Golmaal: Thanks to the Secure TimeCache for a Faster DRAM Covert Channel

DRAMSEC 22

Ajaykumar kushwaha, Ajay jain, Mahendra patel and Biswabandan Panda

Dept. of Computer Science and Engineering, Indian Institute of Technology Bombay

I can perform Flush+Reload attack.

You mean, you want to send first accesses of the reloaded cache lines to DRAM.

Won’t that increase bandwidth of Covert channel in DRAM ? 😜

I will Implement TimeCache to mitigate it.

Yes !!! Big Brains 😉

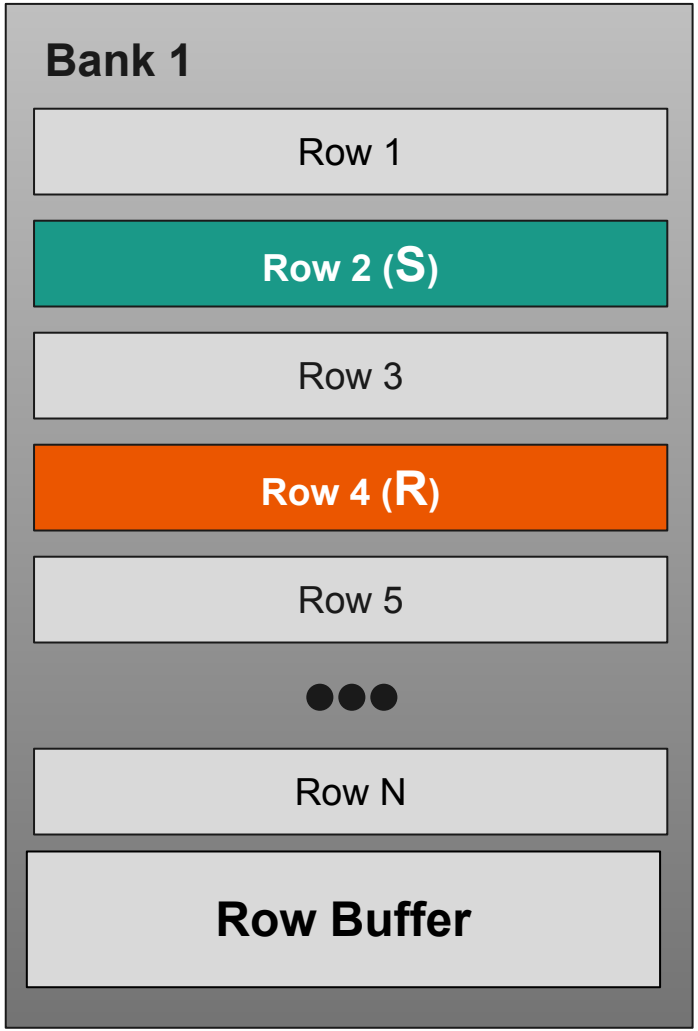
Background

- DRAM Covert channel
- TimeCache

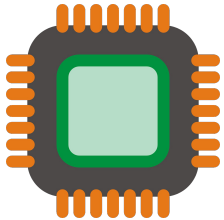
DRAM Row-Buffer conflict covert channel*

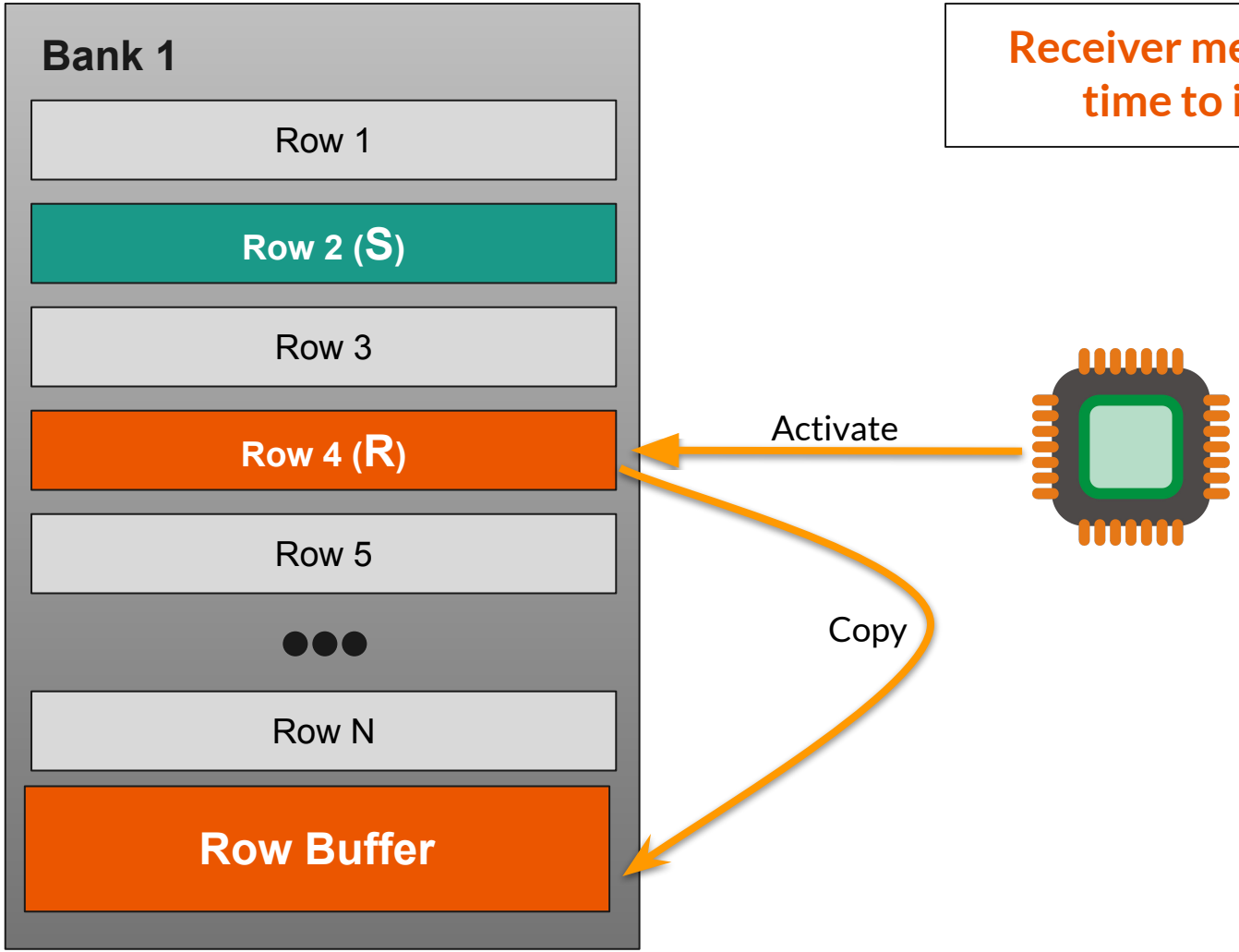
- Sender and receiver agree on a bank (can be hardcoded)
- Both sender and receiver on host select a **different row inside this bank**
- Receiver measures **access time** for it's selected row
- Sender can transmit 0 by doing **nothing** and 1 by causing **row buffer conflict** by accessing it's own row.
- If measured timing was "**fast**" by the receiver then sender transmitted 0 otherwise 1.

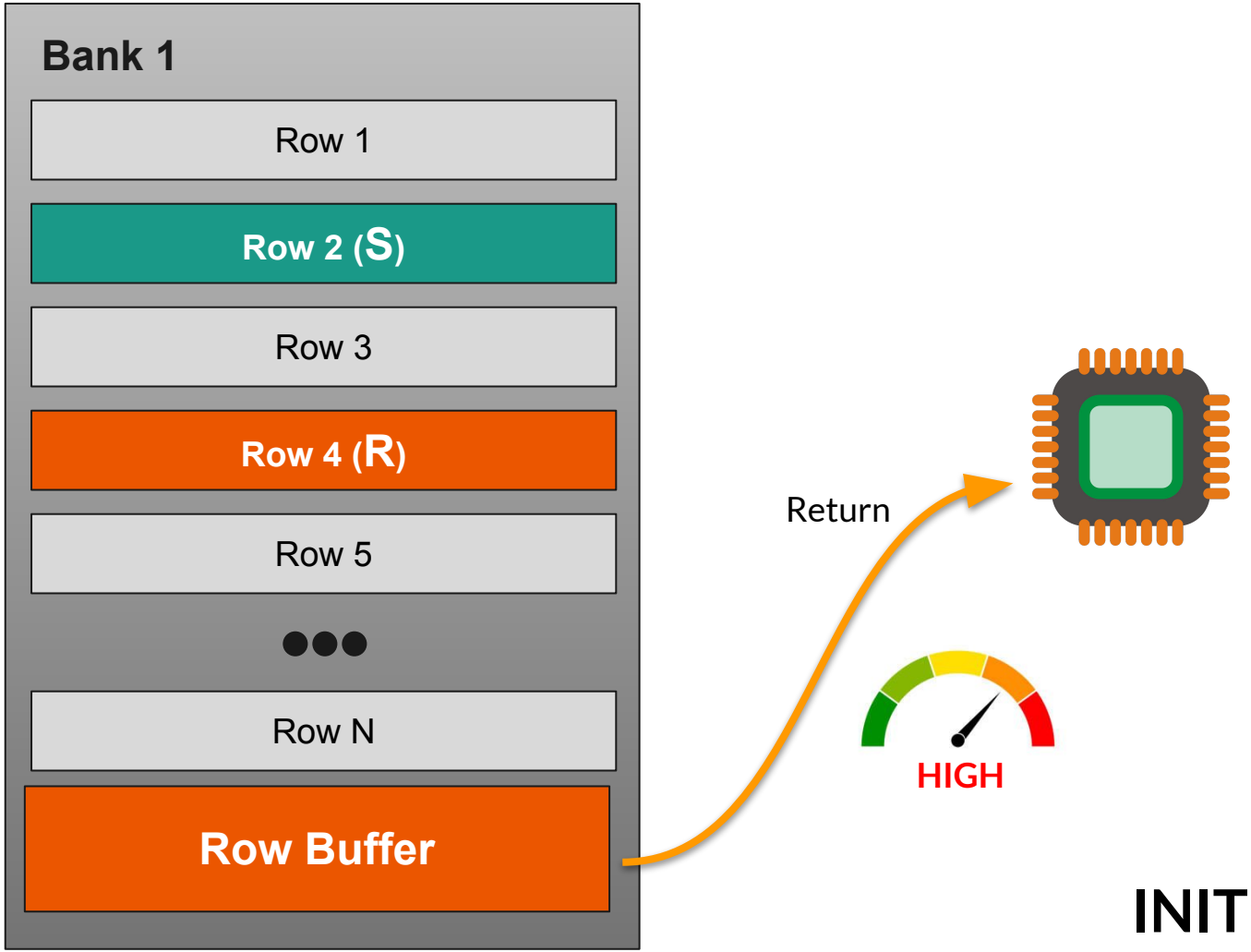
**Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard. 2016. DRAMA: exploiting dram addressing for cross-cpu attacks. In Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16). USENIX Association, USA, 565–581.



