DRAM

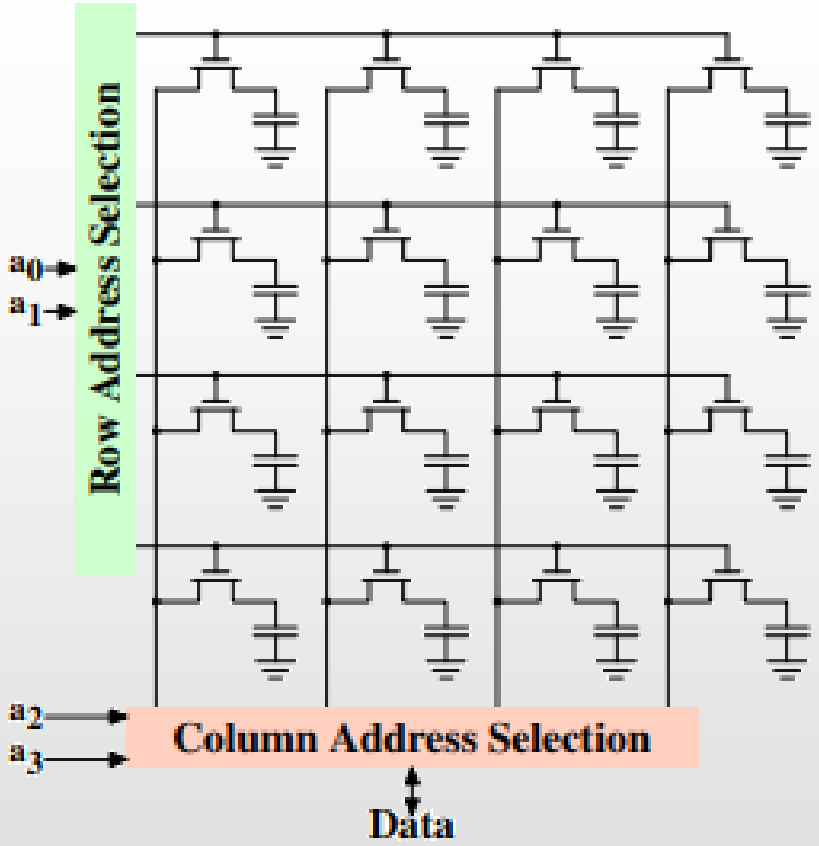
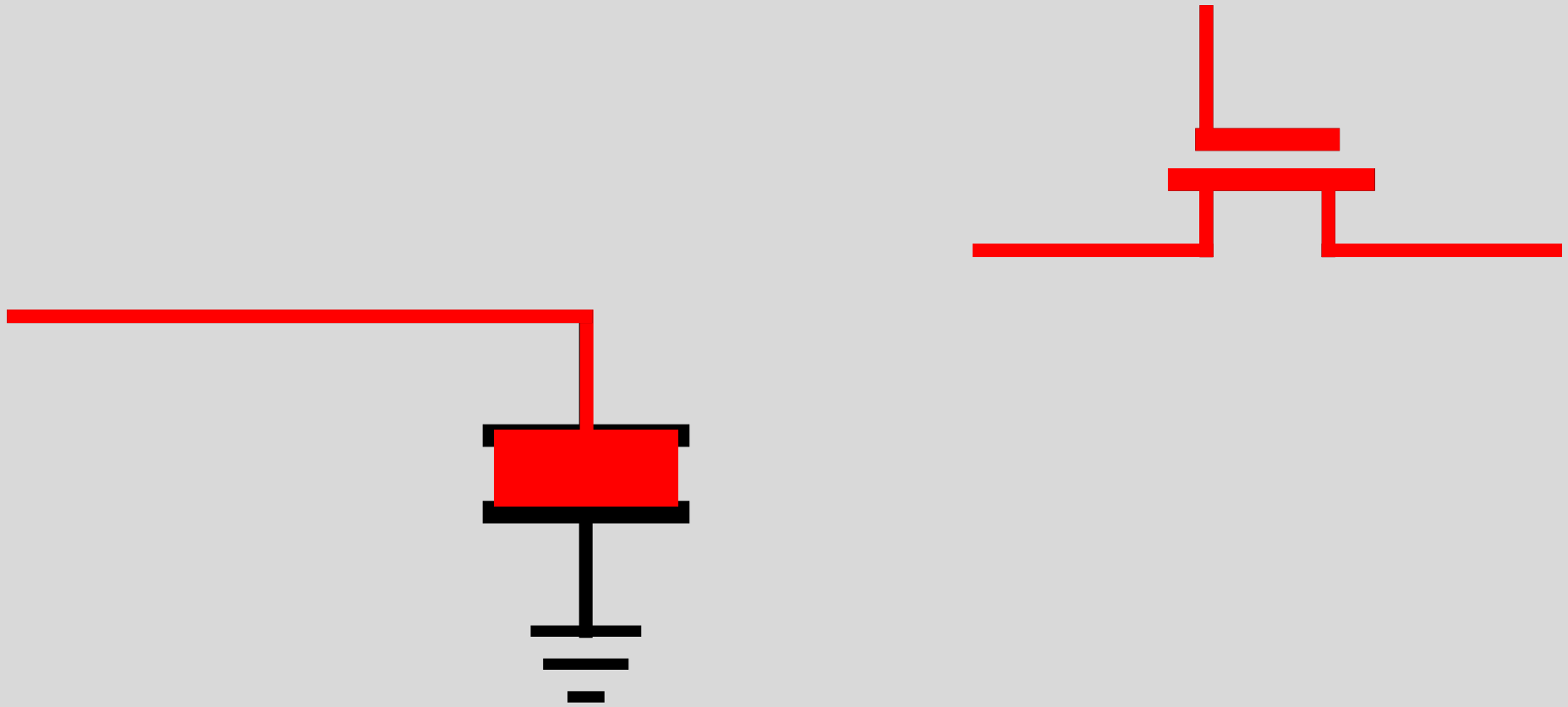
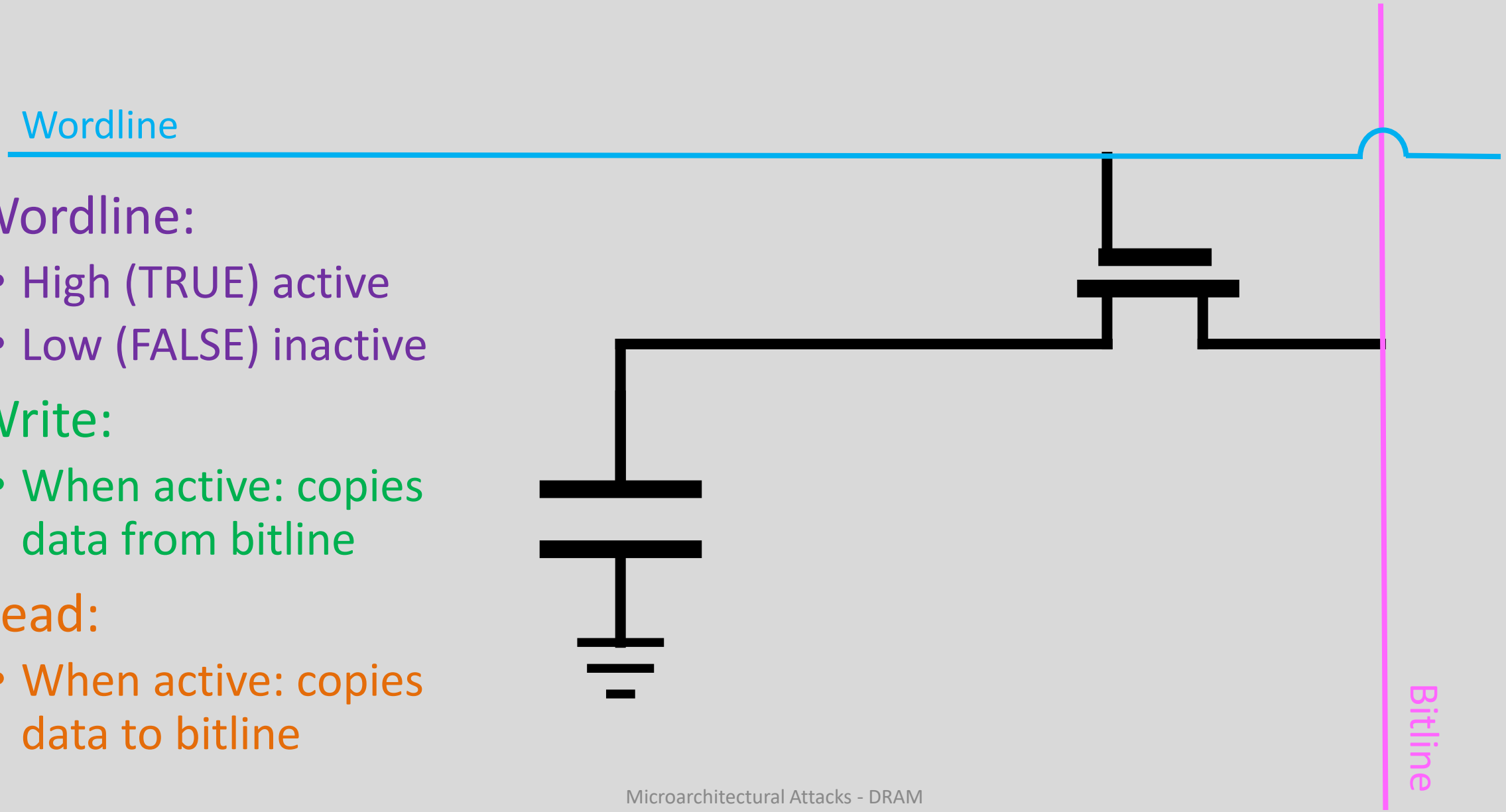


