Local Heating Attacks on Flash Memory Devices

Dr Sergei Skorobogatov

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

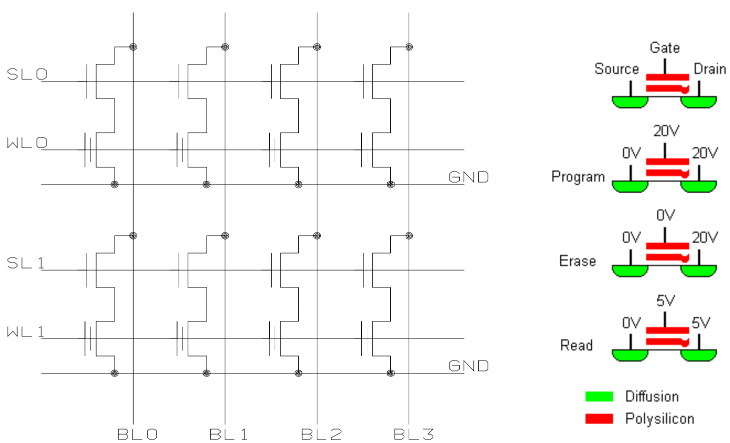
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

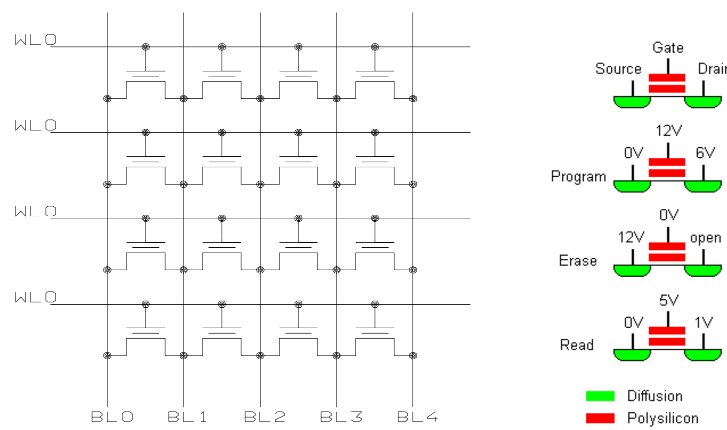
Introduction

- Semi-invasive attacks were introduced in 2002 ("Optical fault induction attacks", CHES-2002)
  - fill the gap between non-invasive and invasive attacks
  - do not require direct access to internal wires
  - local heating was proposed as possible fault attack
- EEPROM and Flash memory
  - used in many microcontrollers, smartcards and secure memories
  - offer non-volatile storage for passwords and encryption keys
  - have limited resource and data retention time
- The presented research shows how local heating can be used to implement modification attacks on EEPROM and Flash memory

Background

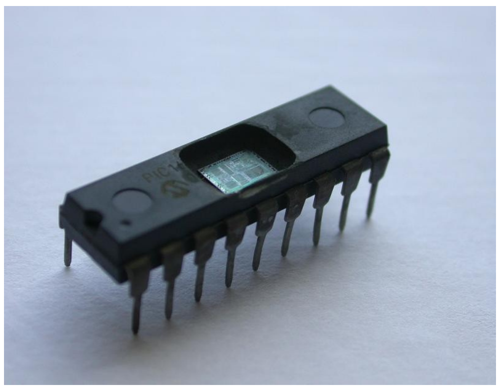
- Structures of EEPROM and Flash memory
- Floating-gate transistor used as a storage element
- Have different cell size and write/erase operation modes
- Limited data retention time is caused by loss of charge on the floating gate. Loss is increased at higher temperature

