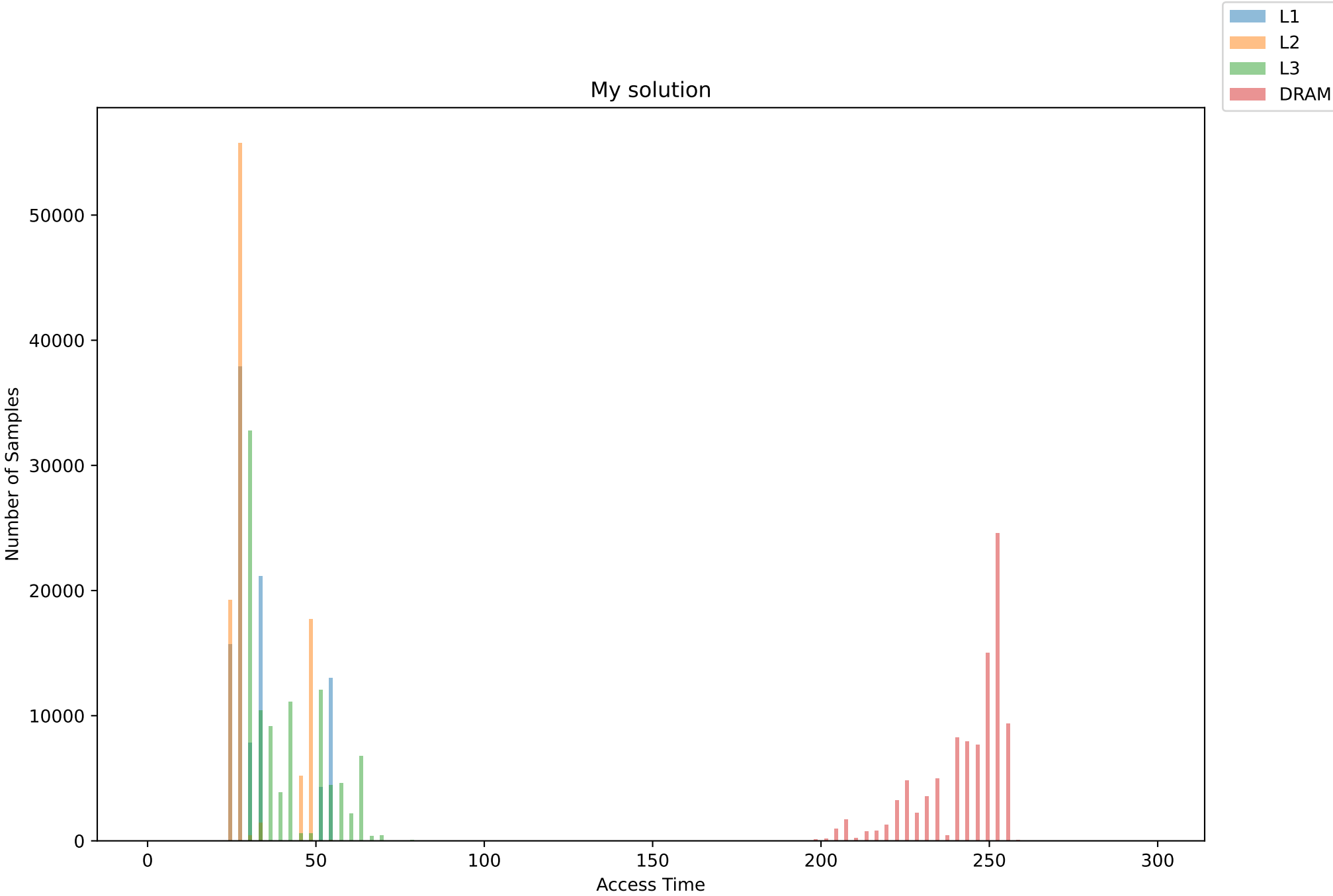
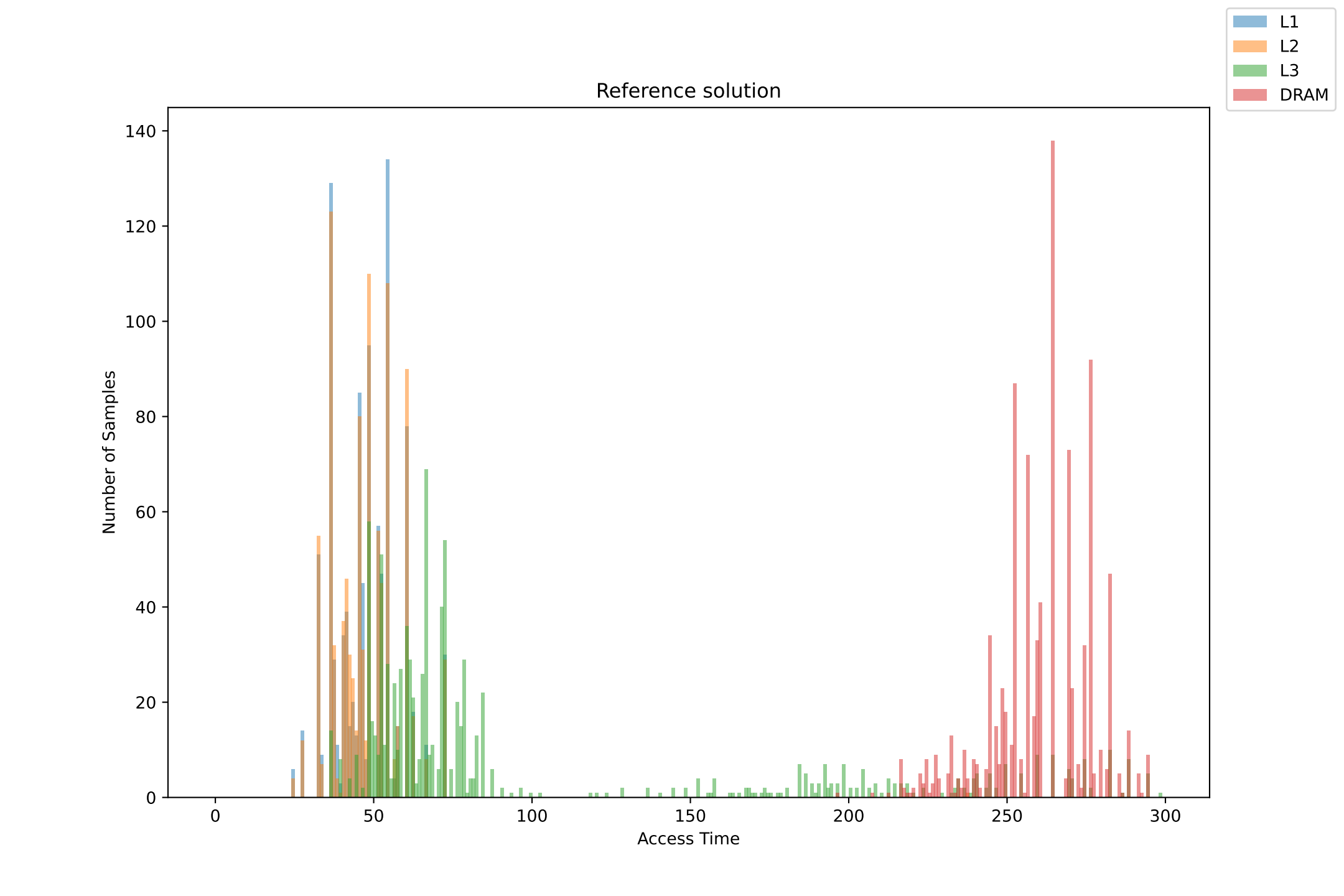

