NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

FDTC 2022

Embedded-EEPROM descrambling via laser-based techniques – A case study on AVR MCU

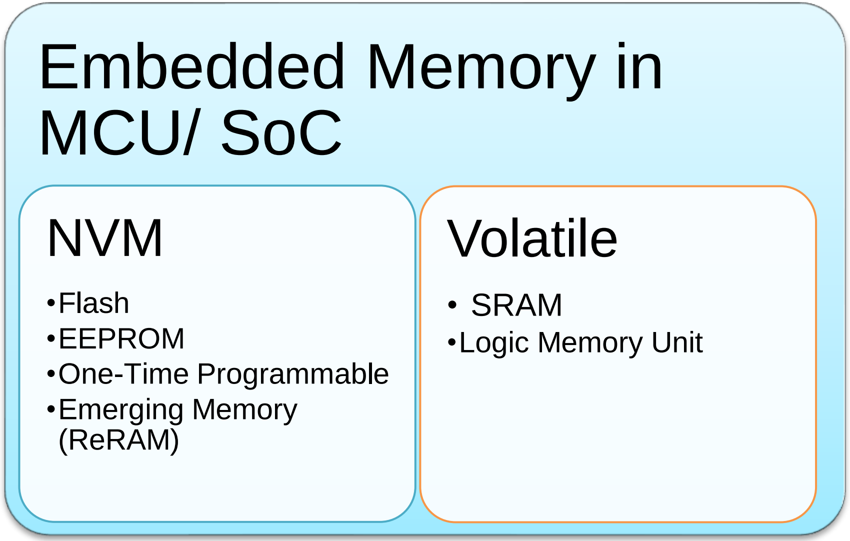
Samuel Chef[1], Chua Chung Tah[1], Jing Yun Tay[1,2], Jason Cheah[1], Chee Lip Gan[1,2]

[1]Temasek Laboratories@NTU, Nanyang Technological University, Singapore

[2]School of Material Sciences and Engineering, Nanyang Technological University, Singapore

Introduction

- Embedded NVM memories may stores different types of assets:
  - Program/Firmware
  - User's information (e.g. Data, Passwords)
  - Encryption Key
- Constitute a target of choice for:
  - Hardware Security Evaluation
  - Forensic Analysis
- Recovering data from embedded memory:
  1. Estimation of bitcell data (i.e. 1 or 0)
  2. Understanding of physical implementation of data (i.e. Addressing/Descrambling)



Embedded Memory in MCU/ SoC

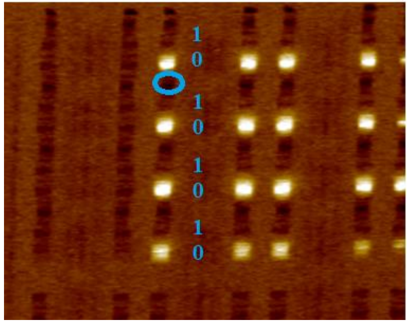
NVM

- Flash
- EEPROM
- One-Time Programmable
- Emerging Memory (ReRAM)

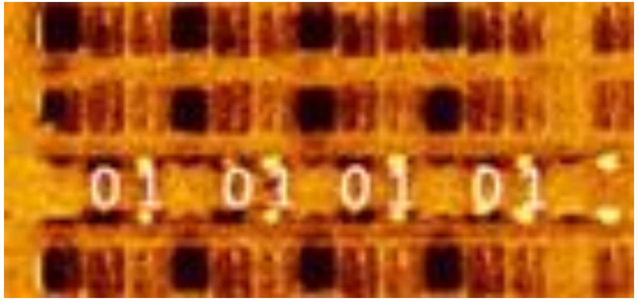
Volatile

- SRAM
- Logic Memory Unit

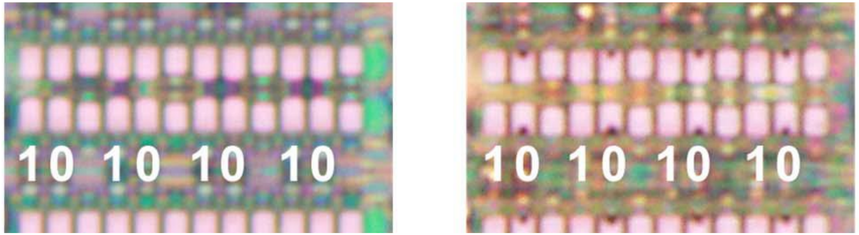
Estimation of bitcells data in Flash/EEPROM