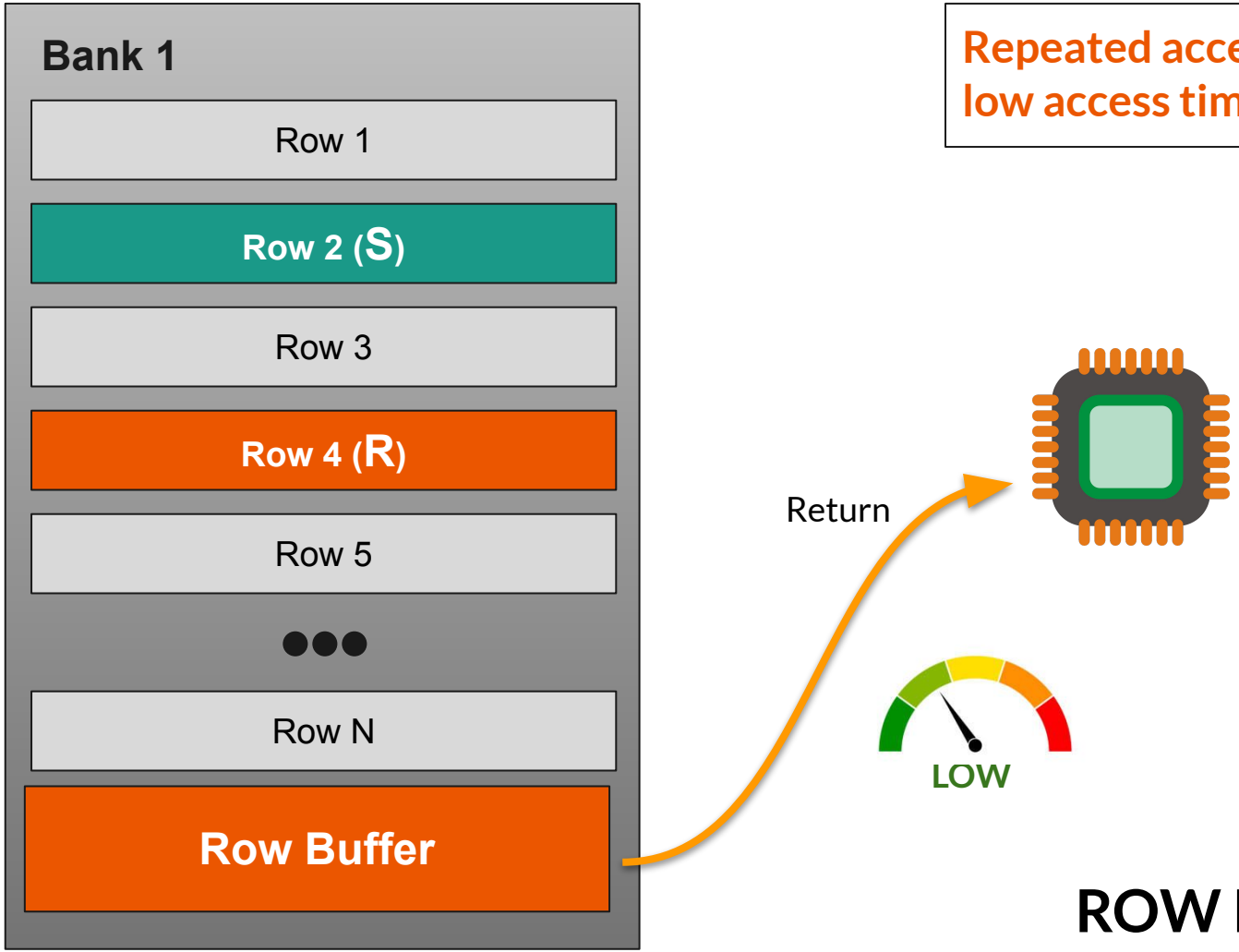
Sender and Receiver decide on One Bank




Bank 1
Row 1
Row 2 (S)
Row 3
Row 4 (R)
Row 5
Row N
Row Buffer
Activate
Copy
Receiver measures access time to its address

