Frontside Versus Backside Laser Injection: A Comparative Study

Stephan de Castro, Jean-Max Dutertre, Bruno Rouzeyre, Giorgio Di Natale, Marie-Lise Flottes

Authors' version
http://dx.doi.org/10.1145/2845999
ACM Journal on Emerging Technologies in Computing Systems (JETC)

A

Front-side vs backside laser injection: a comparative study

Stephan De Castro, LIRMM, University of Montpellier, France
Jean-Max Dutertre, ENSMSE, LSAS, CMP Gardanne, France
Bruno Rouzeyre, LIRMM, University of Montpellier, France
Giorgio Di Natale, LIRMM, UMR CNRS 5506, Montpellier, France
Marie Lise Flottes, LIRMM, UMR CNRS 5506, Montpellier, France

The development of cryptographic devices was followed by the development of so-called implementation attacks, which are intended to retrieve secret information exploiting the hardware itself. Among these attacks, fault attacks can be used to disturb the circuit while performing a computationin order to retrieve the secret. Among possible means of injecting a fault, laser beams have proven to be accurate and powerful. The laser can illuminate the circuit either from its frontside (i.e., where metal interconnections are first encountered) or from the backside (i.e., through the substrate). Historically, frontside injection was preferred because it does not require the die to be thinned. Nevertheless, due to the increasing integration of metal layers in modern technologies, frontside injections do not allow anymore to target any desired location. Indeed, metal lines act as mirrors and they reflect and refract most of the energy provided by the laser beam. Conversely, backside injections, while being more difficult to set up, allow increasing the resolution of the target location and remove the drawbacks of frontside technique. This paper compares experimental results from frontside and backside fault injections. The effectiveness of the two techniques is measured in terms of exploitable errors on an AES circuit, i.e., errors that can be used to extract the value of the secret key used during the encryption process. We will show that, conversely to what is generally assumed, frontside injection can provide even better results compared to backside injection, especially for low-cost beams with large laser spot.

Categories and Subject Descriptors: [**Authors' version**]:

Additional Key Words and Phrases: Laser Fault Injection, Frontside injection, Differential Fault Analysis

ACM Reference Format:
Stephan de Castro, Jean-Max Dutertre, Bruno Rouzeyre, Giorgio Di Natale and Marie Lise Flottes, 2014. Front-side vs backside laser injection: a comparative study. *ACM Trans. Embedd. Comput. Syst.* V, N, Article A (January YYYY), 15 pages.
DOI:http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

The wide spreading of hardware cryptographic devices to protect privacy leads to the emergence of many types of attack aiming to retrieve secret information. Among these attacks, so-called "fault attacks" rely on disrupting the circuit during the computation of the cryptographic algorithms ([BDL97][BS97]). One of the most effective techniques to inject fault in a circuit is the use of laser beams.

Laser injections can be performed either through the frontside of a circuit (metal layer side) or through its backside (substrate side). Historically, fault attacks first exploited frontside injection [SA03]. Nevertheless, due to the increasing integration of metal layers in modern technologies, frontside injections do not allow anymore to target any desired location. Indeed, metal lines act like mirrors and they reflect and refract most of the energy provided by the laser beam. Metal density can reach up to 10 layers for new technologies as depicted in Figure 1 [MBV08]. On the contrary, backside injections, while being more difficult to set up due to the necessary thinning pre-process, allow increasing the resolution of the target location and remove the drawbacks of frontside technique.

Even if frontside laser injection does not allow precisely controlling the target fault location in modern technologies, its use could be still effective when the purpose is to generate an exploitable fault, i.e., an error that can be successfully used to extract the

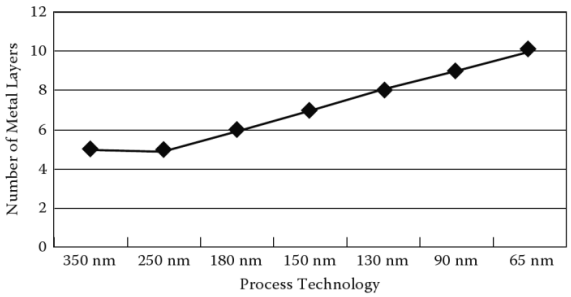

Fig. 1. Number of metal layers available in various CMOS technologies [MBV08]

value of a secret key used during an encryption process for instance. The aim of this work is to verify whether this assumption is correct or not. We experimentally performed both frontside and backside laser fault injections on a circuit implementing the Advanced Encryption Standard (AES) algorithm [AES01]. The effectiveness of both attacks is compared in terms of attack successes, i.e., obtained number of exploitable faults. The paper is structured as follows. The underlying photoelectric-induced current phenomenon and differences between frontside and backside injection techniques are described in section 2. A brief description of the AES algorithm and related fault attack requirements are provided in section 3. Experimental set-up and target circuit description are given in Section 4. Then, injection results are compared in section 4. Limitations and possible countermeasures are discussed in section 5. Finally Section 6 presents some conclusions drawn from this work.

2. FRONT-SIDE VS BACKSIDE INJECTION

2.1. Photoelectric effect

When light emitted by a laser hits a CMOS device, the deployed energy is turned into electrical current because of the photoelectric effect [Hab65]. If the energy of photons emitted by the laser is sufficient, these photons create electronhole pairs along their path through the silicon.

