Flipping Bits in DRAM using Laser Induced Localized Heating

Saurav Mathur, Nirmit Jallawar, Swamit Tannu

University of Wisconsin-Madison

Abstract—This paper demonstrates an experimental testbed to inject precise faults in DRAM using an inexpensive and commercially available laser setup. We use a diode laser to heat the minuscule area on the DRAM chip package to create a local hot spot, which results in elevated temperatures that induce bit-flips without reading or writing the data to the memory. We test 30 DRAM chips manufactured by four vendors across three DDR generations. Our setup shows consistent and repeatable faults on all DRAM chips, which can help elucidate error mechanisms and enable novel fault-injection studies for DRAM memories.

1 Introduction

Historically, architects and system developers have trusted the resiliency of hardware and formulated the defenses assuming on-chip data is to a certain degree safe against selective perturbations. Unfortunately, this is no longer true. With rapidly degrading transistor reliability and sophisticated adversaries, hardware-focused cyber-attacks are rising, and many of the attacks can leverage physical and remote fault injection strategies. For example, recent demonstrations use glitching to break crypto-wallets [1]. With the increasing footprint of personal devices that carry sensitive information and perform critical tasks, we must broaden our understanding of physical attacks. To that end, we demonstrate an experimental setup that can selectively flip bits inside a DRAM chip without reading or writing data, instead by using a laser to heat the DRAM chip package. The high sensitivity of modern DRAMs to temperature changes results in an exponential increase in the leakage of charge as temperature rises, leading to retention errors. We exploit this effect to induce faults in the DRAM by using lasers. We use a laser beam to elevate the temperature of a small part of the DRAM chip package beyond the rated operating temperature. For our experiments, we use a high-power but inexpensive laser setup that is typically used for engraving and amateur laser cutting projects. Our experimental setup can demonstrate the following –

1) By shining a laser on the DRAM chip, we can cause local hot-spots on the package that can induce bit-flips in the memory.
2) Using a laser mounted on the CNC machine, we can move the laser precisely to induce faults on the different parts of the die.
3) The bit-flips are repeatable, i.e. two runs with identical incidence on the chip package produces almost identical errors.
4) We demonstrate controlled transient faults for DDR3, DDR4, LPDDR4 modules with both ARM and x86 architectures.

Why target DRAM? DRAMs are ubiquitous due to their high density and low costs. Unfortunately, aggressive scaling of DRAM technology that has enabled affordable memory capacity also causes significant system-level reliability and security challenges. For example, due to shrinking sizes, current DRAM cells are significantly more vulnerable and can have dramatically higher error rates compared to older generations. The reduction in DRAM cell size results in leaky capacitors that lead to reduced retention in DRAMs [6]. Furthermore, the shrinking of DRAM cells has also caused security vulnerabilities such as Row Hammer (RH), wherein repeated accesses of a physical memory location can flip bits in the neighboring memory locations without explicitly accessing the memory locations [2], [7]. Secure memory systems are essential to enable secure computer systems, and aggressive scaling of memory technology can introduce additional attack vectors. Studying how we can perturb the data in DRAM can provide us insights into unknown and unexplored attack vectors.

Fault Injection for DRAM. Previously demonstrated fault-injection methods that can be applied on DRAMs are - Rowhammer, Voltage Glitching, and Signal Injection, as shown in Table 1. It is possible to flip bits inside memory using the Rowhammer attack. However, fault injection with Rowhammer can be slow and non-deterministic. Furthermore, to inject faults using Rowhammer, we need to reverse engineer the row mappings and beat the state-of-the-art memory controller policies such as Targeted Row Refresh (TRR) designed specifically to mitigate the Rowhammer faults. Consequently, Rowhammer fault injection is not practical and may not be used across multiple systems as it is. On the other hand, perturbating bits in the Register File, SRAM, and Flash-based memories in a microcontroller using voltage glitching is a widely known technique, and recent demonstrations on SGX showcase how it can be used for modern server and desktop machines. However, injecting faults in DRAM by undervolting memory to induce precise faults can be non-trivial as memory controllers enforce strict signal and data integrity checks. The signal injection can be performed by connecting external hardware to the exposed DRAM bus used to send commands and read and write from DRAM. However, for this type fault injection is only possible when memory pins are exposed and accessible.

We focus on thermal fault injection. Our work is inspired by [8], which used a desk lamp to heat the DRAM chips to induce random faults in memory. However, faults induced by homogeneous heating in the DRAM chip are not controllable and precise. Instead, we use laser that can enable controlled fault injection. Furthermore, the laser-induced fault injection method can be used with any architecture and DDR generation to uncover vulnerabilities in DRAM memories.

