Using Optical Emission Analysis for Estimating Contribution to Power Analysis

Sergei Skorobogatov
Computer Laboratory
University of Cambridge
Cambridge, United Kingdom
e-mail: sps32@cam.ac.uk

Abstract—**This paper shows that optical emissions from an operating chip have a good correlation with power traces and can therefore be used to estimate the contribution of different areas within the chip. I present a low-cost approach using inexpensive CCD cameras. The technique was used to recover data stored in SRAM, EEPROM and Flash of a 0.9 µm microcontroller. The result of a backside approach in analysing a 0.13 µm chip is also presented. Practical limits for this analysis in terms of sample preparation, operating conditions and chip technology are also discussed. Optical emission analysis can be used for partial reverse engineering of the chip structure by spotting the active areas. This can assist in carrying out optical fault injection attacks later, thereby saving the time otherwise required for exhaustive search.**

Keywords: optical emission analysis; semi-invasive methods; side-channel attacks

I. INTRODUCTION

Confidentiality and integrity of sensitive information stored in smart cards and secure microcontrollers is a matter of great importance to both developers and chip manufacturers. Therefore, such sensitive data as passwords, encryption keys and confidential information are often stored in encrypted form and decrypted only when necessary. That might prevent invasive attacks applied directly to the on-chip storage memory widely exploited in the late 1990s [1]. However, as encryption/decryption is usually done by the CPU, cryptographic keys and unencrypted data appear in data RAM, CPU registers and Cache memory. All these storage elements have transistors switching whenever a value of data is changed. Switching of transistors causes information leakage through various channels including power supply line, electromagnetic emission and even optical emission. The first two channels were widely exploited in side-channel attacks like differential power analysis (DPA) [2] and electro-magnetic analysis (EMA) [3]. Protection against these attacks has become a very important and challenging task. In order to reduce the traceability of data in various structures, secure chip design solutions were offered, for example, for SRAM [4]. It is important that simulation results [5] are validated in experiments with real chips. For example, for EMA analysis, cartography of the emission from the chip performing cryptographic operation can be done [6, 7]. On one hand, that reveals most leaking areas and helps positioning the sensor for better signal-to-noise ratio. On the other hand, it does not help in developing adequate countermeasures, as low spatial resolution of the EMA sensors prevents locating the transistors or gates leaking the most.

This paper compares optical emission analysis and conventional power analysis. If any correlation is found, it would help in locating transistors contributing most to the power trace and thus design more secure chips. For example, the design can be optimised in a way that the leakage is either reduced or precisely balanced and therefore not carrying information. As optical analysis requires visibility of the chip surface without the need of any physical contact, it forms a semi-invasive attack [8]. The results presented in Section 4 show that optical emission can be registered without using extremely expensive equipment as hobbyist astronomical CCD cameras can register enough photons when the exposure time is set to several minutes.

Optical emission analysis was widely used in various failure analysis techniques [9] and even for attacking AES implementation in a PIC microcontroller [10]. However, the latter involved the use of very expensive equipment (photomultiplier arrays) and sophisticated chip preparation technique (substrate thinning) together with increasing the power supply voltage to 7 V (above the absolute maximum rating!) and acquiring the data for 12 hours.

The low-cost approach presented here could pose a serious security threat because optical emission analysis allows direct observation of changing data bits unachievable with other side-channel attack methods like DPA and EMA, which give only Hamming weights of information and not the position of the bits. This is because power analysis is applied to a whole chip, electromagnetic emission analysis to a large area on the chip, while optical analysis can be scaled down to a single transistor. If optical emission analysis becomes affordable to low-budget attackers, it could pose a big problem to the hardware community.

This paper is organised as follows. Section 2 describes the underlying physics of the optical emission as well as the existing methods of analysis. Section 3 introduces the experimental setup, while Section 4 shows the initial results. Section 5 discusses limits and possible improvements together with further results.

II. BACKGROUND

The existence of photon emissions associated with the switching of transistors was well known to the semiconductor industry community for more than two

decades. Analysis of optical emissions from switching transistors inside semiconductor chips has been used in failure analysis for many years to detect any abnormalities in chips functionality. Most digital circuits built today are based on CMOS technology which uses complementary transistors as the basic element. When a CMOS gate changes its state several effects associated with photon emission take place [11]. From all these effects, hot carrier luminescence contributes most to the optical emission. The spectrum of hot-carrier emission ranges from 500 nm to above 1200 nm with maximum emission in the region between 900 nm and 1100 nm [12]. The main problem associated with the optical emission analysis of operating semiconductor chips is that not every switching of a transistor results in emission of a photon. That means photon emissions must be integrated for some time. The number of emitted photons can be calculated according to the equation on page 173 in [13]. Depending on the chip technology it varies from 10^{-2} to 10^{-4} photons per switching.

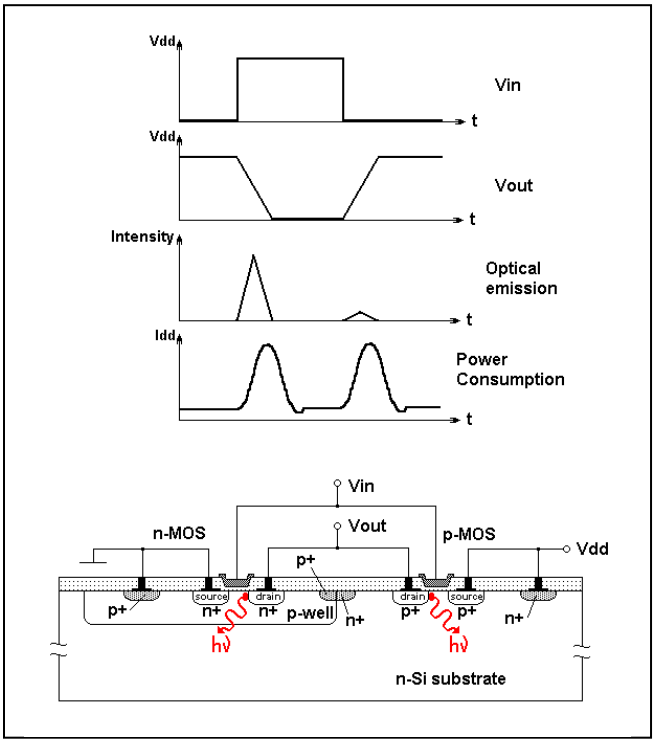

Figure 1. Photon emission from a switching CMOS inverter.

