Security evaluation at design time against optical fault injection attacks

H. Li and S. Moore

Abstract: The security of cryptographic processors is endangered by optical fault injection attacks. Transistors hit by a pulse of photons causes them to conduct transiently, thereby introducing transient logic errors, such as register value modifications, memory dumping and so on. Attackers can make use of this abnormal behaviour and extract secure information that the devices try to protect. This paper presents a simulation methodology to evaluate the security of cryptographic processors against optical fault injection attacks at design time. This simulation methodology involves exhaustively scanning the layout, incorporating the exposed cells into a circuit simulator and examining the response of the circuit in detail. Simulation performed on a test chip demonstrates that optical fault injection could harm the security of the cryptographic processors in various ways. Experiments conducted on the same test chip spot the same vulnerabilities, thus indicating the validity of the proposed simulation methodology.

1 Introduction

Secure microcontrollers and smart cards are widely used cryptographic devices for applications demanding confidentiality and integrity of sensitive information. They are also used for services requiring mutual authentication and non-repudiation of the transactions. These devices generally have an embedded cryptographic processor running cryptographic algorithms such as triple DES, AES or RSA. The algorithms encrypt data using secret keys, which should be kept safe in the devices so that attackers cannot directly read out the key value or deduce it from side-channels [1, 2, 3]. However, it is not sufficient for the cryptographic processors to withstand the above passive attacks; they should also endure attacks that inject faults into the devices and then cause exploitable abnormal behaviour. The abnormal behaviour may be data error setting part of the key to a known value, or a missed conditional jump reducing the number of rounds in a block cipher. A glitch inserted on the power or clock line was the most widely known fault injection technique [4], but many chips nowadays are designed to detect glitch attacks. Optical fault injection introduced by Skorobogatov [5] in 2002 appears to be a more powerful and dangerous attack. It involves illumination of a target transistor which causes it to conduct transiently, thereby introducing a transient logic error. Such attacks are practical as they do not require expensive equipment that is needed in invasive attacks. Invasive attacks require decapsulation and deprocessing to get direct access to the internal components of the device.

To keep cryptographic devices secure against optical fault induction attacks, effort has been made through the design of cryptographic devices. However, in common industrial practice, the security evaluation of the secure device designs is only performed after chips are manufactured. This post-manufacture analysis is time consuming, error prone and very expensive. This has driven our study of 'design-time security evaluation' which aims to exhaustively examine the response of secure processors under optical illumination through simulation, so as to assess their security level against optical fault injection attacks at design time.

The rest of the paper is organised as follows. In Section 2, we introduce the physical mechanism of laser radiation, ionisation and charge absorption. In Section 3, we present our simulation methodology that includes layout scanning, exposed node list extraction and circuit simulation that incorporates transient voltage supplies to these exposed nodes. In Section 4, we demonstrate simulation results on our test chip from which vulnerability is successfully identified and verified by experiment results. Section 5 presents a discussion of defence technologies followed by a brief conclusion in Section 6.

2 Background

Optical fault injection is not entirely new. Since semiconductor devices were invented, they were found to be sensitive to ionising radiation in the space environment, caused by protons, neutrons, alpha particles or other heavy ions [6]. Pulsed lasers were then used to simulate the effects of ionising radiation on semiconductors [7]. Depending on several factors, laser illumination may cause no observable effect, a transient disruption of circuit operation, a change of logic state, or even permanent damage to the device under test [8].

2.1 Ionisation and charge collection

It has long been known that laser ionisation and absorption is a fundamental band-to-band absorption process, where a pulsed laser with photon energy greater than the band gap of the semiconductor material excites

IEE Proceedings online no. 20055021

doi:10.1049/ip-ifs: 20055021

Paper first received: 22 July 2005 and in revised form 15 December 2005

The authors are with Computer Laboratory, University of Cambridge, JJ Thomson Avenue, Cambridge CB3 0FD, UK

E-mail: Huiyun.Li@cl.cam.ac.uk

carriers from the valence to the conduction band [9], and produces electron-hole pairs within the semiconductor material. In more detail, each absorbed photon is assumed to produce a single electron-hole pair. However, when pulsed lasers are focused to small spots, the resulting high power densities may cause additional absorption mechanisms such as two-photon absorption, which involves simultaneous absorption of two photons and thus a highly nonlinear increase in the absorption [9]. Furthermore, free-carrier absorption occurs, which does not produce ionisation but increases the energy of carriers within conduction or valence bands.

When the excited charge amount reaches the critical charge Q_{crit}, the charge necessary to flip a binary '1' to a '0' or vice-versa, a single event upset (SEU) then occurs. Device immunity is determined by its threshold linear energy transfer (LET). The threshold LET (LET_{th}) is defined as the minimum LET required to produce a voltage change (ΔV) sufficient for an SEU, then mathematically:

$$LET_{th} \propto \Delta V (= \frac{Q_{crit}}{C}) \qquad (1)$$

where C is the capacitance of the struck node.

2.2 Metal shielding effect

The previous Subsection introduces the physical mechanism of laser ionisation and charge collection in semiconductors. However, metal on top of the sensitive junctions prevents the light from penetrating these regions directly, so that has to be taken into consideration for fault injection. The metal shielding reduces the average incident energy in proportion to the surface metallisation square [10]:

$$P_e^m(x) = P_e(x)(1 - K_m) \qquad (2)$$

where $P_e(x)$ is the incident energy without metal shielding effect; $P_e^m(x)$ is the incident energy with metal shielding effect; $K_m = S_m/S$; S is the total top surface area under illumination, while S_m is the metallisation area within.

