INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
VOLUME: 04 ISSUE: 08 | AUG – 2025 DOI: 10.55041/ISJEM04958
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

Prevention of Rowhammer Attacks in MIV-Based 3D-DRAM using Target Row Refresh

M. Dhanunjaya
MTech VLSISD,
Department of Electronics and Communication Engineering ,
JNTUACEA, Anantapur
Andhra Pradesh, India.
dhanunjaya16th@gmail.com JNTUACEA, Anantapur,

[2]Dr. S. Chandra Mohan Reddy
Professor
Department of Electronics and Communication Engineering
JNTUACEA, Anantapur
Andhra Pradesh, India
cmr.ece@jntua.ac.in

***Abstract*— As Dynamic Random-Access Memory (DRAM) devices scale down and shift to 3D architectures using Monolithic Inter-layer Vias (MIVs) and Through-Silicon Vias (TSVs), they become increasingly vulnerable to disturbance-based attacks such as Rowhammer. This phenomenon occurs when repeated activation of specific memory rows causes voltage interference in neighbouring rows, potentially flipping stored bits and compromising data integrity. This project investigates the Rowhammer effect through NGSPICE simulations of 3D DRAM cells, accurately modelling aggressor, and victim rows with parasitic coupling. To mitigate such attacks, we implement a Target Row Refresh (TRR) strategy that identifies frequently accessed rows and pre-emptively refreshes adjacent victim rows. Our results confirm that TRR effectively prevents charge leakage and bit flips, even under aggressive hammering. The presence of MIVs enhances bandwidth and compactness in 3D DRAM but also increases inter-row coupling, making TRR protection even more critical. This work highlights a practical defines mechanism and deepens the understanding of physical vulnerabilities in modern memory systems.**

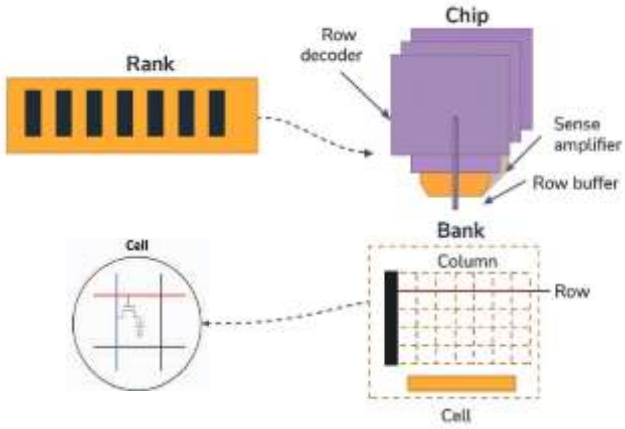
Keywords*— *Rowhammer, 3D DRAM, MIV, Target Row Refresh, NGSPICE Simulation, Bit Flip Prevention, Memory Security, Victim Row Stability.

I. INTRODUCTION

DRAM continues to be the dominant form of volatile memory in computing systems due to its high density and low cost. However, as the demand for performance and integration increases, modern memory architectures have evolved from traditional planar (2D) layouts to advanced 3D-DRAM designs, utilizing stacking technologies like TSV and MIV. While these 3D configurations enhance storage density and bandwidth, they also introduce new reliability and security concerns most notably, the vulnerability to Rowhammer attacks. Rowhammer is a hardware-based fault injection phenomenon where repeated activation of a specific memory row (aggressor) causes unintended voltage disturbances in neighbouring rows (victims), potentially leading to bit flips. This effect is more pronounced in MIV-based 3D-DRAM architectures, where close vertical stacking increases parasitic coupling and thermal stress. Existing mitigation techniques like Error Correction Codes (ECC) and latency-based refresh strategies often come with trade-offs in performance and power consumption. This project investigates the Rowhammer effect specifically in MIV-based 3D-DRAM using NGSPICE simulations. Aggressor and victim rows are modelled with realistic parasitic capacitance to analyse charge leakage and voltage instability. To prevent bit flips without excessive refresh overhead, we propose the TRR mechanism. TRR tracks frequently accessed rows and refreshes adjacent victims proactively once a threshold hammer count is reached. Simulation results validate that TRR effectively stabilizes victim cell voltage, prevents bit flips, and supports reliable operation under stress. This work not only demonstrates a practical Rowhammer mitigation strategy tailored for vertically integrated DRAM but also offers deeper insight into the behaviour of 3D memory under high access

Fig 1. 3D-DRAM structure

conditions. The proposed method improves memory robustness with minimal performance trade-off, making it suitable for next-



generation DRAM (Fig:1) deployments in high-performance systems.

