Is PRAC Enough?

Salman Qazi

How did We Get Here?

- DDR4 Defenses Defeated
- Lesson: Memory can be deployed for years before being proven insecure
- Clashing Interests
  - Trust issue: Customers want security assurances
    - But TRR implementations are opaque
  - Trade Secrets / Competitive advantage : Suppliers want freedom to innovate
    - They can’t agree to a single implementation
- Desirable characteristics in a practical solution:
  - Principled
  - Practical
  - Partitioning of concerns
  - future-Proof (at least somewhat)

PRAC is a Framework

- Specification describes an interface and general principles
  - E.g. per-row counter, ALERT signal usage, etc.
- **No universal implementation**
- DRAM requirements are not universal
  - Different device characteristics based on underlying technology
- **Implementation based on trade offs in the design of a specific chip**
- Flexibility to optimize
- Complexity of the problem
  - “Count the number of activates, refresh neighbors at threshold, and ALERT if more time needed” doesn’t do justice.
  - Conceptually simple, the devil is in the details

What can Go Wrong? : Correctness

- Specification Violations
  - E.g. Subtle misinterpretation of the specification that leads to a vulnerability
- Incorrect assumptions about the underlying media
  - E.g. hammer count, blast radius, On-Die ECC behavior, data dependency behavior, previously unknown disturb mechanisms, etc.
  - DRAM will evolve
- Implementation bugs
  - E.g. Correct high-level design, but missing corner cases
- Unforeseen security implications
  - E.g. A mismatch between the perceived and actual threat model. E.g. side channels

What can Go Wrong: Power and Performance

- Average Case
- Pathological / Malicious
- Already an active area of research

My Starting Position

Is PRAC a good solution to DRAM read disturbance?

It is a good starting point for discussion.

A shared set of assumptions makes discussion practical.

Are we missing anything?

Definitely

Can we (and should we) do much better (and hopefully not worse)?

Probably