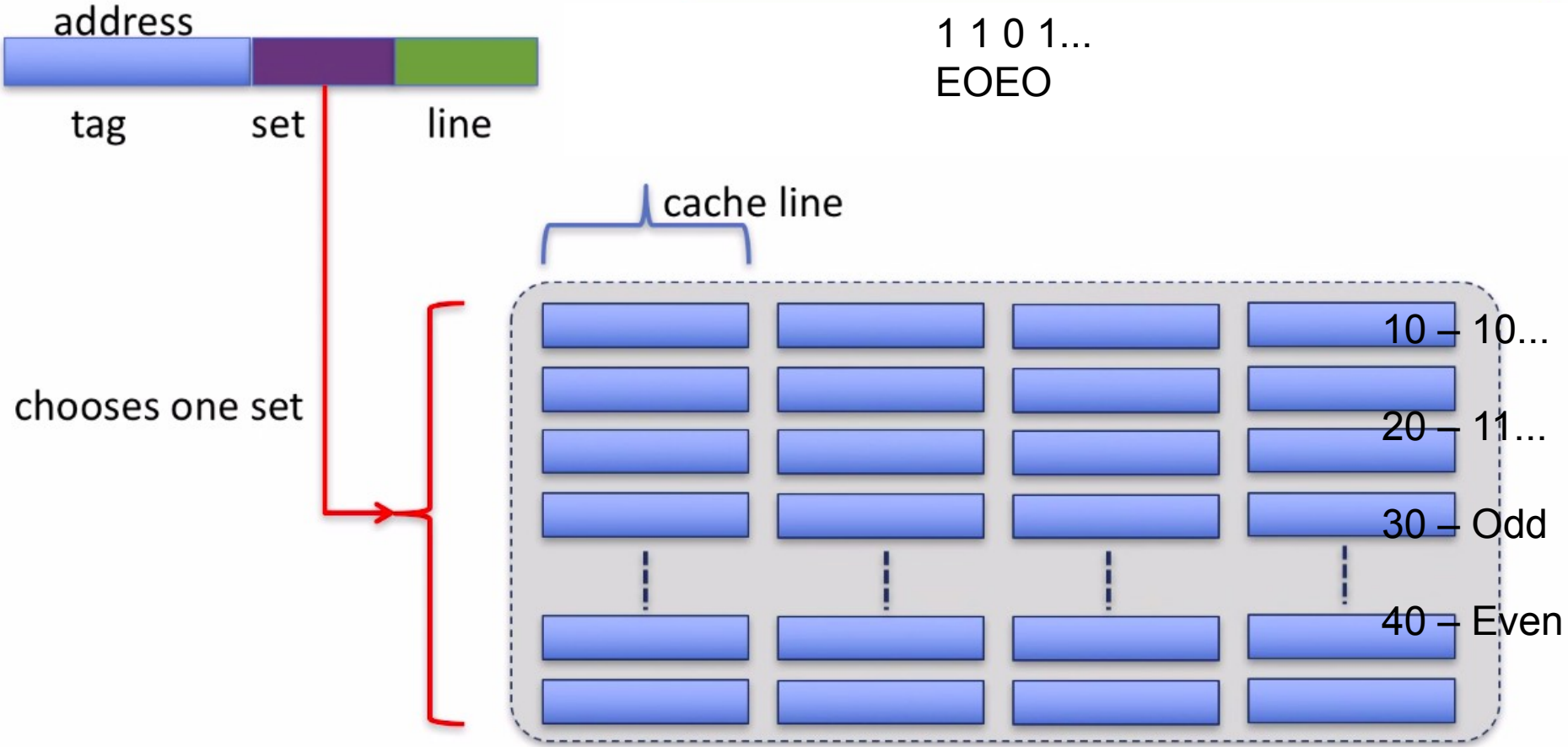
MICRO ARCHITECTURAL ATTACKS

CACHE COVERT CHANNEL : LAB1


address
tag
set
line
cache line
chooses one set
10 – 10...
20 – 11...
30 – Odd
40 – Even

1 1 0 1...
EOEO

Task 0 : Whats the Bit Logic, A>B or B>A?? is 1

Task 1 : Determine the Comn Rate(Bits/Sec) and BER (Error/1000 Bits)

