Аналітичний огляд та аналіз трендів вразливості RowHummer для різних виробників DRAM

An analytical overview and trend analysis of RowHummer vulnerabilities for various DRAM vendors

Валентин Мазурок [A]

Corresponding author: аспірант кафедри кібербезпеки, e-mail: valentin.mazurok@gmail.com, ORCID: 0009-0006-2174-0800

Володимир Луценко [A]

к.тех.н., старший науковий співробітник, доцент кафедри, e-mail: lutsenkovn@ukr.net, ORCID: 0000-0001-7632-1730

Valentyn Mazurok [A]

Corresponding author: Graduate Student of the Cyber Security Department, e-mail: valentin.mazurok@gmail.com, ORCID: 0009-0006-2174-0800

Vladimir Lutsenko [A]

Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Department, e-mail: lutsenkovn@ukr.net, ORCID: 0000-0001-7632-1730

[A] Київський політехнічний інститут імені Ігоря Сікорського, м. Київ, Україна

[A] Ihor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Received: May 8, 2024 | Revised: June 22, 2024 | Accepted: June 30, 2024

DOI: 10.33445/sds.2024.14.3.16

Мета роботи: провести аналітичний огляд вразливості жорстких дисків типу SSD та проаналізувати трендів вразливості RowHummer для різних виробників DRAM. Сформувати прогнози розвитку.

Результати дослідження: показано тренд до збільшення кількості вразливих до RowHummer чіпів DRAM через зменшення технічного процесу вироблення блоків пам'яті.

Практична цінність дослідження: Знайдені паттерни вразливості та основні причини RowHummer можуть сприяти кращому розумінню та покращенню методів захисту пам'яті SSD в цілому.

Цінність дослідження: Представлено дані тестування нових чіпів пам'яті кількох виробників DRAM. Також використано комбінований метод аналізу на основі минулих напрацювань в галузі захисту від RowHummer атак.

Майбутні дослідження: Це дослідження відкриває шляхи для майбутніх досліджень динаміки розвитку захисту від атак типу RowHummer та суміжних атак на пам'ять сторонніми каналами.

Тип статті: аналітична.

Purpose: to conduct an analytical review of the vulnerability of SSD hard drives and analyze the trends of RowHummer vulnerabilities for different DRAM manufacturers. Make development forecasts.

Findings: Shows a trend toward an increase in the number of RowHummer-vulnerable DRAM chips due to a decrease in the technical process of manufacturing memory blocks.

Practical implications: The discovered vulnerability patterns and root causes of RowHummer can contribute to a better understanding and improvement of SSD memory protection methods in general.

Value: Test data for new memory chips from several DRAM manufacturers is presented. A combined method of analysis based on past developments in the field of protection against RowHummer attacks was also used.

Future research: This research paves the way for future research on the evolution of defenses against RowHummer-type attacks and related third-party memory attacks.

Paper type: analytical.

Ключові слова: RowHummer, SSD, RAM, DRAM, атаки на пам'ять.

Key words: RowHammer, SSD, RAM, DRAM, attacks on memory.

Вступ

Ізоляція пам'яті є ключовою властивістю надійної та безпечної обчислювальної системи. Доступ до адреси пам'яті не повинен мати небажаних побічних ефектів для даних, що зберігаються в інших адресах. Однак у міру того, як технологічний процес зменшується, мікросхеми пам'яті стають більш уразливими до перешкод та наведень, або навіть явищ, коли різні комірки пам'яті заважають роботі одна одної.

У статті ISCA 2014 [1] показано процес створення помилок у даних, що знаходяться у стандартних мікросхемах динамічної оперативної пам'яті (DRAM), які продаються та використовуються в сучасних системах. Багаторазове читання з тієї самої адреси в DRAM може пошкодити дані в сусідніх адресах. Зокрема, коли рядок DRAM відкривається (тобто активується) і закривається (тобто попередньо заряджається) неодноразово. Коли такі операції пророблено достатньо разів протягом інтервалу оновлення DRAM, один або більше

бітів у фізично суміжних рядках можуть бути змінені. Цей режим збою пам'яті зараз широко називають RowHamamer [2, 3].

