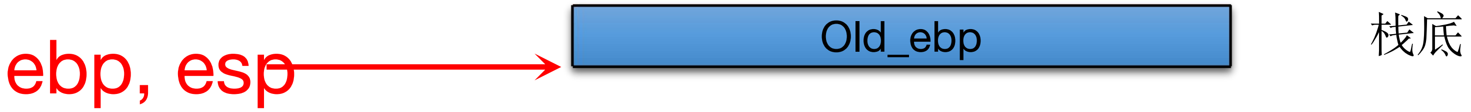
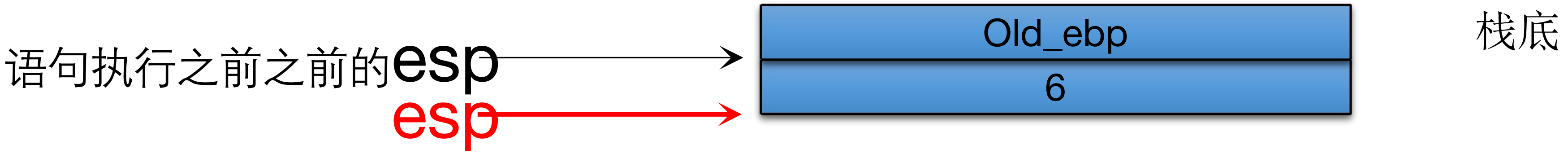
```
push ebp
mov  ebp,esp
push 6
push 5
call AFunc
add esp,8
```



PS: 执行语句之前的EBP在此栈空间的更高处

```
push ebp
mov  ebp,esp
push 6
push 5
call AFunc
add esp,8
```



