Using Voters May Lead to Secret Leakage

Jan Bělohoubek, Petr Fišer, Jan Schmidt
Faculty of Information Technology
Czech Technical University in Prague
Prague, Czech Republic
{jan.belohoubek, petr.fiser, jan.schmidt}@fit.cvut.cz

***Abstract*—The security of many digital devices strongly depends on a secret value stored in them. To mitigate security threats, high protection of such a value must be provided. Many attacks against (cryptographic) hardware as well as attack countermeasures were presented recently. As new attacks are invented continuously, it is important to analyze even potential threats to mitigate device vulnerability during its lifetime. In this paper, we report a novel voter-related vulnerability, which can be potentially misused to compromise the secret value stored in an embedded device.**

I. Introduction

Digital devices already became a natural part of human lives and they still continue to penetrate into new areas [1], [2]. The vital development in this area is driven by technology scaling opens novel reliability-related issues [3], [4]. Further, the security requirements are still rising with the number of digital devices deployed into critical application areas [2], [5]. This is the main reason why the research of security-reliability interplay is important. The secondary reason for this kind of research is that fault-tolerant approaches can be used to prevent certain security threats [6], [7].

In this paper we report a novel vulnerability originating in combinational logic, particularly in conventional voters. Hardware redundancy (e.g., triplication) with voters is used in digital designs to increase fault-tolerance or even to mitigate certain *fault attacks (FA)* [6], [8], [9], [10], [11].

Let us suppose that an invasive attack (e.g., optical – laser – attack) is directed against a single-bit voter logic with error-free inputs (that is, all-0 or all-1). In such a case, the voter's *fingerprint* in the side channel (e.g., power trace) will differ depending on the voter state.

If the voter input is classified as a secret value, the presented vulnerability escalates into a real threat – the secret value may be compromised by *combined attack mechanism* [12]: an *optical attack* combined with *simple power analysis*. A successful attack requires precise control over an attack location, in particular, the laser beam positioning.

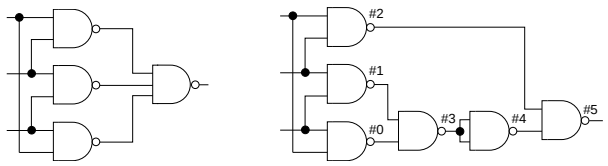
The requirement of a precise laser beam location control and also knowledge of circuit layout may appear strong, however, there is a long history of using lasers for diagnostic purposes in digital design [13] and since the vulnerable part (the voter) is large enough, its precise targeting is completely possible and proved [8], [14], [15], [16], [17]. For any serious worst case design security evaluation, one must assume a *white box model*: the potential attacker with knowledge of the circuit architecture. Anything else is called *Security by Obscurity*.

II. Voter Properties Enabling Secret Leakage

When analyzing the circuit security, it may be unclear, why a circuit like a voter deserves special attention, compared to the rest of the combinational logic. In fact, it is the voter's dedicated structure, mission, and location in the circuit, which makes it the ideal target for a potential attacker, as explained below.

The majority voter is a compact digital circuit. In a fault-free environment, all voter inputs are equal and the voter's output value matches the voter inputs. If any of the voter inputs is affected by a fault, the voter masks the fault and produces the majority of inputs at its output (the error-free output).

For the purpose of this paper and for simplicity, we use the conventional 3-input majority voter (TMR) design as shown in Figure 1a mapped to 2-input NAND gates (Figure 1b).



(a) Conventional NAND-based majority voter

(b) Majority voter mapped to 2-input NAND gates

Fig. 1. 3-input NAND-based majority voter

A conventional voter has the number of properties, which make it simpler to extract the voter's input value by combining fault injection and side channel emission measurement:

(i) Skorobogatov has shown, that reading individual bits from digital devices is possible when transistor sizes are large enough to allow precise laser beam localization on a single transistor [18]. However, transistor sizes in circuits manufactured in a recent CMOS process are too small. In contrast, the voter size for conventional technologies, e.g. for 180nm (and also for sub-100nm processes), is large enough for precise fault-injection into the voter area only [8]: **the physical fault injection localization is possible**, even with relatively cheap equipment [17], [18].