Теоретичні основи дослідження

Загалом помилки спотворення даних виникають щоразу, коли існує достатньо сильна взаємодія між двома компонентами схеми (наприклад, конденсаторами, транзисторами, провідними доріжками), які повинні бути ізольовані один від одного. Залежно від того, який компонент взаємодіє з іншим компонентом, а також від того, як вони взаємодіють, можливе багато різних режимів спотворення.

Існує один конкретний режим спотворень, який впливає на стандартні чіпи DRAM трьох основних виробників на ринку. Коли напруга рядка даних змінюється неодноразово, в деяких комірках в сусідніх рядках витікання заряду відбувається набагато швидше. Такі вразливі комірки, якщо їх викликати достатньо часто, не можуть утримувати достатній заряд навіть протягом 64 мс (інтервал часу, через який вони оновлюються). Зрештою, це призводить до того, що комірки втрачають дані та накопичують помилки. Це і є механізм RowHammer.

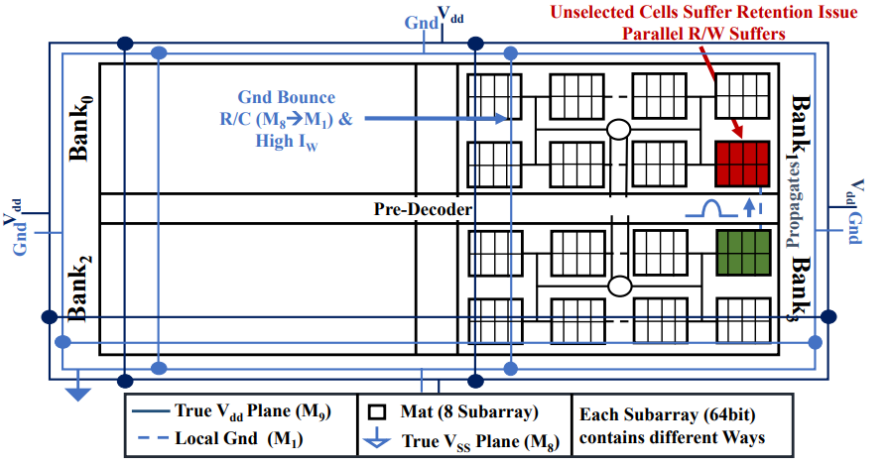

Рисунок 1 – Схема зміни значення сусідньої комірки пам'яті при RowHummer

Без аналізу існуючих чіпів DRAM на рівні мікросхеми, що заборонено через конфіденційність цих даних, неможливо зробити остаточні заяви про те, як саме відбувається перетікання чи витікання зарядів з комірок і, як наслідок, як збільшити їх непроникність. В статті ISCA 2014 [1] висувається гіпотеза, заснована на попередніх дослідженнях і висновках, що може бути три способи атаки. Принаймні два великих виробники DRAM підтвердили всі три гіпотези є потенційними причинами помилок та збоїв. Першою є зміна напруги лінії живлення, яка може ввести шум у сусідні рядки через електромагнітні наведення [4]. Це частково активує сусідній ряд транзисторів, для доступу на короткий проміжок часу, та сприяє витоку заряду з уразливих елементів. Таким чином, якщо рядок викликати значну кількість разів, щоб задіяти такі вразливі комірки, перш ніж вони будуть оновлені, заряд у таких клітинках виснажується до такого рівня, що початкові значення клітинок більше не підлягають відновленню. Друга — мости — це добре відомий клас несправностей DRAM, у яких між елементами непов'язаними дротами, з'єднаннями та/або конденсаторами утворюються провідні канали [5]. Третя ж — безперервне перемикання рядка даних протягом сотень годин. Це може значно пошкодити його та призвести до ін'єкції гарячих носіїв через *p-n* перехід [6]. Якщо деякі з "гарячих носіїв" вводяться в сусідні ряди, це може змінити кількість заряду в їхніх елементах або змінити характеристики транзисторів доступу, щоб збільшити їх негерметичність.

Постановка проблеми

Проблема безпеки пам'яті типу RowHammer стала важливою в сучасних комп'ютерних системах, оскільки такі атаки можуть призвести до витоку конфіденційної інформації. Аналіз уразливості DRAM різних виробників в контексті RowHammer стає актуальним для оцінки рівня захищеності пам'яті від цього типу атак. Тому дослідимо рівень протидії різних чіпів DRAM до атак типу RowHammer та прослідкуємо тренд розвитку.