语句执行之前之前的esp

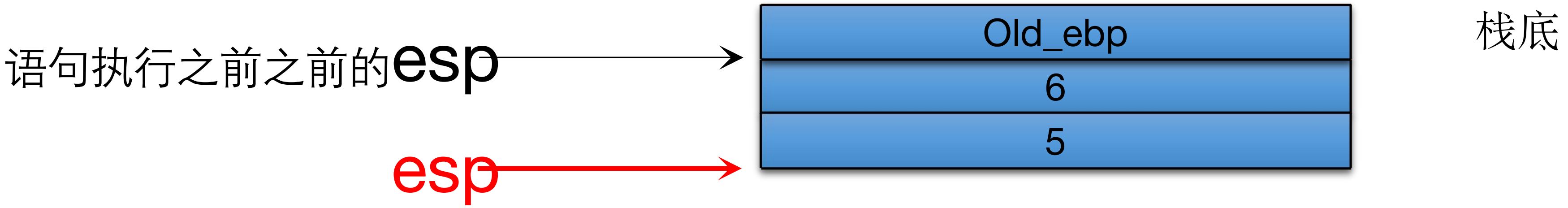
esp

Old_ebp

6

栈底

```
push ebp
mov  ebp,esp
push 6
push 5
call AFunc
add esp,8
```



语句执行之前之前的esp

esp

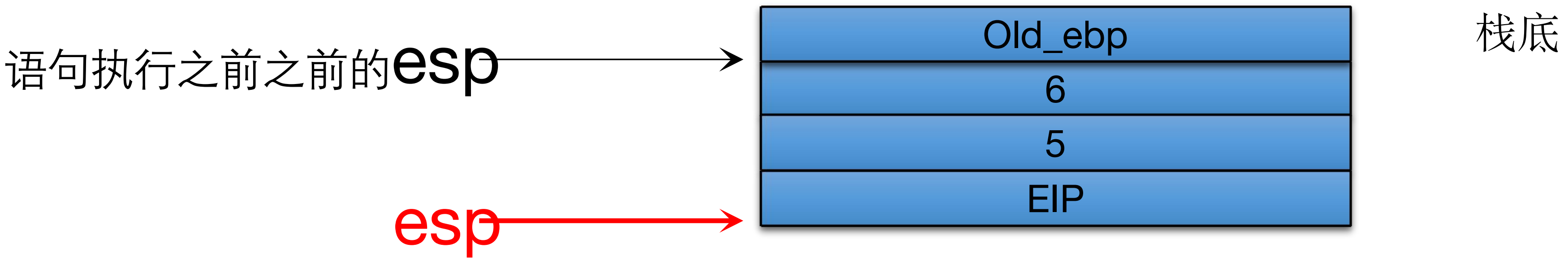
Old_ebp

6

5

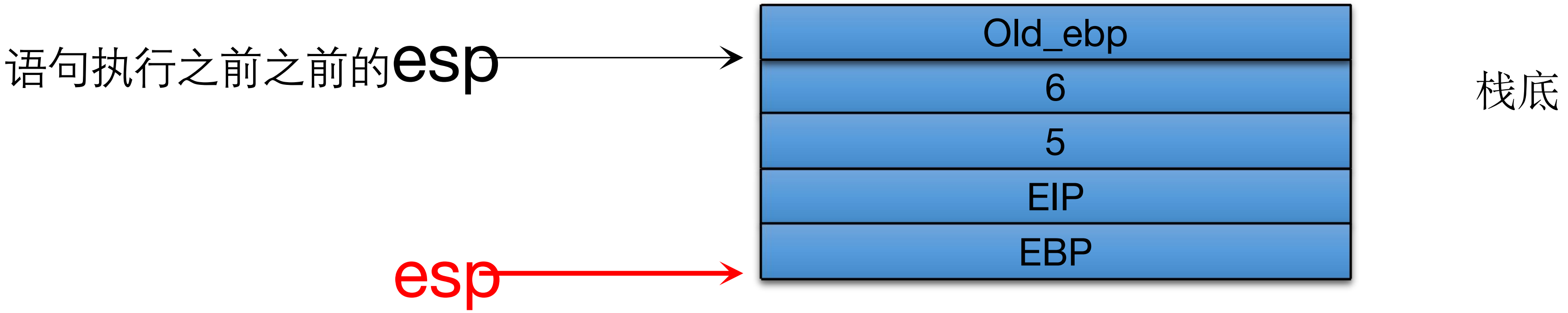
栈底

```
push ebp
mov  ebp,esp
push 6
push 5
call AFunc
add esp,8
```



```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8
```

```
AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

Old_ebp

6

5

EIP

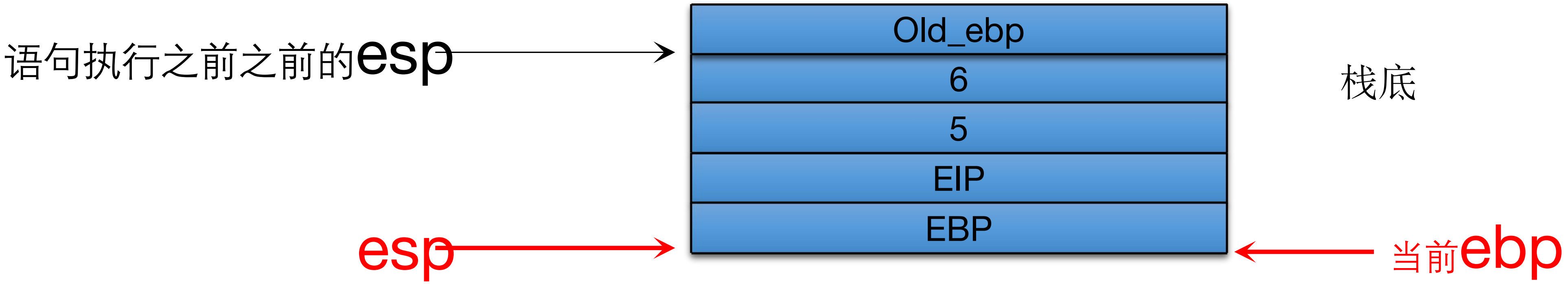
EBP

esp

栈底