A way to deal with metal shielding in an attack is to deprocess the chip; that is, to remove layers by using wet chemical etching, plasma etching or mechanic polishing [11]. The internal components are thereby exposed to laser illumination and the metal shielding effect is eliminated. Note that this may well break the chip, especially a smart card chip when the metallisation is a defence grid or an interior bus.

Another approach to bypass the metal shielding effect is to perform the backside laser attack (from the substrate), if the test structure package allows. Beware that the wafer bottom side reflection coefficient for silicon is normally slightly larger than that of the top side refection coefficient for silicon oxide [10].

2.3 Classes of attackers

Abraham *et al.* defined attackers of IBM cryptographic products into three classes according to their expected abilities and attack strengths [12]. Following this classification, and porting it to optical fault induction attacks, we categorise the attackers into three types according to their knowledge about the system and the resolution that their laser scan equipment allows:

- *Type I (not knowing layout, targeting many transistors):* They are outsiders with moderately sophisticated tools. They do not have detailed knowledge of the layout, and can only perform moderately low resolution scans of the chip, targeting a group of neighbouring transistors; for example, by using laser directly without a microscope. A laser beam diameter typically ranges from 20 μm to 0.8 mm in size. A confocal microscope focuses its beam to a smaller spot. The focal spot diameter relates to focal length of the focusing lens, laser wavelength and diameter of the input beam. The focal spot sizes can be well below 1 μm. However, the divergence of laser beams increases as spot size decreases. A beam focused to a 1 μm spot only maintains that spot size for a distance of a few μm along the beam.
- *Type II (not knowing layout, targeting a single transistor):* They are outsiders with sophisticated tools. They do not have detailed knowledge of the layout, but can perform high resolution scans of the chip targeting individual transistors in order to determine what faults can be injected.
- *Type III (knowing layout, targeting a single transistor):* They are knowledgeable insiders, having detailed information of the layout of the chip under attack, and information about the program code. They also have access to highly sophisticated tools such as a probing-station with a high resolution focused laser allowing any single transistor to be targeted.

Type I attackers are especially dangerous, since the economic costs for training and equipment are relative low. They therefore represent the largest group of potential attackers. This threat has become increasingly relevant as transistor dimensions and supply voltages are constantly scaling down. In deep submicron technologies (gate lengths below 0.35 μm are considered to be in the deep submicron region), it is easier to introduce and propagate transient voltage disturbances as the capacitance associated with individual circuit nodes is very small, and large voltage disturbances can be produced from relatively small amounts of deposited charge. Also, due to the fast speed of deep submicron circuits, the voltage disturbances can propagate more easily. The security and economics of Type I attacks indicate that they are the most dangerous, so are the focus of this work.

Type II and Type III attackers on the other hand can conduct an attack on any transistor node during a cryptographic program execution, knowing or not knowing its specified functionality. The demanding large capital investment and detailed internal knowledge prevent most attackers falling into these categories. However, they are still of interest. Such attackers have higher capability to manipulate the circuit so more defensive effort is required from chip designers. Other than being malevolent attackers, Type II and Type III can also involve manufacturing test expertise in the IC industry. They aim to evaluate the chip products before shipment. From this perspective, security evaluation at design time helps succeed in industrial evaluation for faster time-to-market. Type II differs from Type III in that Type II attackers have no detailed knowledge about the layout of the chip. This is often the case for attackers targeting a design implemented in a 'glue-logic' approach, which is widely used in smart cards [13]. Glue-logic scrambles parts of the chip and makes it virtually impossible to distinguish functional blocks physically so as to make reverse engineering and microprobing attacks much more difficult. However, exhaustive laser scans of the chip can identify the vulnerabilities.

2.4 Modelling optical fault induction

Numerical device modelling for radiation effects has long been in existence. It can be made at a number of different levels, from physical device models through to digital abstractions.

2.4.1 Physics-based device models: Earliest work for device simulation is that of one-dimensional drift-diffusion models [14]. In a drift-diffusion (DD) model, current equations are derived from the Boltzmann transport equation considering a steady state situation and some numerical approximations for the simplicity of a 1-D geometry. These equations are discretised and solved on a mesh using finite-difference or finite-element techniques [15].

The alternative device modelling is based on hydrodynamic and energy balance (EB). It has fewer assumptions [16], but is more computationally intensive, based on five or six equations of state rather than the three as in the drift-diffusion method.

The 1-D device models based on drift-diffusion equations for carrier densities and models based on hydrodynamic and energy balance have evolved to 2-D and 3-D device modelling approaches. Many charge collection and SEU studies have been performed using these models. An early comparison of 2-D and 3-D charge-collection simulations showed that while the transient responses were qualitatively similar, quantitative differences existed in both the magnitude of the current response and the time scale over which collection was observed [17]. The comparison implies that 2-D simulations can provide basic insight whilst 3-D simulations become necessary when truly predictive results are to be obtained.

2.4.2 Circuit simulations: Although fully 3-D device simulators were first reported in the literature in the early 1980s [18], only in the last few years have fully 3-D device simulators become commercially available [8]. Even optimised for high-end workstations, a fairly large 3-D device simulation can still take a few hours. Even 2-D device models are too computationally expensive for simulating response of a large circuit to optical fault injection. Therefore, in order to exhaustively examine the effect of optical fault injection on a large circuit, we need to relate the collection of charge in individual device junctions to the changes in the circuit currents and voltages. A common circuit model for charge collection at a junction due to direct funneling or diffusion is a double-exponential, time-dependent current pulse [19], with a typical rise time on the order of tens of picoseconds and a fall time on the order of 200–300 ps [20]. The actual magnitude and time profile of the current model depends on material parameters, the ion species, the ion energy, device dimensions and the hit location relative to the junction. If the time profile (or the shape) of the collection current pulse is not important to the circuit response to the hit, then analytical current models can usually adequately describe the induced current pulse. If, however, the time profile is critical to the circuit response, more accurate models for the current pulse are necessary, such as those derived from a device simulation. In an optical fault injection attack introduced in [5], the shape of the collection current is not important to the circuit response to the attack, and a piece-wise linear (PWL) pulse can even be used to represent the induced current pulse for the purpose of simplicity.