A CMOS gate consists from a pair of n-MOS and p-MOS transistors. Whenever a transistor is switched, power consumption increases due to current flows into parasitic capacitances and leakage currents. According to [14] the optical emission from an n-channel transistor takes place when the output goes from high to low state, and from a p-channel when it goes from low to high, that is when the transistor opens. The emission from an n-channel transistor is much higher due to better mobility of electrons compared to holes. Also, the photons are emitted from a region close to the drain where the electric field is higher. The example in Fig. 1 given for n-type substrate, however, the same outcome applies for p-type substrates which appear to be more common in modern chips.

Another problem associated with optical analysis is the dark current of the sensor, which adds noise in the measurement and increases the time necessary to achieve a reasonable signal-to-noise ratio. When emitted photons are collected, there are also some losses from mechanical constraints, as they are emitted in all directions, plus there are losses inside the sample and collecting optics. As a result, only about 5% of the emitted photons reach the sensor. When it comes to the sensor itself, photons are only registered with a certain probability called quantum efficiency (QE). Some ways of increasing the percentage of registered photons can be used. One is thinning the sample for backside approach to reduce the losses on absorption, another is using near-infrared (NIR) optics and sensors more sensitive in that region.

Primarily, two optical emission analysis techniques which provide a 2D mapping of the emission from a chip surface are used in failure analysis: picosecond imaging circuit analysis (PICA) and photon emission microscopy (PEM). PICA uses an array of photomultipliers, such as Quantar Technology Mepsicron II [15], which combines time-resolved capabilities of a photomultiplier tube (PMT) with position sensitivity of a 2D detector offering spatial resolution of about 60 µm. PEM uses special CCD cameras sensitive in the NIR region, for example, Hamamatsu H4880 with active water cooling to achieve substantial noise reduction [16]. In both techniques, the camera is usually attached to a special NIR microscope for observing the emission from the desired area on a chip surface. However, PEM cannot achieve the picoseconds precision available from PICA, but it relies on photon collection over a long period of time. Both techniques are very expensive and available to well funded laboratories only. Characteristics of the above mentioned sensors are summarised in Table 1. For modern deep-submicron chips, special preparation techniques are required, namely thinning of the substrate and anti-reflection coatings to reduce the loss of photons through absorption and reflection.

TABLE I. COMPARISON OF PHOTOSENSITIVE ARRAYS

Type of camera	Parameters				
	Wave-length nm	*QE at 900 nm*	*QE at 1000 nm*	*Dark current e^-/s*	*Time re-sponse*
Quantar Mepsicron II S25	180–940	1%	0%	0.005	50 ps
Hamamatsu C4880-21	200–1200	50%	20%	0.3	20 ms
Hamamatsu C4880-50	200–1100	30%	10%	0.01	20 ms

For characterisation of emission from individual transistors in failure analysis, PMT or avalanche photodiodes (APD) are commonly used. They have very good time-resolving capabilities, but cannot provide any location

information. However, data acquisition time for single-point detectors is measured in minutes versus hours for 2D detectors like Mepsicron [17].

III. Experimental Method

In the first set of experiments I used a common microcontroller, the Microchip PIC16F628 [18], with on-chip SRAM, EEPROM data memory and Flash program memory. The microcontroller was programmed with various simple test subroutines which emulated operations commonly occurring in secure microcontrollers and smart cards. These included SRAM reading and writing, XORing data, EEPROM and Flash reading. The microcontroller was running from a 20 MHz external clock, corresponding to 5 MIPS or 200 ns instruction cycle (except branches). In order to increase the emission, the power supply was set to 6 V, which is outside normal operating conditions, but still below the absolute maximum rating.

I analysed the suitability of three different types of sensors – PMT, APD and CCD. For PMT a very simple setup was used with a decapsulated microcontroller placed inside black antistatic foam with its surface facing the sensor aperture (Fig. 2). As the PMT has a large aperture, there was no need to precisely position the chip. The whole setup then was placed inside an opaque bag to prevent the influence of ambient light.

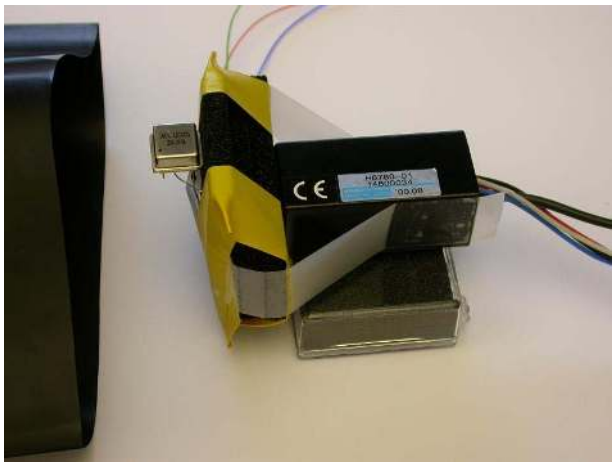

Figure 2. The test setup with H6780-01 PMT sensor.

For the APD and CCD camera experiments a microscope setup with the chip in a test socket was used. The samples were opened using standard techniques described in [1, 9]. The equipment used consisted of a test board mounted on a motorised XYZ-stage and the sensor mounted on an optical microscope with long-working distance objectives (Fig. 3). For all experiments I used low-resolution 2×, 10× and 20× objectives, which are relatively inexpensive compared with high-resolution objectives used in failure analysis for laser imaging. To prevent any photons from entering the setup from the outside, the gap between the chip and the optics was shielded with an opaque material. In addition, all experiments were performed in a dark room.