```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

Old_ebp

6

5

EIP

EBP

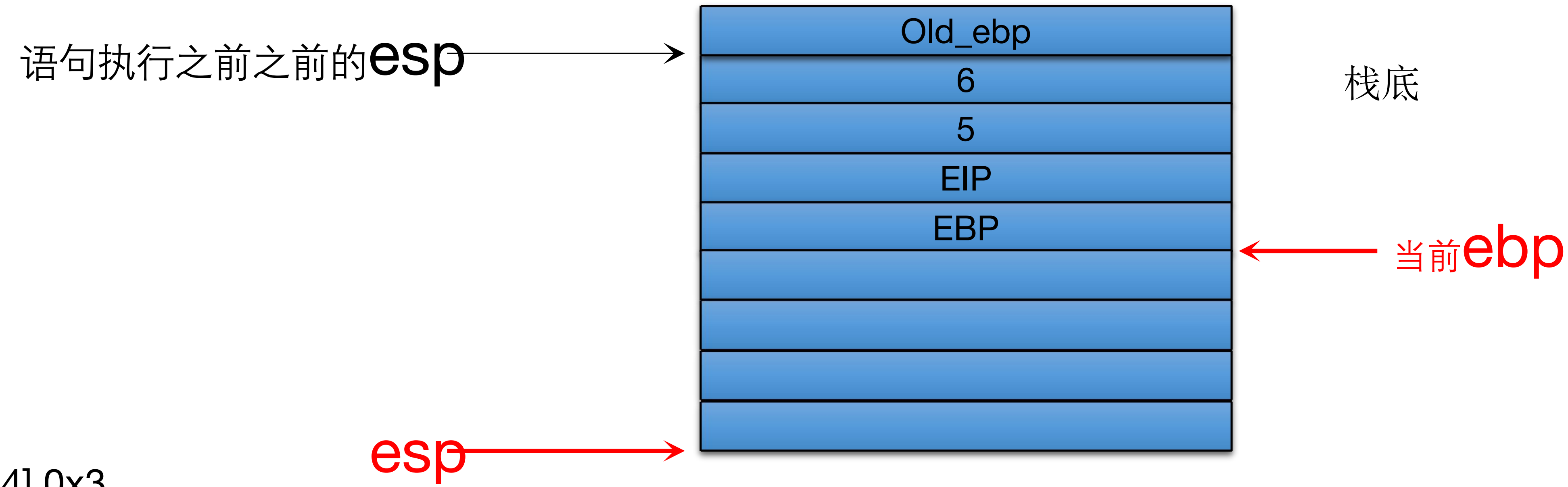
栈底

esp

当前ebp

```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8
```

```
AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

Old_ebp

6

5

EIP

EBP

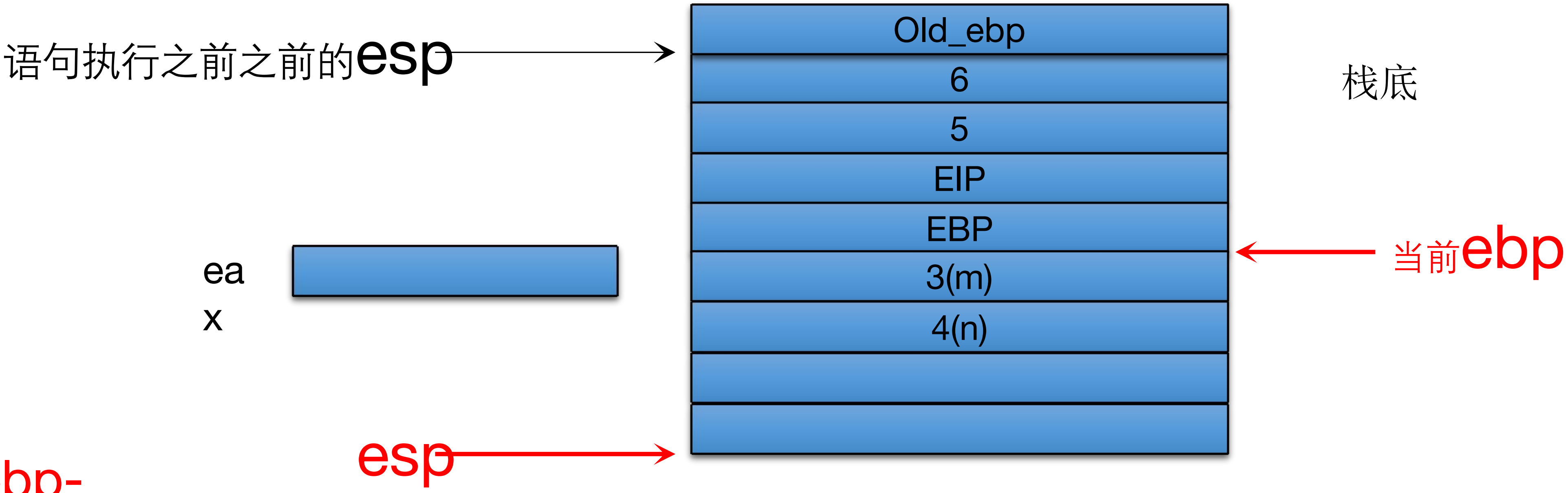
栈底

当前ebp

esp

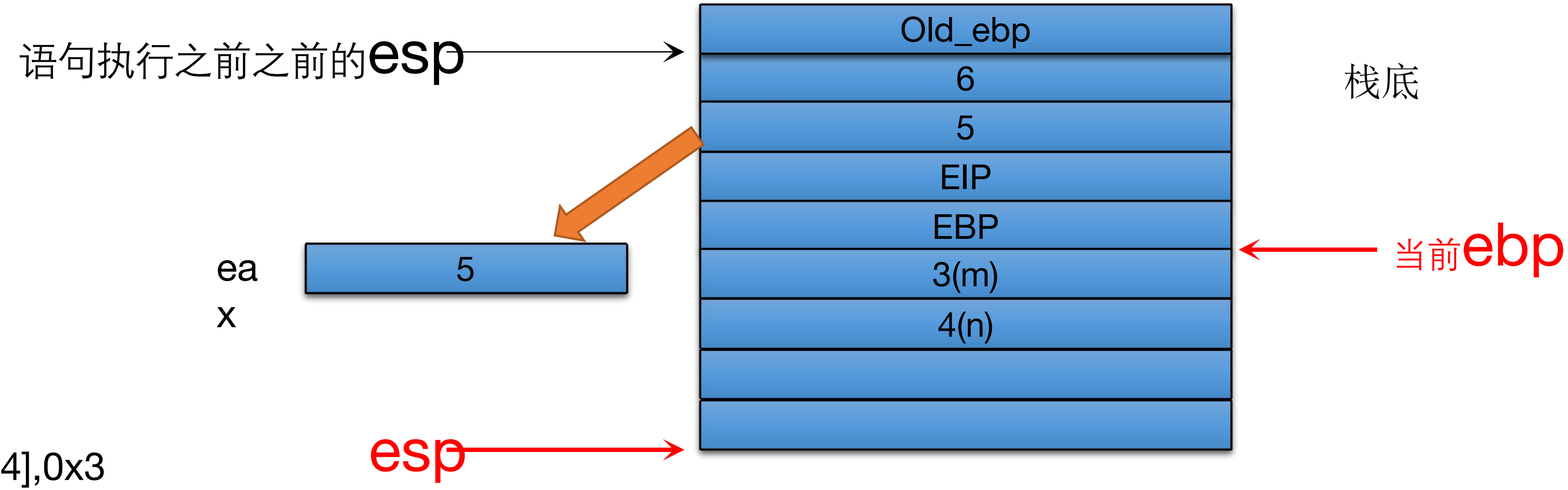
```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
```



