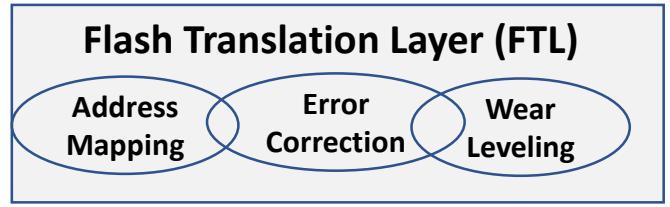
Data Recovery from “Scrubbed” NAND Flash Storage: Need for Analog Sanitization

Md Mehedi Hasan and Biswajit Ray

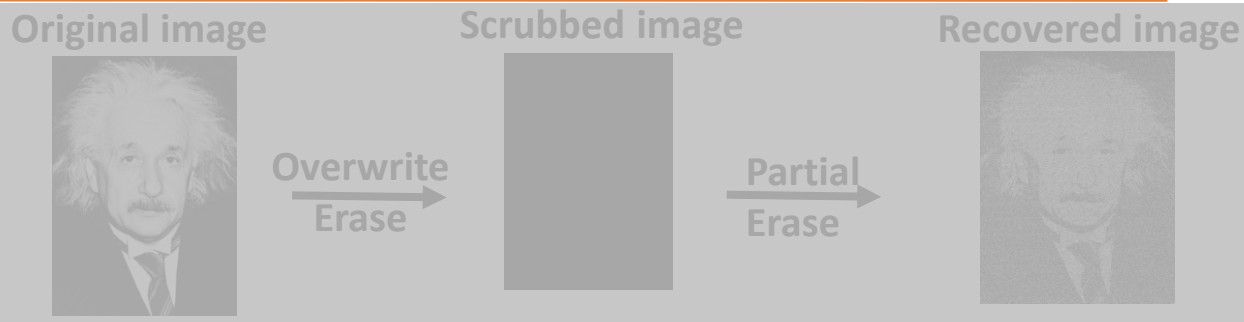
Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, AL 35899 USA

Outline

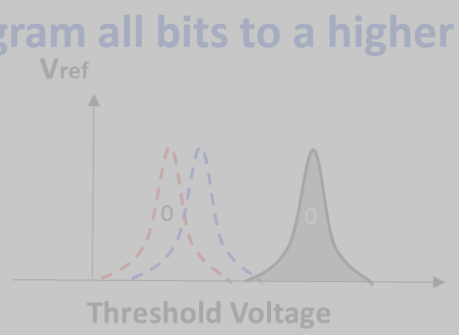
- **Motivation and background**
  - NAND memory system
  - State-of-the-art sanitization methods
  - Threat model

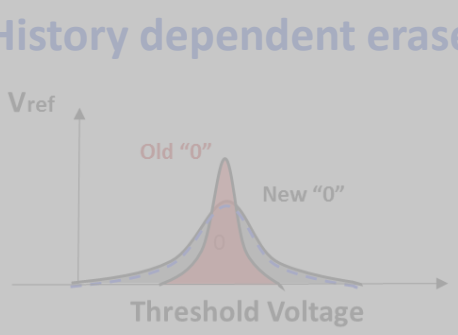


- **Experimental evaluation**
  - Attack demonstration
  - Bit recovery efficiency



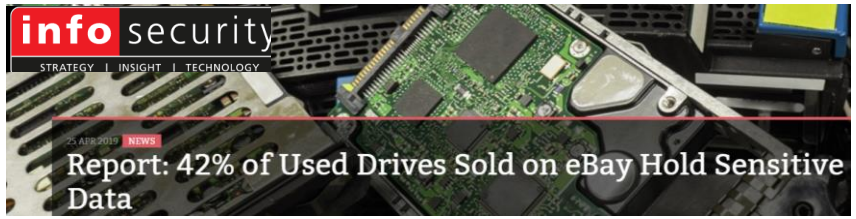
- **New ideas and conclusion**
  - Page-level analog sanitization
  - Future work





Motivation: Preserving user privacy

- According to the Data Protection Act (DPA) 2018, the deletion of information must be real
- Unfortunately, flash users don't have the capability for instant data sanitization



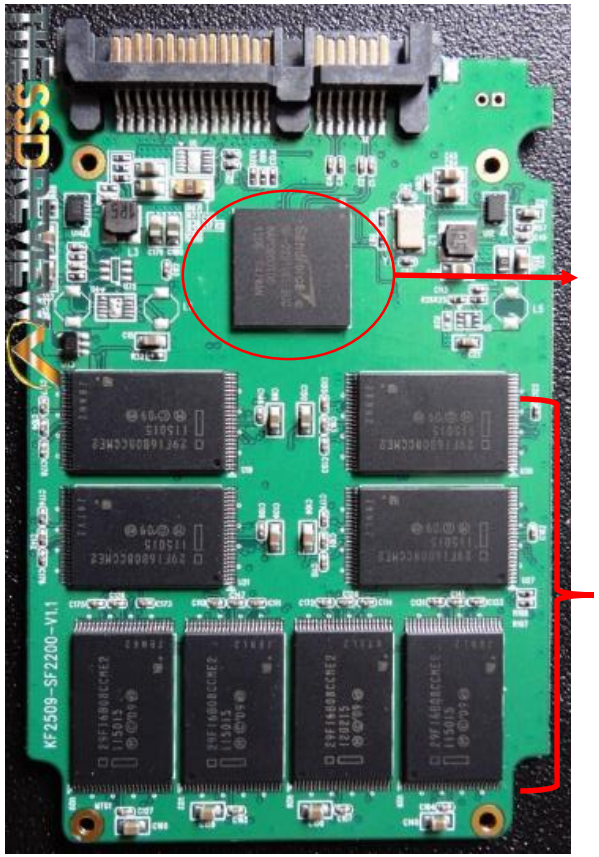
42% of used SSDs and HDDs sold on eBay contain PII & enterprise data

