When Failure Analysis Meets Side-Channel Attacks

Jérôme Di Battista, Jc Courrège, Bruno Rouzeyre, Lionel Torres, Philippe Perdu

When Failure Analysis Meets Side-Channel Attacks

Jerome Di-Battista[1,2], Jean-Christophe Courrege[1], Bruno Rouzeyre[2], Lionel Torres[2], and Philippe Perdu[3]

[1] Thales Information Systems Security, 18 Avenue Edouard Belin, 31400 Toulouse, France
jerome.dibattista@cnes.fr
[2] Université de Montpellier, Laboratoire du LIRMM, 161 rue Ada, 34095 Montpellier Cedex 5, France
[3] Centre National d'Etudes Spatiales CNES, 18 Avenue Edouard Belin, 31400 Toulouse, France

Abstract. The purpose of failure analysis is to locate the source of a defect in order to characterize it, using different techniques (laser stimulation, light emission, electromagnetic emission...). Moreover, the aim of vulnerability analysis, and particularly side-channel analysis, is to observe and collect various leakages information of an integrated circuit (power consumption, electromagnetic emission ...) in order to extract sensitive data. Although these two activities appear to be distincted, they have in common the observation and extraction of information about a circuit behavior. The purpose of this paper is to explain how and why these activities should be combined. Firstly it is shown that the leakage due to the light emitted during normal operation of a CMOS circuit can be used to set up an attack based on the DPA/DEMA technique. Then a second method based on laser stimulation is presented, improving the "traditional" attacks by injecting a photocurrent, which results in a punctual increase of the power consumption of a circuit. These techniques are demonstrated on an FPGA device.

Keywords: Side-channel, Failure analysis, Light emission, Laser stimulation, FPGA.

1 Introduction

During the last 20 years, failure analysis has become a serious concern for the electronics industry. Its purpose is to locate the source of a defect in order to characterize it, the defect being a problem linked to the environemental conditions, an intrinsic problem in the circuit, or both. More generally, failure analysis should ensure that the detected problem does not occur again [1]. The strongest constraints are the size reduction for CMOS technology components and the increasing complexity of integrated chips (several millions of gates). Currently the most used analysis tools are based on laser stimulation and light emission techniques. Concurrently, during the last 10 years, non-invasive and semi-invasive

S. Mangard and F.-X. Standaert (Eds.): CHES 2010, LNCS 6225, pp. 188–202, 2010.

techniques have received a lot of attention from the hardware security community. Among them, so-called side-channel attacks are the most popular. Different leakage sources [2][3] such as power consumption, electromagnetic field, or time response of the circuit, are correlated to the processed data. Thus, by inspecting this information, and with the help of appropriate software tools, it is possible to retrieve the secret data used in the embedded cryptography circuits, typically the cipher key. From an attacker point of view, side-channel attacks present many advantages, as most of them require only low-cost instrumentations, and they are non-destructive.

These two activites apparently different can be combined. Indeed, the failure analysis techniques can be used to extract another kind of side-channel signal or to improve existing side-channel attacks. Inversely, the vulnerability analysis can be used to extract complementary information about the circuit behavior. In this paper two examples of application, light emission and laser stimulation, are presented.

The light emission phenomenon has been mainly studied for failure analysis. Many techniques have been developed to extract and process the light emitted by the electronic components in order to localize different kinds of defects [4] (junction avalanche, oxide breakdown...). In this paper we mainly focus on the light emitted by NMOS transistors during commutation. Indeed, in [5], the author demonstrates the possibililty to set up an attack based on light emission, by implementing part of an AES algorithm on a PIC16F84A microcontroller previously opened from the backside. The purpose of this attack was to recover the secret key stored in the microcontroller RAM. Using this work as a starting point, two approaches have been developed; in [6] the author demonstrates the possibility of using a low-cost system to perform the same kind of experiments on a PIC16F628 and provides some interesting results for a FPGA circuit. In parrallel, we had chosen to study the Time Resolved Emission (TRE) technique which allows us to count the number of photons emitted by a transistor or by a group of transistors as a function of time, implemented on a more expensive failure analysis equipment [7]. Our purpose is to show that the extracted TRE signal can be used to gather sensitive data, such as a side-channel signal, exploitable by a statistical post-processing method (e.g. DPA or CPA).

In the same way as light emission, the techniques based on laser stimulation have been mainly developed in failure analysis [8][9]. On the one hand, the laser stimulation at a 1064 nm wavelength allows to induce a local photocurrent [10], either to detect a latch-up mechanism and inter-level shorts or to locate open circuits and direct semiconductor damage (LIVA, OBIC). On the other hand, the laser stimulation at a 1340 nm wavelength can also induce a thermal variation to detect a resistance variation by measuring the power consumption across a circuit (TIVA, OBIRCH). In [11], the author demonstrates the possibility to increase the consumption of a SRAM cell transistors in a microcontroller by applying a photocurrent (639 nm laser). Starting from these experiments, we studied the possibility to use this method to improve a side-channel attack, by reducing the number of power consumption curves necessary to perform the attack.