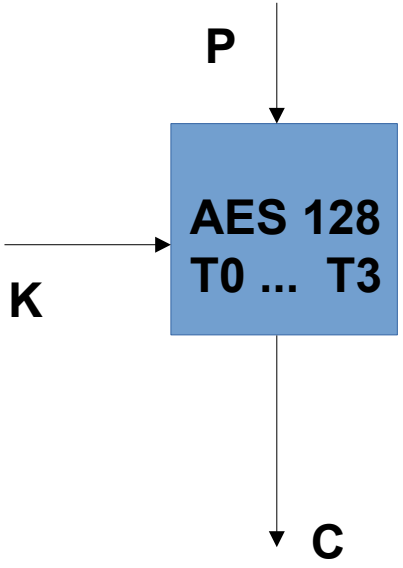
Task 2: Double the Comn Rate and find BER

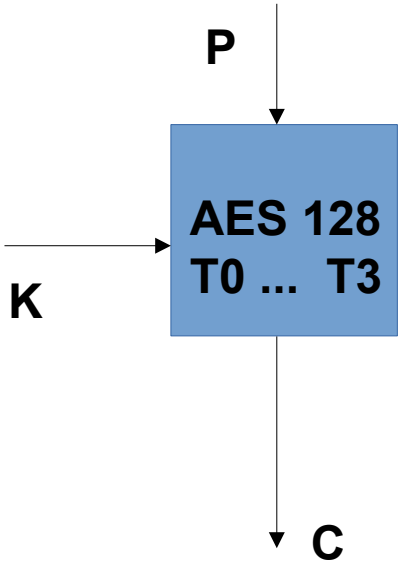
Check system cache from following:-

- lscpu
- /sys/devices...

To run the code
taskset -c 4 ./receiver <4 distinct set numbers>

CACHE TIMING ATTACK : LAB2


P
AES 128
T0 ... T3
K
C

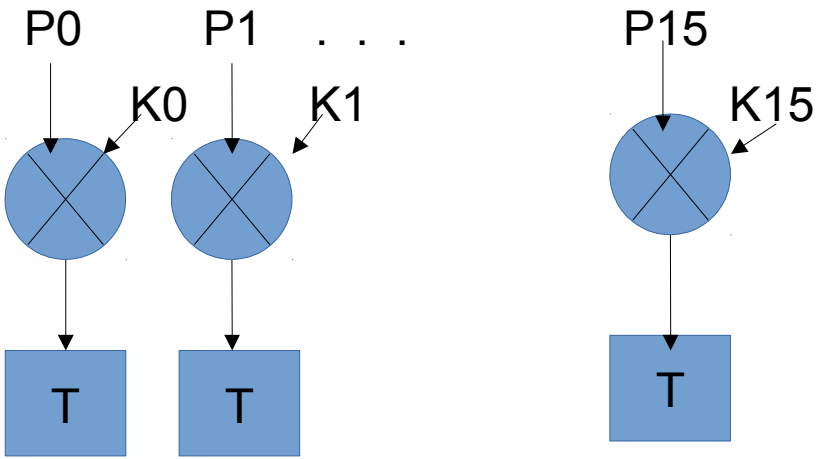


T0 [P0 xor Ko] **T0[P4 xor K4]**

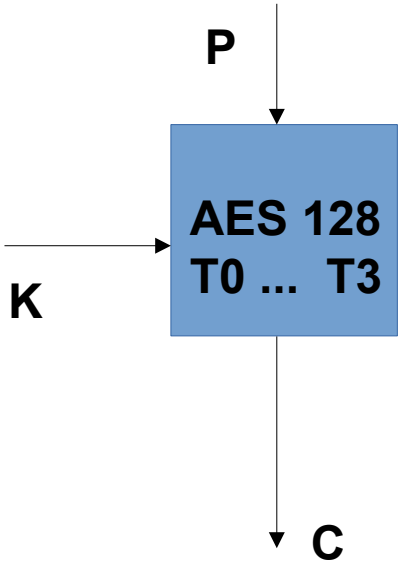
T1 [P1 xor K1] **T1[P5 xor K5]**

T2 [P2 xor K2]

T3 [P3 xor K3]