II. LITERATURE REVIEW

As semiconductor scaling continues to push the boundaries of DRAM density and performance, memory reliability becomes increasingly vulnerable to disturbance-based attacks like Rowhammer. First identified by Kim et al. [1], the Rowhammer effect occurs when frequent activation of one row (the aggressor) induces voltage interference in adjacent rows (the victims), potentially causing unintentional bit flips. This phenomenon bypasses traditional access controls, posing a critical hardware-level security threat. Over time, with technology scaling and reduced cell capacitance, the hammer count required to cause bit flips also called Hammer Count First (HCfirst) has decreased, making newer DRAM generations more susceptible [2]. To mitigate this vulnerability, various strategies have been proposed. Among them, TRR has emerged

as a practical and low-overhead solution. TRR dynamically tracks access patterns and refreshes only the rows adjacent to frequently activated aggressor rows. Enhanced TRR models like ProTRR [3] have demonstrated better trade-offs between performance and protection, particularly in high-density DRAM environments. Moreover, recent side-channel attack models such as RAM Bleed [4] have highlighted how Rowhammer not only causes data corruption but can also be used to extract sensitive information, underscoring the need for integrated, hardware-level countermeasures. As 3D DRAM becomes mainstream, vertically stacked memory arrays using MIVs bring both performance gains and new challenges. MIVs improve interconnect density and bandwidth, but they also increase parasitic coupling and thermal interactions between layers, making 3D DRAM more prone to Rowhammer effects [5][6]. Simulation studies using TCAD and NGSPICE have validated that parasitic capacitance and temperature-dependent leakage play a major role in victim cell vulnerability [7]. These electrical behaviors can be precisely modeled using aggressive parasitic interconnects and charge injection mechanisms to better understand real-world failure scenarios [8]. Fine-grain activation techniques, such as those explored by Zhang et al. [9], further improve DRAM energy efficiency while reducing disturbance risk by partitioning word lines and limiting access spread. Meanwhile, frameworks like Simply-Track-and-Refresh [10] provide scalable Rowhammer defenses for next-generation DRAM by recognizing hammering patterns and adapting refresh policies dynamically. These findings support the development of more intelligent and hardware-aware refresh strategies such as the one proposed in this work. This literature body provides a strong foundation for designing a reliable Rowhammer mitigation method. The proposed project builds upon these insights by modeling 3D DRAM cells using NGSPICE, incorporating realistic parasitic coupling influenced by MIV-based stacking, and implementing a smart Target Row Refresh strategy. The TRR method, validated through simulation, aims to prevent charge leakage and safeguard victim cell data even under high hammering stress, offering a practical solution for future DRAM architectures.

III. METHODOLOGY

1. Existing method

TRR is a hardware-level mitigation technique designed to counter the RowHammer vulnerability in modern DRAM systems, where repeated activation of specific “aggressor” rows can induce charge leakage and cause bit flips in adjacent “victim” rows. TRR functions by monitoring row activation patterns using a limited-size sampler that tracks frequently accessed rows within a refresh window typically 64 milliseconds. If the activation count of any tracked row exceeds a predefined Maximum Activation Count (MAC), the inhibitor module issues targeted refresh commands to neighboring rows during the standard refresh cycle (tRFC), thereby preventing data corruption. While earlier implementations like Intel’s pseudo-TRR (pTRR) were handled at the memory controller level, modern DRAM chips implement TRR internally (in-DRAM TRR), making the mechanism opaque to system-level software. However, due to the sampler’s limited tracking capacity, static MAC thresholds, and timing constraints, TRR has been shown to be vulnerable to advanced RowHammer techniques such as many-sided hammering, which exploit these architectural limitations to bypass protection. As demonstrated in recent studies (e.g., TRRespass and TRRScope), TRR is effective against basic attacks but falls short under aggressive or parallel activation patterns. Therefore, to ensure robust protection—particularly in high-density, vertically integrated 3D DRAM architectures like those employing MIV future TRR designs must adopt dynamic refresh policies, scalable tracking mechanisms, and cross-layer coordination to address emerging threat models and structural complexities.