```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

Old_ebp

6

5

EIP

EBP

3(m)

4(n)

栈底

当前ebp

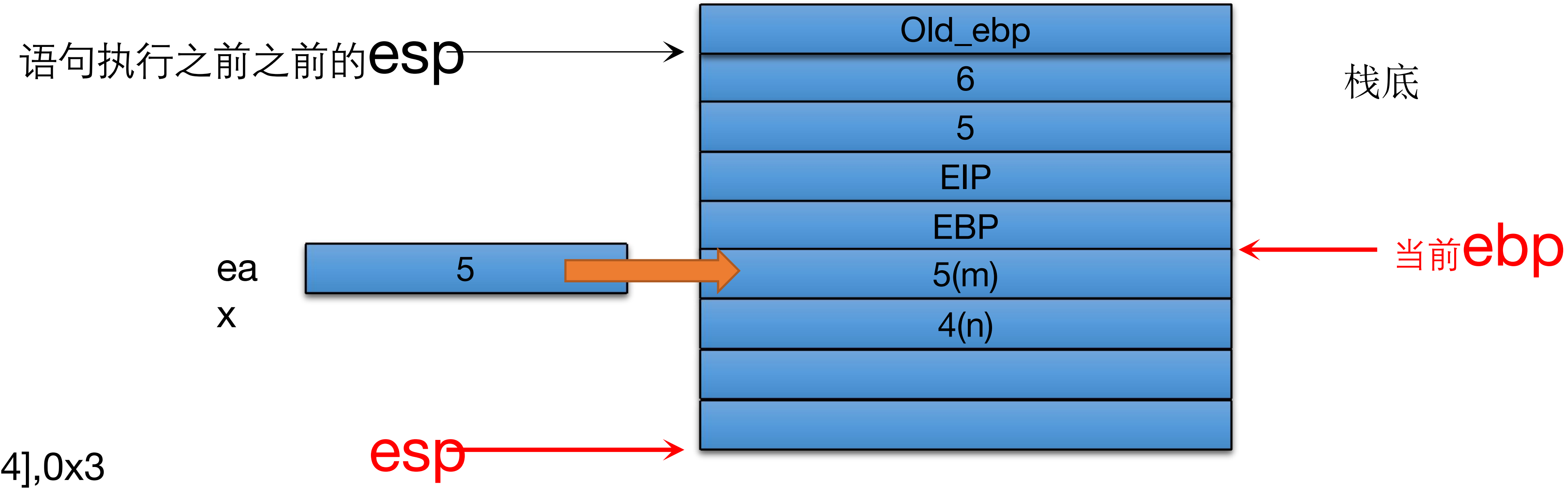
eax

5

esp

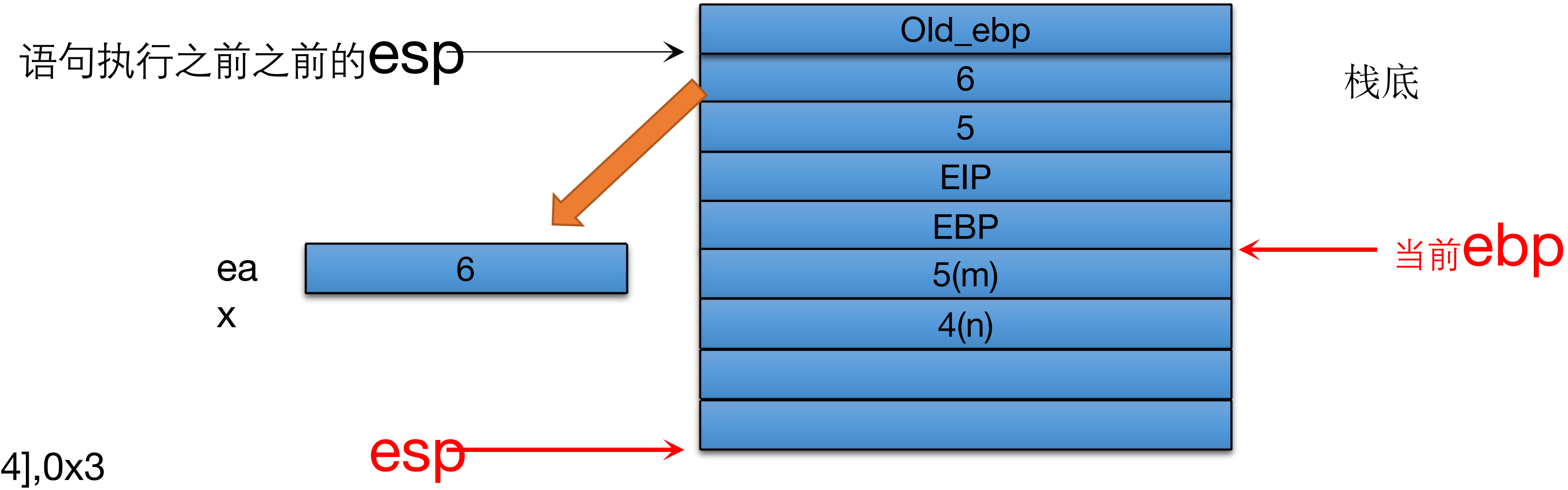
```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