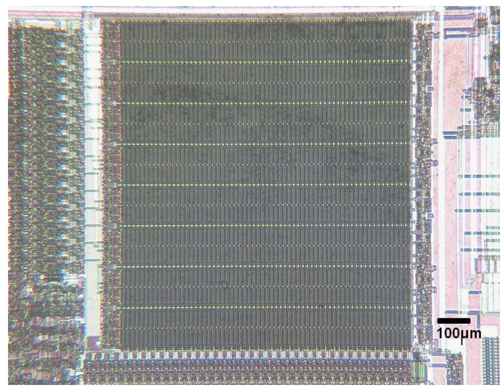


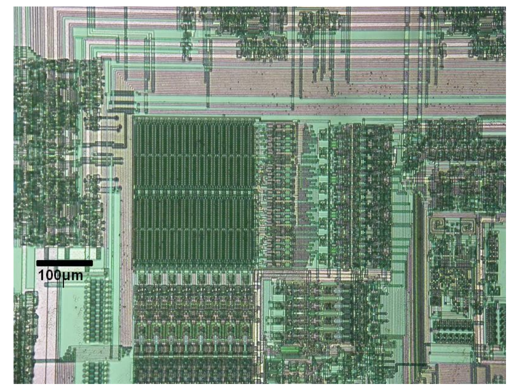


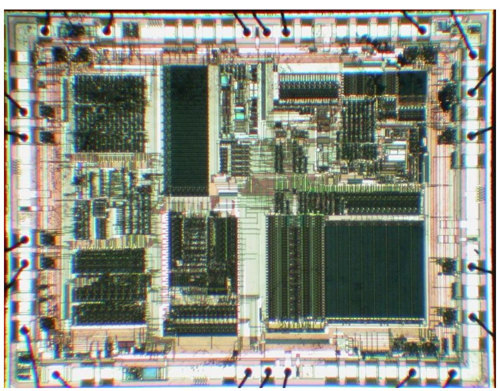
Experimental setup

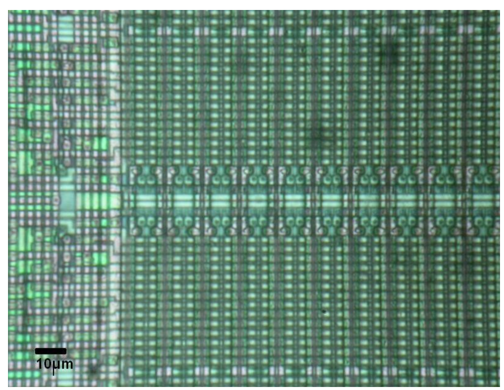
- Sample preparation
- Locating Flash and EEPROM