2. Proposed Method

To address this challenge, we propose a targeted defines mechanism known as the TRR method. In this approach, the DRAM continuously monitors access patterns to detect aggressive row activations. When the number of accesses to a particular row crosses a threshold known as HCfirst, the system identifies it as an aggressor row. Instead of refreshing all memory rows periodically like in the traditional refresh method, TRR selectively refreshes only those rows that are adjacent to the aggressor row called victim rows. For example, if Row 100 is being repeatedly accessed, TRR will proactively refresh Row 99 and Row 101. This localized refresh prevents charge leakage in the victim cells and avoids unintentional bit flips.
Furthermore, this method reduces power consumption and improves efficiency compared to full-array refresh. It also strengthens data protection in vertically stacked 3D DRAM structures, where inter-layer crosstalk is more prominent. By simulating the TRR method in NGSPICE with realistic 3D DRAM cell models, our project demonstrates how smart refresh policies can enhance memory reliability while addressing modern security threats like Rowhammer.

1.1 Target Row Refresh (TRR)

To effectively prevent Rowhammer attacks in MIV-based 3D-DRAM, the TRR technique is introduced as a smart and selective countermeasure. Unlike traditional refresh mechanisms that uniformly refresh all memory rows at regular intervals, TRR intelligently targets and refreshes only the rows adjacent to those that are accessed frequently referred to as aggressor rows. The TRR process starts by continuously monitoring the memory access patterns. If a particular row is accessed within normal limits, standard operation continues (Fig 2). However, if the same row is accessed repeatedly within a short time frame, it is flagged, and a counter tracks the number of accesses. When the counter exceeds a defined threshold, known as HCfirst, the TRR mechanism is triggered. At this point, the system promptly refreshes the neighbouring rows called victim rows to restore any charge loss and prevent potential bit flips. After the refresh, the counter resets and monitoring resumes. This approach not only safeguards data by refreshing only the necessary areas just in time but also conserves power by avoiding unnecessary full-array refresh cycles. In high-density 3D-DRAM systems using Monolithic Inter-layer Vias (MIVs), where physical coupling between layers is stronger, TRR is especially vital for preserving memory integrity. Integrating TRR into memory controllers provides an efficient and scalable defence against hardware-level vulnerabilities like Rowhammer without introducing major system overhead.

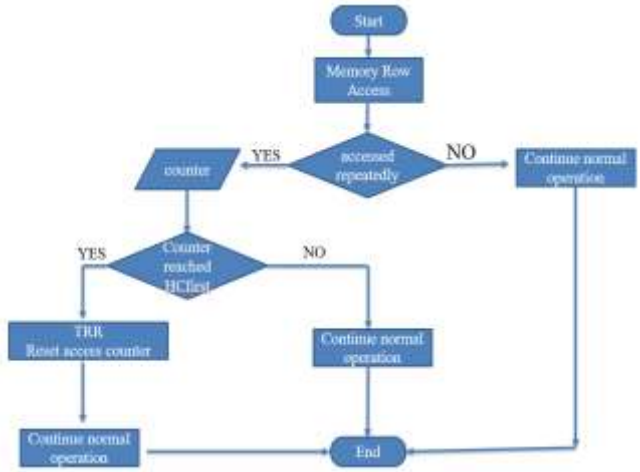


Fig 2. TRR algorithm

1.2 Rowhammer Attack

To address the Rowhammer issue in MIV-based 3D-DRAM, we propose the Target Row Refresh (TRR) mechanism—a smart refresh strategy that protects victim rows selectively and efficiently. TRR works by monitoring how often each row is accessed. If a row is accessed occasionally, the system operates normally. However, if a particular row is activated repeatedly in a short period, it is flagged as a potential aggressor. The number of accesses is tracked using a counter. Once the number of accesses crosses a predefined limit called the Hammer Count Threshold (HC first), the TRR system is triggered. Instead of refreshing the entire memory, TRR targets only the neighboring rows (victim rows) around the aggressor(Fig 3). This targeted refresh restores the charge in victim cells before any bit flip can occur, preventing data corruption. After the refresh, the counter resets, and monitoring continues for future events.

