Thor's Hammer - Rowhammer Attack

Nicholas Quinlan, Nicholas Green, Cameron Gavin, and Dr. Dean Sullivan

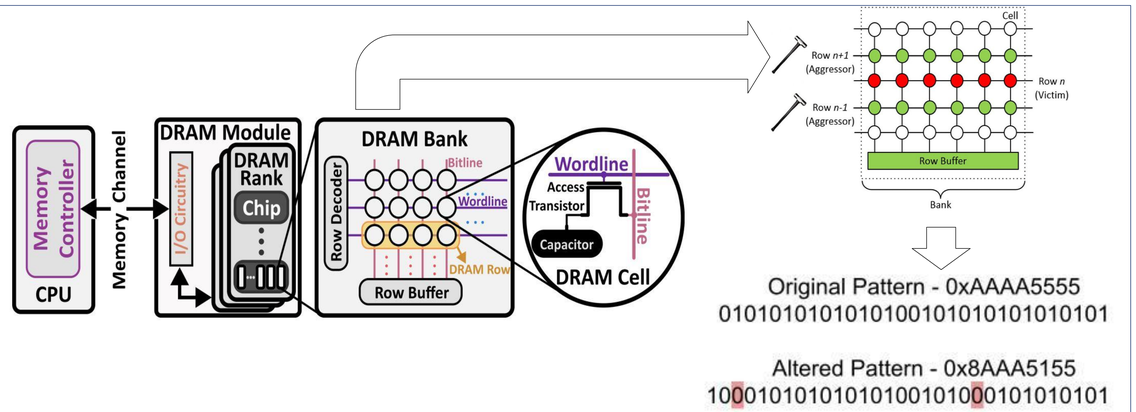
Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH 03824

Introduction

The purpose of this project is to demonstrate a rowhammer attack using a field programmable gate array (FPGA) interfaced with dynamic random-access memory (DRAM).

A **rowhammer** attack takes advantage of a vulnerability that is present in Double Data Rate (DDR) chips. By rapidly activating a physical memory row it is possible to cause **data corruption**.

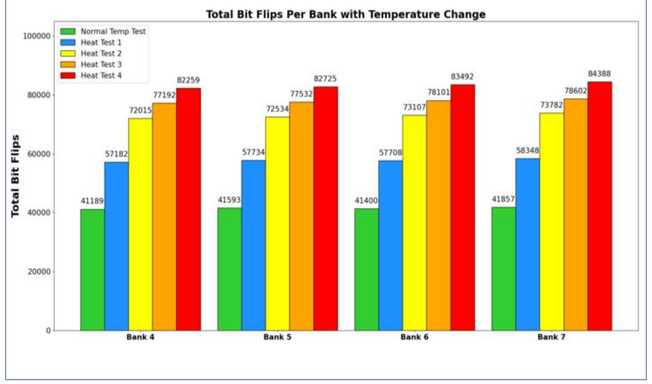
The Vulnerability in Double Data Rate Memory



Original Pattern - 0xAAAA5555
01010101010101001010101010101

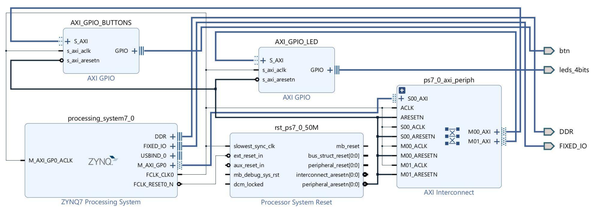
Altered Pattern - 0x8AAA5155
10001010101010100101000101010101

Heat Test Series Results

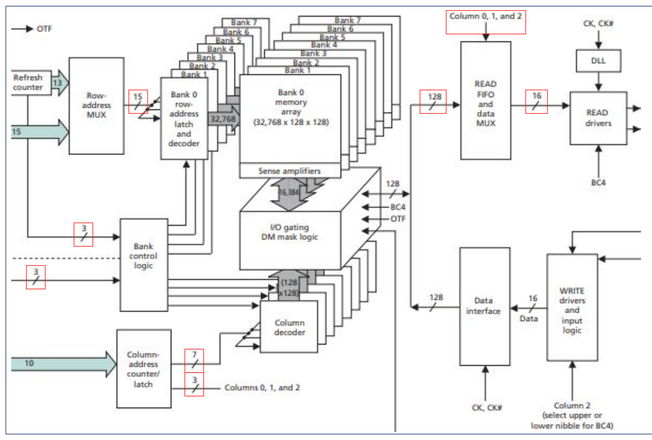


Methodology

- An FPGA was used because it creates an interface that provides precise control over the DRAM being tested.
- The **Zybo Z7 FPGA** has a processor which includes a central processing unit (CPU), and CPUs have memory controllers, which is a necessary component for this system.
- The Zybo has a 1 GB DDR3L with 32-bit bus @ 1066 MHz chip, which was used as the **victim DDR module**.