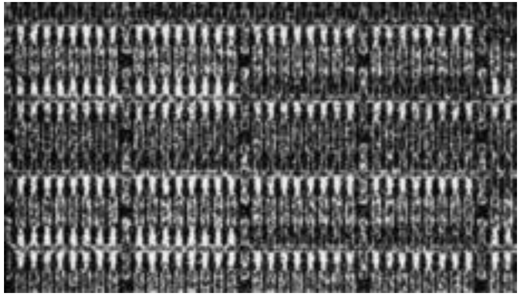
Scanning Capacitance Microscopy
(Tay et al., 2019)



Scanning Non-Linear Dielectric Microscopy
(Zeng et al., 2021)



Selective Chemical Staining
(Zeng et al., 2022)



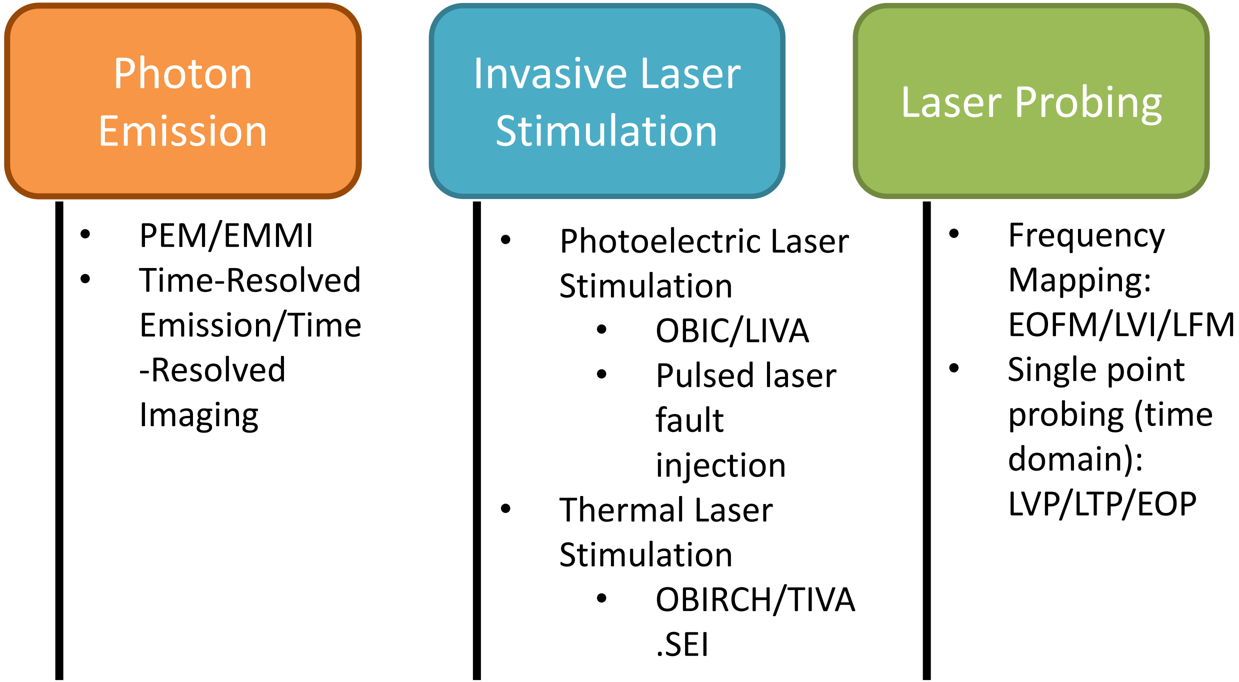
Scanning Electron Microscopy
(Courbon et al., 2018)

