ALARM: Active LeArning of Rowhammer Mitigations

Amir Naseredini[1,2], Martin Berger[1,3,4],
Matteo Sammartino[2,5] and Shale Xiong[6]

1. University of Sussex
2. Royal Holloway University of London
3. Montanarius Ltd
4. Turing Core, Huawei
   2012 Labs, Huawei R&D UK
5. University College London
6. Arm Ltd

s.naseredini@sussex.ac.uk

Outline

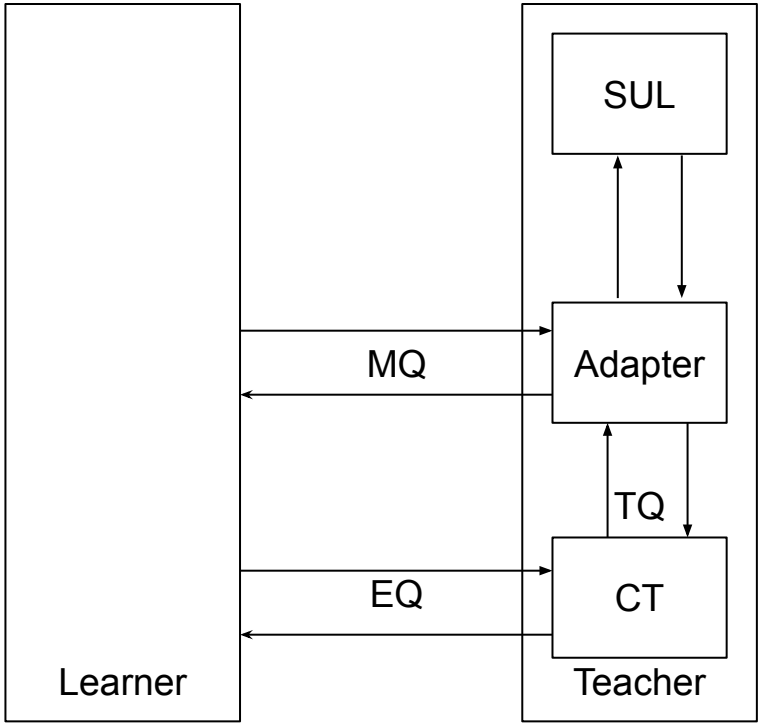
- Introduction to the Problem
- Active Learning
- Rowhammer Machine
- ALARM
- Experiments
- Conclusion

Introduction to the Problem

- Well, … Rowhammer!
- Vendors’ secrecy about mitigations
  - Error Correction Code - ECC
  - Target Row Refresh - TRR
- The history of Rowhammer gives us no confidence
- Towards learning
  - Large parameter space
  - Complex DRAM-access protocols
  - A vague picture of mitigations

