Hgame2023week3-gydybnc

kmusic

dnspy

在smc后面下断点把data保存出来再放回去

kmusic里关键代码，一眼z3

```
from z3 import *

num=[]
for i in range(13):
    temp=BitVecs(f'num[{i}]',50)
    num=num+temp

print(num)
s = Solver()
s.add(num[0] + 52296 + num[1] - 26211 + num[2] - 11754 + (num[3] ^ 41236) + num[4] *
63747 + num[5] - 52714 + num[6] - 10512 + num[7] * 12972 + num[8] + 45505 + num[9] -
21713 + num[10] - 59122 + num[11] - 12840 + (num[12] ^ 21087) == 12702282 )
s.add( num[0] - 25228 + (num[1] ^ 20699) + (num[2] ^ 8158) + num[3] - 65307 + num[4] *
30701 + num[5] * 47555 + num[6] - 2557 + (num[7] ^ 49055) + num[8] - 7992 + (num[9] ^
57465) + (num[10] ^ 57426) + num[11] + 13299 + num[12] - 50966 == 9946829 )
s.add( num[0] - 64801 + num[1] - 60698 + num[2] - 40853 + num[3] - 54907 + num[4] +
29882 + (num[5] ^ 13574) + (num[6] ^ 21310) + num[7] + 47366 + num[8] + 41784 + (num[9]
^ 53690) + num[10] * 58436 + num[11] * 15590 + num[12] + 58225 == 2372055 )
s.add( num[0] + 61538 + num[1] - 17121 + num[2] - 58124 + num[3] + 8186 + num[4] +
21253 + num[5] - 38524 + num[6] - 48323 + num[7] - 20556 + num[8] * 56056 + num[9] +
18568 + num[10] + 12995 + (num[11] ^ 39260) + num[12] + 25329 == 6732474 )
s.add( num[0] - 42567 + num[1] - 17743 + num[2] * 47827 + num[3] - 10246 + (num[4] ^
16284) + num[5] + 39390 + num[6] * 11803 + num[7] * 60332 + (num[8] ^ 18491) + (num[9]
^ 4795) + num[10] - 25636 + num[11] - 16780 + num[12] - 62345 == 14020739 )
s.add( num[0] - 10968 + num[1] - 31780 + (num[2] ^ 31857) + num[3] - 61983 + num[4] *
31048 + num[5] * 20189 + num[6] + 12337 + num[7] * 25945 + (num[8] ^ 7064) + num[9] -
25369 + num[10] - 54893 + num[11] * 59949 + (num[12] ^ 12441) == 14434062 )
s.add( num[0] + 16689 + num[1] - 10279 + num[2] - 32918 + num[3] - 57155 + num[4] *
26571 + num[5] * 15086 + (num[6] ^ 22986) + (num[7] ^ 23349) + (num[8] ^ 16381) +
(num[9] ^ 23173) + num[10] - 40224 + num[11] + 31751 + num[12] * 8421 == 7433598 )
s.add( num[0] + 28740 + num[1] - 64696 + num[2] + 60470 + num[3] - 14752 + (num[4] ^
1287) + (num[5] ^ 35272) + num[6] + 49467 + num[7] - 33788 + num[8] + 20606 + (num[9] ^
44874) + num[10] * 19764 + num[11] + 48342 + num[12] * 56511 == 7989404 )
s.add( (num[0] ^ 28978) + num[1] + 23120 + num[2] + 22802 + num[3] * 31533 + (num[4] ^
39287) + num[5] - 48576 + (num[6] ^ 28542) + num[7] - 43265 + num[8] + 22365 + num[9] +
61108 + num[10] * 2823 + num[11] - 30343 + num[12] + 14780 == 3504803 )
s.add( num[0] * 22466 + (num[1] ^ 55999) + num[2] - 53658 + (num[3] ^ 47160) + (num[4]
^ 12511) + num[5] * 59807 + num[6] + 46242 + num[7] + 3052 + (num[8] ^ 25279) + num[9]
```

```
+ 30202 + num[10] * 22698 + num[11] + 33480 + (num[12] ^ 16757) == 11003580 )
s.add( num[0] * 57492 + (num[1] ^ 13421) + num[2] - 13941 + (num[3] ^ 48092) + num[4] *
38310 + num[5] + 9884 + num[6] - 45500 + num[7] - 19233 + num[8] + 58274 + num[9] +
36175 + (num[10] ^ 18568) + num[11] * 49694 + (num[12] ^ 9473) == 25546210 )
s.add( num[0] - 23355 + num[1] * 50164 + (num[2] ^ 34618) + num[3] + 52703 + num[4] +
36245 + num[5] * 46648 + (num[6] ^ 4858) + (num[7] ^ 41846) + num[8] * 27122 + (num[9]
^ 42058) + num[10] * 15676 + num[11] - 31863 + num[12] + 62510 == 11333836 )
s.add( num[0] * 30523 + (num[1] ^ 7990) + num[2] + 39058 + num[3] * 57549 + (num[4] ^
53440) + num[5] * 4275 + num[6] - 48863 + (num[7] ^ 55436) + (num[8] ^ 2624) + (num[9]
^ 13652) + num[10] + 62231 + num[11] + 19456 + num[12] - 13195 == 13863722)
s.add(num[0] == 236,num[1]==72,num[2]==213,num[3]==106,num[4]==189,num[5]==86)

if s.check()==sat:
    d = s.model()
    print(d)
    flag = [int(str(d[num[i]])) for i in range(13)]
    print(flag)
#####################################################
num=[0]*13
array = [132,47,180,7,216,45,68,6,39,
246,124,2,243,137,58,172,53,200,99,91,83,13,171,80,108,235,179, 58, 176,28, 216,
36,11,80, 39,162,97,58,236,130,123,176,24,212,56,89,72]
num[1] = 72
num[7] = 53
num[11] = 93
num[5] = 86
num[10] = 15
num[9] = 199
num[12] = 133
num[4] = 189
num[0] = 236
num[6] = 7199182931829522494
#num[3] = 4611686018427388010
num[3]=106
num[8] = 120
#num[2] = 17267276898211922133
num[2]=213
print(num)
for i in range(len(array)):
    temp=array[i]^num[i%len(num)]
    if temp>=28 and temp <=128:

        print(chr(temp),end='')
    else :
        print('')
#hgame{z3_1s_very_u5eful_1n_rever5e_engin3ering}
```

z3解出来中间有一个乱码，最后flag猜了一下

patchme

attach上去之后跟着跑

再检查有没有成功patch的地方改下两个标志位之后运行即可