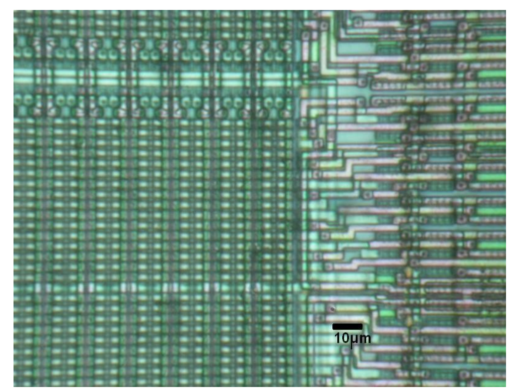






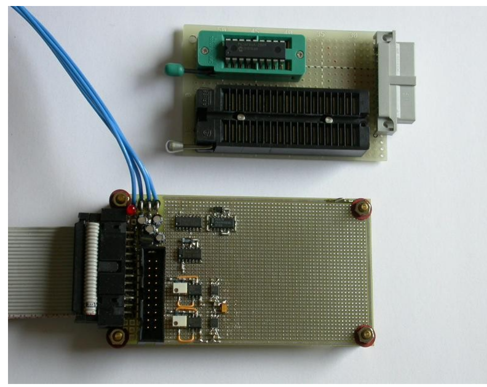


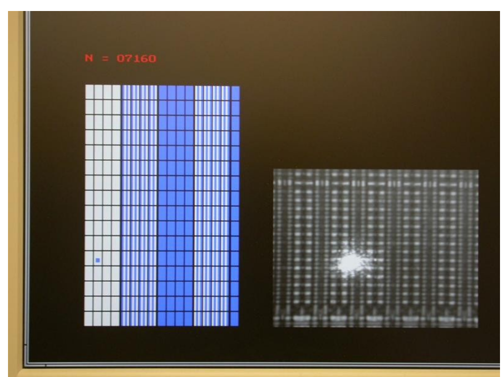




Experimental setup

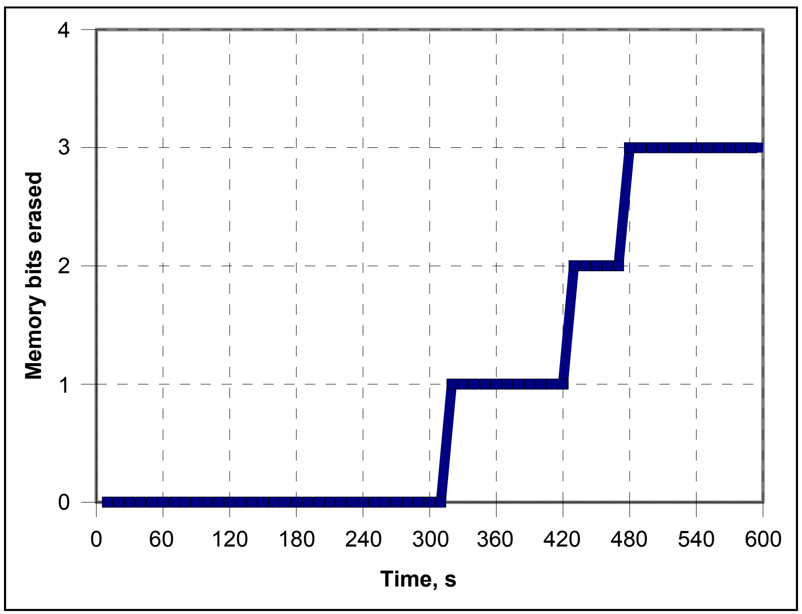
- Localised heating using cw lasers
- Test board and software were used for analysis
- For comparison a whole chip was heated up on a hotplate

