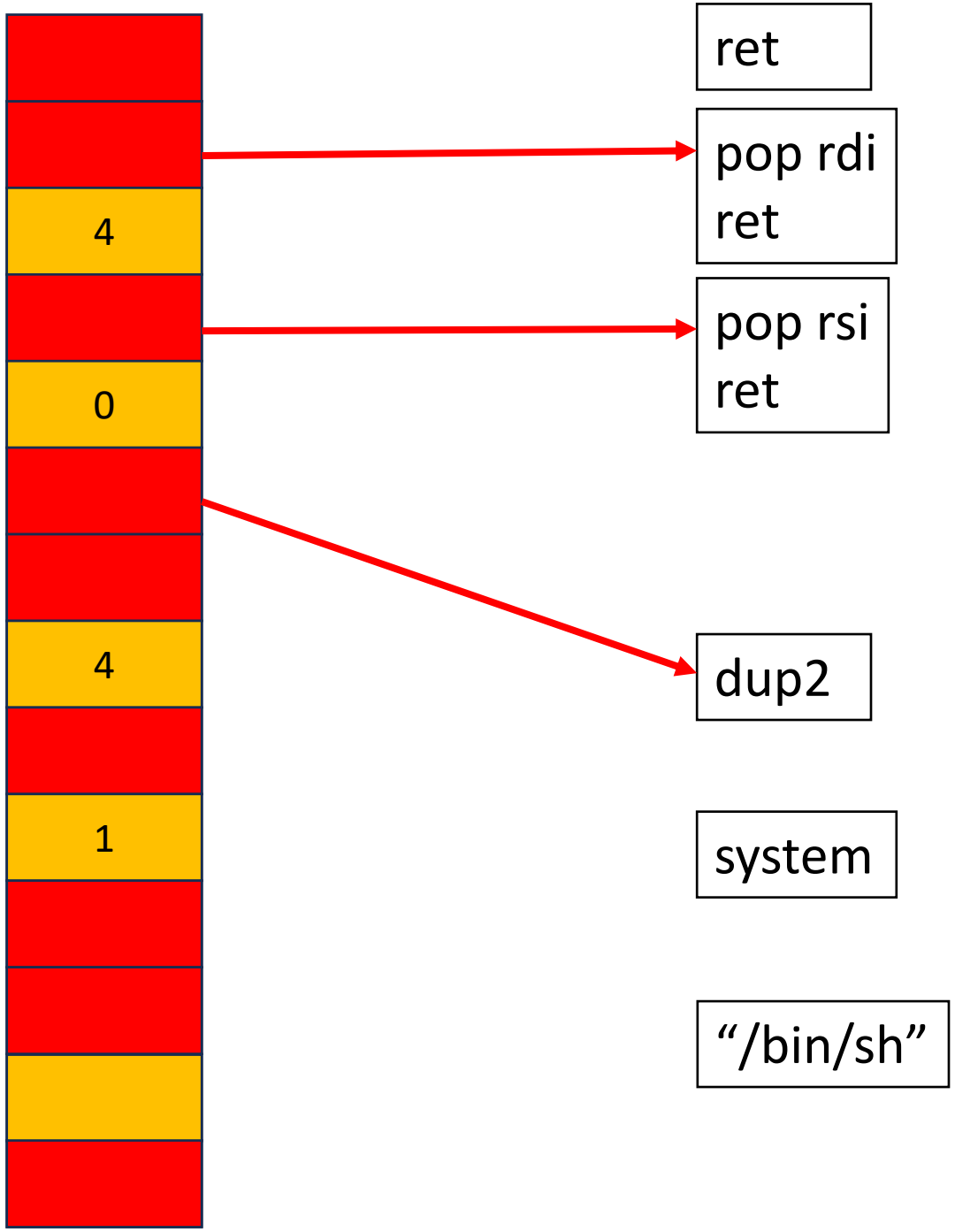
system

“/bin/sh”