2.4.3 Mixed device/circuit simulations: Recently, the simultaneous solution of device and circuit equations has been increasingly used. With this technique, known as mixed device/circuit simulation of SEU, the struck device is modelled in the 'device domain' using multi-dimensional device simulation, while the rest of the circuit is represented by SPICE-like compact circuit models. The two domains are tied together by the boundary conditions at contacts, and the solution to both sets of equations is rolled into one matrix solution [21, 22]. The advantage is that only the struck device is modelled in multiple dimensions, while the rest of the circuit consists of computationally efficient SPICE models. This decreases simulation times and greatly increases the complexity of the external circuitry that can be modelled. However, as circuits grow exponentially in density and complexity, comprehensive mixed device/circuit simulation is impractical.

3 Simulation methodology

The flow of designing and evaluating a test chip against optical fault injection attacks is outlined in Fig. 1. A major concern with this traditional approach is that security evaluation occurs too late in the design cycle to allow for efficient repair. The deficiencies in this approach often result in costly and frequent design re-spins. As a comparison, the procedure with evaluation in the design flow is demonstrated in Fig. 2. This design flow can spot design oversights or errors at an early stage to avoid costly silicon re-spins.

3.1 Simulation procedure

The procedure for simulating optical fault injection attacks is shown in Fig. 3. A co-simulator is used to combine a Verilog simulator (or simulators supporting

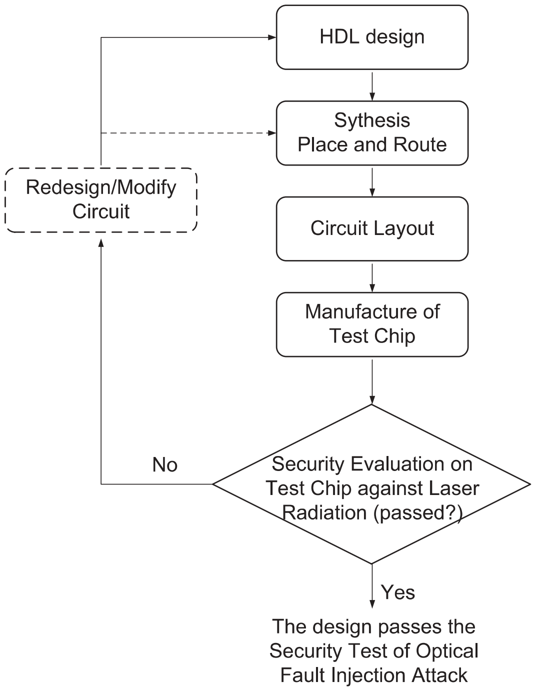

Fig. 1 *Flow chart exhibiting the iterative process to design and evaluate a test chip against optical fault injection attacks, after [23]*

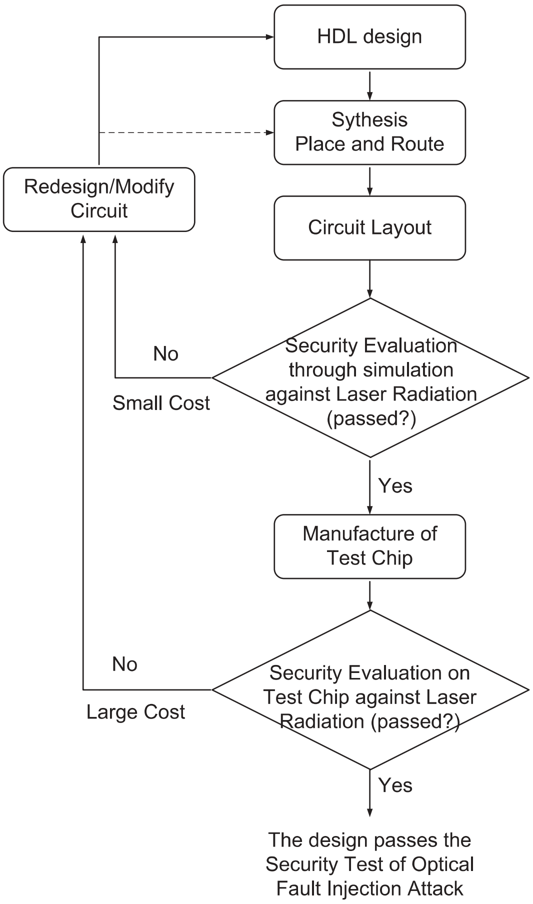

Fig. 2 *Flow chart exhibiting the iterative process to design and evaluate a test chip against optical fault injection attacks with the aid of design-time security evaluation*