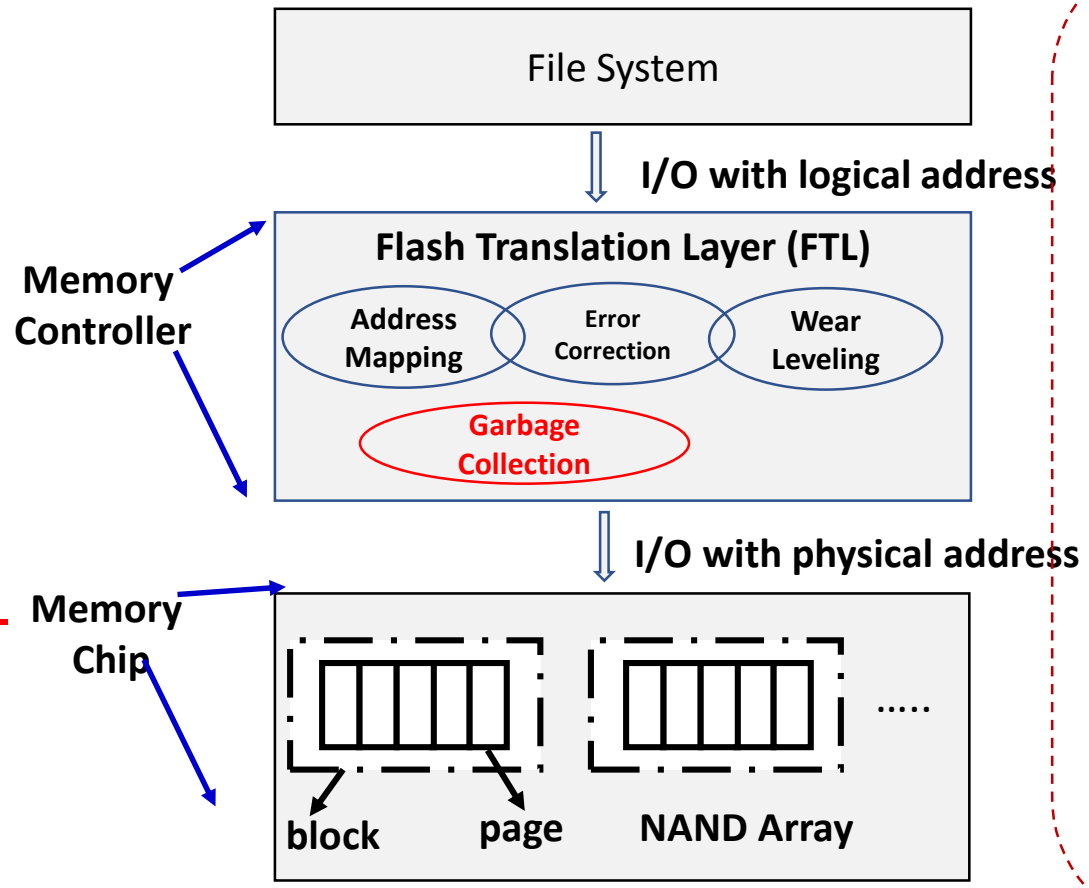
14 May 2019 | Author: Jay Jay

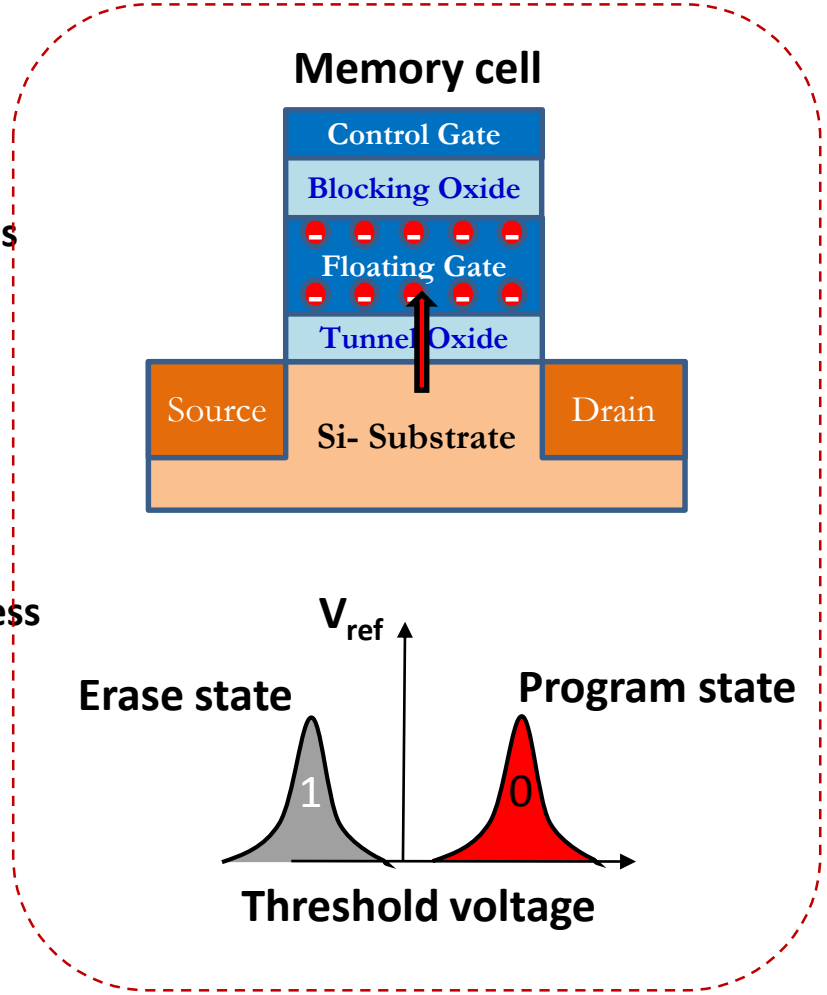
Data remains in the non-volatile flash media long after user-deletion