Most PMT and APD modules are relatively expensive, and I managed to evaluate only two types of PMT sensors: Hamamatsu H10330-25 [19] and H6780-01 [20], and one APD sensor Sensl PCDMini-0020 [21]. The selection of the CCD camera was a more challenging task. As most sensor parameters are available from datasheets, there was no need in testing many cameras. I was looking for inexpensive CCD cameras with parameters close to the ones used for failure analysis. That means with reasonable sensitivity in NIR region and as little dark current noise as possible. The noise blinds the sensor, thus preventing long-time integration of the image. This is especially important for optical emission analysis as we deal with just a few photons per second. The higher the noise, the longer is the integration time required to achieve a reasonable signal-to-noise ratio. However, very long integration is not desirable due to the fact that the internal dark current might saturate the sensor completely. As CCD cameras are not single-photon-registration devices, only differential analysis of captured frames can be performed to find any difference in processed data.

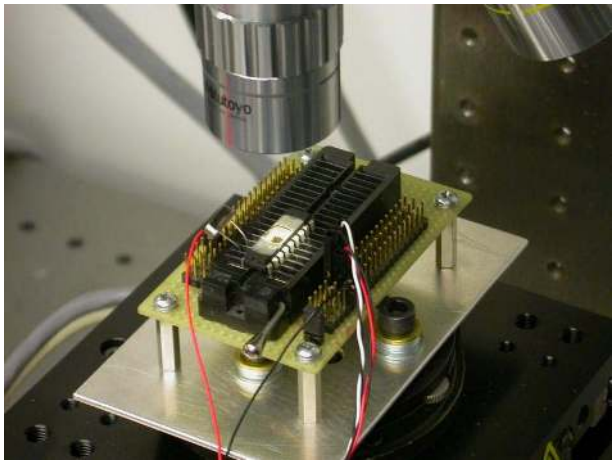

Figure 3. The test setup with CCD camera.

Main applications for low-noise cameras sensitive in the NIR region are surveillance and astronomical observation. Astronomical cameras seemed particularly suitable as they normally have active cooling down to 10–20 °C below ambient temperature, to reduce the dark current noise. These cameras normally have above 1 megapixel resolution and are relatively inexpensive, with prices starting from as little as $1000, while bare sensors start from $250. For most applications 640×480 pixels are enough and such surveillance cameras sell for under $100. However, as they do not have active cooling, slightly longer acquisition will be necessary. For my experiments I used the monochrome hobbyist astronomical Starlight Xpress SXV-H9 camera with Sony EXview HAD sensor [22], which has extended NIR sensitivity and reduced dark current noise. Table 2 summarises various sensors that I tested during my experiments, together with two other CCD sensors for comparison: the Sony Super HAD CCD often found in CCTV devices and a normal low-cost monochrome CCD

camera. As can be seen, CCD cameras have significantly lower dark current compared to PMT and APD, however, they cannot register fast processes.

TABLE II. COMPARISON OF OPTICAL SENSORS

Type of camera	Parameters				
	Wave-length nm	*QE at 900 nm*	*QE at 1000 nm*	*Dark current e^-/s*	*Time re-sponse*
Hamamatsu H10330-25	850–1250	2%	2%	2000	900 ps
Hamamatsu H6780-01	250–850	<1%	0%	400	780 ps
Sensl PCDMini-0020	400–1100	2%	<1%	50	200 ps
Sony Super HAD CCD	300–1050	8%	1%	0.02	10 µs
Sony EXview HAD CCD	300–1100	12%	5%	0.02	10 µs
Average monochrome CCD	400–1000	<5%	<1%	>1	>10 µs

IV. RESULTS

For the first set of experiments I used the Hamamatsu H10330-25 and H6780-01 PMT sensors. The first one has good sensitivity in the NIR spectrum, but low quantum efficiency and high dark current, while the other has lower quantum efficiency in NIR region, but a lower dark current. For both sensors acquisition over some period of time was necessary, ranging from tens of minutes to over an hour. I used an Agilent MSO8104A digital storage oscilloscope for averaging the signal. It was placed in color-graded mode with infinite persistence with enabled histogram. However, this mode does not allow downloading of raw time-series data and the analysis is only possible with the oscilloscope software and screen shot as an output. As the results of the acquisition were similar for both sensors, the less expensive about $1000 Hamamatsu H6780-01 sensor can be used with slightly increased integration time. Fig. 4a shows the result of a 60-minute long acquisition from the microcontroller with trigger signal at the top for reference. Bottom shows count of trigger events for photons in the oscilloscope's histogram mode. The higher the peaks, the more photons were registered at that time. For comparison, results from simple power analysis for the same setup measured on a 10 Ω resistor are presented in Fig. 4b. The clock signal supplied to the PIC was also recorded for reference. The long acquisition time was required not only because of the low quantum efficiency of the PMT, but also due to slow trigger rate of the oscilloscope in color-graded infinite persistence mode.

Good correlation can be observed between the locations of peaks in these two measurements. It can be seen that the maximum number of photons are emitted during transition of the clock signal and they are proportional to the power consumption, but the much higher bandwidth used for the optical signal leads to narrower peaks. However, the advantage of the optical analysis over the power analysis is that it can be applied to a small area on a chip surface, for example, by using hole in a foil, a tape aperture or a microscope. The higher bandwidth of the PMT sensor could allow precise measurements of data-dependent events, thus potentially compromising the security of chips with DPA protection.

