GHammer: A GPGPU Rowhammering Attack

Georgios Anagnopoulos, Sotiris Ioannidis
Distributed Computing Systems Laboratory,
Institute of Computer Science, Forth Heraklion Greece
{ganagno, sotiris}@ics.forth.gr

Introduction

Rowhammer [1] [2] is a side effect in Dynamic Random-Access Memory (DRAM) that causes a charge leak to memory cells, which can eventually alter the contents of adjacent memory cells that were not even addressed. In this work, we examine the feasibility of the Rowhammer attack in GPGPU hardware architectures and provide insight regarding our results.

Methods

We use the *Double-Sided* pattern in order to access the pointers on the host memory from the GPU threads.

- **Sequential Hammer**: all threads access the same pointers concurrently in a linear sequence.
- **Strided Hammer**: threads access the locations based on their thread index (using the runtime environmental variables provided by the CUDA API).
- **Flushing Hammer**: half threads hammer the target pointers and the other half blindly read a preallocated dummy memory fragment.
- **Fenced Hammer**: kernels are fenced using the `__threadfence_system()` and synchronized with the host at every hammer iteration.

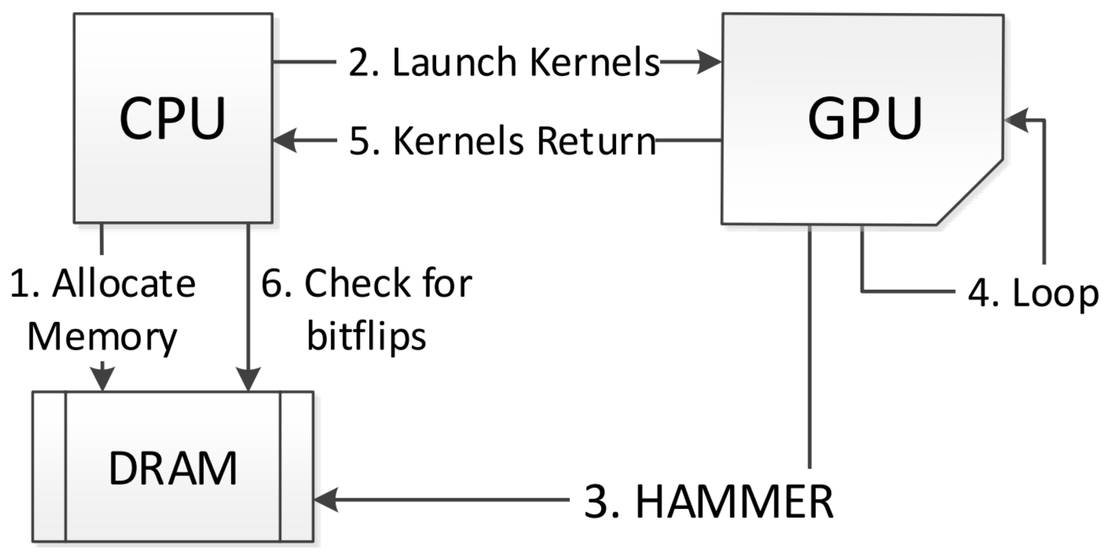

Figure 1: Workflow of the GPU rowhammering. After completion, the process repeats from step 2.