Motivation for descrambling

- **Challenges**:
  - When studying a new device, results may not be as expected:
    - Different type of transistors?
    - Physics does not apply to this reference?
    - Data not organized as initialy assumed?
  - Number of samples to carry out the analysis can be limited
  - Data can be scrambled and/or not follow an obvious sequence
- **How to verify/understand data location and organization (i.e. descrambling)?**

Semi-Invasive Analysis and Optical Techniques

- Enable access to internal signals.
- May assist in:
  - Localization of assets
  - Recovery of assets



Photon Emission

- PEM/EMMI
- Time-Resolved Emission/Time -Resolved Imaging

Invasive Laser Stimulation

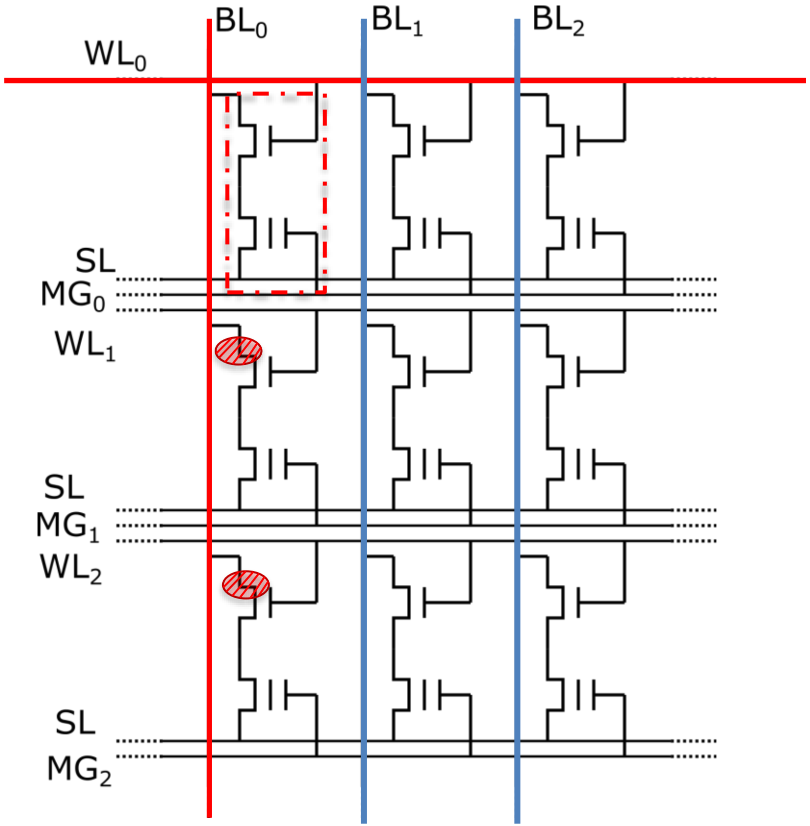
- Photoelectric Laser Stimulation
  - OBIC/LIVA
  - Pulsed laser fault injection
- Thermal Laser Stimulation
  - OBIRCH/TIVA .SEI

Laser Probing

- Frequency Mapping: EOFM/LVI/LFM
- Single point probing (time domain): LVP/LTP/EOP

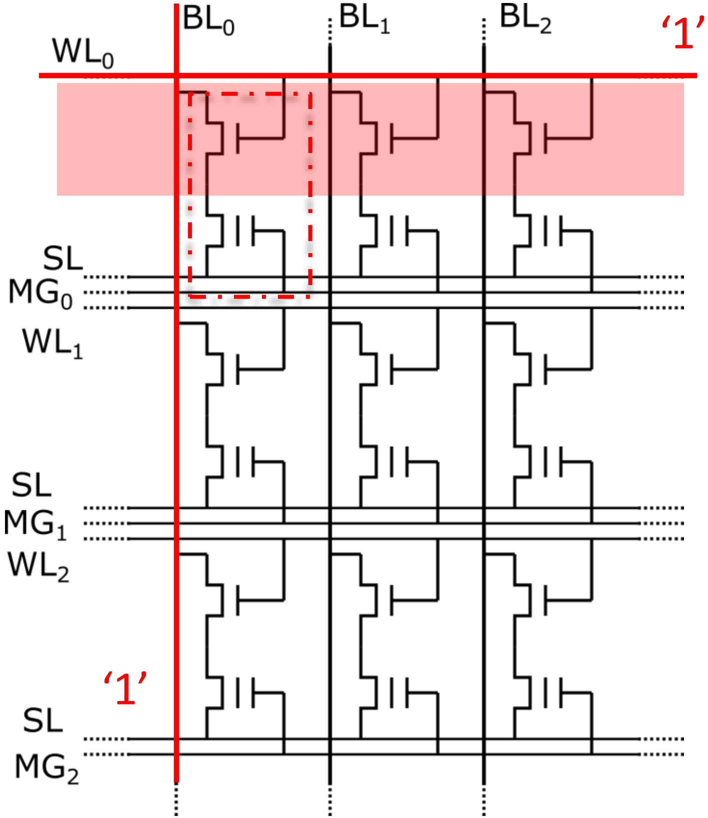
Bitline/Column localization: Laser Fault injection