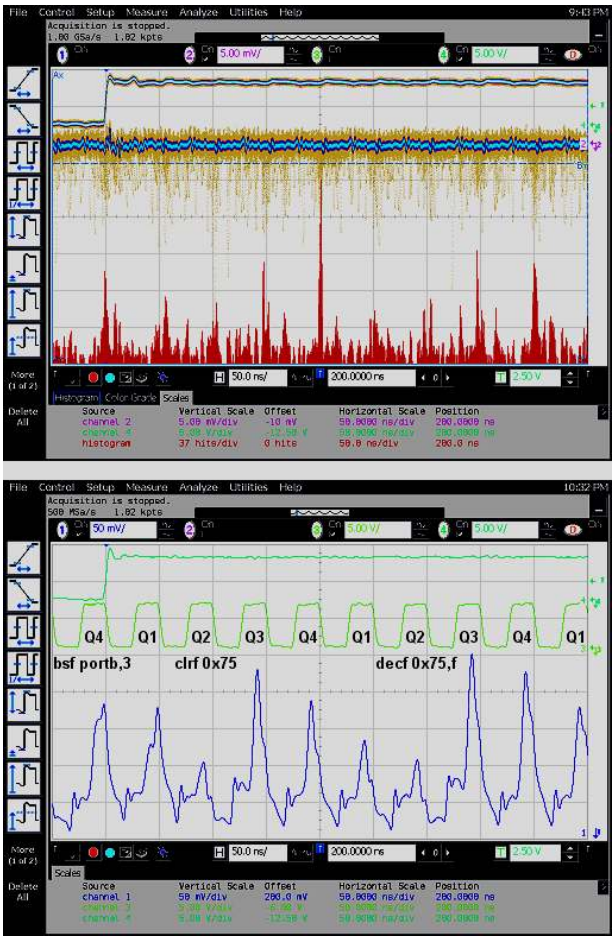

Figure 4. (a) data acquired with H6780 PMT sensor, (b) raw power trace.

PMT sensors have certain downsides. They have high dark current noise, as well as low sensitivity in the NIR spectrum, both resulting in long acquisition times. Also the setup turned out to be sensitive to electromagnetic interference, for example, mobile phone had to be kept away.

It was hard to achieve any useful results with the APD sensor mounted on the microscope camera port. This may be due to its small aperture size, high dark current and low sensitivity in the NIR region. Even two hours of acquisition were not enough to achieve any reasonable signal-to-noise ratio. As such sensors are more expensive than PMT, I did not try to find any other suitable APD sensors.

The monochrome hobbyist astronomical CCD camera was used in the following experiments to observe optical emission from the decapsulated PIC16F628 chip. The exposure time and resolution were set through the camera

software. My first experiment was aimed at estimating the time necessary to acquire any distinguishable optical emission from the chip. The microcontroller was programmed to read its internal EEPROM and SRAM in a continuous loop (**incf eeadr, f; bsf eecon1, rd; movf eedata, w; decf 0x75, f**). It turned out that a 30-minute exposure time was more than enough to observe the emission from the chip die, even at a low magnification (Fig. 5).

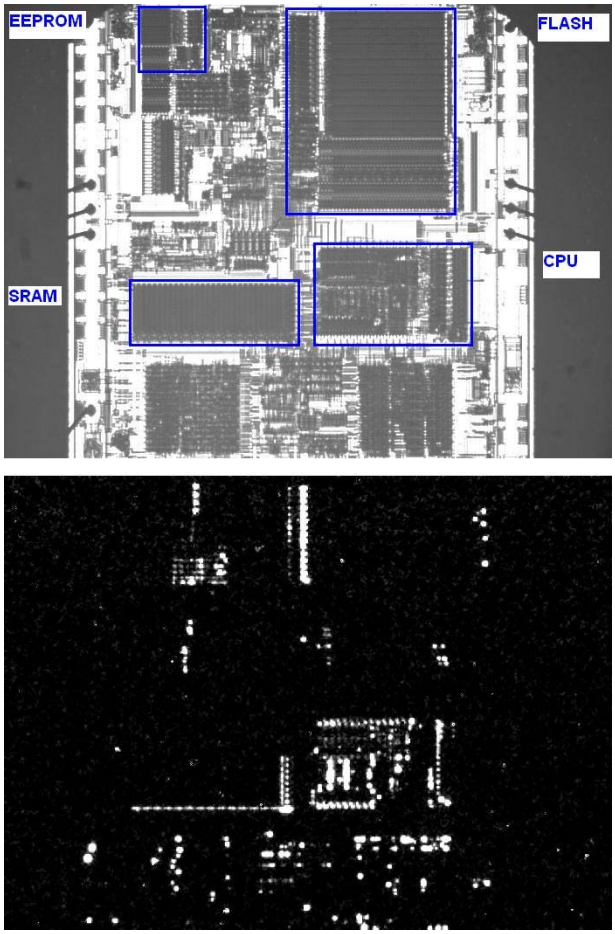

Figure 5. Image of the die with 2X lens: (a) optical, (b) photon emission.

The result of the above observation can be used for reference purposes. As the locations of SRAM, EEPROM and Flash can be easily found under an optical microscope, areas of maximum emission from each part can be noted for further analysis with a higher magnification. The data read from EEPROM can be clearly observed with just a 10× objective lens. An exposure time of only five minutes was necessary to achieve good signal-to-noise ratio; the data (56h) can be read manually without the need of any post processing (Fig. 6).

The same technique can be applied to SRAM. Optical emission from the SRAM area during the read operation of a memory location holding A6h value (**movf 0x75, w**) is shown in Fig. 7. However, a memory write operation of the same value (**movwf 0x75**) will result in almost the same image. This is because memory access in the PIC16F628 microcontroller is done as a read-modify-write operation. It can be noticed that the area responsible for the memory write operation became brighter for the bits set in the A6h value. A closer look at the image reveals that there are two write transistors – one for writing "0" and another for "1". This reflects the fact that an SRAM cell has two control lines – one for setting it and another for resetting. This results in the value being almost indistinguishable in the power trace but particularly visible in the optical emission picture. Comparison of the emission from the "0" and "1" areas allows to read out data even where a carefully balanced circuit design would prevent power analysis.