Fault Injection Method	Fault Injection in DRAM	Limitation	Precision	Fault Injection Speed
Row Hammer [2]	Demonstrated	Obfuscated row mapping	Moderate	Slow
Voltage Glitching [3], [4]	Not demonstrated	Memory controller checks[1]	Low	Slow
Signal Injection [5]	Demonstrated	Intrusive and high overhead	Low	Unknown
This work	Demonstrated	Chip specific laser tune up	High	Fast

TABLE 1
Summary of Fault Injection Methods for DRAM

2 Laser-Based Fault Injection for DRAM

In this section, we will discuss the principle of laser-induced fault-injection, and the motivation for using it on DRAM chips.

2.1 DRAM Faults at Elevated Temperatures

DRAM cells are vulnerable to an increase in operating temperature(-40° to 100°). Prior work shows that an increase in operating temperature can significantly increase the error rate of DRAM [9]. In addition, recent studies show vulnerability to Row Hammer errors amplifies with increasing temperatures or within specific temperature ranges [10]. The probability of a DRAM cell failure increases with higher temperatures, especially for weaker memory cells prone to bit-flips due to fabrication defects. We leverage this phenomenon to inject faults by increasing the DRAM temperature.

2.2 Lasers for Inducing Bit-Flips in DRAM

The prior work on DRAM characterization focuses on understanding DRAM behavior within the specified operating temperature range. In this paper, we focus on using localized heating that selectively elevates the temperature of the minuscule area on the chip package beyond the operating temperature.

For performing fault injection, we shine a laser beam with 425nm wavelength on a DRAM chip. The laser emits monochromatic light which is focused using a lens to create a sharp spot on the chip package surface. The light incident on the chip is absorbed by the package surface, elevating the temperature in a small area. Typically, laser engravers/cutters utilize elevated temperatures to burn off a layer of surface material. By controlling the laser power and duration, we can control the temperature and area of the hot-spot.

2.3 Advantage of Laser-Induced Faults

Not all DRAM cells are created equal. DRAM cell retention has a large variance. On the DRAM die, there are weak memory cells that have significantly lower retention time and a higher chance of failure. On average, the retention time reduces with the increasing temperature due to increased charge leakage. We leverage this phenomenon to induce bit flips by locally heating the DRAM die using lasers.

Unlike injecting faults on the address or data bus, the laser-induced faults can be induced spatially over almost all the address space. Furthermore, using a laser, we can cause bit-flips with a significantly faster rate in the targeted area of the memory. As the faults are induced by heating the parts of the DRAM package beyond the operating temperatures, even the most conservative DRAM refresh strategies are not enough to prevent errors in the memory.

Moreover, the rate of induced faults does not depend on knowing the internals of DRAM memory. For example, for effective fault injection using a row-hammer, we need the physical row mapping to perform targeted hammering activation. Any changes incorporated by DRAM vendors to prevent memory errors using refresh strategies such as targeted row refresh (TRR) can reduce the effectiveness of the fault-injection methodology.

The elevated temperature of DRAM cells primarily drives our laser-induced fault injection, and it is independent of the architecture and memory controller design. In this paper, we show that with careful calibration, we can induce errors in all tested DDR3, DDR4, LPDDR4 DIMMs driven by ARM and x86 CPUs.

Laser-induced faults are tied to the physical location of cells. In our setup, we can move the laser head precisely in the XY plane, enabling the ability to print faults on the DRAM chip to potentially introduce arbitrary faults.

2.4 Key Hypotheses

In this paper, we test the following hypotheses using our experimental setup -

1) Diode laser can induce local hotspots on the DRAM chip, which result in localized bit-flips on the physical memory.
2) Laser-induced bit flips are repeatable as they exploit the physical characteristics of DRAM cells.
3) As modern DRAMs use true-cell and anti-cell encoding to avoid bias in DRAM errors, we hypothesize that our setup would be able to induce both $1 \longrightarrow 0$ and $0 \longrightarrow 1$ errors.
4) Rapid and localized heating can subvert the DRAM fail-safe such as thermal shutdown and adaptive refresh.

3 Experimental Setup and Methodology

In this section, we first summarize our experimental setup and then discuss the methodology used in our experiments.