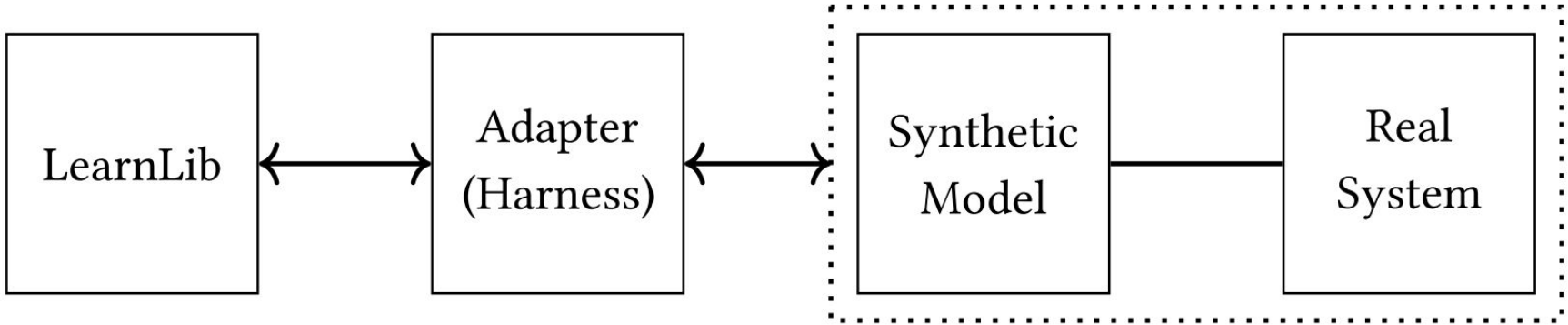
Introduction to Active Learning

- Active Learning?
- ~~Deep Learning~~ vs Active Learning
  - Infer an automaton model
  - No labelled training data
  - No information about the mitigations
  - We need to refine the learning
  - The output model is interpretable
- Similar work successfully analysed
  - TLS
  - TCP
  - SSH
  - Cache replacement policies



How to use Active Learning?

- Translation
- Abstraction
- Determinisation
- Adapter

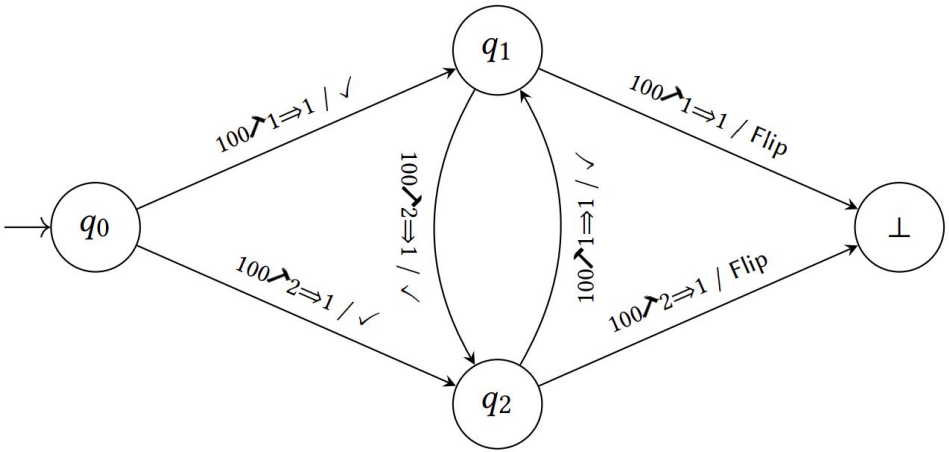


Rowhammer Machine

A Rowhammer machine is a tuple:

$$\langle Q, q0, \text{ACC}, \text{OBS}, \delta \rangle$$

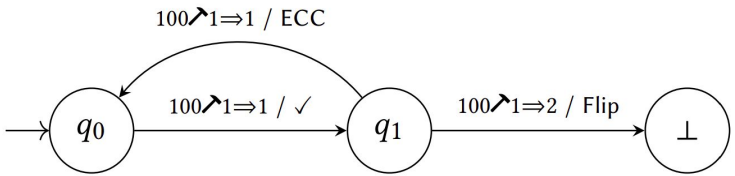
- Input: $a \nearrow r \Rightarrow f$
  - a: access
  - r: row
  - f: flippable
- Output:
  - ✓
  - FLIP
  - ECC
  - TRR

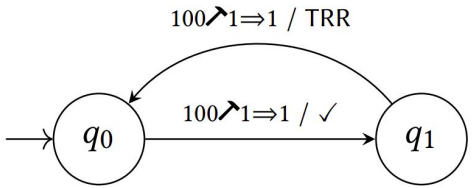


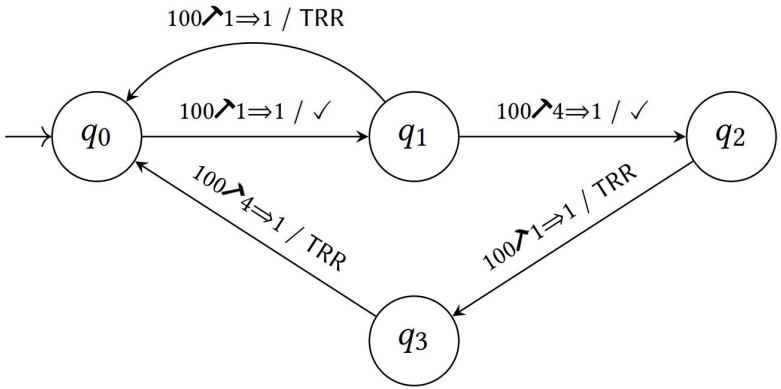
a: $100 \nearrow 1 \Rightarrow 1$
b: $100 \nearrow 2 \Rightarrow 1$

