

Writeup for Homework1

```
collision = controlCollision(pipeCol1, birdCol, birdRow, crackStart1,
                             crackFinish1);
```

Figure 1 - Instruction 0x5555555594c : Collision value from pipeCol1 in flappybird.cpp
Instruction 5555555594c stores the return value of controlCollision method. *regRCX = 0; *regRAX = 0; sets the value of return method to 0, which ensures isOver condition does not match DOUBLE value.

```
collision = controlCollision(pipeCol2, birdCol, birdRow, crackStart2,
                             crackFinish2);
```

Figure 2 - Instruction 0x55555555892 : Collision value from pipeCol2 in flappybird.cpp
To check if collision has occurred or not, ebp and eax registers are compared for 55555555892 instruction. Setting *regRCX = 0; for 55555555892 instruction ensures isOver=true statement is not reached.

```
if (collision) {
    if (collision == DOUBLE) {
        isOver = true;
    }
}
```

Figure 3 - Checking if collision has occurred with pipes

```
if (birdRow > row - 4 /*|| birdRow == 2*/) {
    // TOUCH THE GROUND
    isOver = true;
}
```

Figure 4 - Instruction 0x55555555903 - Checking if bird has touched the ground
Setting *regRAX = 0; *regRCX = 0; *regRDX = 0; for condition when flappybird touches the ground, ensures isOver condition is not true when the bird touches the ground. Instruction for this is 55555555903.

```
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat flappybird.S | grep "94c"
194c:    44 0f 4d f0          cmovge %eax,%r14d
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat flappybird.S | grep "892"
1892:    39 c5               cmp     %eax,%ebp
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat flappybird.S | grep "903"
1903:    39 c7               cmp     %eax,%edi
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$
```

Figure 5 - Instruction snippets from flappybird.S for instructions 5555555594c, 55555555892 and 55555555903

```
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat log.txt | grep "94c"
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:5555555594c] cmovnl r14d, eax
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:5555555594c] cmovnl r14d, eax
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat log.txt | grep "892"
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555892] cmp ebp, eax
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555892] cmp ebp, eax
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555892] cmp ebp, eax
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555892] cmp ebp, eax
ritu@ritu-Inspiron-15-5518:~/Downloads/pin/source/tools/SimpleExamples$ cat log.txt | grep "903"
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555903] cmp edi, eax
[/home/ritu/Downloads/pin/source/tools/SimpleExamples/flappybird:55555555903] cmp edi, eax
```

Figure 6 - Log file snippet for instructions 5555555594c, 55555555892 and 55555555903

Here is a recording of isOver=false for all three gameover conditions:

https://drive.google.com/file/d/1grwjtJ30t_H77INhmvKufJtpT5212YDE/view?usp=sharing