A Powerless and Non-volatile Counterfeit IC Detection Sensor in a Standard Logic Process Based on an Exposed Floating-Gate Array

Muqing Liu and Chris H. Kim

University of Minnesota, Minneapolis, MN

liux3300@umn.edu

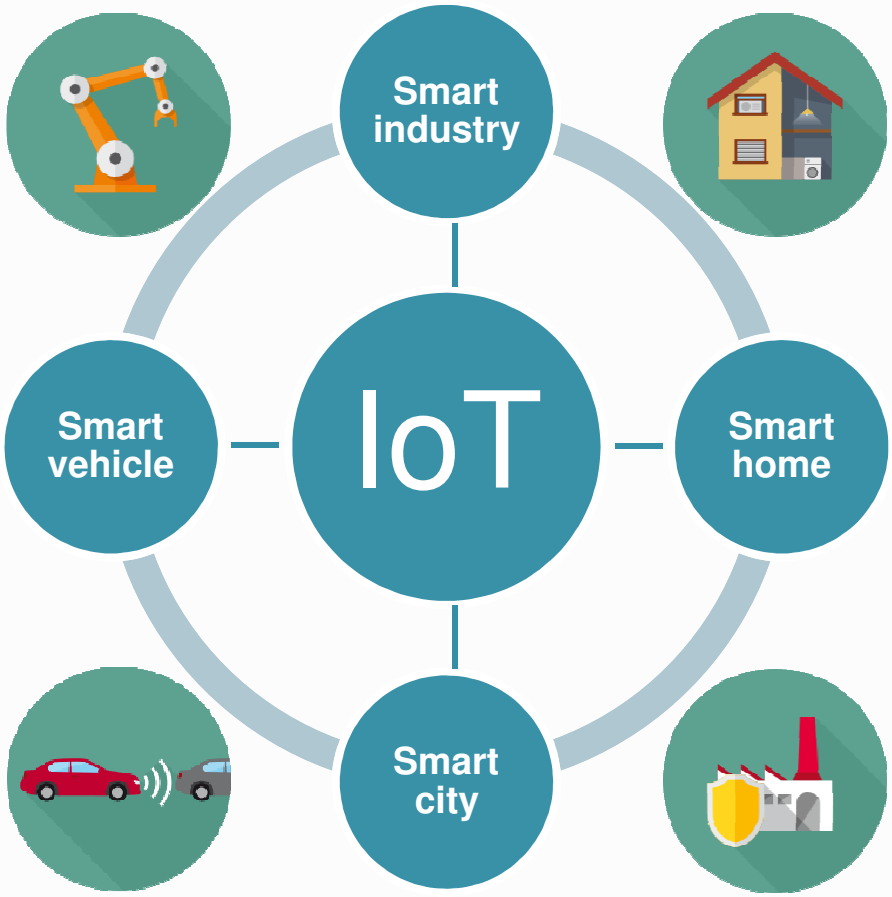
Outline

- Motivation
- Proposed counterfeit IC detection sensor
- 0.35µm test chip measurement results
- Summary

Outline

- **Motivation**
- **Proposed counterfeit IC detection sensor**
- **0.35µm test chip measurement results**
- **Summary**

Internet of Things (IoT) and Security



Source: Infineon

Fake devices

Fake servers

Hackers

Eaves-dropping

Counterfeit Types

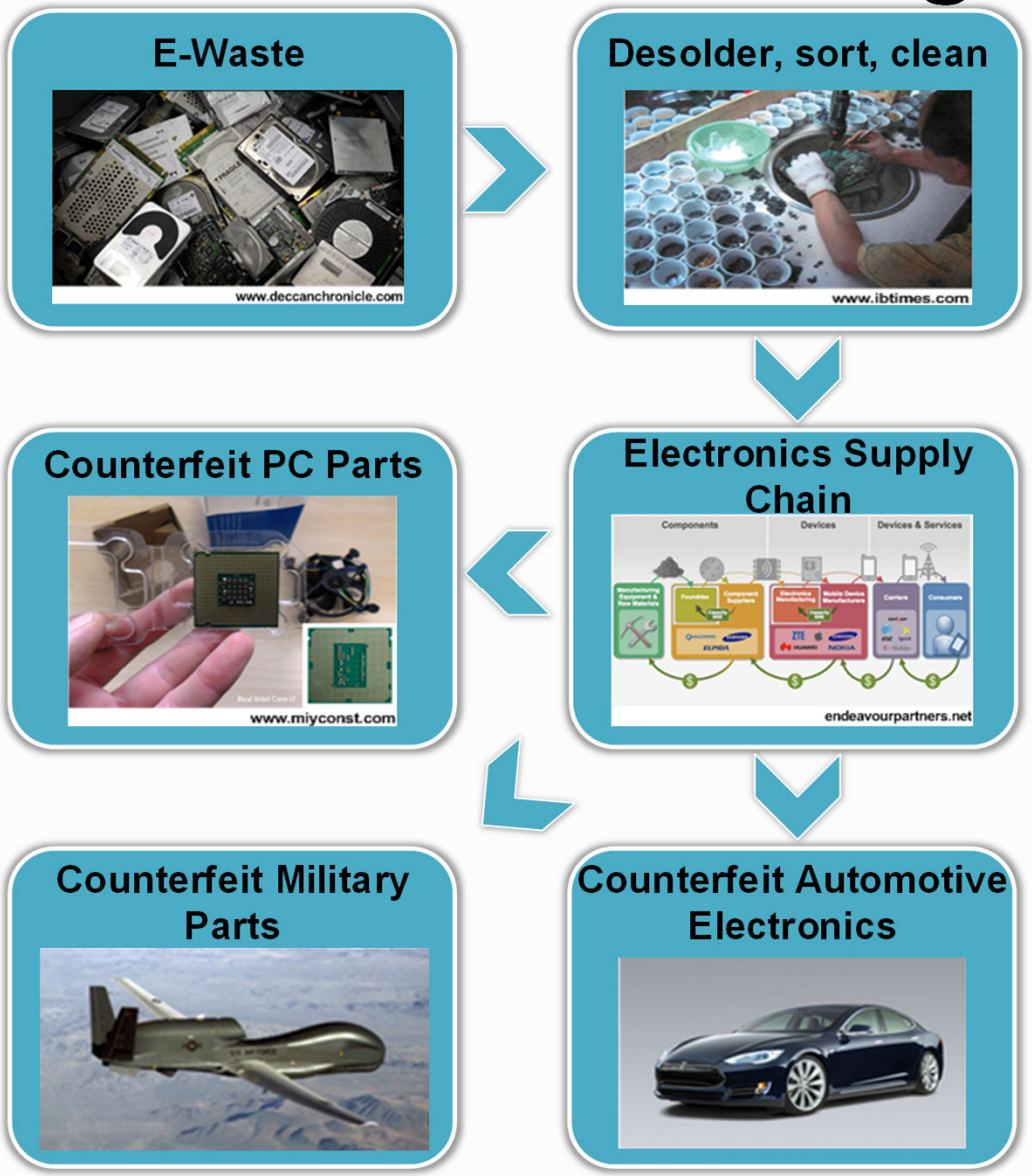
More than 80% of counterfeits

- Recycled
- Remarked
- Overproduced
- Defective
- Cloned
- Tampered
- Forged Documentation

80%

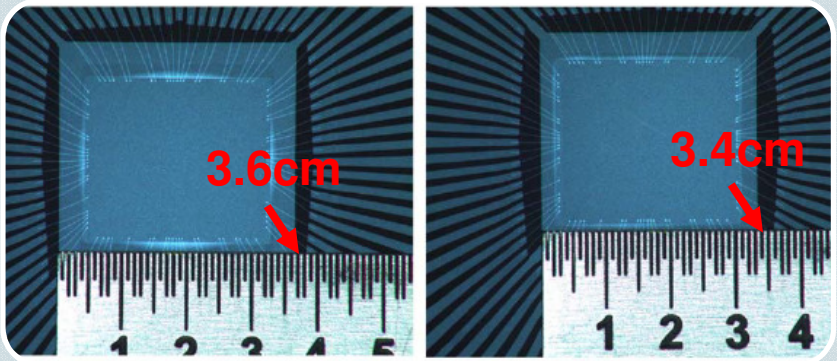
U. Guin, *et al.*, Proceedings of IEEE, Aug. 2008.

