Hardware Security implications of Reliability, Remanence and Recovery in Embedded Memory

Dr Sergei Skorobogatov

http://www.cl.cam.ac.uk/~sps32 *email: sps32@cam.ac.uk*

UNIVERSITY OF CAMBRIDGE

Outline

- Introduction
- Data remanence, data retention and Hardware Security
- Data remanence
  - SRAM with battery
  - NVM: EEPROM and Flash memory
- Data retention in NVM
  - reliability of EPROM, EEPROM and Flash memory
- Limitations and improvements
- Future work
- Conclusion
- The slides are available online: http://www.cl.cam.ac.uk/~sps32

Introduction

- Data Remanence is about residual information left in memory
  - could compromise security if sensitive information is recovered from erased memory
  - could help to improve reliability by maintaining data after power glitch
  - SRAM is volatile and loses information within seconds after power loss
  - EEPROM and Flash memory can be erased to wipe off any sensitive information
- Reliability of data storage
  - data retention time varies between devices: from months to decades
  - if device fails the manufacturer needs to find the cause of the problem
- Hardware Security is about protecting information from unauthorized access and preventing data recovery
  - secure authentication
  - secure storage for data, keys and passwords
  - research into new attack technologies
  - develop countermeasures through understanding of flaws
  - predict new attack methods to come up with possible mitigations

Why hardware security is important?

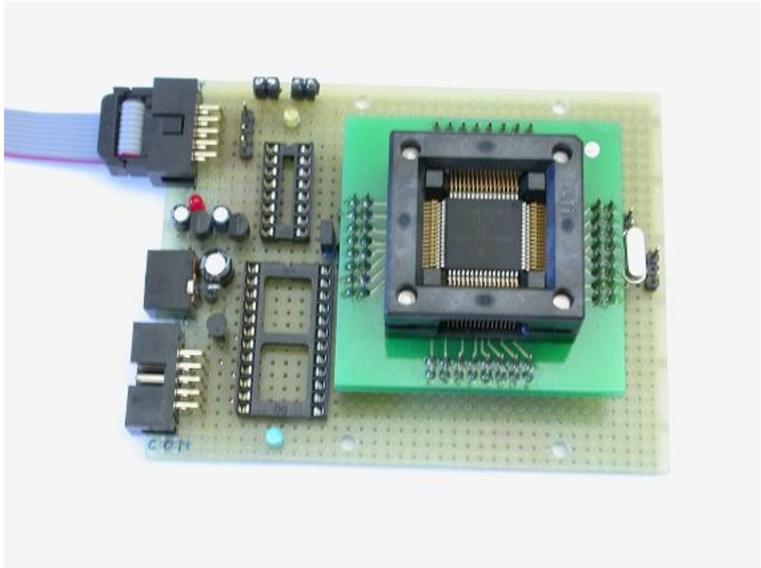
- Understand data remanence effect
  - low temperature data remanence in SRAM
  - data remanence in EEPROM and Flash memory
- Improve the security of devices
  - reducing the data remanence time
  - evaluating the security and exposing vulnerabilities
  - finding ways for improvements
- Improve the reliability of devices
  - evaluating devices
  - understanding the cause of the problem
  - developing new solutions
- Understand the failure mechanism to improve future devices
  - through research into Failure Analysis methods
  - interdisciplinary research into nano-scale structures

