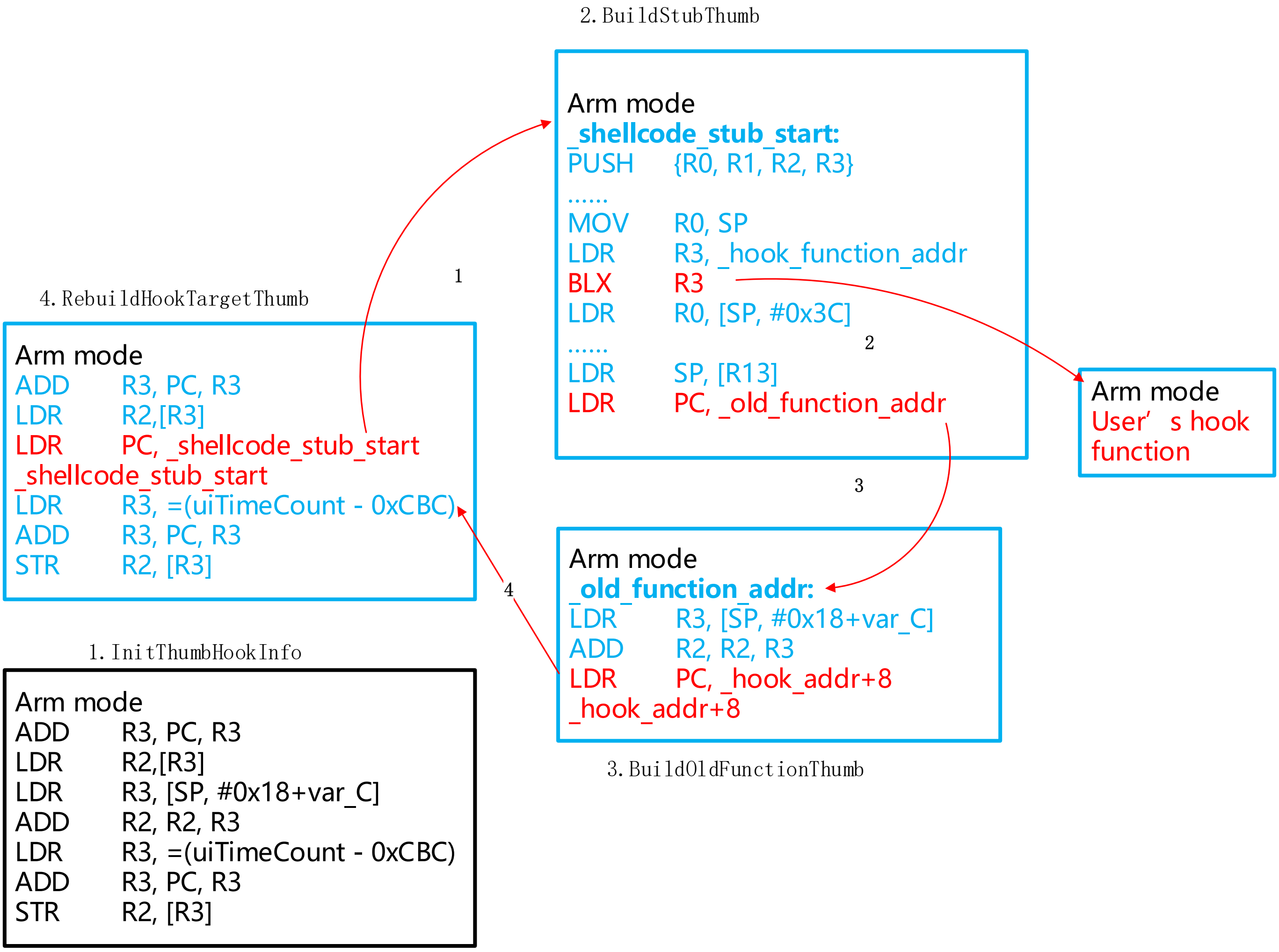

2. BuildStubThumb

```
Arm mode
_shellcode_stub_start:
PUSH     {R0, R1, R2, R3}
......
MOV      R0, SP
LDR      R3, _hook_function_addr
BLX      R3
LDR      R0, [SP, #0x3C]
......
LDR      SP, [R13]
LDR      PC, _old_function_addr
```

```
Arm mode
User’ s hook
function
```

4. RebuildHookTargetThumb

```
Arm mode
ADD      R3, PC, R3
LDR      R2,[R3]
LDR      PC, _shellcode_stub_start
_shellcode_stub_start
LDR      R3, =(uiTimeCount - 0xCBC)
ADD      R3, PC, R3
STR      R2, [R3]
```

```
Arm mode
_old_function_addr:
LDR      R3, [SP, #0x18+var_C]
ADD      R2, R2, R3
LDR      PC, _hook_addr+8
_hook_addr+8
```

3. BuildOldFunctionThumb

1. InitThumbHookInfo

```
Arm mode
ADD      R3, PC, R3
LDR      R2,[R3]
LDR      R3, [SP, #0x18+var_C]
ADD      R2, R2, R3
LDR      R3, =(uiTimeCount - 0xCBC)
ADD      R3, PC, R3
STR      R2, [R3]
```