Методологія дослідження

Багато статей [1, 2, 3] містять детальний експериментальний аналіз різних характеристик RowHammer для тодішніх чіпів, включаючи його поширеність у чіпах DRAM, залежність від шаблону доступу, залежність від шаблону даних, залежність від температури, кореляцію адрес між рядками пам'яті жертви та агресора, кількість бітів у захищеному рядку, які змінюються через RowHammer у сусідньому рядку, кількість рядків, які постраждали через RowHammer у сусідньому рядку, зв'язок уразливих RowHammer комірок із компрометованими комірками, які потребують вищої частоти оновлення та повторюваність помилок RowHammer. Той факт, чи рядок пам'яті є вразливим до RowHammer можна прослідкувати в багатьох схожих за структурою та часом виробництва системах, тому цю інформацію можна систематизувати та аналізувати з кожним новим поколінням чіпів.

Одним із ключових висновків зібраної інформації із зазначених вище статей є те, що помилки, викликані RowHammer, передбачувано повторюються. Іншими словами, якщо значення клітинки буде пошкоджено за допомогою RowHammer, значення тієї самої клітинки, швидше за все, знову буде пошкоджено за допомогою RowHammer. Ця повторюваність дозволяє створювати повторювані атаки на безпеку контрольованим способом, якщо зловмисник знає основні зовнішні характеристики встановлених на машині фізичних пристроїв.

Використовуючи експериментальну інфраструктуру тестування DRAM на основі FPGA [8] було протестовані 239 модулів DRAM, виготовлених трьома основними виробниками (A, B, C) за останні одинадцять років (2013–2023). Дані також було оновлено для найновіших чіпів. Дослідження виявили, що 220 із протестованих схем вразливі до RowHammer. Найперша помилка була в чіпах виробництва 2013 року. Це показано на малюнку 1, де показано частоту помилок, яку ми виявили в усіх 239 перевірених модулях, де модулі класифіковані на основі дати виробництва.

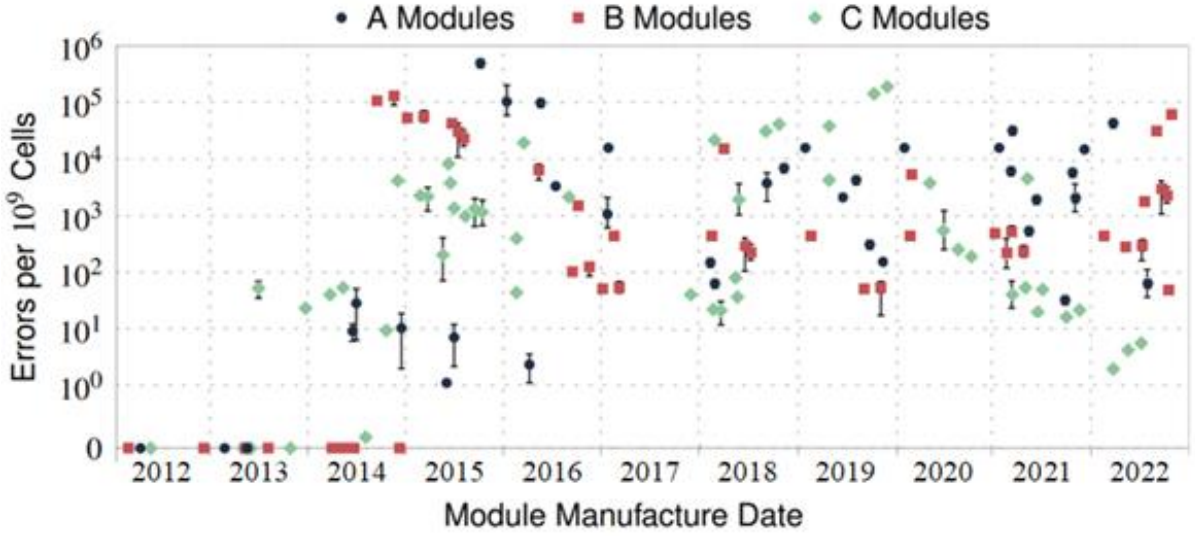

Рисунок 2 – залежність кількості RowHammer помилок від року виробництва DRAM чіпів.