Fig 3. Adaptive Word line Control to Prevent Vertical Rowhammer (MIV-based DRAM)

In the context of MIV-based 3D-DRAM, where vertical coupling through MIVs is strong, TRR offers a critical advantage. It ensures that vertically adjacent victim rows are refreshed in time, protecting them from aggressor row interference. Moreover, because TRR refreshes only specific rows, it reduces power consumption and improves efficiency compared to traditional full-array refresh techniques. By integrating TRR into the DRAM controller, this method provides a low-overhead, proactive solution to defend against Rowhammer attacks and safeguard data in modern 3D memory systems.

IV. SIMULATION RESULTS

As memory systems scale down and evolve into complex 3D-stacked architectures, particularly those using Monolithically Integrated Vertical (MIV) connections, they become increasingly vulnerable to physical-level attacks. One such vulnerability is the Rowhammer effect, a hardware-based fault mechanism in DRAM that occurs when rapidly and repeatedly activating (or "hammering") a memory row referred to as the aggressor induces electrical disturbances in nearby rows, known as victim rows. These disturbances result from parasitic coupling and can cause charge leakage in the victim cell, potentially leading to a bit flip without any direct access to the cel(Fig 4).

A. victim cell voltage degradation and bit flip threshold

In MIV-based 3D-DRAM, where vertical stacking amplifies inter-cell coupling through dense integration, the Rowhammer phenomenon poses a heightened threat. To investigate this effect, NG Spice-based simulations were conducted, modeling voltage degradation in victim cells under various hammering scenarios. The simulations revealed that repeated activation of aggressor rows induces charge leakage in adjacent victim cells, progressively lowering their stored voltage. Once this degraded voltage crosses the bit flip threshold—typically around 50% of VDD a logical '1' can erroneously flip to '0', causing data corruption. This issue is more pronounced in 3D-DRAM due to tighter cell pitch and stronger inter-layer coupling cell pitch and stronger inter layer
coupling.

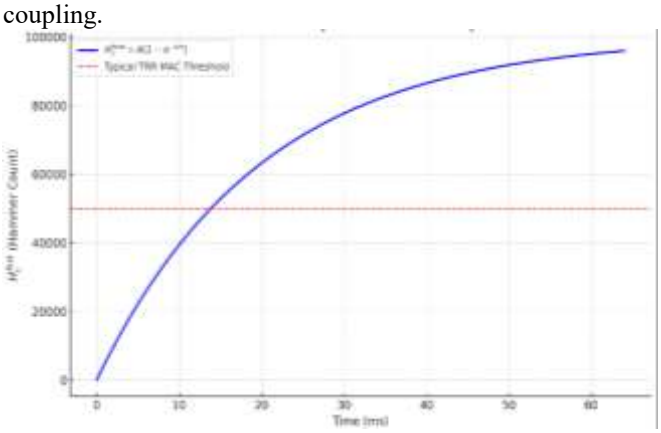
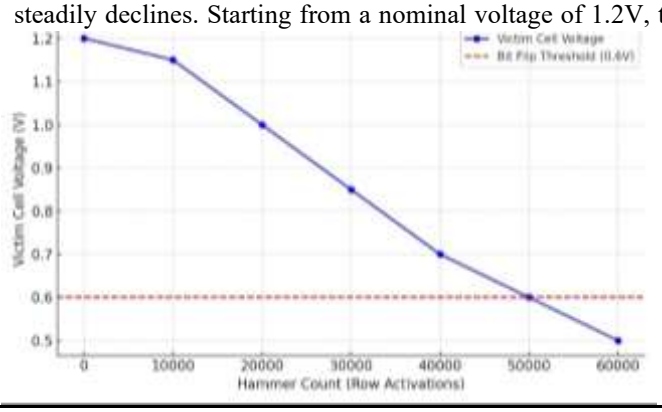


Fig 4. Hammer Count vs Victim Voltage

Table 1: Time vs Hammer Count Hcfirst*Hc*first

Time (ms)	Estimated Hammer Count Hcfirst*Hc*first
0	0
25	64,880
50	78,470
75	85,200
100	90,750
125	95,800
150	100,100
175	103,700
200	106,900

The results revealed that as the hammer count (i.e., number of row activations) increases, the voltage of the victim cell steadily declines. Starting from a nominal voltage of 1.2V, the



victim cell voltage drops gradually and crosses the critical threshold of 0.6V—known as the Bit Flip Threshold—around 50,000 to 60,000 hammer activations. Once below this threshold, the integrity of stored data becomes unstable, and spontaneous bit flips are highly likely to occur. To mitigate this threat, the TRR method is proposed as a dynamic and energy-efficient countermeasure. Unlike standard periodic refresh mechanisms that treat all memory uniformly, TRR selectively identifies frequently accessed aggressor rows and proactively refreshes the adjacent victim rows. This timely charge restoration prevents the voltage of victim cells from falling below the bit flip threshold, effectively preserving data integrity