My solution
L1
L2
L3
DRAM
Number of Samples
0
10000
20000
30000
40000
50000
0
50
100
150
200
250
300
Access Time


Reference solution
L1
L2
L3
DRAM
Number of Samples
Access Time
0
20
40
60
80
100
120
140
0
50
100
150
200
250
300

CSE 291F Lab 1

Fall 2022

Discussion Question 6

Describe your communication protocol. Please refer to Section 2.2 for the components involved in a protocol.

Communication protocol:

We use huge pages of 2 MB to ensure that we have full control over cache index bits and some cache tag bits.

Given that the L2 cache has 512 Sets, we can use different sets to encode different numbers. The L2 cache byte offset is bit 5-0, and the L2 cache index bit is 14-6. We use bits 13 - 6 (8 bits) in the L2 cache index bit to encode the transmitted 8-bit number.

(1) Encode: what is the sender's action for sending 8-bit number;

The sender reads the user's input number **n**, and then repeatedly reads cache lines with different tags with cache index **n**. This will evict all lines in the **n**th L2 cache set. The sender takes 5000 cycles to perform a full cache set eviction.

(2) Receive: what is the timing measurement strategy used by the receiver, such as the number of addresses to access;

The receiver uses Prime and probe. It performs Prime and probe for each cache set (cache index is 0-255), it first reads the cache lines of 8 different tags in the same cache set (bit 20-15 are numbers 0-7), and then waits for the sender does a possible evict (waiting 15000 cycles to make sure the sender's eviction happens) and then checks by access latency if these 8 cache lines are still in L2.

(3) Decode: what is the threshold to be used to distinguish among all 8-bit numbers.

In order to reduce the impact of noise as much as possible, we record the average access latency of the **last ten times** for each cache set. If the probe access latency of a cache set **n** is greater than 400 cycles, it is determined that the sender sends the number **n**.

To further reduce noise, we adjust the receiver's waiting time and sender's sending time so that the receiver can receive 150 signals for each number sent by the sender. We make the receiver record the most recent 256 signals received. If a signal appears more than 120 times, it is considered that the number **n** sent by the sender is received, and then the number **n** is printed out.

By using the above Communication protocol, we can achieve a very stable cache covert channel with relatively good bandwidth.