Electronics Counterfeiting Threat



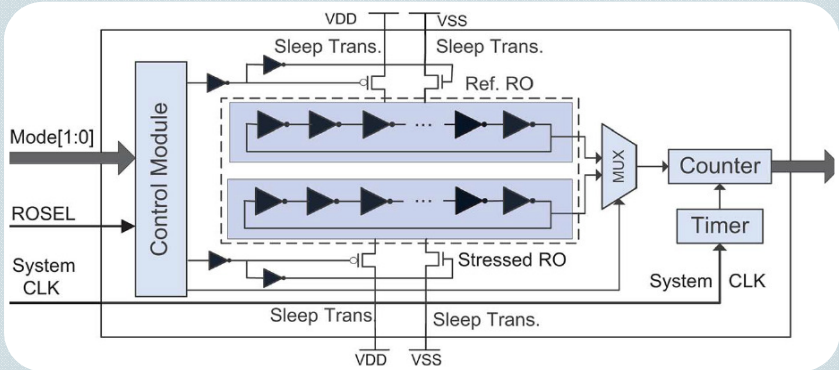
Counterfeit IC Detection

X-ray Imaging



Source: Honeywell

IC Recycling Sensor



X. Zhang, *et al.*, DAC, Jun. 2012.

Physical Inspection

- Straightforward method
- Costly and time consuming
- An expert required to interpret the test results
- Invasive, destructive

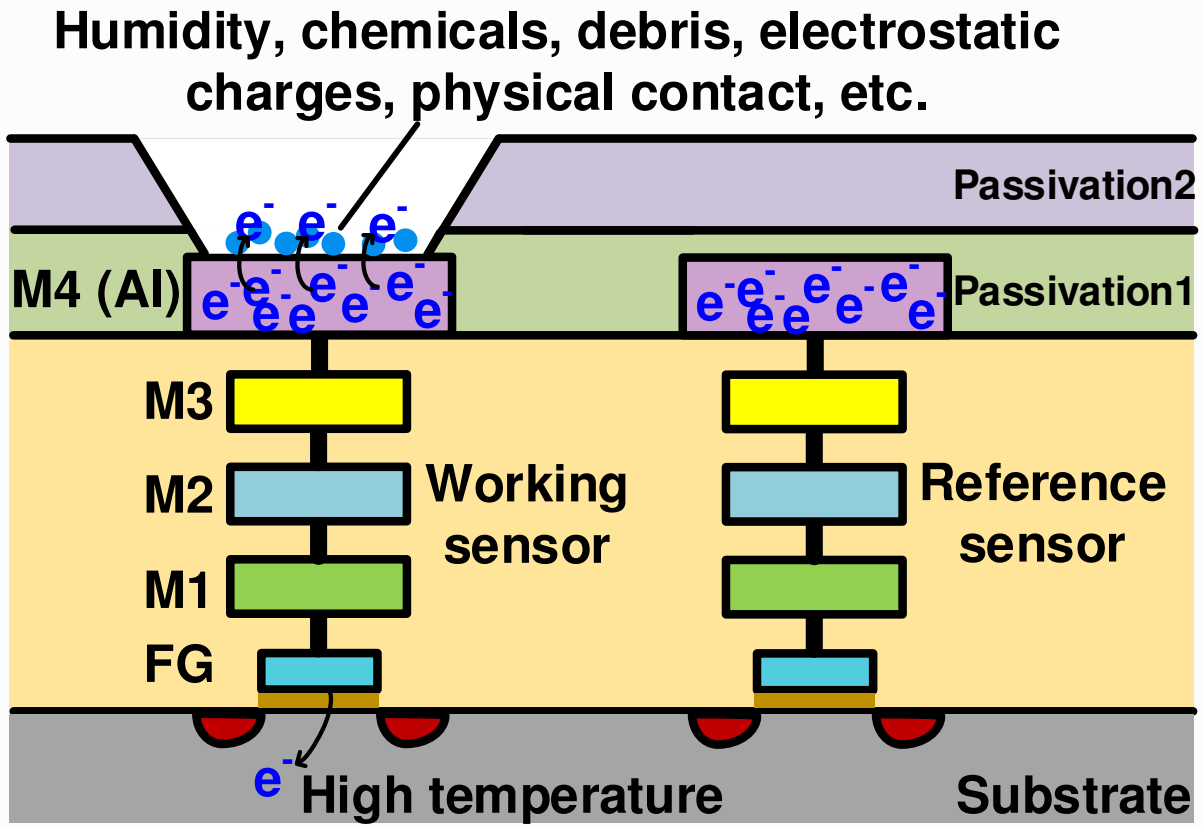
Electrical Test

- Verify functionality and performance
- Measure the usage time of the chip
- Cannot detect physical attacks

Outline

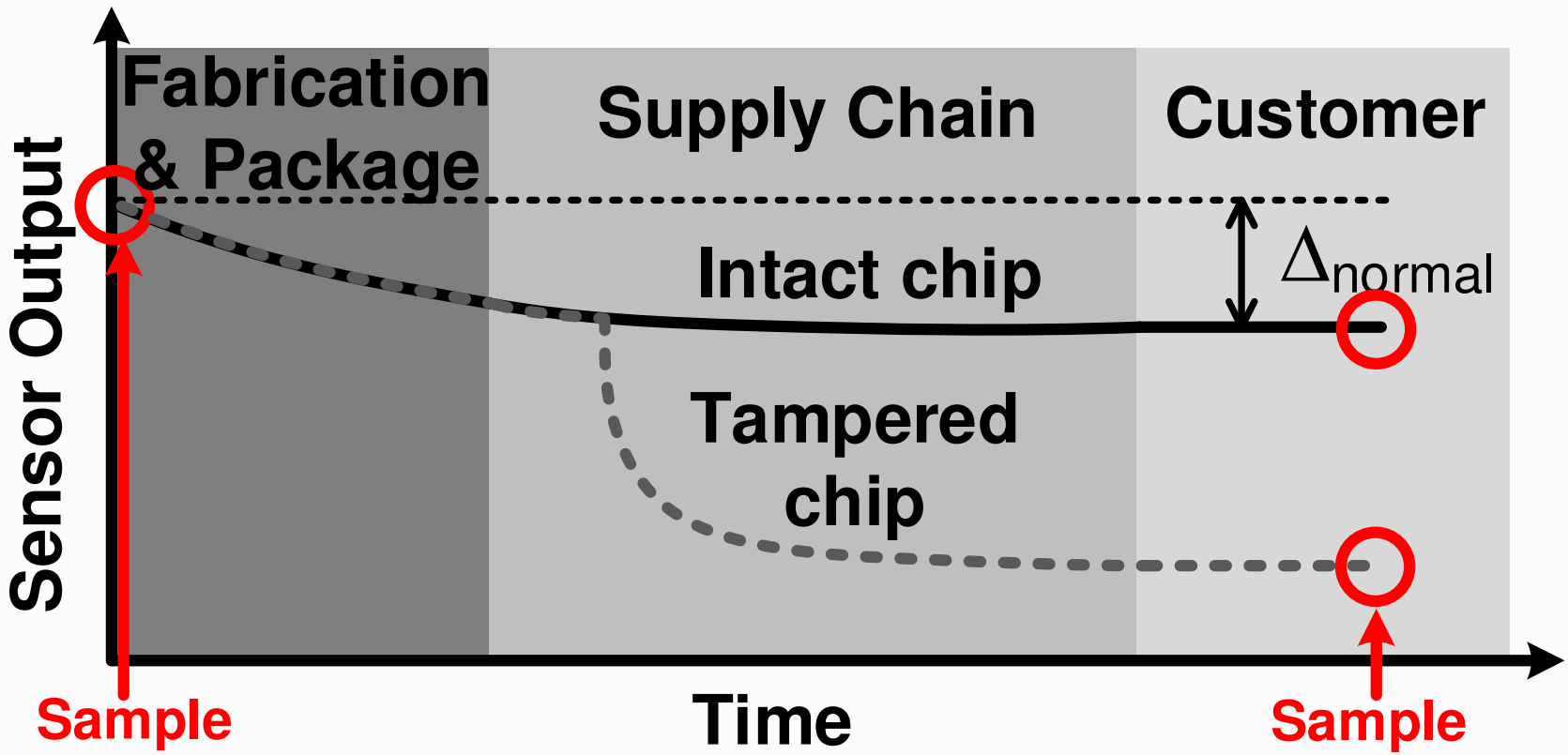
- Motivation
- **Proposed counterfeit IC detection sensor**
- 0.35µm test chip measurement results
- Summary