Результати

Як видно з рисунку 2 та зібраних даних - усі модулі DRAM з 2013–2014 років були вразливими до RowHammer, що вказує на те, що такі атаки є відносно недавнім явищем, яке впливає на більш просунуті покоління технологічних процесів.[7] Ці дані можна інтерполювати в відповідні графіки, щоб зрозуміти тренд розвитку технологій та відповідних виробничих процесів. Також це допоможе побачити певні залежності і зрозуміти наскільки виробники боряться з таким типом вразливостей.

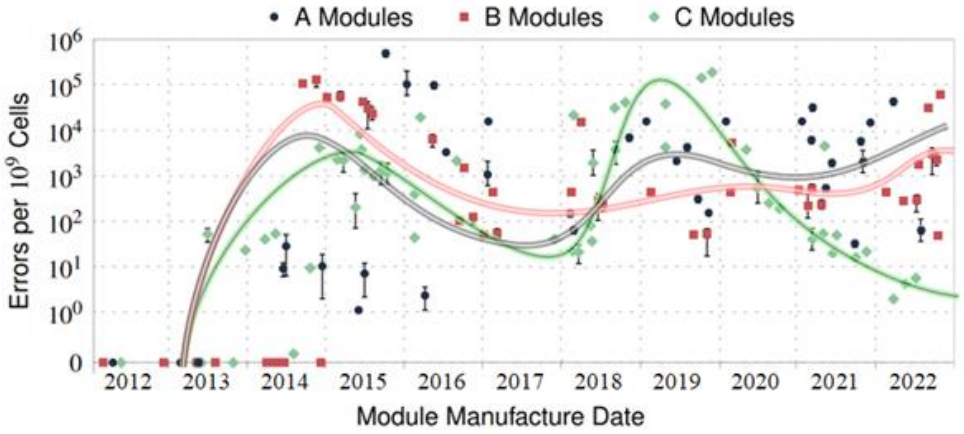

Рисунок 3 – Графіки тренду даних протестованих чипів

Бачимо значний тренд на зростання кількості помилок в розробників А та В. Даний результат може бути спричинений кількома факторами:

- Зменшення технологічного процесу, задля збільшення густини пам'яті і як наслідок більша схильність до витікання заряду між комірками.
- Здешевлення виробництва задля збільшення конкуренто-спроможності, як наслідок погіршення безпекових протоколів при виробництві.

Щодо модулів виробника С – їх тренд вказує на покращення захисту від даного типу атак, зокрема через більший технологічний процес. Також слід зважати на різні лінійки виробників, що можуть показувати абсолютно різні результати в тестуванні. Через це для повноти даних і вірної класифікації сформуємо зони скупчення та виділимо їх характеристики. Важливо розуміти, що боротьба виробників з проблемою RowHummer дійшла до масового виробництва в середині 2017 року, тому буде логічним розділити зони на два відрізки, до та після.

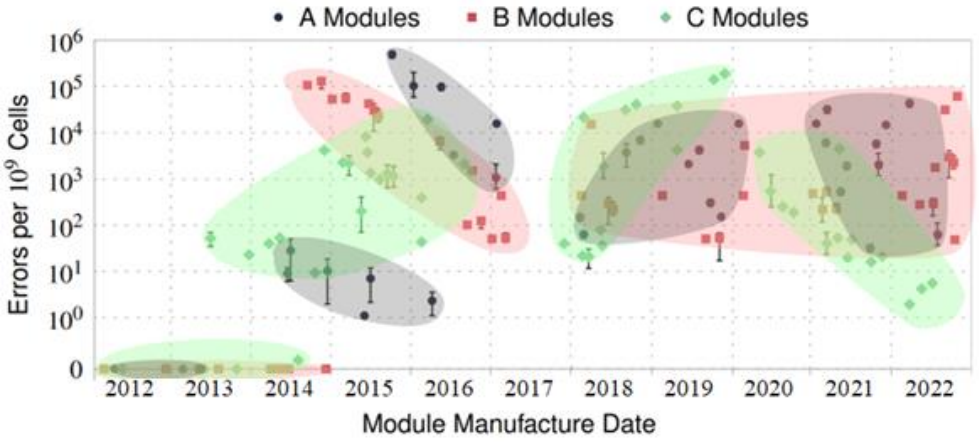

Рисунок 4 – Скупчення RowHammer помилок для різних виробників

Для першого скупчення бачимо що усі виробники не вразливі до RowHummer через низьку густину пам'яті.