We experimented both methods on an FPGA Actel Proasic3 A3PE600 in flash technology (0.13μm, 7 metal layers, 600k system gates, single chip). This type of circuit offers a very high flexibility, as it is completely customizable, reconfigurable and non-volatile. These particularities make the FPGA a good test sample to be analysed on different testing or failure analysis equipments. However FPGAs make the analysis more difficult than ASICs, as the regular structure of FPGA logic elements does not permit to localize sensitive components such as SRAMs or EEPROMs (by using for instance an optical microscope). Furthermore, the attacked microchip is in 0.13μm technology, which may complicate the measurements due to lower power supply and light emission. To overcome this problem, the acquisitions have to be performed from the backside of the chip, even though this requires a more sophisticated sample preparation [12].

2 Light Emission as a Side-Channel Signal

2.1 Background

Currently, most digital circuits are based on CMOS technology. One of the particularities of CMOS transistors is that photons are emitted during their commutation. Indeed when a current flows between the source and the drain, the electrons gain energy and accelerate due to the electrical field. The radiative "de-excitation" of the charge carriers in the pinch-off zone generates photons which are visible in the near-infrared spectral range [13]. This emission is predominant for a transition from 0 to 1. For a 1 to 0 transition the emission is usually too low to be acquired. This phenomenon produces an asymmetric light emission profile for the two transition types (0 to 1 and 1 to 0). This asymmetry can then be used to extract relevant information from the circuit.

To observe the light emitted, the chip needs to be opened either from its backside or frontside, depending on its package type. Furthermore, the light emission quality depends on the quality of the package opening process [14]. For the backside package opening, the silicon substrate is mechanically thinned down and polished. Indeed the thinning is necessary to decrease the absorption rate of the silicon substrate, and also to maximize the generation of photocarriers in the silicon [15]. On the other hand, when working on the frontside, a chemical process is used, which is easier to perform. Nevertheless, because of the increasing number of metal layers in the circuits that act as a light screen, this technique is less and less used.

The photons emitted can be collected by a specific device equipped with a high sensitivity photon sensor mounted on the optical axis of a conventional microscope. Many types of optical sensors, working with different wavelength efficiencies, can be used (CCD, InGaAs, InSb...). However, due to small transistor size and high silicon doping in the most recent technologies, at normal power supply voltage, the photon emission is maximum in the 900 nm - 1100 nm range. In this spectral range InGaAs detectors have the best quantum efficiency, as shown in Fig.1.

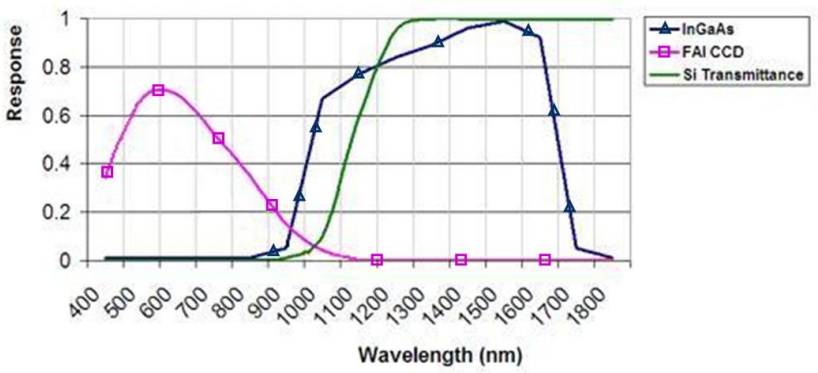

Fig. 1. Comparison of sensor technologies in relation to the silicon transmittance: response as a function of wavelength

In order to perform our experiments we identified two main complementary techniques able to produce time and spatial information: the Picosecond Imaging Circuit Analysis (PICA) and TRE techniques.

The PICA system acquires the light emitted, conserving time and space information. More precisely, the PICA sensor delivers the time and position of each photon emitted by the targeted circuit zone [16]. This technique has been initially developed to identify any functionality problem using temporal information during backside inspections [17].

The PICA system can be coupled with the TRE technique to target a single transistor or a specific zone in the circuit under inspection. The TRE can produce an histogram of the number of photons emitted as a function of time [18]. These histograms are called "TRE curves" and are shown in Fig.4.

2.2 Experimental Method

Since the light emitted depends on the operation executed, there is a straight correlation between TRE waveforms and the cryptographic calculations. This correlation can be exploited through a DPA process. The aim of the DPA is to reveal the secret keys of cryptographic devices based on a large number of power consumption traces that have been recorded during the data encryption of a cipher algorithm. The main advantage of this process is that it only requires knowledge of the cryptographic algorithm that is executed [2]. After extraction of part of a sub-key, the missing parts can be gathered by iterating the process. For our purpose, we replaced the power consumption acquisitions by light emission traces (TRE).