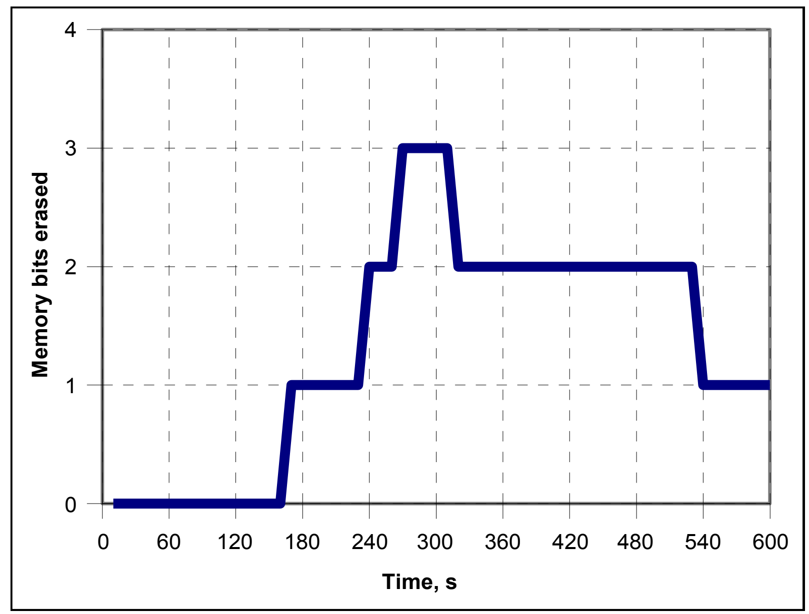




Results

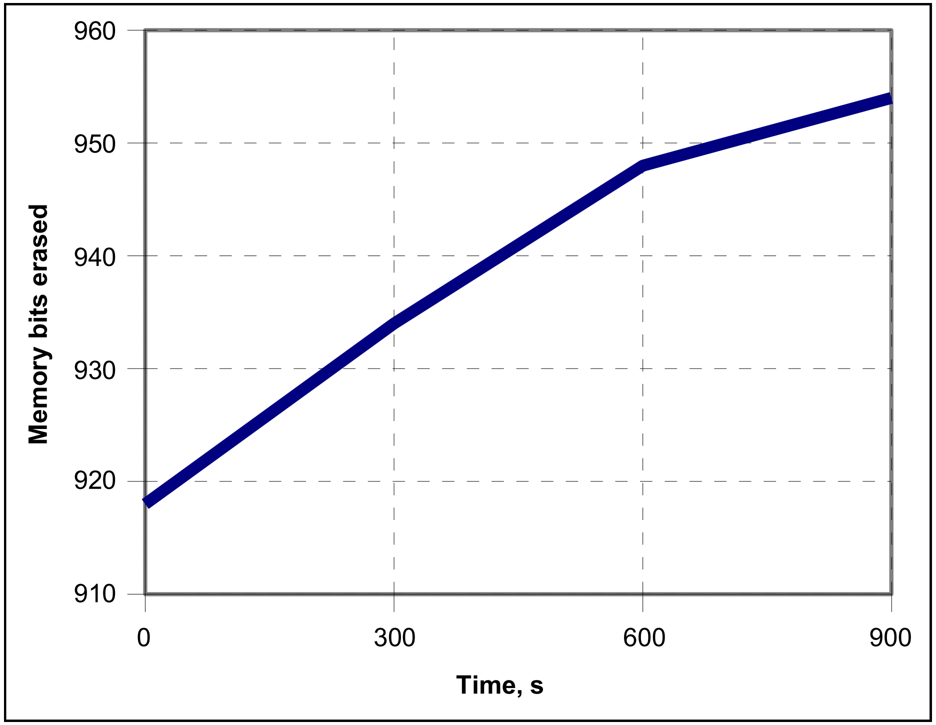
- Heating EEPROM cells with a 650 nm cw laser
  - 50 mW laser erases one cell and eventually two neighbour cells
  - 100 mW laser erases faster but causes permanent damage to the memory cells





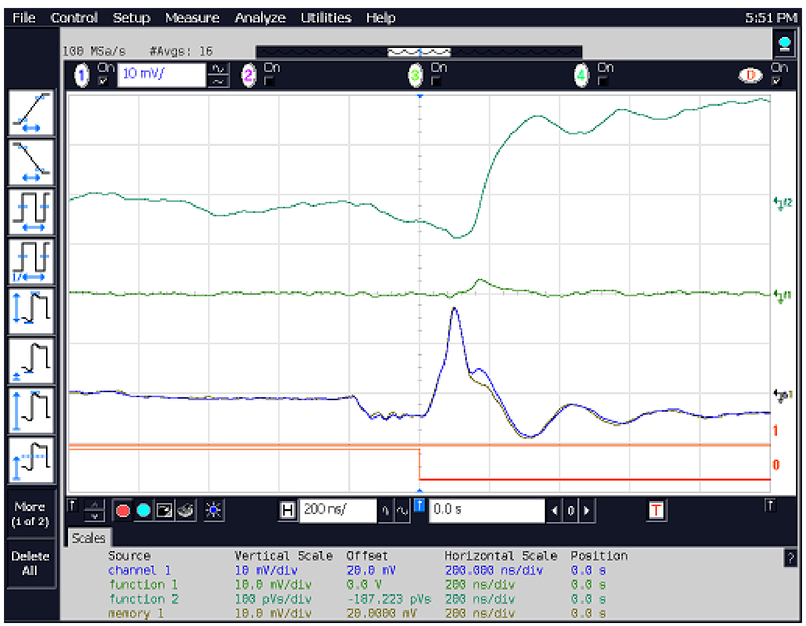
Results

- Heating on a hotplate at 450ºC
  - partially erased sample was used
  - aluminium foil was used to prevent loss of heat
  - plastic degrades at higher temperature

