DFRWS

Improving the Reliability of Chip-Off Forensic Analysis of NAND Flash Memory Devices

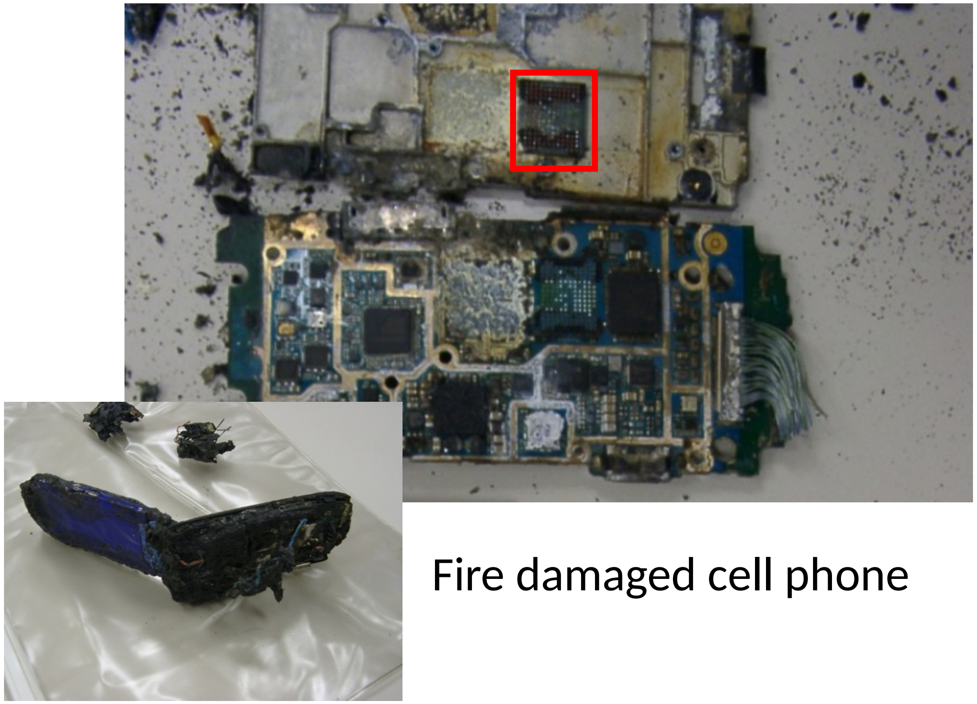
Aya Fukami, Saugata Ghose, Yixin Luo, Yu Cai, Onur Mutlu

National Police Agency
JAPAN

Carnegie Mellon

ETH zürich

Example Target Devices for Chip-Off Analysis



Fire damaged cell phone

Water damaged smartphone

No way to boot those devices:
investigators turn to chip-off forensic analysis

Chip-Off Forensic Procedure

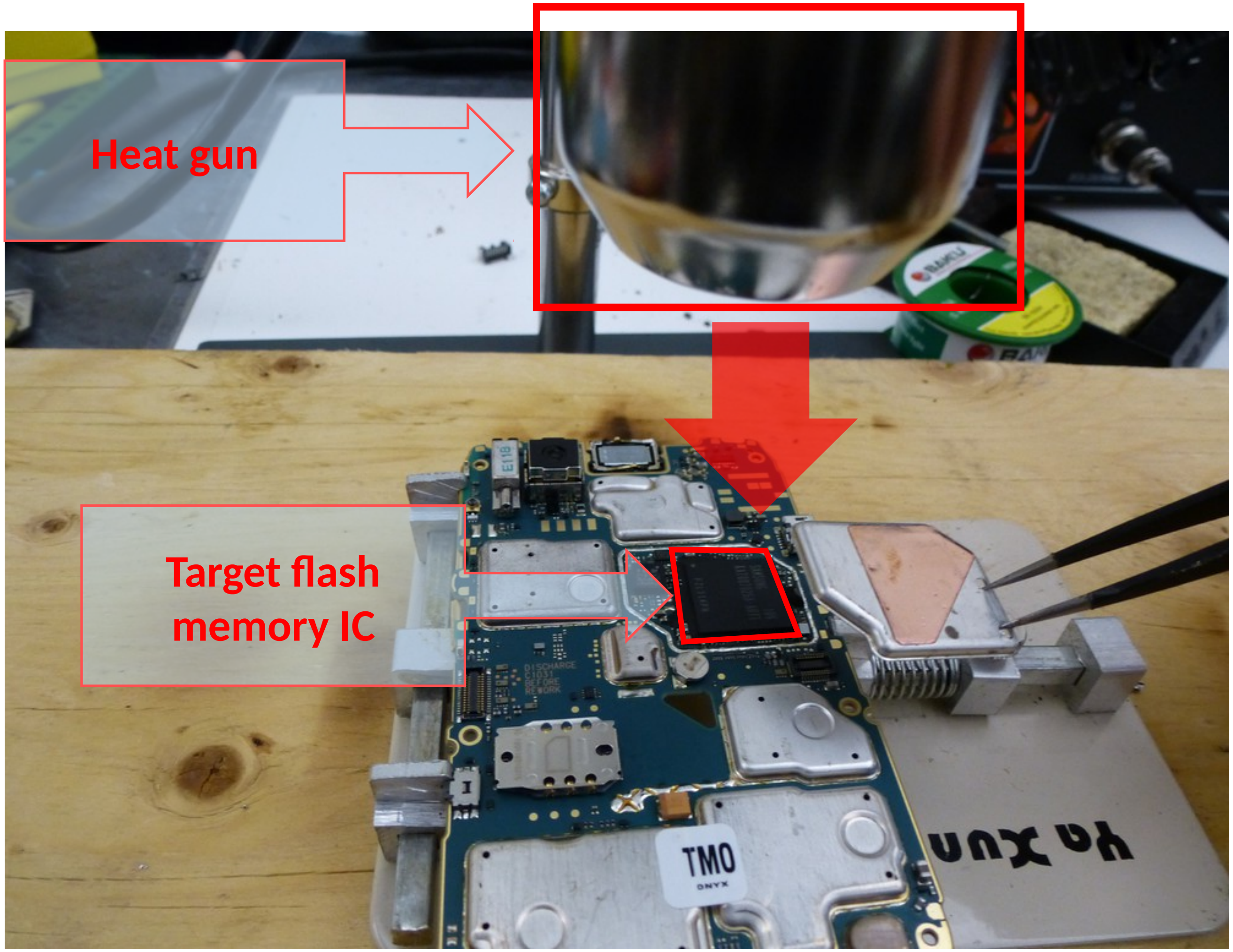
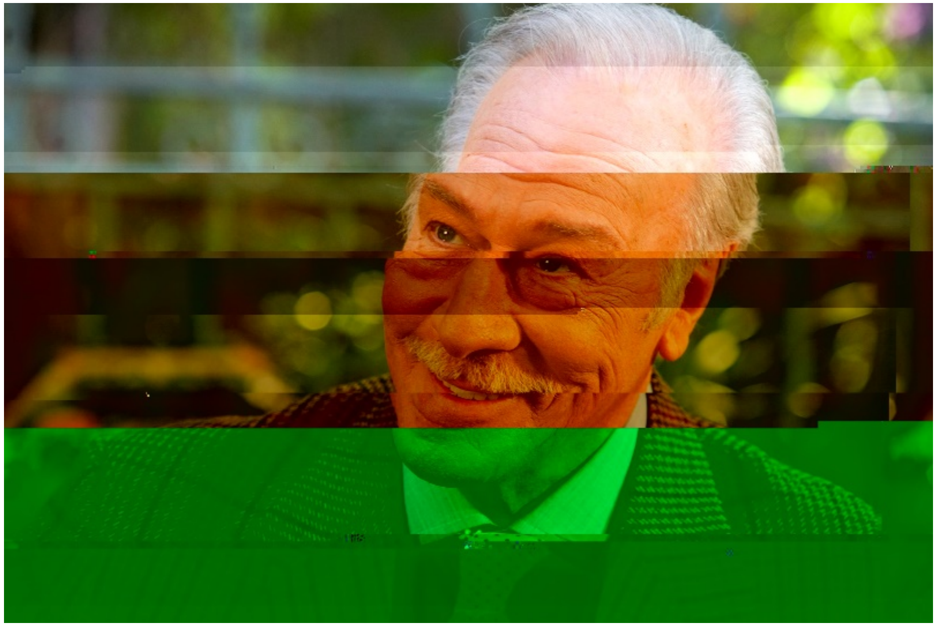
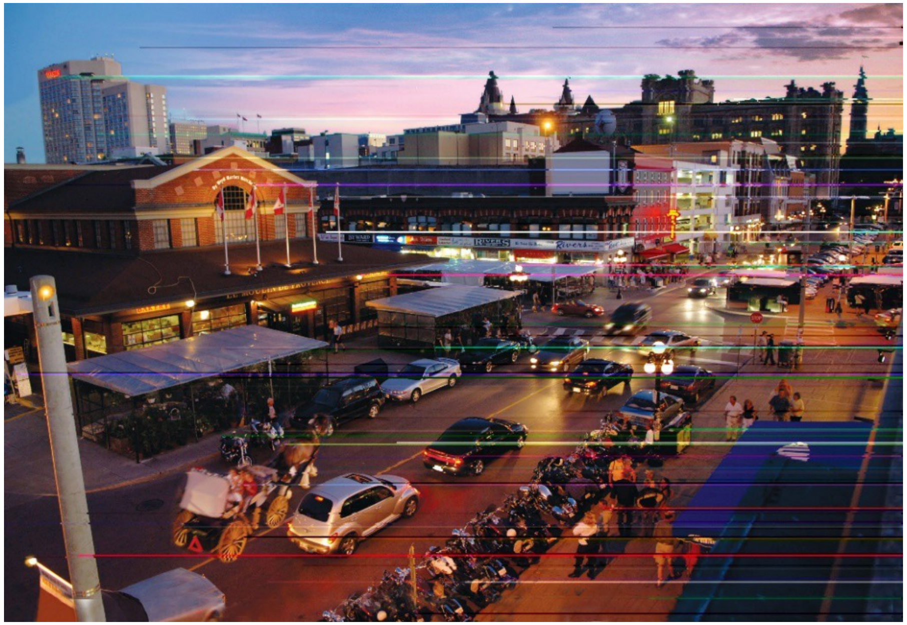


