

ERRATA

Sigries is not safe when transitioning from heavy mode back to light mode, despite the claim in the original paper. During this transition, Sigries is vulnerable for one refresh window.

This vulnerability exists because heavy mode does not necessarily sample every row that accumulates activations. Heavy mode is designed to sample aggressor rows whose number of activations approaches the Rowhammer threshold with very high probability. However, if a row receives fewer activations during one refresh window, it may remain unsampled. After the transition into light mode, this row may receive additional activations without being refreshed by the DRAM *and* still avoiding DRFM. The sum of the row activations in these two intervals could reach the Rowhammer threshold, yet no DRFM is issued.

We have identified two independent fixes for this vulnerability. The first requires a hardware logic change. When transitioning back to light mode, Sigries must run both heavy and light modes concurrently for one additional refresh window. Heavy mode is exited only after this additional window completes.

The second fix requires only a configuration change with no hardware changes. As currently implemented, Sigries's exposure window is twice as large as claimed in the original paper: less than two hours per year. This exposure can be reduced back to less than one hour per year by doubling the minimum duration of heavy mode. The minimum heavy-mode duration is a configuration parameter described in Section V-C.

The authors would like to thank Moin Qureshi from Georgia Tech for pointing out that the original claim was incorrect.