Виробник А представлений двома різними лінійками до 2014 року, і як бачимо преміальна має значно нижчі показники відтворюваності даної вразливості. На даний момент вони разом з виробником В вийшли на плато і мають схожі характеристики вразливості. Тренд вказує на незначний ріст, але це може змінитись з переходом до нових технологій. Модулі виробника С, не зважаючи на ріст вразливості в минулі роки, показує хорошу захищеність ближче до наших днів. Тренд також вказує на це.

Обговорення

Враховуючи, що RowHammer є настільки критичною вразливістю, важливо знайти як негайні, так і довгострокові рішення проблеми RowHammer (а також пов'язаних проблем, які можуть спричинити подібні вразливості). Метою негайних рішень є забезпечення того, щоб існуючі системи були полагоджені таким чином, щоб уразливі пристрої DRAM, які вже є в польових умовах, не могли бути скомпрометованими. Метою довгострокових рішень є гарантія того, що майбутні пристрої DRAM не страждатимуть від проблеми RowHammer, коли вони будуть випущені в масмаркет. Довгострокові рішення вже розробляються і втілюються, як ми можемо бачити з графіків, але поки ринкові відносини перемагають, рішення переходять в вимір програмного забезпечення. Такі рішення скоріше короткострокові, бо можуть бути подолані хакерами.

З огляду на те, що швидкі та негайні рішення вимагають механізмів, які вже існують у системах, що вже працюють – вони принципово більш обмежені. Через це першим індикатором вразливості RowHummer на який звертають увагу є частота з якою будуть оновлюватись комірки пам'яті. Тобто інтервали часу через які вони будуть перезаряджатись. Популярне швидке рішення, описане та проаналізоване в статті ISCA 2014 [1], полягає у збільшенні цієї частоти оновлення пам'яті таким чином, щоб ймовірність індукування помилки RowHammer зменшилась. Кілька великих виробників систем (зокрема Apple, HP, Cisco, Lenovo та IBM) прийняли це рішення та випустили патчі безпеки, які підвищили частоту оновлення DRAM у контролерах пам'яті. Незважаючи на те, що це рішення може бути практичним і ефективним для зменшення вразливості, воно має значні недоліки, пов'язані зі збільшенням енергоспоживання, зниженням продуктивності системи та погіршенням якості користувацького досвіду.

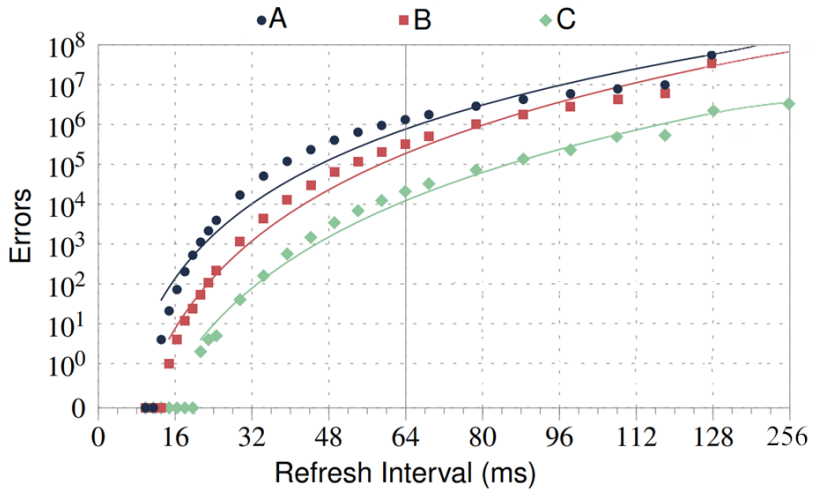

Рисунок 5 – Кількість помилок спричинена RowHammer у найуразливіших модулях DRAM виробників A, B, C, в залежності від інтервалу оновлення

З графіка видно, що частота оновлення має бути збільшено в 7 чи 8 разів від номінального значення сьогодні, якщо ми хочемо усунути всі помилки, викликані RowHammer з тестів вище. Оскільки оновлення пам'яті вже є значним тягарем для енергоспоживання, продуктивності та якості обслуговування, його збільшення на будь-яку значну цифру лише погіршить ситуацію. Тим не менш, підвищення частоти оновлення, ймовірно, є найпрактичнішим миттєвим рішенням для RowHammer, яке не потребує суттєвих змін у системі. Але все ж потрібно шукати більш практичні постійні рішення, що будуть підходити під виклики сучасності, зокрема для нестаціонарних систем.