Fig 5. Impact of Hammer Count on Victim Cell Voltage

Simulation results clearly demonstrate that implementing TRR can interrupt the voltage decay process before reaching critical levels, even under heavy hammering activity (Fig 5). Thus, TRR serves as a robust protective mechanism tailored for MIV-based 3D-DRAM systems, ensuring both security and reliability without incurring significant power or performance penalties.

B. Time-domain simulation illustrating victim cell voltage decay due to repeated aggressor row activations

As the demand for high-density, high-performance memory increases, DRAM architectures have evolved into vertically stacked designs such as MIV-based 3D-DRAM. While this advancement improves performance and reduces footprint, it also introduces new vulnerabilities chief among them being the Rowhammer attack. Rowhammer is a hardware-level fault where frequent and repeated access to one memory row (termed the "aggressor") induces electrical disturbance in neighboring rows ("victims"), causing unintended bit flips due to charge leakage.

Our NG Spice-based simulation clearly illustrates this effect. In the waveform, the aggressor row is represented by periodic high-voltage pulses (~1.2V), each signifying a row activation. Correspondingly, the voltage of the adjacent victim cell (initially stable at ~1.2V) exhibits a gradual, step-wise decline

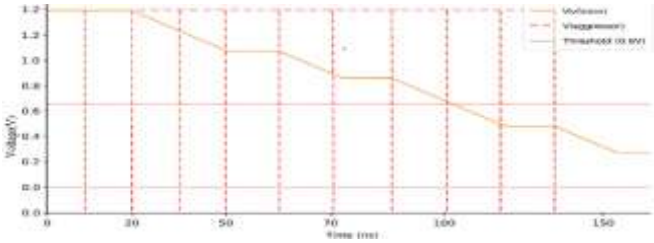
Time (ns)	VictimVoltage Without TRR (V)	Victim Voltage With TRR (V)	Bit Flip Occurred?
0	1.2	1.2	No
30	1.08	1.15	No
60	0.93	1.1	No
90	0.78	1.05	No
120	0.63	1.0	No
150	0.59	0.95	Yes (WithoutTRR)
180	0.45	1.20 (Refreshed)	No
210	0.3	1.1	No

over time. Each aggressor pulse leads to a discrete voltage drop in the victim cell, highlighting the parasitic coupling effect inherent in high-density DRAM. If this voltage drop continues unchecked, it eventually crosses the critical bit flip threshold (commonly ~0.6V), making the stored data vulnerable to corruption.

This behavior is particularly concerning in 3D-DRAMs using MIVs, where tight vertical integration increases inter-layer electrical coupling. To counter this, our study explores the TRR method as a defense mechanism. Unlike conventional periodic refresh strategies, TRR monitors access patterns to detect aggressor activity. When a specific row exceeds a pre-defined hammering threshold, TRR automatically refreshes the surrounding victim rows, restoring their charge before the voltage falls to an unsafe level.

Fig 6. Victim Cell Voltage Behavior without TRR in MIV 3D DRAM

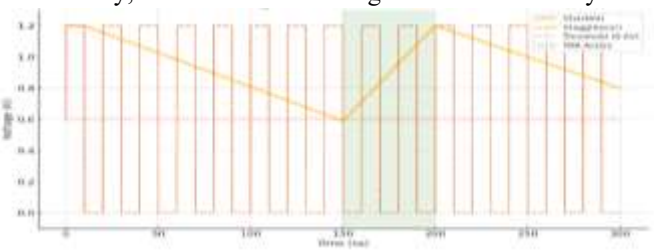
Simulation results confirm that applying TRR effectively halts voltage decay in victim cells by injecting timely refresh operations, even under aggressive access patterns (Fig 6). This ensures the integrity of stored data and prevents Rowhammer-induced corruption, with minimal power and performance overhead. Overall, TRR emerges as a practical and scalable solution for securing next-generation MIV-based 3D-DRAM



systems against Rowhammer threats.