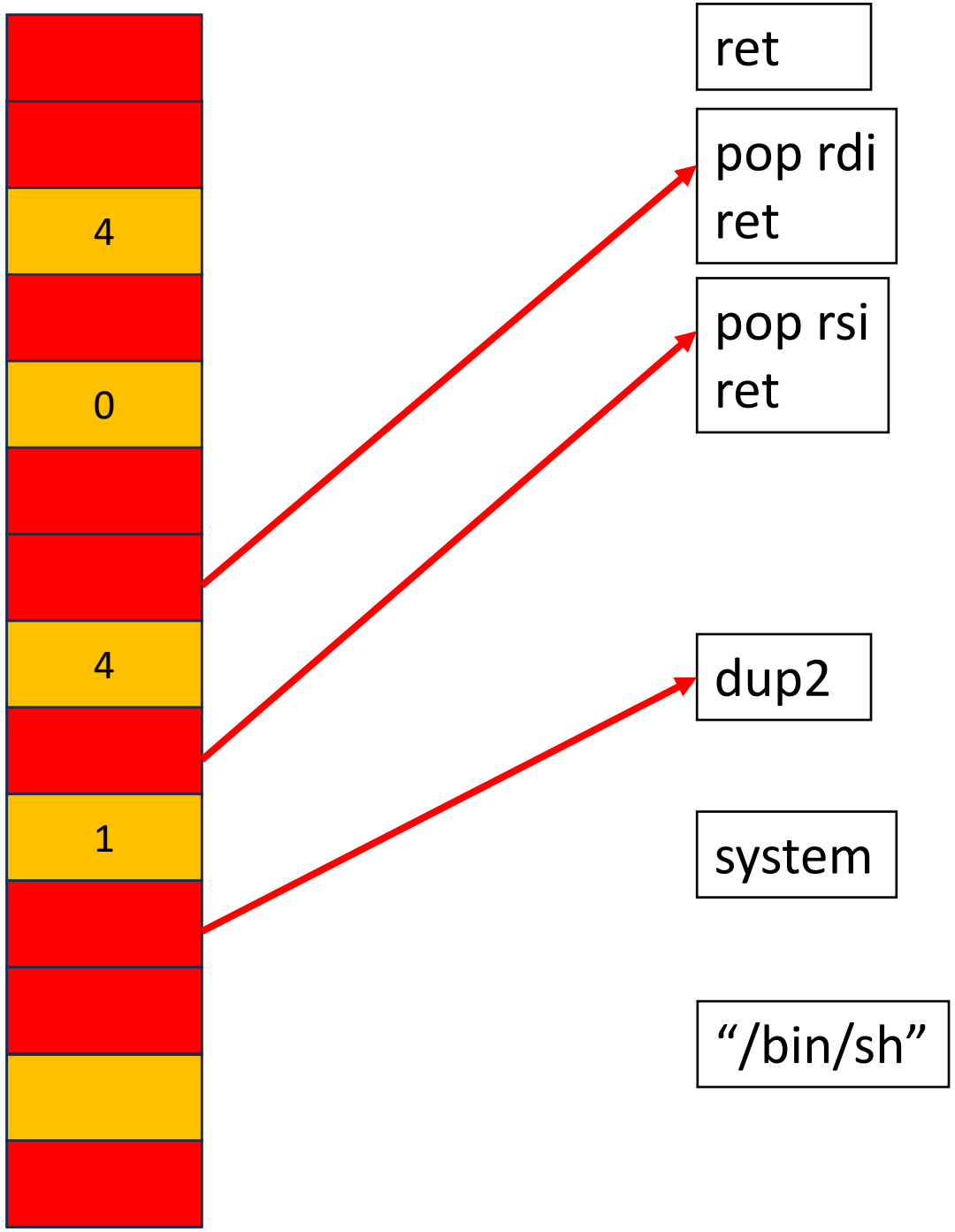
dup2(4, 0);
dup2(4, 1);
system(“/bin/sh”);