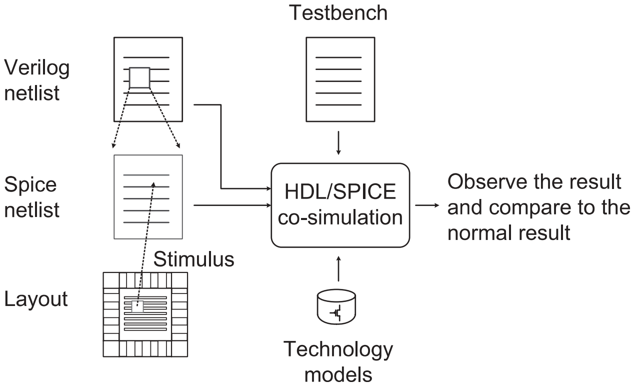

Fig. 3 *Simulation procedure for optical fault injection attack*

other hardware description languages (HDLs)) and a SPICE-like simulator. The modules of interest in the Verilog netlist are swapped out with the full transistor-level netlist. Within the transistor-level netlist, the cells under attack are instantiated into transient stimuli according to the layout scanning process. The stimuli are in essence voltage pulses supplied via tri-state buffers to the nodes under attack. The HDL/SPICE integration allows the simulation to have gate-level speed and transistor-level accuracy. The scanning process in this paper is performed with Cadence Silicon Ensemble™, and the HDL/SPICE co-simulator is chosen to be Synopsys NanoSim™ integrated with the Synopsys Verilog simulator, VCS™. Other similar and commercially available simulation environments include Cadence AMS™, Mentor Graphic ADVance MS™, Dolphin Integration SMASH™.

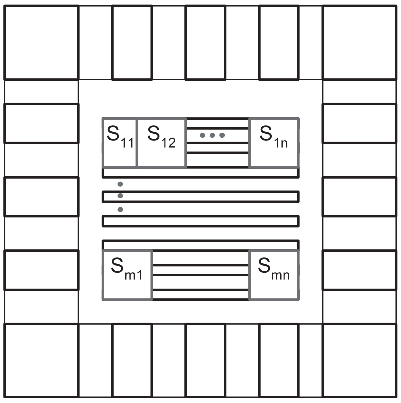

Fig. 4 *Layout scanning to extract groups of exposed cells*

The layout can be scanned with any size of laser illumination spot, which can target from a single transistor to hundreds of transistors, depending on the equipment used by the attackers as described in Section 2.3. The scans can be performed over a particular area such as the ALU, register file, or even the whole processor. Figure 4 illustrates scanning in simulation, where each scan (S_{11}, $S_{12} \ldots S_{mn}$) generates a list of logic cells under attack. For example, in a particular scan, exposed cells are listed as follows:

```
m/datapath/U355      m/datapath/fi_reg_4  m/U1490  m/U1506
m/datapath/alu/U33  m/U1458              FC_299   m/U1223
```

Among the selected cells, FC299 is a filler cell and the rest are logic cell instances. We first discard the filler cell, then check the standard cell library, mapping the logic cells to their internal nodes, especially the nodes connected to *n*-type transistors (or connect the nodes to *p*-type transistors depending on the process technologies, especially the substrate type and the well type, see Appendix for details). In addition to what may be considered a useful attack mechanism, negative effects are also possible. These include the possibility that latch-up may be induced by the generation of photocurrents in the bulk. Of less concern when using readily available infra-red and visible laser light sources is the ionisation of gate- and field-oxides due to the large band gap energy of silicon dioxide (which would require a laser with a wavelength in the UV-C range). Ionisation of this type is common when higher energy forms of radiation are absorbed. The subsequent accumulation of positive charge results in a long-term shift in transistor characteristics.

Based on the fact that optical attack is substantially more effective at turning on *n*-type transistors than their *p*-type counterparts (or more effective at turning on *p*-type transistors than *n*-type, depending on the process technologies, especially the substrate type and the well type, see Appendix for details), the laser radiation will result in one of three behaviours in a given logic gate:

- The laser radiation is not strong enough to cause either the *n*-type or the *p*-type CMOS transistors to conduct, so no state change occurs at the logic cell output.
- The laser radiation switches on the *n*-type but not *p*-type transistors, so abnormal behaviour may occur.

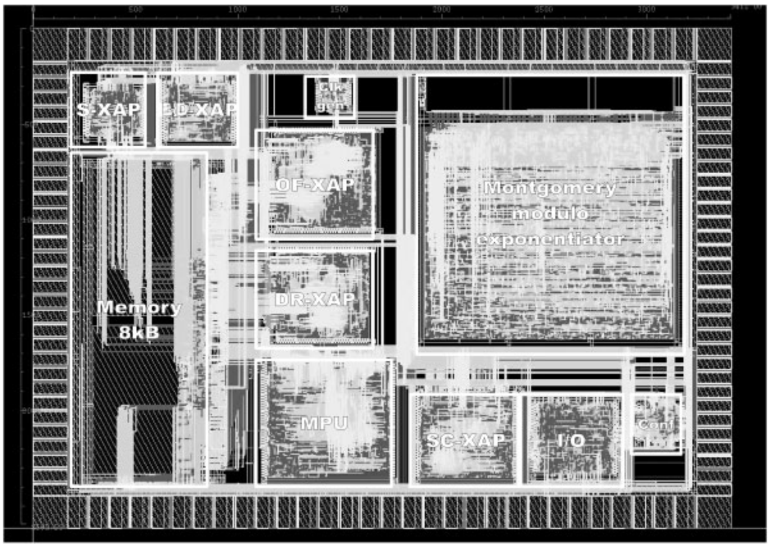

Fig. 5 *The microprocessor (S-XAP) on the chip is under simulation test*

- The laser radiation is strong enough to cause both *n*-type and *p*-type CMOS transistors to conduct in a logic gate. This results in large leakage current or even a strong VDD-to-GND short circuit, which may damage the circuit eventually if no current limit protection is provided.

Of the three behaviours, only the second is considered as a successful attack in respect of security sabotage, and is therefore the focus of this simulation methodology. This allows us to simply focus on *n*-type transistors in the simulation of security evaluation targeting Type I attackers. Apparently, in the case where the laser can target a single *p*-type transistor and successfully switch it on, the attacker is able to manipulate the circuit more capably. This situation falls into the category of Type II and III attackers and requires layout scans over every single transistor.