Photo courtesy: “Chip-Off BlackBerry Bold 9780” http://www.forensicswiki.org/wiki/Chip-Off_BlackBerry_Bold_9780

Recovered Data after Chip-Off





Uncorrectable errors remain in recovered data when raw data is acquired through chip-off procedure

Brief Summary of the Paper

- ***Our Goal***:
  - Identify error sources in NAND flash memory during chip-off
  - Quantify errors in NAND flash memory introduced in chip-off
  - Identify a mitigation process to reduce errors introduced during chip-off analysis
- ***Our findings***:
  - Long storage time of devices increases errors in NAND flash memory
  - Heat in chip-off increases uncorrectable errors
  - Read-retry mechanism can reduce errors introduced during chip-off

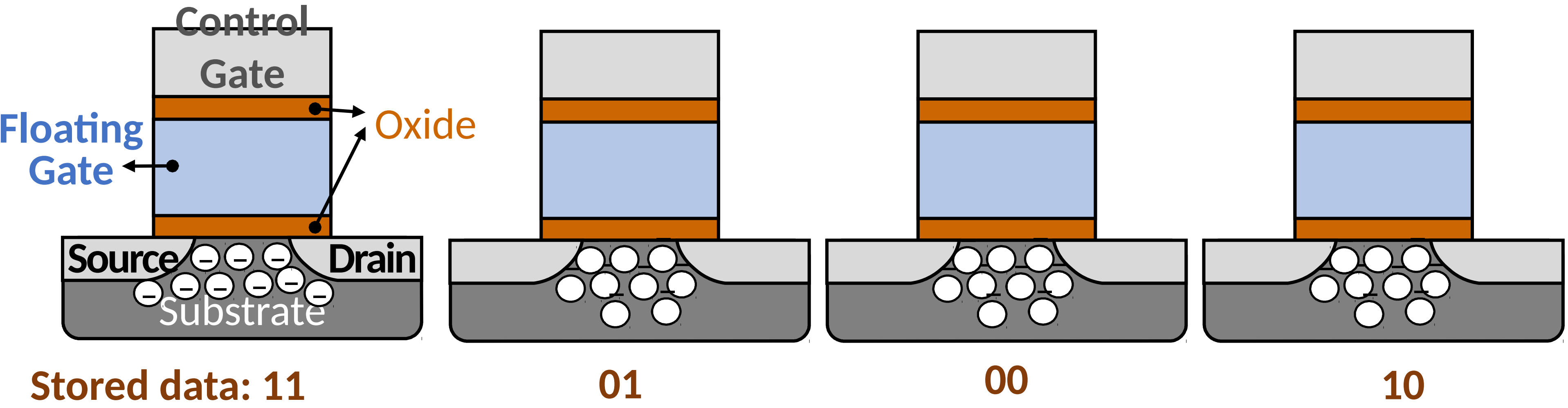
Talk Outline

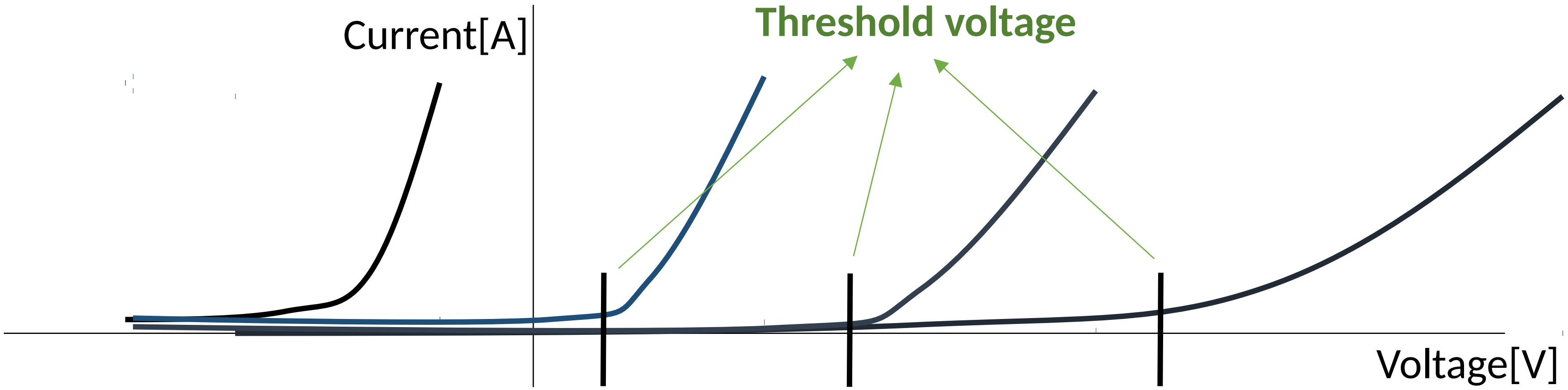
- Background
  - Basic operation of NAND flash memory
- Testing Methodology and Experimental Results
  - Retention error
  - Errors introduced by heat
- How to Improve Reliability of Chip-off Analysis
  - Read-retry operation