- As reported by several research groups, laser fault can be triggered during read operations in NOR flash.
- Originates from the reversed bias drain/well junction in off-state transistors connected to the read cell bitline.
- Provides the column information.
- Works only one way (e.g. only when the cell being read stores ‘1’).



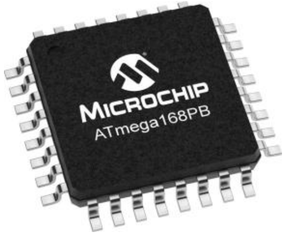
Wordline/Row Localization: Laser Probing

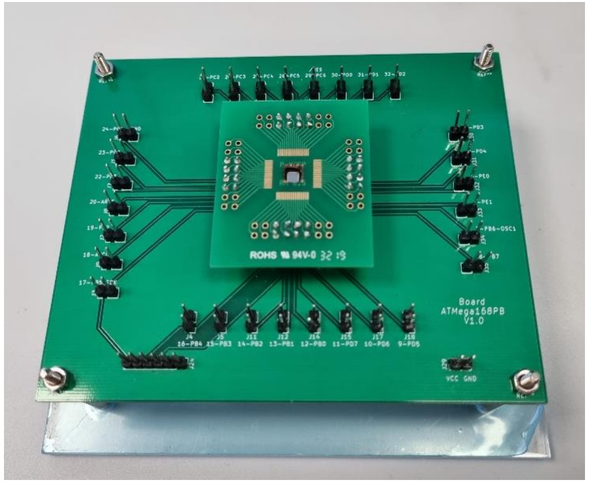
- Laser probing consists in monitoring the change of reflectance due to transistors biasing.Of use for:
  - Probing internal signals in ICs.
  - Generate frequency mapping image (i.e. localization of nodes operating at a specific frequency)
- During a read operation, all the transistors connected to the same WL signals are switched on => Can Laser probing help?