Old_ebp

6

5

EIP

EBP

5(m)

4(n)

栈底

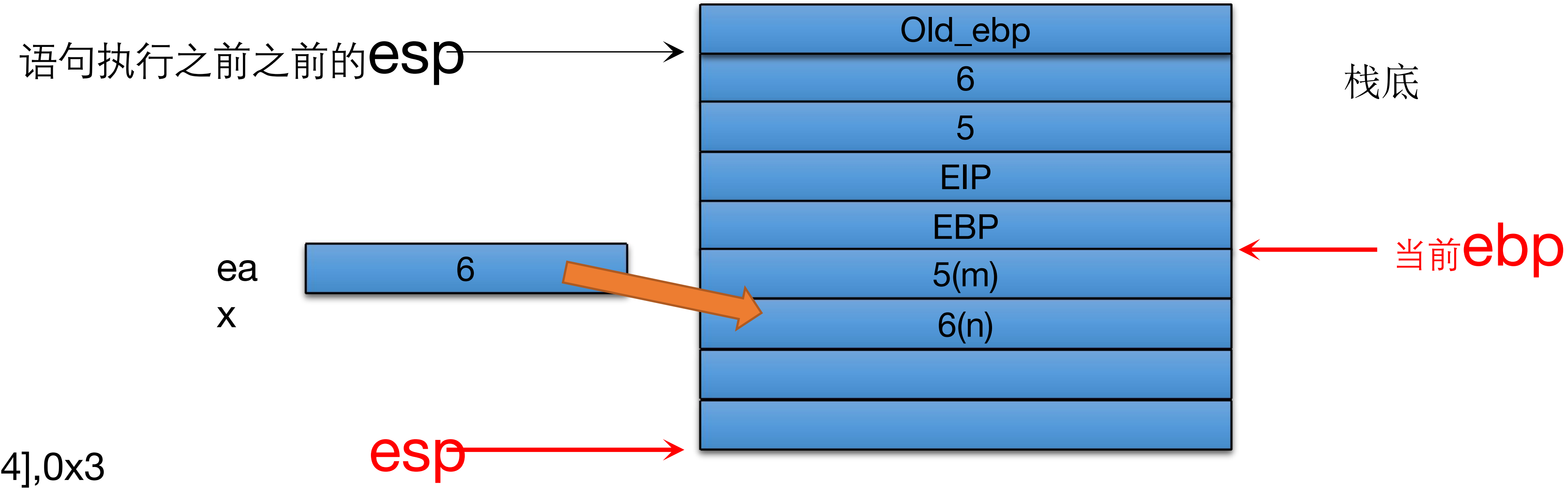
当前ebp

eax 6

esp

```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8
```

```
AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

栈底

Old_ebp

6

5

EIP

EBP

5(m)

6(n)