3.1 Summary of Experimental Setup

Goal. The goal of our experimental setup is to induce precise bit flips by using local heating effects. We hypothesize that by creating hotspots on the DRAM package using a laser, we can cause significant charge leakage in the targeted DRAM cells, which can result in filliped bits. Figure 1(a) show an illustrative schematic of our experimental setup and Figure 1(b) is the picture taken during the experimental run.

3.2 Laser

To test our hypothesis, we select a laser with appropriate frequency, power, and spot size to induce errors. The frequency of the laser determines what fraction of the incident energy is absorbed by the package. The majority of the DRAM packages are built using epoxy resins that absorb light in the UV and visible range [11]. Through our experiments, we

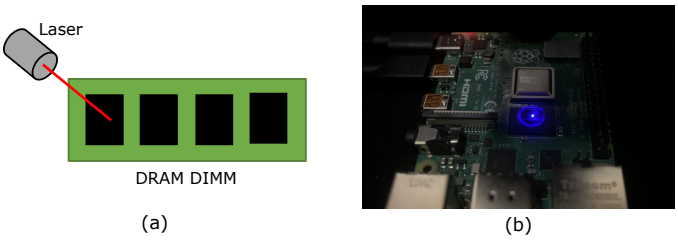

Fig. 1. (a) DRAM Testing setup schematic (b) Setup used to induce the faults experimentally on Raspberry-Pi4

determine that errors can be induced using a blue laser (425 nm) with power in the range of 4W - 5.5W. In addition, a highly focused laser spot of 0.12*0.15mm gives us precise control over heating a specific location on the chip.

3.3 Laser Engraver

We use the ORTUR Laser Master-2 Engraver [12], which is designed for amateur engraving and laser cutting projects. The ORTUR laser engraver uses the vertically mounted (Z-axis) laser head on the CNC machine, which can move the downward-pointing laser in the XY-plane with high precision. The mounted laser head has a beam of wavelength 425 nm and configurable power with a maximum of 5.5W. By enclosing the engraver, we create a safe Class IV laser that powers off when any unauthorized movement is detected.

3.4 Specification of DRAM Chips under Test

We use X86 and ARM-based systems for our evaluations and the DDR3, DDR4, and LPDDR4 DIMMs. Table 2 summarizes the specifications of DRAMs used in our evaluations. Note that all the DIMMs used in our evaluations are SO-DIMMs that are horizontally mounted, as our current setup uses a vertically mounted laser head. For DDR4 and DDR3 evaluations, we use Intel® CPUs with Haswell® and Kirbylake® microarchitecture, respectively, whereas we use Raspberry-Pi4 with ARM® architecture to test LPDDR4 chips.

Protocol	Number of Chips	Vendors	Chip Capacity
DDR4	16	A, B, C	512MB, 1GB, 2GB
DDR3	12	A, B, C, D	512MB, 1GB
LPDDR4	2	A	4GB

TABLE 2
Specifications of Test DRAM Chips

3.5 DRAM Testing Methodology

To test DRAM chips and log memory errors, we use Memtest86-Pro software [13]. Memtest-86 enables a standardized testing environment with tiny a memory footprint and deterministic memory mapping. For consistency, we need a memory testing framework that operates with a small memory footprint to avoid memory corruption and errors in the testing and logging sequence. For example, during high power testing, the number of errors can exceed more than hundreds of thousands, jeopardizing the consistency of test sequences on the conventional operating systems.

The laser beam is set to move in fixed patterns over the memory chip. While we shine the laser on the chip, the Memtest86 software runs in the background and helps us infer the faults. We vary the location of the laser on the chip to target different physical addresses. This helps us infer which locations on the chip are more vulnerable to errors. By varying the power and speed of the beam, we can increase/decrease the frequency of faults. Furthermore, by changing the time duration for which the laser is run, we can determine the amount of energy required for single/multi-bit faults.

We use a Bit Fade Test to infer the induced faults in memory. Using Memtest-86, we write the memory with either all 0s or all 1s. Once we write to the memory, we wait for a short duration (30 seconds). We then shine laser over the chip for 2 minutes with varying shapes, speed, and optical power across different runs. After waiting for a short duration (30 seconds), we read back the data present in memory, and log an error if it does not match the initially written data.

Moreover, we verify that our testing methodology does not cause any permanent damage to memory chips. Using our laser engraver, we shine laser across the entire chip on multiple SODIMMs for 10 minutes at the maximum power. We then stress test the SODIMM for multiple test cycles using the RAMCHECK LX module [14] and infer that no memory chips have any permanent damage.