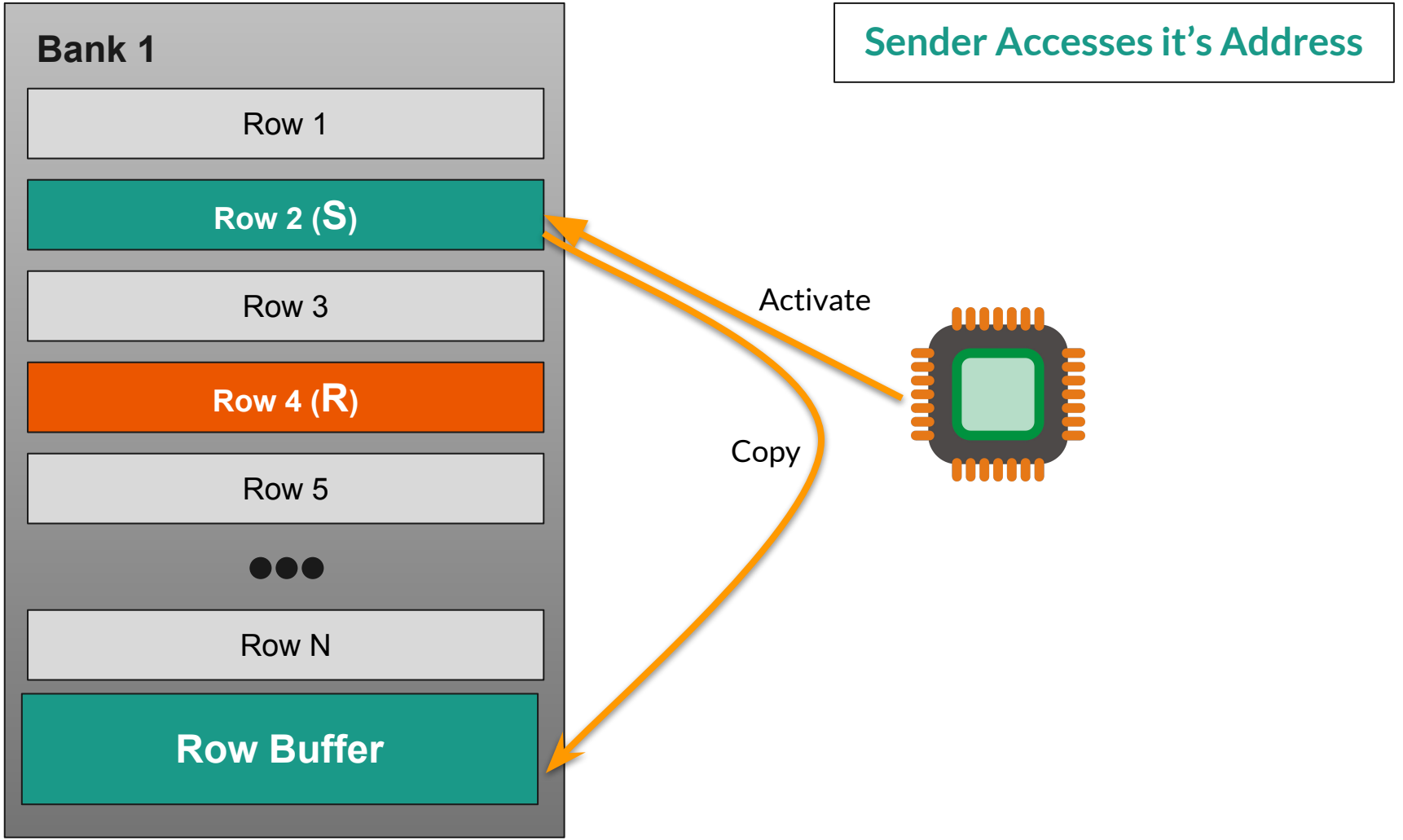


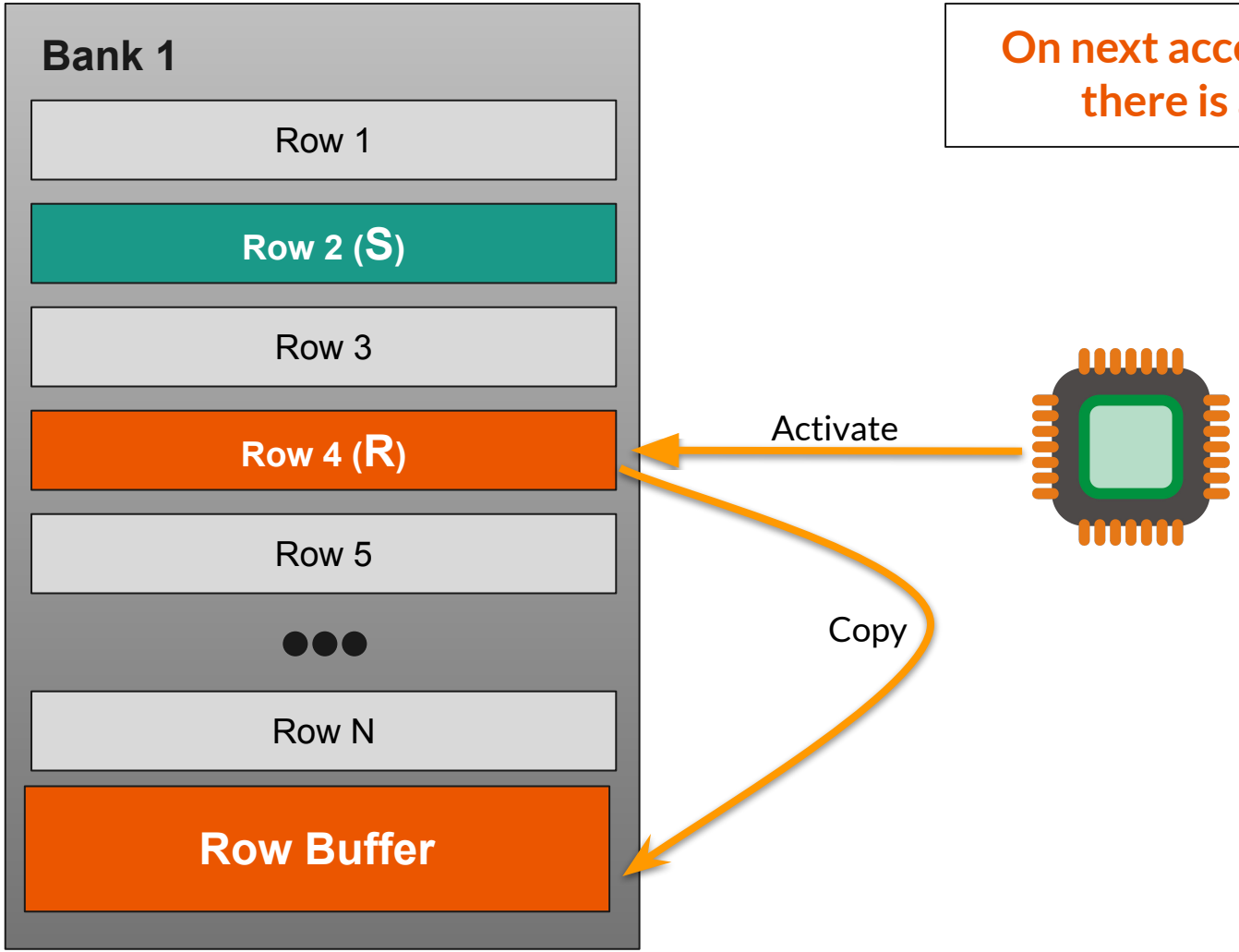
INITIALIZATION



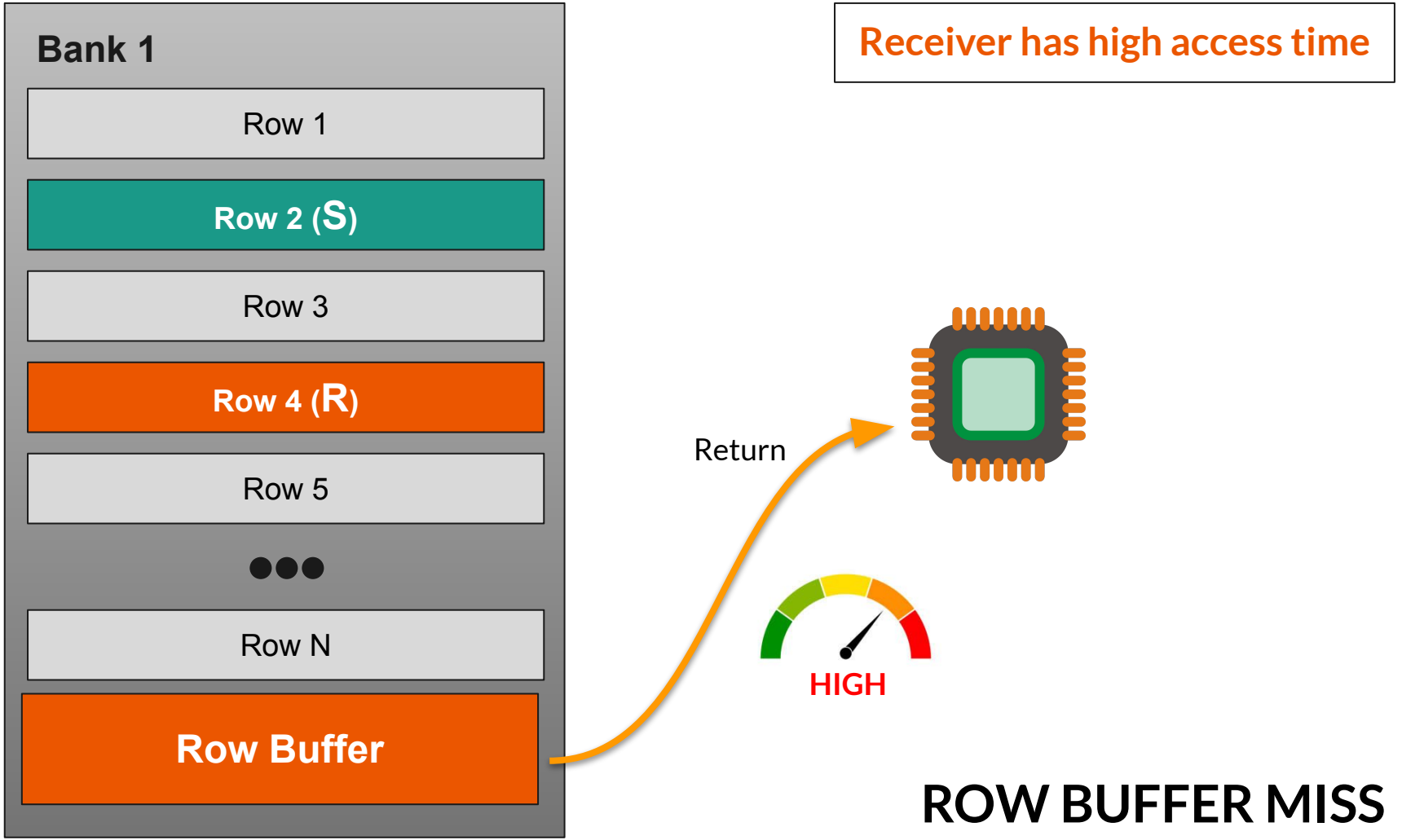
Repeated access always have low access time

ROW BUFFER HIT


Bank 1
Row 1
Row 2 (S)
Row 3
Row 4 (R)
Row 5
Row N
Row Buffer
Activate
Copy
Sender Accesses it's Address



On next access of receiver, there is a row miss


Bank 1
Row 1
Row 2 (S)
Row 3
Row 4 (R)
Row 5
Row N
Row Buffer
Return
HIGH
Receiver has high access time
ROW BUFFER MISS

Background

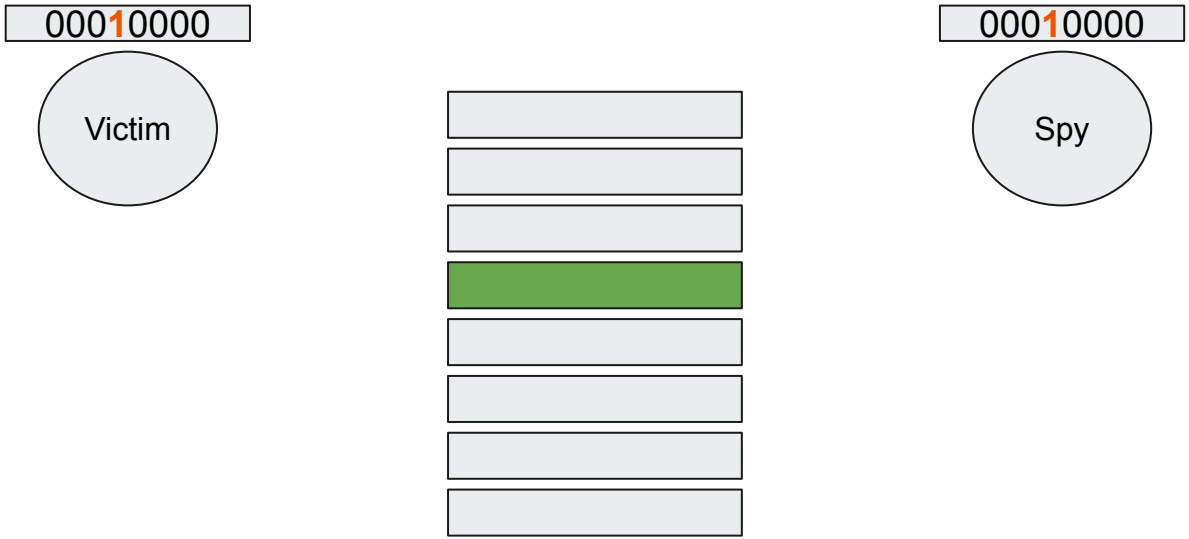
- DRAM Covert channel
- TimeCache

TimeCache*

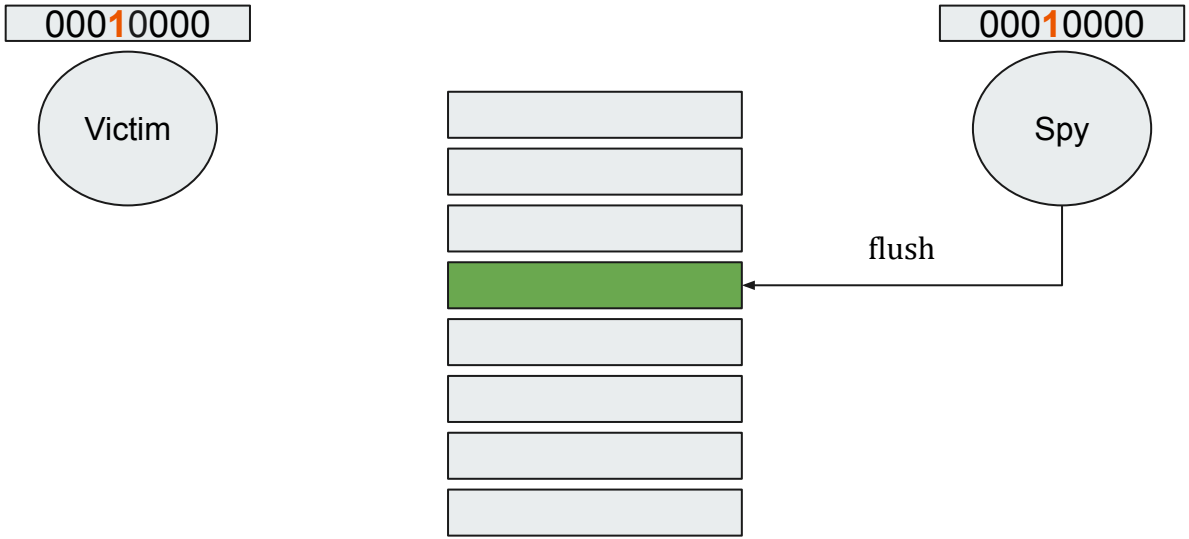
- For flush+reload attack, **first access** of attacker for **time measurement** is important.
- Resolution : **Delay first access**
  - To all cache lines → For each process, first access is **always Miss**.
  - Create a miss, even if it is a hit
  - **S-bit** denotes if it is the first access to the cache line by the process.

**D. Ojha and S. Dwarkadas, "TimeCache: Using Time to Eliminate Cache Side Channels when Sharing Software," 2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA), 2021, pp. 375-387, doi: 10.1109/ISCA52012.2021.00037.

