Reducing the Silicon Area Overhead of Counter-Based Rowhammer Mitigations
Loïc France, Florent Bruguier, David Novo, Maria Mushtaq, Pascal Benoit

To cite this version:
Loïc France, Florent Bruguier, David Novo, Maria Mushtaq, Pascal Benoit. Reducing the Silicon Area Overhead of Counter-Based Rowhammer Mitigations. 18th CryptArchi Workshop, May 2022, Porquerolles, France. lirmm-03738883

HAL Id: lirmm-03738883
https://hal-lirmm.ccsd.cnrs.fr/lirmm-03738883
Submitted on 26 Jul 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Reducing the Silicon Area Overhead of Counter-Based Rowhammer Mitigations

Loïc France, Florent Bruguier, David Novo, Maria Mushtaq, and Pascal Benoit

Abstract

Modern computer memories have shown to have reliability issues. The main memory is the target of a security threat called Rowhammer, which causes bit flips in adjacent victim cells of repeatedly activated aggressor rows [1]. This issue is becoming more important as DRAM technology scales down, with the required aggressor activations to corrupt a victim going from 130k for DDR3 [1] to around 10k for the most recent LPDDR4 memories [2]. Numerous countermeasures have been proposed, implemented either in software [3], [4] or in hardware [1], [5]–[10]. Among the hardware-based proposals, some rely on probability, randomly refreshing neighbors of activated rows [1], [5], [6], while others rely on row activation counters to detect aggressor rows before acting to prevent the corruption [7]–[9]. Counter-based hardware mitigation proposals offer the lowest performance overhead, as the mechanism only acts when an aggressor is detected and does not disturb the system for harmless applications. However, they require a lot of counters to track row activations. Considering the unrealistic amount of counters needed to track every row, those mitigation exploit different most-frequent-elements detection algorithms to reduce the number of counters needed while keeping a complete protection and a minimal false positive rate. Most of them offer a bank-level attack detection, with a separate set of counters for each bank. In this talk, We will show you that by changing the counting granularity from bank-level to rank-level, we can further reduce the total required number for counters from 20% for DDR3 to 70% for DDR5, thus reducing the silicon area and energy overheads of such mitigations.

Index Terms

Security, Rowhammer, DRAM.

REFERENCES