The acquisition system used is a Hamamatsu Tri-PHEMOS equipment [19]. This equipment is composed of an InGaAs camera coupled with a photon counting system. Thanks to this apparatus, we were able to carry out a successfull measurement campaign using a Hamamatsu high performance InGaAs camera (high infrared sensitivity in the 950 nm to 1400 nm range). The optical sensor

of the InGaAs camera (resolution of 640x480 with a pixel size of 20μm x 20μm) associated with a Solid Immersion Lens (SIL) allows to obtain a resolution of 300 nm and to observe a structure on a 65 nm chip. Moreover, the Tri-PHEMOS equipment is able to perform both static and dynamic light emission measurements with very high precision.

For the experiment we choose to implement part of a cipher algorithm on a FPGA device as shown in Fig.2. A specific test board was built, as shown in Fig.3. It is composed of a FPGA mechanically opened from the backside (silicon s down to 70μm), and laid upside down. In addition, a built-in potentiometer can be used to increase the FPGA core voltage (1.5V to 3V) in order to increase the light emission activity. In this experiment we performed the measurements at the typical voltage level (1.5V).

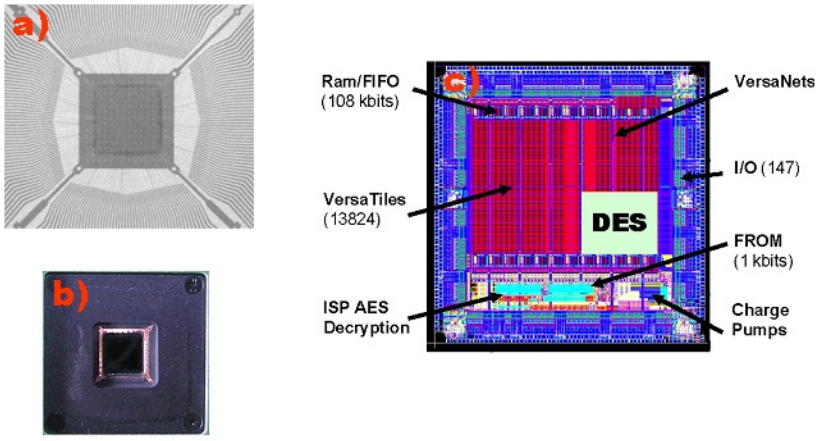

Fig. 2. Different view and informations about the FPGA Actel Proasic3e a) x-ray image b) Picture of the FPGA open from the backside c) Layout informations [20] with location of the DES implementation

The target of our attack was a fragment of a Data Encryption Standard (DES) cipher algorithm. Indeed, in order to simplify our experiment and lighten the data processing, the chosen target was the first round of the DES algorithm, and more specifically the first SBOX. Our goal was to validate the theory and the method efficiency on a small part of the DES algorithm.

Prior to these acquisitions, the light emission activity induced by the 'crypto-processor' needs to be localized in order to start the acquisition. This is done by a static scan, consisting in acquiring the light emitted for a few minutes in order to obtain a photon cartography of the whole FPGA. During this time, the cryptoprocessor encrypts the same message. Then the acquisition window is placed on the emissive area of the cryptoprocessor. Indeed, one asset of this method is that, if the cryptoprocessor can be turn on/off it can be easy to locate the area where it is implemented. The most relevent point is that it is usually sufficient to know the location of the cipher block in order to position a TRE aquisition

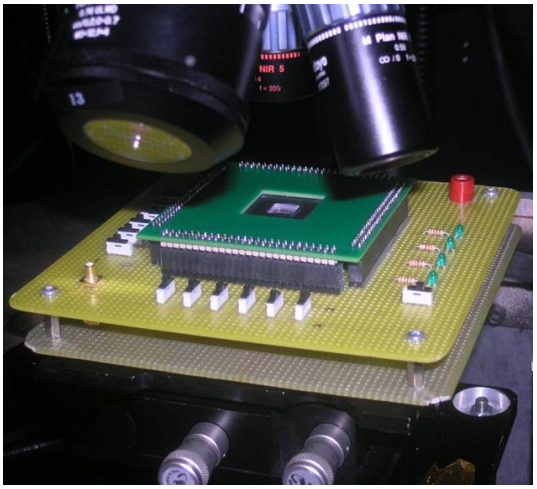

Fig. 3. FPGA test board

window on it. Furthermore, it is not necessary to know either the architecture of the algorithm, or its implementation, as the overall light emission of the cipher block is collected instead of a specific area (SBOX output, XOR operation...). It is then the data post-treatment on the TRE curves which will give us the expected results.