A current is the result of charges movement. As a consequence of the photoelectric effect, two mechanisms put the charges created by the laser in movement and therefore induce a transient current. A PN junction is taken as an example to present these mechanisms.

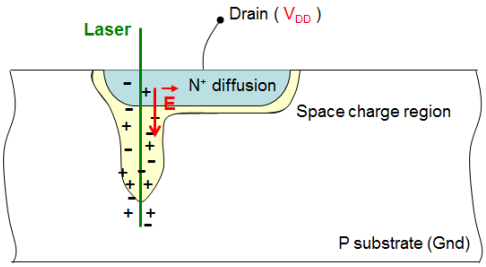

Fig. 2. The mechanism responsible for Optical Beam Induced Current [DdCS+14]

Figure 2 depicts a reverse biased PN junction (drain to Vdd, substrate to Gnd). This polarization creates a wider space charge region at the interface between the P and N regions. As the laser beam goes through the PN junction and the silicon, it creates electronhole pairs. Then the charges that are close enough to the junction are moved (attracted or repulsed depending on the charge) by the effect of both the electric field and the diffusion effect (movement of charges in order to maintain an equal concentration of charges among all the silicon). The charges that are far from the junction recombine themselves without any effect on the induced current at the drain of the junction.

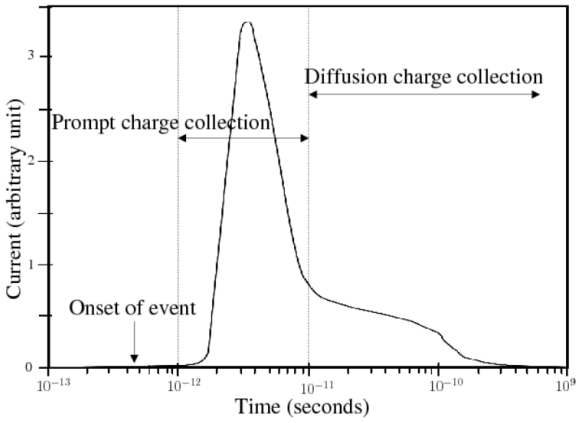

Fig. 3. Typical shape of nodal current at a p-n junction [WA08]

Figure 3 shows the typical shape of the induced transient current at the drain node created by the laser. The electric field and the diffusion effects can be differentiate on the shape. The prompt collection corresponding to the electric field effect induces a high current during a short time. The diffusion-induced current has a decreasing amplitude that lasts longer than the prompt collection. This is due to the speed of the diffusion phenomenon in silicon.

Equation (1) represents an accurate enough model of the current shape observed in Figure 3.

$$I(t) = \frac{Q}{\tau_a - \tau_b}(e^{\frac{-t}{\tau_a}} - e^{\frac{-t}{\tau_a}}) \tag{1}$$

Where Q is the charge deposited by the laser strike, τ_a is the collection time constant which is a process-dependent collection time constant of the junction and τ_b is the laser-track establishment time constant which is relatively independent of the technology. Typical value of τ_a and τ_b can be found in [CCIC90].

The induced current can be high enough to temporarily invert the output logic level of a logic cell, thus possibly generating an error in the circuit. The following subsection details how faults can be generated within a digital circuit, by means of a laser injection

2.2. Single Event Transient (SET) and Single Event Upset (SEU)

The mechanism by which the induced current changes a logic value is presented in 4 on an inverter.

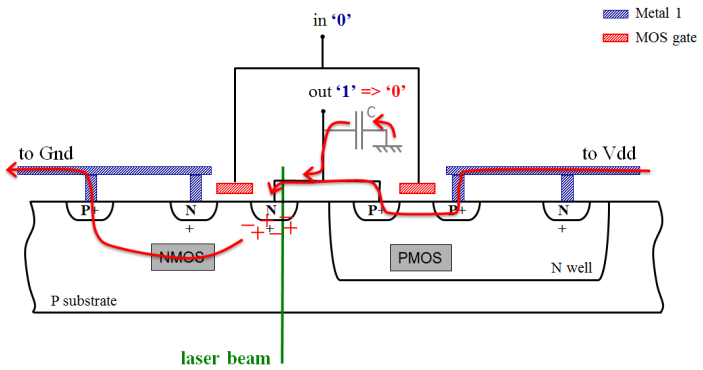

Fig. 4. : Effect of the induced current on an inverter gate (cross section) [DdCS+14]

Let assume the input of the inverter being equal to logic value '0', its output being '1'. The NMOS transistor is in OFF mode, with a reverse biased PN junction below its drain. The PMOS Transistor is in ON mode. Assuming stationary conditions, the equivalent output capacitance (i.e., the sum of all gate/wire capacitances connected to this output) is fully charged.

If a laser beam reaches the drain of the NMOS transistor, a transient current flows from the drain to the Gnd through the bulk. This current moves electrons from both Vdd and the equivalent output capacitance toward Gnd. As a consequence, the gate output capacitance is discharged. When the illumination duration is large enough, the output capacitance is discharged at the point where the output voltage falls under the threshold voltage of the next logic gates, thus causing a transient logic fault, the so-called Single Event Transient (SET). As the laser illumination ceases, the ON mode PMOS ensures that the output loaded capacitance is restored, thus ensuring that the output voltage goes back to logic value '1'.

SETs have different effects on the circuit behavior according to the target cell and the time of the illumination. If the SET created on a gate output propagates to a memory element (no logical masking), and affects its input during the latching window of the memory element, the circuit stores an erroneous value (e.g. Figure 5). The SET has no further effect otherwise.