Attack Code Overview



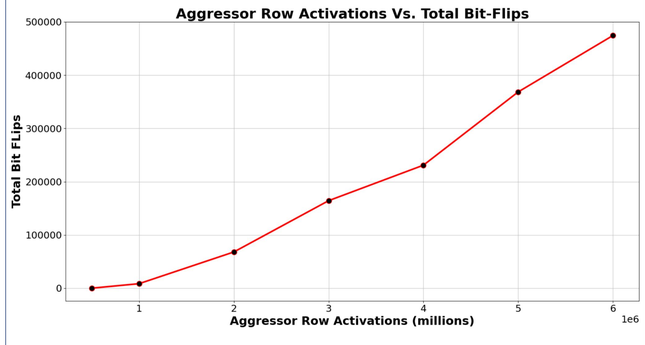

```
hammer_func(addr, words, pattern) {
        // initialize memory pattern to check later
        for each bank in DRAM
            for each column of the bank
                set bank, col = pattern
            end for
        end for

        // perform rowhammer attack and report bit flips
        for each bank in DRAM
            for HAMMER_ATTEMPTS
                activate row at victim_row - 1
                activate row at victim_row + 1
            end for
            for each column of the bank
                values = words at bank, col
                if read values do not equal initialized pattern
                    /* bitflip has been found */
                    ...
                end if
            end for
        end for
}
```

Conclusions

- DRAM is more vulnerable as the temperature increases, which can be caused by both malicious actors and normal operation.
- More activity on a row increases the chance of inducing bit flips.
- The circuit-level failure of modern DRAM memory compromises system security by breaking memory isolation.
- Although this vulnerability was discovered nearly a decade ago, this is still a relevant security threat, and can be paired with other stimuli to become even more effective and dangerous.

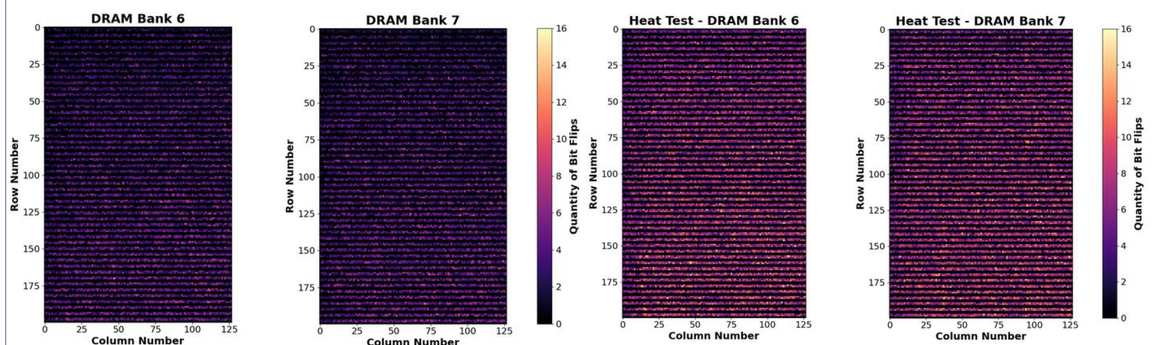
Attacks with Variable Activity



Rowhammer Attack with Variable Temperature

DDR Map - No Heat

DDR Map - Heated



Acknowledgements

The Resilient Architectures Laboratory supplied the necessary equipment to create this project.

References

Micron. (n.d.). Digi-key. 4Gb: x4, x8, x16 DDR3L SDRAM Description. Retrieved April 14, 2023, from https://media.digikey.com/pdf/Data%20Sheets/Micron%20Technology%20Inc%20PDFs/MT41K256M16_MT41K1G4_MT41K512M8_DS.pdf

Baidu Security X-Lab. (2019, April 25). PC security facing another "heavy hammer", Baidu Security discovers a new rowhammer attack. Retrieved April 14, 2023, from https://medium.com/baiduxlab/pc-security-facing-another-heavy-hammer-baidu-security-discovers-a-new-rowhammer-attack-be3dce8d1e92

Bobrowicz, Sam. "Zybo Z7." *Zybo Z7 - Digilent Reference*, https://digilent.com/reference/programmable-logic/zybo-z7/start.