Висновки

Отже вразливість пам'яті RowHammer є серйозною проблемою для сучасних технологій. Вона є однією з нових перешкод для "Закону Мура" і потребує значних змін у внутрішній архітектурі сучасних електронних схем. Через їх постійне зменшення у розмірах і зменшення виробничого процесу транзисторів все важче не зважать на мікровзаємодію та ефекти поля, що призводять до дефектів та помилок, іноді умисних – чим є і RowHummer.

З нашого дослідження існуючих чипів можна зробити висновок що технології деяких виробників не можуть тримати удар від даної вразливості, зокрема виробники A та B. Інші ж проводять роботу над помилками і демонструють позитивний ріст, як от виробник C.

Як би там не було, проблема присутня у всіх вироблених сучасних чіпів і програмні заплатки лише маскують проблему, тому потрібно повертатися саме до технічного виконання. Лише повне переосмислення даних схем зможе викорінити проблему RowHummer при постійному зменшенні технологічного процесу з вбудованих систем пам'яті.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

Kim, Y.et al. (2014), "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors," in ISCA (pp. 361-372) doi: 10.1109/ISCA.2014.6853210.

Aga, M. T. et al. (2014), "When Good Protections go Bad: Exploiting anti-DoS Measures to Accelerate Rowhammer Attacks," in HOST (pp. 8-13), doi: 10.1109/HST.2017.7951730

Chandrasekar, K. et al. (2016), "Exploiting Expendable Process-margins in DRAMs for Run-time Performance Optimization," in DATE (pp. 1-6), doi: 10.7873/DATE.2014.186.

Seaborn, M. and T. Dullien (2015), "Exploiting the DRAM Rowhammer Bug to Gain Kernel Privileges,". Retrieved from: http://googleprojectzero.blogspot.com.tr/2015/03/exploitingdram-rowhammer-bug-to-gain.html.

Chao, M.-T. et al. (2009), "Fault Models for Embedded-DRAM Macros," in DAC (pp. 714-719), https://doi.org/10.1145/1629911.1630097

Al-Ars, Z. et al. (2006), "DRAM-Specific Space of Memory Tests," in ITC, https://doi.org/10.1109/TEST.2006.297701

Chia, P.-F. et al. (2010) "New DRAM HCI Qualification Method Emphasizing on Repeated Memory Access". In Integrated Reliability Workshop.

Liu, J. et al. (2013), "An Experimental Study of Data Retention Behavior in DRAM Devices: Implications for Retention Time Profiling Mechanisms," ISCA, https://doi.org/10.1145/2485922.2485928

References

Kim, Y.et al. (2014), "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors," in ISCA (pp. 361-372) doi: 10.1109/ISCA.2014.6853210.

Aga, M. T. et al. (2014), "When Good Protections go Bad: Exploiting anti-DoS Measures to Accelerate Rowhammer Attacks," in HOST (pp. 8-13), doi: 10.1109/HST.2017.7951730

Chandrasekar, K. et al. (2016), "Exploiting Expendable Process-margins in DRAMs for Run-time Performance Optimization," in DATE (pp. 1-6), doi: 10.7873/DATE.2014.186.

Seaborn, M. and T. Dullien (2015), "Exploiting the DRAM Rowhammer Bug to Gain Kernel Privileges,". Retrieved from: http://googleprojectzero.blogspot.com.tr/2015/03/exploitingdram-rowhammer-bug-to-gain.html.

Chao, M.-T. et al. (2009), "Fault Models for Embedded-DRAM Macros," in DAC (pp. 714-719), https://doi.org/10.1145/1629911.1630097

Al-Ars, Z. et al. (2006), "DRAM-Specific Space of Memory Tests," in ITC, https://doi.org/10.1109/TEST.2006.297701

Chia, P.-F. et al. (2010) "New DRAM HCI Qualification Method Emphasizing on Repeated Memory Access". In Integrated Reliability Workshop

Liu, J. et al. (2013), "An Experimental Study of Data Retention Behavior in DRAM Devices: Implications for Retention Time Profiling Mechanisms," ISCA, https://doi.org/10.1145/2485922.2485928