Talk Outline

- Background
  - Basic operation of NAND flash memory
- Testing Methodology and Experimental Results
  - Retention error
  - Errors introduced by heat
- How to Improve Reliability of Chip-off Analysis
  - Read-retry operation

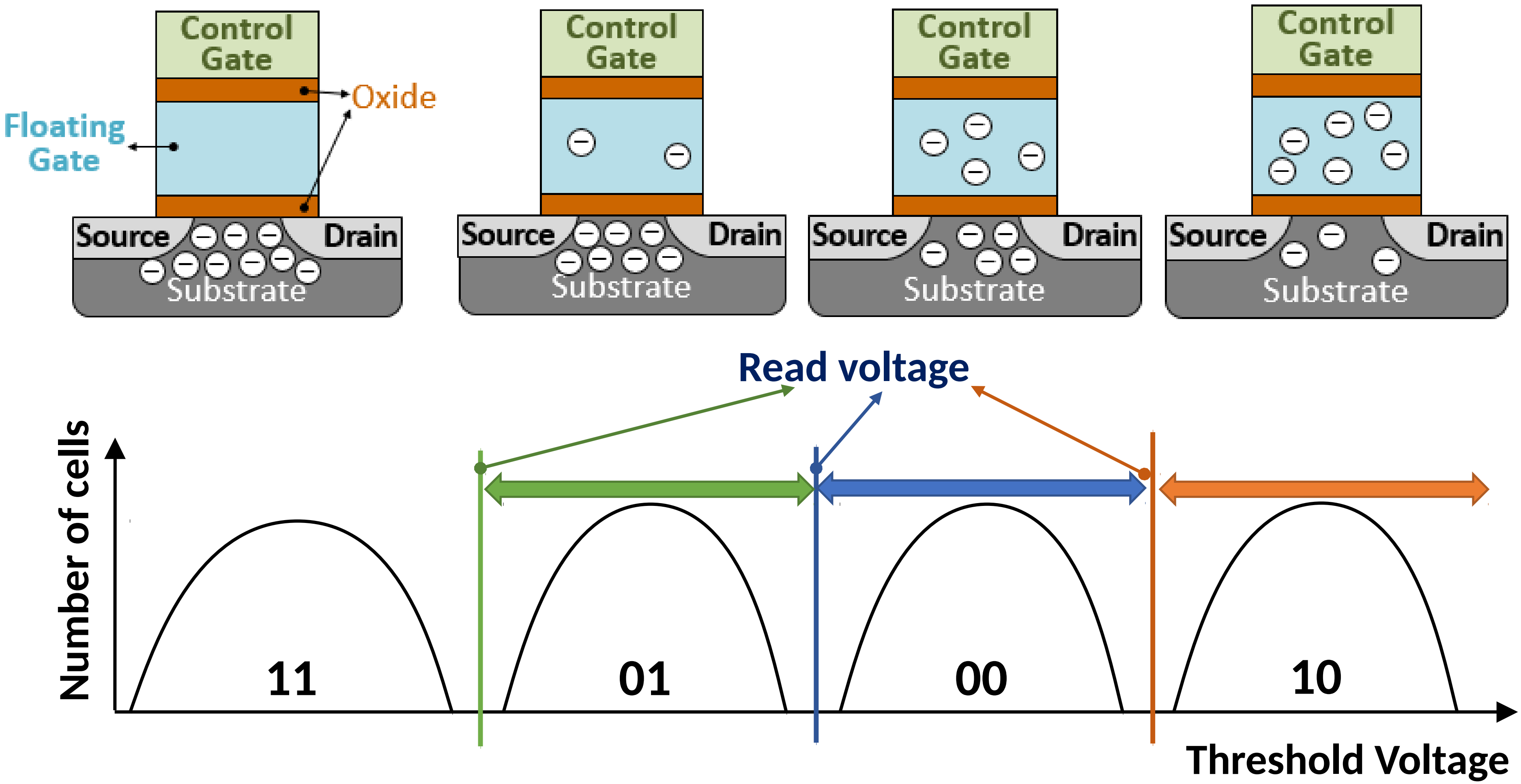
MLC NAND Flash Memory Cell Operation





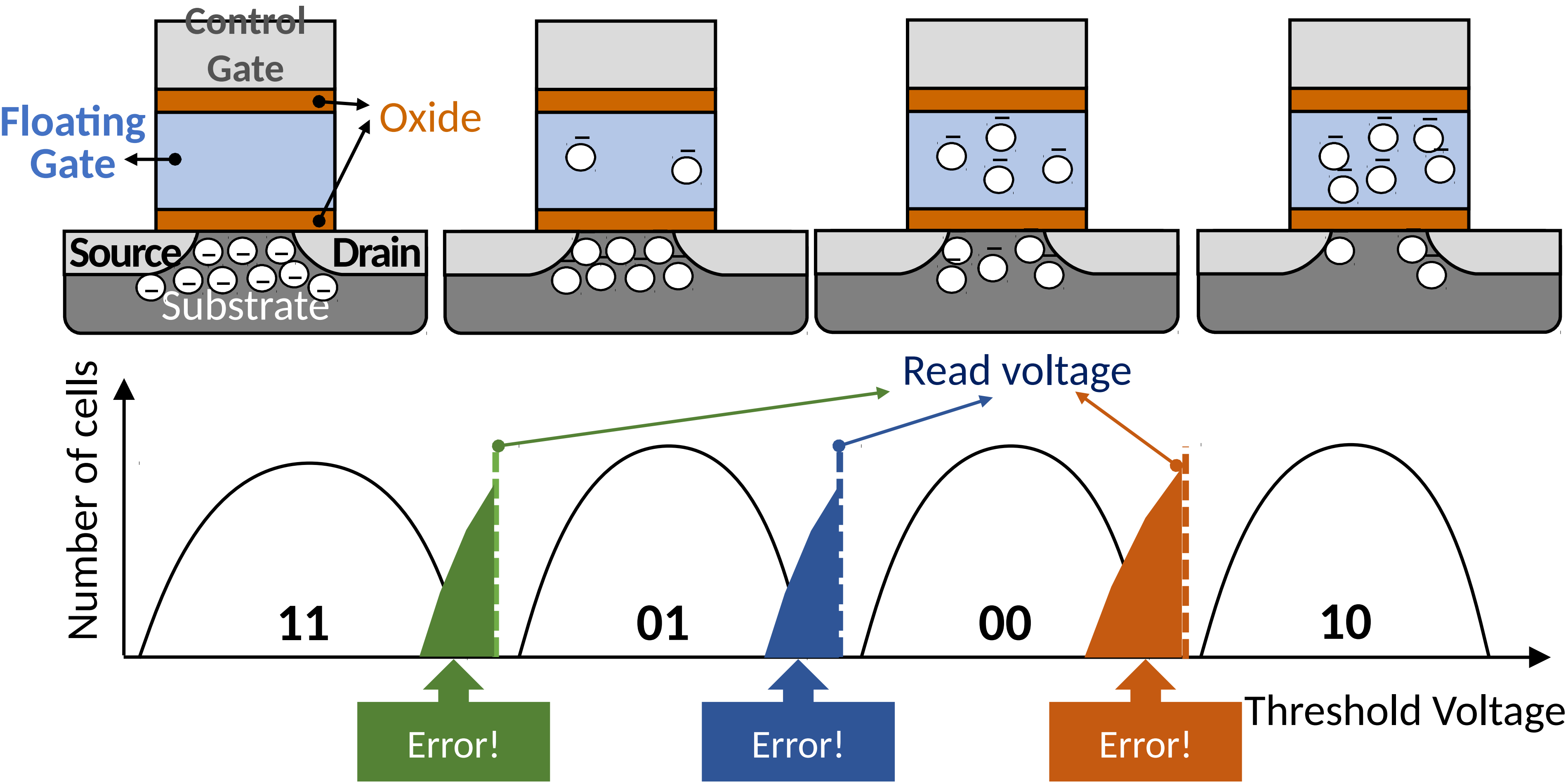
Amount of charge = Threshold voltage of the cell = Stored data value