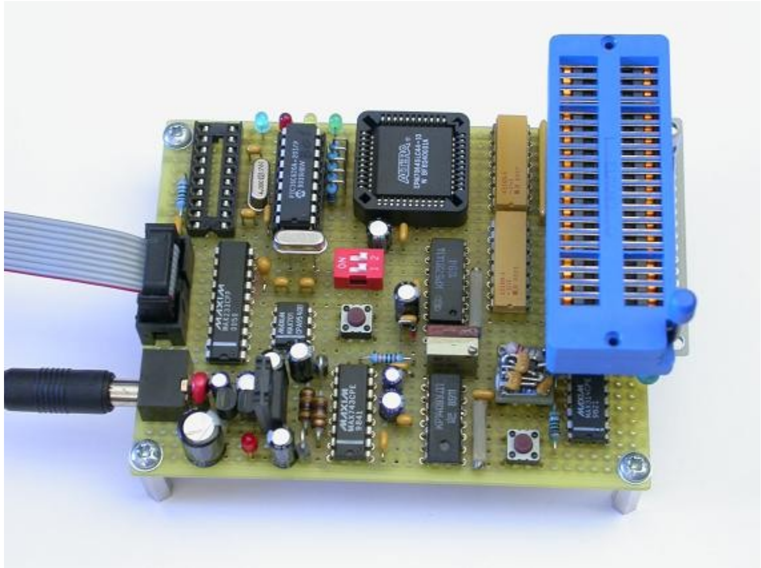
Low temperature data remanence in SRAM

- Reported in 1980s
  - the cause of the problem was understood and helped to avoid burning-in of data
  - tested on individual SRAM samples in 2001
  - countermeasures were developed for sensitive applications
- Also affects DRAM
  - cold boot attack
- Countermeasures
  - erasing the memory on detection of low temperature
  - disconnecting the battery to wipe off the data on detection of tampering
  - special memory cells: fast erasure, asymmetric design
- Is this still a problem for modern semiconductor devices?
  - modern chips do not have external SRAM – everything is embedded
  - modern fabrication processes have transistors with lower leakage
  - find a solution for reliable memory erasure without the need for custom memory cells

Data remanence experiments

- Microcontrollers with embedded SRAM
  - Freescale MC68HC908AZ60, MC68HC908AZ60A
  - Texas Instruments MSP430F112, MSP430F427
- Microcontrollers with embedded Flash memory
  - Microchip PIC16F873
  - Atmel Atmega163, ATtiny12



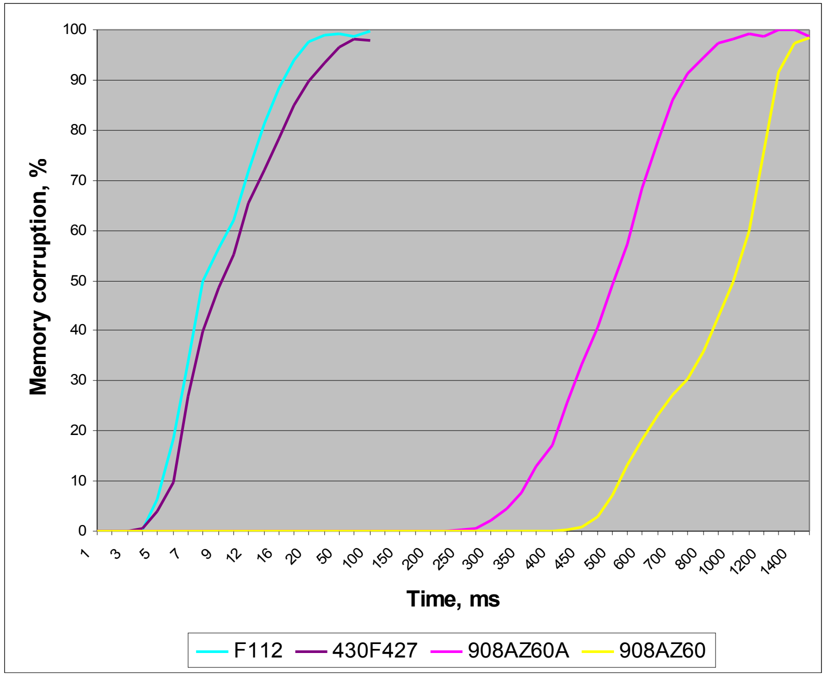


Data remanence experiments with SRAM

- Heating
  - with Peltier elements up to +80ºC (+176ºF)
- Cooling
  - with Peltier elements down to −20ºC (−4ºF)
  - with Freeze-It aerosol down to −40ºC (−40ºF)
- Monitoring with digital thermometer