After obtaining the list of exposed cells for each scan, we then supply the internal nodes with transient voltage pulses via tri-state buffers. The `enable` signals of the tri-state buffers are synchronised with the target instruction execution during a cryptographic program operation. Then those output nodes connected to the voltage supplies are transiently brought down as if the transistors were conducted. Compared to the current pulses used in the existing modelling techniques introduced in Section 2.4, these voltage pulses can be easily implemented in the simulation at the circuit level as external stimuli, rather than being dealt with at the device level. The co-simulation shown in Fig. 3 integrates the voltage pulses, attacked nodes and attacked cells in SPICE, whilst the rest of the circuit remains in Verilog. Analysing the response and comparing it to that of the normal operation, we can evaluate the security of the circuit design against optical fault injection attacks. If it fails, modification or even redesign of the circuit is required as demonstrated in Fig. 2. If it passes, then designers can continue to have the test chip manufactured.

4 Results

4.1 Optical attack simulation results

Simulation of optical fault injection attacks has been carried out on a test chip, fabricated in UMC 0.18 μm 6 metal layer CMOS process as part of the G3Card project [24, 25]. The substrate/well formation is a *p*-substrate with twin-well (according to the Appendix, *n*-type transistors are easier to switched on in this technology, so are simulated). Figure 5 shows a picture of the test chip which contains five 16-bit microcontroller processors with different design styles. This paper addresses the synchronous processor (S-XAP) on the top left corner.

```
...

ld      ah,@(1,x)   ; load first argument
nop
nop
nop
xor     ah,@(2,x)   ; XOR operation
nop
nop
nop
st      ah,@(3,x)   ; save result
...
```

Fig. 6 *Fragment of the instruction program used for the evaluation*

The aim of the test is to exhaustively examine the ALU and the decoder to determine if it is susceptible to optical fault injection attacks. We target simple instructions (e.g. XOR (exclusive OR), shift, load, store etc.) which can give a good indication of how the hardware reacts to operations of cryptographic algorithms. The fragment of an instruction program, shown in Fig. 6, is used for the evaluation, where the processor loads the first argument to register AH, XOR it with the second argument from memory, then saves the result back to memory. The laser attack is synchronised with the

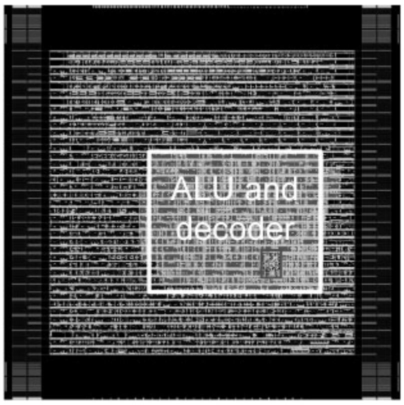

Fig. 7 *Screen shot of scanning procedure over the layout ALU and decoder of processor S-XAP*

XOR operation, meaning the transient voltage sources will be activated at this moment in simulation.

The simulation procedure is implemented as introduced in Section 3. We scan the ALU and the decoder of processor S-XAP with a scanning square size of about 300 μm^2, to cover 10–15 logic cells. Figure 7 shows the screen-shot of the scanning procedure. The spot is moved within the area horizontally each time by one cell width (about 4 μm), then vertically by one cell height (about 6 μm). The scanning produces 120 lists of cells. For each list, we connect the internal nodes to transient voltage sources and incorporate the stimuli into the SPICE netlist. Then the Verilog/HSPICE co-simulation running the above simple instruction program is performed to examine the circuit response during each optical attack.

The exhaustive examination of the 120 simulation runs shows different results:

1. The processor results in deadlock in many cases, which is desirable in terms of security, provided this does not leak secret information.
2. Some other cases show normal program execution. This implies the introduced fault may be part of the ‘don’t care’ state of the subsequent operation of the circuit [8].
3. Two failures are also revealed:

(a) The first disrupts the XOR operation by changing the value in the AH register.

(b) The second failure causes a memory dump. Instead of executing an XOR operation, the processor keeps reading the contents of the whole memory. We suspect the memory dump occurred when the microprocessor decoder was struck in the test, which resulted the opcode being modified from ‘1101’ (standing for XOR) to ‘0001’ (standing for LOAD).

Modifying register values implicates setting part of the key to a known value becomes feasible to the attackers. Whilst dumping memory is dangerous to designs implemented with an architecture where a single storage structure is used to hold both instructions and data. If the memory contains passwords and decryption keys, then by carefully analysing the dumped memory, one can break the cryptographic device. In contrast, a design implemented with Harvard architecture [26] could offer better protection against microprobing attacks, as it uses physically separate storage for instructions and data. The same trick applied to a Harvard microcontroller would reveal only the program code, whereas the data memory containing sensitive information will not be available.

It takes about 10 min to run the scanning process (containing 120 scans) with Cadence Silicon Ensemble™. Then it takes about 4 h to complete the 120 runs of HDL/SPICE co-simulation, with each run to have 14 000 transistors simulated in Synopsys NanoSim™ and the rest tens of logic gates simulated in Synopsys VCS™. All the simulation work is done on a 1.6 GHz AMD Athlon processor with a 2 GB memory.

4.2 Experimental Results

A laser fault injection experiment was conducted by Gemplus® on the same test chip to provide a side-by-side comparison [25]. The test chip was mounted in ZIF (zero-insertion force) socket, which was mounted on the bottom side of the test board, thus easing access for the laser attack. The laser is synchronised with the executed program (same as the piece used in the simulation) via an interrupt signal from a particular I/O pin, as shown in Fig. 8.

