Late Breaking Results: Thermally Assisted RowPress-RowHammer Synergy for Cross-Row Bit Flips

Filip Roth Tronnes-Christensen[1], Ranyang Zhou[1], Gamana Aragonda[1], Abeer Matar A. Almalky[2], Mohaiminul Al Nahian[2], Adnan Siraj Rakin[2], Shaahin Angizi[1]
[1]New Jersey Institute of Technology, USA [2]State University of New York at Binghamton, USA
arakin@binghamton.edu, shaahin.angizi@njit.edu

***Abstract*—In this work, we shed light on a previously uncharacterized *thermal-assisted disturbance* vulnerability in modern DDR4 DRAM by exploiting the temperature sensitivity and dense cell layout of scaled memory devices, a phenomenon we call HeatHammer. HeatHammer operates by first *RowPressing* the near aggressor, keeping it activated long enough to raise its local temperature, delay refresh operations, and erode its electrical isolation, and then *RowHammering* the far aggressor to induce bit flips in the victim row. This thermally weakened state significantly amplifies disturbance propagation, closely resembling the Half-Double effect [1]. Elevated temperatures accelerate charge leakage, shrink retention time, and reduce sense margins, thereby enabling disturbance effects to traverse through the compromised near aggressor via capacitive coupling and charge sharing. We evaluate this vulnerability on DRAM chips from two leading DRAM manufacturers and demonstrate that HeatHammer can substantially degrade the effectiveness of existing mitigation mechanisms such as Target Row Refresh (TRR).**

I. Introduction

Modern DRAM is increasingly susceptible to disturbance-based faults, prompting vendors to deploy in-DRAM mitigation techniques such as *Target Row Refresh* (TRR) [2], which attempts to detect frequently activated "aggressor" rows and proactively refresh adjacent "victim" rows. However, TRR implementations are proprietary, heuristic-driven, and inconsistent across vendors, enabling attackers to bypass them using carefully crafted access patterns. *RowHammer* [3] exploits rapid, repeated activation, precharge cycles on aggressor rows to induce charge leakage and bit flips in nearby cells through electrical interference. Evolving variants, including double-sided, many-sided, and frequency-shifting hammering, demonstrate that TRR alone provides incomplete protection. Recently, researchers identified *RowPress* [4], a complementary disturbance mechanism in which an attacker holds a row open for extended durations (i.e., long `tRAS`), creating quasi-static electric field stress that leaks charge into adjacent rows without requiring high-frequency activations. RowPress is especially challenging for TRR to detect because TRR focuses primarily on activation counts rather than prolonged row-open times [5]. Environmental conditions further exacerbate these vulnerabilities. Elevated temperature accelerates charge leakage, reduces DRAM cell retention time, and lowers the activation/press-duration threshold required to induce bit flips, thereby amplifying the effectiveness of both RowHammer and RowPress attacks. As a result, disturbance errors persist as a fundamental technology-scaling challenge, even in modern DDR4/DDR5 devices equipped with TRR.

While a combined RowHammer and RowPress attack has already been examined by Luo et al. [6], our work investigates a distinctly different activation pattern inspired by Google's Half-Double study [1], focusing on a different inherent weakness in DRAM. We show that combining the two disturbance phenomena affects not only the bit flip rate but also the distance across which flips can propagate.

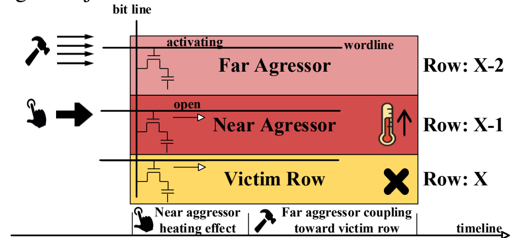

Fig. 1. HeatHammer exploit.

II. HeatHammer

The HeatHammer exploit exposes an intrinsic thermal-assisted disturbance vulnerability in certain DDR4 DRAM modules. The tightly packed geometry of scaled memory arrays accelerates local temperature buildup, which, akin to the *Half-Double* effect [1], enables disturbance-induced bit flips to propagate across multiple rows. Using a simple interleaved access pattern shown in Fig. 1 (not previously explored in any prior work), HeatHammer first RowPresses the near aggressor (row X-1), and subsequently RowHammers the far aggressor (row X-2), ultimately inducing bit flips in the victim row (row X). RowPressing keeps the near aggressor open for an extended duration, raising its local temperature, delaying scheduled refreshes, and accelerating charge decay. This thermally weakened near aggressor provides reduced electrical isolation for the victim row. Elevated DRAM temperature further exacerbates this condition by accelerating capacitor leakage, shortening retention time, reducing sense-amplifier margins, and shrinking available refresh slack. Under these circumstances, the subsequent RowHammering of the far aggressor can more easily disturb the victim row, with disturbance effects propagating through the compromised near aggressor via capacitive coupling, charge leakage, and charge sharing.