2.3 Results

In Fig.4 the light emission activity of the area where the cipher algorithm is implemented and the corresponding TRE curves are shown. A first message M1 (Fig.4a) is sent to the algorithm, followed by a second M2 (Fig.4b). We can notice that the variation of the input vector sent to the cipher algorithm generates a time and space variation of the emitted light, producing some sensitive differences between the TRE curves. In this way we obtain a TRE curve for each cryptographic calculation, which can then be used as a side-channel signal.

The full set of message vectors ($2^6 = 64$) is sent to the device. In order to obtain the TRE curves, each of the vectors is sent at a frequency of $10MHz$ during 20 seconds, also it has been verified that 5 seconds are sufficient. We used a longer acquisition time to ensure that the camera acquired a number of photons high enough to generate meaningful TRE curves. Each vector is sent to the FPGA in alternance with a zero message. This alternation is needed to force the transisitors to reset. When reseted transistors switch to 1, light emission happens; therefore reseting the transistors force them to emit light. This process generates a set of 64 TRE curves.

Once the TRE curves are acquired, it becomes possible to process them in order to try to extract the key. In our case, the chosen discriminant to classify the curves in the transition groups (0 to 1 or 0 to 0) is based on the chosen

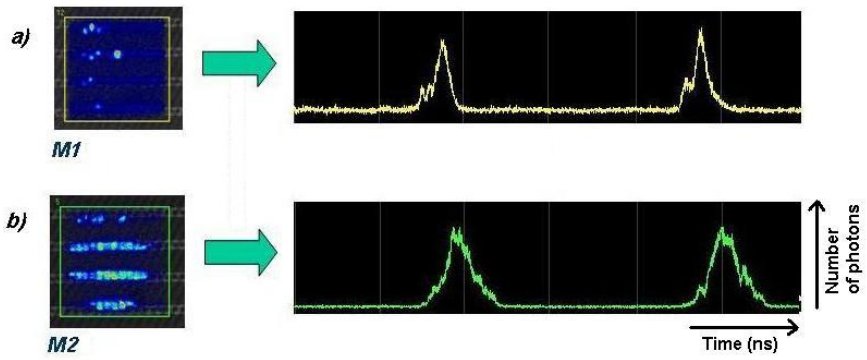

Fig. 4. Variation of TRE curves in function of the light emission activity

bit at the SBOX output, since during the acquisition we forced a reset between each message by sending a zero value. The differential curves resulting from the statistical processing on each output bit are shown in Fig.5.

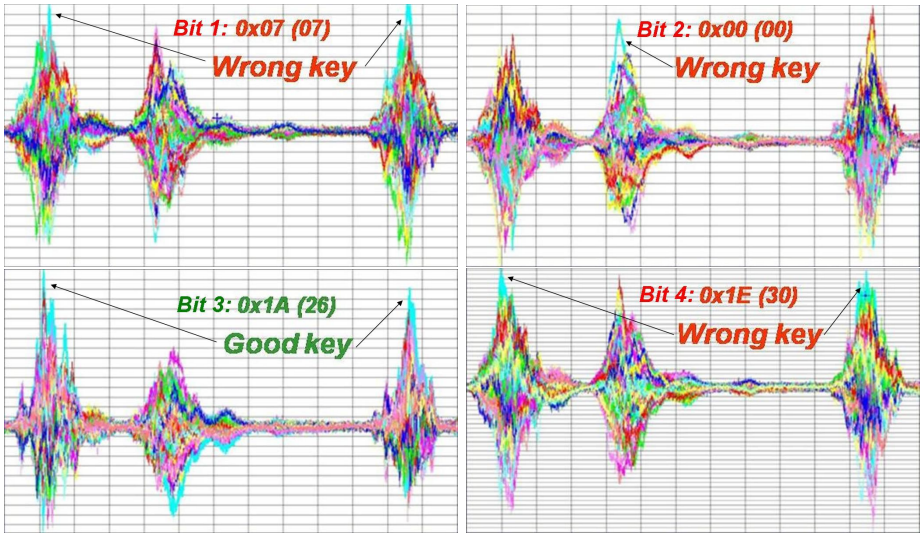

Fig. 5. Differential curves of the 64 key hypothesis for each output bit (number of photons emitted as a function of time(μs))

The attack performed on the third bit reveals the right key; however, the attacks on the first, second and fourth bits are inconclusive. On the other hand, if we sum up the four output bits to enhance the differences between the differential curves [21] we obtain the results shown in Fig.6. These results show that the curve for the right sub-key stands out. This result demonstrate, by targeting the whole cipher block with a TRE acquisition window (without a real precision),

the possibility to exctract a sub-key by using light emission leakage. In the next section, we propose to demonstrate that laser stimulation coupled with the DPA method could be an innovative technique for side-channel analysis.