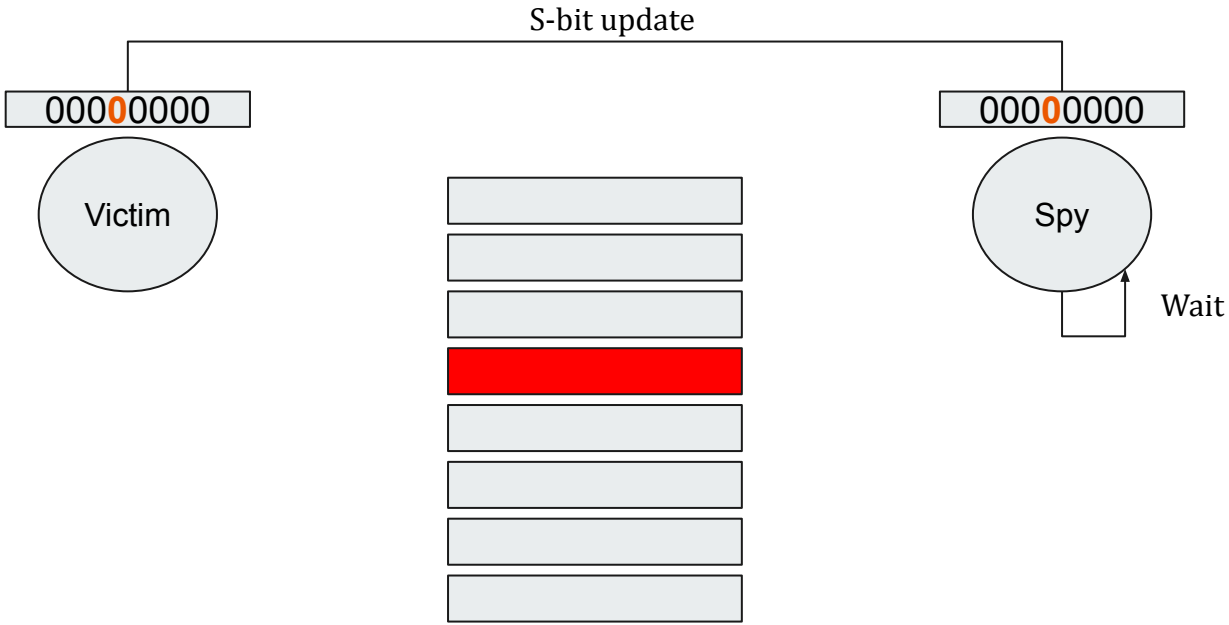
Example



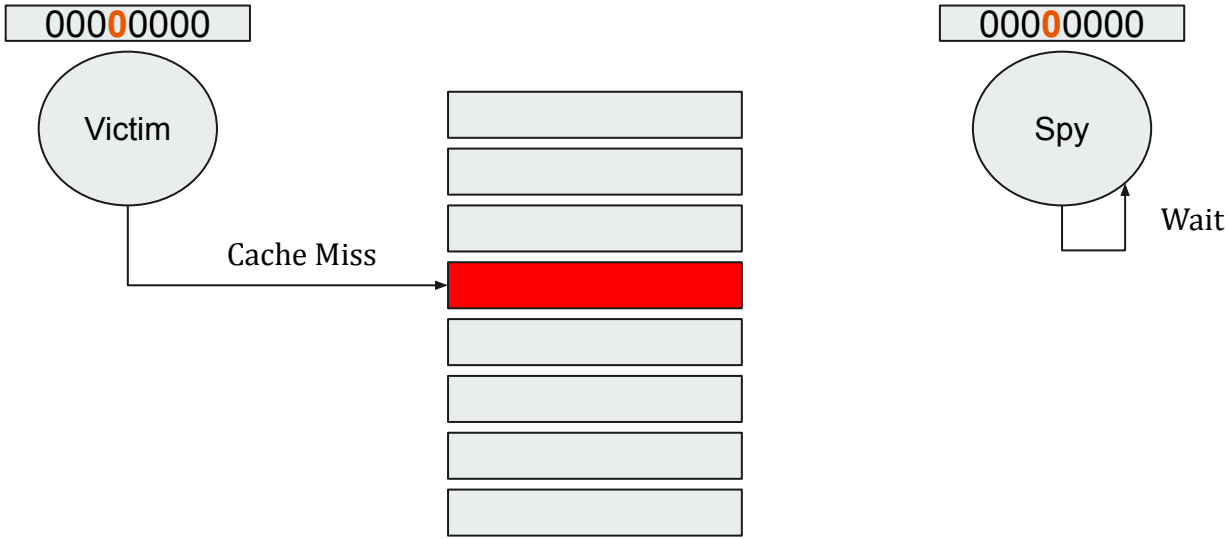
Example



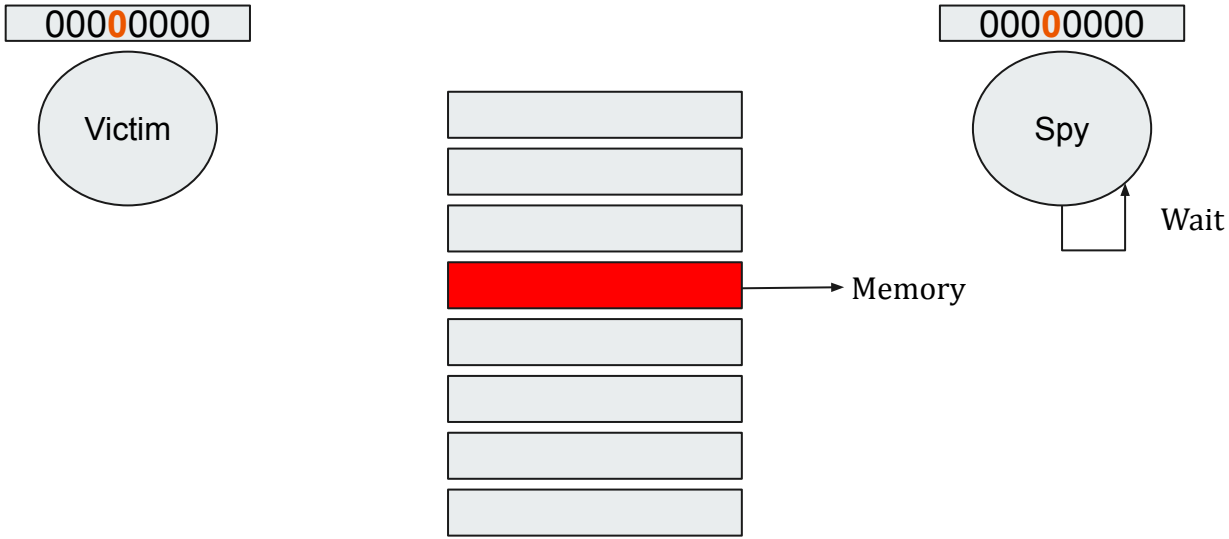
Example



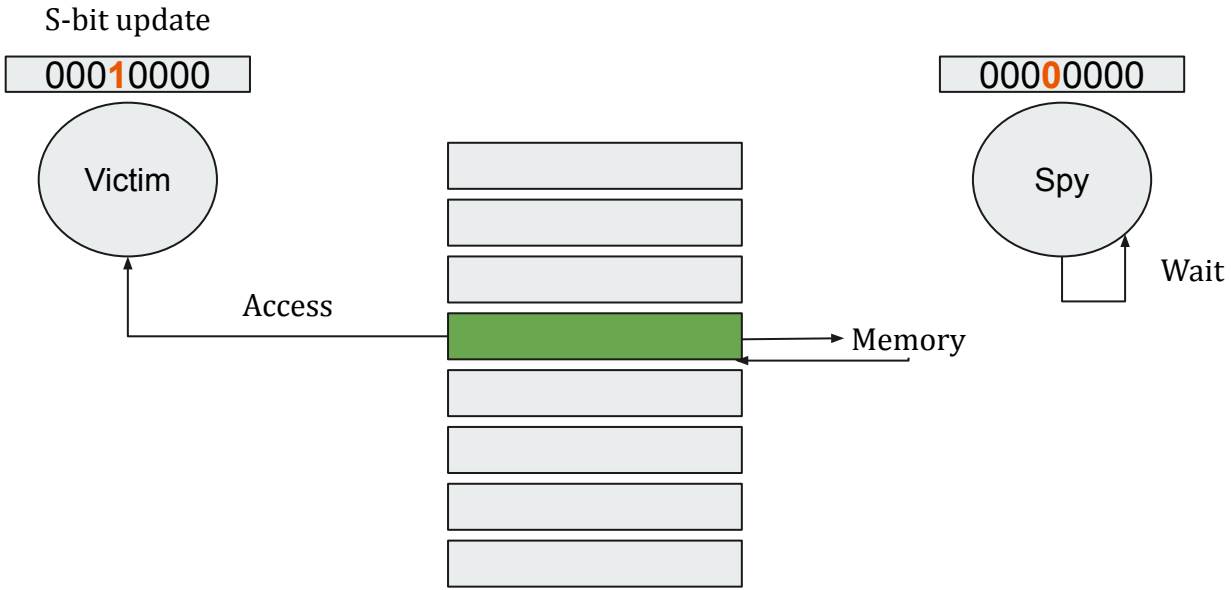
Example



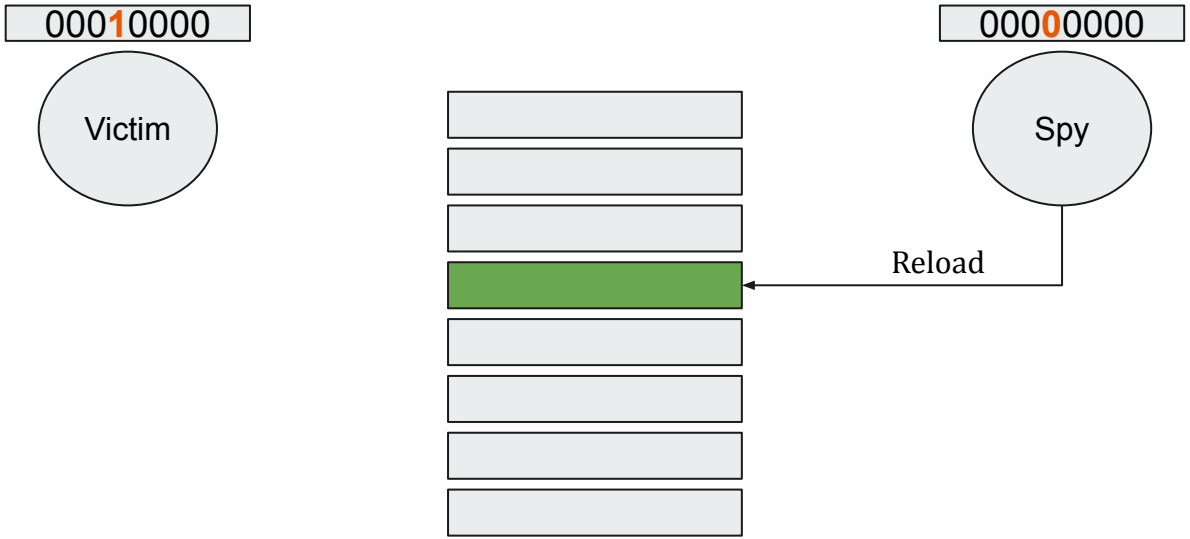
Example



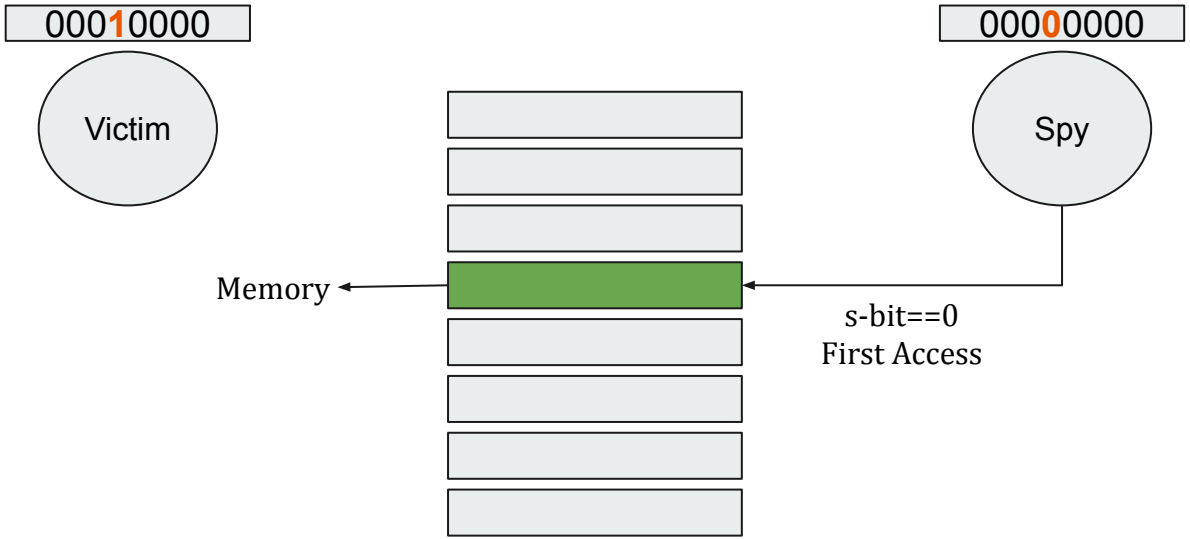
Example


S-bit update
00010000
Victim
Access
Memory
00000000
Spy
Wait

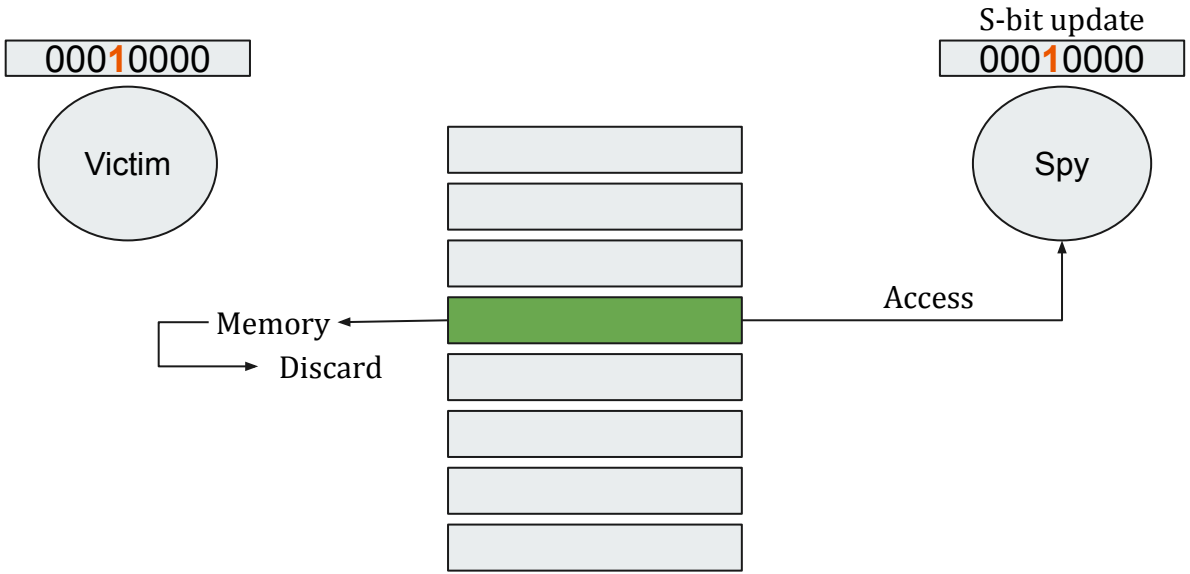
Example



Example