If a storing element is directly aimed as in Figure 5.b, the timing constraints are more permissive than for a SET to induce an error. Indeed, the logic value stored in the memory cell can be directly flipped (Single Event Upset: SEU). Thereby, the erroneous logic value is released to the next clock cycle.

2.3. Front-side and backside injection characteristics

Laser injection can be performed shooting either from the front-side or the backside of the chip. In the following paragraphs we sketch the characteristics, main advantages and drawbacks of these two techniques.

Front-side injection can be performed using any kind of wavelength (green or infrared). The absorption depth is defined as the distance after which the energy decreases by 37%. Figure 6 depicts the penetration depth of the silicon depending on the wavelength used. For the green wavelength ($532nm$), the penetration depth is almost $1\mu m$. For the infrared wavelength ($1064nm$), the absorption depth is a few hundreds of μm. Green wavelength is therefore preferred for frontside injections since the energy is absorbed near the surface of the silicon, where transistors are built. Conversely, for backside injections the laser beam has to traverse the whole wafer (generally between

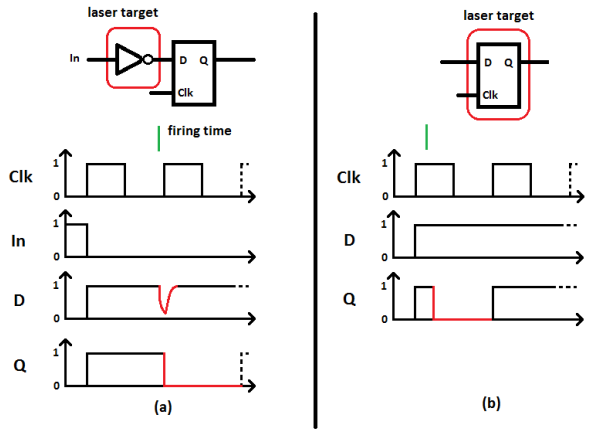

Fig. 5. SET (a) and SEU (b) mechanisms

$300\mu m$ and $500\mu m$) in order to reach the laser-sensitive PN junctions. Infrared wavelength is thus a mandatory choice since the absorption depth is in the order of the wafer thickness (a green laser beam would not reach the laser sensitive parts of the target).

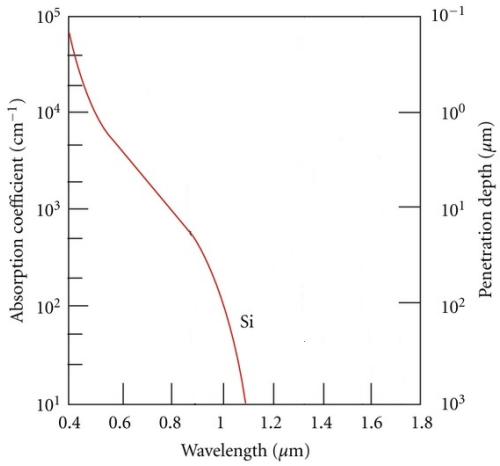

Fig. 6. Penetration depth in Silicon depending on the wavelength [Pou00]

Concerning the efficiency and complexity of the injection set-up, front-side injection is generally easier to do than backside injection since it only requires the chip to be un-packaged, it does not require any other manipulation of the silicon die [Mir11]. Unpackaging can be done (mechanically or chemically) in few minutes. Nevertheless, this type of injection is difficult to realize due to the increasing number of metal layers. Indeed, metal interconnects reflect most of the light coming from the laser beam, thus reducing the target silicon area as shown in Figure 7.

In order to perform a backside injection in the best conditions, the wafer has to be thinned. This is done either mechanically using an expensive equipment or with chem-

ical products. The mechanical thinning uses a spinning tools that can scratch or polish the silicon, the thinning operation last around few hours for one circuit [Mir11]. The chemical thinning is cheaper but requires to manipulate dangerous products and to know well the protocol in order not to destroy the circuit. More details on this technique can be found in [CLMFT14][Tar08]. Mechanical thinning is preferred for backside injection due to the better thinning accuracy of this method. Generally a wafer thickness is between $300\mu m$ and $500\mu m$. It has to be thinned down to $100\mu m$ (Figure 7). It allows, together with a good tune of the laser energy to create a fault without damaging the circuit.[Sch81] [Pal91]

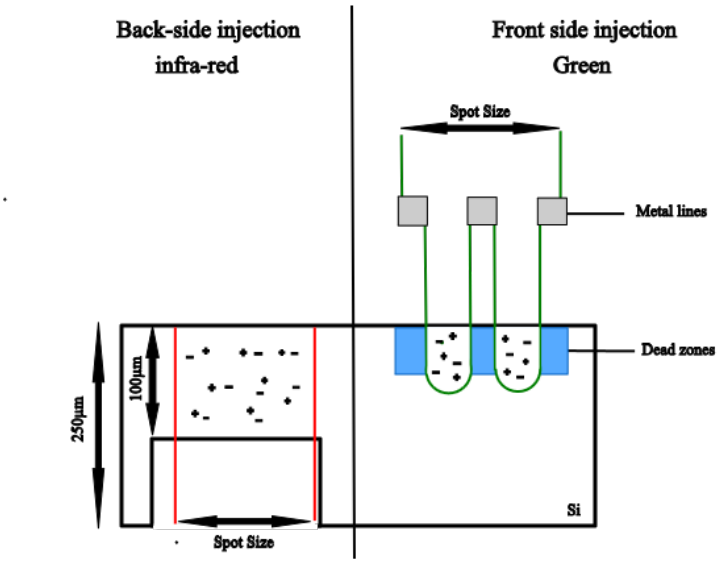

Fig. 7. Front-side and backside injection constraints

Table I summarizes the characteristics of each injection way.