当前ebp

eax

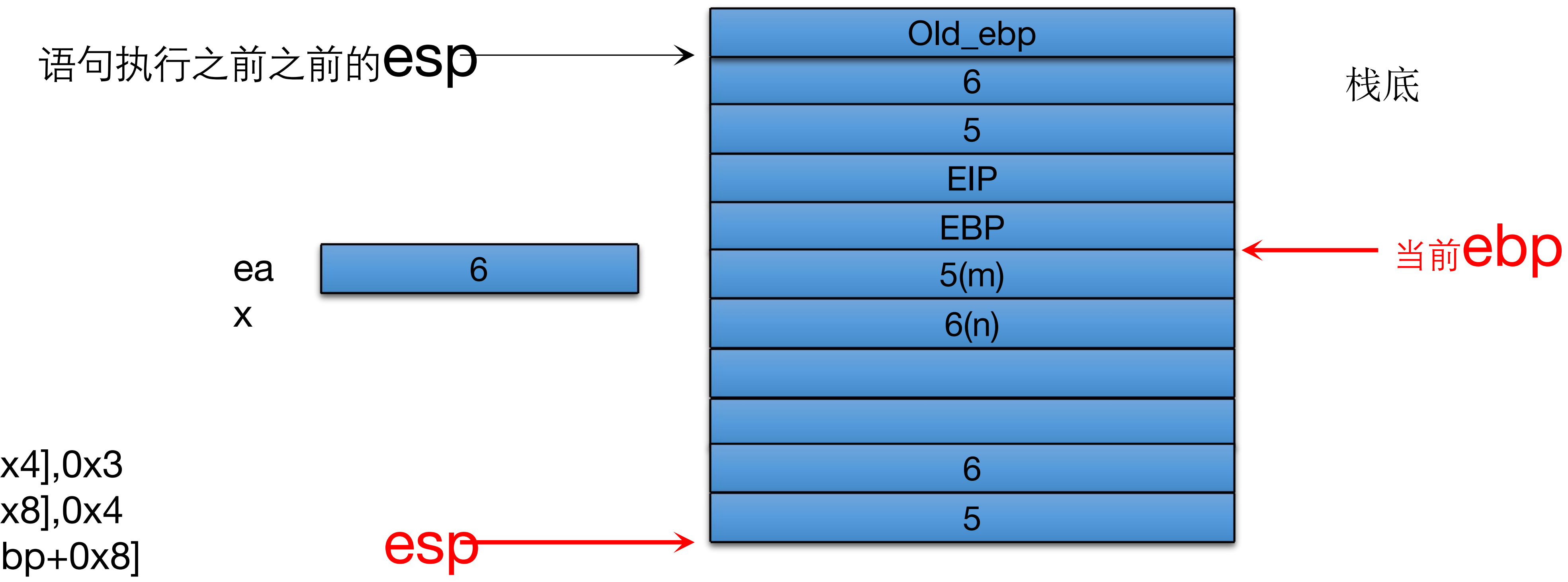
6

esp

```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8
```

AFunc

```
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

栈底

当前ebp

esp

eax

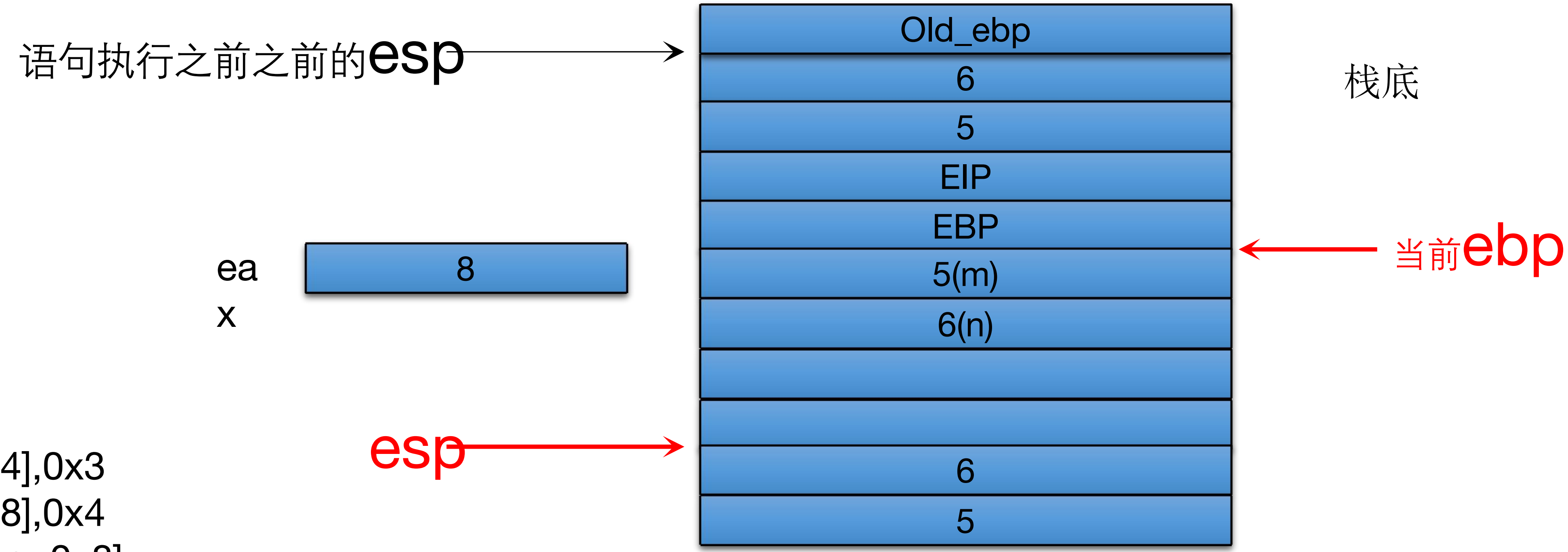
6

Old_ebp
6
5
EIP
EBP
5(m)
6(n)

6
5

```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



语句执行之前之前的esp

栈底

Old_ebp

6

5

EIP

EBP

5(m)

6(n)