Eflash with Exposed Floating Gate



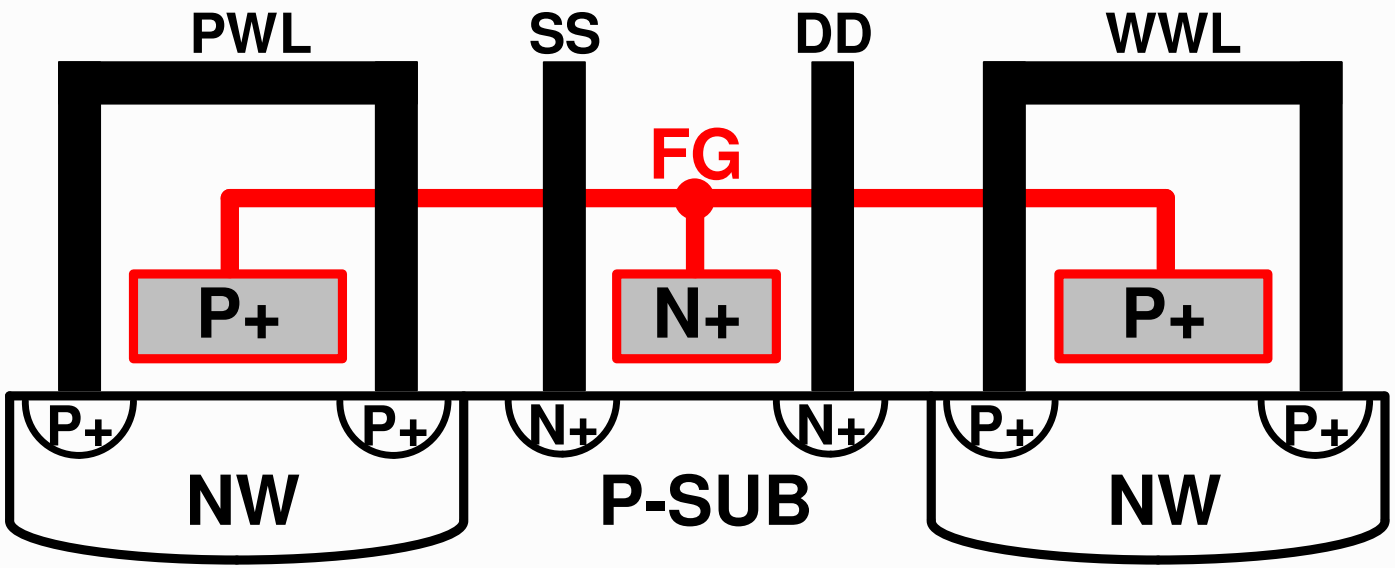
- Expose floating gate (FG) to the environment.
- Non-volatile and powerless.
- No process overhead, no back-end processing.

Counterfeit IC Detection Scheme



- Δ_{normal} **should account for drift and retention loss under normal conditions.**

Logic Compatible Embedded Flash

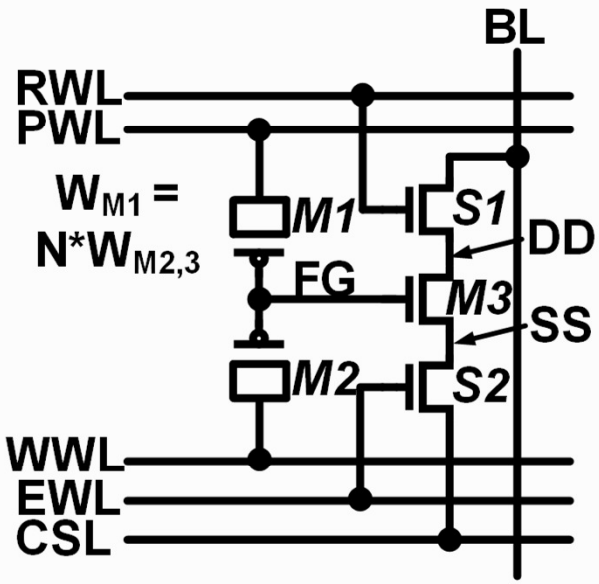


Coupling device Program/Read device Erase device

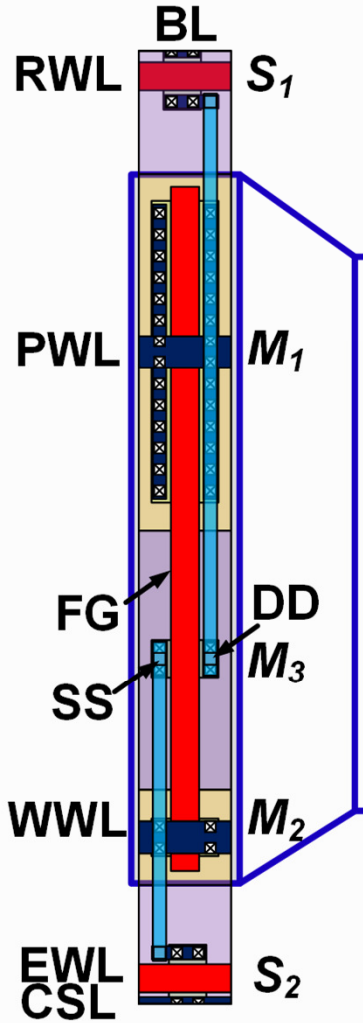
S. H. Song, *et al.*, JSSC, May 2013

- No process overhead, logic-compatible
- Floating gate formed by back-to-back gates.
- Higher coupling ratio reduces write voltage.

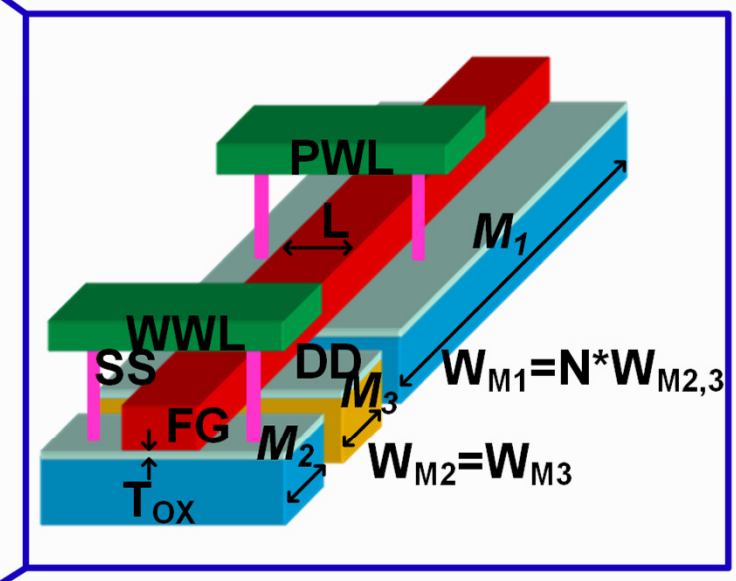
Logic Compatible Embedded Flash



Coupling ratio (CR) = N/(N+1)