Table I. Front-side and backside injection characteristics

	Front-side	Backside
Wavelength used	Green (532nm) or infrared	Infrared (1064nm)
Absorption depth	$\approx 1\mu m$	$\approx 100\mu m$
Characteristics	Presence of metallization	Has to be mechanically thinned

3. TEST VEHICLE AND ERRORS

Backside laser injection allows high accuracy in terms of geometric location of the target spot, permitting very precise attacks on every parts of a circuit. While this characteristic might suggest that backside attack is the best approach to successfully performing a fault attack on a crypto-processor, we show in this section that in some cases it is possible to use front-side injections.

In the sequel of the paper, we consider as a test vehicle, some known fault attacks on a circuit implementing the AES cryptographic algorithm [AES01]. The AES algorithm

is briefly described in subsection 3.1 Then, fault attacks requirements are presented in subsection 3.2.

3.1. AES presentation

The Advanced Encryption Standard (AES) is a cryptographic symmetric algorithm. In this paper we focus on the AES 128 (128 bits for both the plaintext/cyphertext and the secret key). The AES algorithm's internal operations are performed on two dimensional arrays of bytes called State and a Round key. The State consists of 4 rows of bytes and each row has 4 bytes. The four bytes in each column of the State array form a 32-bit word, with the row number as the index for the four bytes in each word.

The AES-128 algorithm is an iterative algorithm. After addition (i.e a bitwise xoring) of the initial secret key K_0, 10 rounds (iterations) are executed. Figure 8 shows typical operations performed during one round: SubBytes, ShiftRows, MixColumns and AddRoundKey. The first 9 rounds consist of these 4 transformations while the 10^{th} round excludes the MixColumns transformation. After each round, the result is stored in a 128-bit "round-register".

The SubBytes operation is performed thanks to 16 Substitution boxes (Sbox), each of them substitutes the value of one byte M_i of the State, i=0 to 15. The SubBytes operation is the only nonlinear operation in the algorithm. The ShiftRows operation is a row-based permutation of the State bytes. The MixColumns is a column-based transformation of each column of the State. Finally the AddRoundKey operation consists of adding (xor operation) the corresponding round key Ki to the state. Round keys K_1, to K_{10} are derived from the initial secret key K_0.

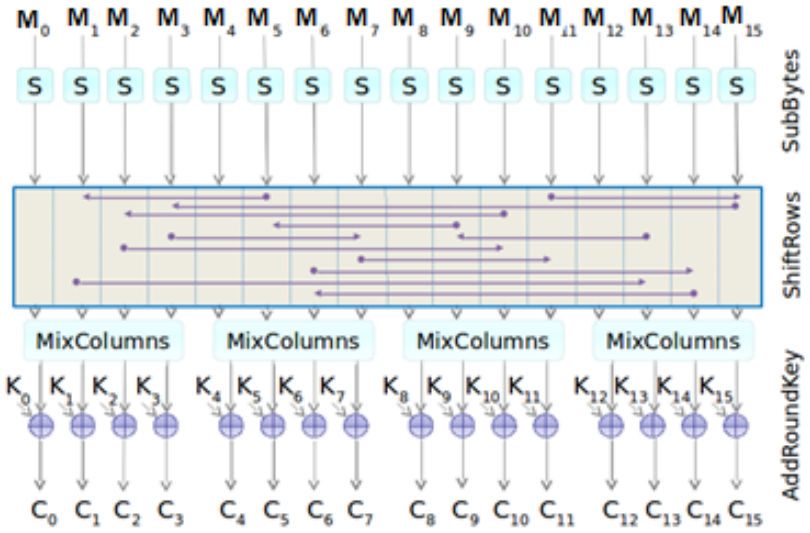

Fig. 8. AES encryption of the i^{th} round

3.2. Fault attacks and exploitable errors

Fault attacks are a powerful mean to retrieve secret keys of cryptographic algorithms, like the AES. In order to exploit the effect of the injection, the produced fault has to

fulfill some requirements for the attack to be successful. These requirements concern a specific time of injection and the location of the induced error (in terms of bits or bytes to be faulted).

Table II summarizes some known attacks on AES as well as their requirements. Column 2 gives the target value to be faulted. Column 3 reports the requirement necessary to perform the attack in terms of spatial accuracy. For instance, in [BS03], a single bit in the plaintext M_0 has to be faulted. Conversely, if more than one bit is faulted, the attack fails.