Background: NAND flash memory system

Solid State Drive

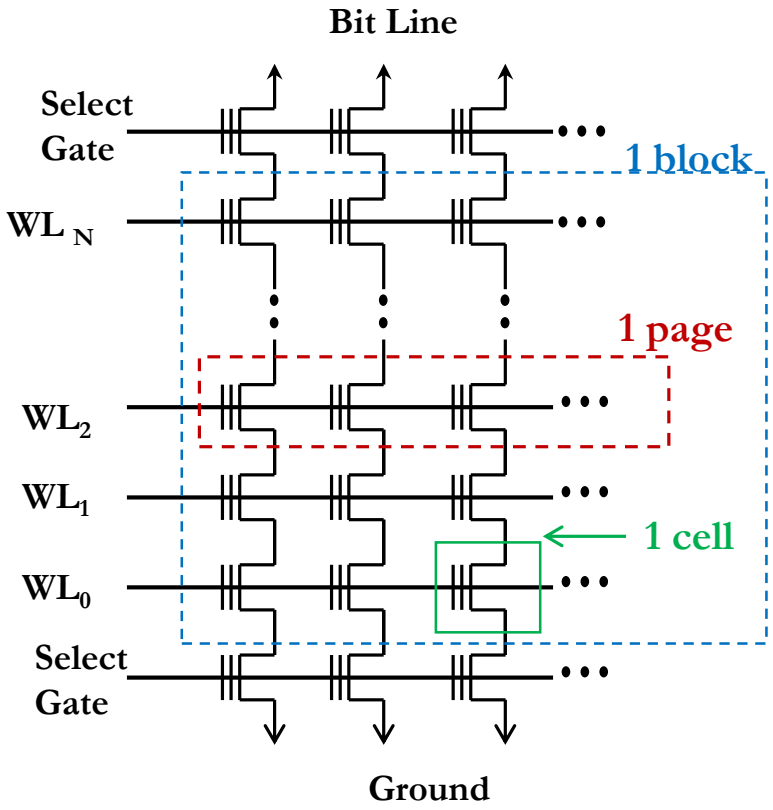


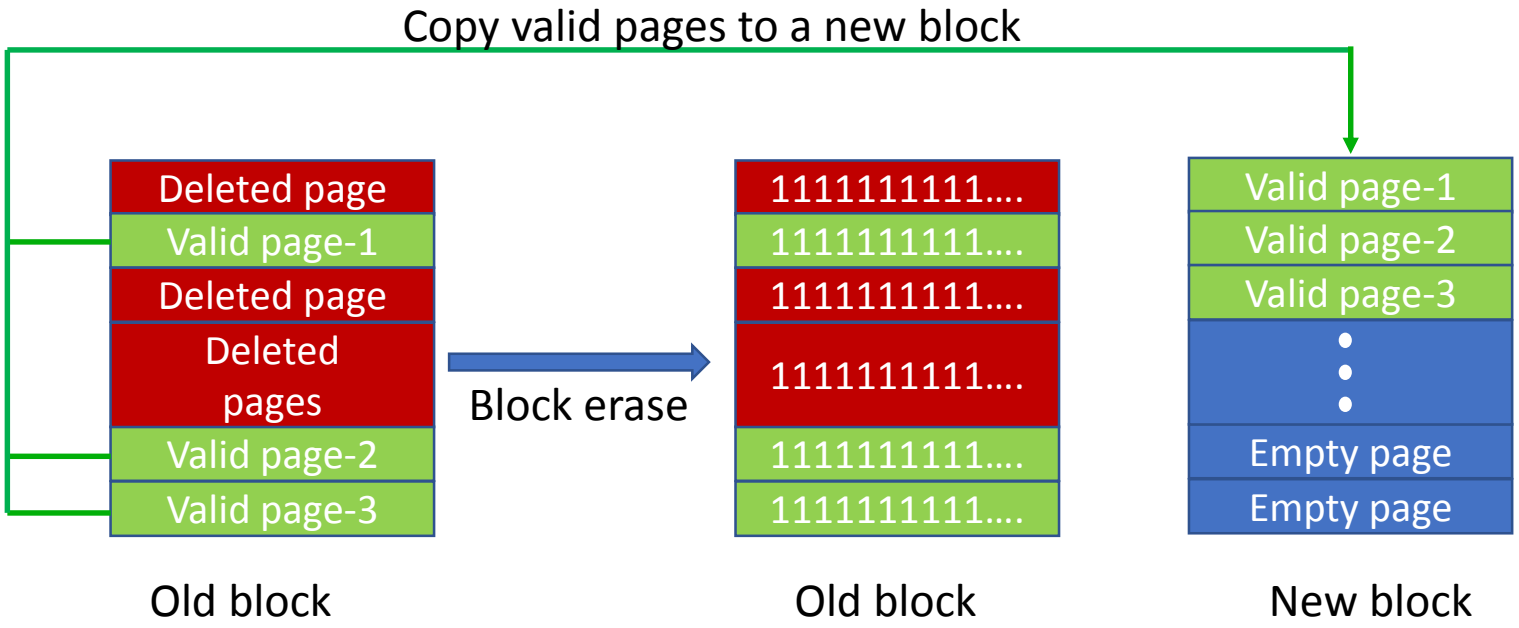




Flash is a charge based analog memory

Why instant-sanitization is a problem?



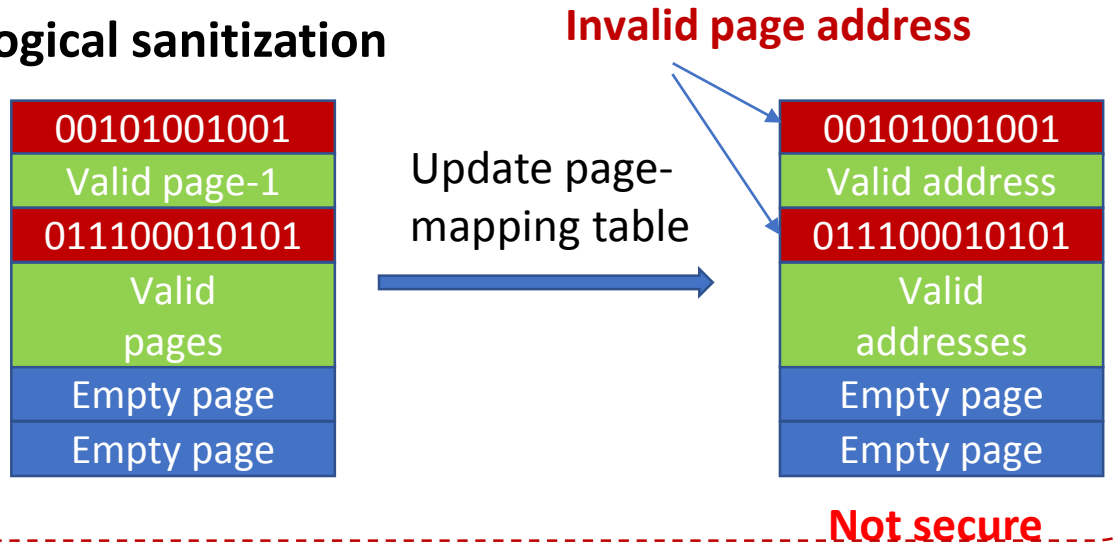


- Erase takes place block by block
- Write/read happens page by page

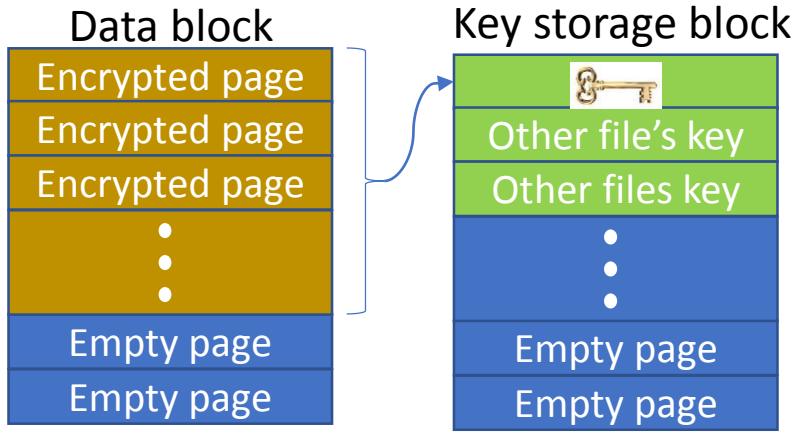
- Hefty overhead is involved for using block erase
- No command is available for page deletion