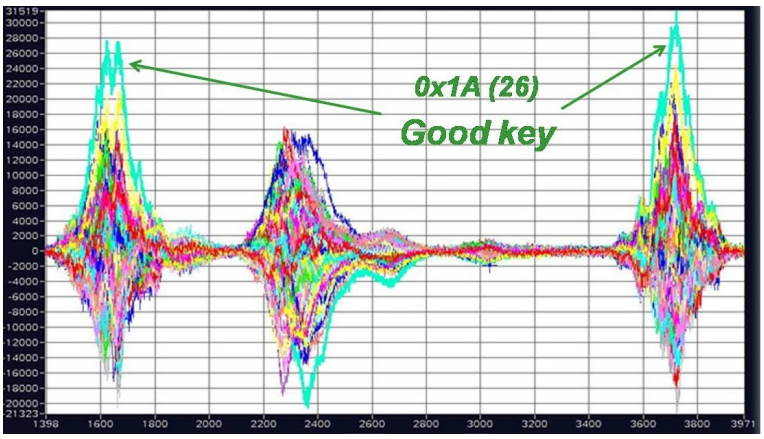

Fig. 6. Sum of differential curves for each output bit (number of photons emitted as a function of time(μs))

3 Laser Stimulation to Improve Side-Channel Attacks

3.1 Background

The photoelectric laser stimulation is a failure analysis technique that uses a scanning laser beam to induce a current flow. This one can be collected and analyzed to generate images that represent the semiconductor sample properties [10]. Indeed, when the laser beam scans the surface of the sample, some electrons into the conduction band are excited thanks to the 'single-photon absorption' phenomenon. In the single-photon absorption process, a single photon excites one conduction band electron. This can only occur if that single photon carries enough energy to overcome the band gap of the semiconductor (1.2 eV for Silicon) and provide the electron with enough energy to make it jump into the conduction band. The creation of charge carriers by excitation of the semiconductor with an optical beam results in a current flow that can be collected and used for imaging. The IC current variations induced by the laser beam is converted into a contrast variation to form an image [8].

One limitation of this technique is that for modern integrated circuits, it is hard to transmit light uniformly to the semiconductor itself. This non-uniform transmission of light is caused by the presence of several metal layers and other materials above the semiconductor. In such instances, one solution is to perform the imaging from the backside through the substrate. However the spatial resolution is limited due to a compromise between being able to transmit the beam

through the substrate, and allowing the beam to be absorbed by the semiconductor for the generation of electron-hole pairs that are measurable as a current, as shown in Fig.7.

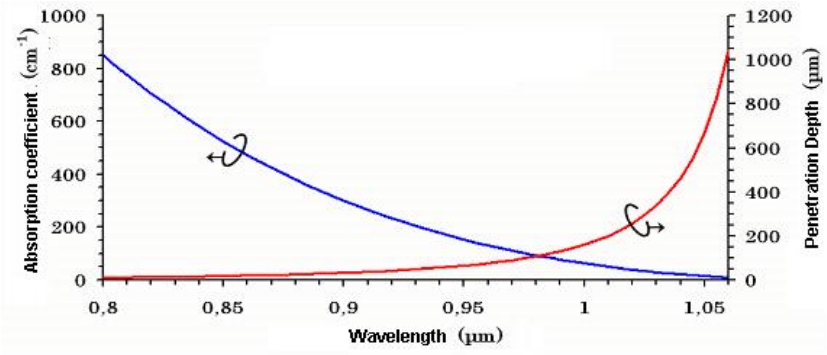

Fig. 7. Absorption coefficient and penetration depth as a function of wavelength [22]

The laser stimulation can be performed by a specific device equipped with a laser beam mounted on the optical axis of a conventional microscope. Two types of laser beams, working with different wavelength, can be used: 1064 nm to induce a photocurrent effect and 1360 nm to induce a thermal effect (and a small photocurrent effect as well). However, the present experiment involves the use of the photocurrent effect, thus the 1064 nm (or less) wavelength is chosen.

3.2 Experimental Method

The aim of this experiment is to extend the method described by Skorobogatov [11] to a DPA attack on a DES cipher algorithm, implemented on a FPGA. With the help of a scanning laser equipment used in failure analysis activities, it becomes possible to scan a chosen area into the FPGA corresponding to the location where a critical function (SBOX, end of round, XOR) of the DES is implemented. Theoretically, the laser induces a current on the chosen scanning area. This additional current should increase the consumption of the circuit during the algorithm encryption, and thus improve the attack by reducing the number of power consumption acquisitions.

The light source used is the Meridian I acquisition system from DCG Systems [23], equipped with a laser scanning microscope system (LSM) with two different lasers for induced current and thermal stimulation (1064 nm and 1340 nm). For the experiment, we implemented a full DES cipher algorithm on the same FPGA device (Actel Proasic3) as for the light emission experiment. This FPGA is opened from the backside and mounted on the same specific test board. The main interest of the FPGA implementation is that it is possible to choose the area where the different DES sub-blocks are implemented on the FPGA programmation grid, as shown in Fig.8.