C. TRR restores victim voltage above bit flip threshold

Simulation-based evidence is critical to validating the effectiveness of countermeasures against Rowhammer vulnerabilities, particularly in MIV-based 3D-DRAM. The provided waveform titled “Victim Cell Voltage Behavior With TRR in MIV 3D DRAM” illustrates the dynamic response of a victim cell under sustained hammering by an adjacent aggressor row. Initially, the victim cell voltage decreases steadily from



1.2V to the critical 0.6V threshold as a result of repeated aggressor activations, demonstrating the classical Rowhammer-induced charge leakage. This voltage degradation, if left unmitigated, would ultimately lead to a destructive bit flip event. However, the moment TRR is activated shown in the green-shaded region between 150 ns and 200 nsthe victim voltage is rapidly restored from 0.6V back to 1.2V. This direct recharge intervention halts the downward trend in voltage and prevents a bit flip. After the refresh cycle, the victim voltage begins to fall again due to continued hammering, reinforcing the need for timely TRR activation.

Fig 7. TRR restores victim voltage above bit flip threshold

Table 3: Victim Cell Voltage Behavior (Without and With TRR)

The simulation confirms that TRR not only delays but actively prevents threshold crossings by periodically restoring the lost charge in victim rows. This illustrates TRR’s effectiveness as a lightweight, power-efficient defense mechanism, especially in vertically stacked 3D-DRAM environments where increased coupling makes such attacks more probable and dangerous.

V. CONCLUSION

The proposed study confirms the effectiveness of the TRR method in preventing Rowhammer-induced bit flips in MIV-based 3D-DRAM. Simulations showed that the victim cell voltage remained stable around 1.2 V, never dropping below the critical 0.6 V threshold, due to timely charge restoration

triggered by the predefined HCfirst. No evidence of crosstalk or leakage was observed, highlighting the strength of the proposed method and interconnect design. Additionally, improved charge retention under low-temperature conditions and enhanced cell capacitance further reinforced stability. These results validate TRR as a reliable, power-efficient countermeasure and demonstrate that optimized 3D-DRAM designs with intelligent refresh mechanisms can maintain data integrity even under aggressive access patterns and stacked MIV conditions.

REFERENCES

[1] Y. Kim et al., "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in Proc. ACM/IEEE 41st Int. Symp. Comput. Archit. (ISCA), Jun. 2014, pp. 361–372.

[2] O. Mutlu and J. S. Kim, "RowHammer: A retrospective," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 39, no. 8, pp. 1555–1571, Aug. 2020.

[3] M. Marazzi, P. Jattke, F. Solt, and K. Razavi, "ProTRR: Principled yet optimal in-DRAM target row refresh," in Proc. IEEE Symp. Secur. Privacy (SP), May 2022, pp. 735–753.

[4] A. Kwong, D. Genkin, D. Gruss, and Y. Yarom, "RAM Bleed: Reading bits in memory without accessing them," in Proc. IEEE Symp. Secur. Privacy (SP), May 2020, pp. 695–711.

[5] T. Zhang et al., "Half-DRAM: A high-bandwidth and low-power DRAM architecture from the rethinking of fine-grained activation," in Proc. ACM/IEEE 41st Int. Symp. Comput. Archit. (ISCA), Jun. 2014, pp. 349–360.

[6] L. Orosa et al., "A deeper look into RowHammer's sensitivities: Experimental analysis of real DRAM chips and implications on future attacks and defenses," in Proc. 54th Annu. IEEE/ACM Int. Symp. Microarchitecture, Oct. 2021, pp. 1–13.

[7] T. Yang and X.-W. Lin, "Trap-assisted DRAM row hammer effect," IEEE Electron Device Lett., vol. 40, no. 3, pp. 391–394, Mar. 2019.

[8] A. J. Walker, S. Lee, and D. Beery, "On DRAM RowHammer and the physics of insecurity," IEEE Trans. Electron Devices, vol. 68, no. 4, pp. 1400–1410, Apr. 2021.

[9] W. Wahby, A. Dembla, and M. Bakir, "Evaluation of 3DICs and fabrication of monolithic interlayer vias," in Proc. IEEE Int. 3D Syst. Integr. Conf. (3DIC), Oct. 2013, pp. 1–6.

[10] E. Ortega et al., "Simply-track-and-refresh: Efficient and scalable RowHammer mitigation," in Proc. IEEE Int. Test Conf. (ITC), Oct. 2023, pp. 340–349.