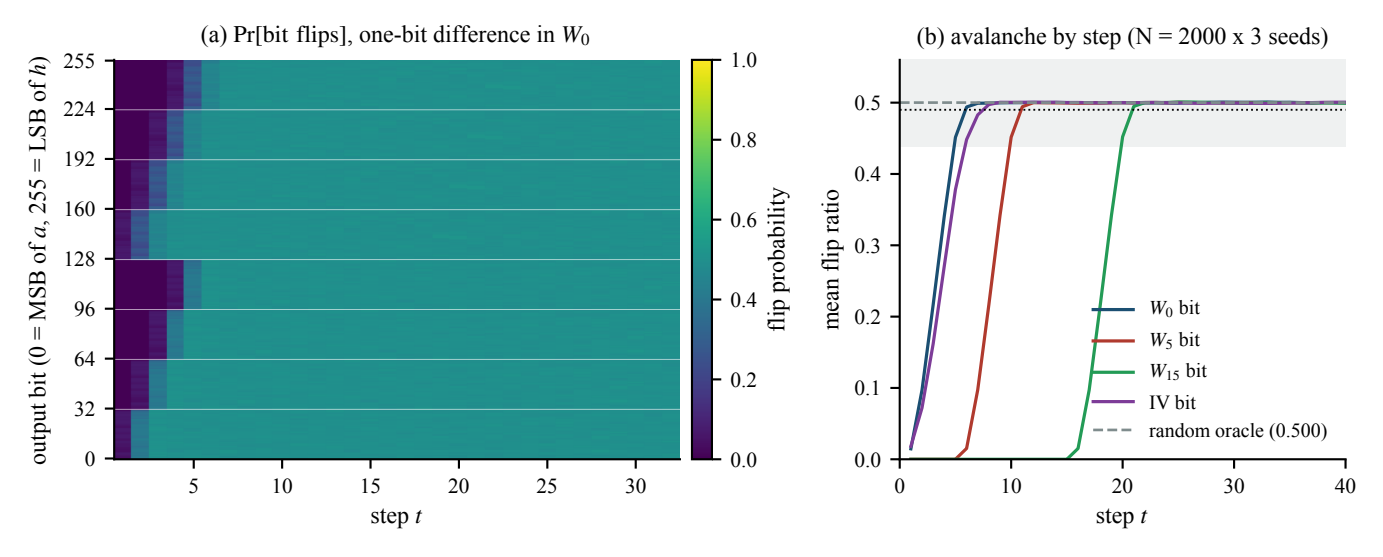

(a) Pr[bit flips], one-bit difference in W_0
output bit (0 = MSB of a, 255 = LSB of h)
255
224
192
160
128
96
64
32
0
5
10
15
20
25
30
step t
flip probability
1.0
0.8
0.6
0.4
0.2
0.0
(b) avalanche by step (N = 2000 x 3 seeds)
mean flip ratio
0.5
0.4
0.3
0.2
0.1
0.0
0
10
20
30
40
step t
W_0 bit
W_5 bit
W_{15} bit
IV bit
random oracle (0.500)