Figure 2.7: Dynamic RAM Schematic

Basic Electronics



DRAM Cell

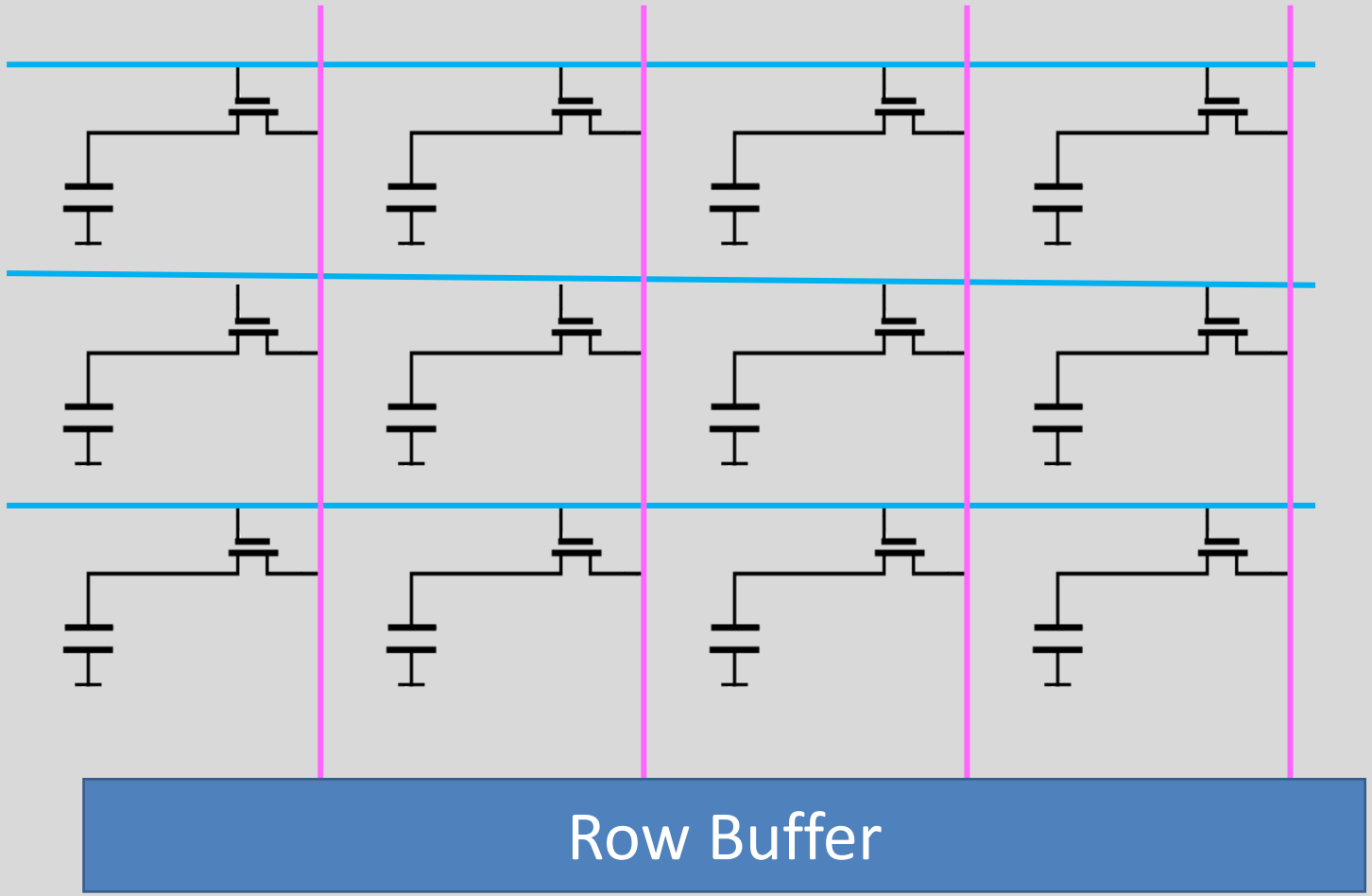


- Wordline:
  - High (TRUE) active
  - Low (FALSE) inactive
- Write:
  - When active: copies data from bitline
- Read:
  - When active: copies data to bitline

DRAM Array Organisation

- Activation: copies a row to the row buffer