Table II. Some known attacks on AES 128 [Mir11]

	Target	Focalization
[BS03]	Data(M_0)	Bit
[CNSM03]	Data 7*(M_8)+Key 4*(K_9)	Byte
[Gir03]	Data 16*(M_9)	Bit
[PjQ03]	Key 4*(K_9)+4*(K_{10})+Data 4*(M_8)	Byte
[PjQ03]	Data 4*(M_9) or 1*(M_8)	Byte
[CT05]	Round counter	Round counter value
[PMC+11]	Round counter	Byte
[DLV03]	Data 4*(M_9)	Byte
[RM07]	Data before first subbyte	Bit or Byte
[KQ08]	K_7	Byte
[AMT]	Data at 8^{th} round input	Byte
[AM11]	first column of K_8	Byte

Therefore, based on state-of-the-art fault-based cryptanalysis, it appears that only specific and precisely controlled faults can be exploited in order to retrieve the secret information. The fault has to be injected at the right moment and has to affect either only one bit, or only one byte without impacting other data. While lasers have a sufficient timing accuracy to fulfill the first requirement, spatial accuracy and focalization are more difficult to manage.

In the following section we compare front-side and backside injections in terms of focalization, i.e., the efficiency to fulfill these fault-attack requirements, namely single-bit fault and single-byte fault.

4. EXPERIMENTAL PARAMETERS AND RESULTS

4.1. Experimental set-up

The circuit used for the experimentations is a prototype that has been developed by Ecole Normale Superieur des Mines de Saint-Etienne (ENSMSE). The circuit has been designed with 130nm AMS CMOS technology. Its operating frequency is 25MHz. AES implementation uses a full parallel 128-bit data path. Every AES operation is implemented in a block (AddRoundkey, MixColumns, ShiftRows and Subbytes), plus two 128 bit registers (State and Round Key) and a Finite State Machine (FSM) scheduling the different operations. A round of this AES is computed within a clock cycle, i.e., 40ns. In this circuit, the registers are scattered as shown in Figure 9. Each square represents a $100\mu m * 100\mu m$ area. Blue squares contain the register of the corresponding byte (plus logic gates). For example, square #15 is the register storing the value of the fifteenth byte of the state. All the AES operations are implemented using logic gates scattered among the circuit.

This circuit is put on a PCB board linked with a FPGA, the FPGA is used as an interface between the PC and the PCB. A picture of this assembly is given in Figure 10. Signal of interests (consumption, firing of the ciphering) are measured directly by an oscilloscope from the PCB board. The PC controls the FPGA (send data, read data, ciphering).

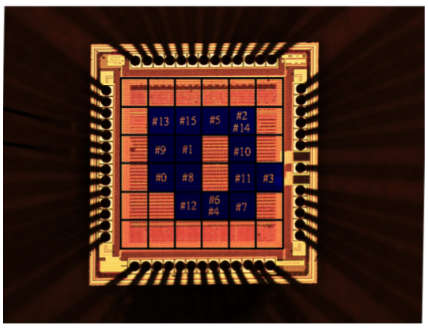

Fig. 9. Mapping of registers on the chip (courtesy [RDT13])

Fig. 10. FPGA board linked with the PCB board and the AES for backside injection

When the cipher command is sent to the circuit, the FPGA generates a signal with two triggers. The first one corresponds to the warming up time (around $200\mu s$ for each shot) of the laser source. The second one corresponds to the beginning of the AES ciphering. The delay between these two triggers can be tuned (by $40ns$ step) in order to focus a specific time during the ciphering of the AES. The firing time can be set by the attacker with an accuracy of around the jitter time, here $10ns$. The circuit is put on a XY table under the laser source. The spatial accuracy of the XY table is about $1\mu m$. Thus laser shot can be done with an accuracy (in time and space) precise enough to perform powerful attack.

4.2. Experimental parameters

The main goal of this work is to check whether fron-side laser injection can provide exploitable results. Indeed, the common assumption is that front-side injection is not effective since most of the light is reflected by metal layers and, for the same reason, the light that reaches the transistors is not controllable. The experimental results presented in this section will prove that front-side laser-injection can also provide relevant results under certain experimental conditions. More specifically, we investigated the use of a large laser beam, similar to those used by attackers with low-cost laser benches at their disposal.

We focus our study on the injection at the ninth round of the AES since we perform Piret and Quisquater attack [PjQ03]. The determination of the nature of the injected fault (multi-byte, single-byte and single bit) is performed by comparing the erroneous

and the correct ciphertexts. Since we know the plaintext, the injection instant and the secret key, we can easily understand which fault has been injected (single-byte or single bit) by performing the inverse function performed by the AES round.

Concerning the timing of the laser beam, it has a 10ns jitter, which represents a quarter of the round duration.

The summary of the laser bench characteristics we used for the experiments is given in Table III:

Table III. Frontside and backside injection parameters

	Frontside	Backside
Pulse width	5ns	5ns
Wavelength used	Green (532nm)	Infrared (1064nm)
Laser Energy	525nJ	675nJ
Spot size	$125\mu m * 125\mu m$	$50\mu m * 50\mu m$

From Table III it can be seen that we deliberately selected a non-performant laser beam for front-side fault injection (high quality laser equipments can have spot size down to $1\mu m * 1\mu m$ and pulse widths of a few ns).

Concerning the energy of the laser, we increased its value step by step until a fault was obtained, thus maximizing the number of faults injected without damaging the circuit.

We supposed that we do not know the layout of the circuit. Therefore we created a map of the circuit by performing 10,000 injections for all the locations of the circuit. We consider as a location a square with a size equivalent to the one of the laser spot.

So, we consider that a location with lots of single-byte faults modifying the same byte is the location of the memory cells storing this byte. This first step leads to the Figure 9. For this location, we compare the number of laser shots and single-byte faults obtained.