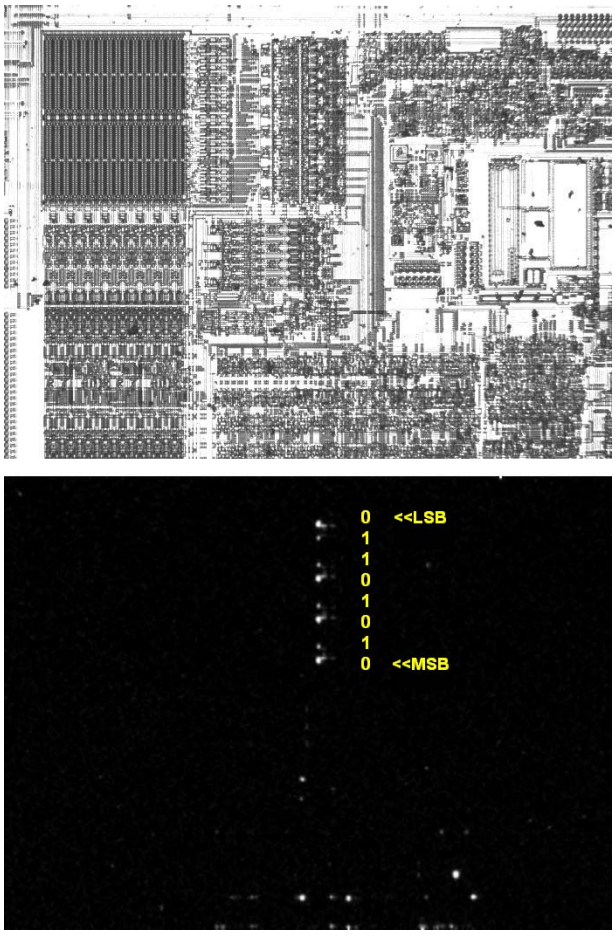

Figure 6. Image of the EEPROM with 10× lens: (a) optical, (b) emission.

XOR operations are used in many cryptographic primitives. Fig. 8 shows the result of XOR operation between the memory location holding A6h value and the register with C3h value (**movlw 0xA6; movwf 0x74; movlw 0xC3; xorwf 0x74**). Another observation that can be made concerns the actual source of leakage. As can be seen, it is mainly address decoders and bus drivers that contribute most to the emission with negligible contribution from the actual memory cells. One way of measuring contribution from a particular area involves integrating the pixel values on the

image in that area, as they are proportional to the number of emitted photons.

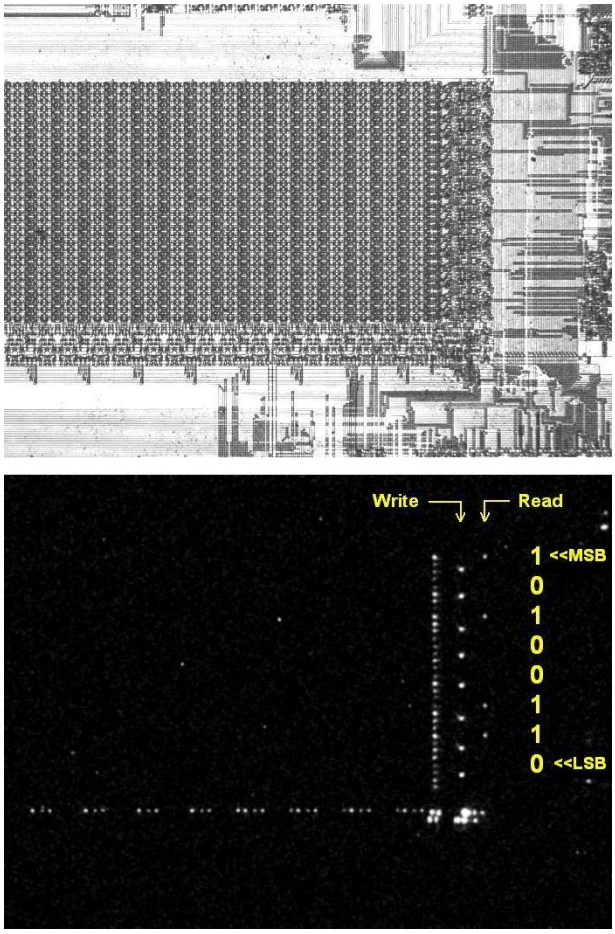

Figure 7. Image of the SRAM with 10× lens: (a) optical, (b) emission.

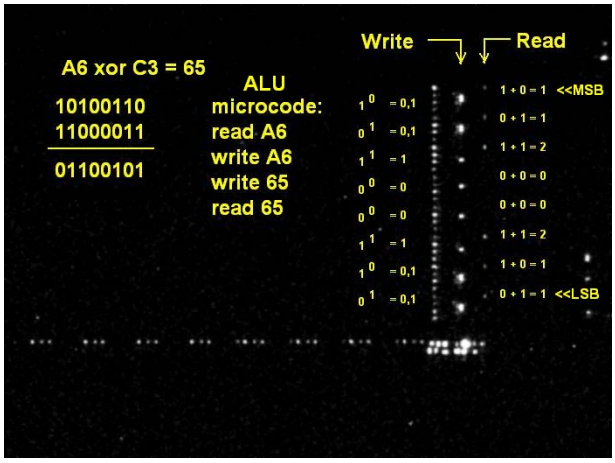

Figure 8. Emission image for XOR operation in SRAM.

V. Implications and Further Improvements

The above results were achieved on a relatively old microcontroller PIC16F628 built with 0.9 µm technology with two metal layers. I therefore compared the results with a newer version of this microcontroller, the PIC16F628A built with 0.5 µm technology [23]. Its higher density of metal wires together with interlayer polishing slightly reduces the number of photons which reach the sensor, resulting in the emission image being approximately three times less intensive (Fig. 9) than for its predecessor in Fig. 5.