5 T tables in this implementation
256 elements/1024 bytes

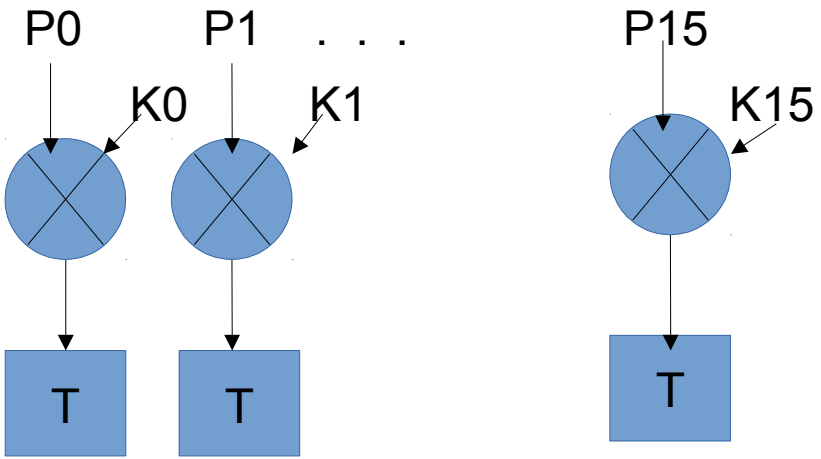


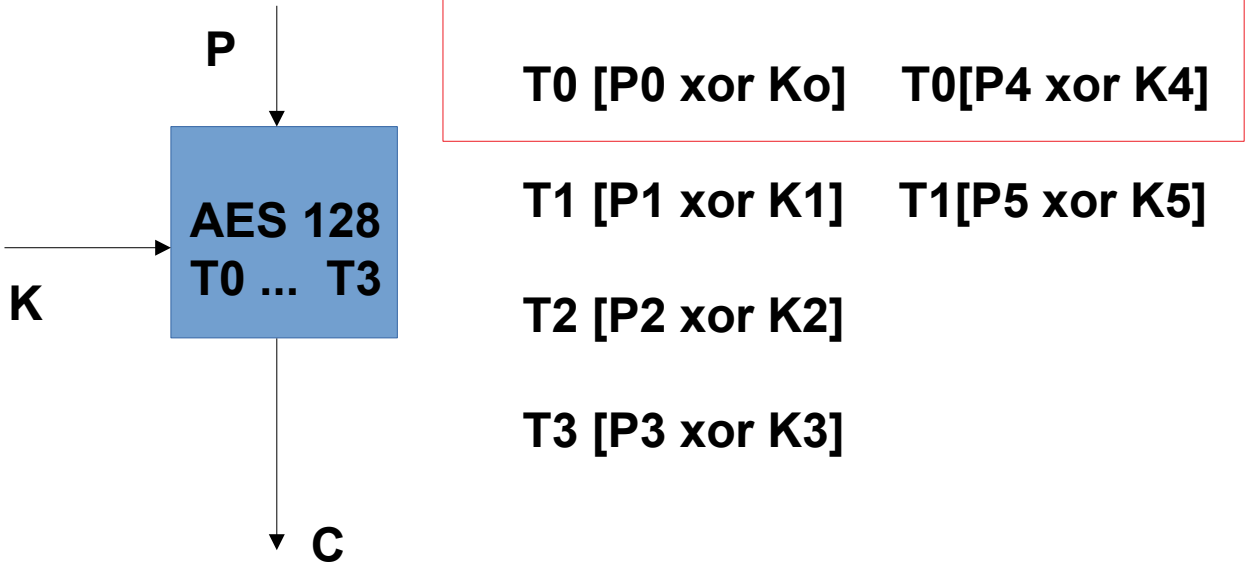
T0 [P0 xor Ko] T0[P4 xor K4]

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

T2 [P2 xor K2]

T3 [P3 xor K3]



