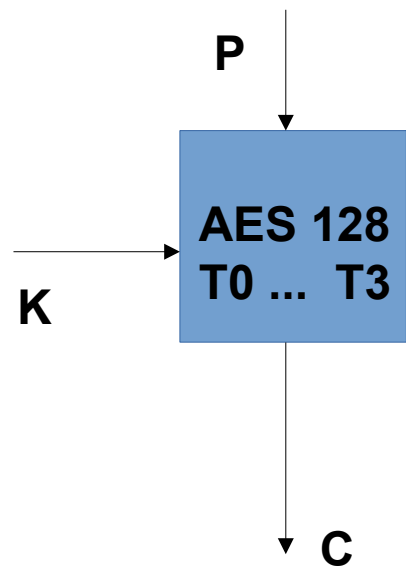
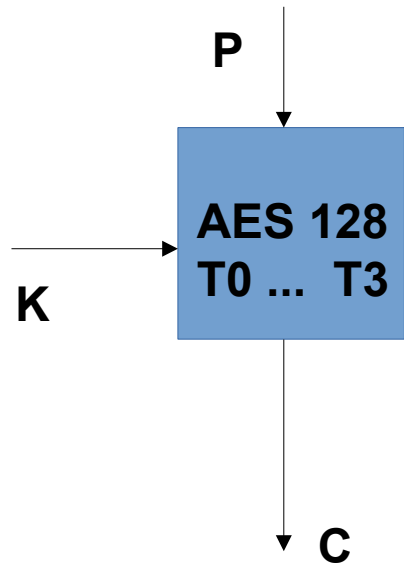


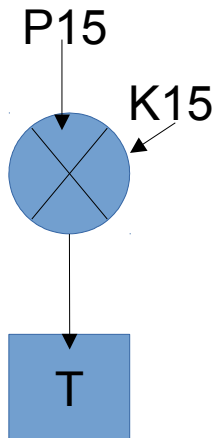
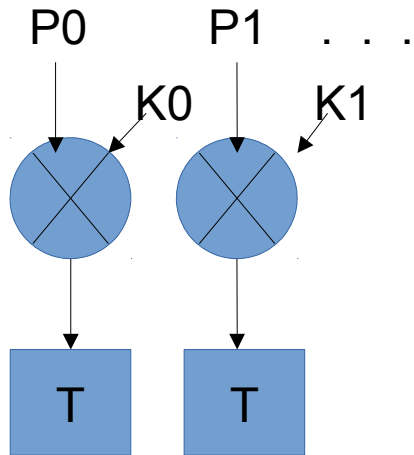
MICRO ARCHITECTURAL ATTACKS : LAB2



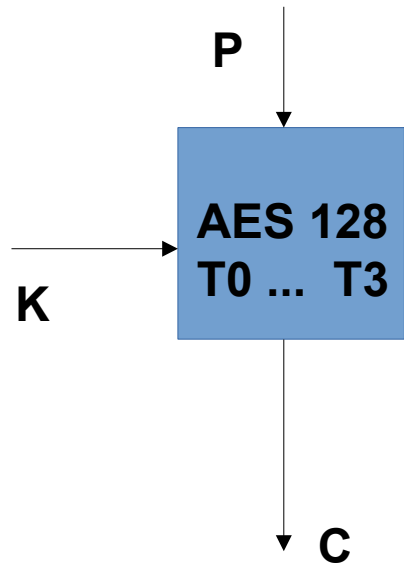




$T0 [P0 \text{ xor } K0] \quad T0[P4 \text{ xor } K4]$
 $T1 [P1 \text{ xor } K1] \quad T1[P5 \text{ xor } K5]$
 $T2 [P2 \text{ xor } K2]$
 $T3 [P3 \text{ xor } K3]$