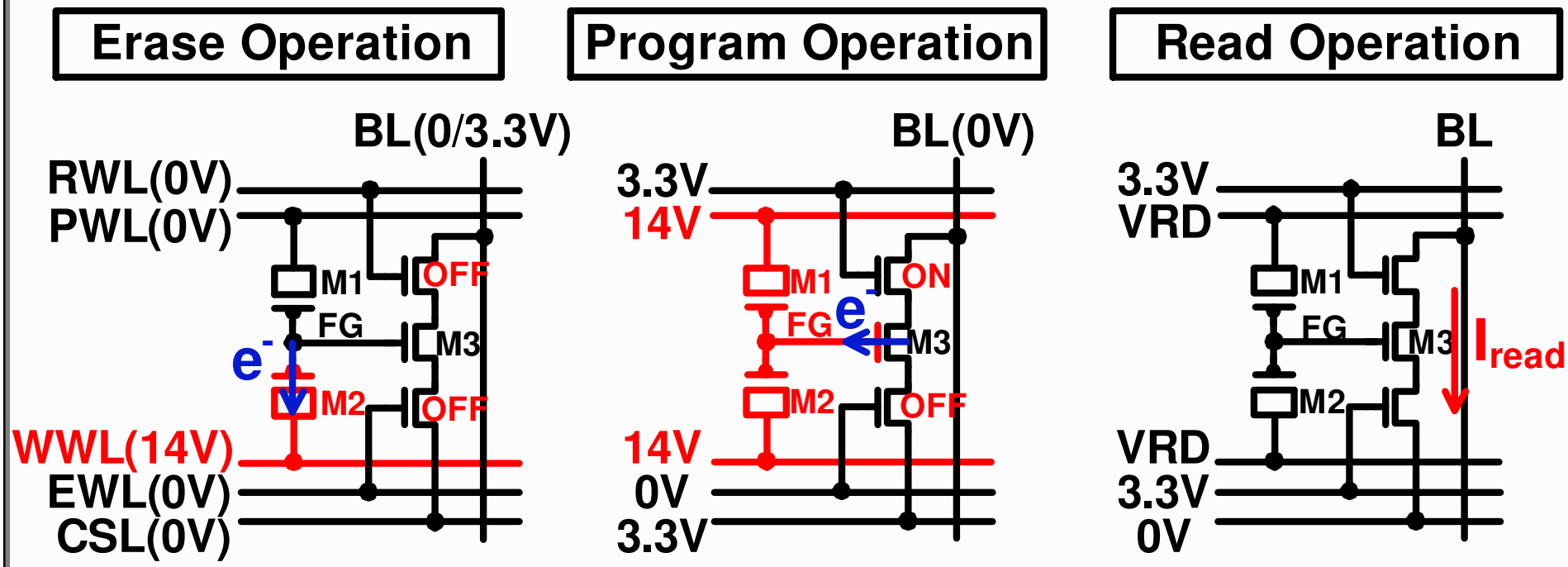
S. H. Song, *et al.*, JSSC, May 2013



5T Single-Poly (Core 3T)

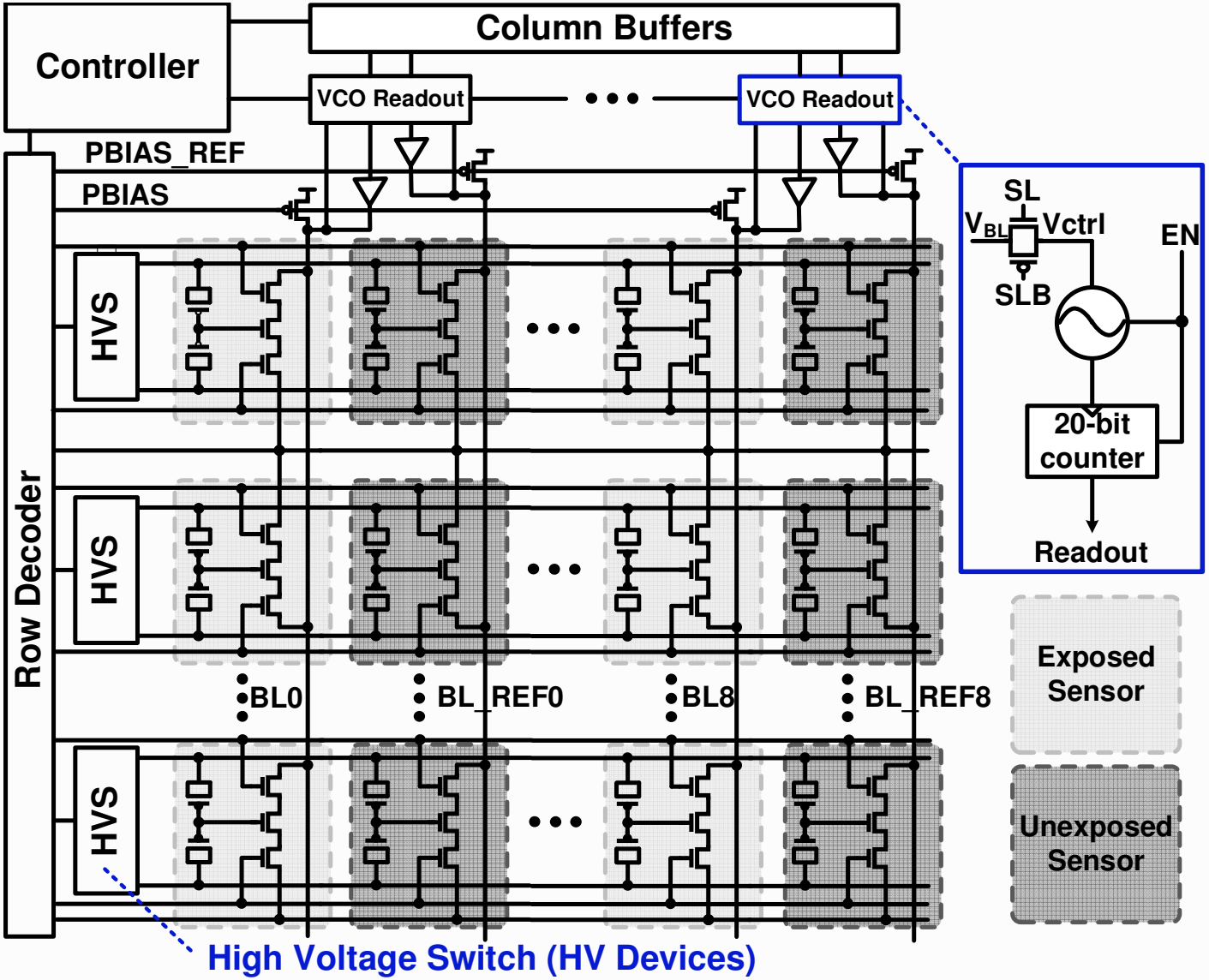
- **Coupling ratio determined by the sizing ratio between M1 and M2/3.**