Equation (2) defines the injection rate. This rate compares the number of faults injected into the circuit with respect to the number of performed laser shots. The number of faults includes all types of faults, not only those occurring during the ninth round of the AES. In other words, the injection rate show whether the laser is an efficient mean of injecting a fault in the circuit.

$$Injection\ rate = \frac{\#faults}{\#laser\ shots} \tag{2}$$

We focus our experimentation on faults occurring during the ninth round of the AES since we want to implemented the attacks described in [Gir03] [PjQ03]. Therefore, we want to evaluate how many faults can be succesfully exploited, i.e., we want to measure the number of obtained single-byte or single-bit faults. The single-byte fault rate given in equation (3) compares the number of single-byte faults to the overall numbers of faults injected in the ninth round.

$$Single\_byte\ fault\ rate = \frac{\#Single\_byte\ faults}{\#faults} \tag{3}$$

Among all these obtained single-byte faults, we try to sort them out depending on the affected byte of the State. For each affected byte, equation (4) allows comparing the number of single-byte faults to the number of laser shots performed at this location. This rate allows measuring the easiness to perform single-byte attacks.

$$Single\_byte\ shot\ rate = \frac{\#Single\_byte\ faults}{\#laser\ shots} \tag{4}$$

The same rates defined in 3 and 4 and be defined also for single-bit faults.

$$Single\_bit\ fault\ rate = \frac{\#Single\_bit\ faults}{\#faults} \tag{5}$$

The single bit fault rate given in equation (5) compares the number of injected single-bit fault among all the faults occurring during the ninth round of the AES.

This rate allows measuring the accuracy of the injection. Indeed, for a single-bit fault, the injection has to be accurate enough to disrupt a few number of gates or one memory cell. The single-bit shot rate depicted in equation (6) measures the probability of obtaining a single-bit fault.

$$Single-bit\ shot\ rate = \frac{\#Single-bit\ faults}{\#laser\ shots} \tag{6}$$

4.3. Experimental results

In this section, we expose and analyze the experimental results obtained performing front-side and backside injections. We will characterize the effect of the injections by means of the rates described before in section 4.2.

4.3.1. Font side vs. backside injection results. First, we compare both ways of injection in terms of injection rate. As table IV shows the injection rate for front-side injection is about 55% whereas the injection rate for backside injection rate is 100%. This means that with the correct injection parameters and a wide spot size, the attacker is sure to inject a fault in the circuit while performing a backside attack. For front-side injection the rate is only about 55% even with a large spot size.

Nevertheless, the single-byte fault rate is about 78% for the front-side injection while it is only 32% for backside injection. This result is counter-intuitive because the spot size of front-side injection is wider than the one used for backside injection so more logic gates should be disrupted. Moreover, if we focus on the single-bit fault rate, its value is 4% for front-side injection and 0.2% for backside injection. Again, front-side injection seems to be more effective than backside injection in terms of exploitable results.

These results can be explained by the presence of the metal layers on top of the chip. Indeed, a part of the laser beam is reflected by the metal, not participating to the fault injection phenomenon. However, the metal layers also act as a shutter, by reducing the illuminated area of silicon. Therefore, even if a large laser spot is used, the actual silicon area that is affected by the injection is much narrower.

Table IV. Injection rate and fault rates

	Injection rate (%)	Single-byte fault rate (%)	Single-bit fault rate (%)
Front-side	55.4	78	4
Backside	100	32	0.4

Table V gives shot rates for both frontside and backside injection for each byte of the round register. It can be seen that for each byte the rate is higher for front-side injection than for backside injection. This means that, when low-cost laser equipements are used, it is easier to inject single-byte faults from front–side than from back-side.

Moreover, for front-side injection there is a disparity in the rate between bytes. This disparity is larger for front-side injection than for backside injection. This can be explained by the fact that some logic gates and memory cells are in dead zones i.e. shadowed areas. Thus, it's more difficult for the attacker to get fault on these particular bytes with this circuit. In order to get the information given by these bytes, the attacker has to make an exhaustive search of the corresponding bytes value.

Table V. Shot rates

	Single-byte shot rate (%)		Single-bit shot rate (%)	
Byte #	Front-side	Backside	Front-side	Backside
0	28	0.5	3.3	0
1	1.8	0.4	1	0
2	15	0.3	0.9	0.2
3	32	0.4	6.2	0
4	29	0	5	0
5	5	0	0	0
6	18	0.1	5	0
7	45	0.1	1.6	0
8	17	0.1	2.5	0
9	2.5	0.1	1	0
10	6	0	3.3	0
11	34	0.1	2.2	0
12	1	1	0	0
13	15	0	1.4	0
14	24	0	1.6	0
15	6.9	0.1	2.9	0

Experiments show that with a large spot size, front-side injection is a good option to inject exploitable faults according to this result, we analyse in the sequel how front-side injection is a better option than backside injection according to the spot size.

4.3.2. Equivalent size measurement. We want to estimate the size of the silicon area illuminated when injecting from front-side. As the metal lines cannot be removed without altering the circuit's operation, we suppose that injecting from backside gives the same results of an injection from front-side without metal layes (with the same spot size and energy).

We therefore reduced the spot size used for backside injection until the same injection results as those of front-side injection are obtained.