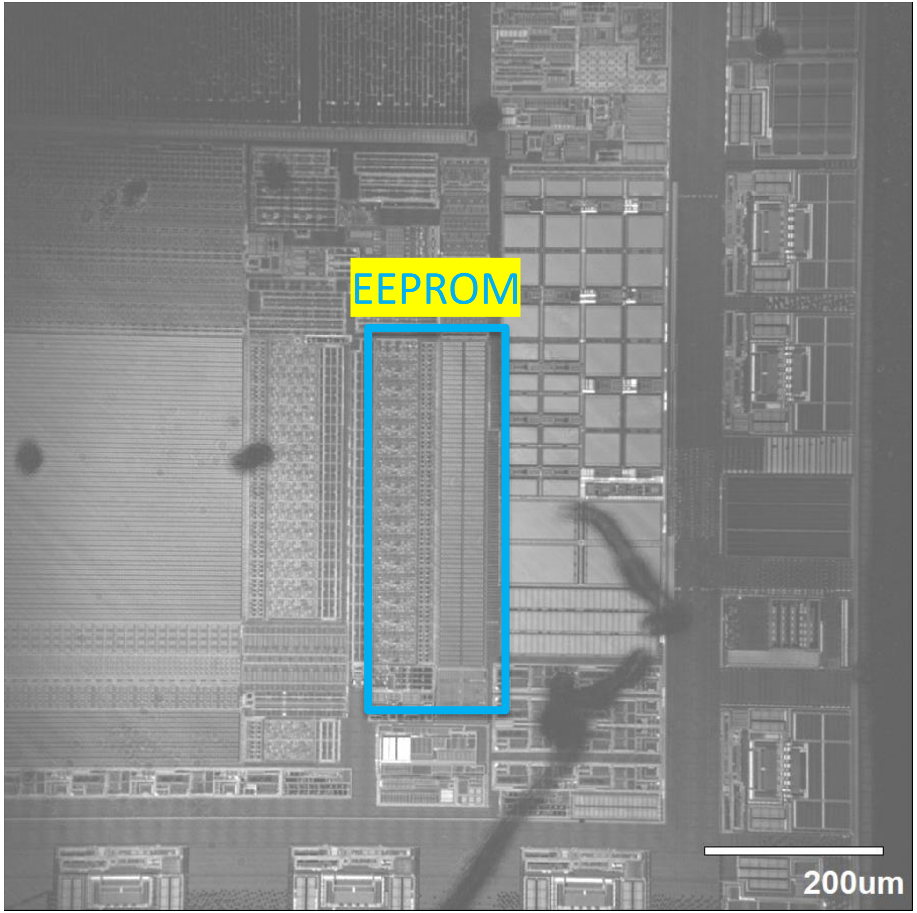


Application: Target

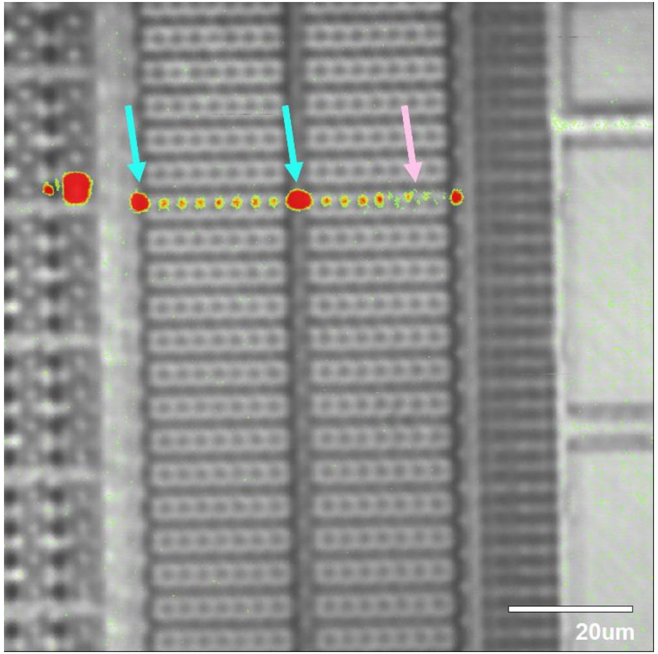
- DUT: AVR ATMega168 PB
  - 8 bits MCU
  - Technology 130 nm
  - 512B EEPROM