Eflash Basic Operations

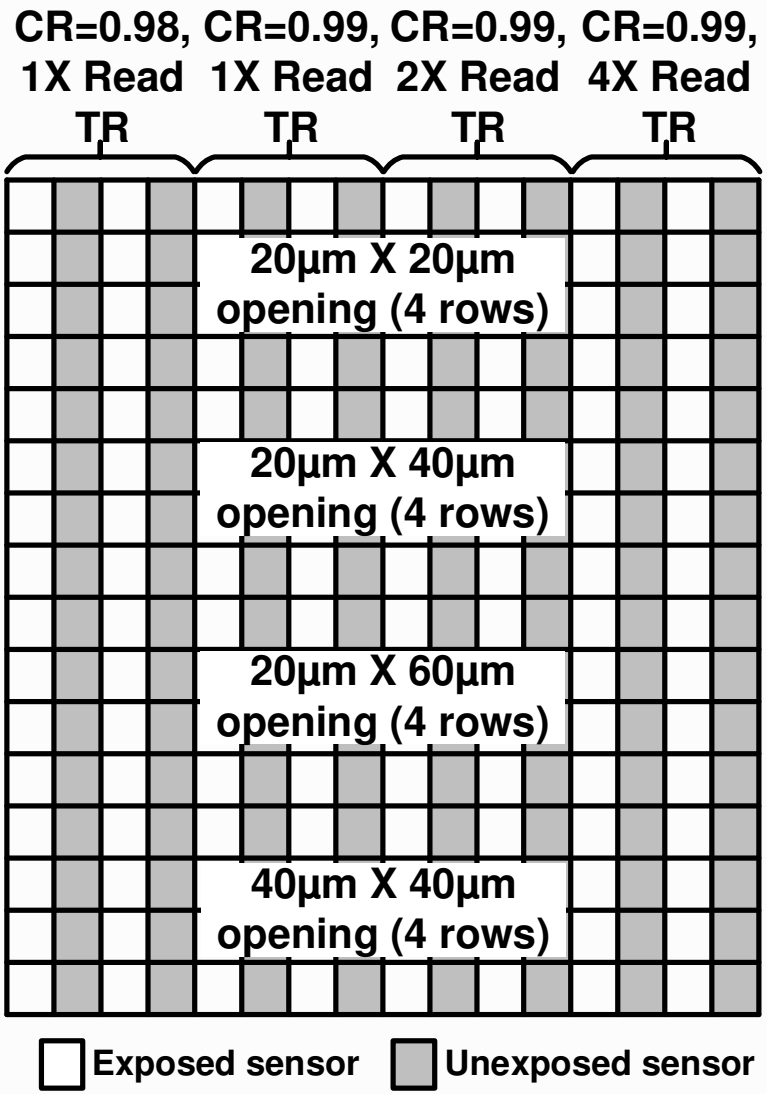


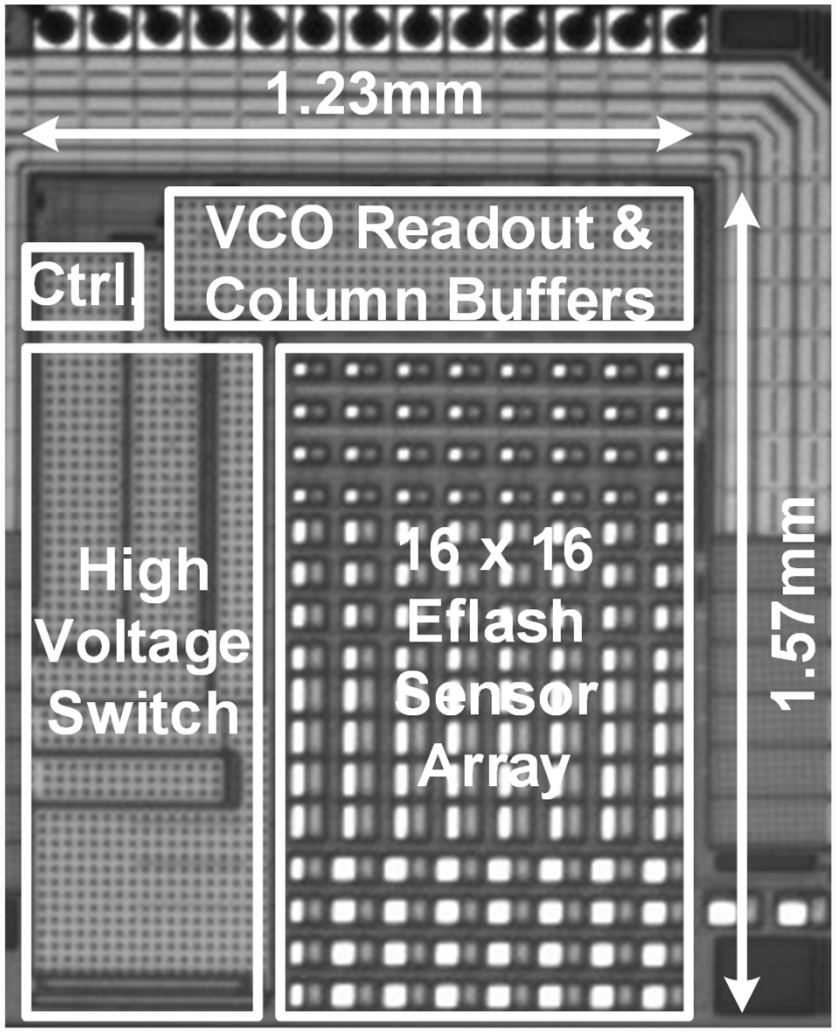
- **Erase and program mechanism: Fowler-Nordheim (FN) tunneling.**