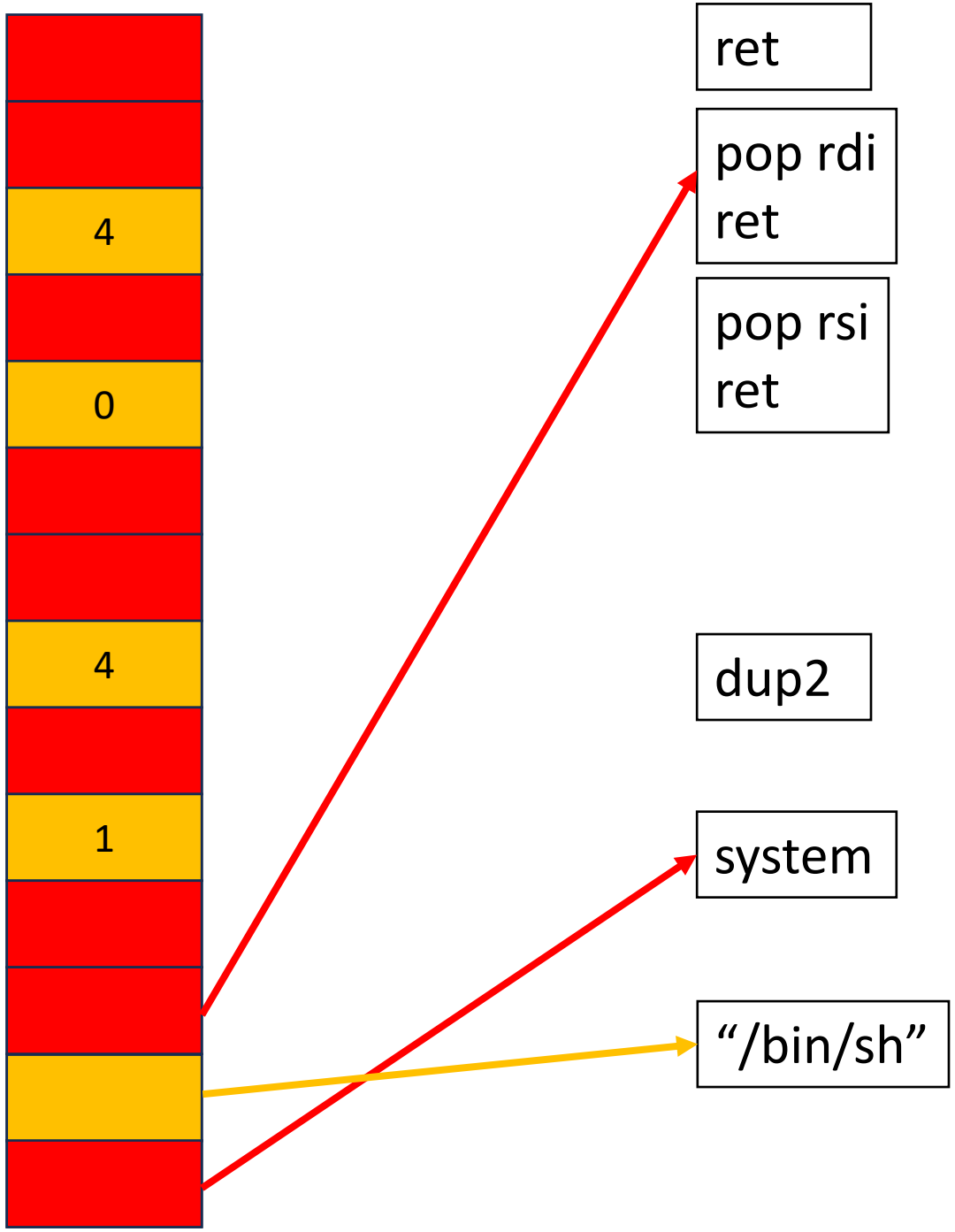
dup2(4, 0);
dup2(4, 1);
system(“/bin/sh”);



dup2(4, 0);
dup2(4, 1);
system("/bin/sh");



dup2(4, 0);
dup2(4, 1);
system(“/bin/sh”);



dup2(4, 0);
dup2(4, 1);
system(“/bin/sh”);