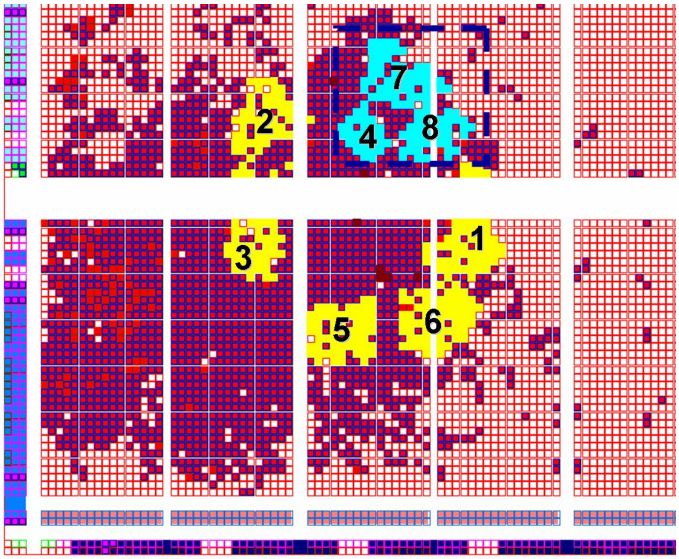

Fig. 8. Location of the DES SBOX on the FPGA programmation grid

The first challenge is the choice of the power laser source, since it is necessary to ensure that the power is neither too low to generate enough photocurrent nor, too strong to avoid a fault injection. For the considerate wavelength, several tests revealed that the maximum power at which the algorithm generates errors is 15-18 mW, therefore a laser power of 10-11 mW is chosen. The second challenge is to select an area for the laser scan, for instance SBOX area. After several trials we selected the area including the 4th, 7th and 8th SBOX (dotted in Fig.8), offering the possibility to scan three SBOX at the same time with a 1μm laser spot size at 20x zoom lens. Once these steps are complete, a first DPA attack is performed without any laser scan in order to have a reference, followed by a second DPA attack with the laser scan on the area previously identified.

3.3 Results

During the first acquisition process, without any scanning laser, 16000 random messages are sent. The differential process results, considerate as a reference, are shown in the table in Fig.9. The table details the attack results on each bit of each SBOX. The discriminant used is on the one hand a DPA chosen bit at the End of Round (first four rows), and on the other hand a CPA [24] Hamming Weight at the End of round (last row).

A second acquisition process with a scanning laser (with a scan frequency of 200 khz) is then performed, with the same random messages. In Fig.10 the table shows the comparison between the numbers of power traces necessary to perform the attack with and without the laser scan. The discriminant used

	Sbox 1	Sbox 2	Sbox 3	**Sbox 4**	Sbox 5	Sbox 6	**Sbox 7**	**Sbox 8**
Bit 0	YES	NO	YES	YES	NO	YES	NO	NO
Bit 1	NO	YES	YES	YES	YES	YES	NO	NO
Bit 2	YES	YES	YES	NO	NO	NO	YES	YES
Bit 3	YES	YES	YES	NO	NO	NO	YES	YES
CPA	YES	YES	YES	NO	NO	YES	YES	NO

Fig. 9. DPA result laser stimulation at the end of the round without (16000 curves)

is again a DPA chosen bit at the End of Round (first eight columns), or a CPA Hamming Weight at the End of round (last two columns). In each case the number of curves necessary to obtain the right sub-key is shown.

	Bit 0		***Bit 1***		***Bit 2***		***Bit 3***		***CPA***	
Laser state	OFF	ON	OFF	ON	OFF	ON	OFF	ON	OFF	ON
SBOX 4	~11000	~6500	~11500	~6500	NO	~9000	NO	~9500	NO	YES
SBOX 5	NO	~14500	~10000	~9500	NO	NO	NO	NO	NO	NO
SBOX 6	~11500	~9500	~10000	~7500	NO	NO	NO	~12500	YES	YES
SBOX 7	NO	~9000	NO	~8500	~10500	~6500	~11500	~6500	YES	YES
SBOX 8	NO	NO	NO	NO	~12000	~9500	~13500	~10000	NO	NO

Fig. 10. Comparison between both DPA results with and without laser stimulation and numbers of curves necessary to perform the attack - (laser 1064 nm / power 11 mW)