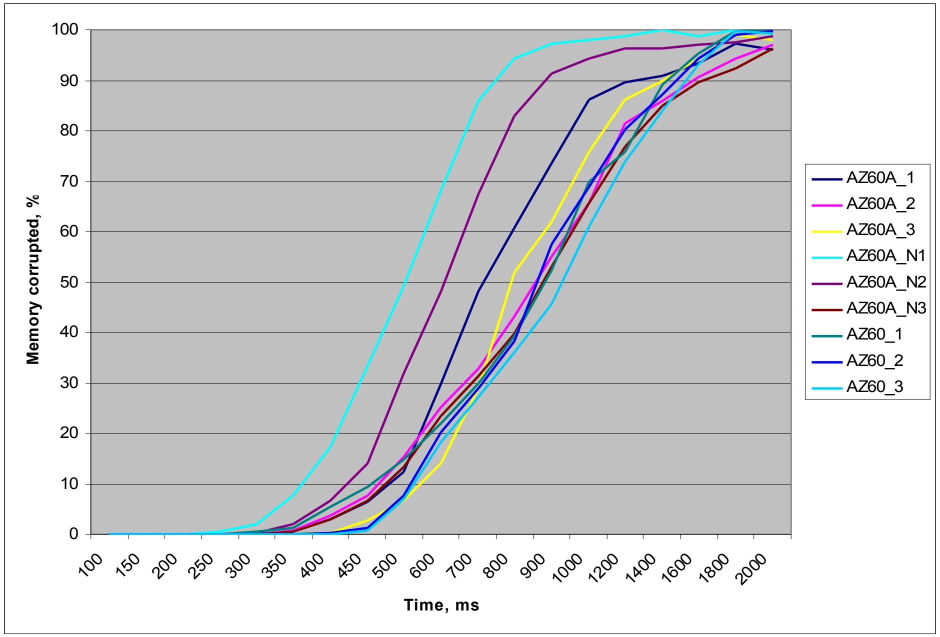
Data remanence experiments with SRAM

- Measuring data remanence at room temperature: +20ºC (+68ºF)
  - fill the memory with test patterns (all 0s, all 1s, random)
  - ground all I/O lines
  - connect power supply line to GND for required time
  - power up the chip and read the memory
- Data remanence time for 50% corruption is less than 1 second



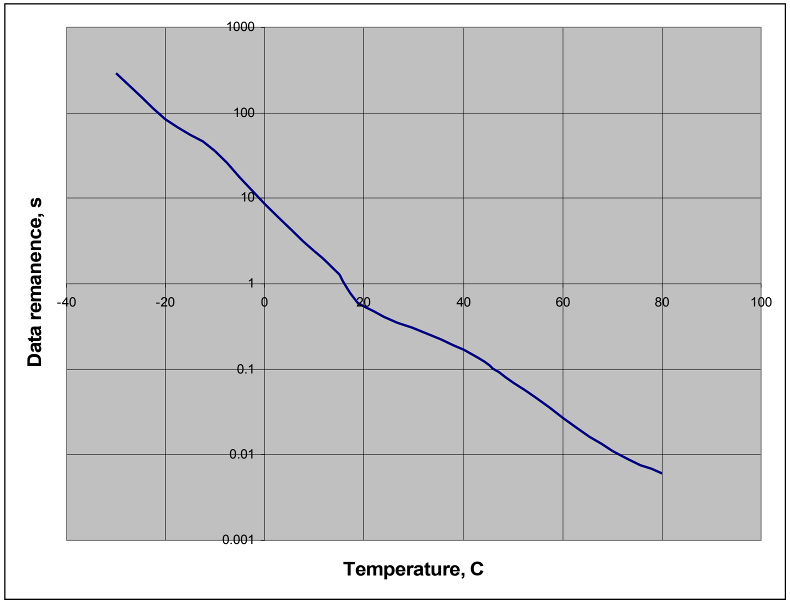
Data remanence experiments with SRAM

- Measuring variation of data remanence time between similar chips
  - room temperature of +20ºC (+68ºF)
  - 3 samples of Freescale MC68HC908AZ60 (0.8µm process)
  - 3 samples of Freescale MC68HC908AZ60A (0.5µm process, mask 2J74Y)
  - 3 samples of Freescale MC68HC908AZ60A (0.5µm process, mask 3K85K)
- Time variation between samples from the same batch could be larger than between different devices