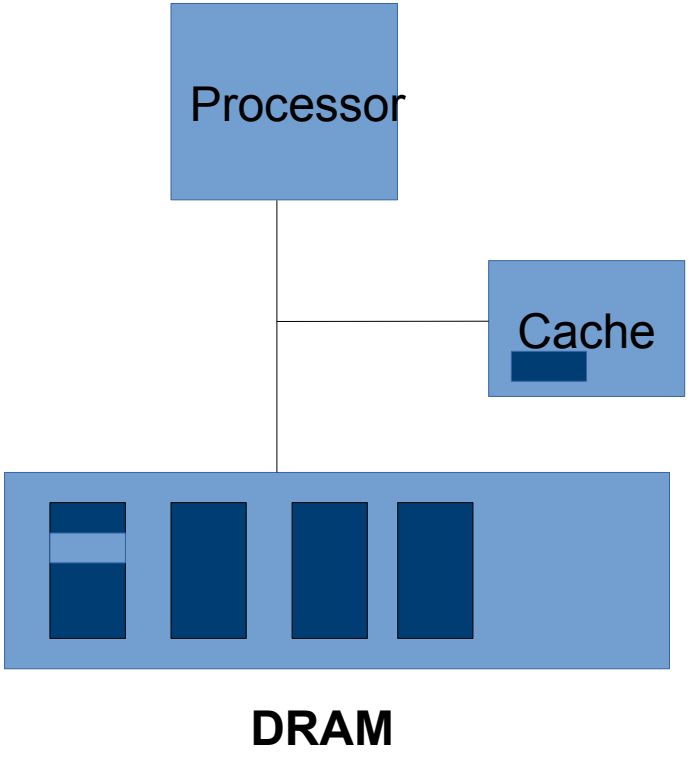


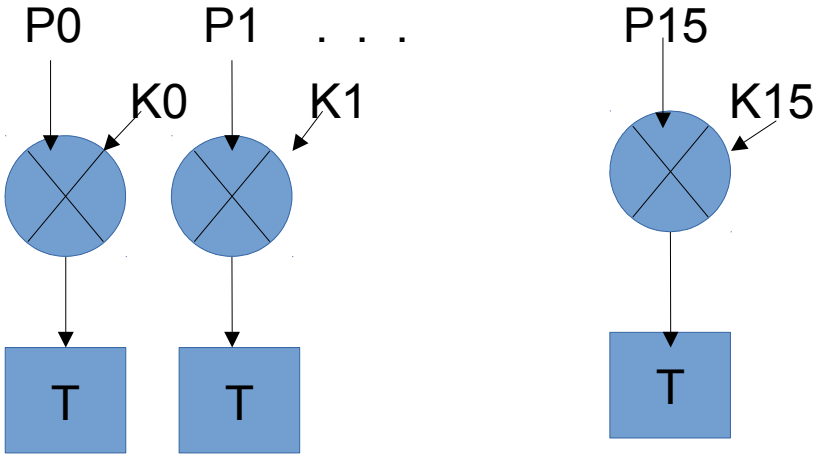
T0 [P0 xor Ko] T0[P4 xor K4]

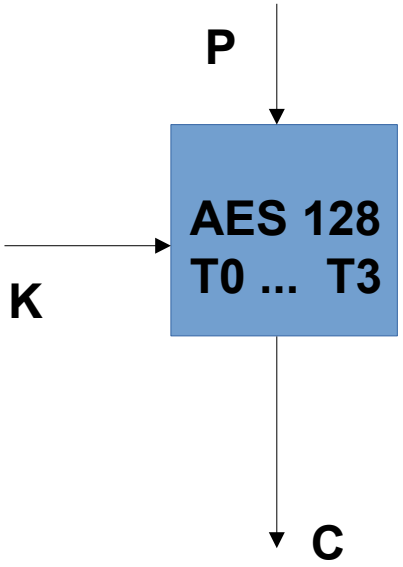
T1 [P1 xor K1] T1[P5 xor K5]

T2 [P2 xor K2]

T3 [P3 xor K3]





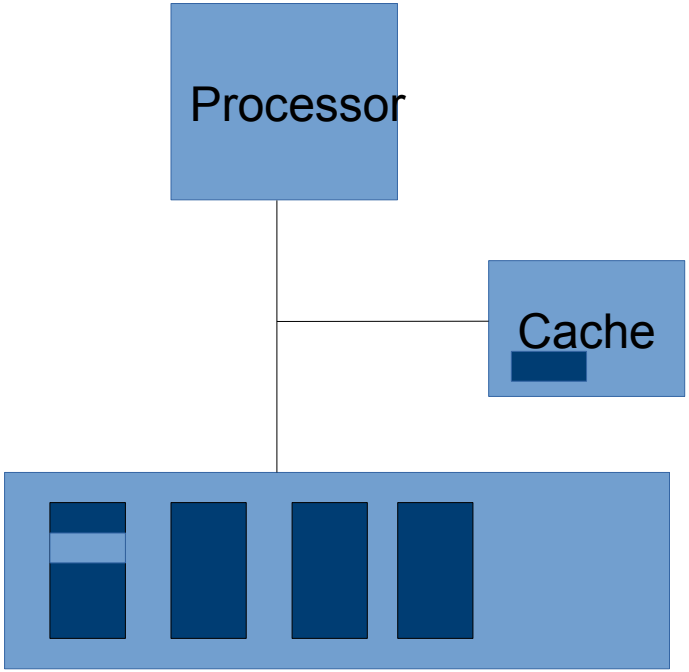


T0 [P0 xor Ko] T0[P4 xor K4]