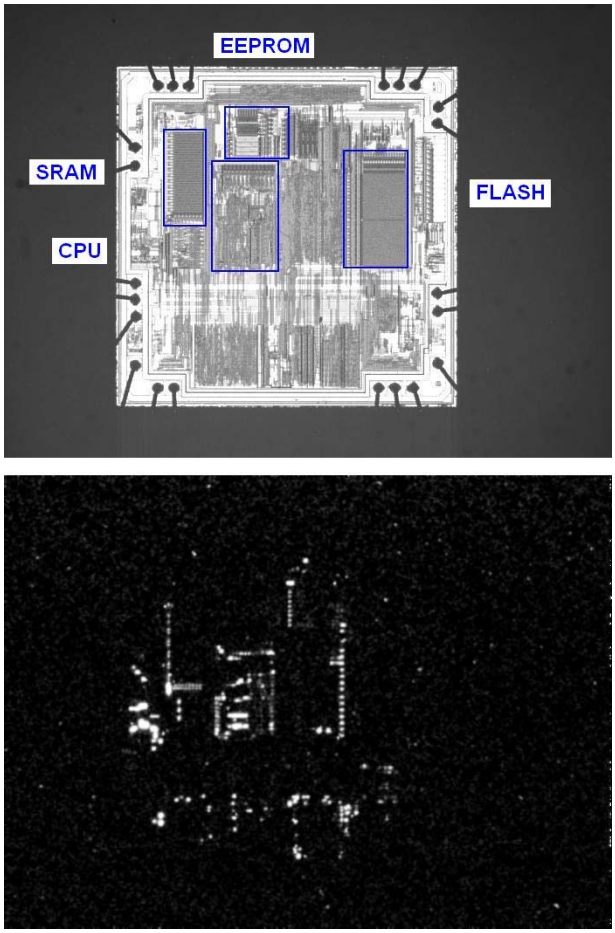

Figure 9. Image of the die with 2× lens: (a) optical, (b) photon emission.

One possible improvement of the attack is to approach memory cells from the rear side of the chip. However, in this case the optical sensor should be sensitive to infrared light with wavelength longer than 1000 nm. A set of experiments was carried out for emission analysis of the PIC16F628 chip from both sides. The backside chip preparation is much simpler as no chemicals are required for opening up the chip. The plastic can be milled away with low-cost engraving tools available from many DIY shops. Then the copper heatsink can be removed with a screwdriver and the die surface cleaned with solvent. However, in order to achieve the same signal-to-noise ratio, approximately ten times longer exposure time was required. The result of a 30-minute

exposure of the EEPROM area for both approaches with 10× objective lens is presented in Fig. 10 with the backside image flipped for easier comparison. For backside imaging, the intensity could be improved with substrate thinning and anti-reflection coating. However, these techniques are expensive. All my backside experiments were carried out on untreated rear surfaces of the dies, thus are low-cost and simple.

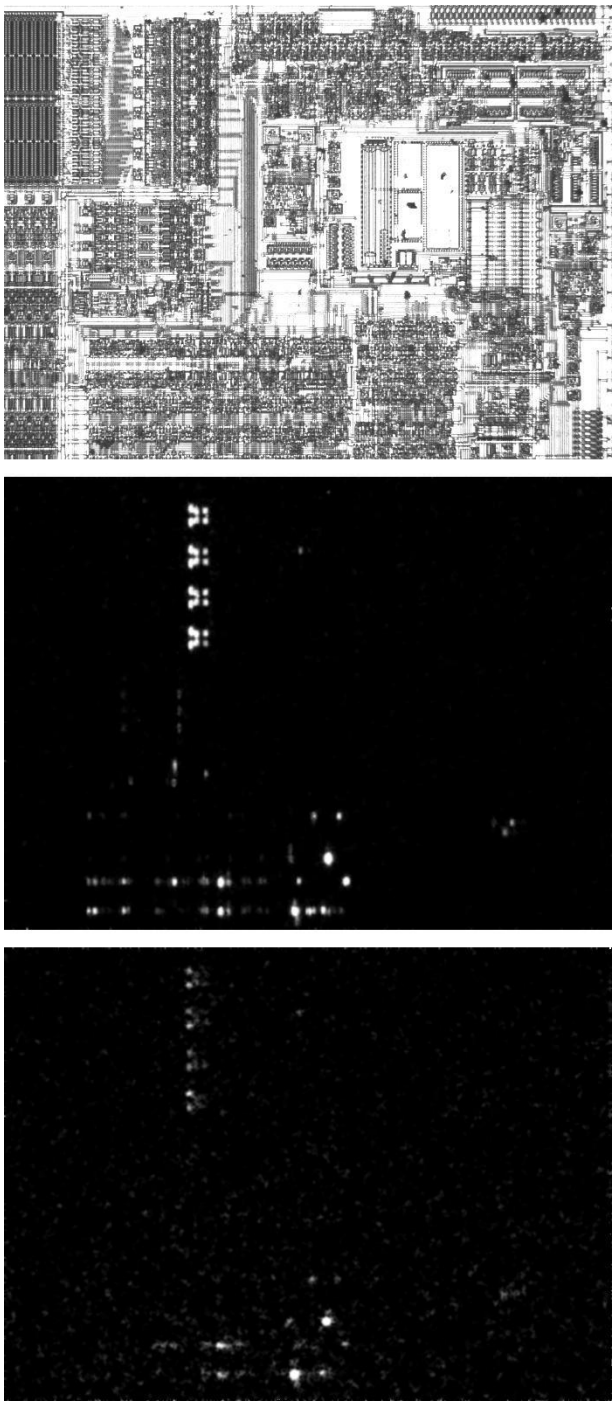

Figure 10. (a) optical image, (b) front, and (c) rear emission images.