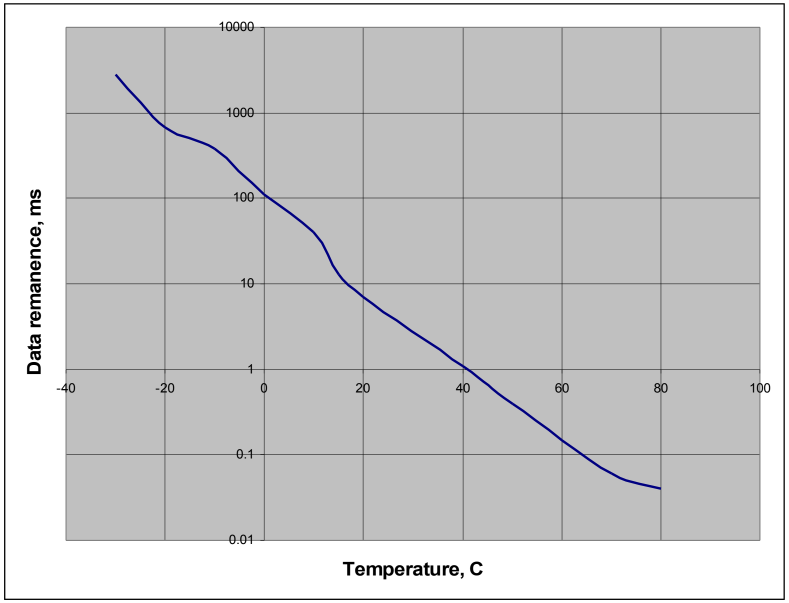


Data remanence experiments with SRAM

- Low and high temperature testing on samples of MC68HC908AZ60A and MSP430F112
  - cooling down to −30ºC (−22ºF)
  - heating up to +80ºC (+176ºF)
- Almost linear in logarithmic scale
  - MC68HC908AZ60A: from 5 minutes at −30ºC to 10ms at +80ºC
  - MSP430F112: from 3 seconds at −30ºC to 50µs at +80ºC



