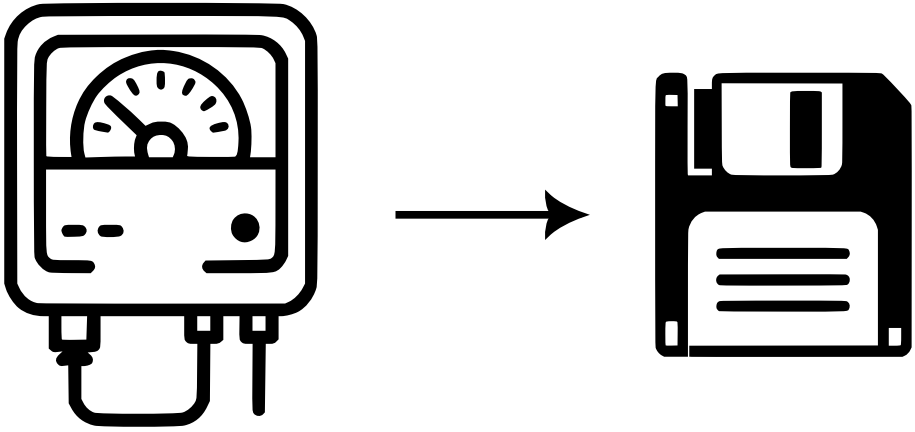
Fraunhofer AISEC

Be Write Back

An in-depth Study of Fault Injection Effects on FRAM Technology

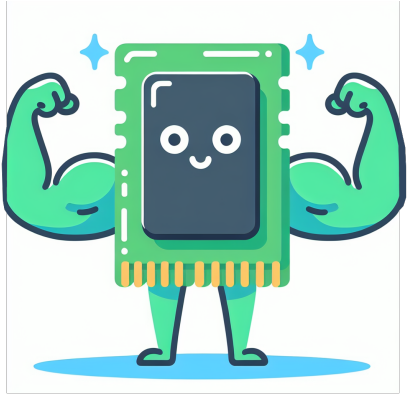
Valentin Huber, Marc Schink, August 12, 2025

Intro



Why FRAM?

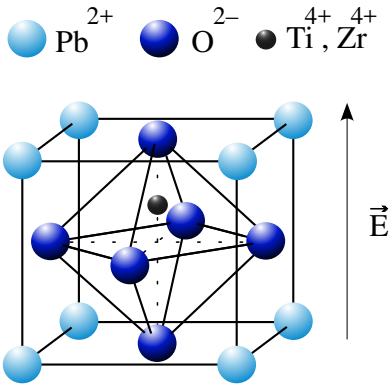
- Non-Voltatile
- Low Power
- Fast Writes
- Strong Endurance



How does FRAM work?

Ferroelectric Capacitor

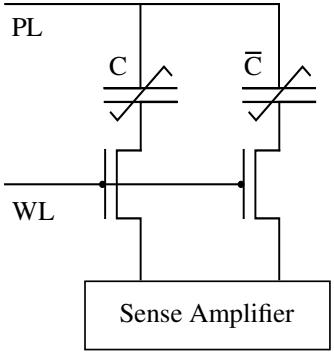
- Ferroelectric Material
- PZT Crystal
- Can be Polarized
- Switchable by E-Field
- Keeps Polarization



How does FRAM work?

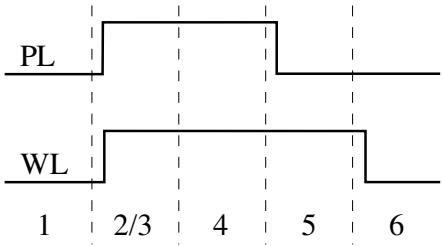
Memory Cell

- Sense Polarization Change
- Switch vs no Switch
- 2T-2C Architecture
- Access with Word-Line
- Control with Plate-Line



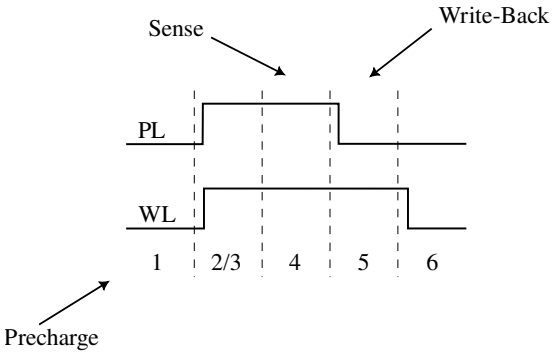
Read operation:

1. Precharge
2. Row Access
3. Polarization
4. Sense
5. Write-Back
6. Close



Vulnerabilities

- Precharge Suppression
- Sense Amplifier Bit-Flip
- Plate-Line Timing Violation



Vulnerabilities

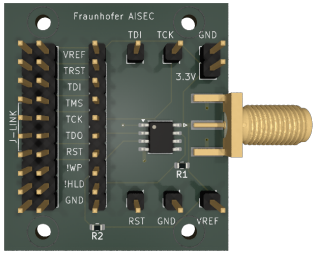
Plate-Line Timing Violation

- Focus: Plate-Line timing violation
- Advantage: Don’t care if device crashes
- Idea: Close cell early
- Solution: Simply cutoff power -> **Crowbar Glitch**

External Memory

Devices

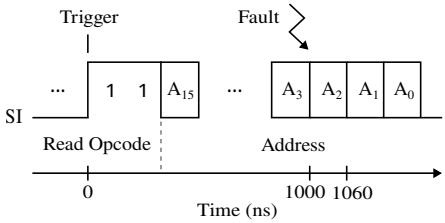
- 4 External Memories
- 3 Manufacturers
- 16 KiB Density
- SPI Interface
- 3.3V Supply Voltage
- SOIC-8 Package



