Data remanence in non-volatile semiconductor memory (Part II)

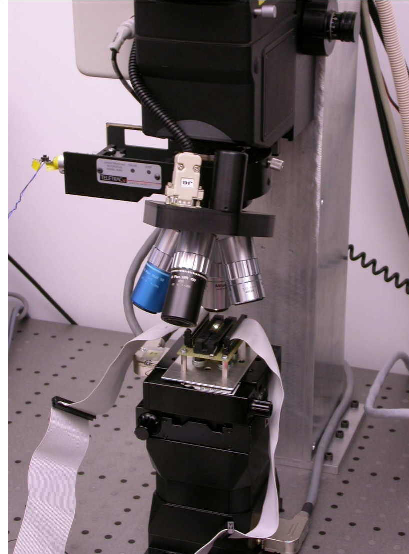
UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

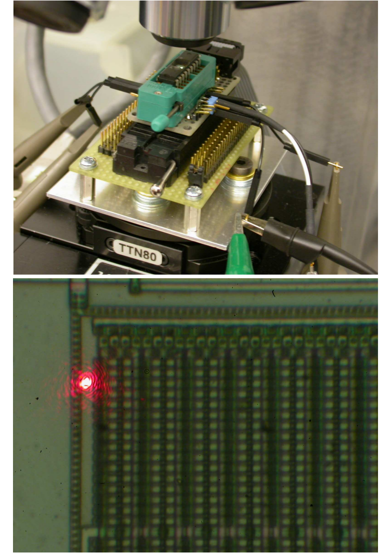
Sergei Skorobogatov

Introduction to the semi-invasive approach

Data remanence is the residual physical representation of data that has been erased or overwritten. Microcontrollers and smartcards keep secret data and cryptographic keys in non-volatile reprogrammable memory, such as EEPROM or Flash. These memories store bits of information in the form of charge in the floating gate of a transistor. After an erase operation, some of this charge remains. If this residual charge can be detected (in one way or another), previously stored information could be recovered, which may represent a security risk.

The semi-invasive approach requires access to the chip surface, and as opposed to invasive methods, the passivation layer of the chip remains intact. These techniques do not require physical access to the internal wires inside the chip, thus reducing the preparation time. Crucial to semi-invasive analysis is an optical microscope suitable for laser operation, with long working distance and high-resolution objectives. This allows working with partially depackaged chips and focusing the laser at sub-micron features.

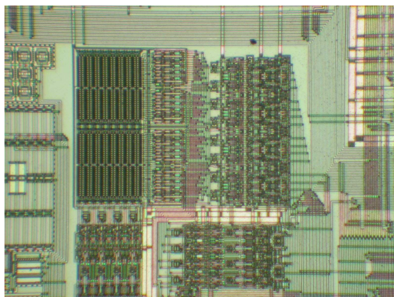


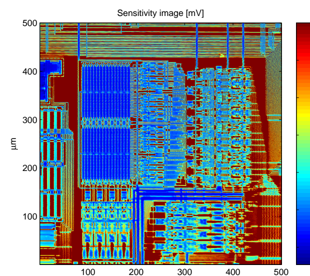


Laser microscope used for semi-invasive analysis, test board with a chip and the laser focused with 100× objective

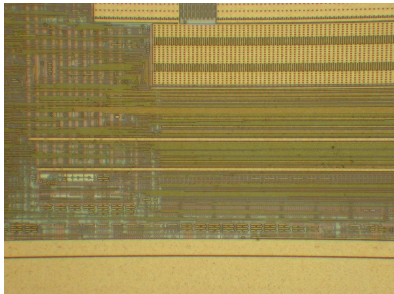
Semi-invasive data recovery from erased memory

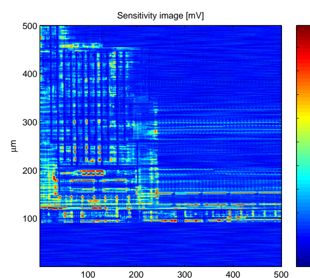
The fast write/erase process in EEPROM and Flash memory leaves very little chance to recover information using non-invasive techniques. However, semi-invasive optical fault-injection techniques allow us to influence the on-chip sense amplifiers such that they can distinguish minor changes in the threshold voltage of erased floating-gate transistors inside memory cells. This makes it possible to detect the 'before-erase' state of the memory cell.



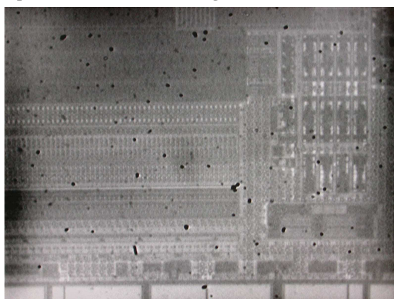


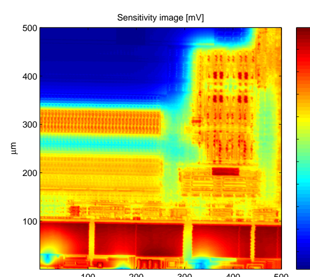
Optical and laser-scanned images of EEPROM area in PIC16F84A microcontroller





Optical and laser-scanned images of EEPROM area in ATmega8 microcontroller





Infrared rear-side and laser-scanned images of EEPROM area in ATmega8 microcontroller

In order to find light-sensitive points on the chip surface, a standard laser scanning technique can be applied to the chip, revealing the locations that produce a high photocurrent. By comparing the scanned image with the optical image, exact locations within the read sense amplifiers, where the laser pulses should be injected, can be found.

Modern semiconductor chips are built using deep submicron technologies (0.18 μm or smaller), which, together with five or more metal layers covering the chip surface, make semi-invasive analysis ineffective. In such chips, only small areas on the surface are light sensitive.

One improvement could be approaching memory read-sense amplifiers from the rear side of the chip. In this case, laser radiation with a longer wavelength (>1000 nm) must be used, together with suitable microscope optics and near-infrared cameras, for example, Mitutoyo FS70L microscope with NIR objectives and a Hamamatsu C2741-03 camera. However, such lasers cannot be focused at an area smaller than 0.6 μm because of diffraction limits. In this case, reducing the thickness of the silicon substrate might be required, such that shorter laser wavelengths may be used.

One possible countermeasure could be to rewrite all memory locations to their charged state before the erase operation. Our tests have shown that, in this case, it becomes infeasible to distinguish between previously programmed and non-programmed memory cells.

Nevertheless, the fact that data can be recovered from erased memory cells in such devices can pose a significant security risk. Security devices should be tested for possible data remanence effects.

Sergei Skorobogatov: Data Remanence in Flash Memory Devices. CHES 2005 Workshop, LNCS 3659, Springer-Verlag, ISBN 3-540-28474-5, pp. 339–353

www.cl.cam.ac.uk/~sps32/
2006-07-20