State-of-the-art sanitization methods

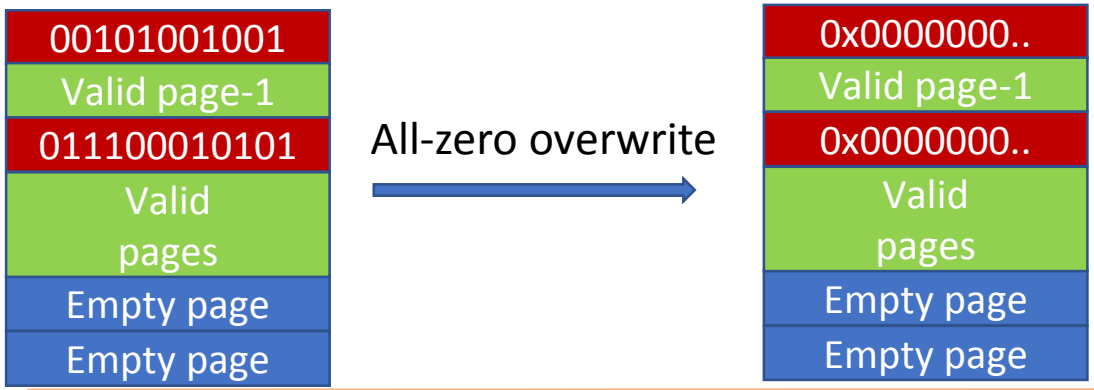
1) Logical sanitization



2) Encryption based sanitization



3) Over-write based sanitization

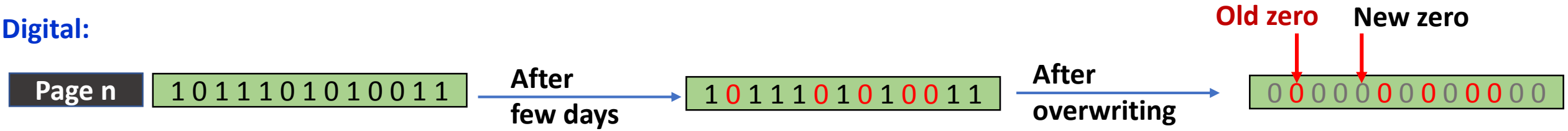


Key points:

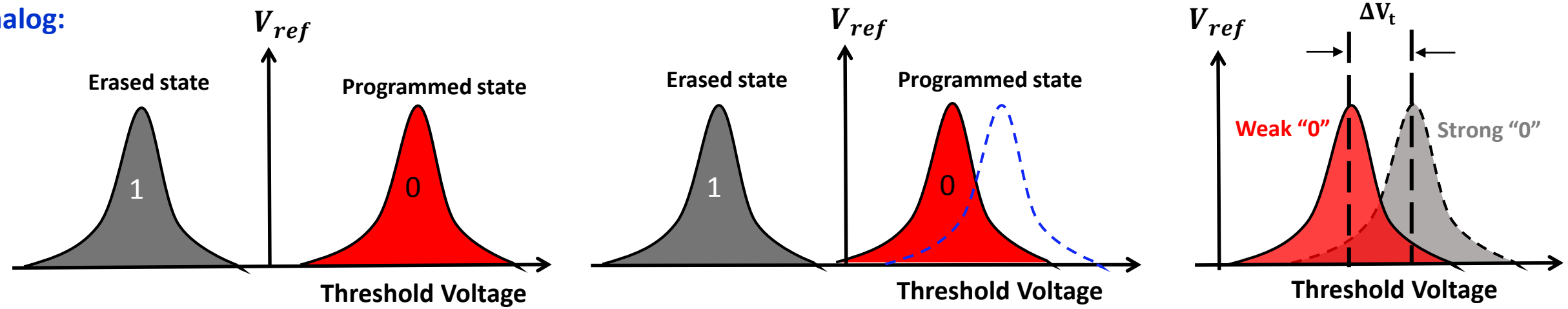
- **Logical sanitization is quick but not secure**
- **Encryption techniques are used in high end system. It also needs key-sanitization.**
- **All-zero overwrite offers page level digital sanitization**

Does all-zero overwrite ensure true sanitization?

Digital:



Analog:

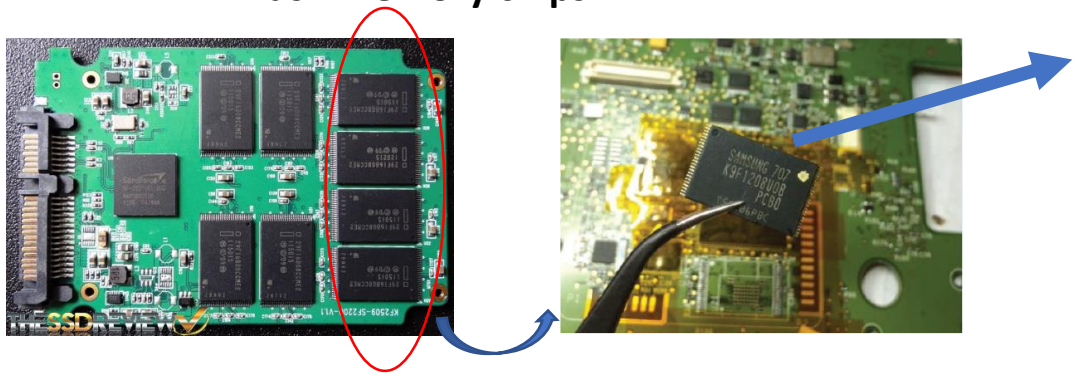


Key points:

- **Flash memory slowly loses charge due to data retention effects**
- **All-zero overwrite crates strong and weak zeros with different threshold voltages**

Threat model and experimental set-up

Flash memory chips



Adversarial Model and Assumptions:

