Optically enhanced position-locked power analysis

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

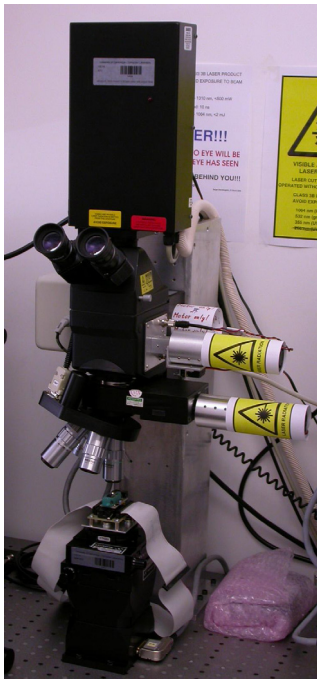
Sergei Skorobogatov

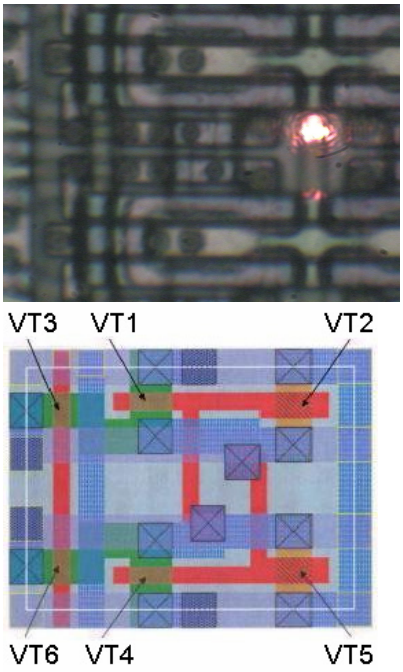
Introduction to the technique

Optical enhancement of power analysis is a new and innovative technique that allows the current through an individual transistor to become visible in the circuit's power trace. In conventional power analysis, power consumption is measured for a whole chip rather than on a small area of interest. As a result, power transitions in areas that are not relevant to the data processing also affect the power trace. Also, the power fluctuations are affected by the number of bits being set or reset (Hamming weight of data), rather than the actual value of the manipulated data.

Optical enhancement to power analysis techniques presupposes a semi-invasive approach which requires access to the chip surface. However, this technique does not require physical access to the internal wires inside the chip, thus reducing the preparation time compared to invasive methods. Crucial to semi-invasive analysis is an optical microscope suitable for laser operation, with a long working distance and high-resolution objectives. This allows working with partially depackaged chips and focusing the laser at sub-micron features.

By focusing a laser on a specific area on the chip surface, it is possible to monitor the logic state of an individual transistor, as well as the activity of a particular memory cell. This is highly useful for security analysis, allowing faster and less expensive solutions.





Laser microscope with PIC16F84 board, laser focused on its SRAM cell with 100× objective and similar cell layout

Experimental results

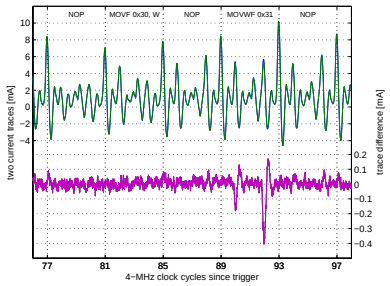


Fig.1. Write: (0x00→0xFF) and same with laser on VT1

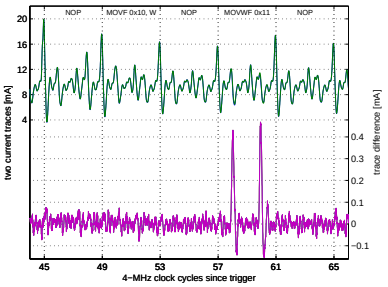


Fig.2. Write: compare (0x00 → 0x00) and (0x01 → 0x00)

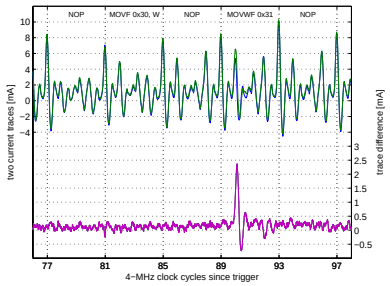


Fig.3. Write: (0x00→0xFF) and with laser on VT1+VT4

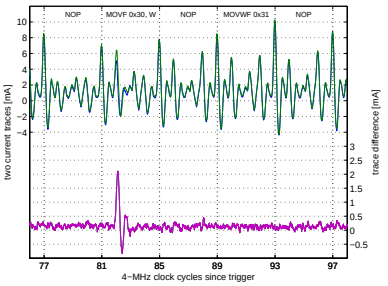


Fig.4. Read: (0xFF) and same with laser on VT1+VT4

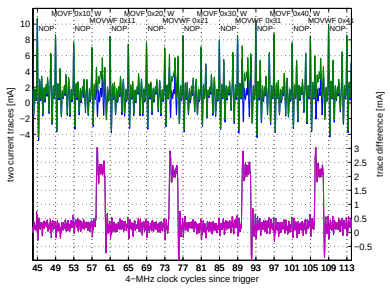


Fig.5. Access: (0x00, 0xFF) and with laser on VT3+VT6

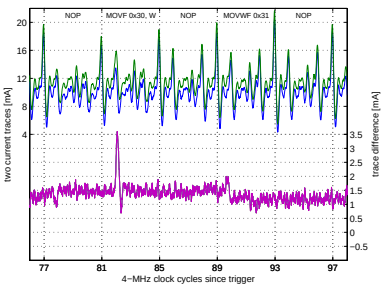


Fig.6. Read: (0xFF) and with IR rear laser on VT1+VT4

When a laser is focused on the VT1 transistor of the PIC16F84 SRAM memory cell and writing into this cell happens, an about 0.4 mA change in the power trace can be observed (Fig.1). For comparison, the conventional power analysis results showed a similar change in the power consumption for a single-bit difference in the memory contents (Fig.2). However, the same technique applied to the memory cells being read, did not produce any noticeable results, unless many power traces were averaged. This is because writing into an SRAM cell causes a significantly larger current response than a read operation, in which laser-injected current is not high.

By focusing the laser on the region between the VT1 and VT4 transistors, significantly higher changes in the power trace can be observed (Fig.3), and what is more important, for both write and read operations (Fig.4), thus allowing access detection. This happens because the timing characteristic of the cell changes when both inverters are influenced with a laser.

Interesting results were achieved with the laser focused on the area between the cell-select transistors (VT3 and VT6). In this case, access to any of the memory cells inside the memory array column produced a very noticeable difference in the power consumption (Fig.5). The same response was obtained when a laser with higher power was focused between VT1 and VT4. These approaches can be used for access-event triggering.

Modern chips normally have multiple metal layers over their active areas, preventing direct access with a laser beam. Accessing the chip from its rear side can circumvent this obstacle and the power-trace difference is very similar to the one from the front side (Fig.6).

Sergei Skorobogatov: Optically Enhanced Position-Locked Power Analysis. CHES 2006 Workshop, LNCS 4249, Springer-Verlag, ISBN 3-540-46559-6, pp. 61–75