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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

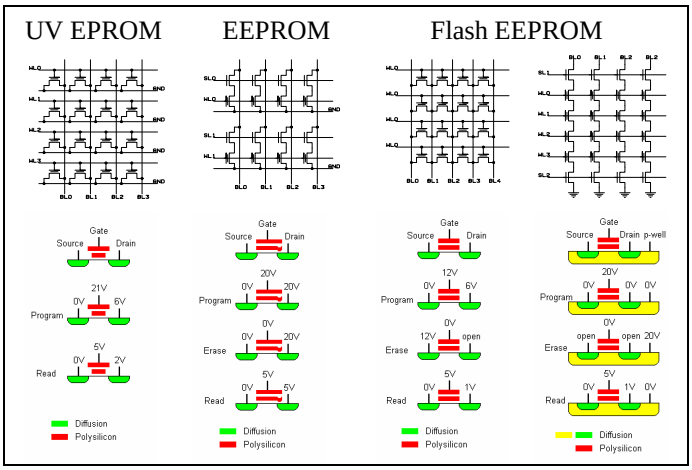
Sergei Skorobogatov
Web: www.cl.cam.ac.uk/~sps32/
Email: sps32@cl.cam.ac.uk

Introduction

Data remanence is the residual physical representation of data that has been erased or overwritten. In non-volatile programmable devices, such as UV EPROM, EEPROM or Flash, bits are stored as charge in the floating gate of a transistor. After each erase operation, some of this charge remains. It shifts the threshold voltage (V_{TH}) of the transistor which can be detected by the sense amplifier while reading data.

Microcontrollers use a 'protection fuse' bit that restricts unauthorized access to on-chip memory if activated. Very often, this fuse is embedded in the main memory array. In this case, it is erased simultaneously with the memory. Better protection can be achieved if the fuse is located close to the memory but has a separate control circuit. This allows it to be permanently monitored as well as hardware protected from being erased too early, thus making sure that by the time the fuse is reset no data is left inside the memory.

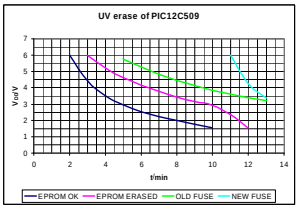
In some smartcards and microcontrollers, a password-protected boot-loader restricts firmware updates and data access to authorized users only. Usually, the on-chip operating system erases both code and data memory before uploading new code, thus preventing any new application from accessing previously stored secrets.



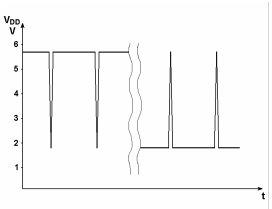
Structure, cross-section and operation modes for different memory types

How much residual charge is left inside the memory cells after a standard erase operation? Is it possible to recover data from erased memory?

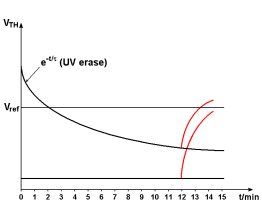
Non-invasive data recovery from erased memory



EPROM memory state at various V_{DD}

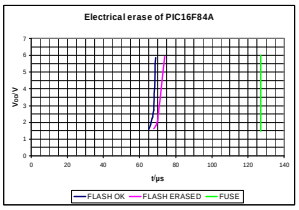


Power glitching technique

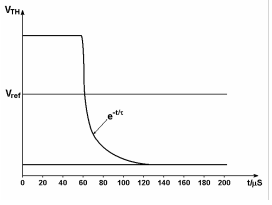


Charge alteration technique

Erasing EPROM with UV light is a very slow process, typically taking 10–20 minutes. Usually, the read sense amplifier compares the threshold voltage of memory transistors with half of the power-supply voltage. This allows the memory to operate under a wide range of supply voltages. We can change the power supply voltage briefly, to affect this reference voltage enough to sense the 'erased' data, without disturbing normal operation of the device. If the floating gate was discharged deeply enough to reveal no data at any supply voltage, another technique can be used. It involves careful injection of a precisely controlled amount of charge into every memory cell, thus shifting their threshold voltages to the level where a difference between programmed and non-programmed cells can be detected.

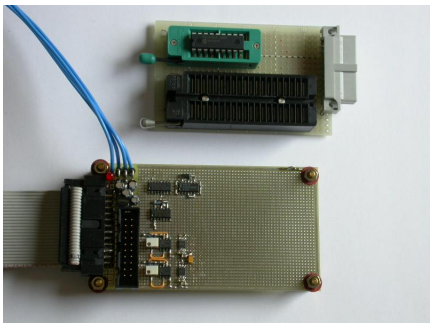


Flash memory state at various V_{DD}



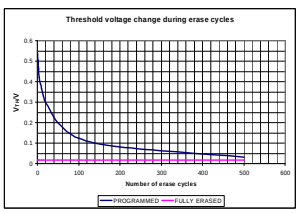
Charge loss during electrical erase

The fast write/erase process in EEPROM and Flash memory leaves us no chance to recover information using the above techniques. If the floating gate is discharged exponentially, like a capacitor, by the time the security fuse is reset, no significant charge would be left inside the floating-gate transistor. Taking into account that a standard erase cycle is 10 ms long, this ensures protection against attempts to recover erased data.

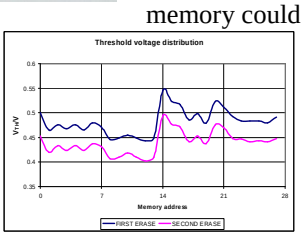


Test board for data remanence evaluation

To investigate the actual situation with data remanence in EEPROM and Flash devices, a special test board was built. It applies power glitches synchronized to the clock signal. By exploiting one of the previously found vulnerabilities of EEPROM/Flash memory in conjunction with power glitching, precise measurements of the threshold voltage for each individual memory transistor became possible. Applying this technique to the Microchip PIC16F84A microcontroller revealed that, even after a hundred consecutive erase cycles, the program code inside the Flash memory can be fully restored. However, the EEPROM data memory could be recovered only if less than ten bulk erase cycles were applied.



Threshold change during erase cycles



V_{TH} distribution along the memory

Only a fraction of all microcontrollers are vulnerable to the above techniques, because many benefit from voltage monitors and internal supply stabilizers. In addition, rewriting all the memory locations to their charged state makes data recovery infeasible. Nevertheless, the fact that data can be recovered from erased memory cells in such devices can form a significant security risk. Secure devices should be tested for possible data remanence effects.