MLC NAND Cell Vth Distribution



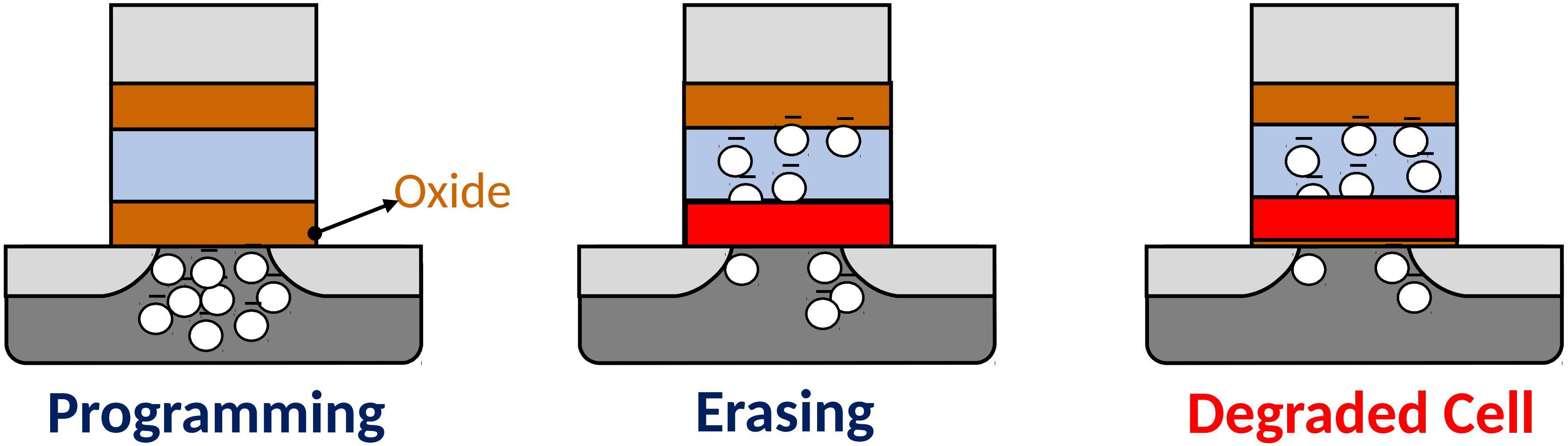
Threshold voltages need to be between each read voltage

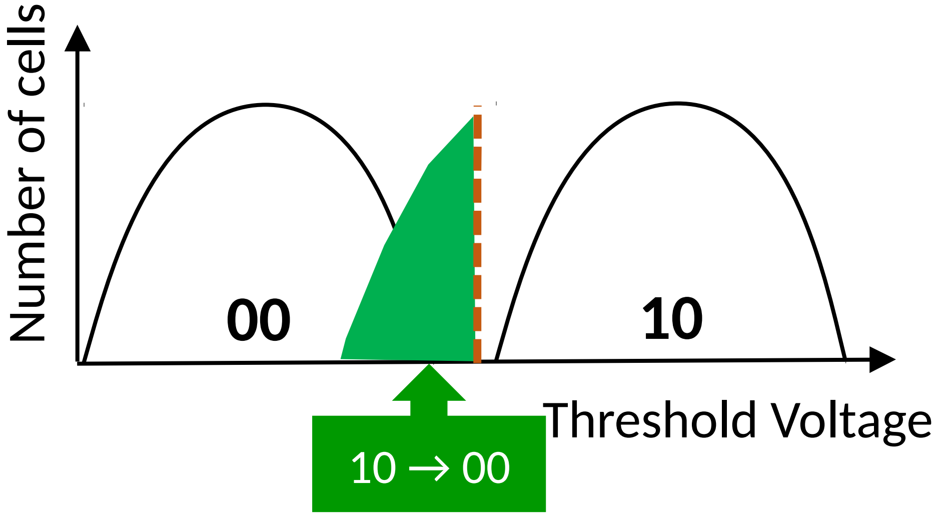
Retention Error on MLC NAND Flash Cell



- ***Charge leakage over time causes threshold voltage shifts***
  - ***Data error in result is called retention error***

NAND Flash Cell Degradation



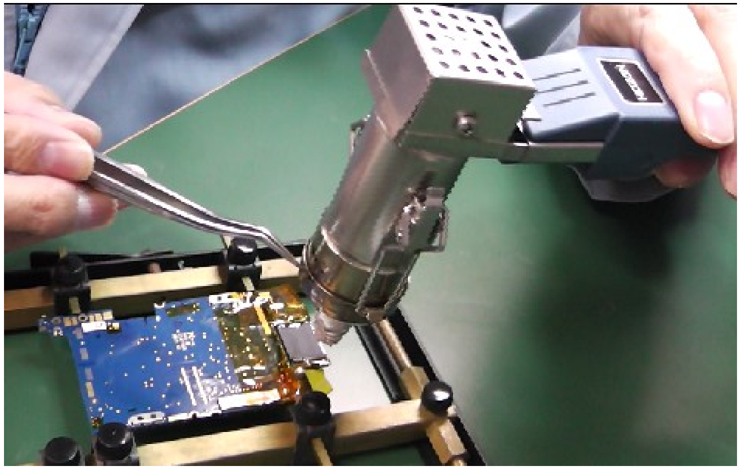


Repeated programming and erasing (P/E cycle) accelerates charge leakage

NAND Flash Error Sources During Chip-off

- Heat guns or electrical rework machines
  - De-solder NAND flash memory chips with heat
- Required temperature and duration: 250 °C (482 °F), ~2 minutes

High temperature accelerates charge leakage



Error Correction Codes (ECC)