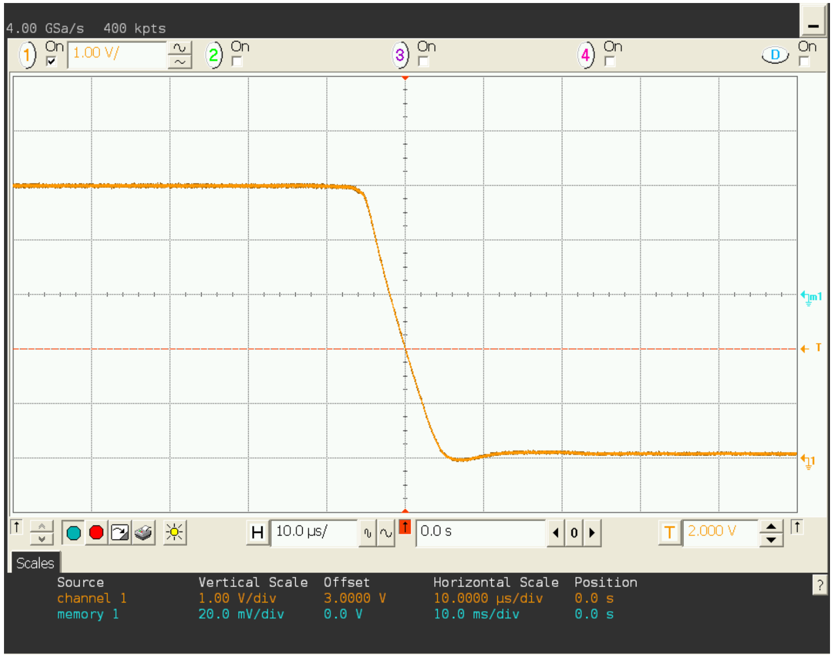
MC68HC908AZ60A



MSP430F112

Data remanence experiments with SRAM

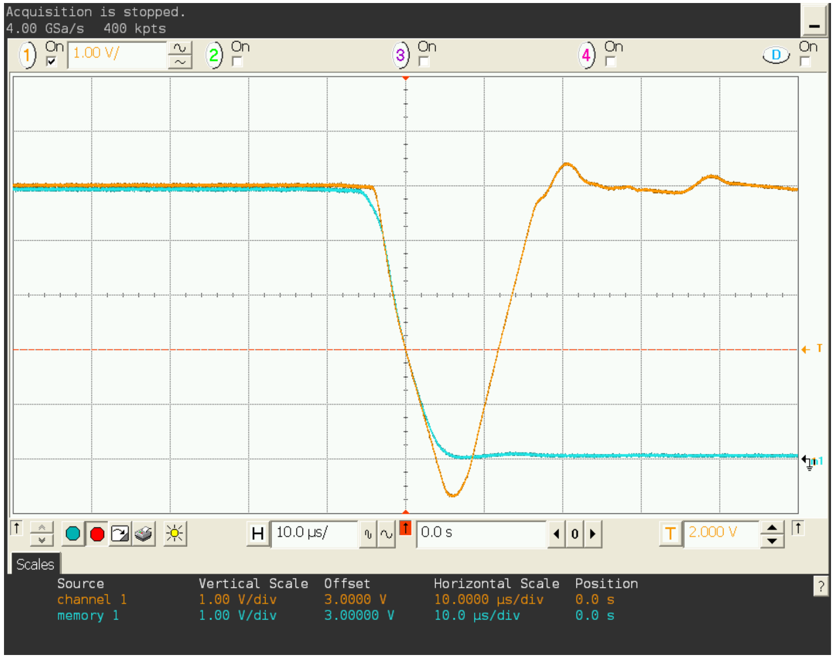
- Switching off the power supply
  - gradually reducing the voltage from Vcc to GND within 5µs then bringing it back
  - applying a glitch that surges below GND level for a very short time
- Glitch parameters
  - must go below −0.6V to take effect
  - formed using OpAmp with capacitive load



```
4.00 GSa/s  400 kpts
```

1.00 V/ | 10.0 µs/ | 0.0 s | 2.000 V

```
Source          Vertical Scale  Offset       Horizontal Scale   Position
channel 1       1.00 V/div      3.0000 V     10.0000 µs/div     0.0 s
memory 1        20.0 mV/div     0.0 V        10.0 ms/div        0.0 s
```



```
Acquisition is stopped.
4.00 GSa/s  400 kpts
```

1.00 V/ | 10.0 µs/ | 0.0 s | 2.000 V

```
Source          Vertical Scale  Offset       Horizontal Scale   Position
channel 1       1.00 V/div      3.0000 V     10.0000 µs/div     0.0 s
memory 1        1.00 V/div      3.00000 V    10.0 µs/div        0.0 s
```

Data remanence experiments with SRAM

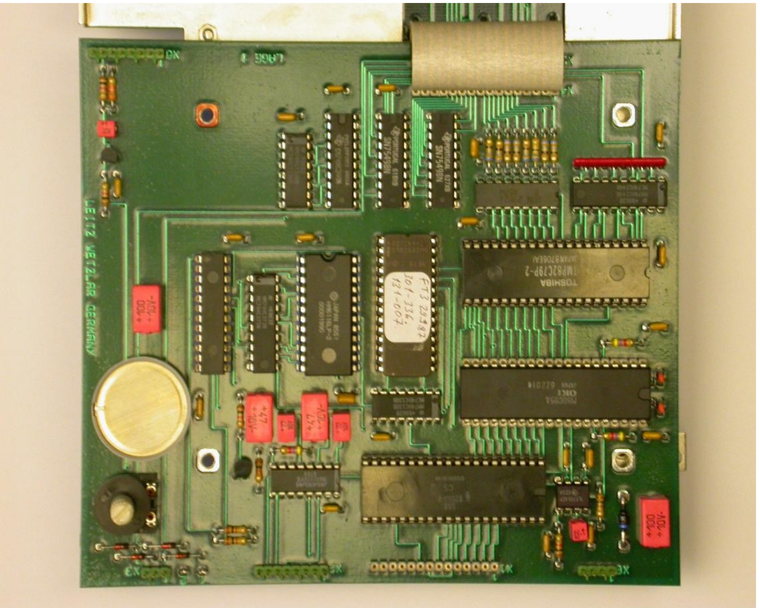
- Glitch effect on the data remanence time of MC68HC908AZ60
  - was reduced from 1 second to 5μs at +20ºC (+68ºF)
  - was reduced from 8 minutes to 10μs at −30ºC (−22ºF)
- Glitch effect on the data remanence time of MC68HC908AZ60A
  - was reduced from 0.5 seconds to 5μs at +20ºC (+68ºF)
  - was reduced from 5 minutes to 8μs at −30ºC (−22ºF)
- Glitch effect on the data remanence time of MSP430F112
  - was reduced from 8ms to 3μs at +20ºC (+68ºF)
  - was reduced from 3 seconds to 5μs at −30ºC (−22ºF)