Fraunhofer AISEC

External Memory
Setup

- Read single byte and inject fault
- Chipwhisperer for timing and glitch injection
- MOSI as trigger signal
- Timing depends on memory row size
- Reading always accesses complete memory row
- Glitch length is irrelevant



External Memory

Results FM25L16B & CY15B016Q

- Complete memory row is affected (64 bit)
- Bit-Line dominates outcome of glitch
- Less so memory address
- Single set of sense amplifiers
- Results of CY15B016Q similar

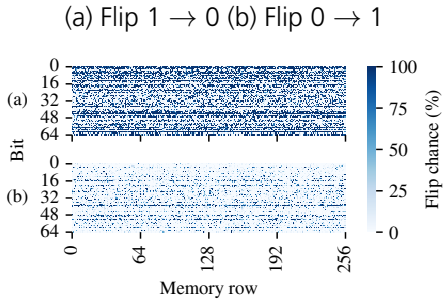


Figure: FM25L16B

External Memory

Results MR45V032 & MB85RS16

- Complete memory row is affected (16 bit)
- Bit-Line dominates outcome of glitch
- Multiple sets of sense amplifiers
- No working parameter set identified for MB85RS16.

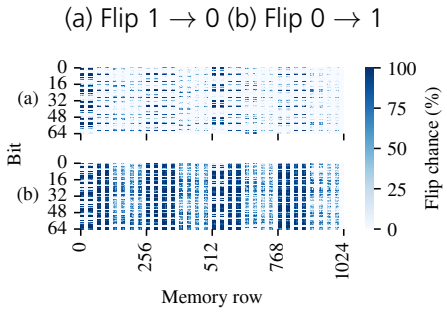


Figure: MR45V032

Fraunhofer AISEC

External Memory

Conclusion

- Complete memory row is affected
- Bit-Line dominates outcome of glitch
- Output has random elements
- Tendencies per device exist

Device	Flip probability (%)	
	$1 \rightarrow 0$	$0 \rightarrow 1$
FM25L16B	49.6	7.3
CY15B016Q0	71.3	2.8
MB85RS16	0.0	0.0
MR45V0320	9.4	22.9

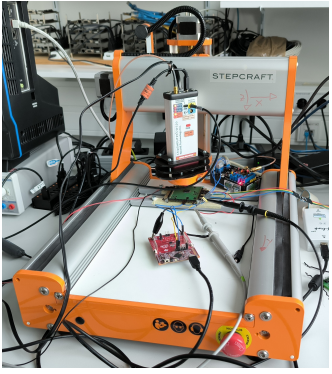
Yes but...

How about real targets?

- MSP430FR family uses FRAM as main memory
- Selected device: MSP430FR5962
- 2T-2C type memory with 64-bit row size
- Device features error-correction (SECDED)
- Has two debug interfaces:
  - JTAG or BSL
  - Configurable through "signatures" that are located in FRAM
  - BSL is always password protected or disabled
  - JTAG is **unlocked** unless signature is all 0x55 or 0xAA

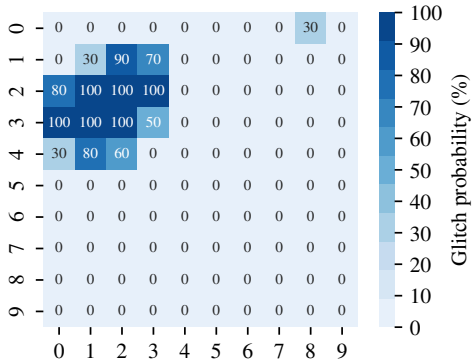
MSP430
Setup

- Voltage Glitch has no Effect
- Switch to EMFI
- Chipshouter and Chipwhisperer
- Coil: 4 mm and CCW
- Pulses with 500 V



MSP430
Vulnerability Analysis

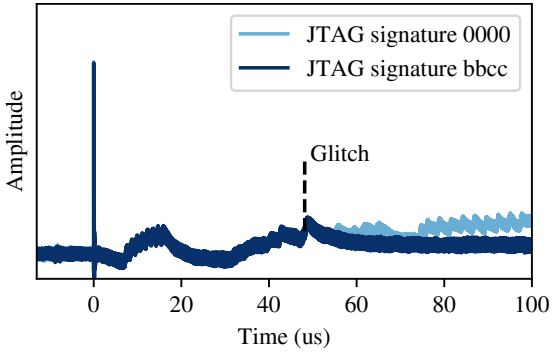
- Pin zero in top left corner
- Glitch during read operation
- Check for any modifications
- High success rate



- Target single read from memory
- Glitch window is 30 ns
- Instructions are modified

- //TRIGGER HIGH
- **mov &target_memory_row, R0**
- //TRIGGER LOW

- Startup time is up to 1 ms
- Large time frame for 30 ns glitch window
- Check if power trace leaks information about signatures
- Startup time & power strongly depends on value of JTAG signature!



MSP430
Unlock

- Use RESET line as trigger input
- Device becomes unlocked in <1 minute
- No matter if fully locked or password protected
- Should work for all devices of MSP430FR5x / MSP430FR6x series

Conclusion

- FRAM read operation is vulnerable to fault effects
- JTAG of real world target can be unlocked
- Vulnerability must be considered during design time

Fraunhofer AISEC

Contact

Valentin Huber, Marc Schink
Department
Hardware Security
forename.surname@aisec.fraunhofer.de

Fraunhofer-Institute for Applied and Integrated Security AISEC
Lichtenbergstr. 11
85748 Garching (near Munich)
Germany