- Adversary has physical access to the flash chip
- Adversary can perform low-level memory operation

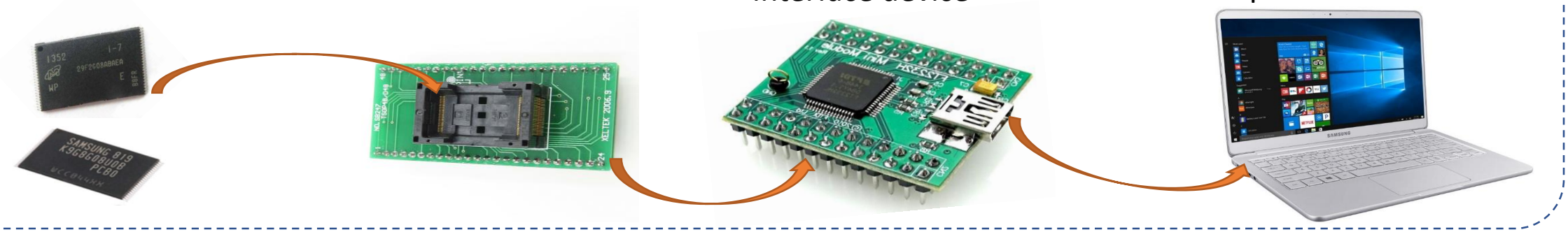
Our Experimental Set-up

Flash memory chip

TSOP Socket

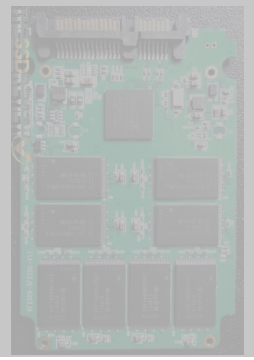
Interface device

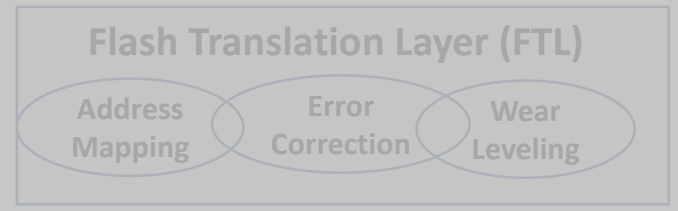
Computer interface



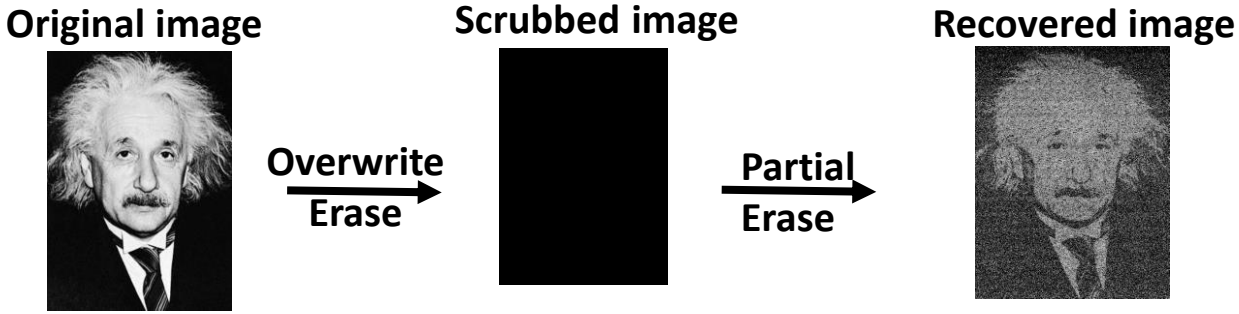
Outline

- Motivation and background
  - NAND memory system
  - State-of-the-art sanitization methods
  - Threat model

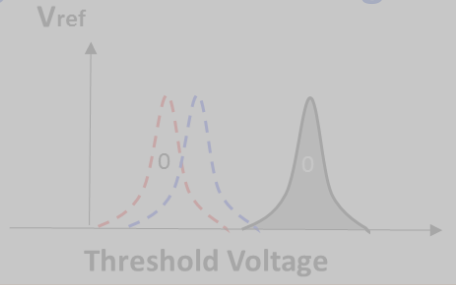


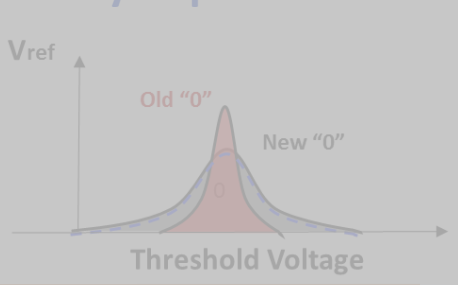


- **Experimental evaluation**
  - Attack demonstration
  - Bit recovery efficiency