Example


00010000
Victim
S-bit update
00010000
Spy
Access
Memory
Discard

Golmaal Covert Channel

- Assumptions and Protocol
- Timing Diagram
- Transmission Channel
- Evaluation

Golmaal Covert Channel Assumptions

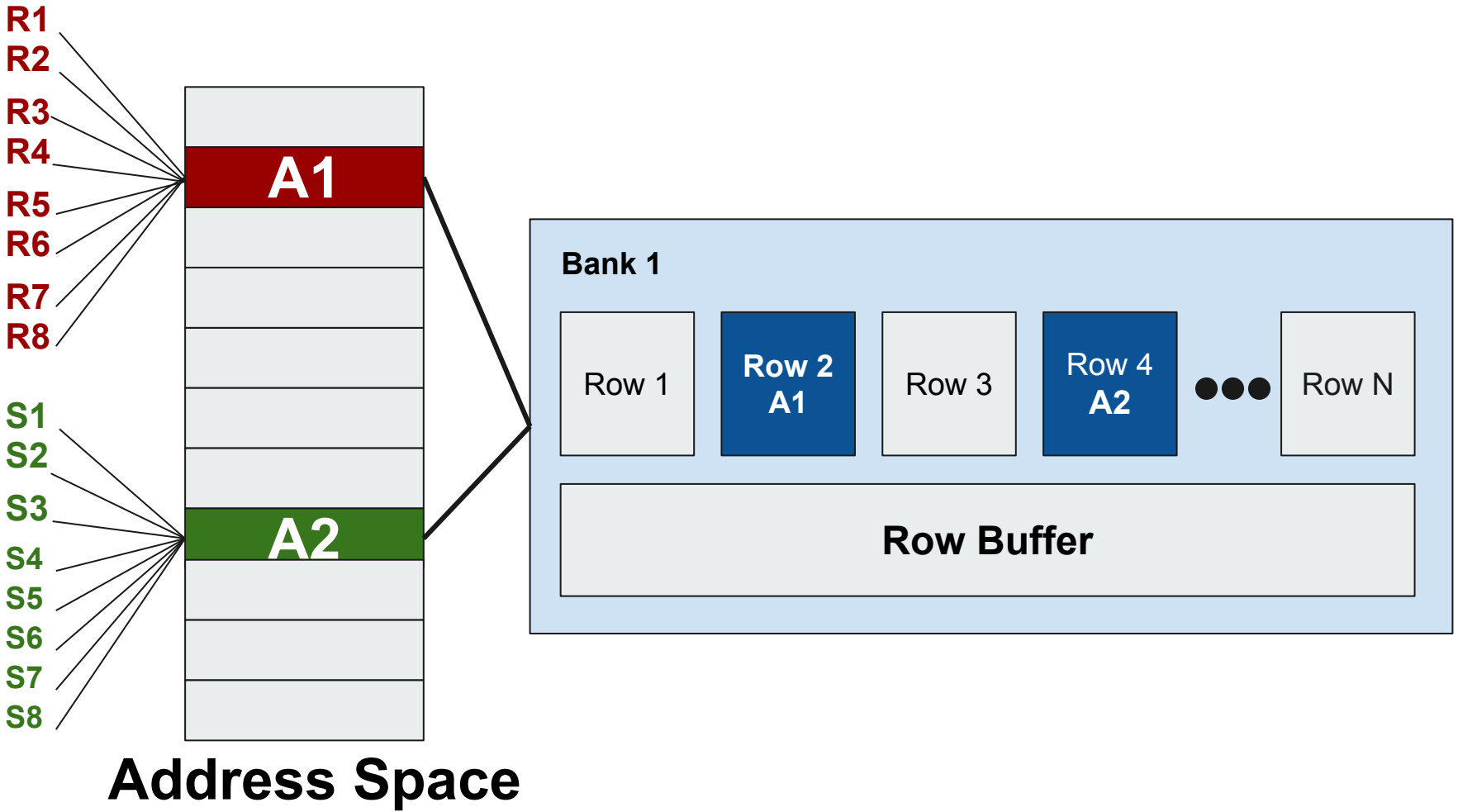
Theoretical Assumptions :

- Shared Memory Agreement.
- Senders and multiple receiver processes are allocated different rows of one DRAM bank of a given rank and channel.