16x16 Eflash Based Sensor Array



Sensor Configuration and Die Photo

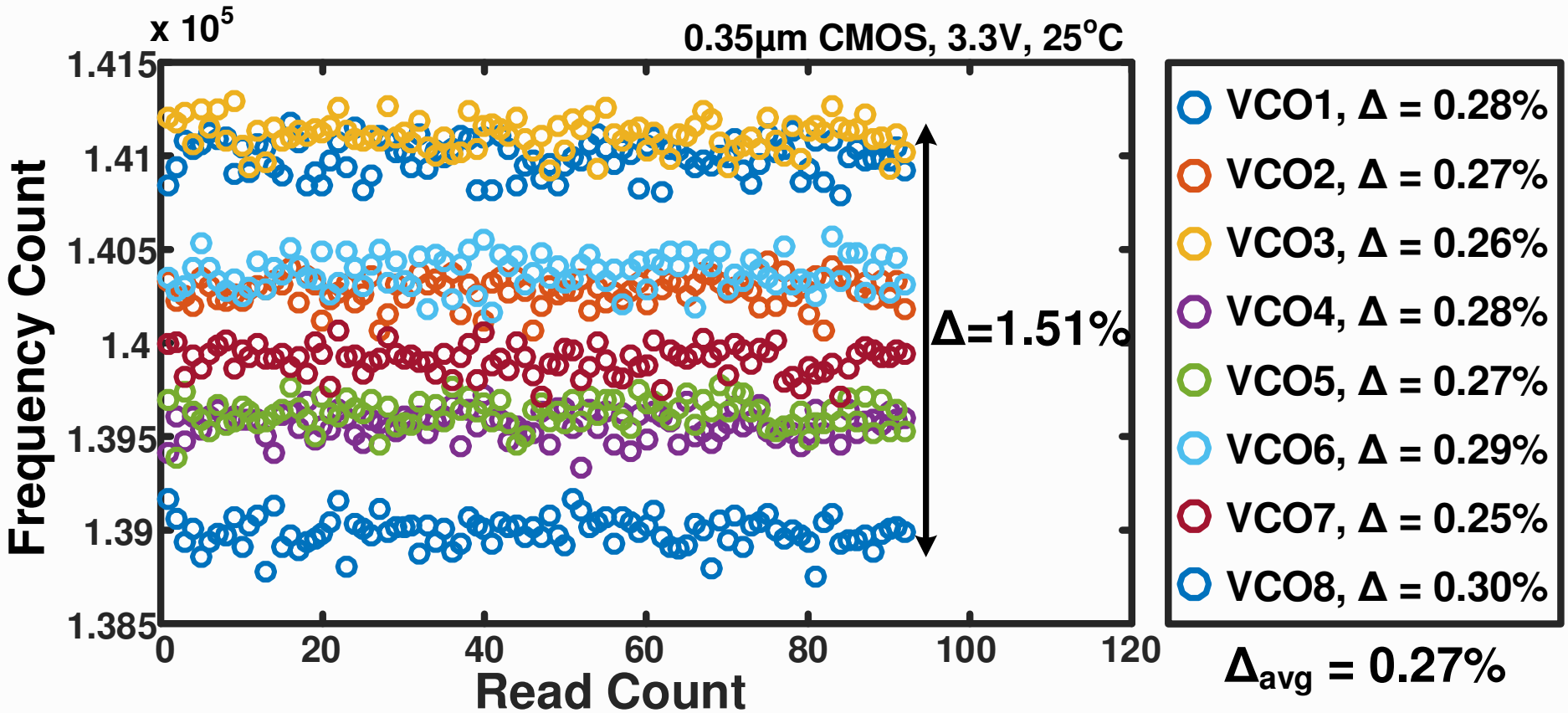




Outline

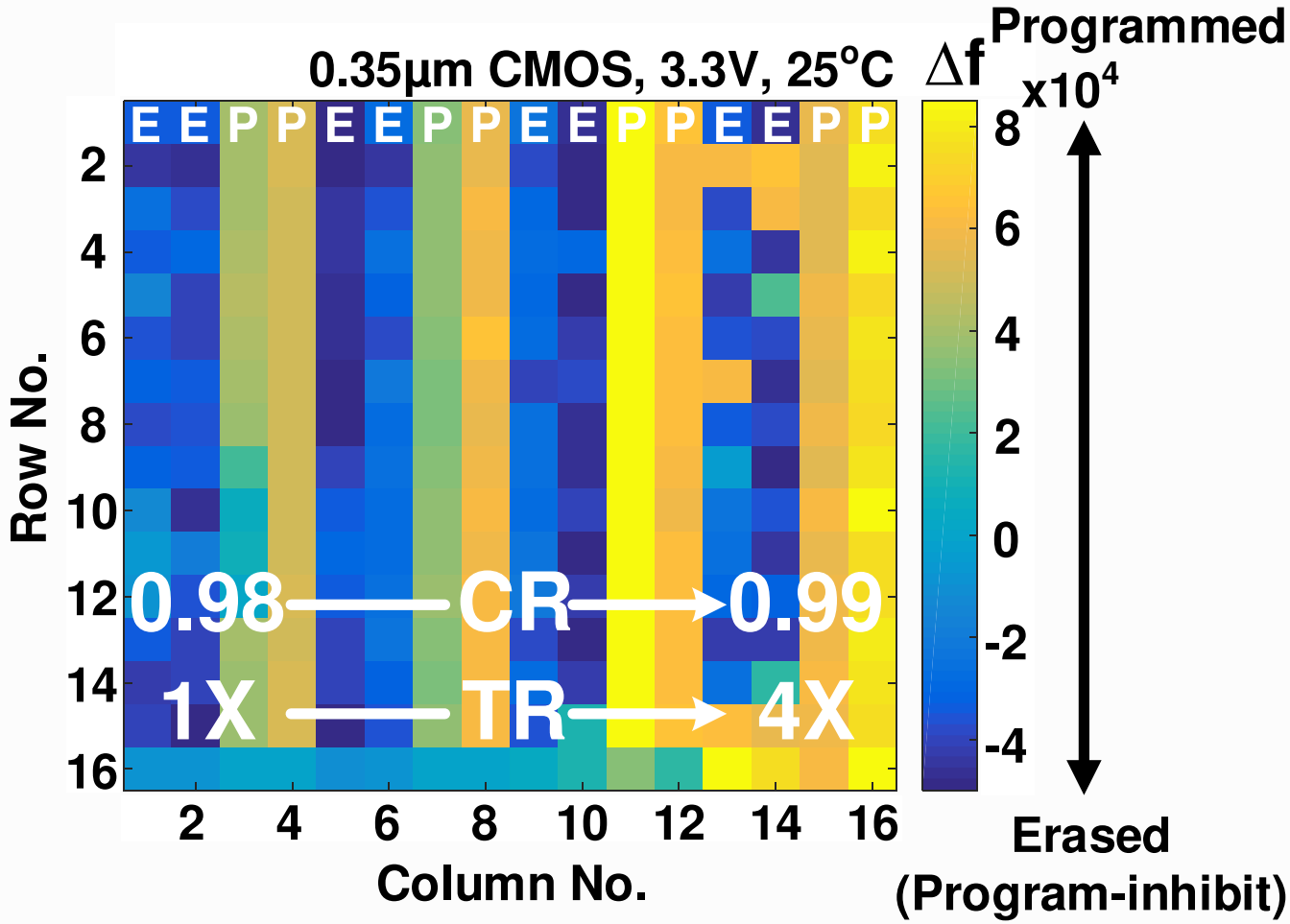
- Motivation
- Proposed counterfeit IC detection sensor
- **0.35µm test chip measurement results**
- Summary

Initial Frequency Characterization



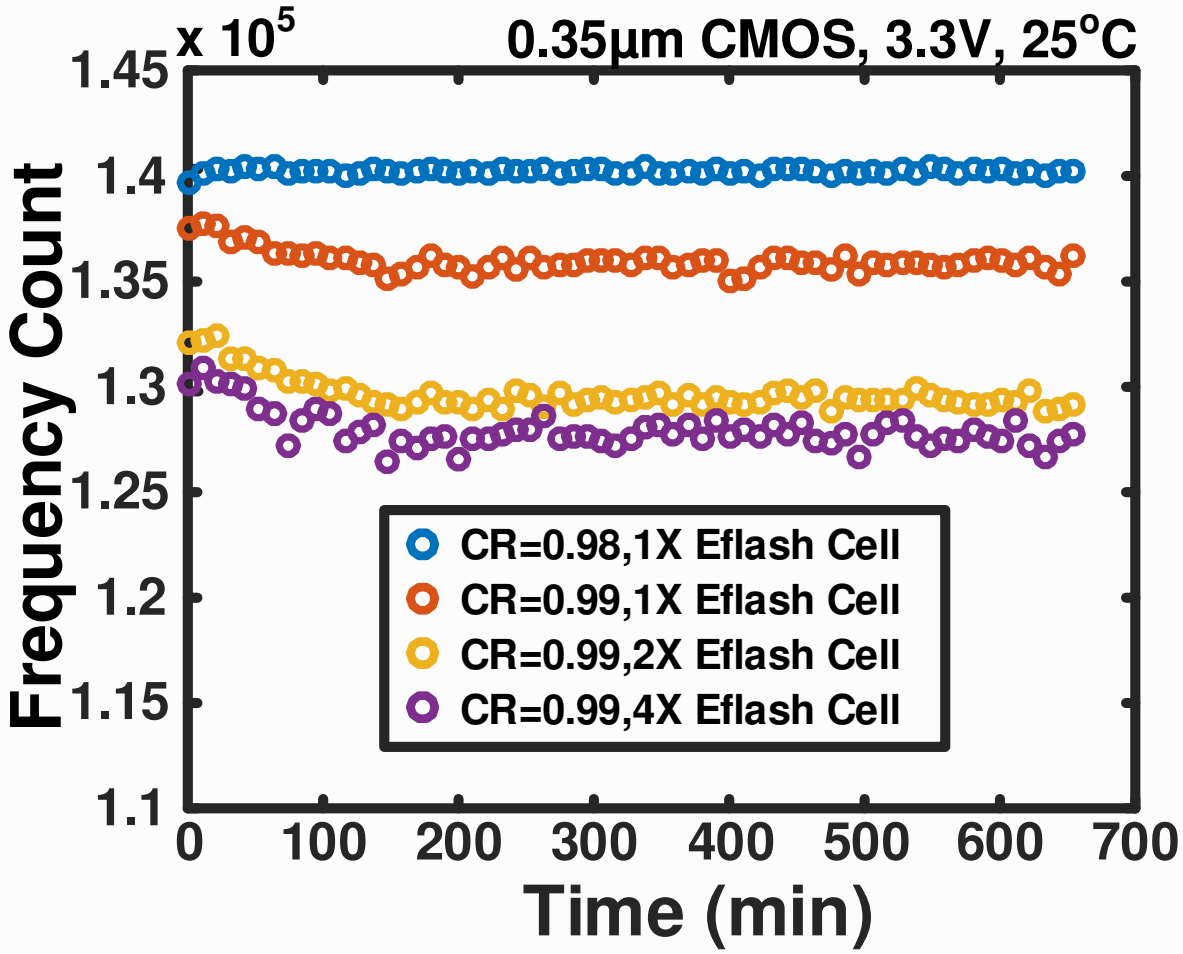
- **Negligible frequency difference/drift between consecutive samples**

Eflash Array Frequency Change Map



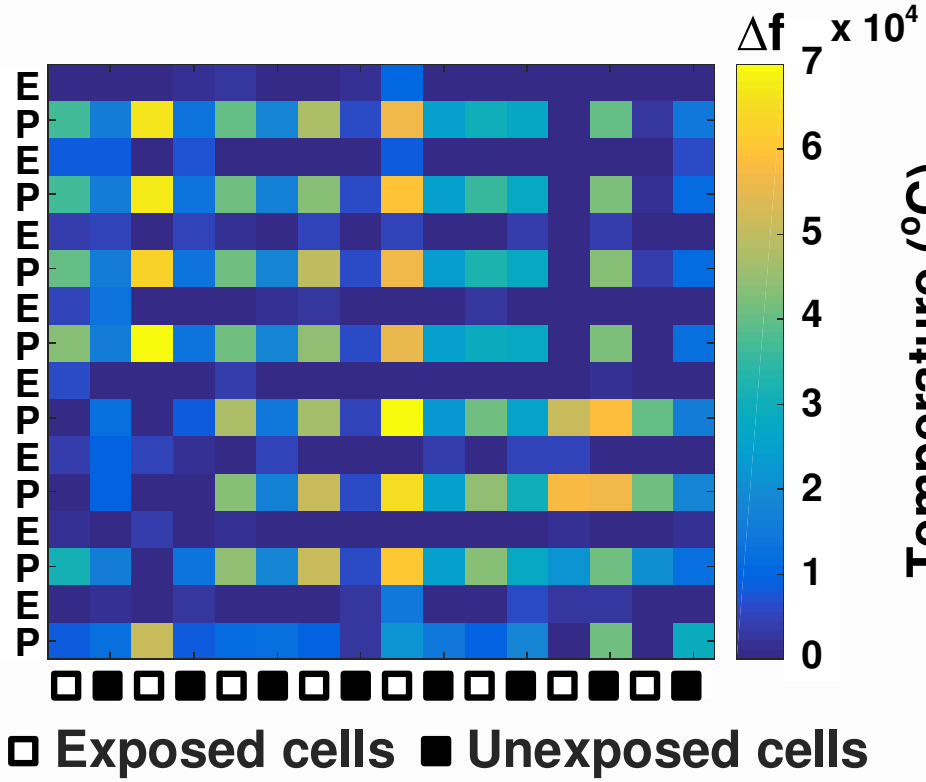
- Higher coupling ratio (CR), larger transistors → more efficient erase/program.