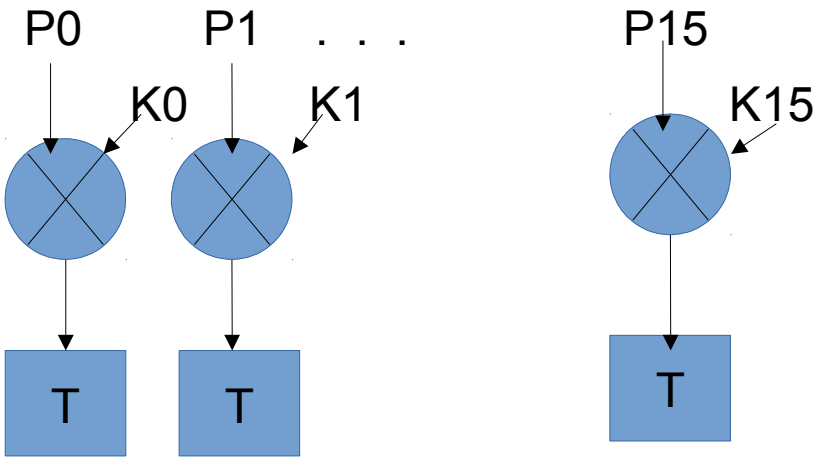
T1 [P1 xor K1] T1[P5 xor K5]

T2 [P2 xor K2]

T3 [P3 xor K3]



DRAM



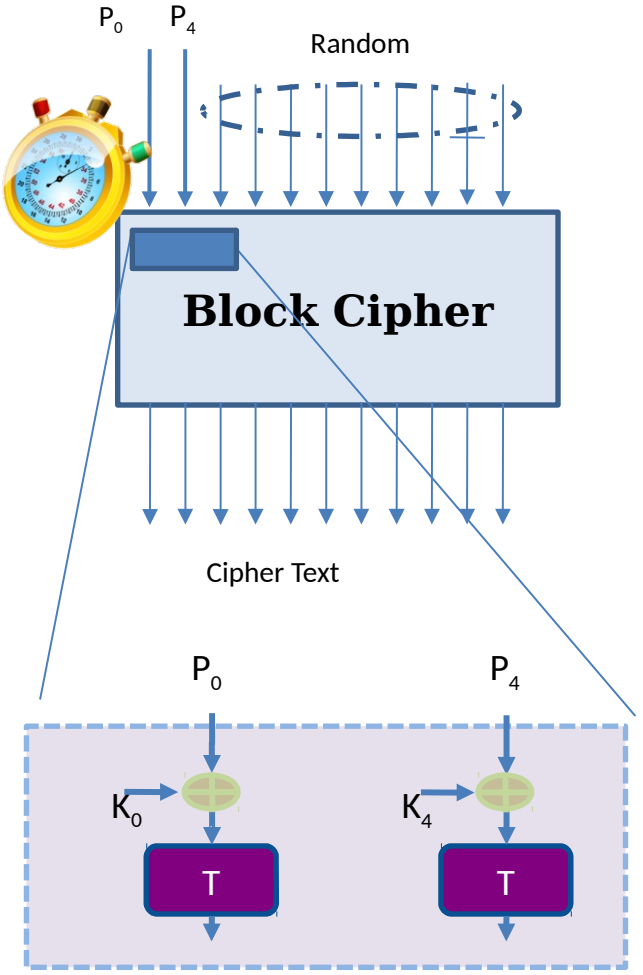
[P0 xor K0] ~ [P4 xor K4]

Cache Hit **Cache Miss**

[P0 xor P4] ~ [K0 xor K4]

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 consequtive time and calculate the reduction in entropy. Why does the entropy increase or decrease?

Task 2 : Run the attack on different types of Ubuntu VMs and check the entropy.