- New ideas and conclusion
  - Page-level analog sanitization
  - Future work

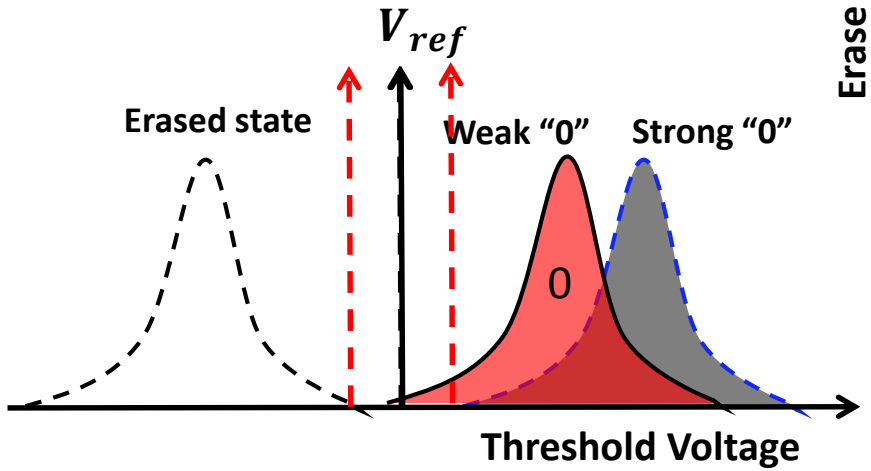


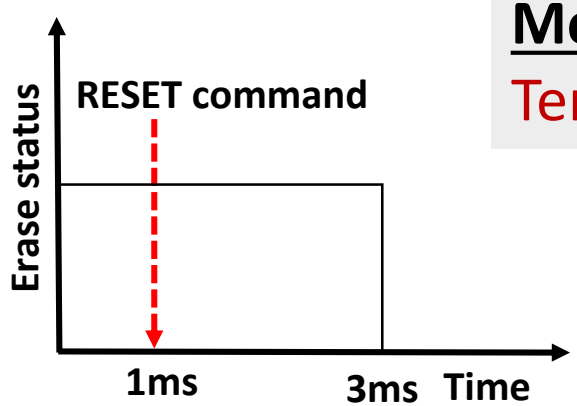


System commands to probe analog properties

Method-1: Read Retry

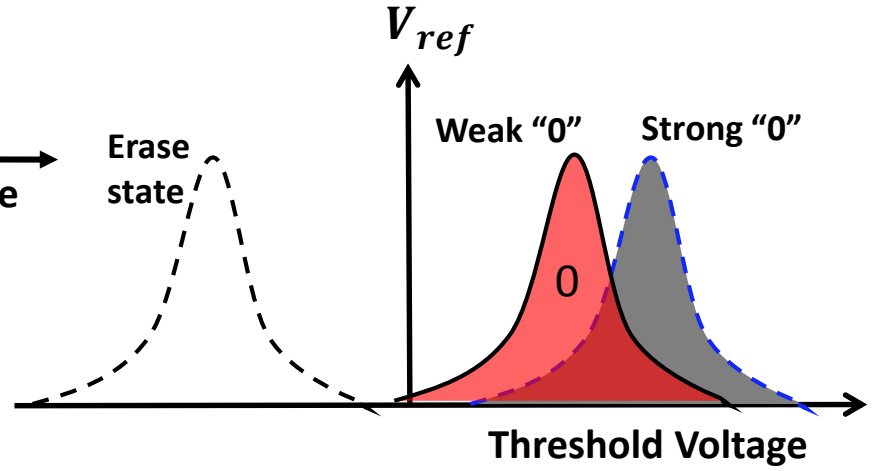
Shifting the read reference level





Method-2: Partial Erase

Terminate erase prematurely



Key points:

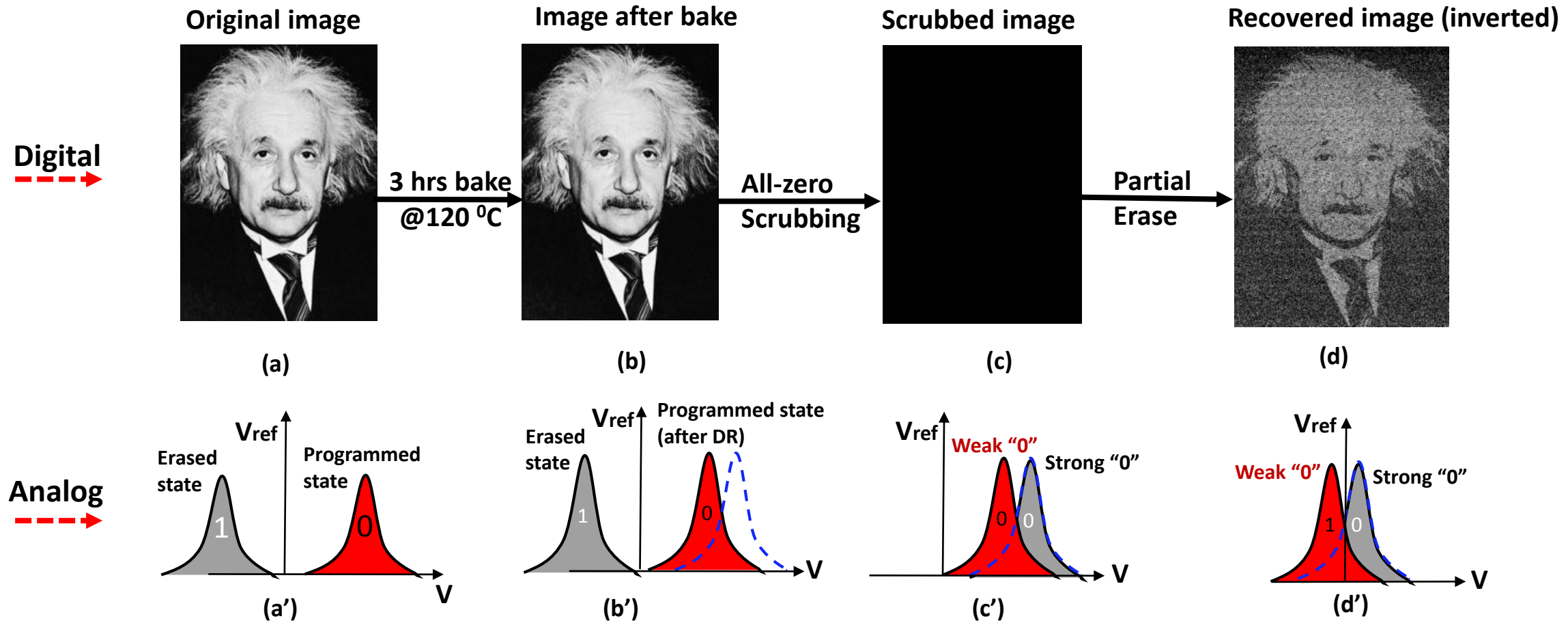
- **Many SLC chips do not offer this feature**
- **Very small voltage (V_{ref}) shifts are allowed**

Key points:

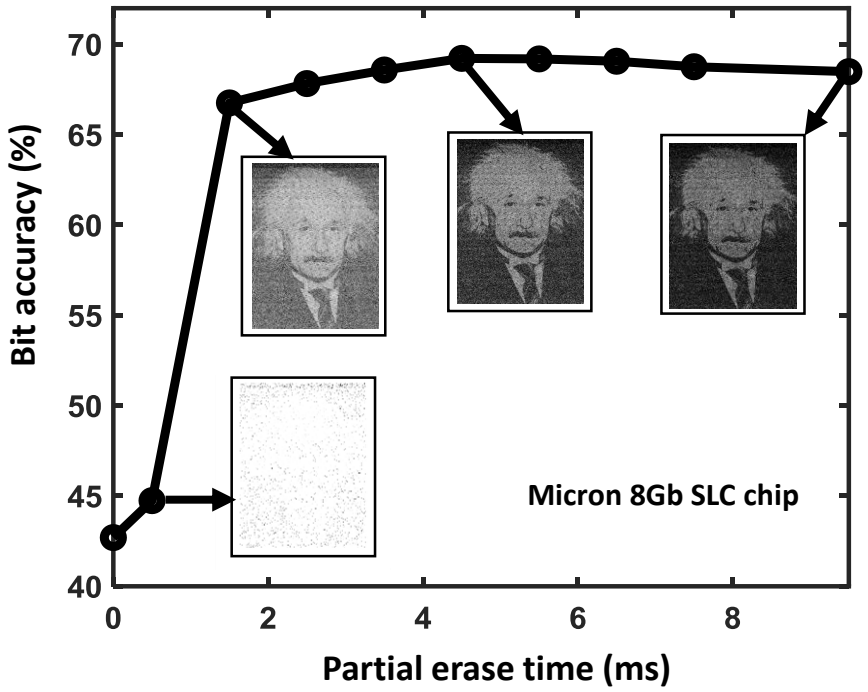
- **Prior characterization of partial erase time is needed**