These results highlight several interesting facts. First, the number of curves required to perform a successfull attack are decreased by approximately half on bits (0,1) of SBOX 4 and bits (2,3) of SBOX 7. Moreover, the attack on bits (2,3) of SBOX 4 and bits (0,1) of SBOX 7 with the laser scan allows to recover the good sub-key, whereas the attack on the same bits without laser stimulation are unsuccessful. Likewise, the CPA on SBOX 4 is successful. These results suggest that the laser has a real influence on the power consumption of the circuits and in particular on the targeted SBOX. Fig.11 highlights the amplitude differences between differential curves with and without a scanning laser (16000 power consumption curves were used). This comparison underlines the influence of laser scans on the efficiency of the attack. Nevertheless the 8th SBOX, although scanned by the laser, is not so impacted (this fact is not yet explained). On the opposite, bits (0,1,3) of SBOX 6 and bits (0,1) of SBOX 5 seems to react to the laser stimulation in a lesser extent. This could be explained

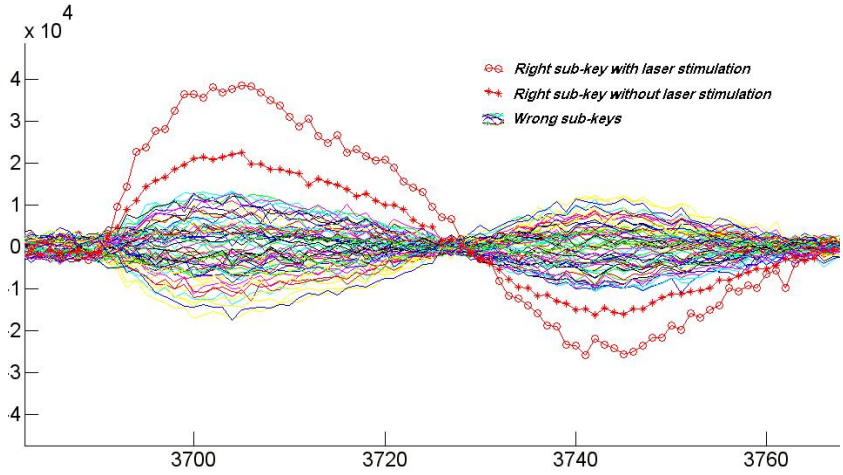

Fig. 11. Amplitude comparison between differential curves on the right key with and without laser stimulation (DPA in 16000 curves on bit 0 of SBOX 4)

by a spreading of photocurrent neighboring SBOX, or by an indirect influence of the scanning laser on the interconnection lines between the two SBOX (e.g. 6 and 7).

4 Conclusion

These different experiments show how failure analysis tools could be effectively applied to perform or enhance side-channel attacks. The light emission techniques allow to localize the different functions implemented on a circuit. With only partial knowledge of the circuit design and by using the TRE technique, light emission enables determination of the internal behavior of the circuit functions. Using the DPA method, we have shown that a differential light emission analysis allows retrieval of the cipher sub-key from a fraction of the DES algorithm implemented on an FPGA that uses a 130 nm technology. Many developments can be carried out based on this method, and multiple perspectives can be considered. First, the efficiency of this technique should be compared to other side-channel methods to further highlight the specific contributions of this method. Moreover, in the experiments reported here, only time information is used. Space information, which is also available, offers the opportunity to refine the process and to improve the method. On the other hand, some countermeasures for this type of attacks have to be developed. A "natural" one is certainly the lack of resolution of the sensors versus the latest CMOS technologies (45 nm or less). The light emission profiles are yet to be investigated for these technologies. A countermeasure, for FPGA devices, could be a dynamic reconfiguration to change the light emission profile, or the insertion of sensors inside the package to detect its opening. We can also notice that the number of TRE curves that

need to be acquired to break this type of unprotected implementation is much higher than those for EMA and DPA.

The second experiment based on a laser stimulation technique allows to partially increase the power consumption of a circuit, by scanning a specific area during the encryption of the cipher algorithm. This way it is possible to significantly reduce the number of curves necessary to perform a DPA attack. For this technique also many developments and perspective can be considered. These recent results require further investigation in order to specify how the laser method could be used. For example it could be interesting to repeat several DPA attacks by scanning the SBOX individually (or all the SBOX chained) to establish a comparative statement detailing how the laser method improves the attack. It would be also interesting to apply this method on a secure cipher algorithm, for instance that uses dual rail implementation [25]. Laser scans could be used to induce an unbalance power consumption and thus exctract the sub-key. Concerning the method itself, it would also be interesting to reproduce the attack using a laser with a wavelength below 1064 nm to increase the photogeneration of free carriers, or to attempt to use other light source (such as halogen light) instead of monowave light laser source. The using of a static laser (without scan mode) to continuously illuminate the area of interest would also be interesting.

The main constraint for these methods is the backside opening of the component and more particularly the silicon thinning step, a process quite hard to control. In any case, at the present time, due to the price of the equipments used in these experiments (beyond 2M euros for the Tri-PHEMOS and 500K euros for the Meridian), the cost of these attack-enhancing method appears to be very high. An interesting point for future research will be to re-do these experiments on a low-cost sytems to validate the real benefit of them, for example in [6] [11] the author shows the possibility to design a low-cost system based on PMT detector coupled with a CCD camera to perform light emission experiments and a 639 nm laser coupled with a CCD camera to perform laser experiments. However, proof that failure analysis and side-channel attacks are compatible has been provided, and further studies are currently under way based on these promising results.