Previous publications on the analysis of emissions from smaller transistors suggest that there is no reduction in the number of emitted photons with moving to deep-submicron chips – even a slight increase due to the higher electric field [24]. A set of experiments was carried out on a modern chip with 0.13 µm technology and 1.5 V nominal core supply voltage running at 20 MHz. The chip has SRAM, Flash and some security features including a cryptoprocessor (full details cannot be disclosed because the evaluation work was done under a non-disclosure agreement). Multiple metal layers inside the chip together with a special surface coating excluded a front-side approach, hence, the experiments were carried out from the rear side. The supply voltage was set to 2.0 V in order to increase the emissions. The area around the internal SRAM was observed with a 20× NIR objective and the optical emission was acquired for 60 minutes (Fig. 11). The image proves that optical emission can be carried out on modern deep-submicron devices with a low-cost CCD camera.

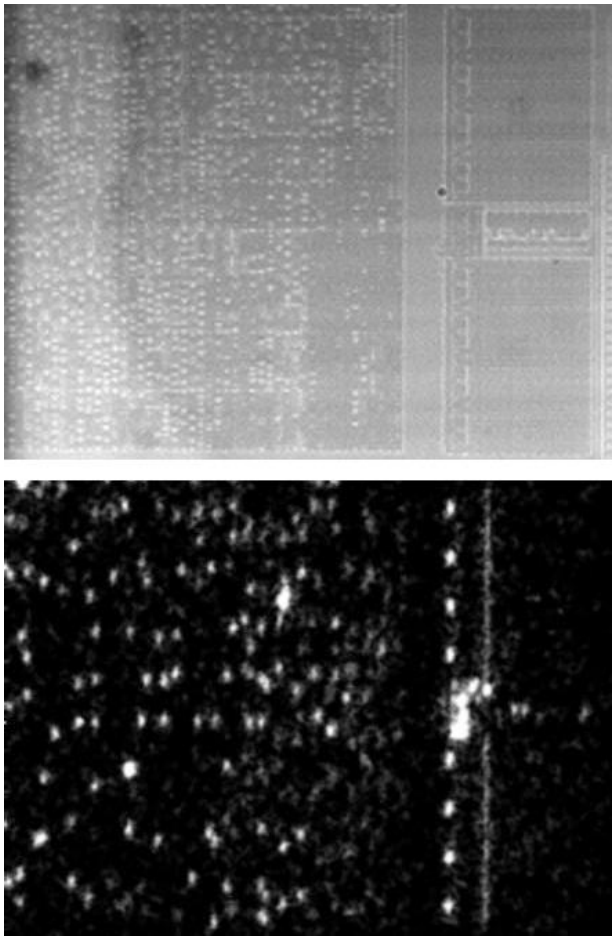

Figure 11. Backside image of the SRAM: (a) optical, (b) emission.

Optical emission depends on the power supply voltage. The higher the voltage, the higher is the emission. A set of experiments was carried out on a PIC16F628 chip showing that the dependency is exponential rather than linear

(Table 3). The photometry values are relative and represent the number of electrons in the CCD well. For comparison, optical emission was measured from the 0.13 µm chip (Table 4). For most chips the optical emission roughly doubles for every 10% increase above the nominal power supply voltage.

TABLE III. EMISSION AT DIFFERENT POWER SUPPLY 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 IV. EMISSION AT DIFFERENT POWER SUPPLY FOR ASIC

	Power Supply Voltage					
	1.5 V	***1.6 V***	***1.8 V***	***2.0 V***	***2.2 V***	***2.5 V***
Photometry results	889	1194	1953	5270	9536	23270

When a sequence of data is read from the memory, it might be more practical to perform differential analysis, because these values will be summarised in the emission image. One way is to perform separate exposures for **n** and **n+1** machine instructions, then subtract one image from another in order to extract the data present during that additional cycle. If that approach is problematic, other techniques can be used to separate the emission from each set of data. One includes termination after a specific number of clock cycles and could be used, for example, to extract the key during key scheduling operation in cryptography. Another technique involves controlling the power supply voltage, as reducing it by 30% blocks 90% of the emission. However, as each exposure takes at least one minute, it is impractical to extract the contents of the whole memory with that approach, but could serve well for passwords and keys.

VI. CONCLUSION

Optical emission analysis allows direct observation of the data processed inside semiconductor chips. For example, data stored in SRAM, EEPROM and Flash memories can be extracted. The work presented in this paper shows that optical emission from an operating chip correlates well with the power analysis measurements. This can help in improving the design of secure blocks inside semiconductor chips. My experiments demonstrated that no expensive equipment or sophisticated sample preparation is required for analysing the optical emission. Instead, low-cost astronomical CCD cameras suffice. The only disadvantage of this approach is the time necessary for acquiring the signal during which the chip must repeat the same operation many times. For modern deep-submicron chips the exposure time could be up to an hour long.

Protection against power analysis and EMA attacks has become a very important and challenging task for industry. Low-cost evaluation methods like those presented in this paper must be considered in security evaluations. Using optical emission-analysis techniques, partial reverse engineering and finding physical locations of data bits can be easier than with other reverse engineering techniques, such as delayering the chip followed by digital imaging and design reconstruction. However, optical emission-analysis techniques have some limitations, especially for modern deep-submicron technologies where multiple metal layers and small transistor sizes prevent easy and precise analysis. Further improvements to these methods might involve approaching the die from its rear side, but this requires longer exposure time due to higher losses in optics and lower quantum efficiency of sensors. Although I used an industrial microscope, some low-cost alternatives exist. For example, an objective lens attached directly to the camera or even a hobbyist microscope might suffice as 10× and 20× magnifications proved to be enough for most observations. My experiments also demonstrated that PMTs are useful for picking up high-bandwidth signals from parts of a circuit. Special acquisition boards might be required though, as standard digital storage oscilloscopes cannot acquire high-frequency signals for a long period of time. Nevertheless, good correlation with power analysis suggests that PMTs can be used as an addition to existing techniques.