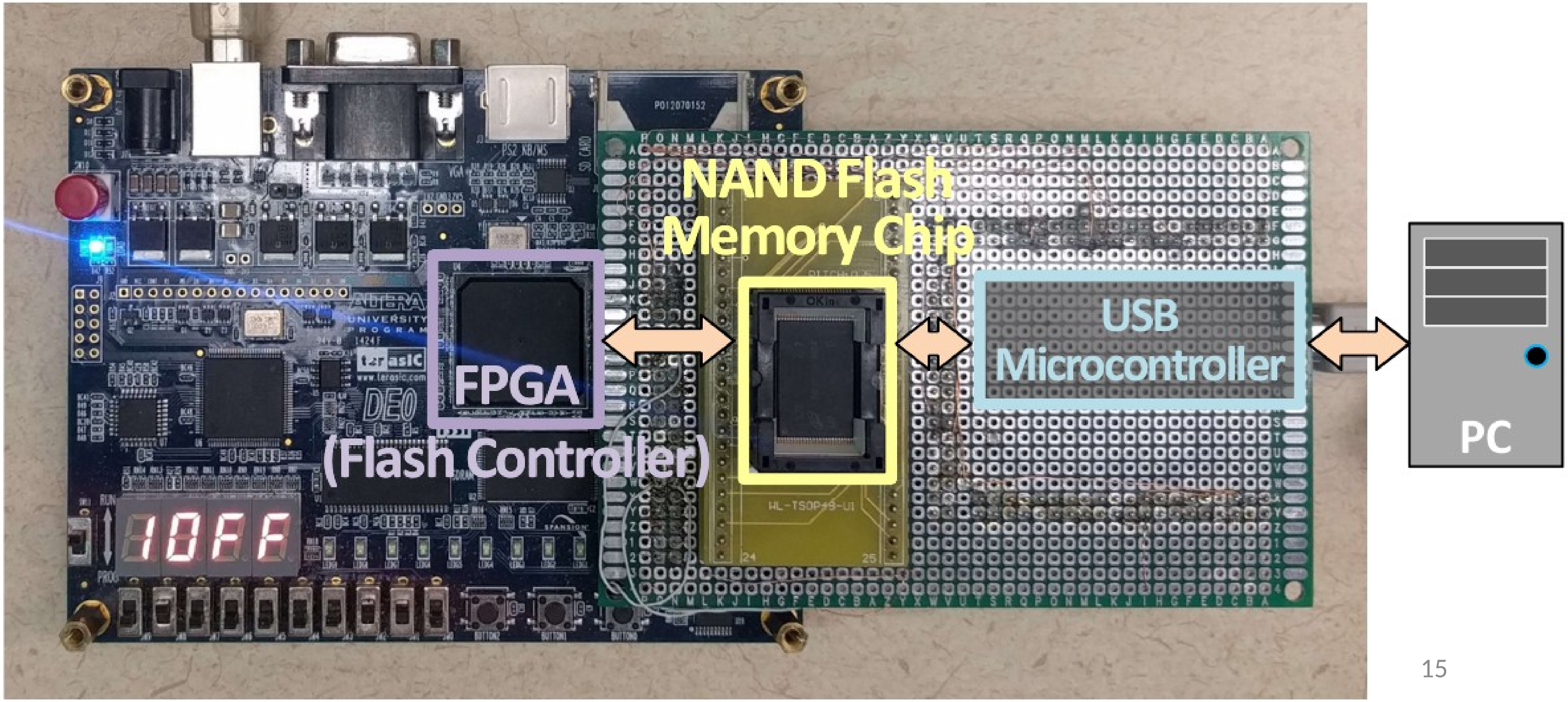
- Flash memory controllers store ECC codewords to correct errors in data
- Typical correction capability for recent chip: 40 bits correction capability per 1KB
- Errors exceeding ECC correction capability: uncorrectable errors

Talk Outline

- Background
  - Basic operation of NAND flash memory
- Testing Methodology and Experimental Results
  - Retention error
  - Errors introduced by heat
- How to Improve Reliability of Chip-off Analysis
  - Read-retry operation

Testing Environment

- Test chips: New 2y-nm NAND flash memory chips from two different vendors (hereafter called Chip A and Chip B)
- Controller: Altera DE0 FPGA

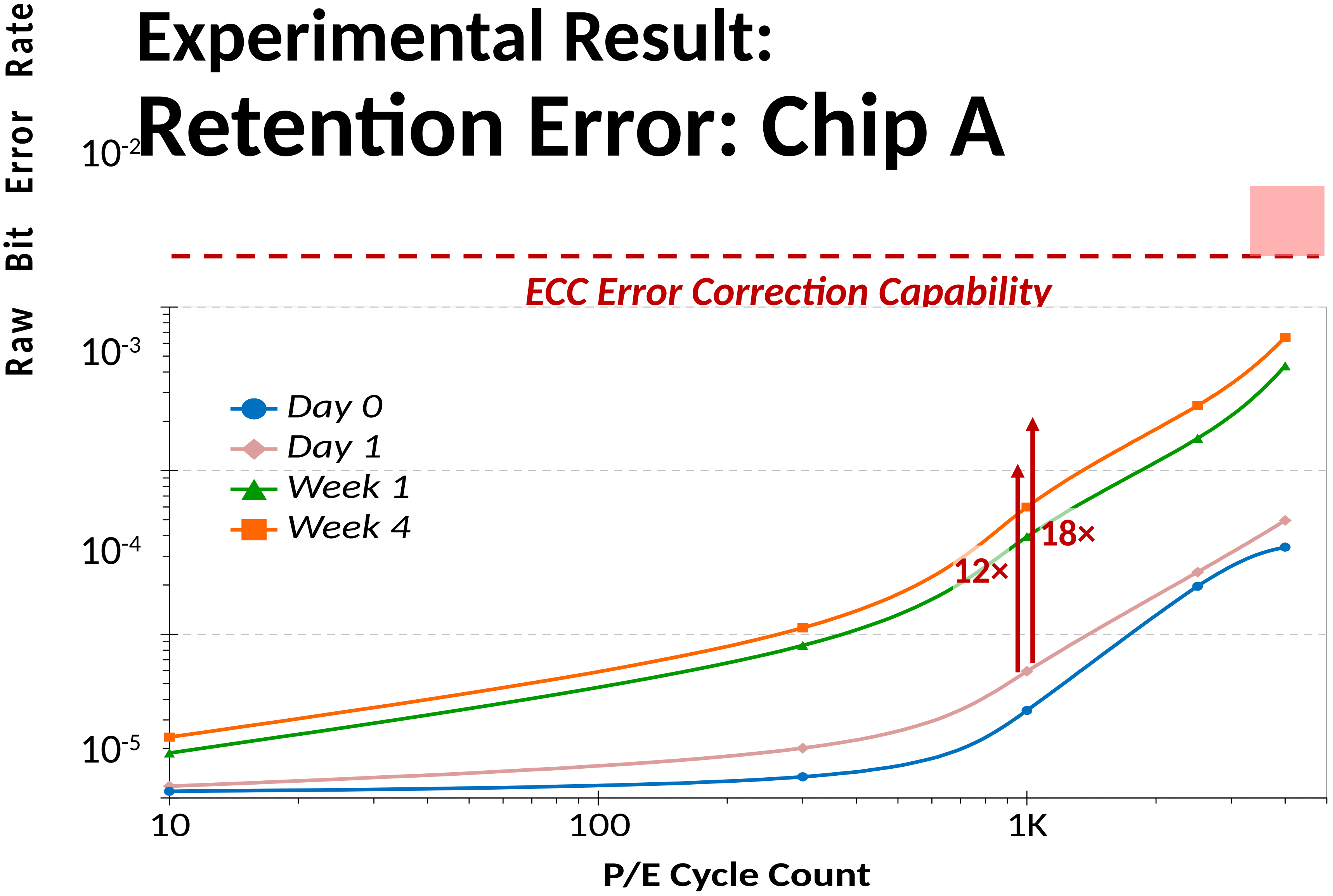


Testing Methodology:
Retention Error Evaluation

- Repeated programming/erasing cycles (P/E cycles)
    - 10, 300, 1000, 2500, and 4000 cycles