5 T tables in this implementation
 256 elements/1024 bytes

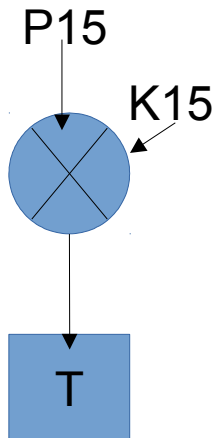
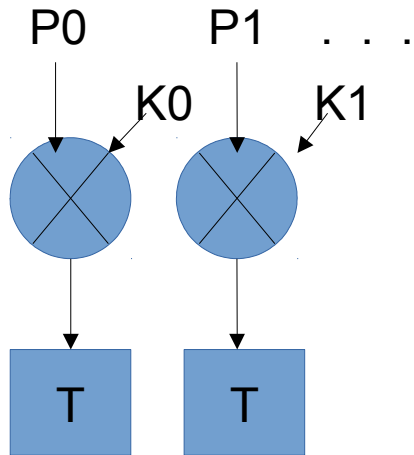


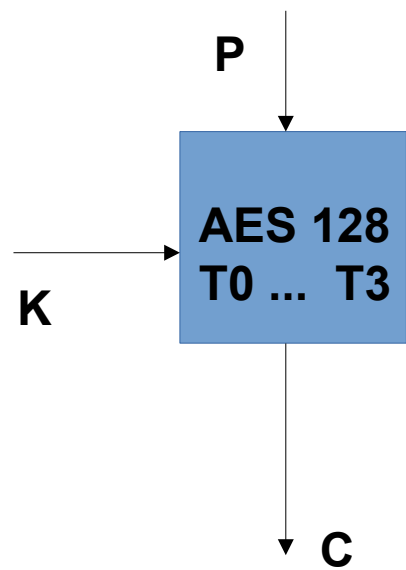
$T0 [P0 \text{ xor } K0] \quad T0[P4 \text{ xor } K4]$

$T1 [P1 \text{ xor } K1] \quad T1[P5 \text{ xor } K5]$

$T2 [P2 \text{ xor } K2]$

$T3 [P3 \text{ xor } K3]$



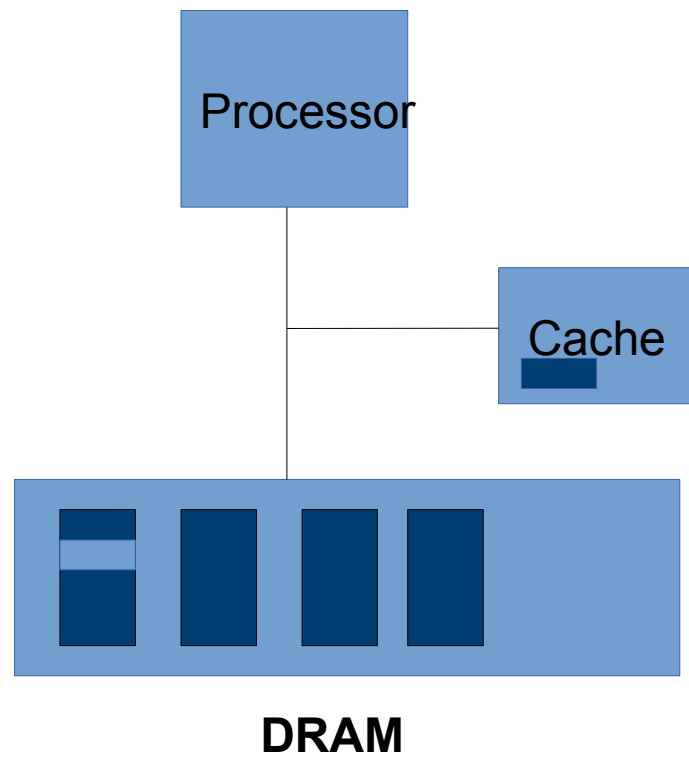
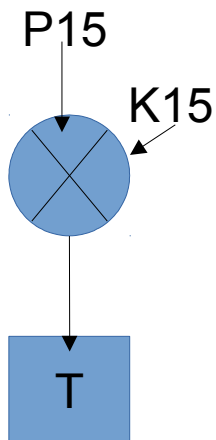
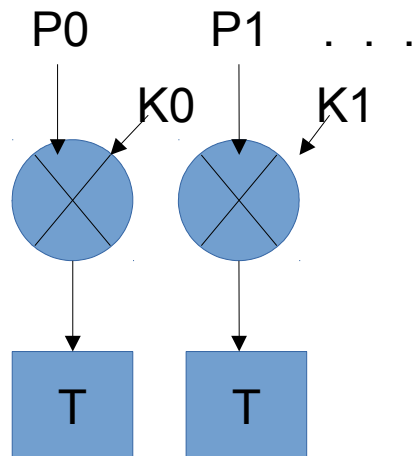