Threat Model and Framework. Our threat model considers modern DDR4 DRAM operating in thermally stressed environments where sustained activation patterns, AI-centric workloads, and dense system integration cause operating temperatures to rise and remain elevated. As DRAM scales, reduced cell capacitance, lower supply voltage, and diminished noise margins increase susceptibility to disturbance effects such as RowHammer and RowPress, while high temperature further accelerates charge leakage and retention loss, shrinking the timing slack available for internal refresh operations. Under these conditions, vendor mitigation mechanisms such as TRR, whose proprietary heuristics primarily rely on activation-count

978-3-9826741-1-7/DATE26/© 2026 EDAA

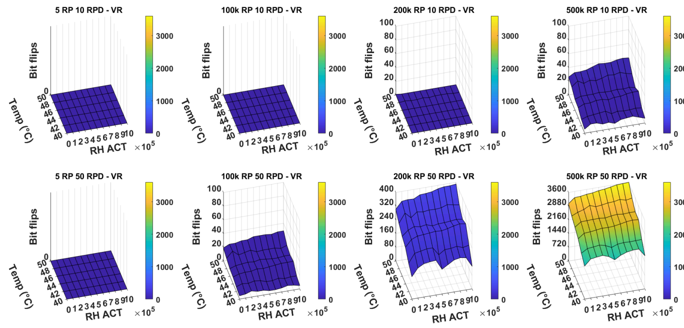

Fig. 2. Experimental results of Samsung chip.

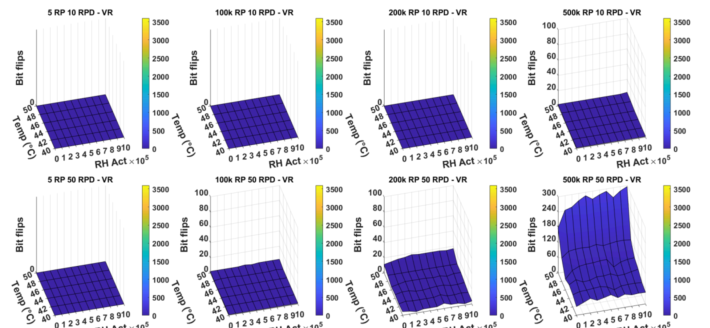

Fig. 3. Experimental results of NEMIX chip.

thresholds, become increasingly fragile and may be bypassed or overloaded when temperature rises, even on devices claimed to be RowHammer-resistant [2], [7]. To rigorously study this vulnerability, we employ a controlled disturbance-testing framework that provides fine-grained manipulation of activation sequences, extended row-open durations, refresh interactions, and environmental conditions on commodity DRAM modules. Each experiment is conducted under stable, precisely regulated temperature settings [4], [8], and memory is initialized with fixed data patterns selected to isolate disturbance-induced behavior. HeatHammer is evaluated across a broad space of RowHammer, RowPress, and temperature configurations [9], with repeated parameter sweeps ensuring statistical consistency and revealing temperature-dependent disturbance trends.

III. Evaluation & Analysis

Framework Setup & Testing Infrastructure. We evaluate HeatHammer using a modified version of DRAM-Bender [10], transforming it into a versatile FPGA-driven DRAM disturbance exploration platform for DDR4 with an in-DRAM compiler API running on the host machine. Our testing infrastructure uses the Alveo U200 Data Center Accelerator Card, which directly interfaces with DDR4 modules and executes HeatHammer by issuing DDR4 command sequences generated on the host. To ensure precise thermal control and reproducibility, all experiments are performed with temperature regulated to within $\pm 0.5°C$ of the target value using an INKBIRDPLUS 1800W temperature controller.

Minimizing Interference. Before performing the attack, DRAM refresh [11] and rank-level ECC are disabled to eliminate masking effects and isolate disturbance-induced behavior. However, proprietary in-DRAM mitigation mechanisms, including TRR [2], [12], remain enabled, allowing us to evaluate HeatHammer under realistic protection settings.

Chips Tested. To concisely characterize HeatHammer's impact while covering architectural diversity, experiments are conducted on two DDR4 devices selected from a large pool of modules: a 16 GB NEMIX 2R×4 RDIMM and a 16 GB Samsung 2R×8 UDIMM.

Experiment Configuration. Each experiment is repeated across multiple RowPress, RowHammer, and temperature configurations. For each iteration seen in Fig. 2 and Fig. 3, a unique combination of RowPress duration (RP) and RowPress loop count (RPD) is used. At the beginning of every run, memory is initialized with a fixed data pattern: the victim row is set to all 1's (0xFF) and the aggressor rows to all 0's (0x00). This configuration emphasizes faults in true-cells, which predominantly manifest as $1 \rightarrow 0$ flips under disturbance-induced charge leakage.

Results & Observations. Our results show substantial variation in vulnerability across both vendors and module types, with the Samsung UDIMM exhibiting generally higher susceptibility. As illustrated in Fig. 2, under the "500 RP 50 RPD" RowPress configuration, row-traversing bit flips increase as the number of RowHammer activations grows from zero to 1M, and intensify further with rising temperature. The NEMIX RDIMM displays similar qualitative behavior (Fig. 3), though with lower flip counts and a noticeably sharper temperature dependence, reinforcing the dominant role of thermal stress in amplifying HeatHammer. Importantly, the occurrence of row-traversing bit flips is not dictated by temperature alone; instead, it emerges from the interplay between RowPress-induced weakening of intermediate rows and subsequent RowHammer-induced disturbances on far aggressors. This strong coupling between the two mechanisms highlights the critical role of thermally assisted multi-stage disturbance propagation in modern DRAM.