- Read/write operate on row buffer
- Precharge: copies row buffer to row

- Capacitors lose charge
  - Each row is refreshed at least once in 64ms



DRAM Structure

Orosa et al. MICRO ‘21

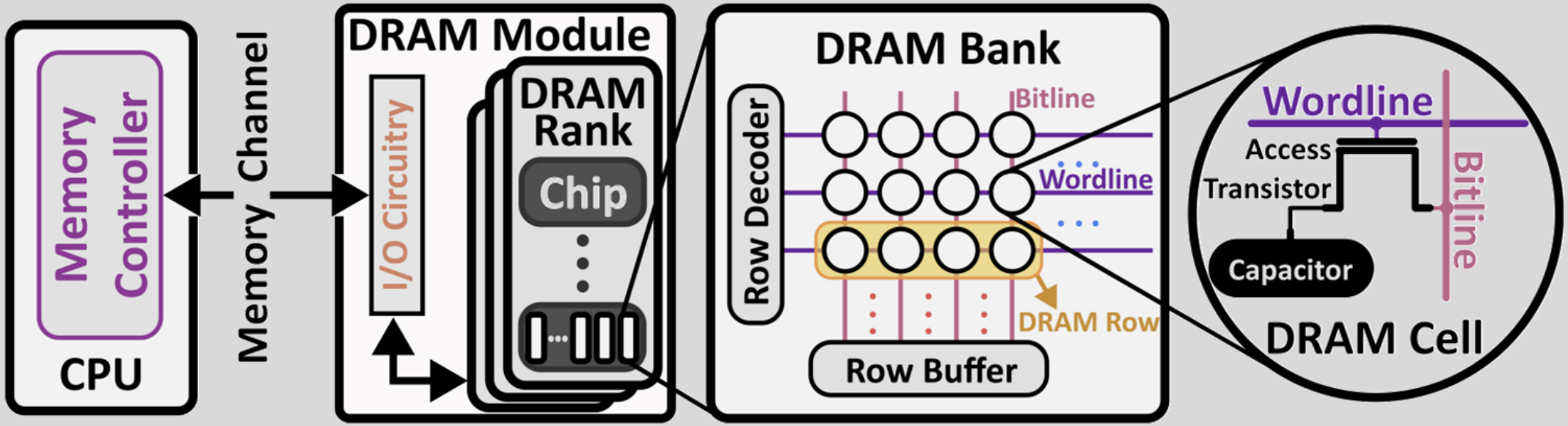
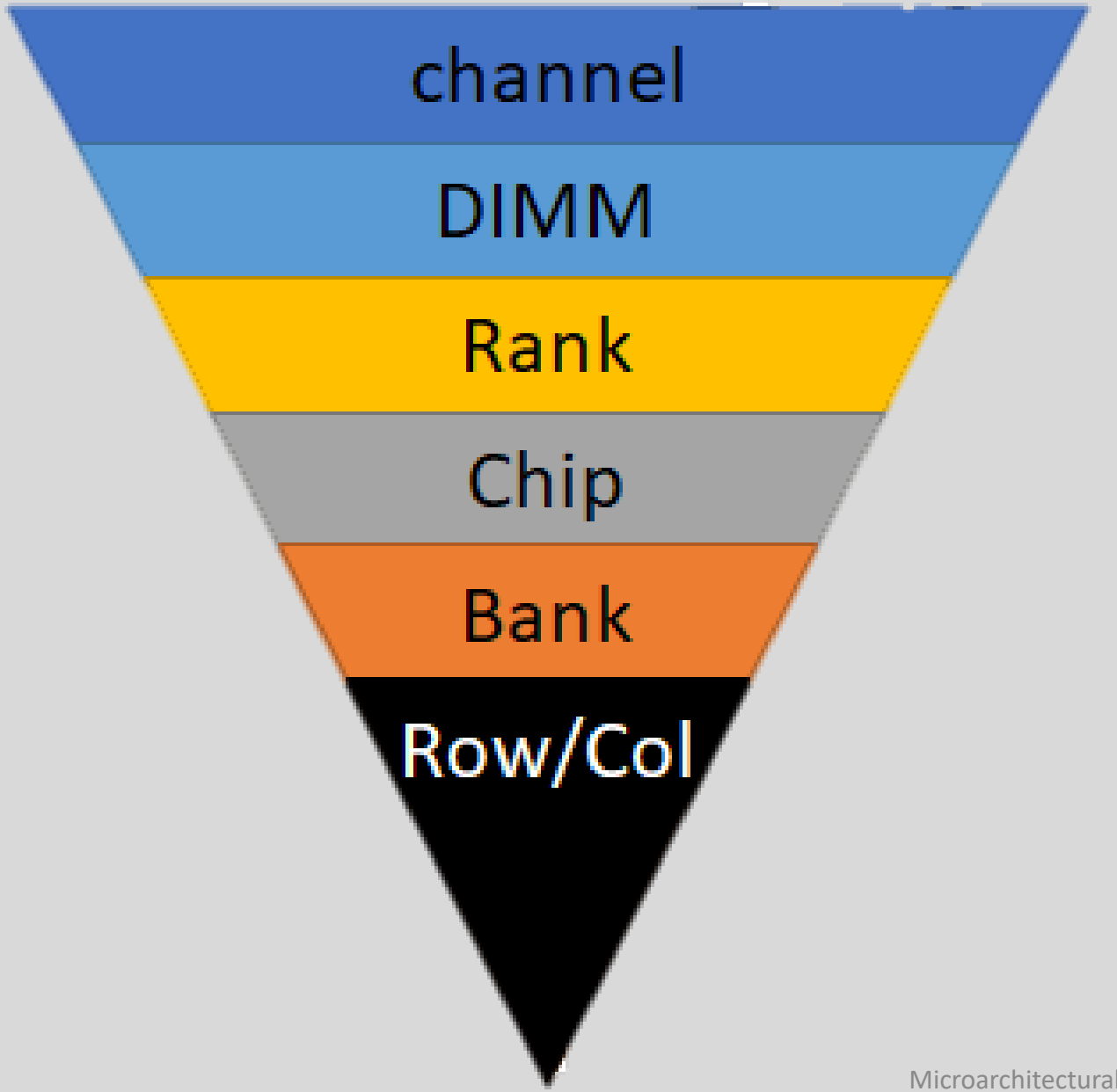
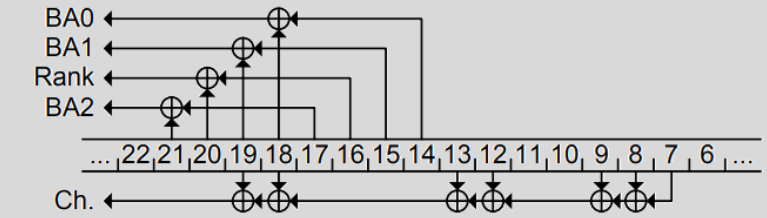