Numerical Assumptions :

- Clflush Cycles = 300
- DRAM Access Cycles = 375(Row Buffer Hit) and 220(Row Buffer Miss)*
- Synchronization Cycle = 400 cycles
- Processor Speed = 4Ghz

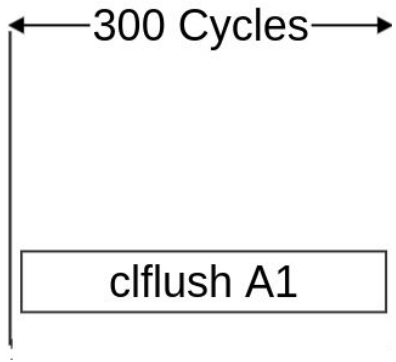
** “DRAM latency in IceLake,” https://www.7-cpu.com/cpu/IceLake.html, 2021


R1
R2
R3
R4
R5
R6
R7
R8
A1
S1
S2
S3
A2
S4
S5
S6
S7
S8
Address Space
Bank 1
Row 1
Row 2
A1
Row 3
Row 4
A2
Row N
Row Buffer

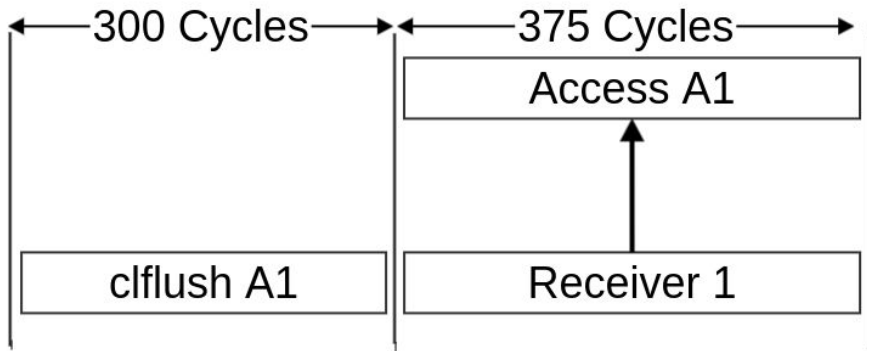
Golmaal Covert Channel

- Assumptions and Protocol
- Timing Diagram
- Transmission Channel
- Evaluation

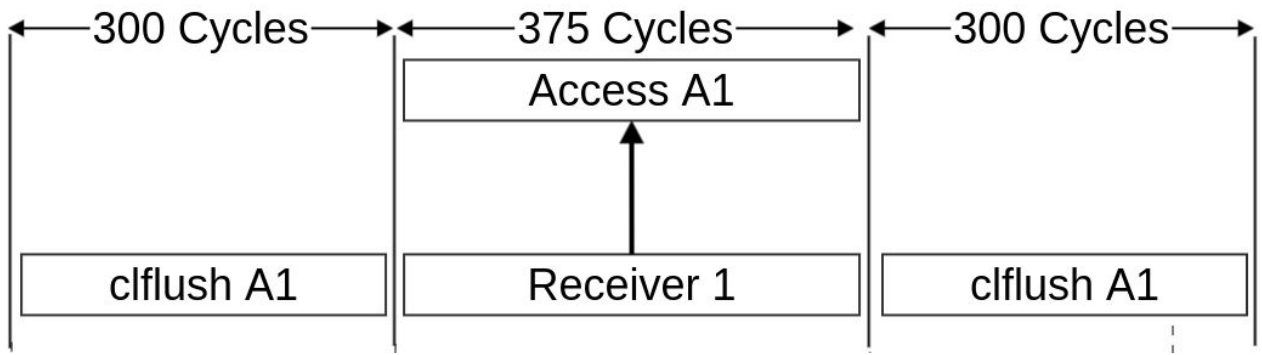
Timing diagram Without time-cache



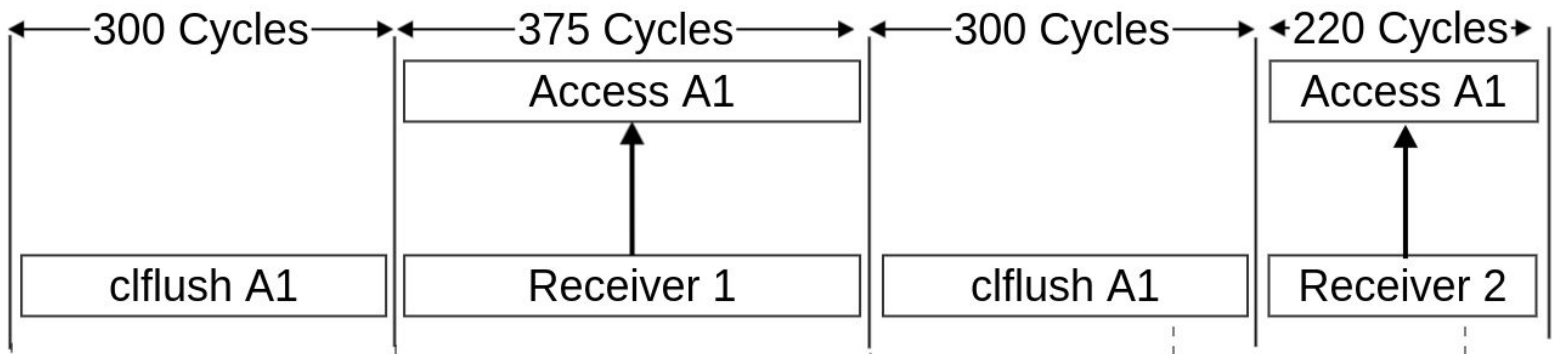