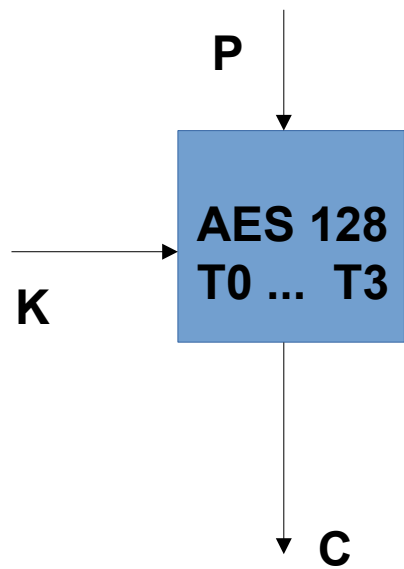
$T0 [P0 \text{ xor } K0] \quad T0[P4 \text{ xor } K4]$

$T1 [P1 \text{ xor } K1] \quad T1[P5 \text{ xor } K5]$

$T2 [P2 \text{ xor } K2]$

$T3 [P3 \text{ xor } K3]$



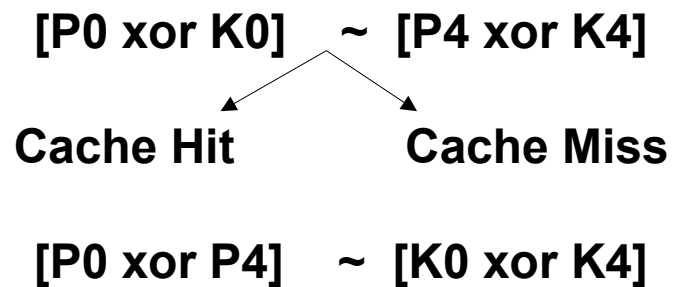
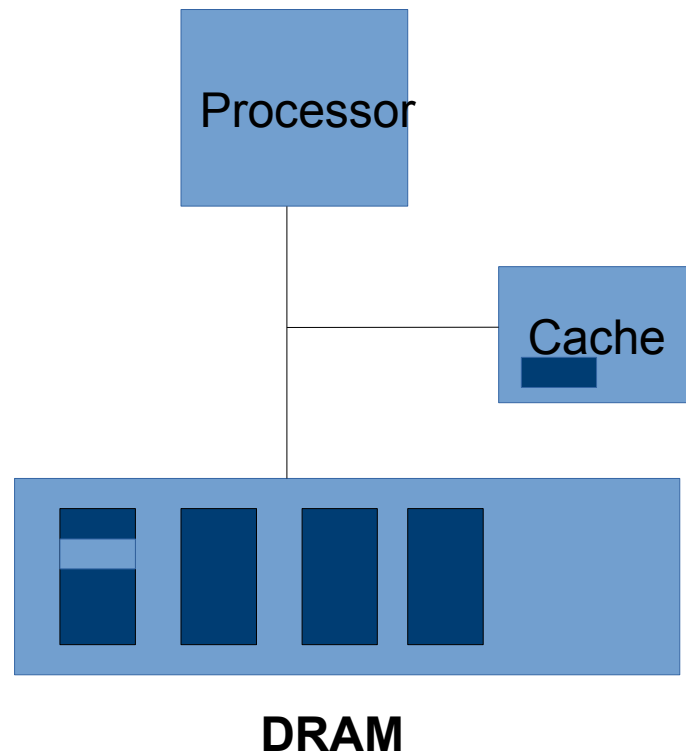
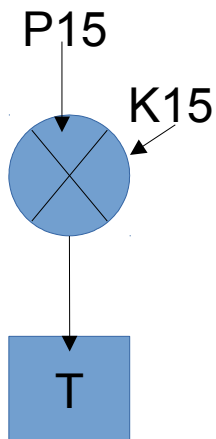
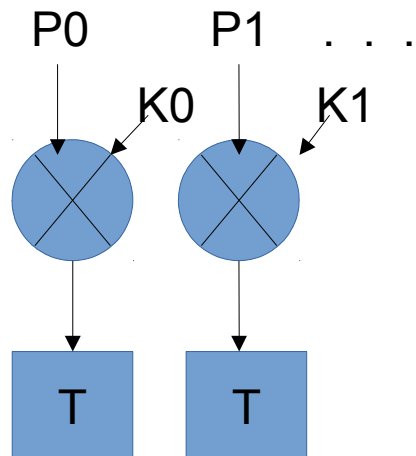