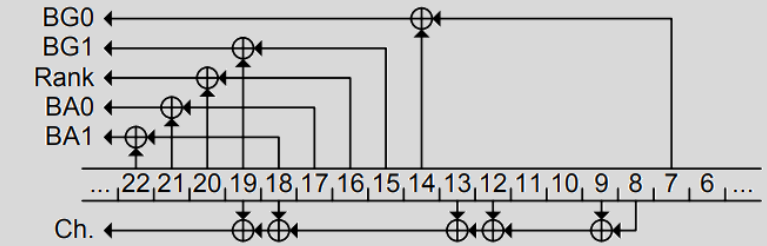
Fig. 1: DRAM organization.

DRAM Hierarchy

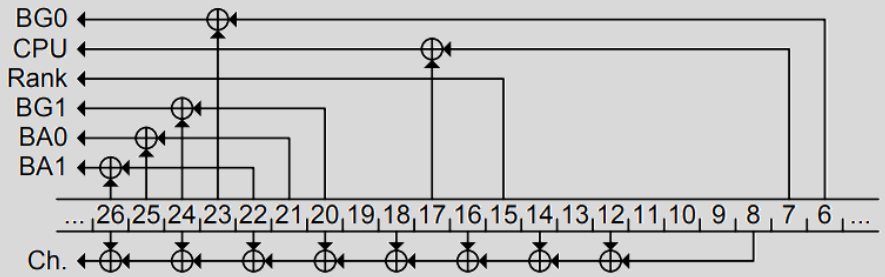




(b) Ivy Bridge / Haswell – DDR3.



(c) Skylake – DDR4.

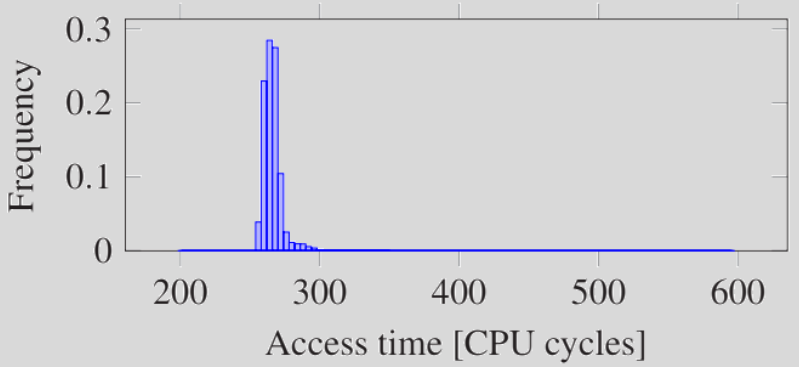


(d) Dual Haswell-EP (Interleaved Mode) – DDR4.