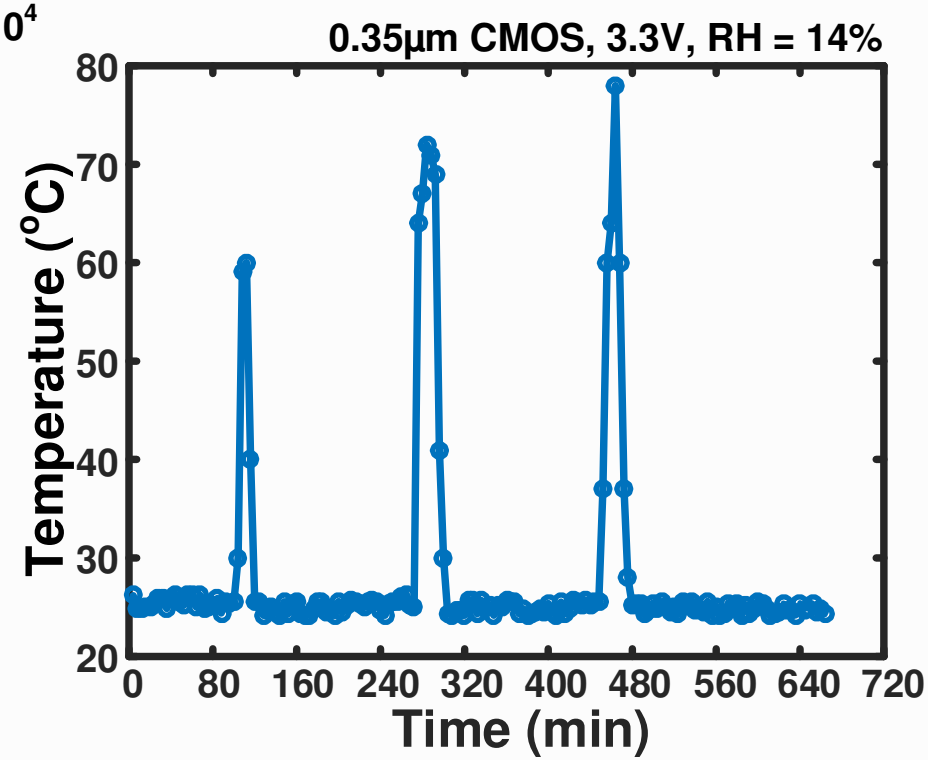
Retention Characteristics



- **Robust retention characteristics if not tampered.**

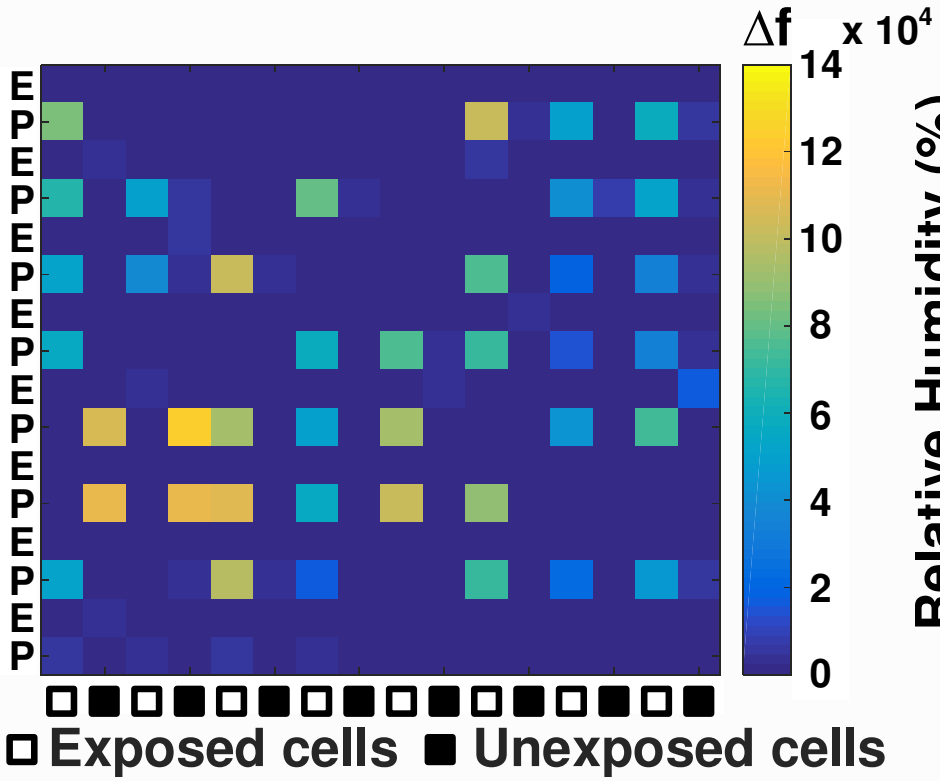
Temperature Attack Results

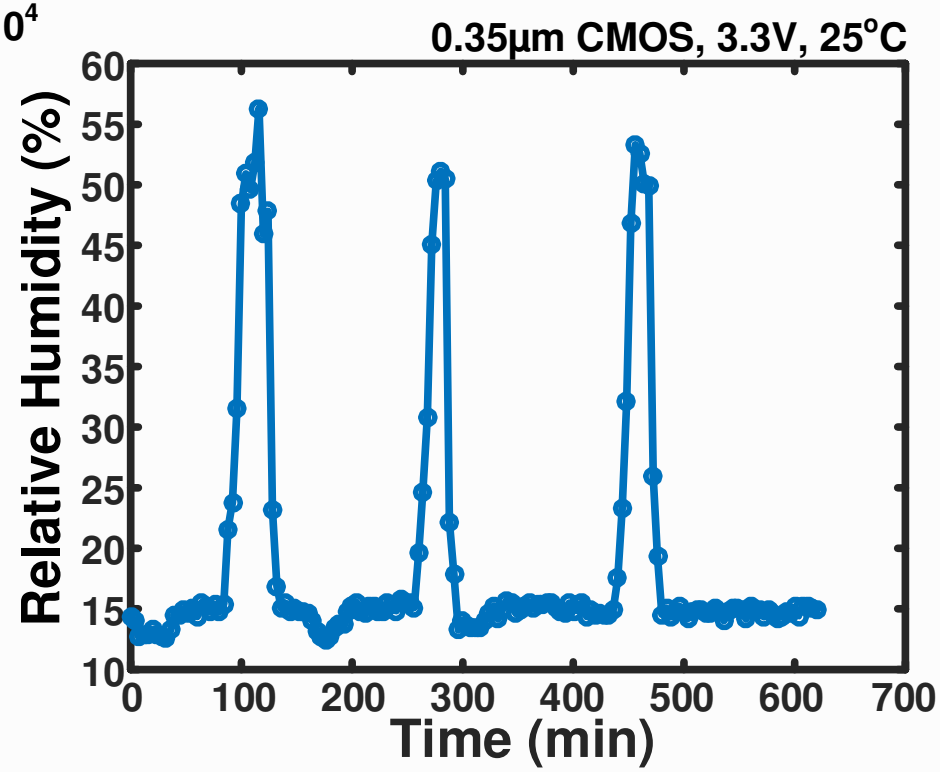




- **Alternate rows are erased/programmed for better charge collection.**
- **Frequency change occurs in programmed cells.**

