Haowen Liu 2020-10-14

Paper information

- Title: Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors
- Authors: Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, Onur Mutlu
- Venue: Minneapolis, MN, USA

Paper content

Summary

This paper was the first to expose the phenomenon of ***Disturbance Errors***, a kind of unexpected *bit-flips*, in modern commodity DRAM and other memory/storage technologies. This phenomenon has become more and more obvious with the DRAM process technology scaling down to smaller dimensions. Malicious attackers can exploit it to break the ***memory isolation security principle*** to cast great threat on computer system.

Disturbance Error is mainly caused by voltage fluctuations on an wordline, which injects noise into an adjacent wordline through **electromagnetic coupling**, **bridges**, and/or **hot-carrier injection**, partially enabling the adjacent row of access-transistors for a short amount of time and facilitates the **leakage** of charge. *Repeated toggling of a DRAM row's wordline* stresses inter-cell coupling effects that accelerate charge leakage from nearby rows. Such a cell **loses too much charge** before *refresh*, it experiences a disturbance error.

This paper designed and carried out ingenious and detailed experiments to explore the **properties** of disturbance errors in all aspects. Here are the results.

- DRAM disturbance errors are caused by **the repeated opening/closing of a row**, *not* by column reads or writes
- **Disturbance Errors are widespread**
  - induce errors in most DRAM modules (110 out of 129) from three major DRAM manufacturers (widespread)
  - *it takes as few as 139K accesses to induce an error*
  - *up to one in every 1.7K cells is susceptible to errors*
  - modules from 2012 to 2013 are particularly vulnerable (caused by development of DRAM: smaller)
  - sudden jumps in the number of errors are followed by gradual descents (occur when a manufacturer migrates away from an old-but-reliable process to a new-but-unreliable process. By making adjustments over time, the new process may eventually again become reliable)
- **Access Pattern Dependence**

    - **the shorter RI(refresh interval), the fewer errors**
    - **the longer AI(activation interval), the fewer errors**
    - fewer activations(RI/AI) induce fewer errors
- **Address Correlation: Aggressor & Victim**
    - While most **words** have just a single victim, there are also some words with multiple victims.
    - large fractions of the rows are **aggressors**: 100%, 99.96%, and 47.04%
    - **the victim cells of an aggressor row** are predominantly localized to two rows or less. In fact, only a small fraction of aggressor rows affect three rows or more: 2.53%, 0.0122%, and 0.00649%
    - **correlation** exists between the address of an aggressor row and those of its victim rows
- **Data Pattern Dependence**
    - Whereas A modules did not favor one direction over the other, B and C modules heavily favored '1' $\rightarrow$ '0' errors.
    - the errors induced in three modules using ***four different data patterns*** are distinctive
    - Except for rare exceptions, every other victim cell had an error in **just a single preferred direction**(**leakage**)
- Sensitivity Results
    - Errors are Mostly Repeatable
    - Victim Cells $\neq$ Weak Cells
    - Not Strongly Affected by Temperature(but affected)

This paper also proposed some mitigations against disturbance error and discuss their feasibility(making different ***trade-offs*** between feasibility, cost, performance, power, and reliability).

- *Make better chips*: may get worse in the future as cells become smaller and more vulnerable
- *Correct errors*: incur a 12.5% capacity overhead and cannot correct multi- bit disturbance errors
- *Refresh all rows frequently*: degrade performance and energy-efficiency
- *Retire cells (manufacturer)*: costly
- *Retire cells (end-user)*: ineffective and inefficient in some cases and costly
- *Identify "hot" rows and refresh neighbors*: identify frequently opened rows and refresh only their neighbors. expensive
- ***PARA***(effective and low-overhead solution): probabilistically refreshing only those rows that are likely to be at risk. Every time a wordline is toggled, PARA refreshes the *nearby rows* ***with a very small probability*** ($p \ll 1$). As a wordline is toggled many times, the increasing disturbance effects are offset by the higher likelihood of refreshing the nearby rows.