Optical emission analysis can be a very good extension to other semi-invasive methods such as optical probing and laser scanning [8]. For example, the optical beam induced current (OBIC) method can locate the active areas inside a chip while the light induced voltage alteration (LIVA) can reveal the state of on-chip transistors [25]. However, optical emission analysis gives the result faster and does not require stopping the clock frequency or placing the device in idle state, which sometimes is not feasible. Another application for this analysis could be in partial reverse engineering of the chip structure by spotting the active areas for various on-chip operations. For example, it can be used for locating the active transistors before carrying out optical fault injection attacks [26] or position-locked power analysis attacks [27]. That way there will be no need to carry out the exhaustive search of all possible places for targeting the laser, thus saving the time.

Like with the introduction of probing attacks in the mid-1990s, power analysis attacks in the late 1990s and optical injection attacks in the early 2000s, optical emission attacks will very likely result in the need to introduce new countermeasures during the design of semiconductor chips.

ACKNOWLEDGMENT

I would like to thank my colleague Dr Markus Kuhn for providing me with a Hamamatsu photomultiplier and for general technical help.

REFERENCES

[1] O. Kömmerling, M.G. Kuhn, "Design principles for tamper-resistant smartcard processors", USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10–11, 1999

[2] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", CRYPTO'99, LNCS, Vol. 1666, Springer-Verlag, 1999, pp. 388–397

[3] J.-J. Quisquater, D. Samyde, “Electromagnetic analysis (EMA): measures and counter-measures for smart cards”, Smart Card Programming and Security (E-smart 2001), Cannes, France, LNCS Vol. 2140, Springer-Verlag, 2001, pp. 200–210

[4] E. Konur, Y. Ozelci, E. Arikan, U. Eksi, “Power analysis resistant SRAM”, World Automation Congress (WAC) 2006, July 24–26, Budapest, Hungary

[5] H. Li, A. A.T. Markettos and S.W. Moore, “Security evaluation against electromagnetic analysis at design time”, Workshop on Cryptographic Hardware and Embedded Systems (CHES), September 2005

[6] L. Sauvage, S. Guilley, Y. Mathieu, “Electromagnetic radiations of FPGAs: high spatial resolution cartography and attack of a cryptographic module”, ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol. 2, Issue 1, March 2009

[7] D. Real, F. Valette, M. Drissi, “Enhancing correlation electro-magnetic attack using planar near-field cartography”, Design Automation and Test in Europe (DATE'09), Nice, France, April 20–24, 2009

[8] S. Skorobogatov, “Semi-invasive attacks – a new approach to hardware security analysis”, Technical Report UCAM-CL-TR-630, University of Cambridge, Computer Laboratory, April 2005

[9] L.C. Wagner, “Failure analysis of integrated circuits: tools and techniques”, Kluwer Academic Publishers, 1999

[10] J. Ferrigno, M. Hlaváč, “When AES blinks: introducing optical side channel”, IET Information Security, Vol. 2, No. 3, 2008, pp. 94–98

[11] G. Deboy, J. Kölzer, “Fundamentals of light emission from silicon devices”, Semiconductor Science and Technology, Vol. 9, 1993, pp. 1017–1032

[12] S. Villa, A.L. Lacaita, A. Pacelli, “Photon emission from hot electrons in silicon”, Physical Review B, Vol. 52, 1995, pp. 10993–10999

[13] F. Stellari, F. Zappa, M. Ghioni, S. Cova, “Non-invasive optical characterisation technique for fast switching CMOS circuits”, Solid-State Device Research Conference, Leuvem, Belgium, 1999, pp. 172–175

[14] F. Stellari, F. Zappa, S. Cova, L. Vendrame, “Tools for non-invasive optical characterization of CMOS circuits”, IEDM Technical Digest – International Electronic Devices Meeting, Washington, USA, 1999, pp. 487–490

[15] Quantar Technology Mepsicron II Series Single-Photon Imaging Detector System, http://www.quantar.com/pages/QTI/2601TS.pdf

[16] Alacron, Camera Support, Hamamatsu, http://www.alacron.com/camera/hamamatsu.htm

[17] W. Ng, G. Gao, A. Abraham, T. Lundquist, “Hot carrier luminescence for backside 0.15 µm CMOS device analysis”, Integrated Reliability Workshop Final Report, 2002, pp. 116–119

[18] Microchip PIC16F62X Flash-Based 8-Bit CMOS Microcontroller, http://ww1.microchip.com/downloads/en/devicedoc/40300c.pdf

[19] Hamamatsu Thermoelectric Cooled NIR-PMT Module, http://sales.hamamatsu.com/assets/pdf/parts_H/H10330.pdf

[20] Hamamatsu Metal Package PMT Photosensor Modules, http://sales.hamamatsu.com/assets/pdf/parts_H/H6780-01.pdf

[21] Sensl PCDMini Miniature Photon Counting Device, http://www.sensl.com/pdfs/Datasheets/PCDMini_Datasheet.pdf

[22] Sony Product Information List, Image Sensor, http://www.sony.net/Products/SC-HP/pro/image_senser/index.html

[23] Microchip PIC16F627A/628A/648A Flash-Based, 8-Bit CMOS Micro-controllers with nanoWatt Technology, http://ww1.microchip.com/downloads/en/devicedoc/40044f.pdf

[24] A. Tosi, F. Stellari, F. Zappa, S. Cova, “Hot-carrier luminescence: comparison of different CMOS technologies”, European Solid-State Device Research Conference, 2003, pp. 351–354

[25] C. Ajluni, “Two new imaging techniques promise to improve IC defect identification”, Electronic Design, Vol. 43(14), July 1995, pp. 37–38

[26] S. Skorobogatov, R. Anderson, “Optical fault induction attacks”, Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), LNCS 2523, pp. 2–12

[27] S. Skorobogatov, “Optically enhanced position-locked power analysis”, Cryptographic Hardware and Embedded Systems Workshop (CHES-2006), LNCS 4249, Springer-Verlag, pp.61–75