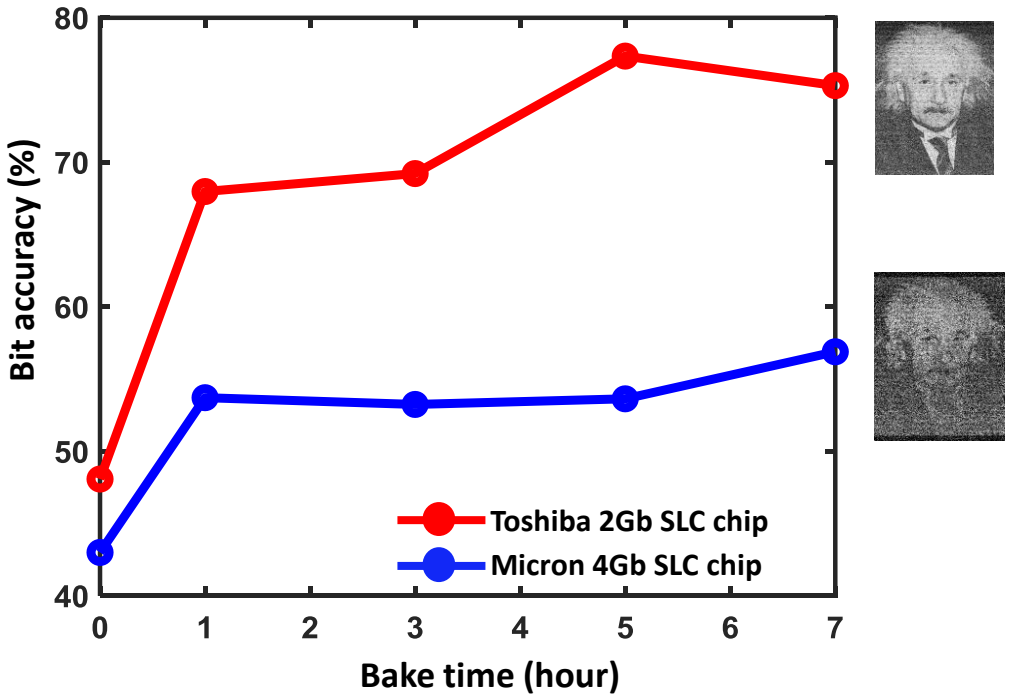
Results: Data recovery process

Data recovery process



Results: Bit accuracy of recovered image



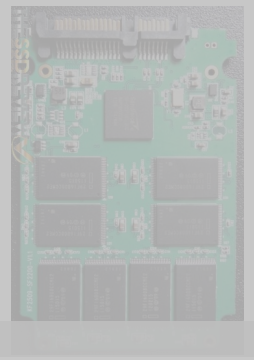


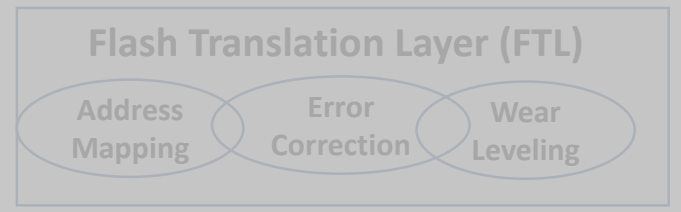
Key points:

- **Approximately 70% bits are correct in the recovered image**
- **Higher the bake time more is recovery efficiency**
- **All the bits are not recoverable due to overlap in Vt distribution**

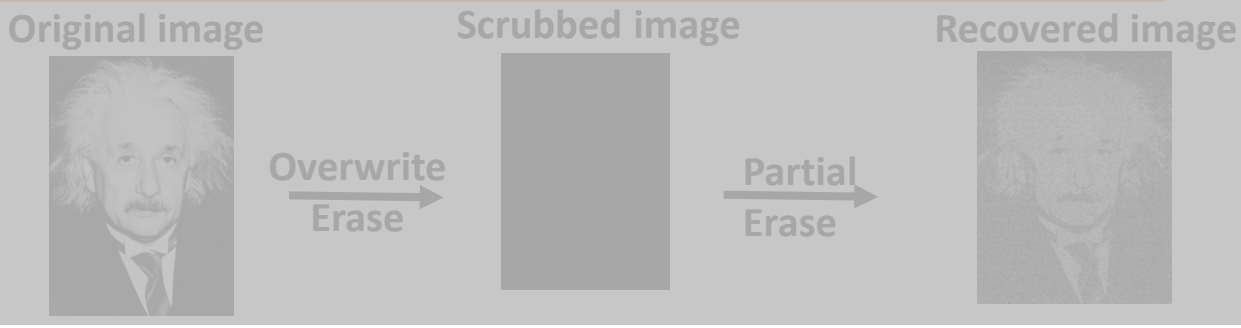
Outline

- **Motivation and background**
  - NAND memory system
  - State-of-the-art sanitization methods
  - Threat model



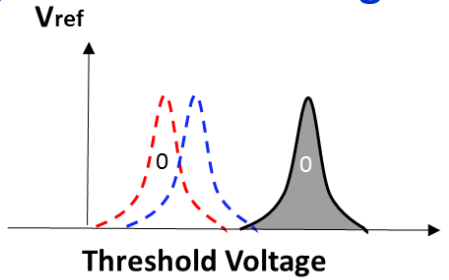


- **Experimental evaluation**
  - Attack demonstration
  - Bit recovery efficiency

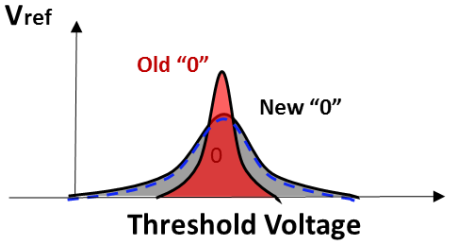


- **New ideas and conclusion**
  - Page-level analog sanitization
  - Future work