Acknowledgment

We would like to thank the Hamamatsu Photonics company that allowed us to perform a succesful measurement campaign on their Tri-PHEMOS system, and also the Hamamatsu team for their technical support. Thanks also to Fabien Battistela and Kevin Sanchez for their precious advice and discussions.

References

1. Perdu, P.: Contribution a l'Etude et au Developpement de Techniques de Localisation de Defauts dans les Circuits Intgrs VLSI, Ph.D. diss., Bordeaux University (2001)
2. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)

3. Quisquater, J.-J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In: Attali, S., Jensen, T. (eds.) E-smart 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)
4. Barton, D.L., Tangyunyong, P., Soden, J.M., Liang, A.Y., Low, F.J., Zaplatin, A.N., Shivanandan, K., Donohoe, G.: Infrared Light Emission from Semiconductor Devices. In: 22th International Symposium for Testing and Failure Analysis, pp. 9–17 (1996)
5. Ferrigno, J., Hlavac, M.: When AES Blinks: Introducing Optical side-channel. IET Information Security 2(3), 94–98 (2008)
6. Skorobogatov, S.: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. In: 6th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 111–119. IEEE-CS Press, Los Alamitos (2009)
7. Di-Battista, J., Perdu, P., Courrege, J.C., Rouzeyre, B., Torres, L., Lionel: Light emission analysis on FPGA: a new side channel possibility. In: 7th Workshop on Cryptographic Architectures Embedded in Reconfigurable Devices, CryptArchi 2009 (2009)
8. Stevens, K.C., Wilson, T.J.: Locating IC Defects in Process Monitors and Test Structures Using Optical Beam Induced Current. Microelectronic Engineering 12, 397–404 (1990)
9. Soelkner, G.: Optical beam testing and its potential for electronic device characterization. Microelectronic Engineering 24, 341–353 (1994)
10. Fritz, J., Lackman, R.: Optical Beam Induced Currents in MOS Transistors. Microelectronic Engineering 12, 381–388 (1990)
11. Skorobogatov, S.: Optically Enhanced Position-Locked Power Analysis. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 61–75. Springer, Heidelberg (2006)
12. Desplats, R., Beaudoin, F., Perdu, P.: Chip Unzip for Backside Sample Preparation. In: 27th International Symposium for Testing and Failure Analysis, pp. 179–187 (2001)
13. Wallinger, T.: Characterization of Device Structure by Spectral Analysis of Photoemission. In: 17th International Symposium for Testing and Failure Analysis, pp. 325–334 (1991)
14. Barton, D.L., Bernhard-Hofer, K., Cole Jr., E.I.: Flip-Chip and Backside techniques. Microelectronics Reliability 39, 721–730 (1999)
15. Baudouin, F.: Localisation de defaut par la face arriere des circuits integres. Ph.D. diss., Bordeaux University, 38–40 (2002)
16. Tsang, J.C., Kash, J.A., Vallett, D.P.: Picosecond imaging circuit analysis. IBM Journal of Research and Development 44, 583–603 (2000)
17. McManus, M.K., Kash, J.A., Steen, S.E., Polansky, S., Tsang, J.C., Knebel, D.R., Huott, W.: Huott: PICA: Backside Failure Analysis of CMOS Circuits Using Picosecond Imaging Circuit Analysis. Microelectronic Reliability 40, 1353–1358 (2000)
18. Kolzer, J., Boit, C., Dallmann, A., Deboy, G., Otto, J., Weinmann, D.: Quantitative Emission Microscopy. Journal of Applied Physics 71(11), R23–R41 (1992)
19. Hamamatsu Photonics, `http://www.hamamatsu.com/`
20. Actel Proasic3 Handbook: 144, `http://www.actel.com/products/pa3/docs.aspx`
21. Bevan, R., Knudsen, E.: Ways to Enhance Differential Power Analysis. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 327–342. Springer, Heidelberg (2003)

22. Sanchez, K.: Développement et applications de techniques d'analyse par stimulation dynamique laser pour la localisation de défauts et le diagnostic de circuits intégrés. Ph.D. diss., Bordeaux University (2007)
23. DCG systems, http://www.dcgsystems.com/
24. Brier, E., Clavier, C., Oliver, F.: Correlation Power Analysis with a Leakage Model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
25. Bystrov, A., Yakovlev, A., Sokolov, D., Murphy, J.: Design and Analysis of Dual-Rail Circuits for Security Applications. IEEE Transactions on Computers 54(4), 449–460 (2005)