T0 [P0 xor Ko] T0[P4 xor K4]

T1 [P1 xor K1] T1[P5 xor K5]

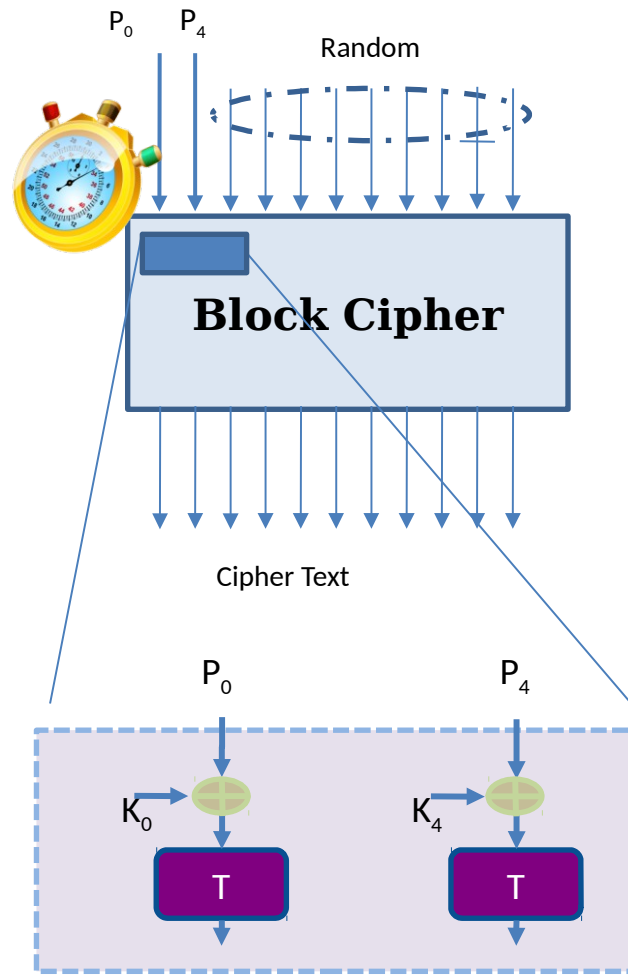
T2 [P2 xor K2]

T3 [P3 xor K3]



Suppose
($K_0 = 00$ and $k_4 = 50$)

- $P_0 = 0$, all other inputs are random
- Make N time measurements
- Segregate into Y buckets based on value of P_4
- Find average time of each bucket
- Find deviation of each average from overall average (DOM)



$$\langle K_0 \oplus K_4 \rangle = \langle P_0 \oplus P_4 \rangle$$

P4	Average Time	DOM
00	2945.3	1.8
10	2944.4	0.9
20	2943.7	0.2
30	2943.7	0.2
40	2944.8	1.3
50	2937.4	-6.3
60	2943.3	-0.2
70	2945.8	2.3
:	:	:
F0	2941.8	-1.7

Average : 2943.57
Maximum : -6.3

Task 1 : Run the code for 10 consecutive time and calculate the reduction in entropy. Why does the entropy increase or decrease?

Task 2 : Run the attack on all three VMs and check the entropy.