Timing diagram Without time-cache



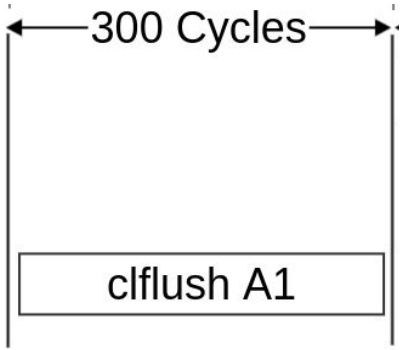
Timing diagram Without time-cache



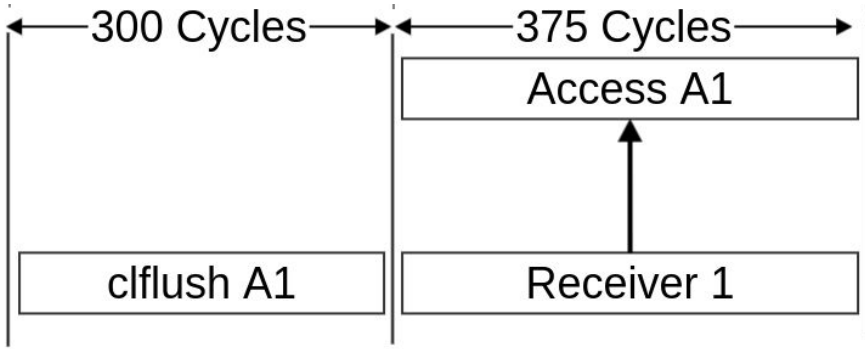
Timing diagram Without time-cache



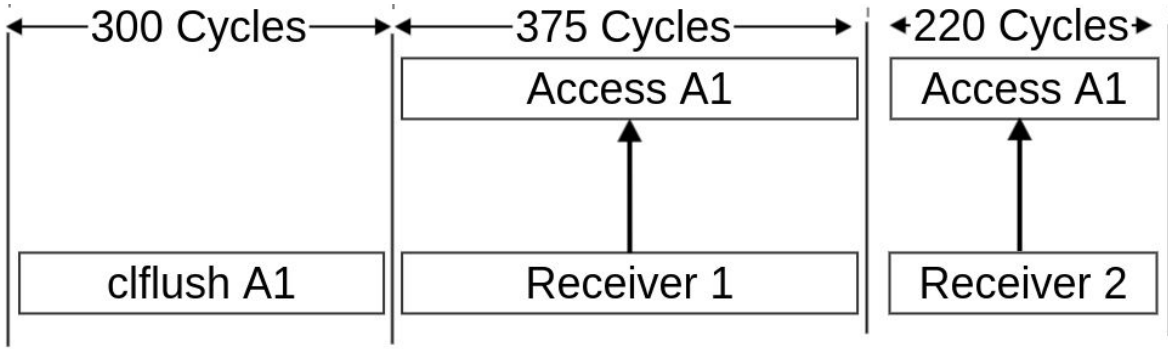
Timing diagram With time-cache



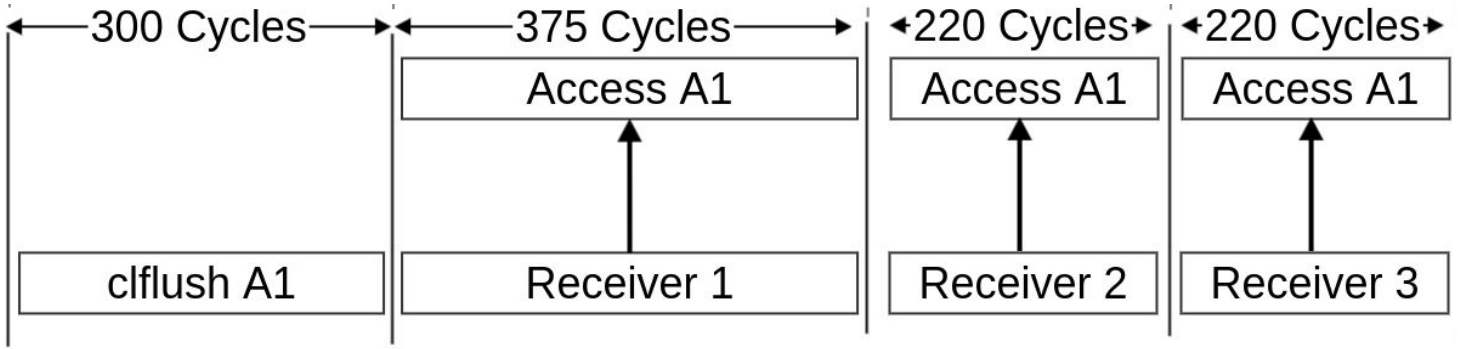
Timing diagram With time-cache



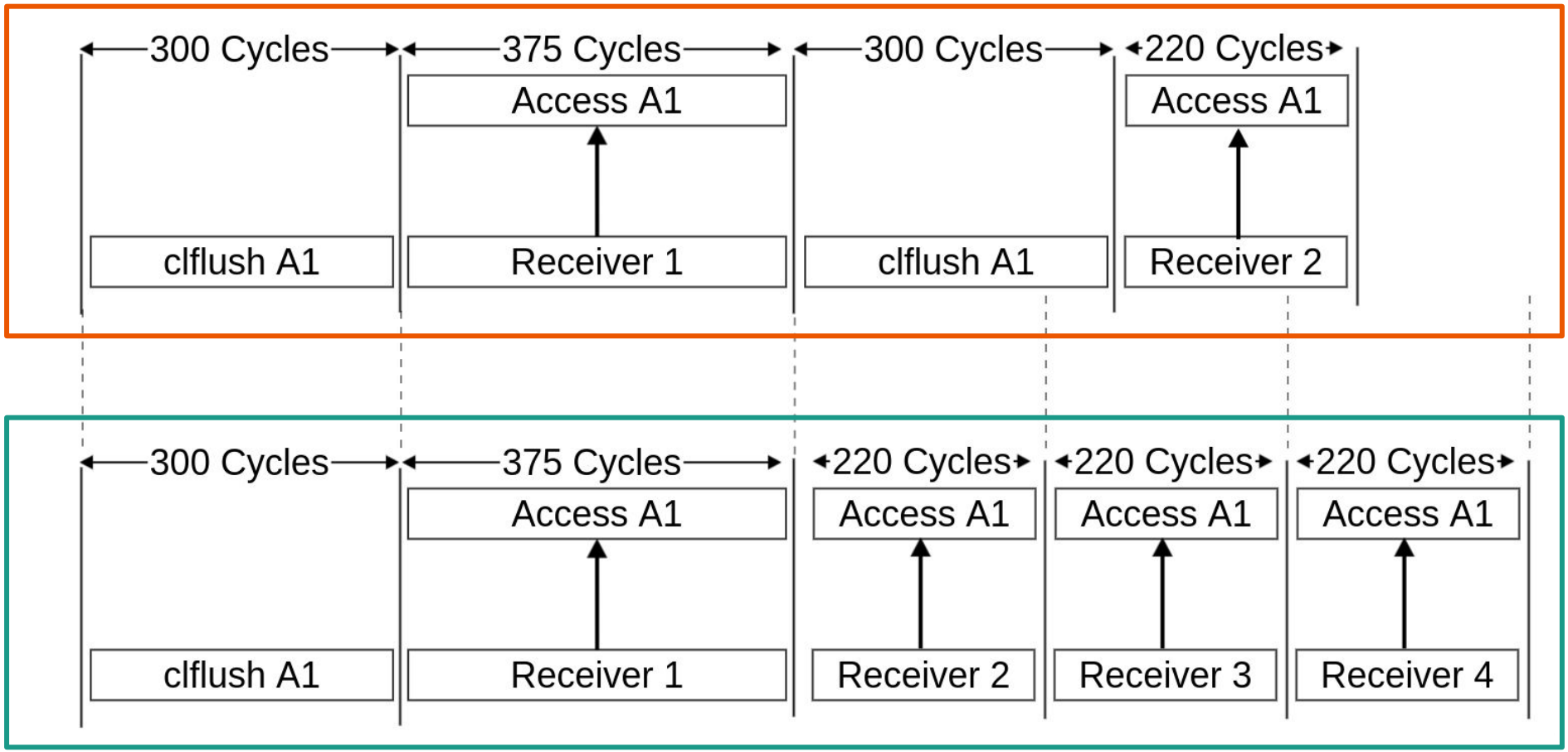
Timing diagram With time-cache



Timing diagram With time-cache



Comparison of timing diagram Without and With time-cache



Golmaal Covert Channel

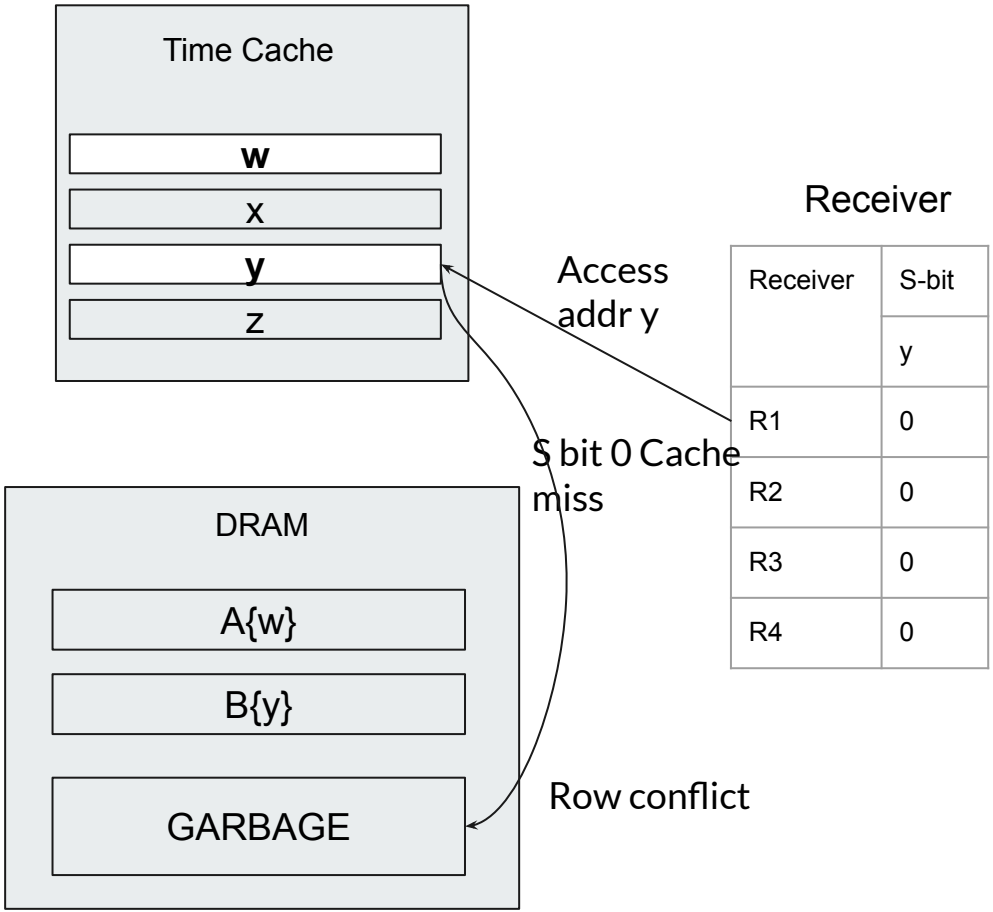
- Assumptions and Protocol
- Timing Diagram
- Transmission Channel
- Evaluation