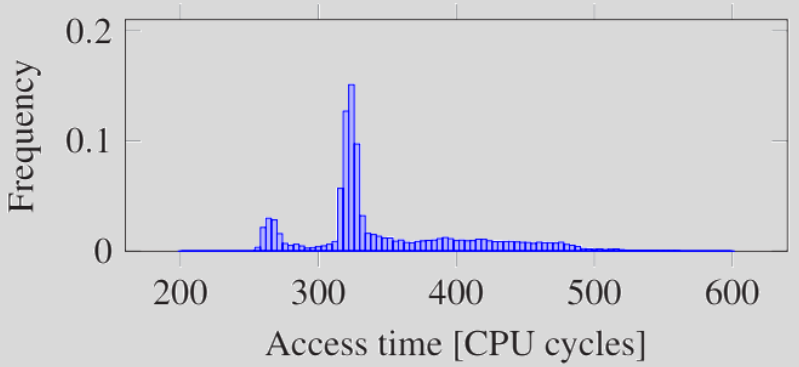
 Pessl et al. USENIX Sec 2016

DRAM Open Row Attack (Pessl et al. USENIX Sec 2016)

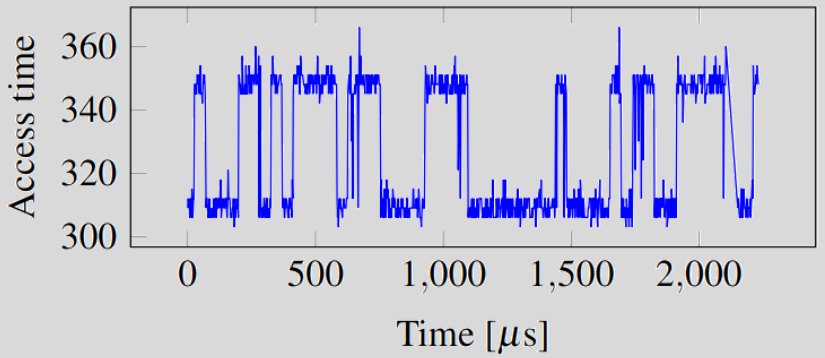
- Covert channel – sender and receiver conflict on same row
- Side channel – observe keystroke timing

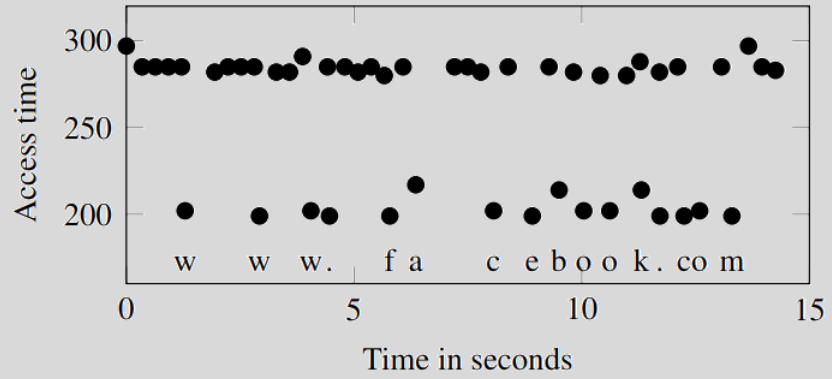


(a) Sender inactive on bank: sending a 0.



(b) Sender active on bank: sending a 1.





Cold Boot Attacks (Halderman et al. USENIX Security 2008)

- Cooling memory down reduces charge leakage
- Can pull memory out of a device, put in another device and read contents

Figure 5: Before powering off the computer, we spray an upside-down canister of multipurpose duster directly onto the memory chips, cooling them to −50 °C. At this temperature, the data will persist for several minutes after power loss with minimal error, even if we remove the DIMM from the computer.

Cold Boot Attack

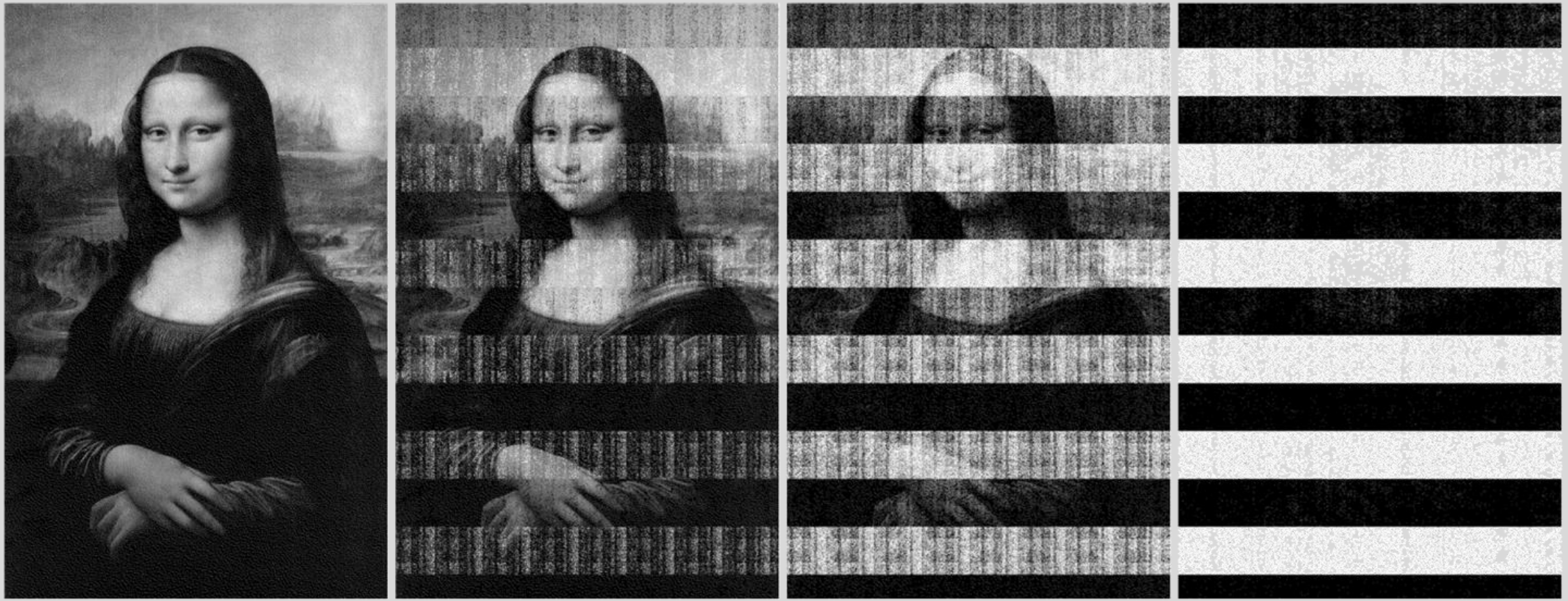
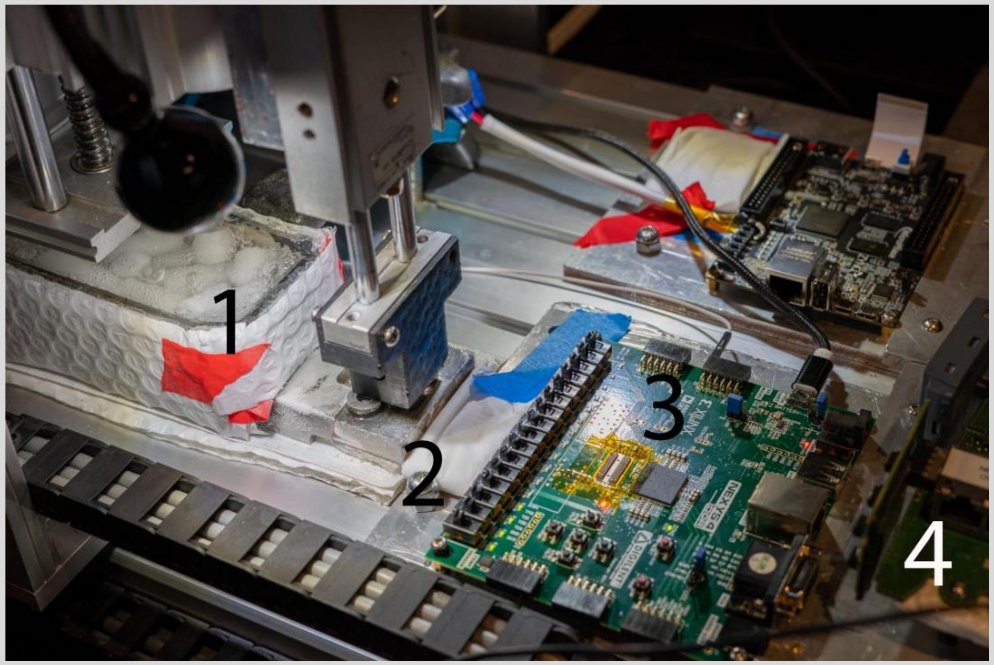