O_1	a	b
ε	✓	✓
a	FLIP	✓
b	✓	FLIP

Rowhammer Machine (Cont'd)

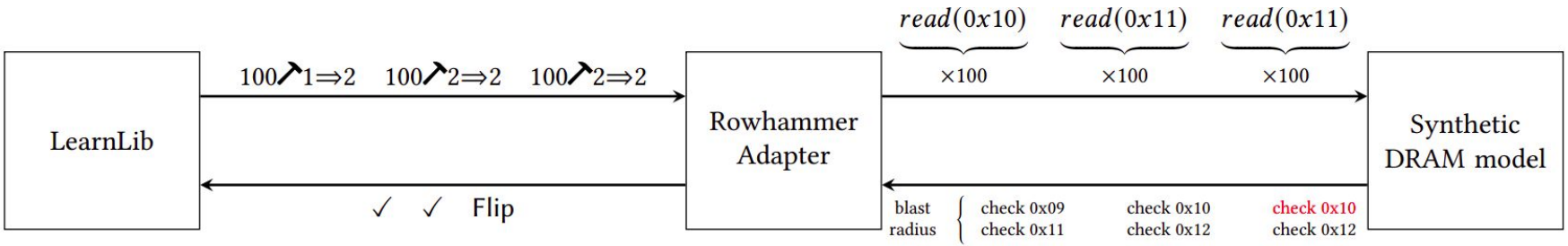






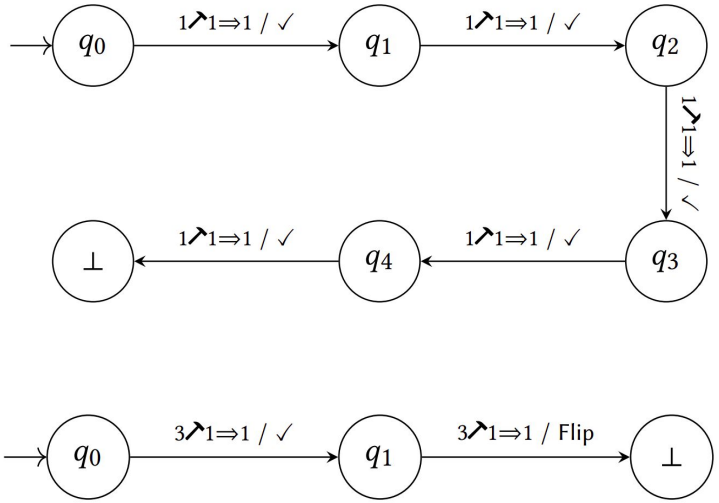
ALARM

- Follows the same ‘Recipe’
- Infers
  - Rowhammer threshold
  - Mitigation parameters
    - TRR size
    - TRR threshold
    - ECC capacity

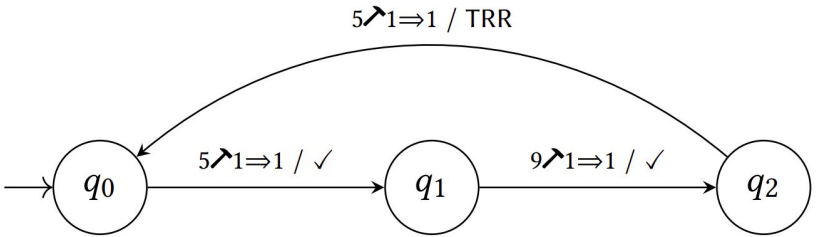


ALARM (Cont'd)