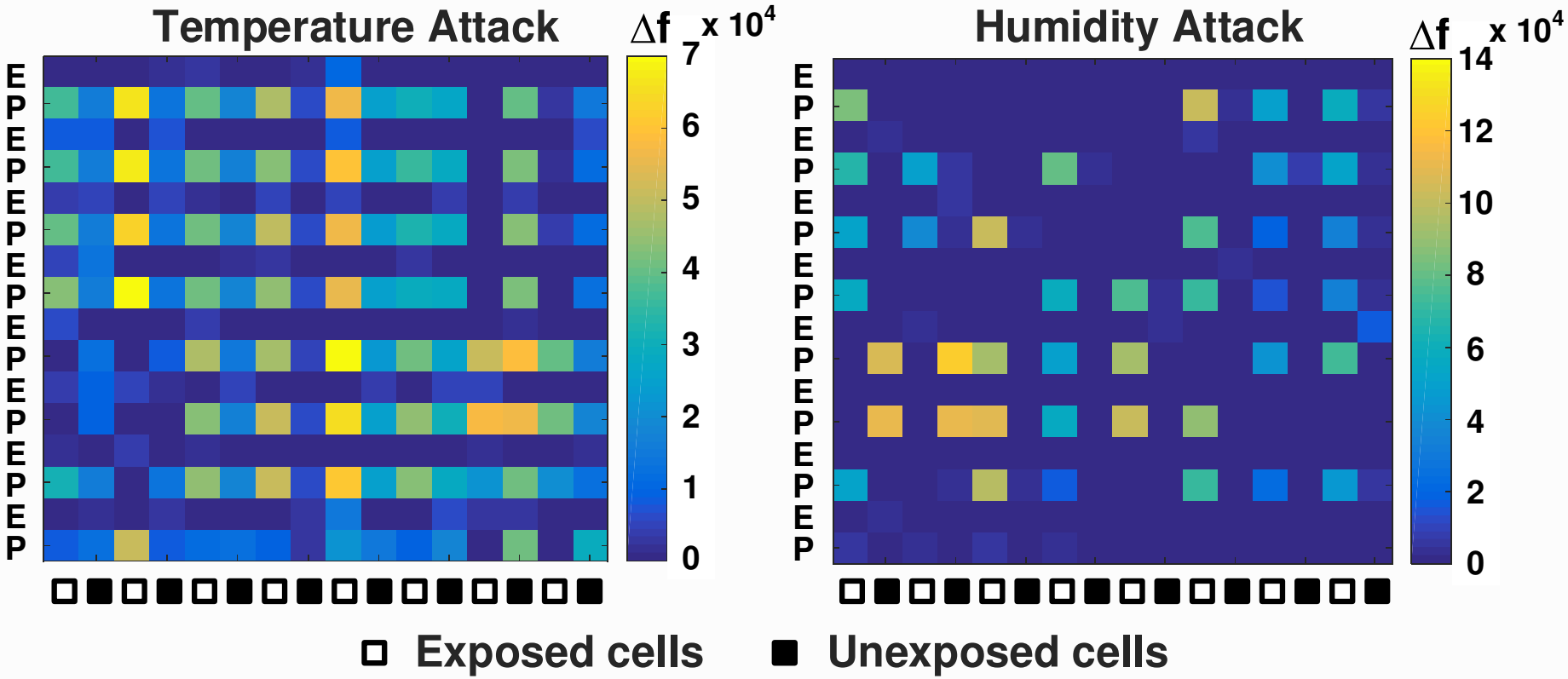
Humidity Attack Results





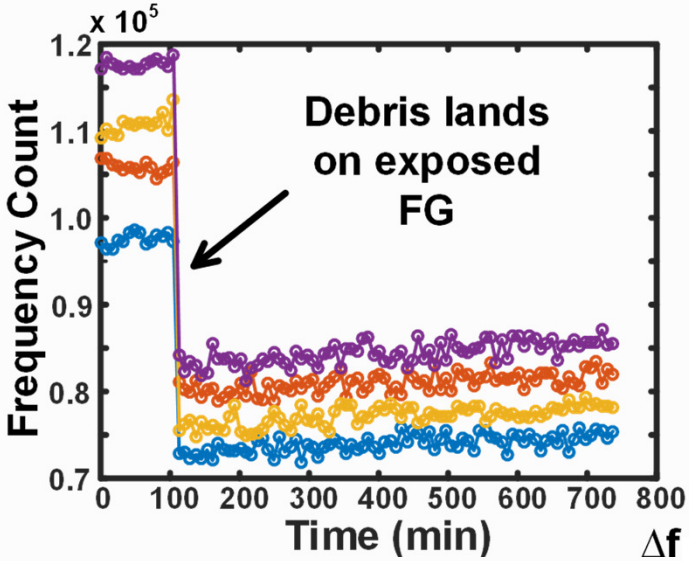
- **Alternate rows are erased/programmed for better charge collection.**
- **Frequency change occurs in programmed cells.**

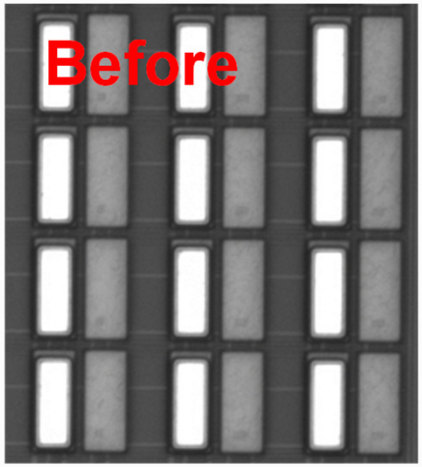
Temperature vs. Humidity Attack

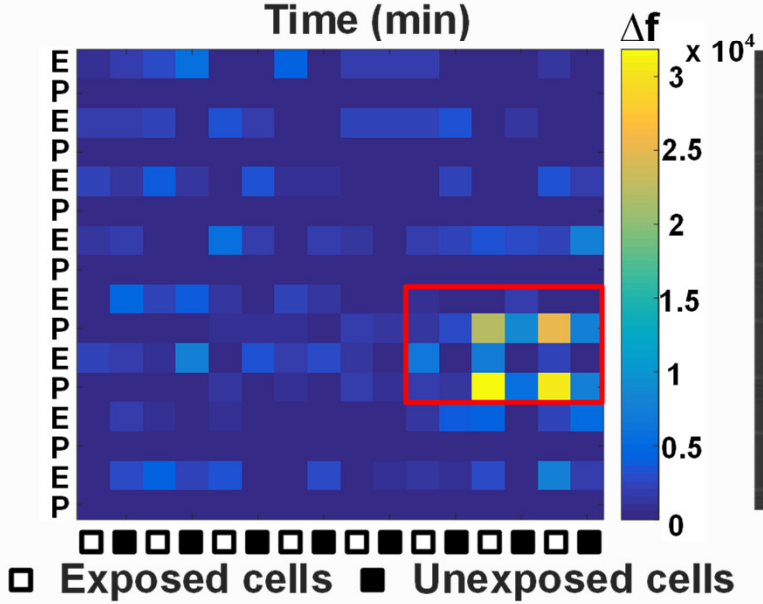


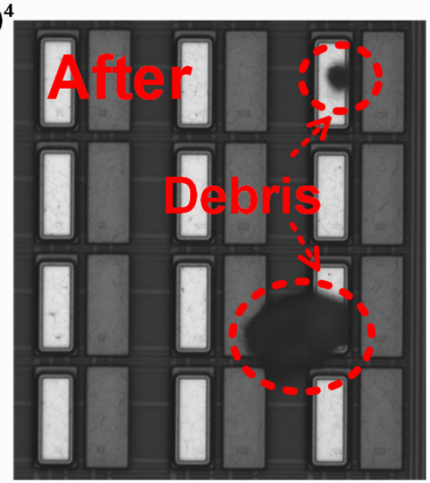
- **Smaller frequency shift in unexposed cells for both type of attacks**

Particle/Debris Attack Results









Summary

- A powerless and non-volatile eflash based counterfeit IC detection sensor demonstrated
- 0.35µm test chip measurement results
  - Temperature attack.
  - Humidity attack.
  - Particles/debris attack.