Figure 4: We loaded a bitmap image into memory on Machine A, then cut power for varying lengths of time. After 5 seconds (left), the image is indistinguishable from the original. It gradually becomes more degraded, as shown after 30 seconds, 60 seconds, and 5 minutes.

Automation (Wu et al. WOOT 2023)



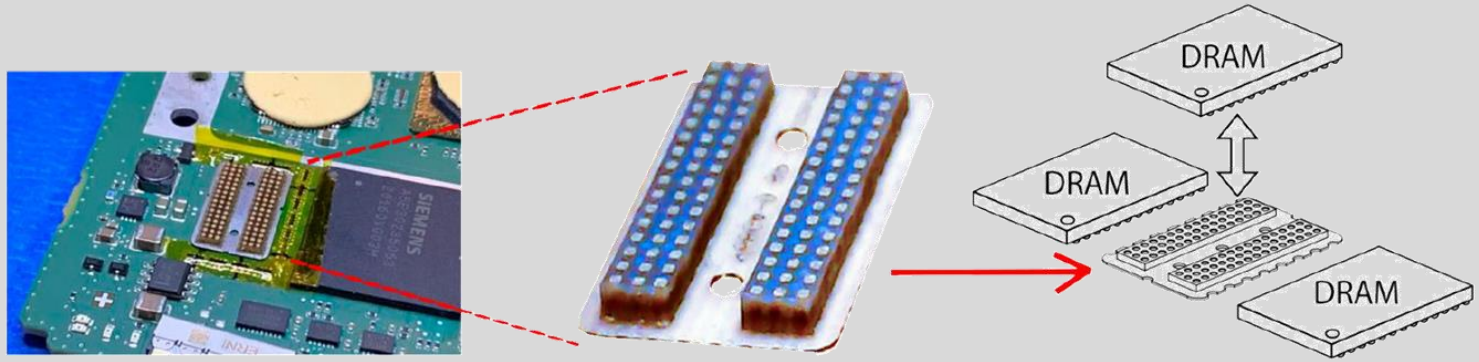
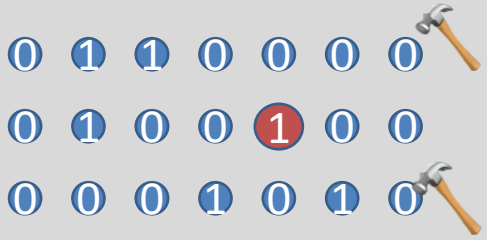


Fig. 2. New method for transferring embedded memory chips, such as BGA DRAM chips that are soldered on the embedded device printed circuit board (PCB) board. Our designed conductive rubber can make all the memory removable at runtime without affecting the function of the target device.

Rowhammer (Kim et al. ISCA 2014)

- Repeatedly toggling a wordline (aggressor row) causes disturbance errors in neighbouring rows
- Repeatable
- One way flip
- Data dependent



Access Pattern	Disturbance Errors?
1. $(open–read–close)^N$	**Yes**
2. $(open–write–close)^N$	**Yes**
3. $open–read^N–close$	No
4. $open–write^N–close$	No