TRANSMISSION

Data: [INIT]01001

Sender

Sender	S-bit
	w
S1	0
S2	0
S3	0
S4	0



Receiver

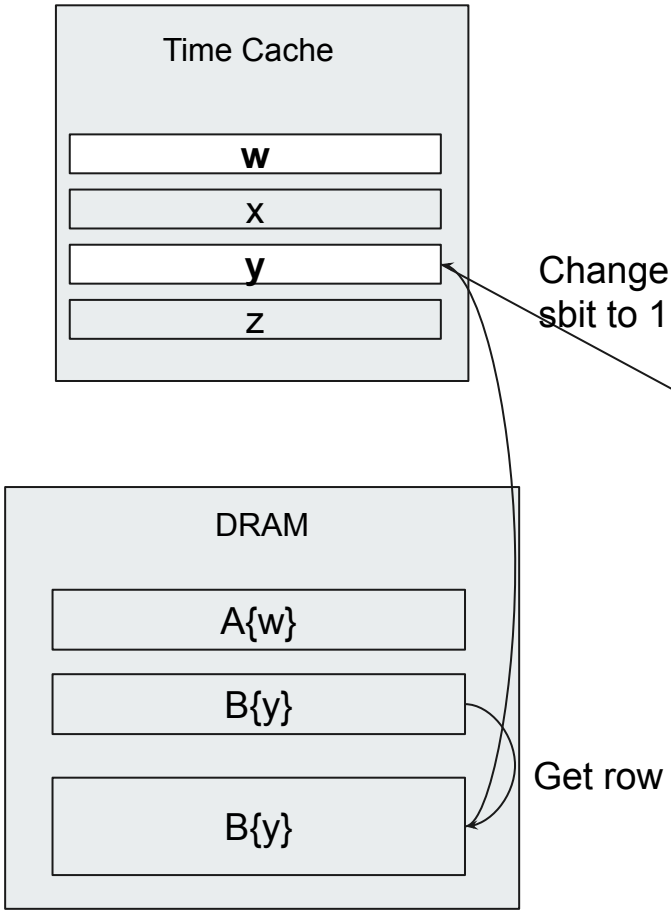
Receiver	S-bit
	y
R1	0
R2	0
R3	0
R4	0

TRANSMISSION

Data: [INIT]01001

Sender

Sender	S-bit
	w
S1	0
S2	0
S3	0
S4	0



Receiver

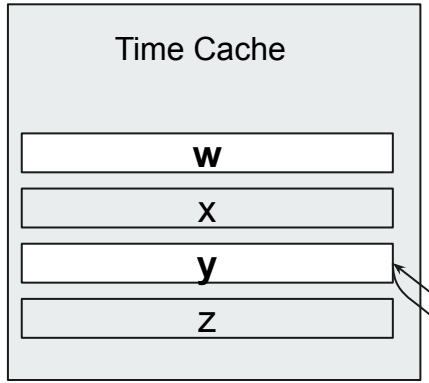
Receiver	S-bit
	y
R1	1
R2	0
R3	0
R4	0

TRANSMISSION

Data: [INIT]**0**1001

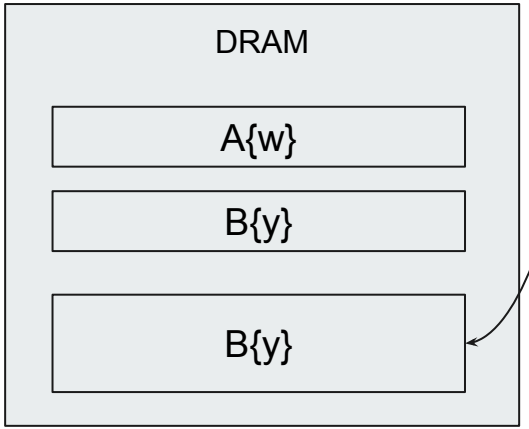
Sender

Sender	S-bit
	w
S1	0
S2	0
S3	0
S4	0



Access addr y

S bit 0
Cache miss



Row hit

Receiver

Receiver	S-bit
	y
R1	1
R2	0
R3	0
R4	0

Low access time

≈ ‘0’ bit

TRANSMISSION

Data: [INIT]01001

Sender

Sender	S-bit
	w
S1	0
S2	0
S3	0
S4	0

Access
addr w

Time Cache

w

x

y

z

S bit 0
Cache miss

DRAM

A{w}

Row
Conflict

B{y}

B{y}

Receiver

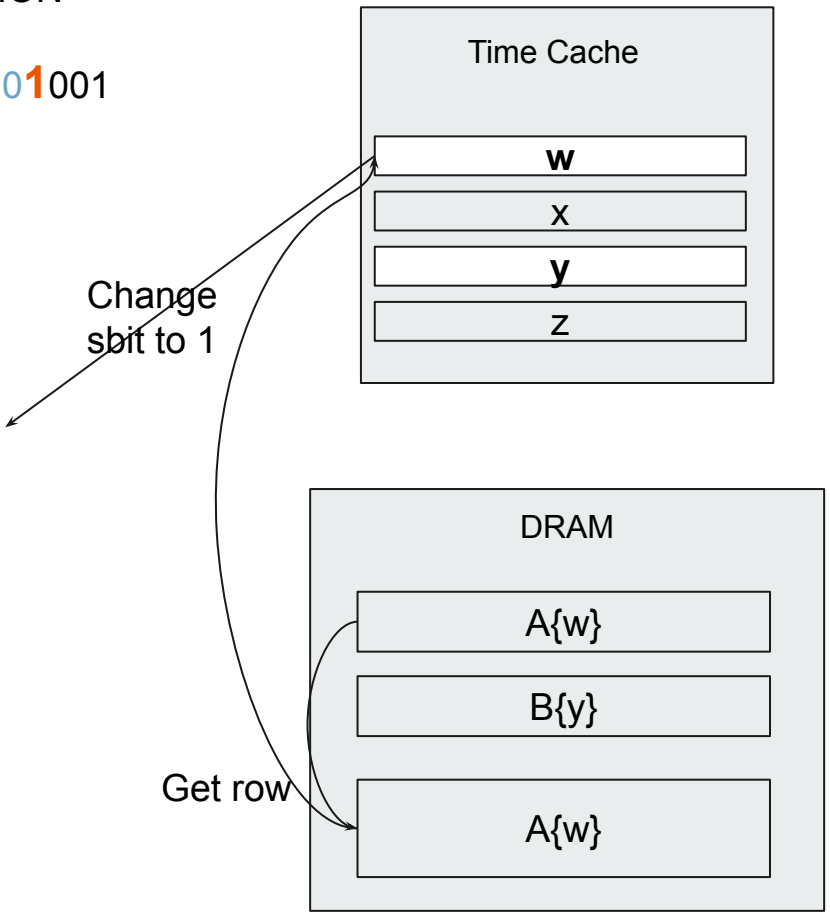
Receiver	S-bit
	y
R1	1
R2	1
R3	0
R4	0

TRANSMISSION

Data: [INIT]01001

Sender

Sender	S-bit
	w
S1	1
S2	0
S3	0
S4	0



Receiver

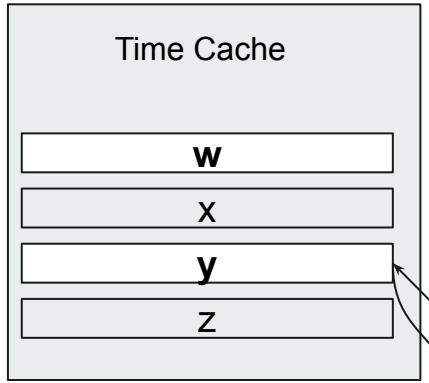
Receiver	S-bit
	y
R1	1
R2	1
R3	0
R4	0

TRANSMISSION

Data: [INIT]01001

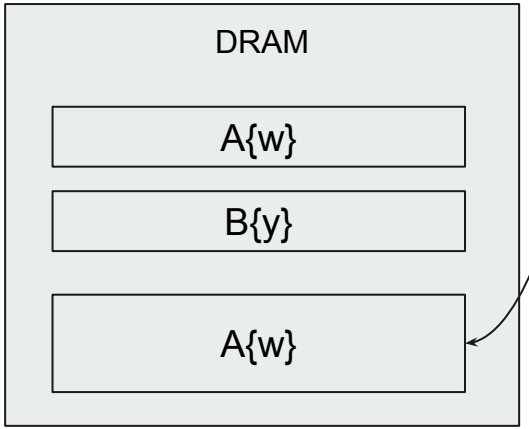
Sender

Sender	S-bit
	w
S1	1
S2	0
S3	0
S4	0



Access addr y

S bit 0
Cache miss



Row conflict

Receiver

Receiver	S-bit
	y
R1	1
R2	1
R3	0
R4	0

≈ High access time

‘1’ bit

Golmaal Covert Channel

- Assumptions and Protocol
- Timing Diagram
- Transmission Channel
- Evaluation

Simulation infrastructure

Simulators :

- Extensively modified ChampSim* microarchitectural simulator
- Ramulator* , a fast and cycle-accurate DRAM simulator

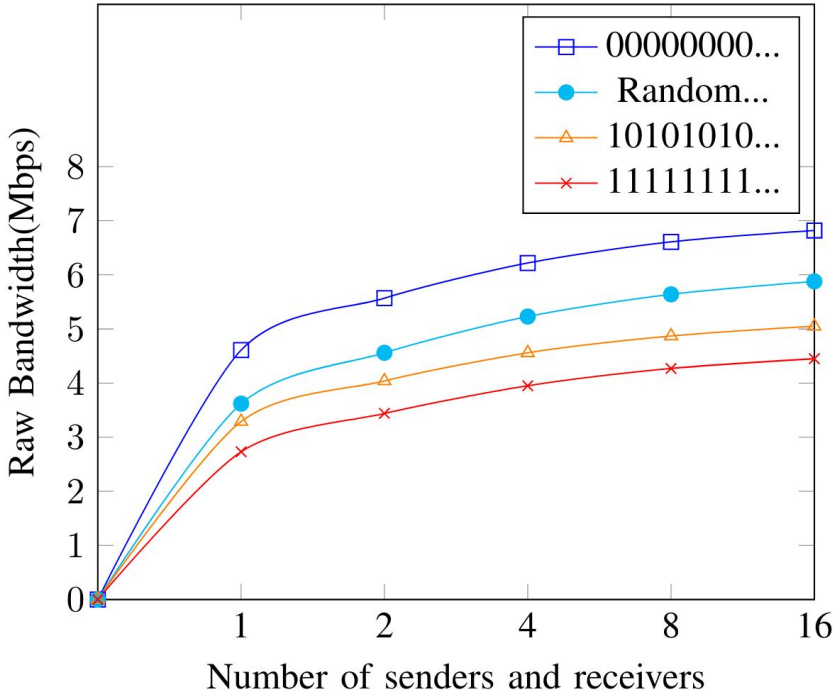
Simulator Parameters and Configurations:

- DDR4 DRAM controllers with a data rate of 3200 MT/sec.
- To synchronize between a pair of sender and receiver processes, we use the wall clocktime.
- To further improve synchronization we use the ***nanosleep*** system call for 100ns after every DRAM access by a sender and a receiver.

** Online. Available: https://github.com/ChampSim/ChampSim, Champ-sim Simulator.
** Y. Kim, W. Yang, and O. Mutlu, "Ramulator: A fast and extensibledram simulator,"IEEE Computer Architecture Letters, vol. 15, no. 1,pp. 45–49, 2016.

Number of Sender-Receiver

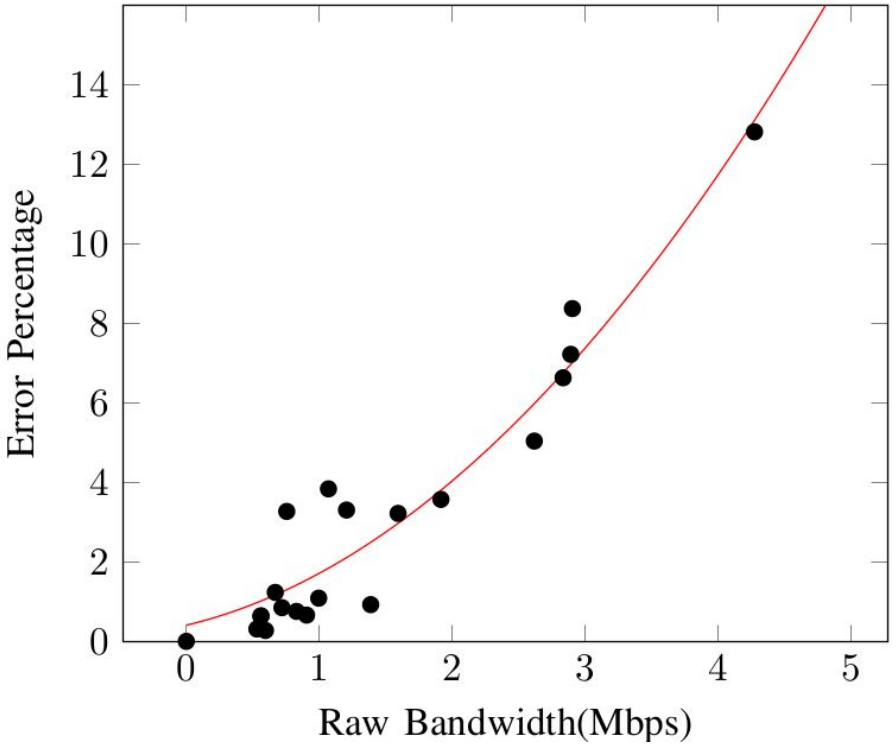
- Data:
  - 000000….
  - Random…
  - 101010…..
  - 111111……



“Bandwidth increases with increase in number of sender and receiver”

Error Percentage

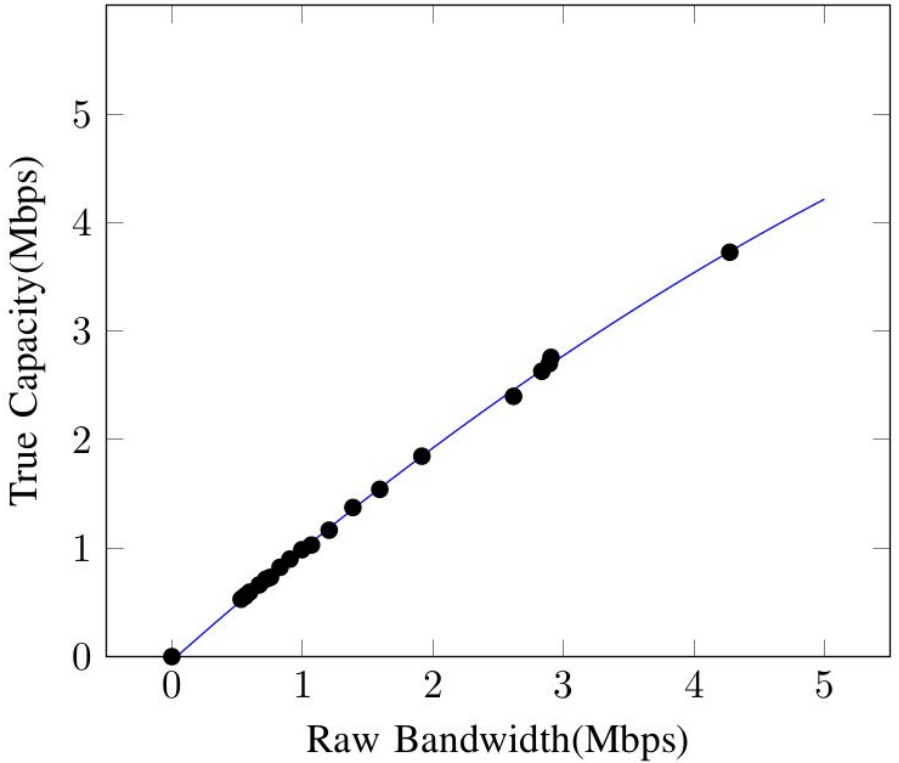
- Eight sender and receiver pair communicating a payload of "**11111111..1**".
- Error percentage is maximum at **4.28 Mbps** with **12.8%** of error.



"As the raw-bandwidth increase so does the probability of error"

Evaluation

- Eight sender and receiver pair communicating a payload of “11111111…1”.
- The maximum True capacity we achieved is 3.72 Mbps while transferring 1111….



Thank You
Any Questions ??