Results

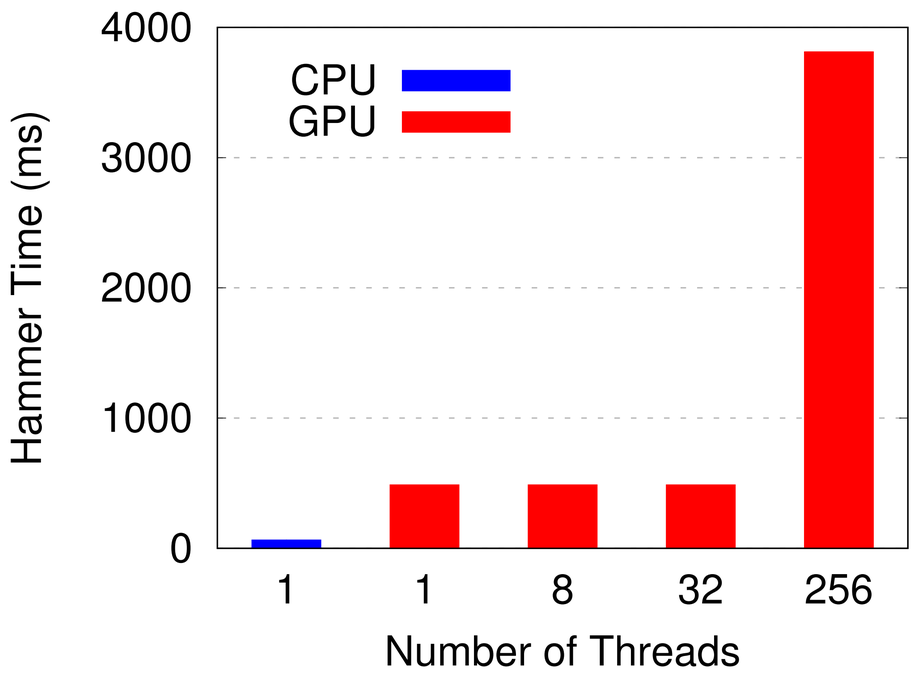

Figure 2: Sequential Hammer

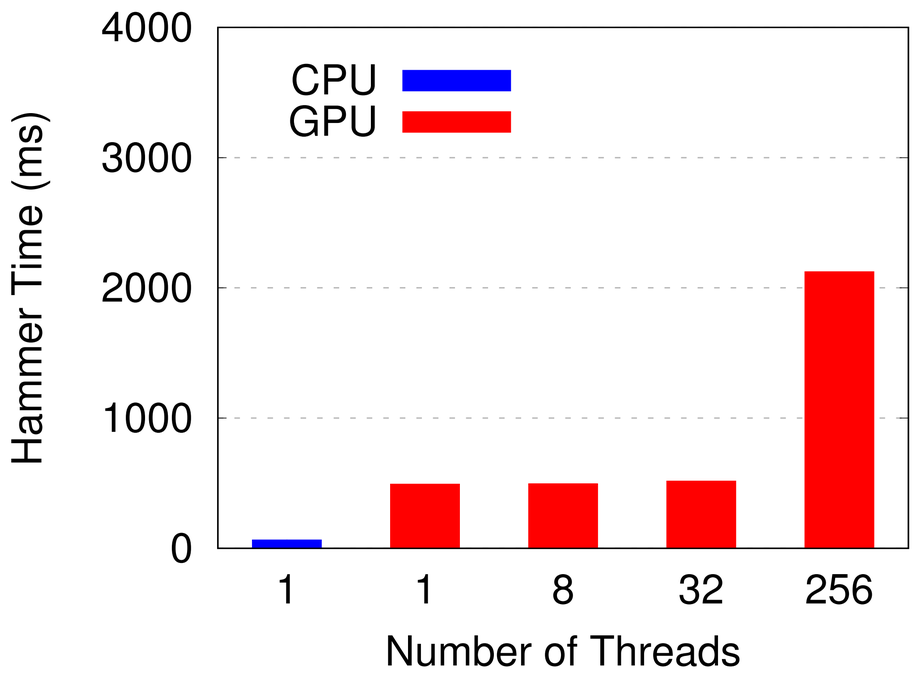

Figure 3: Strided Hammer

For the same amount of load operations (ie.1 GPU thread) the CPU execution is approximately 7.7x faster.

We observe that when using 256 threads,the execution is 1.79x faster compared to the *Sequential Hammering*.

Conclusions

- Our measurements indicate that no bitflip errors occur from the device to the host physical memory.
- Nvidia's current architecture prohibits device memory cache manipulation.
- The number of memory accesses between the host and the discrete GPGPU is capped to the PCI Express bandwidth.

References

[1] Yoongu Kim et al. Flipping bits without accessing them, 2014.

[2] Google Project Zero. Exploiting the dram rowhammer bug to gain kernel privileges, 2015.

Acknowledgements

This work was supported in part by the European commission through the project CIPSEC under Grant Agreement No. 700378