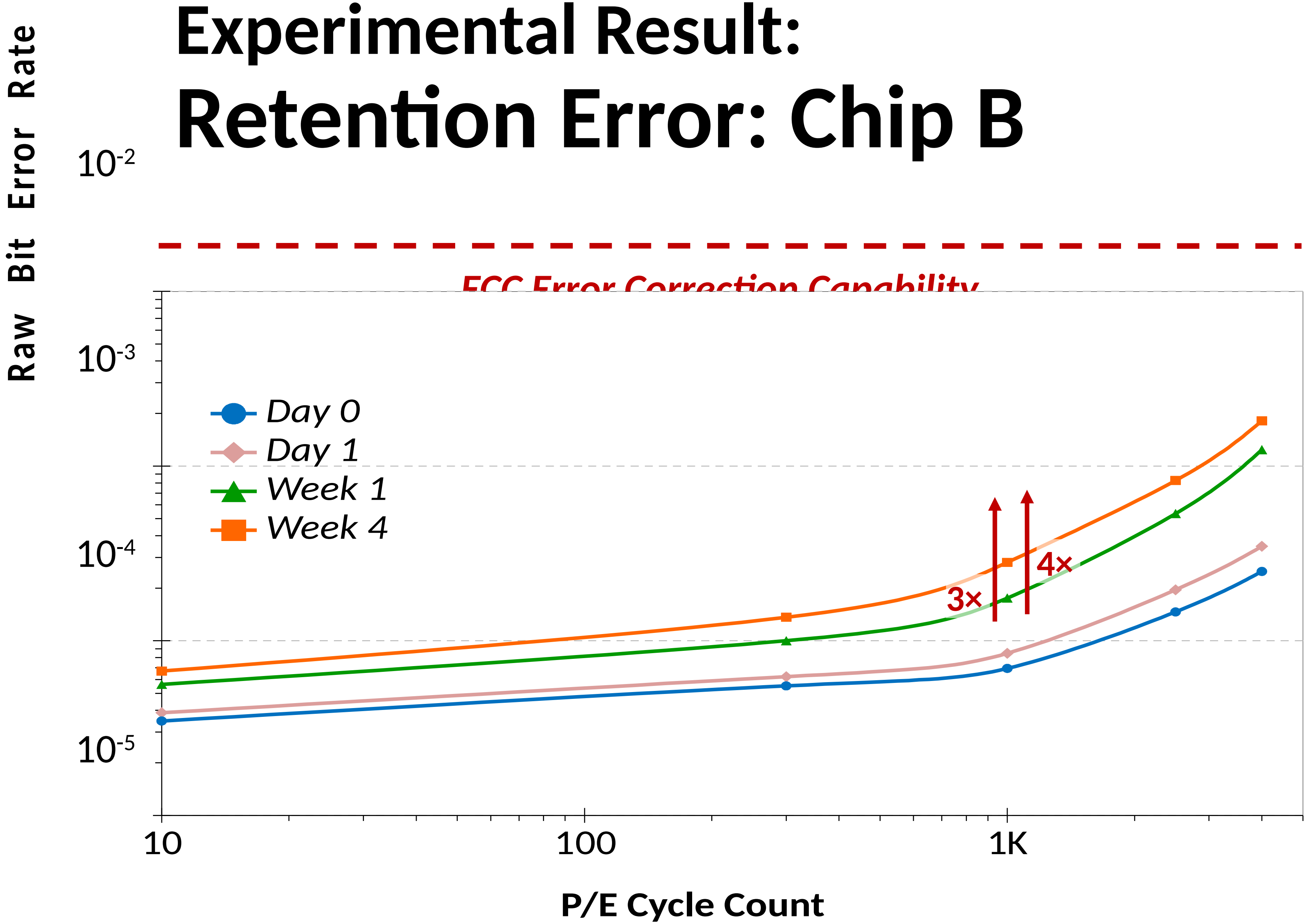
- Raw bit error rate (RBER) measurement at multiple retention age (=wait time after programming)
    - Day 0 and 1, Week 1, 2, 3 and 4

Experimental Result:
Retention Error: Chip A



RBER grows as P/E cycle count and retention age increase

Experimental Result:
Retention Error: Chip B



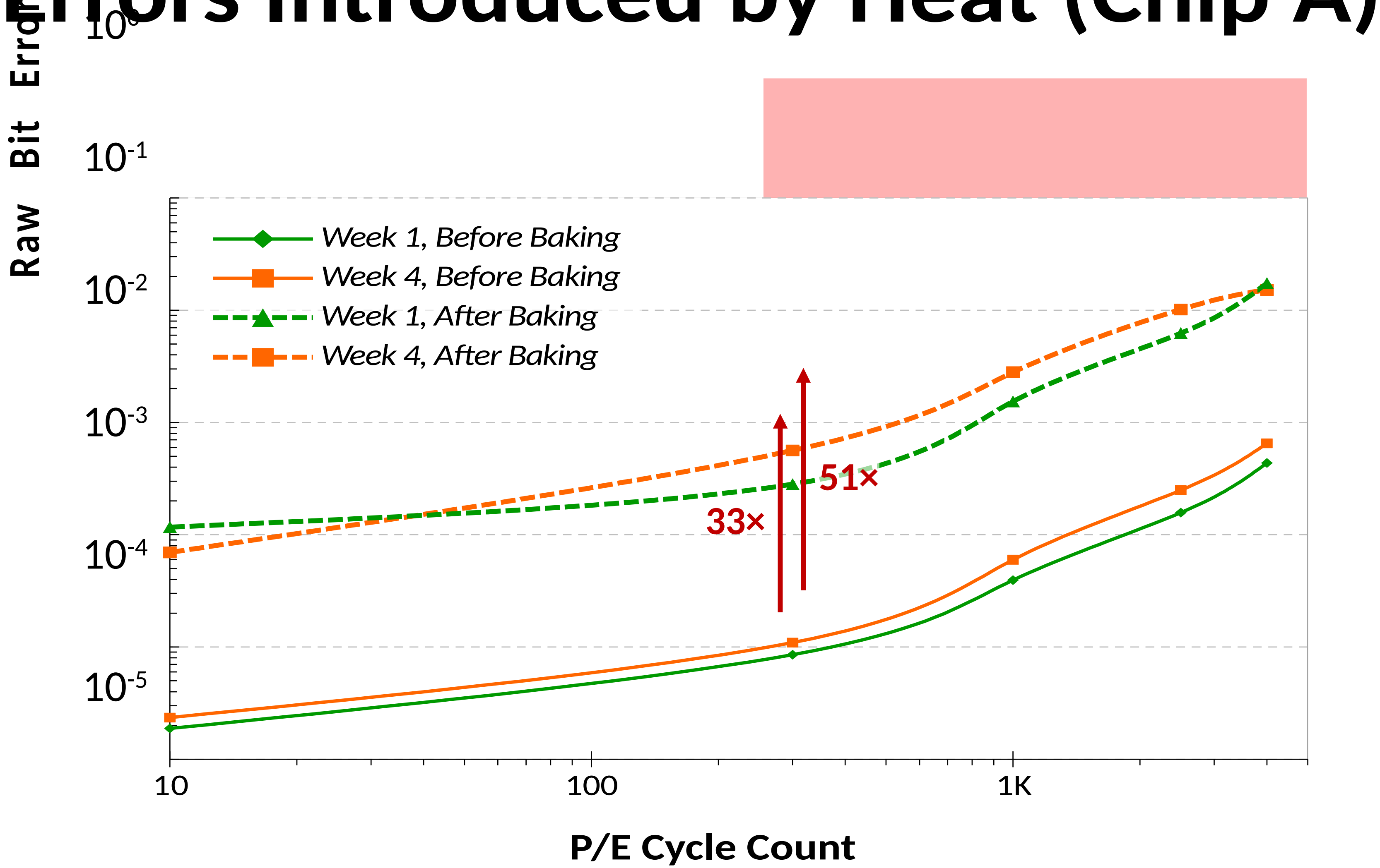
RBER grows as P/E cycle count and retention age increase