1. Reprogram all bits to a higher value

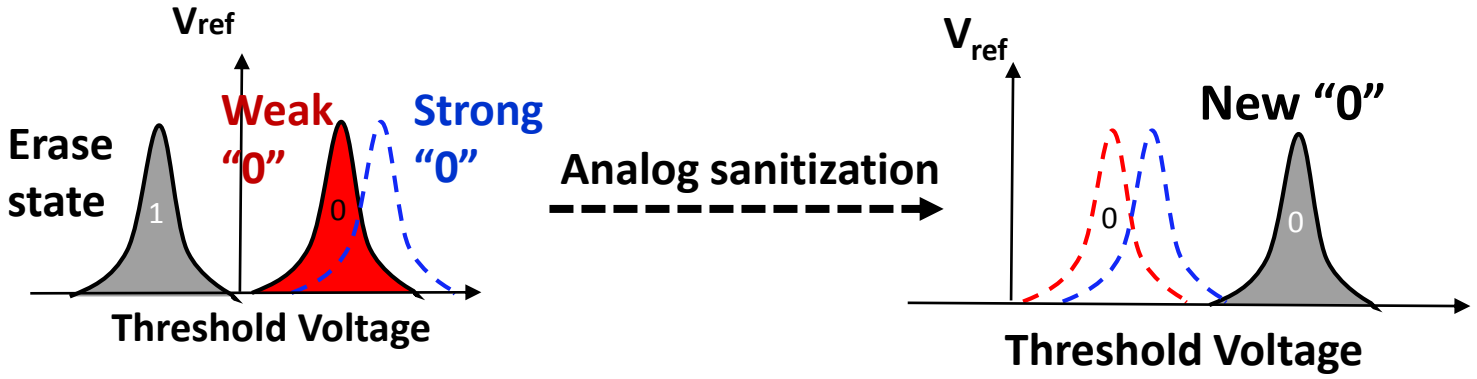


2. History dependent erase



Ideas for analog sanitization

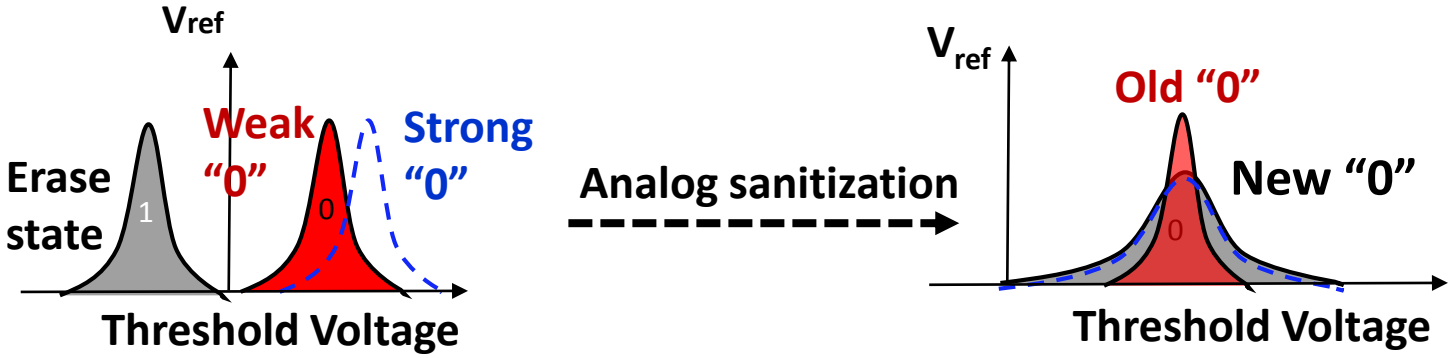
Idea-1: Reprogram all the bits to a higher threshold voltage level



Key points:

- Need design change of flash chip
- Not possible with current chips

Idea-2: Create weak zeros during all-zero overwrite using page creation history

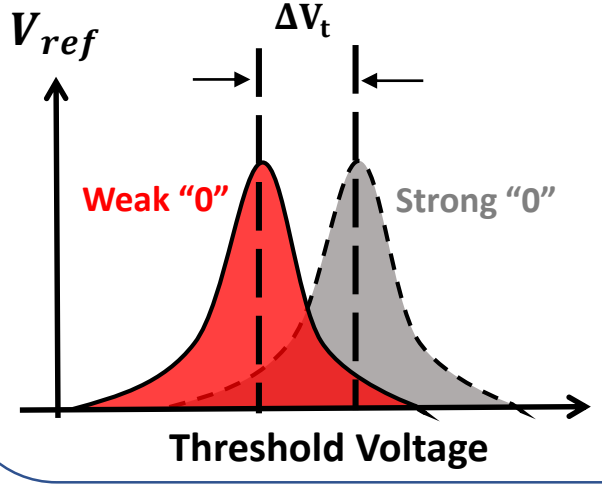


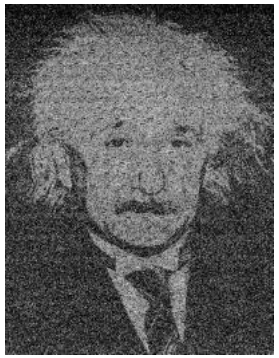
Key points:

- Use partial program for weak-zero creation
- Partial program time depends on state-decay model

Conclusion and future work

1) All-zero overwrite is vulnerable



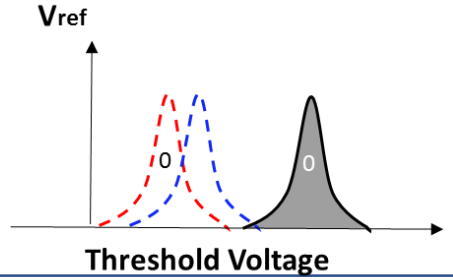


Future Work:

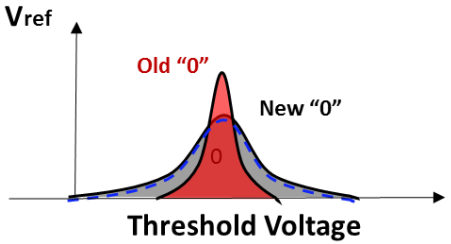
1. Attack demonstration on MLC, TLC and 3D NAND
2. Experimental evaluation of the new ideas

2) New ideas for page-level analog sanitization

1. Reprogram all bits to high voltage



2. History dependent weak-zero erase



Thank You

Mr. Md Mehedi Hasan

email: mh0145@uah.edu

Dr. Biswajit Ray

email: biswajit.ray@uah.edu