The experiments reveal that not every portion of the processor is sensitive to the laser. When there is an actual effect, the processor goes into a failure state in most cases, and the chip has to be reset in order to reload the program. By shooting the laser on the ALU of the processor, we finally obtained effects like modification of the result of XOR operation, which agrees with the first type of failure discovered through simulation. We also succeeded in dumping the data memory in processor S-XAP by shooting the laser on the decoder, in agreement with the second type of failure discovered through simulation.

5 Defences

The vulnerability of the cryptographic processors in optical fault injection attacks may be countered at the system level or the circuit level. System-level defences include the use of error detection and correction (EDAC) circuitry to monitor and correct errors [8]. This approach requires that extra bits of information be stored with the data to reconstruct the original data in the event of an upset. System overhead can be large, but this is sometimes the only method available if relatively susceptible parts must be used. Another important technique is triple-modular redundancy (TMR), which can be implemented at the circuit, system board or module level. Defensive techniques in combinational logic can involve redundant data paths and careful selection of circuit types. An example is the avoidance of all dynamic logic [8], because dynamic logic is highly vulnerable to optical fault injection attacks due to its highly charge-sensitive mode of operation. Security may be further improved by including small optical tamper sensors within each standard cell [25]. They force the generation of error signal when illuminated. These sensors, constructed from one or two transistors, would normally play no part in normal circuit behaviour (only adding a small amount of capacitance). The number of sensors could be adjusted dependent upon the likelihood of the small laser spot size. All the above defences can be used in single or combination in the circuit design and their effect can be evaluated by the proposed simulation methodology.

There are other defensive approaches by means of chip coating. For example, top-layer metal shielding can reflect light and help make an optical attack more

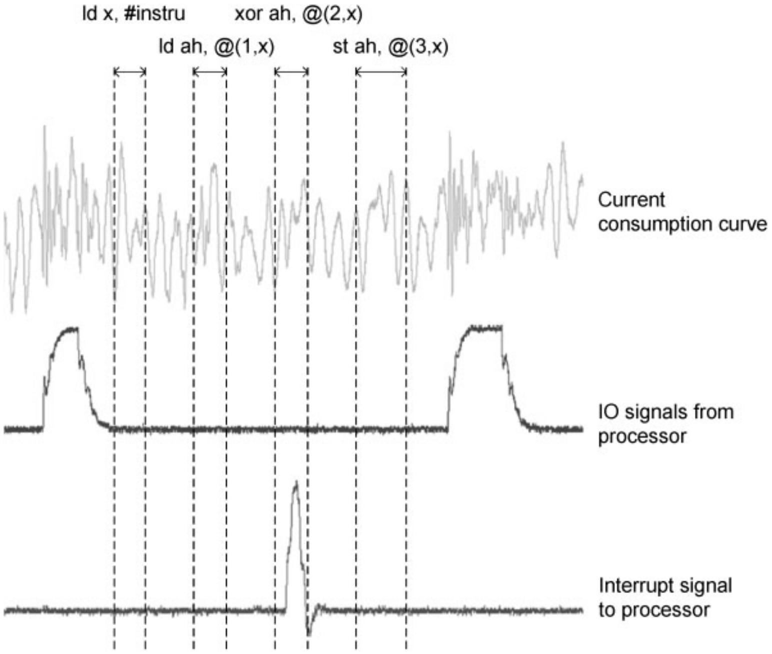

Fig. 8 *Curves for monitoring activity at laser attack, with the interrupt signal synchronised to the XOR logic operation*

difficult. Sensors measuring environment variables such as light can also be used to disable the chip as soon as out-off-bound conditions are detected. The effect from coating defences can not be simulated by the proposed simulation methodology. It should be evaluated by post-manufacturing test.

6 Conclusions

A simulation methodology has been proposed to evaluate the security of cryptographic processors against optical fault injection attacks at design time. This simulation methodology involves exhaustive scans over the layout with any virtual laser spot size according to the attack scenario. Cells under illumination are identified and simulated in SPICE with additional voltage spikes at appropriate nodes which mimic the attack. This SPICE model is co-simulated with the rest of the system represented in Verilog.

Simulation performed on our test chip has demonstrated that the optical fault injection could modify the value stored in registers, so that setting part of the key to a known value becomes feasible to the attackers. Attacks on other area also caused a data memory dump, which can be extremely dangerous if the memory contains passwords and decryption keys. Experimental results revealed the same kind of weaknesses, which gives us the confidence in the proposed simulation methodology.

The proposed simulation methodology can be easily employed in the framework of an integrated circuit design flow. It can spot design overlook/error at an early stage, helping avoid costly silicon re-spins. With this simulation methodology, we are able to move one step closer to a complete security-aware design flow for cryptographic processors.

7 References

1 Kocher, P.: ‘Cryptanalysis of Diffe-Hellman, RSA, DSS, and other cryptosystems using timing attacks’. Proc. 15th International Advances in Cryptology Conference – CRYPTO ’95, pp. 171–183, 1995

2 Kocher, P., Jaffe, J., and Jun, B.: ‘Differential power analysis’. Proc. 19th International Advances in Cryptology Conference – CRYPTO ’99, pp. 388–397, 1999

3 Quisquater, J-J., and Samyde, D.: ‘ElectroMagnetic Analysis (EMA): Measures and counter-measures for smart cards’, In *E-smart*, pp. 200–210, 2001

4 Anderson, R., and Kuhn, M.: ‘Tamper resistance - a cautionary note’. 2nd USENIX Workship on Electronic Commerce Proceedings, pp. 1–11, 1996

5 Skorobogatov, S., and Anderson, R.: ‘Optical fault induction attacks’. Proc. of Cryptographic Hardware and Embedded Systems - CHES2002, pp. 2–12, 2002

