Poster: BLACKSMITH – Scalable Rowhammering in the Frequency Domain

Patrick Jattke
ETH Zurich
pjattke@ethz.ch

Victor van der Veen
Qualcomm Technologies Inc.
vvdveen@qualcomm.com

Pietro Frigo
VU Amsterdam
p.frigo@vu.nl

Stijn Gunter
ETH Zurich
sgunter@ethz.ch

Kaveh Razavi
ETH Zurich
kaveh@ethz.ch

***Abstract*—We present the new class of *non-uniform* Rowhammer access patterns that bypass undocumented, proprietary in-DRAM Target Row Refresh (TRR) while operating in a production setting. We show that these patterns trigger bit flips on *all* 40 DDR4 DRAM devices in our test pool. We make a key observation that all published Rowhammer access patterns always hammer "aggressor" rows *uniformly*. While uniform accesses maximize the number of aggressor activations, we find that in-DRAM TRR exploits this behavior to *catch* aggressor rows and refresh neighboring "victims" before they fail. There is no reason, however, to limit Rowhammer attacks to uniform access patterns: smaller technology nodes make underlying DRAM technologies more vulnerable, and significantly fewer accesses are nowadays required to trigger bit flips, making it interesting to investigate less predictable access patterns.**

The search space for non-uniform access patterns, however, is tremendous. We design experiments to explore this space with respect to the deployed mitigations, highlighting the importance of the *order*, *regularity*, and *intensity* of accessing aggressor rows in non-uniform access patterns. We show how randomizing parameters in the frequency domain captures these aspects and use this insight in the design of Blacksmith, a scalable Rowhammer fuzzer that generates access patterns that hammer aggressor rows with different *phases*, *frequencies*, and *amplitudes*. Blacksmith finds complex patterns that trigger Rowhammer bit flips on all 40 of our recently purchased DDR4 DIMMs, 2.6× more than state of the art, and generating on average 87× more bit flips. We also demonstrate the effectiveness of these patterns on Low Power DDR4X devices. Our extensive analysis using Blacksmith further provides new insights on the properties of currently deployed TRR mitigations. We conclude that after almost a decade of research and deployed in-DRAM mitigations, we are perhaps in a worse situation than when Rowhammer was first discovered.