In order to get an estimation of the size of the silicon areas illuminated by injecting from front-side, we assume that the metal lines are organised in a regular mesh. In this circuit, there are 6 metal layers. The first two (top metal layers) have a metal line width of $12\mu m$ with a pitch of $8\mu m$. For the last four (bottom metal layers), metal line width is about $0.8\mu m$ with a $0.8\mu m$ pitch.

Thus we consider that only the first two metal layers reduce significantly the illuminated silicon area. So we assume that these areas are $8\mu m * 8\mu m$ squares considering the worst case (space between two metal lines of the same layer), the four bottom layers do not hide totally the memory cells of the circuit.

In this circuit a memory cell storing one bit of one byte has a $4.8\mu m * 5.6\mu m$ area. So the illuminated active area of the silicon is wider than a memory cell area. With a spot size of $125\mu m * 125\mu m$, the attacker can illuminate 36 memory cells in the worst case. Indeed, the attacker tries to inject a fault on a byte or bit to perform the attack.

A metal line ($12\mu m$ wide) can create a dead zone large enough to hide a flip-flop from the laser beam. This confirms the loss of manipulability seen in the experimental results.

Backside injections are performed on the circuit. The spot size is reduced until the same single-byte injection rate is obtained as from front-side injection (spot size $125\mu m * 125\mu m$). The reduction of the spot size is done using a shutter. So in order to maintain the same energy that hit the circuit, the energy of the laser beam is increased.

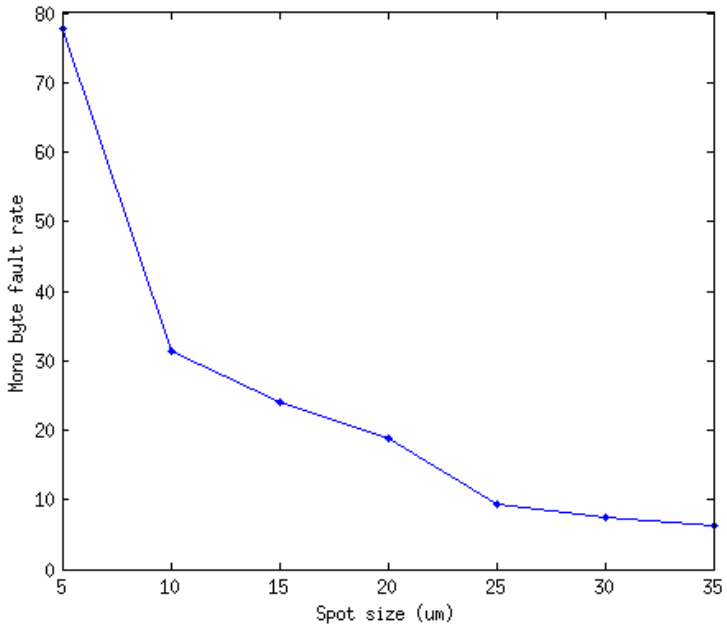

Fig. 11. Single-byte injection rate vs spot size for back side injection

The result of this experimentation is depicted in the Figure 11. For front-side injection, the single-byte injection rate was about 78% with a $125\mu m * 125\mu m$ spot size. In order to get the same rate from backside, the attacker has to reduce the spot size to around $5\mu m * 5\mu m$. This value is almost the same as the $8\mu m * 8\mu m$ given before. This shows that the reduction of the spot size is actually due to the metal interconnects.

5. LIMITATIONS AND COUNTER MEASURE

In this section, we discuss about the limitation of front-side injection and give a counter measure against it. The technology nodes used to implement the circuit has no direct impact on the experimentation presented before. The size of gate will only change the number of gates or memory cells under illumination. The smaller is the technology the more likely multiple bit faults are injected.

The real difference between the technology nodes comes from the number of metal lines layer available as depicted in Figure 1. The experiments presented here give good results for frontside injection because the number of metal lines layer used is small (6 metal layers). The more metal layers are used, the smaller the energy of the laser beam that reaches the silicon. If too many metal layers are present, the number of affected gates might go down to zero. Thus a simple counter measure against front-side laser injection is the addition of extra metal line layers. These extra lines prevent the laser

beam to reach the silicon and thus to induce faults. This shield can be either passive or active. Active shielding consists in putting extra metal lines, these lines drive alarm signals in case of removal attempt of these metal lines. Conversely in passive shielding the extra metal lines do not drive signals.

That's why, if the attacker lack of accuracy in term of laser spot size, the front-side injection can be a good option with a chip using few metal layers.

6. CONCLUSION

In this paper we presented a comparison between front-side injection and backside injection. This comparison leads to the conclusion that even with a low cost bench, i.e., with a large spot size, front-side injection allows an attacker to obtain faults potentially useful to perform a DFA attack. With such a laser bench, front side injection compares favorably with back side injection. Nevertheless, the set of useful faults obtainable through front-side injection depends from the routing of the metal lines and it cannot be controlled by the attacker.

In comparison, this kind of faults requires an expensive laser bench in order to be obtained through the backside (small spot size and accurate tune of the energy step) with the additional benefit that any fault can be potentially obtained.

At the evidence, if the circuit has a shield (metal lines added in order to protect the circuit from probes or injection) on top of it, front-side injection is no more an option of injection unless the shield is removed.

ACKNOWLEDGMENTS

This work has been supported by the contract ANR LIESSE (ANR-12-INSE-0008-01)

The authors want to thank J.B. Rigaud of ENSMSE for the design of the circuit used in this paper.