Table 4. Access patterns that induce disturbance errors

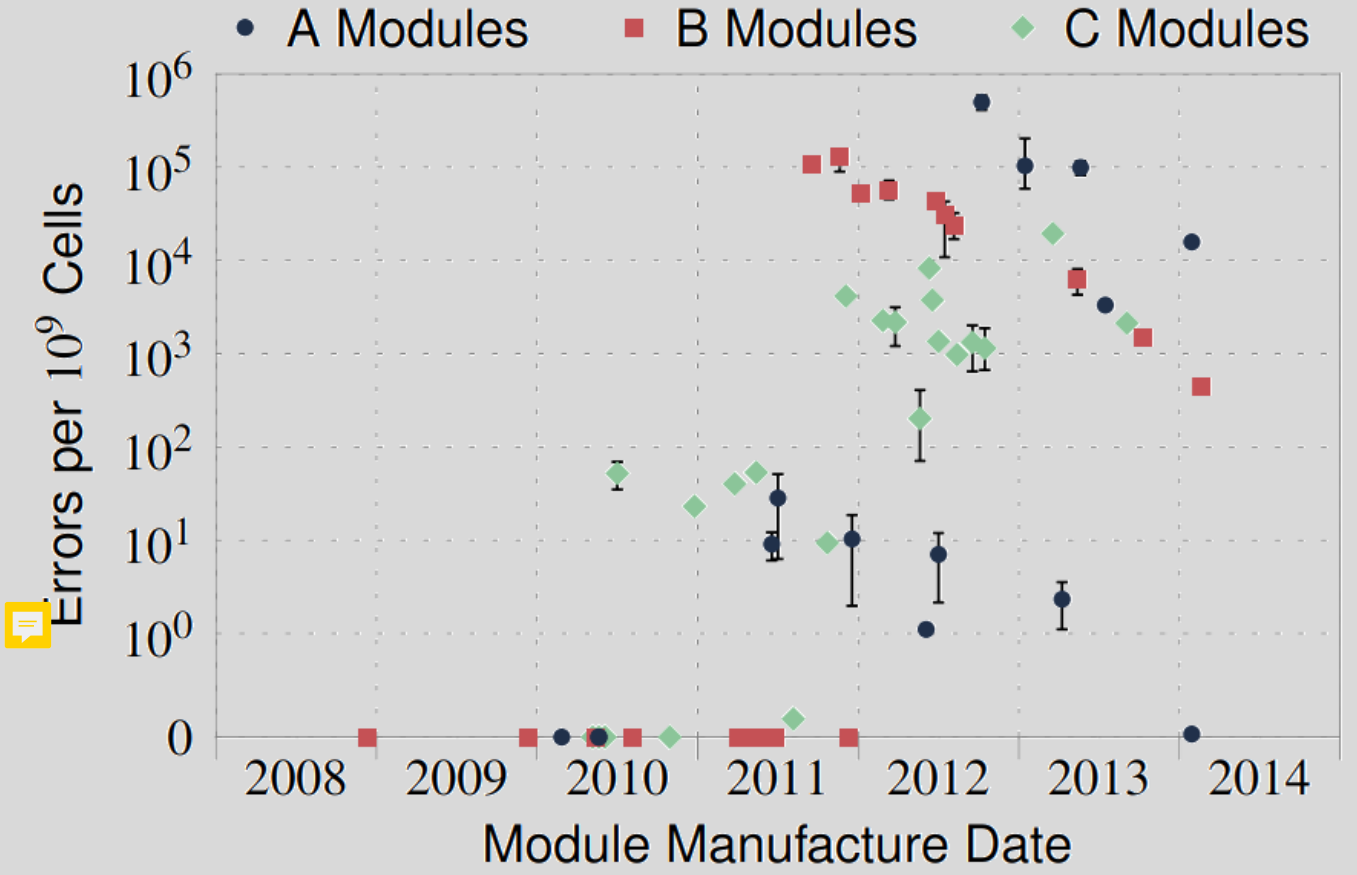
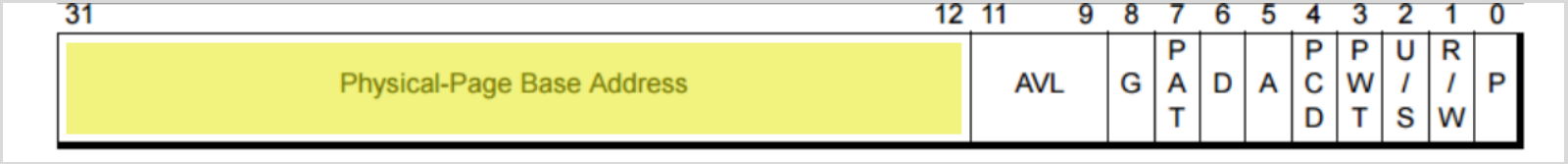
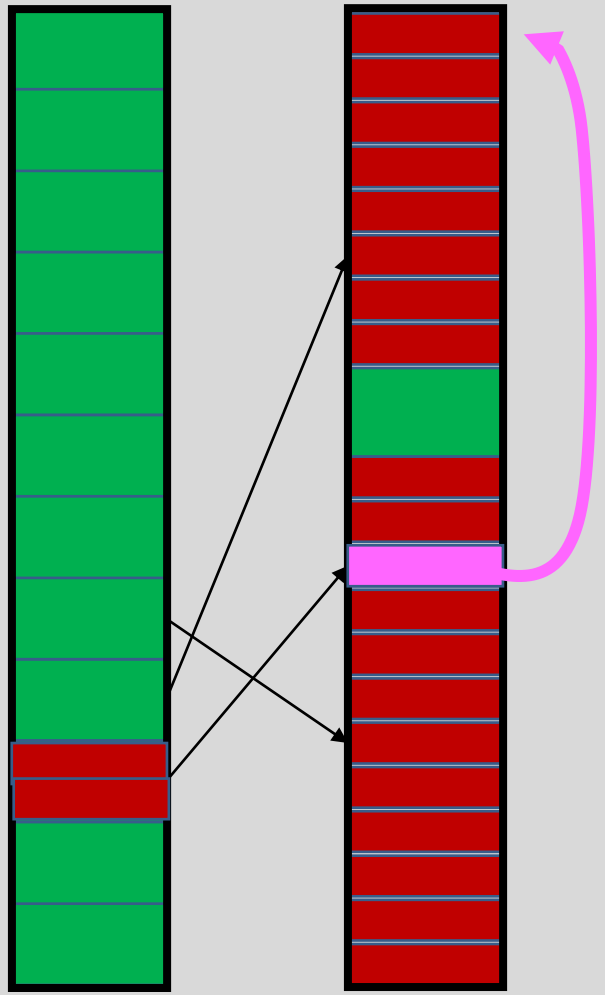