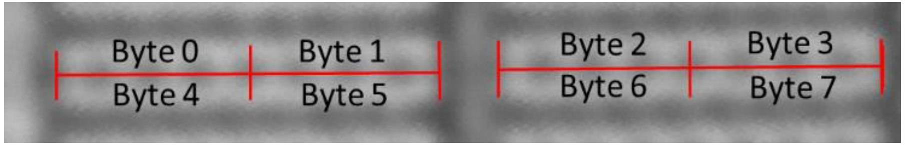


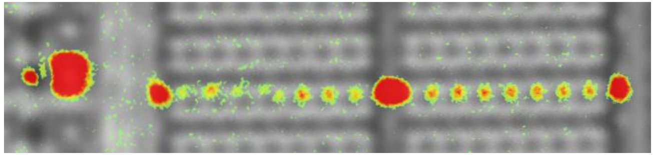




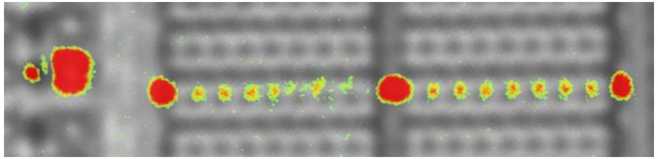
Wordline detection



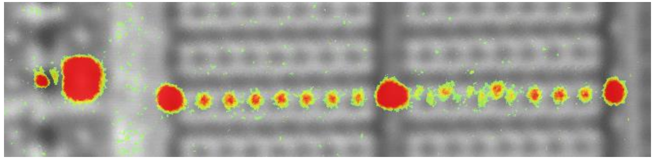




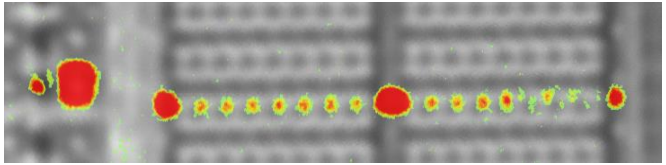
Reading @0x0FC



Reading @0x0FD

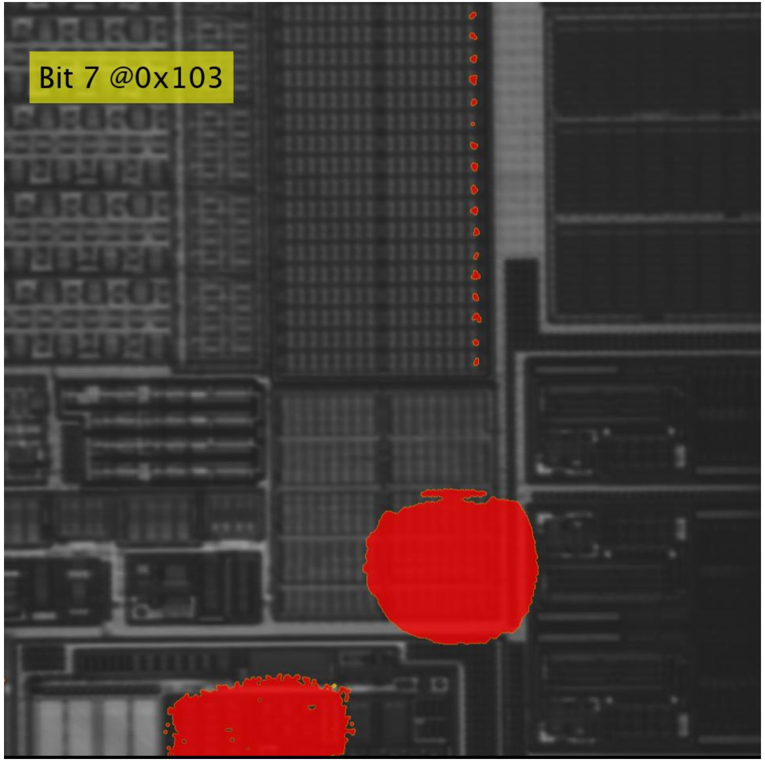


Reading @0x0FE

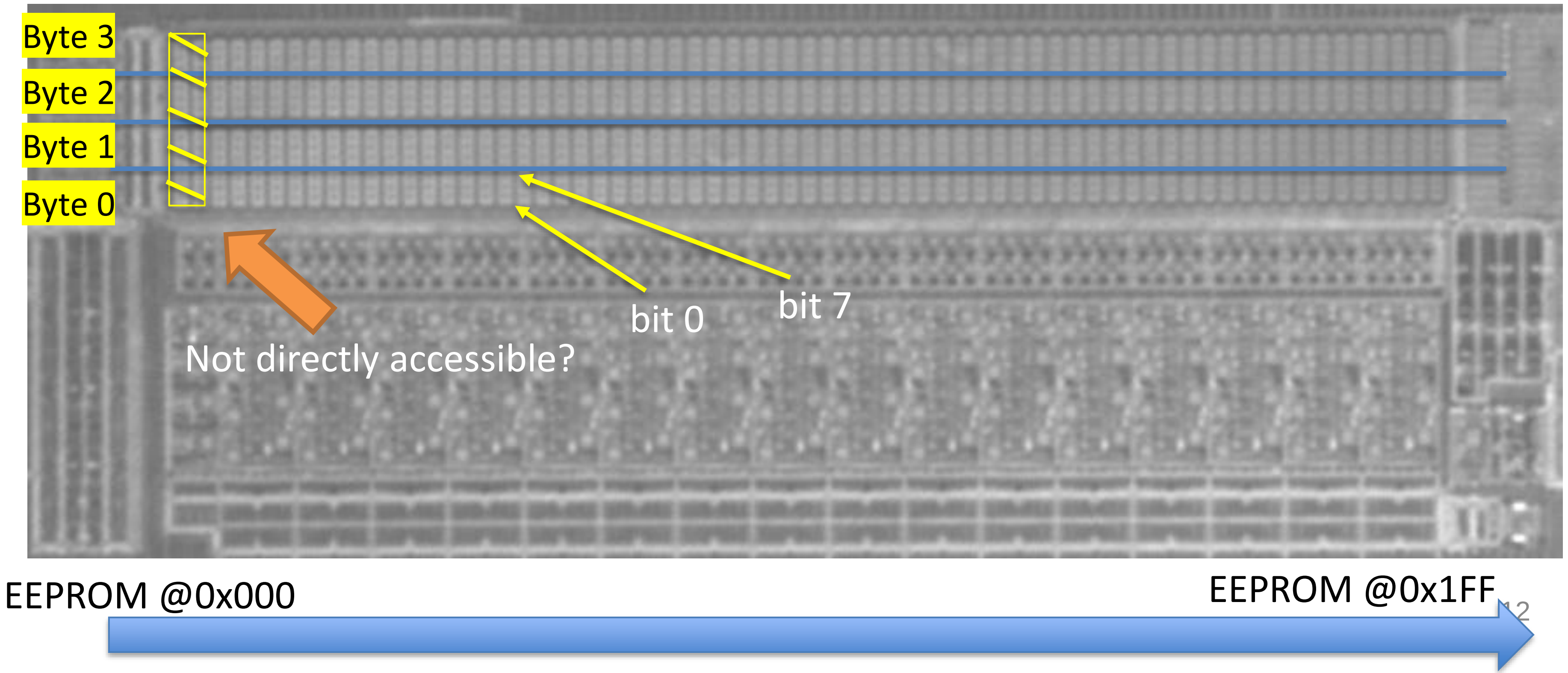


Reading @0x0FF

Bitline detection



EEPROM Descrambling



Not directly accessible?

Summary and Conclusion

- Recovery of data from embedded EEPROM requires ability to estimate cells content and match bitcell location with addresses (descrambling).
- If only a small number of samples is available, methods with limited invasiveness are preferred.
- Discussed a process to recover data organization in embedded EEPROM using laser fault injection (bitline/column) and laser probing (wordline/row).
- Demonstrated proofs of concept in AVR MCU - ATMega168 PB.
- Possible application to more advanced MCUs/SoCs
  - Optical resolution challenge => SIL/VLP
  - Device complexity
  - Heterogeneous packaging

References

J. Y. Tay, J. Cheah, Q. Liu and C. L. Gan, "Study of Front-Side Approach to Retrieve Stored Data in Non-Volatile Memory Devices Using Scanning Capacitance Microscopy," 2019 IEEE 26th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA), 2019, pp. 1-4, doi: 10.1109/IPFA47161.2019.8984802.

X. M. Zeng, Q. Liu, J. Y. Tay and C. L. Gan, "Selective Staining on Non-Volatile Memory Cells for Data Retrieval," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1884-1892, 2022, doi: 10.1109/TIFS.2022.3172222.

X.M. Zeng, Q. Liu, J.Y. Tay, K.Y. Chew, J. Cheah and C.L. Gan, “High resolution front-side visualization of charge stored in EEPROM with scanning nonlinear dielectric microscopy (SNDM)”, Nanotechnology, 2021, 32, 485201

F. Courbon, "Challenges and examples of in-situ memory content extraction techniques," *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2018, pp. 493-496, doi: 10.1109/ICECS.2018.8617941.

THANK YOU!

Any question: csamuel@ntu.edu.sg