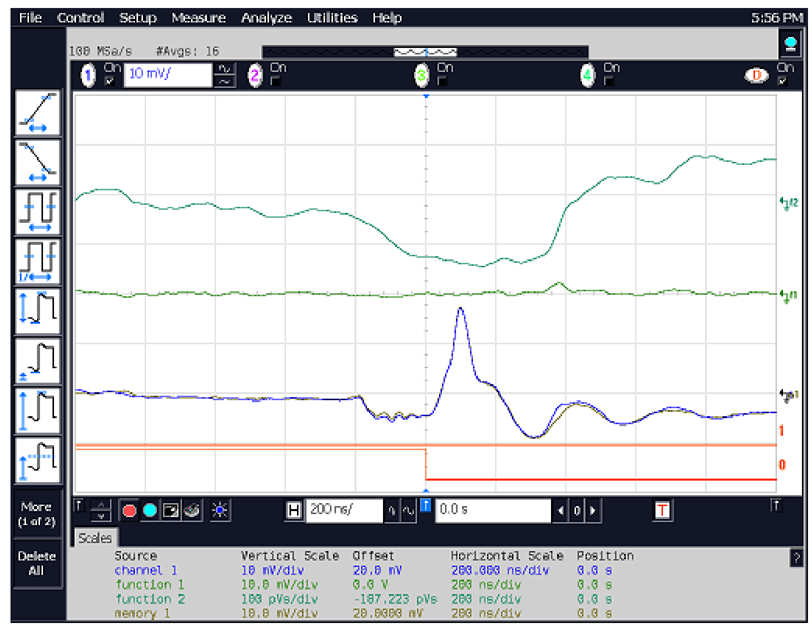


Results

- Detecting partially modified Flash memory cells
  - discharging process is slow and non-reversible
  - modification may result in non-operational chip (CRC, protection)
  - the state of cell is an analog value which is sampled by read-sense amplifier, and that can be noticed in the power trace
  - can be used for locating cells and for data recovery



0x3FFE vs 0x3FFF



0x3FFE vs 0x3FFE (10 mW 30 sec)

Limitations and improvements

- Data recovery
  - slow process
  - high-power lasers can cause damage to memory cells
- Modern chips
  - three or more metal layers prevent direct access by the laser
  - impossible to influence a single cell in 0.5 μm and smaller chips
- Backside approach
  - IR lasers (wavelength > 1000 nm)
  - lower spatial resolution
  - more powerful lasers are required due to loss on absorption
  - with 50 mW laser no noticeable difference after 30 minutes
  - substrate thinning might be required to reduce the time

Countermeasures

- Use modern chips with multiple metal layers
- Metal shielding over sensitive memory areas
- Light sensors
- Encrypt keys and passwords
- Use redundancy check

Conclusions

- EEPROM and Flash memory are sensitive to local heating
- Memory contents can be altered using affordable semi-invasive technique
- Partially modified memory cells can be detected through power analysis techniques, but still undetectable by embedded software
- Possibility of partial reverse engineering of memory structure and its content
- In modern chips it is impossible to alter just a single cell. However, fault attacks can still be carried out
- Backside approach can help in modern chips, but has lower spatial resolution and requires more powerful lasers

Further research

- Fault injection attacks
  - advanced memory extraction techniques
  - real-time injection
- Side-channel attacks
  - optical emission analysis attacks (FDTC-2009, September)
  - improved power analysis attacks: more effective (higher precision and resolution), faster (higher speed) and cheaper (lower cost)