Across both the tested modules, temperature emerges as the dominant factor driving bit flip growth, but with a clear dependence on the RowHammer configuration. This temperature-related behavior aligns with the findings of Luo et al. [4], who demonstrated and observed that the activation count required to induce RowPress bit flips decreases exponentially as temperature increases. The magnitude of this effect is particularly evident in the maximum edge-case results of the NEMIX module, where the bit flip count increases by more than a factor of five as the temperature rises.

Obs. Row-traversing bit flip counts rise with temperature and scale with both RowHammer and RowPress intensity, indicating a strong interdependence among the three factors.

IV. Conclusion

This work identifies a thermal-assisted disturbance weakness in modern DDR4 DRAM and shows that combining RowPress-induced heating with RowHammer interference can induce cross-row bit flips even in TRR-protected devices. HeatHammer requires only simple access patterns, yet its effectiveness grows sharply with temperature, highlighting a strong synergy between thermal stress, RowPress, and RowHammer activity. Experiments across two vendors confirm that elevated temperature significantly weakens intermediate rows, enabling disturbance propagation beyond adjacent boundaries.

Acknowledgments

This work is supported in part by the National Science Foundation (NSF) under grant no. 2216772 and 2228028.

References

[1] A. Kogler, J. Juffinger, S. Qazi, Y. Kim, M. Lipp, N. Boichat, E. Shiu, M. Nissler, and D. Gruss, "Half-double: Hammering from the next row over," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security '22)*. Boston, MA, USA: USENIX Association, 2022, pp. 3807–3824. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/kogler-half-double

[2] X. Zhao, Q. Sun, T. Jiang, Z. Li, Y. Zhang, and S. Ju, "Lightweight rowhammer attacks on mobile devices," 2020. [Online]. Available: https://arxiv.org/abs/2004.01807

[3] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu, "Flipping bits in memory without accessing them: An experimental study of dram disturbance errors," *ACM SIGARCH Computer Architecture News*, vol. 42, no. 3, pp. 361–372, 2014.

[4] H. Luo, A. Olgun, A. G. Yağlıkçı, Y. C. Tuğrul, S. Rhyner, M. B. Cavlak, J. Lindegger, M. Sadrosadati, and O. Mutlu, "Rowpress: Amplifying read disturbance in modern dram chips," in *Proceedings of the 50th Annual International Symposium on Computer Architecture*, 2023, pp. 1–18.

[5] R. Zhou, J. T. Liu, S. Ahmed, S. Angizi, and A. S. Rakin, "Compromising the intelligence of modern dnns: On the effectiveness of targeted rowpress," in *2025 Design, Automation & Test in Europe Conference (DATE)*. IEEE, 2025, pp. 1–7.

[6] H. Luo, I. E. Yüksel, A. Olgun, A. G. Yağlıkçı, M. Sadrosadati, and O. Mutlu, "An experimental characterization of combined rowhammer and rowpress read disturbance in modern dram chips," in *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*. IEEE, 2024, pp. 6–11.

[7] P. Jattke, V. van der Veen, P. Frigo, S. Gunter, and K. Razavi, "BLACKSMITH: Scalable rowhammering in the frequency domain," in *2022 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, 2022, pp. 716–734. [Online]. Available: https://ieeexplore.ieee.org/document/9833772

[8] O. Mutlu and J. S. Kim, "Rowhammer: A retrospective," *IEEE TCAD*, vol. 39, 2019.

[9] L. Orosa, U. Rührmair, A. G. Yaglikci, H. Luo, A. Olgun, P. Jattke, M. Patel, J. Kim, K. Razavi, and O. Mutlu, "Spyhammer: Understanding and exploiting rowhammer under fine-grained temperature variations," *arXiv preprint*, 2022. [Online]. Available: https://arxiv.org/abs/2210.04084

[10] A. Olgun, H. Hassan, A. G. Yağlıkçı, Y. C. Tuğrul, L. Orosa, H. Luo, M. Patel, O. Ergin, and O. Mutlu, "Dram bender: An extensible and versatile fpga-based infrastructure to easily test state-of-the-art dram chips," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 42, no. 12, pp. 5098–5112, 2023.

[11] *JESD79-4D: DDR4 SDRAM Standard*, JEDEC Solid State Technology Association Std., Jul. 2021, dDR4 SDRAM (2 Gb through 16 Gb, x4/x8/x16) – Revision 4D. [Online]. Available: https://store.accuristech.com/standards/jedec-jesd79-4d

[12] H. Hassan, Y. C. Tugrul, J. S. Kim, V. van der Veen, K. Razavi, and O. Mutlu, "Uncovering in-dram rowhammer protection mechanisms: A new methodology, custom rowhammer patterns, and implications," 2021. [Online]. Available: https://arxiv.org/abs/2110.10603