Testing Methodology: Thermal Effect Evaluation

- Baking target chips at 250 °C for 2 mins at different retention age (simulating chip-off procedures)
  - 1 Week
  - 4 Weeks

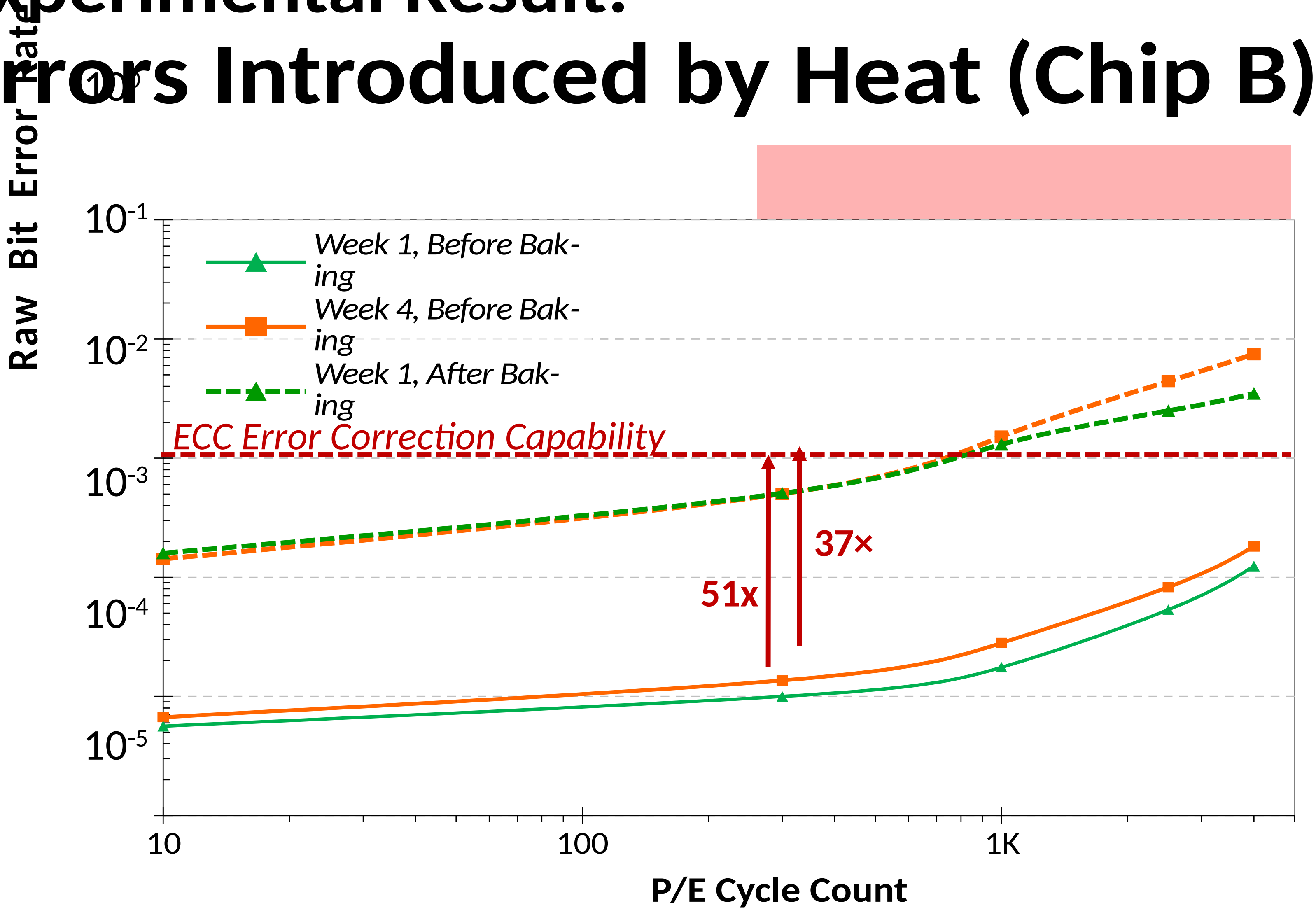
- Raw bit error rate (RBER) measurement after baking

Experimental Result:
Errors Introduced by Heat (Chip A)



Heat introduces errors more than ECC can correct

Experimental Result: Errors Introduced by Heat (Chip B)



Heat introduces errors more than ECC can correct

SAFARI

Experimental Result:
Uncorrectable Errors after Baking

Fraction of pages that contains uncorrectable errors (P/E cycle=300)