4 Experimental Evaluations

This section will discuss the experimental evaluation to test key hypotheses and demonstrate the capabilities of laser-induced fault injection for DRAMs.

4.1 Experimentally Verifying Local Hotspots

Localized heating can cause rapid charge leakage in weak cells resulting in bit-flips. To test the local hotspot hypothesis, we design two experiments that quantify reproducibility and overlap in erroneous addresses. If we can induce the errors in the same set of addresses by repeatedly shining the laser on identical physical locations, we can show that the error mechanism is inherent to the physical memory cells and caused by local heating. To that end, we shine a laser on the DRAM chip package to draw a line, as shown in Figure 2 (a). In this experiment, first, we zero out the memory, and then incident the laser for 180 seconds on the DRAM package, and then we log errors. We repeat this several times with identical laser power and physical location. Figure 2 (b) show the total number of unique error addresses added every additional run. If the errors are repeatable, the number of unique addresses added per experiment would drop quickly with every experiment run. Our evaluations with LPDDR4 chips show that we can induce repeatable errors, as even with a large number of repetitions we do not observe additional unique addresses.

Moreover, we test if the overlapping and disjoint physical locations produce overlapping and disjoint errors, respectively. To that end, we draw a solid line as shown in Figure 2(a) and then a dashed line on the same physical location with identical laser power. The dashed and solid lines have overlapped and non-overlapped regions on the DRAM package. Figure 2(c) shows the total number of errors for solid and dashed lines. Furthermore, it shows an overlap of error addresses and disjoint error addresses between the solid and dashed line. We observe a near-complete overlap for errors produced during dashed and solid lines, almost all the errors observed for the dashed line experiments were observed during solid line experiments. Furthermore, we observed a disjoint set of errors that were present for the solid line but not for the dashed line.

1. Memory Controllers enforce signal integrity checks making under-volting practically challenging for DRAMs

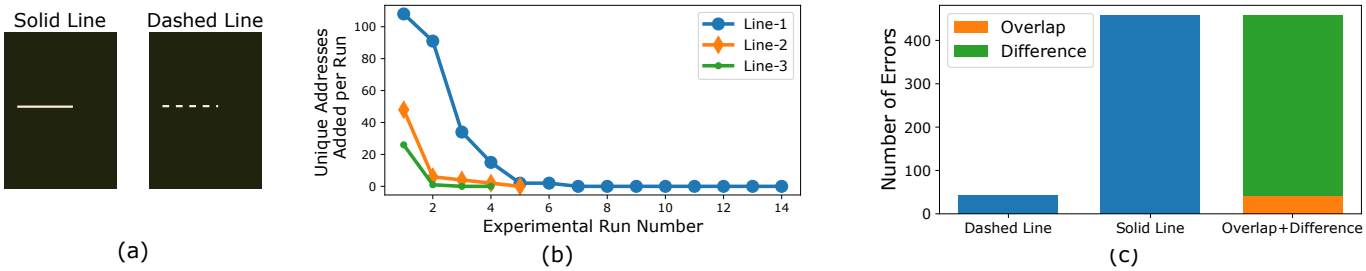

Fig. 2. (a) Illustrative example of lines sketched for repetition and overlap experiments (b) Number of unique errors added for every new experimental run on LPDDR4 chips on three locations (c) Total number of errors logged after sketching a solid and dashed line on DDR3 chip.

4.2 Nature of Bitflips

Single vs. Multi-bit Errors. Our experimental evaluation shows that for the majority of the induced faults, we only flip one bit per four-byte data word. However, by using the laser at its peak power and exposing the package for a longer duration, it is possible to induce multi-bit faults in DRAM chips. Note that multi-bit faults per four-byte data are rare for DDR3 and DDR4 DIMMs that use eight chips/rank. As shown in figure 3 the majority are single-bit faults, whereas only a tiny fraction of faults we observe have multiple bit flips. In contrast, for LPDDR4, about 11% of the errors are multi-bit errors. The multi-bit faults result from the DRAM configuration used for the Rasberry-Pi setup, which uses only one DRAM chip.

Direction of Bit flip Errors. To test if there is any data-dependent bias for laser-induced faults, we test the DRAM chips by writing both all one and all zero data before inducing errors. We observe that we can cause bi-directional faults ($0 \longrightarrow 1$ and $1 \longrightarrow 0$) on our setup. Figure 4 shows that both types of faults are possible and equally likely. We observe that for DDR4 and LPDDR4 there is a wide gap. However, we believe it is an artifact of the test sequence that we use in our experiments, and it can be augmented to avoid such bias.