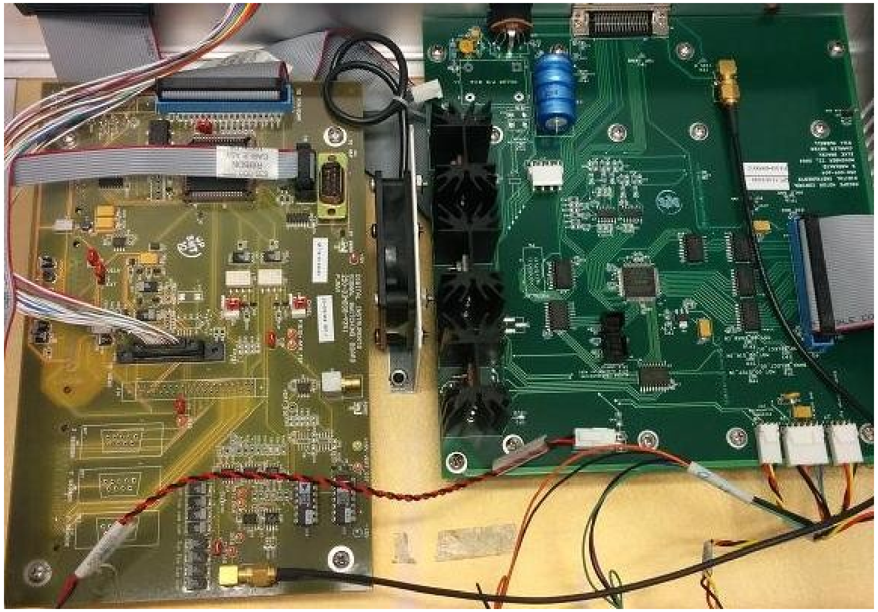
Data remanence experiments with NVM

- The effect of the power glitch on the erase process in EEPROM and Flash memory
  - Security fuses are designed in a way such that their erasure takes longer, this preserves the confidentiality of the code and data memory
  - the power glitch was applied before the Chip Erase command
  - this resulted in the longer time necessary for the main memory array to be erased, but the security fuse erasure was almost unaffected
  - as a result the security of some chips was compromised
- Which chips are affected
  - only old microcontrollers fabricated with 0.6μm and larger process (PIC16F873, Atmega163, ATtiny12)
  - lack of success in glitching modern microcontrollers and SoCs does not mean they are secure – more exhaustive testing might be necessary to confirm their immunity

Data retention in NVM

- Old automotive, industrial and equipment controllers
  - firmware stored in external EPROM, embedded EPROM or EEPROM
  - after certain time equipment starts to fail or behaves in an odd way
- Challenges
  - find the cause of the problem
  - find the way to prolong the life of equipment