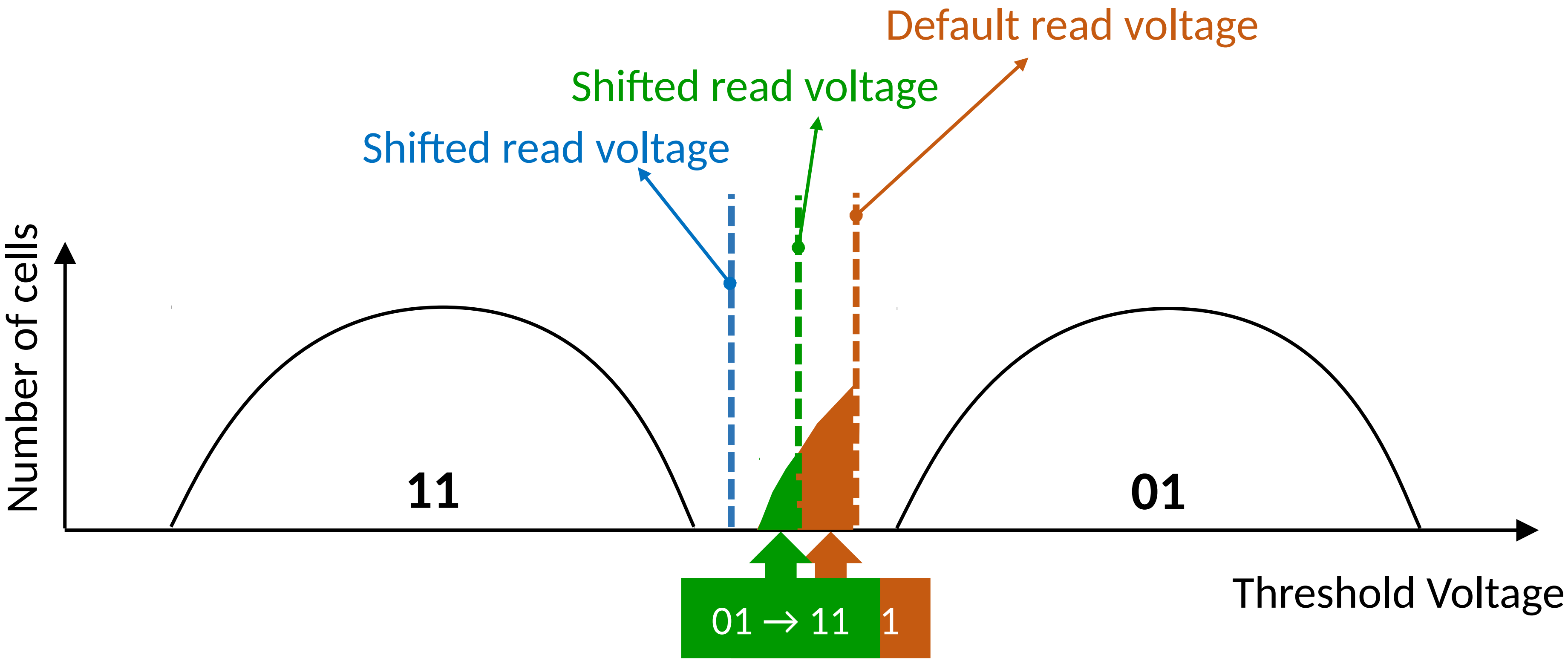
Retention Period before Baking	Chip A	Chip B
1 Week	29.1%	78.1%
4 Weeks	84.2%	83.6%

Heat introduces uncorrectable errors even when the chip has been only lightly used

Talk Outline

- Background
  - Basic operation of NAND flash memory
- Testing Methodology and Experimental Results
  - Retention error
  - Errors introduced by heat
- How to Improve Reliability of Chip-off Analysis
  - Read-retry operation

Read-Retry Mechanism



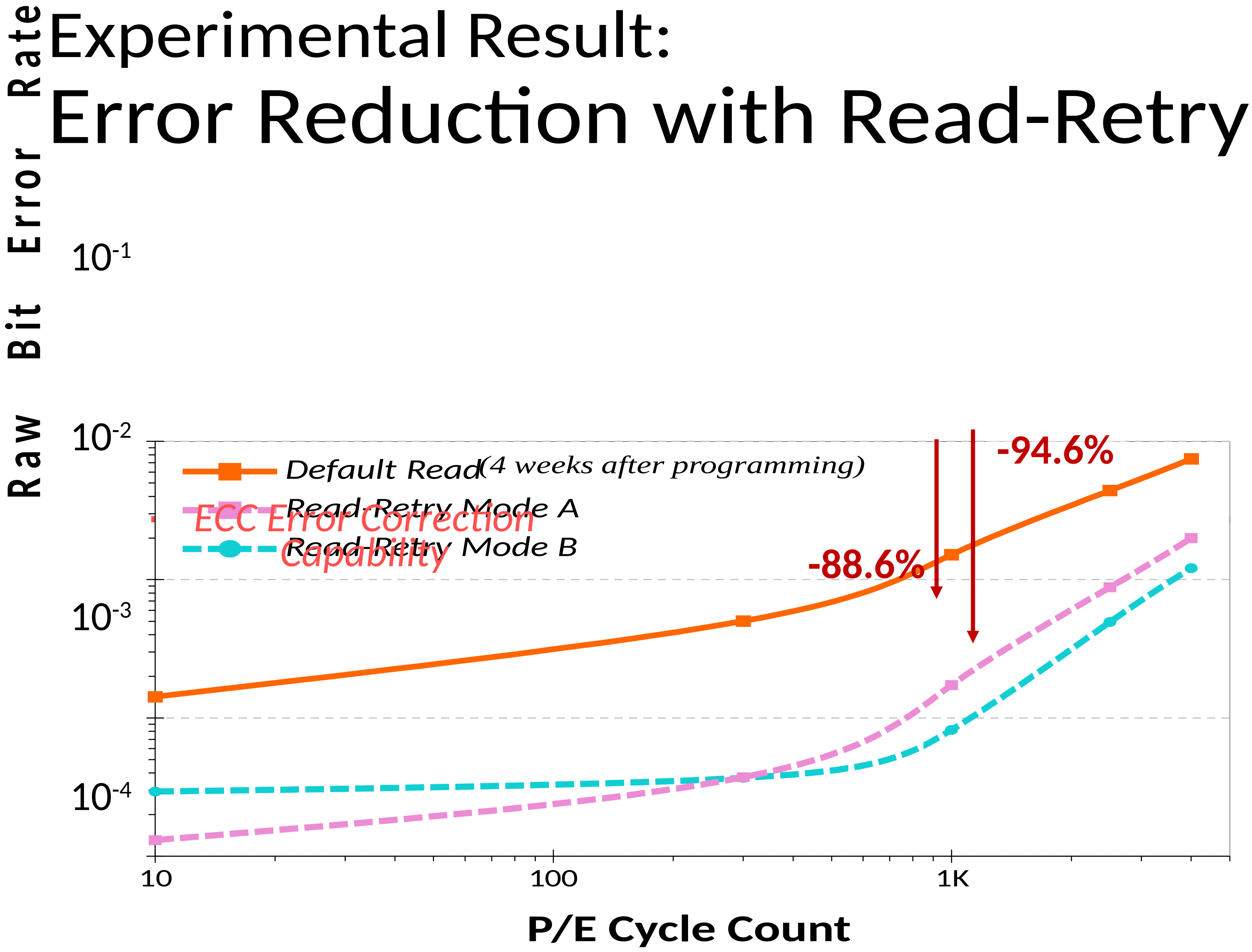
Read-retry mechanism** **shifts the read voltage
to reduce errors caused by threshold voltage shifts

Testing Methodology:
Read-Retry Evaluation

- Read-Retry command found on chip B
  - Implemented as a vendor specific command

- Read operation with read-retry
  - Evaluation of 2 modes (mode A and B)

Experimental Result:
Error Reduction with Read-Retry



Uncorrectable Error Reduction by Read-Retry

Fraction of pages that contains uncorrectable errors (Chip B, after baking)

Read Mode	P/E Cycle Count	
	300	1000
Default	83.6%	99.7%
Read-Retry A	0%	12.1%
Read-Retry B	0%	0%

Read-retry can reduce errors introduced by thermal-based chip-off procedure

Conclusions and Recommendations

- Wait time increases errors
  - Conduct data extraction at the earliest possible time after receiving a device
- Heat introduces uncorrectable errors
  - Keep the temperature as low as possible
- Read-retry can reduce errors
  - Use read-retry after chip-off when available

DFRWS

Improving the Reliability of Chip-Off Forensic Analysis of NAND Flash Memory Devices

Aya Fukami[a,b], Saugata Ghose[b], Yixin Luo[b], Yu Cai[b], Onur Mutlu[b,c]

[a]National Police Agency of Japan, [b]Carnegie Mellon University, [c]ETH Zurich