For an exact physical location, we observe no overlap between $0 \longrightarrow 1$ and $1 \longrightarrow 0$ errors as the cells that fail to retain ones are different than cells that fail to retain zeros. This behavior is not surprising as modern DRAMs use true-cell and anti-cell encoding to mitigate retention errors. We believe, using our experimental setup, we can categorize DRAM cells as the true-cells and the anti-cells.

4.3 Statistics of Laser-Induced Faults

The number of bit-flips primarily depends on the total incident energy, a product of laser power, and time of incidence. We can increase the peak and the average temperature by increasing the laser power. In our experimental setup, we control the duty cycle of the laser using pulse width modulation. As shown in Figure 5(a), the number of errors grows exponentially with incident power. We observe a monotonic increase in the total errors with increasing incident power for most DRAM devices that we test. However, the absolute number of errors depends on the physical location, type of chip, and many other device-dependent factors. For example, Table 3 shows that for identical laser power, the number of errors can change dramatically from one location to another.

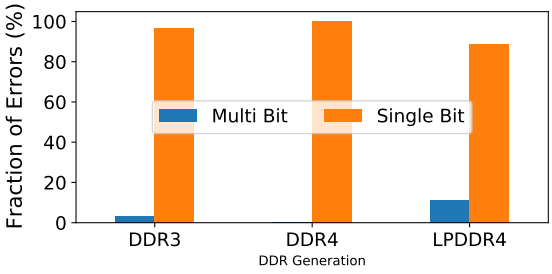

Fig. 3. Fraction of Single and Multi-bit errors for the tested DRAM Chips.

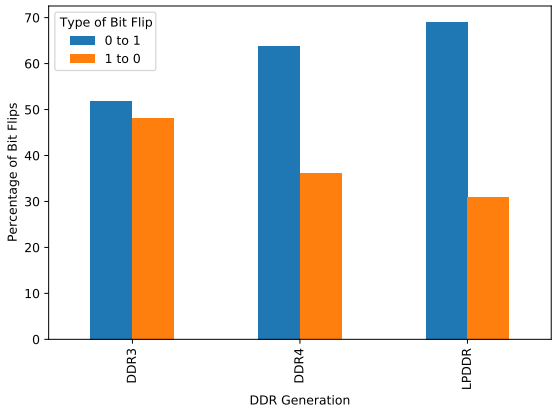

Fig. 4. Direction of laser induced bit-flips for DDR3, DDR4, and LPDDR4.

DRAM Chip	Location-1	Location-2	Location-3
DDR4	0	126	10125
DDR3	56	1751	10540
LPDDR4	42	174	10219

TABLE 3
Not all locations are equally vulnerable.

5 Experimental Challenges

In this section, we will discuss the experimental challenges in enabling precise fault injection.

5.1 Catastrophic Errors

The number of errors induced scales exponentially with laser power as shown in the Figure 5(a). Moreover, beyond certain incident energy, we observe catastrophic errors in our experiments. These catastrophic errors overwhelm the Memtest86, causing memory corruption and crashes. To avoid catastrophic errors, we calibrate the laser power and duration.

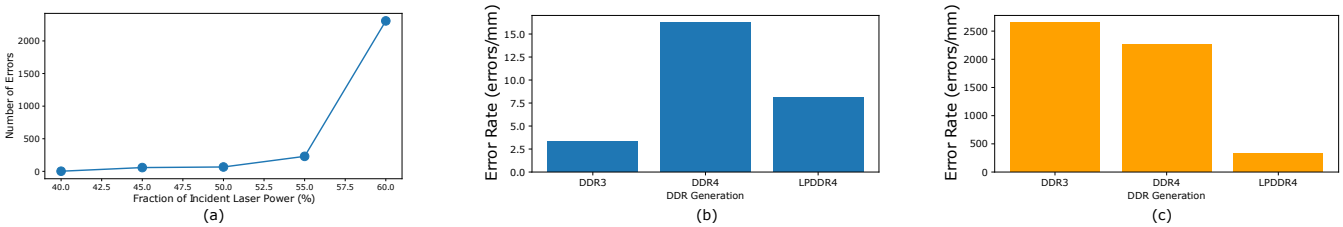

Fig. 5. (a) Number of errors with increasing laser power incident on LPDDR4 chip (b) Number of errors per millimeter of sketched line, with lower than peak incident power (c) Number of errors per millimeter of sketched line, at peak incident power.

