Optical surveillance on silicon chips

Sergei Skorobogatov

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Introduction

Transistors emit photons when they switch. This has been well known for decades and is actively used in failure analysis. So far, observation of such emissions was associated with sophisticated and expensive equipment, because only a very limited number of photons emitted per every switch – usually 10^{-2} to 10^{-4}. The peak of emission is in the near-infrared (NIR) spectrum (900 to 1200 nm) and this poses restrictions on sensors selection. The emission comes from an area close to the drain and primarily from the NMOS transistor (Fig.1). Optical emission significantly increases at higher power supply voltages (Tab.1).

Optical emission has good correlation with power analysis and can be used for characterisation of leaking areas for later improvement of protection against power analysis attacks. A set of experiments was carried out using a PMT sensor attached directly to the opened chip (Fig.2). The results, presented in Fig.3-4, reveal that optical emission has higher bandwidth and thus data appearing at different times can be separated for further analysis.

My research shows that modern low-cost CCD cameras are adequate for detecting photons emitted by modern CMOS circuits. Different sensors used for emission analysis are compared in Table 2. Photomultipliers are very fast, but they have limited sensitivity in the NIR region. Monochrome CCD cameras have good NIR sensitivity and low dark current, which is important with long exposure times.

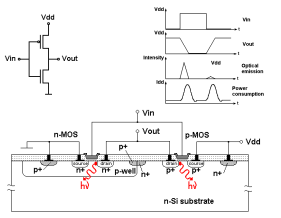


Fig.1. Photon emission from CMOS

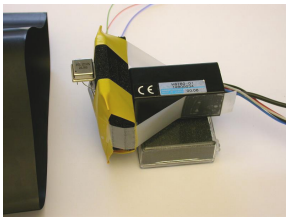


Fig.2. PMT sensor setup

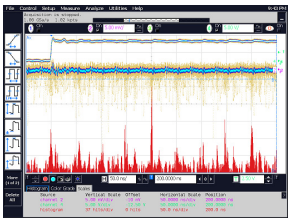


Fig.3. PMT results for PIC16F628

Fig.4. SPA results for PIC16F628

Table 1. Optical emission at different power supply voltages for PIC16F628

Power supply voltage	3.5 V	4.0 V	4.5 V	5.0 V	5.5 V	6.0 V
Photometry results	1046	1286	2427	8400	23292	43026

Table 2. Comparison of optical sensors

Sensor	Wavelength	QE at 900nm	QE at 1000nm	Dark current	Time response
Quantar Mepsicron II, S25	180–940 nm	1%	0%	.005 e^-/s	50 ps
Hamamatsu H6780-01	250–850 nm	0%	0%	400 e^-/s	780 ps
Hamamatsu C4880-21	200–1200 nm	50%	20%	.3 e^-/s	20 ms
Sony Super HAD CCD	300–1050 nm	8%	1%	.02 e^-/s	10 µs
Sony EXview HAD CCD	300–1100 nm	12%	5%	.02 e^-/s	10 µs

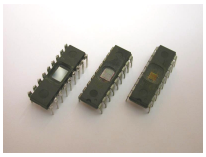
Experimental results

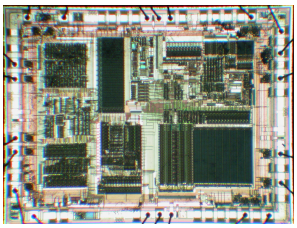
A standard microscope setup (Fig.5) with a CCD camera mounted on top and a sample in a test socket (Fig.6) was used for analysis. Hobbyist astronomical cameras with active cooling appeared to be best suited for low-cost optical emission analysis by having good NIR sensitivity and extremely low dark current. The emission acquired from a microcontroller using a 2× objective lens is presented in Fig.7. A closer look with a 10× objective revealed that the data read from EEPROM, Flash and SRAM is clearly visible (Fig.8-9). It can be observed that the source of leakage is located in row and column selectors and data bus drivers. Emissions from a similar chip built with smaller technology are lower (Fig.10).

Modern deep-submicron chips emit photons as well. However, the front-side approach no longer works due to multiple metal layers which completely block the emission. For chips built with 0.35 µm and smaller technology, a backside approach is required. In order to achieve reasonable emission, the power supply voltage must be increased by 30-50%. The result of an hour-long acquisition with 20× magnification from an SRAM in 0.13 µm FPGA chip is presented in Fig.11.

Optical emission analysis can lead to possible data extraction from semiconductor chips. That way, the security can be compromised in various chips from microcontrollers and smartcards to FPGAs and ASICs. Possible countermeasures include asynchronous designs and employing data encryption.

Fig.5. CCD setup





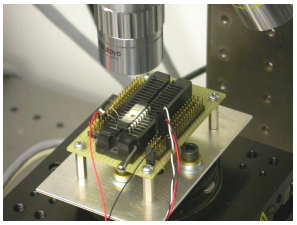


Fig.6. Opened chips, PIC16F628 die, test socket

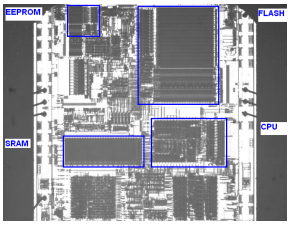


Fig.7. Emission from PIC16F628 (0.9 µm)

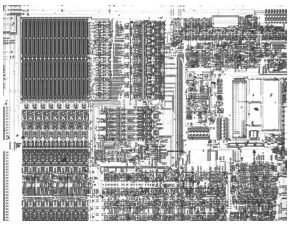


Fig.8. Emission from EEPROM

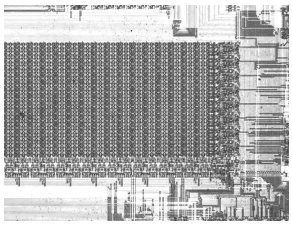


Fig.9. Emission from SRAM

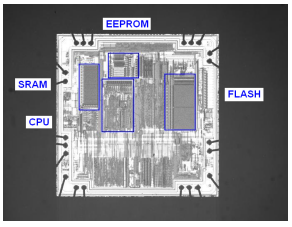


Fig.10. Emission from PIC16F628A (0.5 µm)

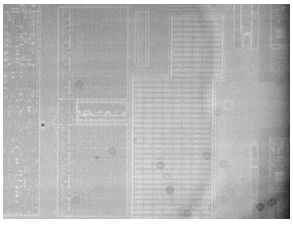


Fig.11. Backside emission from 0.13 µm SRAM

Sergei Skorobogatov, "Using Optical Emission Analysis for Estimating Contribution to Power Analysis", FDTC 2009 Workshop, IEEE-CS Press, ISBN 978-0-7695-3824-2, pp.111–119