Hardware Security

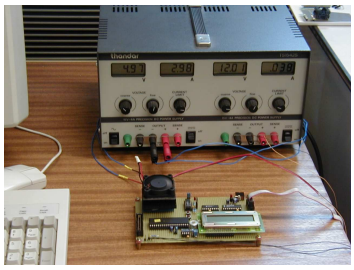
Sergei Skorobogatov

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

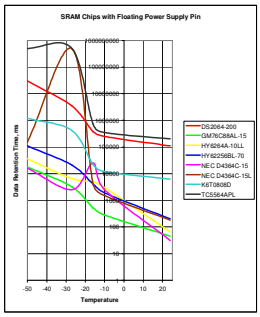
UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Data Remanence in Static RAM

SRAM is used in many security systems and smartcards for temporary storage of secret data and crypto keys. It is commonly believed that the information from such memory disappears immediately after the power supply is removed. Our experiments showed a significant temperature dependent data-retention time in modern SRAMs, of up to 10 hours.



Test board setup

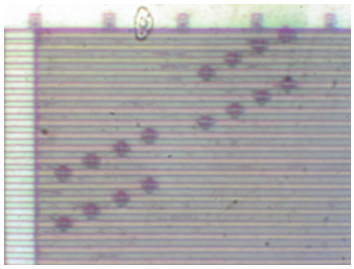


Results for SRAMs

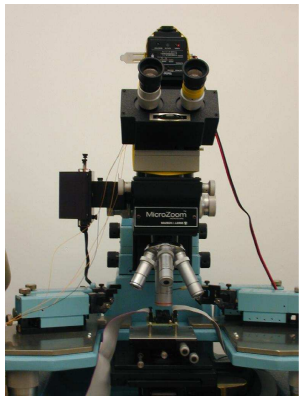
Invasive and Non-invasive Attacks

Secure microcontrollers and smartcards are designed to protect both the confidentiality and integrity of sensitive information. Here we evaluate secure devices against known attacks and search for new ones to design appropriate protection. Attacks tend to be either invasive, using chip testing equipment such as probing stations and focused-ion-beam workstations to extract data from the chip directly, or non-invasive, exploiting unintentional electromagnetic emissions, protocol design flaws and other vulnerabilities of the external interface.

Laser cutter system



Test points on bus created using FIB workstation

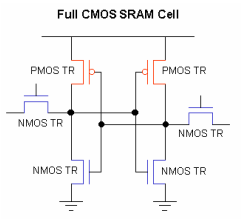


Manual probing station

Semi-Invasive Attacks

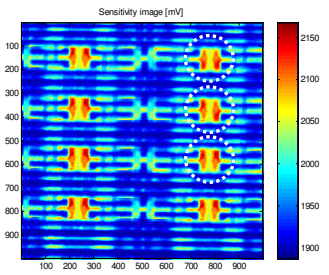
This is our new class of attacks. By "semi-invasive" we mean that, like invasive attacks, they require depackaging the chip to get access to its surface. But the passivation layer of the chip remains intact – no electrical contact is required to the internal metal lines, so there is no mechanical damage to the silicon.

These attacks are not entirely new – UV light has already been used to reset security fuses in some microcontrollers. Our new approach is to use a photoflash lamp mounted on the camera port of a microscope to induce a fault in normal chip operation, causing it to leak sensitive information.

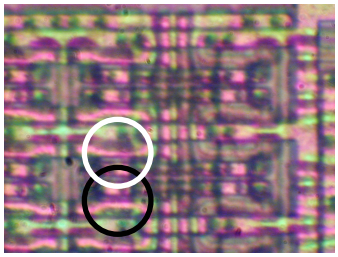


SRAM cell diagram

Photoflash used to inject faults



Laser scanning image of SRAM cells (100×100 µm)



Attack areas on SRAM in microcontroller

We also succeeded in extracting information directly from memory without using the read-out circuitry. To do so, we scanned the chip with a laser while monitoring its leakage current.