6 Binder, D., Smith, E.C., and Holman, A.B.: ‘Satellite anomalies from galactic cosmic rays’, 1975, **22**, pp. 2675–2680

7 Buchner, S.: ‘Laser simulation of single-event upsets’, **34**, 1987

8 Dodd, P.E., and Massengill, L.W.: ‘Basic mechanisms and modeling of single-event upset in digital microelectronics’, 2003, **50**, pp. 583–602

9 Johnston, A.H.: ‘Charge generation and collection in *p-n* junctions excited with pulsed infrared lasers’, 1993, **40**, pp. 1694–1702

10 Nikiforov, A.Y., Chumakov, A.I., and Skorobogatov, P.K.: ‘CMOS IC’s transient radiation effects investigations, models verification and parameter extraction with the test structures laser simulation tests’. Proc. of the 1996 IEEE International Conference on Microelectronic Test Structures, 1996, pp. 253–258

11 Wagner, L.C.: *‘Failure Analysis of Integrated Circuits: Tools and Techniques’,* Kluwer Academic Publishers, 1999

12 Abraham, D.G., Dolan, G.M., Double, G.P., and Stevens, J.V.: ‘Transaction security system’, 1991, **30**, pp. 206–229

13 Philips Semiconductors Leads Industry with Smart Card Security Benchmark. Product news from philips semiconductors. http://www.semiconductors.philips.com/news/content/file_354.html, October, 1998.

14 Gwyn, C.W., Scharfetter, D.L., and Wirth, J.L.: ‘The analysis of radiation effects in semiconductor junction devices’, 1967, **15**, pp. 153–169

15 Selberherr, S.: ‘Analysis and Simulation of Semiconductor Devices’, Vienna, Austria: Springer-Verlag, 1984

16 Lundstrom, M.S.: ‘Fundamentals of Carrier Transport’, Addison-Wesley Publishing Company, 1990

17 Kreskovsky, J.P., and Grubin, H.L.: ‘Numerical simulation of charge collection in two- and three-dimensional silicon diodes – a comparison’, 1986, **29**, pp. 505–518

18 Buturla, E.M., Cottrell, P.E., Grossman, B.M., and Salsburg, K.A.: ‘Finite-element analysis of semiconductor devices: The fielday program’, 1981, **25**, pp. 218–231

19 Messenger, G.C.: ‘Collection of charge on junction nodes from ion tracks’, 1982, **29**, pp. 2024–2031

20 Massengill, L.W.: ‘SEU modeling and prediction techniques’, IEEE NSREC Short Course, 1993, pp. III–1–III–93

21 Rollins, J.G. and Choma, J. Jr.: 'Mixed-mode pisces-spice coupled circuit and device solver', 1988, **7**, pp. 862–867

22 Mayaram, K., Chern, J.H., and Yang, P.: 'Algorithms for transient threedimensional mixed-level circuit and device simulation', 1993, **12**, pp. 1726–1733

23 McMorrow, D., Melinger, J.S., and Buchner, S.: 'Application of a pulsed laser for evaluation and optimization of SEU-Hard designs', 2000, **47**, pp. 559–565

24 G3Card Consortium. 3rd generation smart card project. http://www.g3card.org/.

25 Fournier, J., Moore, S., Li, H., Mullins, R., and Taylor, G.: 'Security evaluation of asynchronous circuits'. Proc. of Cryptographic Hardware and Embedded Systems - CHES2003, pp. 137–151, 2003

26 The free dictionary encyclopedia: Harvard architecture. http://encyclopedia.thefreedictionary.com/harvard\%20architecture.

27 Dodd, P.E., Sexton, F.W., Hash, G.L., Shaneyfelt, M.R., Draper, B.L., Farino, A.J., and Flores, R.S.: 'Impact of technology trends on SEU in CMOS SRAMS', 1996, **43**, pp. 2797–2804

8 Appendix

When laser illumination strikes a microelectronic device, the most sensitive regions are usually the reverse-biased *p*/*n* junction. The high field present in a reverse-biased junction depletion region can very efficiently collect the ionised charge through drift processes, leading to a transient current at the junction contact. An important consideration for charge collection is whether the junction is located inside a well or in the substrate.

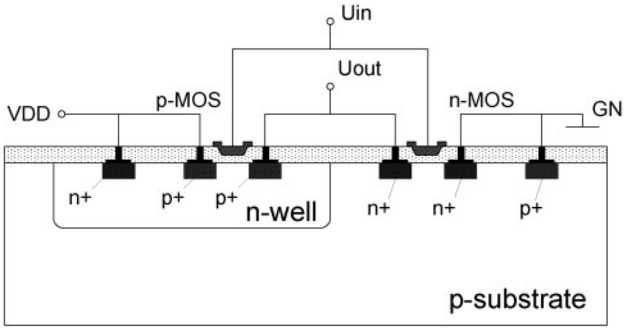

Fig. 9 *Cross-section of a CMOS inverter in a p-substrate + n-well process*

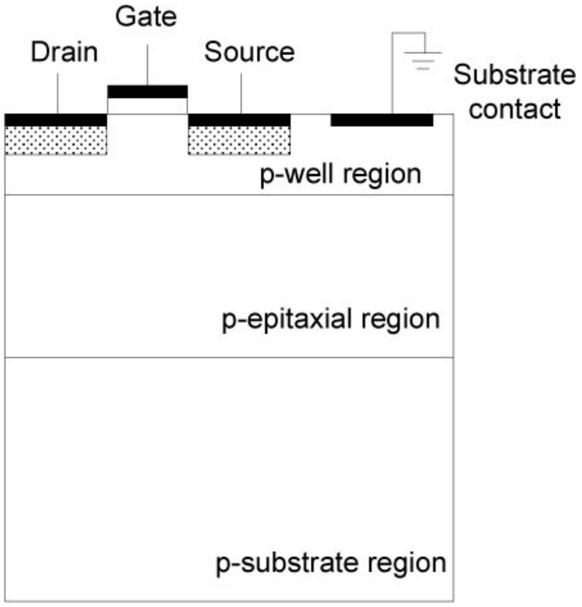

Fig. 10 *Cross-section of a n-MOS in p-well + p-epitaxial + p-substrate process[27]*