- Rowhammer threshold

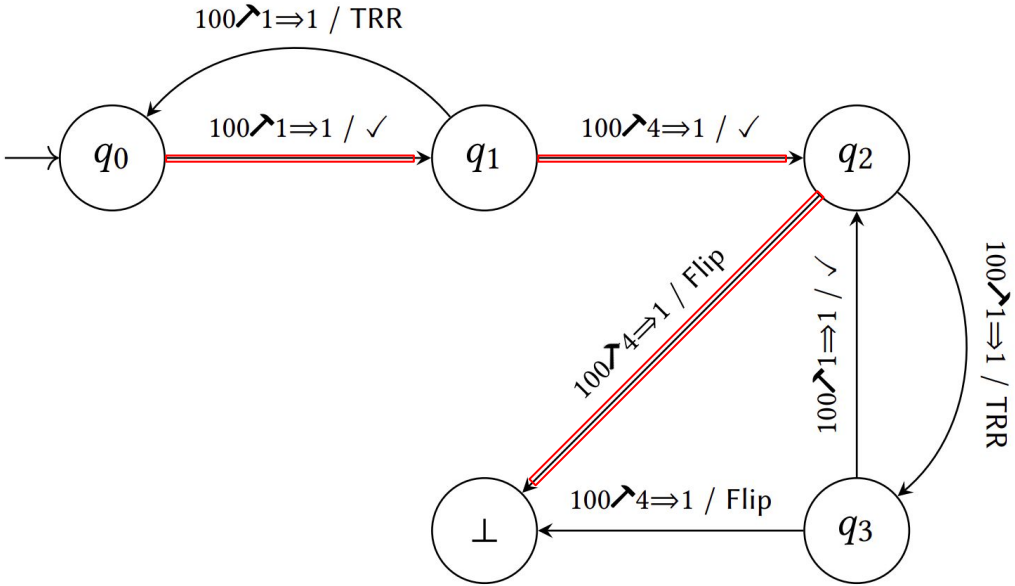


- TRR threshold



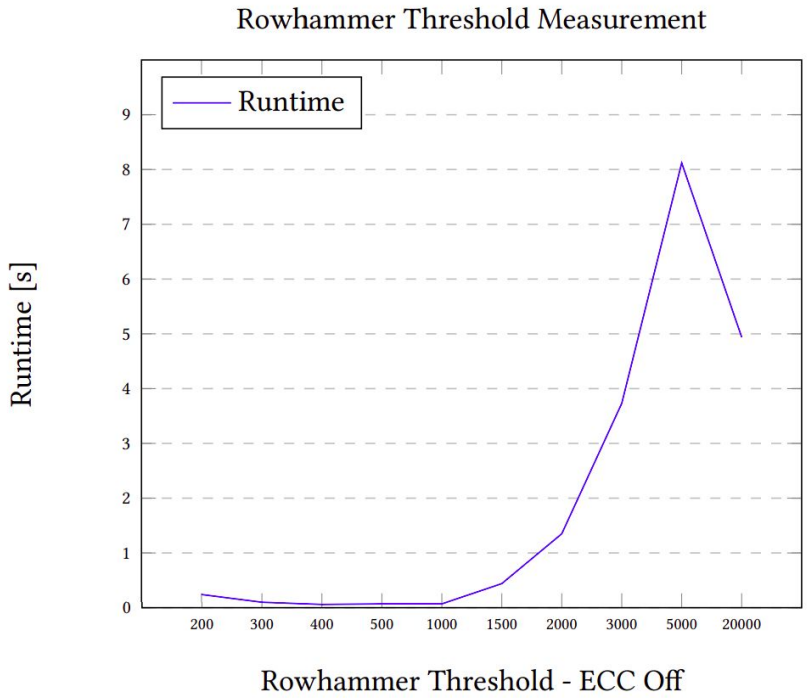
ALARM (Cont'd)

- TRR Size



Experiments

Experiments (Cont'd)



Conclusion

- The issue is still there
- The need for an automated tool
- Future work
  - Move to a simulator, e.g. gem5
  - Move to actual hardware

Thank you

Questions?