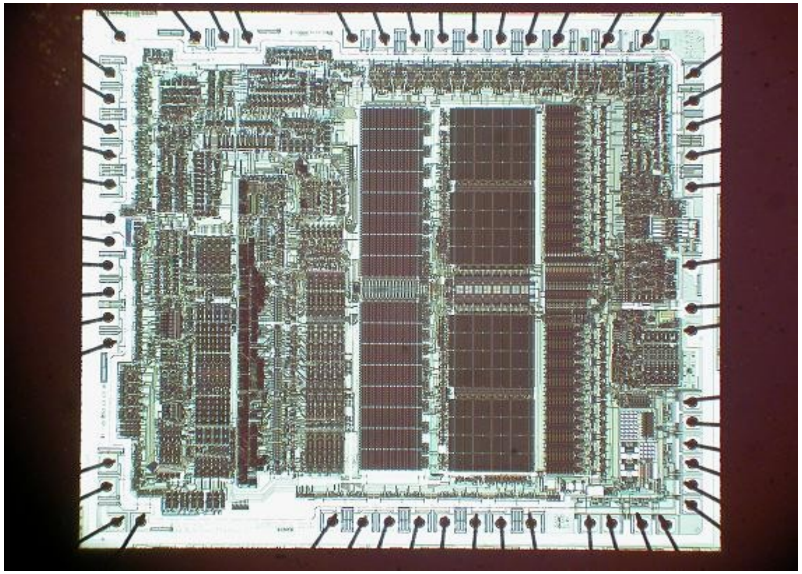


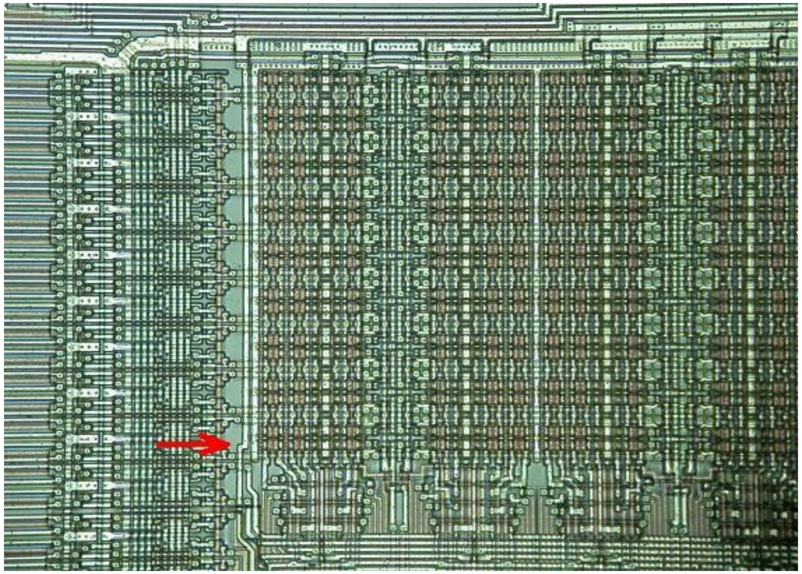
Data retention in EEPROM and Flash

- Data retention time of storage memory
  - Battery backed SRAM: 10–15 years
  - Mask ROM: >100 years
  - UV EPROM: 20–40 years
  - EEPROM: 10–40 years
  - Flash memory: 20–100 years
- Reliability issues
  - information inside the EEPROM and Flash memory cell is stored in the form of electrical charge on the floating gate of storage transistor
  - charge of between 100,000e^- in old devices and 100e^- in modern chips
  - the charge leaks over time especially at higher temperatures
  - read disturb could cause charge leakage during normal read operations
- Hardware security issues
  - similar EEPROM cells are used to control memory mapping and security access
  - if the contents of special fuses is disturbed this could result in malfunction of the embedded controller system

Data retention in EEPROM and Flash

- EEPROM evaluation in MC68HC11A1 microcontroller
  - was used in industrial controller which has stopped working
  - data retention time was specified by the manufacturer as 10 years
  - on-chip EEPROM array has extra row for non-volatile OPTION register
- Accelerating the ageing process
  - UV light was used to slowly erase main memory array and extra row
  - the time until 50% of cells changed their state was the same
  - this confirms the guaranteed retention time for chip configuration as 10 years





Limitations and improvements

- Relatively old devices were tested, hence, latest microcontrollers, SoCs and FPGAs should be tested for data remanence issues
- Power glitching is applied to the whole chip, hence, it has very limited selectivity
- Combining power glitching with laser fault injection could bring new capabilities
- Data retention time should be tested on real devices for critical applications at higher temperatures
- The life of equipment could be extended if the memory contents is refreshed by recovering the information and reprogramming the chip

Future Work and Collaboration

- More extensive involvement with Failure Analysis methods
  - need more interdisciplinary research
  - make improvements to existing methods for direct memory recovery
- Need for closer collaboration between industry and academia
  - test innovative ideas (sometime non-standard and crazy)
  - funding is essential, but it might be possible to go beyond state-of-the-art
- New methods in data recovery from embedded memory
  - combined methods did work for semi-invasive techniques so should do for invasive
  - more research and development is needed to find new innovative solutions
  - Work-in-Progress webpage for latest breakthrough news: http://www.cl.cam.ac.uk/~sps32/dec_proj.html

Conclusion

- Data remanence could pose a problem for modern devices with embedded SRAM
- Data remanence time at low temperatures can be significantly reduced with a power glitch: from minutes to microseconds at −30ºC
- Power glitching could affect the security of semiconductor devices
- Data retention time of EEPROM and Flash memory is affected by high temperature and could result in malfunction of controllers in automotive and industrial applications
- If data storage cells fails this could change a few bits of information, however, if the configuration cell changes its state this could have both security and reliability consequences
- Data remanence and data retention could have an adverse effect on hardware security of semiconductor devices that would result in data recovery by adversaries