Figure 9 shows a cross-section of a CMOS inverter in a *p*-substrate with *n*-well process. There are other substrate and well types, including:

- *p*-substrate(*n*-MOS) + *n*-well(*p*-MOS)
- *p*-substrate + twin-well (*p*-MOS in *n*-well and *n*-MOS in *p*-well)
- *n*-substrate(*p*-MOS) + *p*-well(*n*-MOS)
- *n*-substrate + twin-well (*p*-MOS in *n*-well and *n*-MOS in *p*-well)

As technologies are constantly scaling down, inside-the-well strikes are particularly interesting because of shunt and bipolar effects that can occur in multilayer structures [27]. Figure 10 demonstrates an *n*-MOS transistor implemented in a *p*-substrate with *p*-epitaxial and *p*-well process. As a SEU transient proceeds, holes deposited in the *p*-well are collected at the *p*-substrate contact, raising the well potential and leading to injection of electrons by the source. This results in the turn-on of the horizontal *n*-source/*p*-well/*n*-drain (emitter/base/collector) parasitic bipolar. The movement of the carriers is illustrated in Fig. 11 [27].

Dodd *et al.* [27] studies the gate-length scaling trend in inside-the-well strikes for both *p*- and *n*-substrate technologies (Sandia 2 μm, 1 μm and 0.5 μm). Figure 12 shows the simulated SEU threshold scaling trend of OFF transistors fabricated on *n*-substrate. The upset threshold of the inside-the-well strikes decreases at a much faster rate than that of outside-the-well strikes. Figure 13 displays the scaling trend of OFF transistors fabricated on a *p*-substrate. Similar trend exists except that the inside-the-well (*p*-MOS) strike starts out much

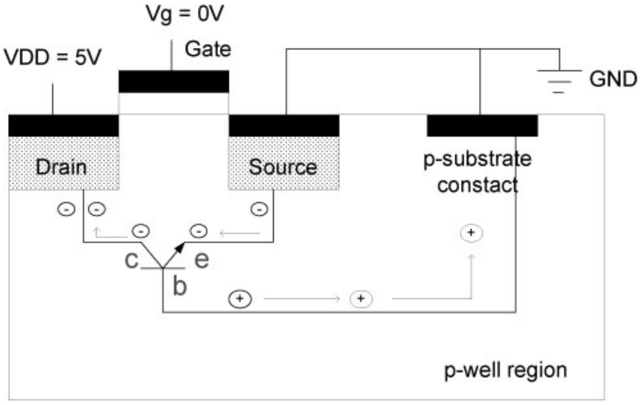

Fig. 11 *The movement of carriers in the parasitic bipolar [27]*

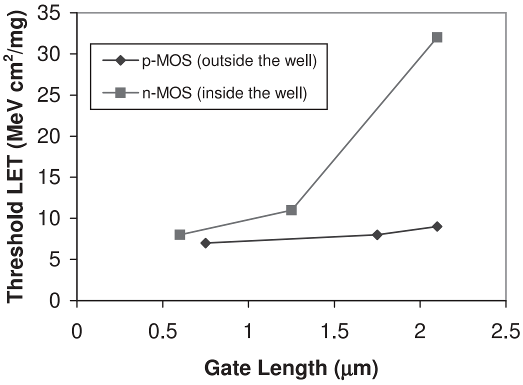

Fig. 12 *Simulated threshold LET vs. gate length in n-substrate technologies, after [27]*

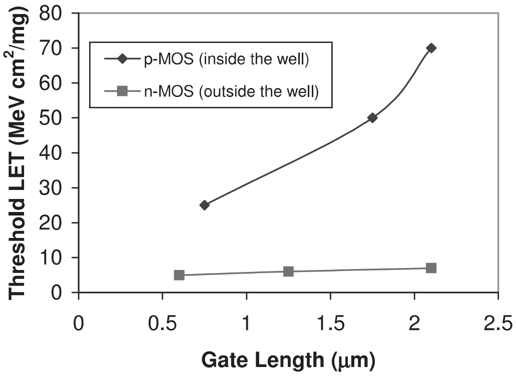

Fig. 13 *Simulated threshold LET vs. gate length in p-substrate technologies, after [27]*

harder (much higher LET threshold than the *n*-MOS counterpart). The weaker bipolar effect for the *p*-well case is simply because in *p*-well, the parasitic bipolar are pnp rather npn. For identical structures, a pnp bipolar will have lower current gain (~1/3) than an equivalent npn due to the lower mobility of holes compared to electrons.

According to the trend shown in Figs. 12 and 13, a rule of thumb is

- for *p*-substrate, either *p*-substrate + *n*-well or *p*-substrate + twin-well: *n*-MOS transistors are easier to switch on
- for *n*-substrate, either *n*-substrate + *p*-well or *n*-substrate + twin-well: above 1 μm technology node, *p*-MOS transistors are easier to switch on; below 1 μm technology, device simulation or experiment is required to determine the minimum upset LET for *n*- and *p*-MOS transistors respectively.

With silicon-on-insulator, the situation will be different but this is not discussed in this paper as all microcontrollers and smart cards nowadays use bulk silicon manufacturing technologies.