Figure 3. Normalized number of errors vs. manufacture date

Memory Spraying (Seaborn and Dullien BlackHat 2015)



- How do we get vulnerable memory to flip?
- Create many copies of vulnerable data – statistically, one will flip
- Linux kernel: replicate page tables
  - Change physical address



Split-based defences

- CAn’t Touch This (Brasser et al. USENIX Security 2017)
  - Split physical memory between user and kernel space.
  - Aggressor rows are not adjacent to page tables

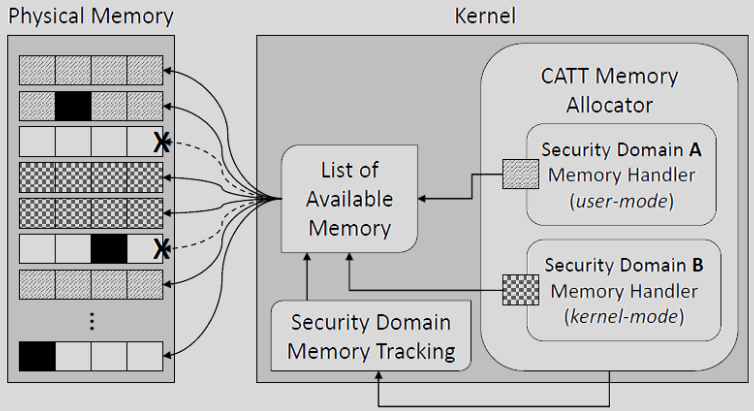


Figure 3: CATT constrains bit flips to the process’ security domain.

- CATTmew (Cheng et al. IEEE TDSC 2019)
  - Re-mapped kernel memory allows violation of these partitions

- PTHammer (Zhang et al. MICRO 2020)
  - Page table access can cause Rowhammer

Memory Massaging

- Flip Feng Shui (Razavi et al. USENIX Security 2016)
  - Exploit page deduplication
  - Attack a known page that contains an RSA public key

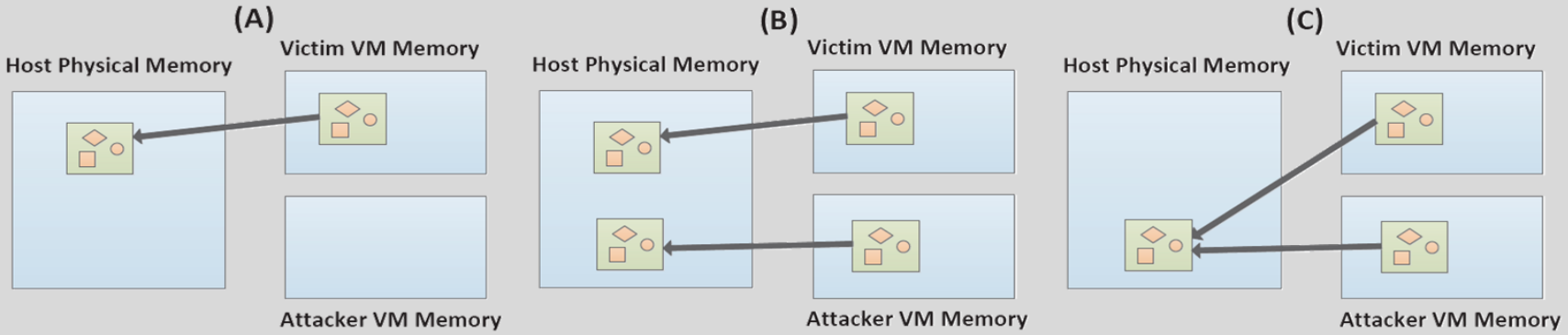


Figure 1: Memory deduplication can provide an attacker control over the layout of physical memory.

- Drammer (van der Veen et al. CCS 2016)
  - Exhausts physical memory
  - Attacks OpenSSL and apt-get

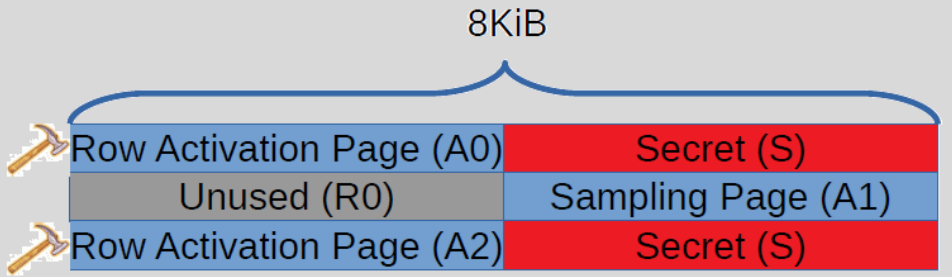
Overcoming countermeasures

- ECC (Cojocar et al. IEEE SP 2019)
  - ECC errors are observable through timing channels
  - Can combine three errors in a row to overcome ECC

- TRRespass (Frigo et al. IEEE SP 2020)
  - TRR – Target Row Refresh – a defence in DDR4
  - Special access patterns can overcome TRR
  - Extensions: SMASH (de Ridder et al. USENIX Security 2021), Blacksmith (Jattke et al. IEEE SP 2022)

Odd stuff

- SGX-Bomb (Jang et al. SysTex 2017)
  - DoS against SGX – flipping a bit stops the machine
- RAMBleed (Kwong et al. IEEE SP 2020)
  - Exploit striped pattern to leak data



(a) Double-sided Rambleed. Here, the sampling page (A1) is sandwiched between two copies of S.

- SpyHammer (Orosa et al. arXiv 2022)
  - Leak DRAM's temperature via Rowhammer
- HammerScope (Cohen et al. CCS 2022)
  - Measure DRAM voltage (activity) with Rowhammer

Evasys

http://tinyurl.com/yt2f4x96

Microarchitectural Attacks and Defenses