A user-level program can cause disturbance errors on pages belonging to other programs by simply generating many DRAM accesses. Because the DRAM process technology is still scaling down to smaller dimensions, this phenomenon is becoming so widespread that it've cast tremendous thread on security of lots of hardwares and softwares.

Strengths

This is a pioneering paper, exposing and exploring a phenomenon rarely known or ignored by researchers and manufacturers. This paper is full of ideas, providing a lot of clues for the later researches.

Another reason for its success is the ingenious and detailed experimental methodology. Except for demonstrating the reason of disturbance errors, the paper explored ***properties*** of disturbance errors in all aspects, in a very short length(***fantastic writing***). And these properties might be the basic rules to exploit or defend against the disturbance errors. Moreover, the paper discussed every property in experiments and give either hypothesis or theory to explain them(***full of ideas***).

The ***PARA*** mitigation mechanism is also a highlight. I'm not sure but the probability-triggering mechanism might be inspired by ***CSMA/CD***, or actually it's a common method in security research?

Weaknesses

Though the exploration of this paper is very comprehensive, there are still some aspects being missed.

- Correlation between DRAM age(times of access, charging state time, using time, etc) and disturbance-error-vulnerability.
- Specific exploitation methods. Though the phenomenon seems very dangerous, maybe it's hard to exploit, because of the complex mechanisms of memory allocation.
- All of the solutions merely treat the symptoms of a RowHammer attack without solving the core circuit vulnerability.
- **Electromagnetic coupling**, **bridges**, and **hot-carrier injection**, which one plays the most important role in Disturbance Error? This is related to how to solve this problem from circuit level.
- What results in victim cell faults in 2 directions?

Thoughts

- Design and carry out experiment in variable-controlling approach to explore the correlation between DRAM age and disturbance-error-vulnerability. The aging of DRAM cells may change the physical property of capacitor, influencing the charging and leaking process. And this property may be exploited by malicious attckers. So we can also do some researches on system program behavior(frequent access to a physical location results in accelerated aging, and more vulnerable to RowHammer).
- Explore **electromagnetic coupling**, **bridges**, and **hot-carrier injection** which one plays the most important role in Disturbance Error, based on the conclusion to work out the mitigation methodology from circuit level.
- To exploit RowHammer, a thorough understanding of operating system and program behavior is necessary.

Takeaways and questions

Actually the knowledge, mechanism and principle in this paper are basic, and the hypothesis and viewpoint are not difficult to think of. However, the author had a pair of wise and far-sighted eyes, and sufficient research experience, and that's why he succeeded. If I come across this phenomenon(and I believe there must be a lot of researchers had found that phenomenon), maybe I just think there's no point to do deeper research. But the one who knows the value and sticks to it is the one who laughs last. So how to get a pair of far-sighted eyes, or the sense of research? Maybe, ***extensive knowledge, enormous research experience and gift of observing life***. And there may be a truth — the simple and more basic(generally come from principles directly), the more widespread, and the more valuable. Actually, there has been already a ***shift of mindset*** among mainstream security researchers: ***general-purpose hardware is fallible (in a very widespread manner) and its problems are actually exploitable***.

Here I have some questions.

- If a DRAM row/bit is more usually used(times of access, charging state time, etc), is it more vulnerable to RowHammer? Or the less used ones are more vulnerable? Are there researches on the correlation between DRAM age and RowHammer-vulnerability?
- Though SRAM like cache isn’t vulnerable to RowHAmmer, does it have similar hardware vulnerability?
- It’s easy to understand ***electromagnetic coupling*** facilitating the ***leakage*** of charge of the adjacent rows. But ***bridge*** and ***hot-carrier injection*** are out of my knowledge, I’ll have some study about them. However, I think the main cause is still the ***electromagnetic coupling***.
- Though according to the paper, the victim cells have errors in ***just a single preferred direction*** because it’s caused by the ***leakage*** and the leakage has only one direction. However, there are also some victim cell faults in 2 directions(leaking in 2 directions?), why?