5.2 Reduced Absorption due to Wearout

The hotspot temperature can not be elevated if the package does not absorb the incident light. Unfortunately, in our setup, we observe that after using the laser on the DRAM package repeatedly, the DRAM package wears out. The wear-out significantly reduces the absorption coefficient of the DRAM package, resulting in fewer errors in the subsequent experimental runs. Note that throughout all our experiments, we have not observed DRAM being permanently damaged, even in the extreme cases of wear out. We believe that this problem can be eliminated by calibrating the laser power and repetition rate.

5.3 Limitations of Current Experimental Setup

The laser mounted on the CNC machine is not precise and introduces a small error in the XY location. Location error can have some impact on the injected faults as not all locations on the package are equally vulnerable. However, with the rare exception of extremely vulnerable chip locations, the error in the XY plane does not impact our ability to induce repeatable errors. By upgrading the engraver, we believe it is possible to improve the CNC precision.

Moreover, The laser engraver can not incident a stationary spot of light for more than 10 seconds. This limitation is imposed by the engraver firmware for safety. Unfortunately, this constrained our ability to test the error resolution on our setup. We believe that by upgrading the laser and engraver, we can enable rigorous testing.

6 Summary

In this paper, we show that by using a laser, we can produce localized hotspots that can induce bit-flips in the DRAM memory. Laser-induced fault injection can perturb the data present in the memory without reading or writing the data. We show that our setup can induce precise and repeatable faults in DDR3, DDR4, and LPDDR4 memory modules from four different vendors. Furthermore, we show that by controlling the power of a laser beam incident on the DRAM chip, we can control the rate of faults induced on our setup. Our experimental evaluations show a strong spatial correlation in the errors and also depict that we can induce bit-flip errors for both true and anti-cells. In summary, we demonstrate a practical experimental methodology to inject faults in the DRAM chips.

References

[1] "Cracking a two million crypto wallet." [Online]. Available: https://www.theverge.com/2022/1/24/22898712/crypto-hardware-wallet-hacking-lost-bitcoin-ethereum-nft

[2] 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.

[3] Z. Chen, G. Vasilakis, K. Murdock, E. Dean, D. Oswald, and F. D. Garcia, "{VoltPillager}: Hardware-based fault injection attacks against intel {SGX} enclaves using the {SVID} voltage scaling interface," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 699–716.

[4] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based fault injection attacks against intel sgx," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 1466–1482.

[5] A. Trikalinou and D. Lake, "Taking dma attacks to the next level," *BlackHat USA*, 2017.

[6] M. K. Qureshi, D.-H. Kim, S. Khan, P. J. Nair, and O. Mutlu, "Avatar: A variable-retention-time (vrt) aware refresh for dram systems," in *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 2015, pp. 427–437.

[7] O. Mutlu and J. S. Kim, "Rowhammer: A retrospective," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 8, pp. 1555–1571, 2019.

[8] S. Govindavajhala and A. W. Appel, "Using memory errors to attack a virtual machine," in *2003 Symposium on Security and Privacy, 2003.* IEEE, 2003, pp. 154–165.

[9] M. Patel, J. S. Kim, and O. Mutlu, "The reach profiler (reaper) enabling the mitigation of dram retention failures via profiling at aggressive conditions," *ACM SIGARCH Computer Architecture News*, vol. 45, no. 2, pp. 255–268, 2017.

[10] L. Orosa, A. G. Yaglikci, H. Luo, A. Olgun, J. Park, H. Hassan, M. Patel, J. S. Kim, and O. Mutlu, "A deeper look into rowhammer's sensitivities: Experimental analysis of real dram chips and implications on future attacks and defenses," in *MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture*, 2021, pp. 1182–1197.

[11] H. Durmuş, H. Şafak, H. Z. Akbaş, and G. Ahmetli, "Optical properties of modified epoxy resin with various oxime derivatives in the uv-vis spectral region," *Journal of Applied Polymer Science*, vol. 120, p. 1490, 05 2011.

[12] "Ortur laser master 2 pro s2 laser engraving machine 10,000mm/min 24v/2a." [Online]. Available: https://ortur.net/products/laser-master-2-pro?variant=40577663828152

[13] "Memtest86 - official site of the x86 memory testing tool." [Online]. Available: https://www.memtest86.com/

[14] I. Inc.., "Ramcheck lx." [Online]. Available: https://www.memorytesters.com/ramcheck_lx/ramcheck_lx_tester.htm