6

5

当前ebp

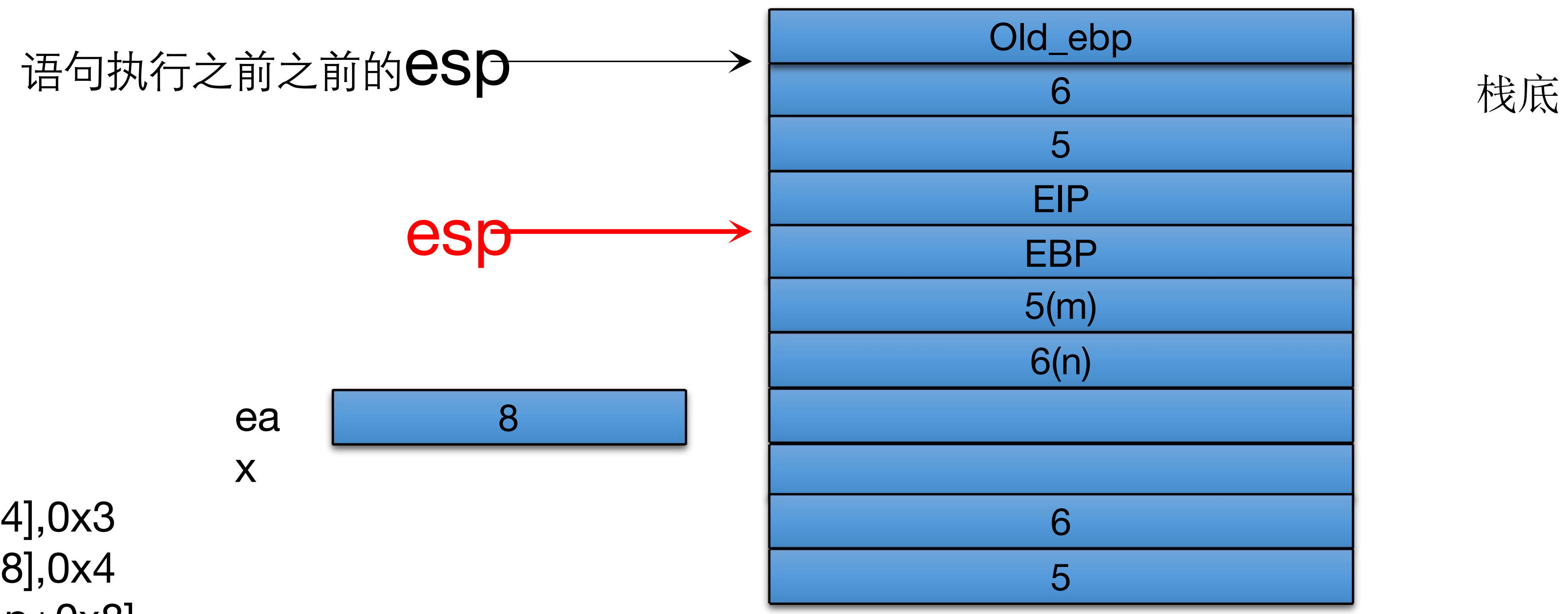
eax

8

esp

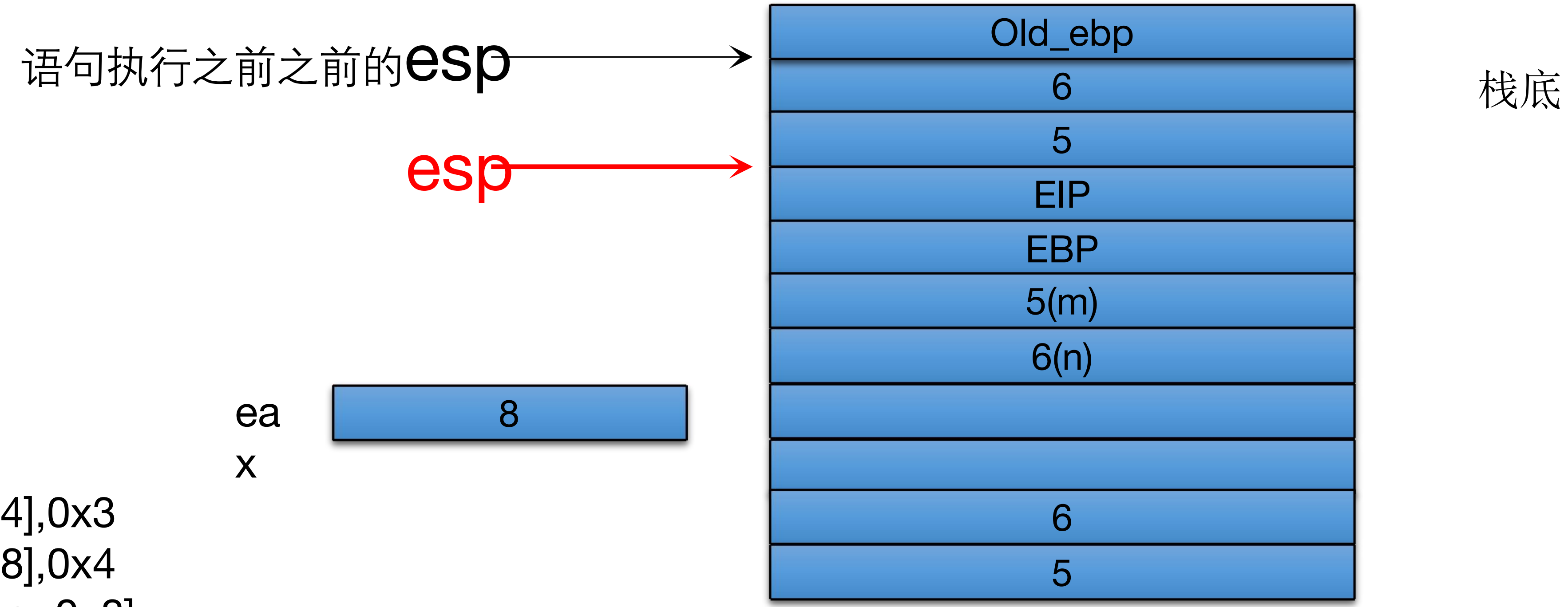
```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



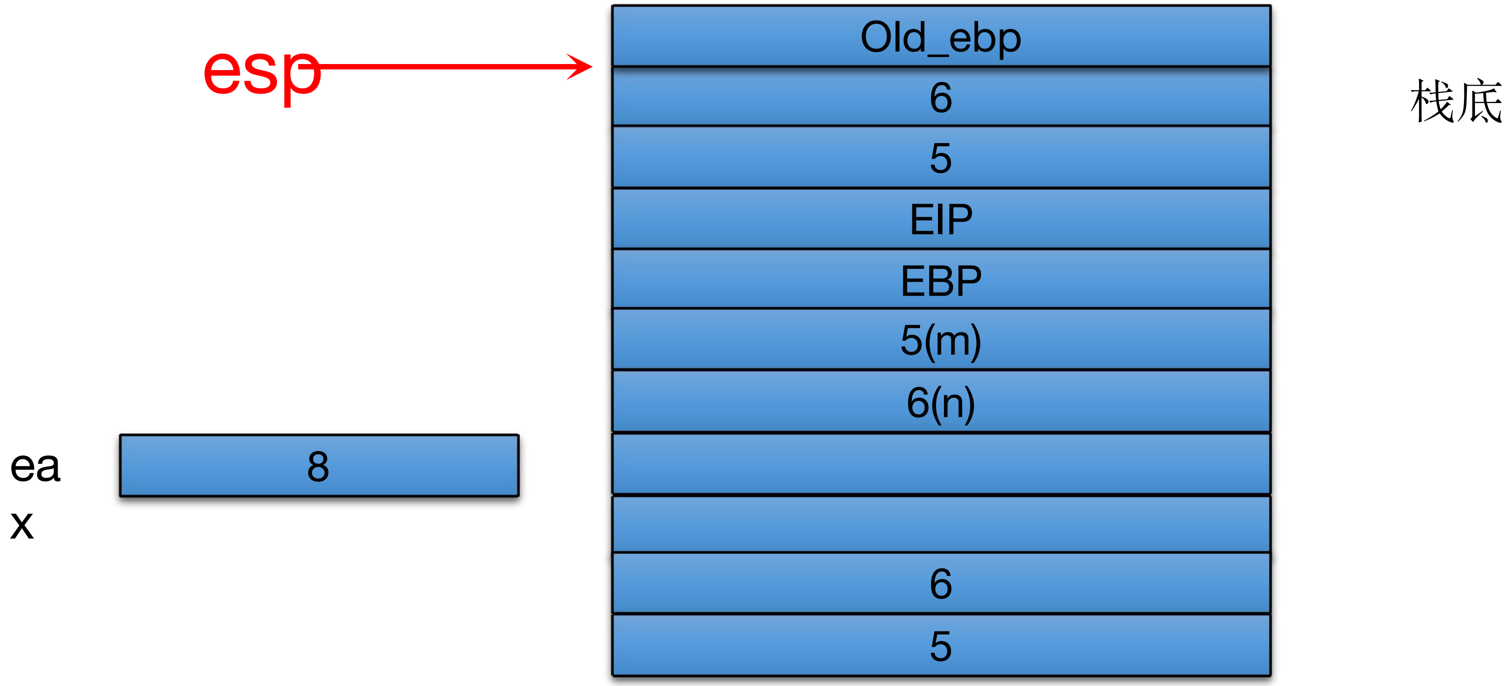
```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8

AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



```
AFunc(5,6);
push 6
push 5
call AFunc
add esp,8
```

```
AFunc
push ebp
mov ebp,esp
sub esp,0x10
mov DWORD PTR [ebp-0x4],0x3
mov DWORD PTR [ebp-0x8],0x4
mov eax, DWORD PTR [ebp+0x8]
mov DWORD PTR [ebp-0x4],eax
mov eax,DWORD PTR [ebp+0xc]
mov DWORD PTR [ebp-0x8],eax
push DWORD PTR [ebp-0x8]
push DWORD PTR [ebp-0x4]
call _BFunc
add esp,0x8
mov eax,0x8
leave
ret
```



esp

Old_ebp

6

5

EIP

EBP

5(m)

6(n)

6

5

栈底

eax

8