REFERENCES

Federal information processing standards publication (FIPS 197). Advanced Encryption Standard (AES), 2001.

S.S. Ali and D. Mukhopadhyay. A differential fault analysis on aes key schedule using single fault. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, pages 35–42, Sept 2011.

Subidh Ali, Debdeep Mukhopadhyay, and Michael Tunstall. Differential fault analysis of aes using a single multiple-byte fault.

Dan Boneh, RichardA. DeMillo, and RichardJ. Lipton. On the importance of checking cryptographic protocols for faults. In Walter Fumy, editor, *Advances in Cryptology EUROCRYPT 97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer Berlin Heidelberg, 1997.

Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '97, pages 513–525, London, UK, UK, 1997. Springer-Verlag.

Johannes Blomer and Jean-Pierre Seifert. Fault based cryptanalysis of the advanced encryption standard (aes). In Rebecca N. Wright, editor, *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 162–181. Springer, 2003.

V.A. Carreno, G. Choi, R.K. Iyer, and Langley Research Center. *Analog-digital simulation of transient-induced logic errors and upset susceptibility of an advanced control system*. NASA technical memorandum. National Aeronautics and Space Administration, Office of Management, Scientific and Technical Information Division, 1990.

F. Courbon, P. Loubet-Moundi, J.J.A. Fournier, and A. Tria. Increasing the efficiency of laser fault injections using fast gate level reverse engineering. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pages 60–63, May 2014.

Chen Chien-Ning and Yen Sung-Ming. Differential fault analysis on aes key schedule and some countermeasures. In *In Information Security and Privacy Proceedings of ACISP 2003*, volume 2727 of lncs. Springer-Verlag, 2003.

Hamid Choukri and Michael Tunstall. Round reduction using faults. *FDTC*, 5:13–24, 2005.

J.-M. Dutertre, S. de Castro, A. Sarafianos, N. Boher, B. Rouzeyre, M. Lisart, J. Damiens, P. Candelier, M.-L. Flottes, and G. Di Natale. Laser attacks on integrated circuits: From cmos to fd-soi. In *Design Technology of Integrated Systems In Nanoscale Era (DTIS), 2014 9th IEEE International Conference On*, pages 1–6, May 2014.

Pierre Dusart, Gilles Letourneux, and Olivier Vivolo. Differential fault analysis on a.e.s. In Jianying Zhou, Moti Yung, and Yongfei Han, editors, *ACNS*, volume 2846 of *Lecture Notes in Computer Science*, pages 293–306. Springer, 2003.

Christophe Giraud. Dfa on aes. In *Advanced Encryption Standard - AES, 4th International Conference, AES 2004*, pages 27–41. Springer, 2003.

D.H. Habing. The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. *Nuclear Science, IEEE Transactions on*, 12(5):91–100, Oct 1965.

Chong Hee Kim and Jean-Jacques Quisquater. New Differential Fault Analysis on AES Key Schedule: Two Faults are enough. In *Eighth Smart Card Research and Advanced Application IFIP Conference - CARDIS 2008*, volume 5189 of *Lecture Notes in Computer Science*, pages 48–60. Springer-Verlag, 9 2008.

David R. Martinez, Robert A. Bond, and M. Michael Vai, editors. *High performance embedded computing handbook : a systems perspective*. CRC Press, Boca Raton, 2008.

Amir-Pasha Mirbaha. *Etude de la vulnérabilité des circuits cryptographiques l'injection de fautes par laser.* PhD thesis, Microélectronique Saint-Etienne, EMSE, 2011. 2011EMSE0636.

E.D. Palik. *Handbook of Optical Constants of Solids II*. Academic Press handbook series. Academic Press, 1991.

Gilles Piret and Jean jacques Quisquater. A differential fault attack technique against spn structures, with application to the aes. In *AES and KHAZAD. CHES 2003, LNCS 2779*, pages 77–88. Springer-Verlag, 2003.

JeaHoon Park, SangJae Moon, DooHo Cho, YouSung Kang, and Ha JaeCheol. Differential fault analysis for round-reduced aes by fault injection. *ETRI Journal*, 2011.

Vincent Pouget. *Simulation expérimentale par impulsions laser ultra-courtes des effets des radiations ionisantes sur les circuits intégrés*. PhD thesis, Bordeaux 1 2000, 2000. Thèse de doctorat dirigée par Fouillat, Pascal et Sarger, Laurent Sciences physiques et de l'ingenieur. Instrumentation et mesures.

C. Roscian, J.-M. Dutertre, and A. Tria. Frontside laser fault injection on cryptosystems - application to the aes' last round -. In *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, pages 119–124, June 2013.

Bruno Robisson and Pascal Manet. Differential behavioral analysis. In *Cryptographic Hardware and Embedded Systems*, pages p413–426, Vienne, Austria, September 2007.

Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pages 2–12, London, UK, UK, 2003. Springer-Verlag.

P. Schmid. Optical absorption in heavily doped silicon. *Phys. Rev. B*, 23:5531–5536, May 1981.

C. Tarnovsky. How to reverse-engineer a satellite tv smart card. https://www.youtube.com/watch?v=tnY7UVyaFiQ, jun 2008.

Fan Wang and V.D. Agrawal. Single event upset: An embedded tutorial. In *VLSI Design, 2008. VLSID 2008. 21st International Conference on*, pages 429–434, Jan 2008.