(ii) The voter depends on a single logic value represented by multiple bits or wires: **fault injection affecting a single logical bit value only is possible**. The voter may be understood as a physical amplifier (to a side channel) of a single logic value at all its inputs.

(iii) The majority voter is designed to mask errors, thus if a subpart of the voter is affected by fault injection, the voter's

output tends to remain stable, limiting the fault-injection effect propagation: **fault injection side-effects tend to be localized to the voter area only** – fault propagation is suppressed.

The result of properties (i), (ii), and (iii) is as follows: if a voter is under attack, while the activity of the digital circuit is suppressed (stable clock signal and inputs), the side channel emissions of the *circuit under attack* are influenced *only* by a single logic value at all the voter inputs.

III. Photoelectric Laser Stimulation (PLS) Modeling

As a laser beam can be used for fault injection with precise location control [8], [19], it is a clear candidate for in-voter fault injection. We decided to use the electrical simulation of the circuit under a precise fault injection to demonstrate the vulnerability severity.

The principle behind the laser fault injection is a *photoelectric effect*. The laser beam passing through silicon creates, as a result of energy absorption, electron-hole pairs along its path. In *Space Charge Regions (SCR)* of PN junctions, the generated electron-hole pairs are separated by the internal electric field, generating the *Optical Beam Induced Current* [14], [20].

To perform accurate electrical simulation of the fault injection process, accurate models of the transistor under laser stimulation are required. Sarafianos et al. published a series of papers related to *Photoelectric Laser Stimulation* (PLS), incrementally describing the electrical model of the pulsed photoelectric laser stimulation of an NMOS and PMOS respectively, e.g., [14], [15], [16].

In following paragraphs, the basic equations related to transistor models under PLS are presented. The in-depth description can be found in Sarafianos et al., e.g. [14], [15], [16].

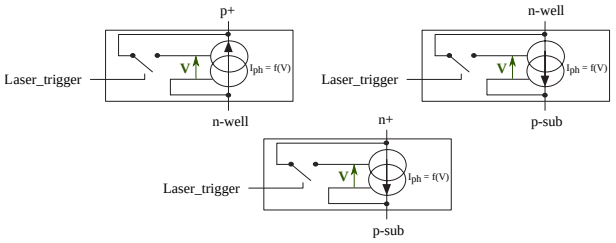


Fig. 2. Current sources representing photocurrent induced in certain PN junctions as used in SPICE model [14], [15], [16]. `Laser_trigger` signal is used to turn the laser in the simulation environment on

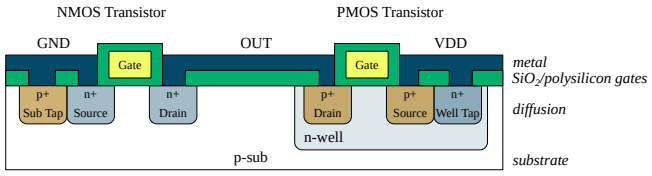


Fig. 3. CMOS cross-section showing the modeled PN junctions

The modeled PN junctions – *p+/n-well*, *n+/p-sub* and *p-sub/n-well* – are shown in Figure 3 (for CMOS technology details refer to, e.g., [21]). The photocurrent induced by a laser beam in any PN junction was simulated by a voltage controlled current source – see Figure 2. The current amplitude is expressed by equation (1).

$$I_{laser} = (a \cdot V + b) \cdot \rho \cdot S, \tag{1}$$

where S is the surface of the sensitive zone ($[\mu m^2]$), a and b are fitting parameters expressing the laser power and technology parameters, V is the reversed bias voltage of the PN junction under laser illumination. Parameters a and b express the dependency on the laser power ($[mW]$) by using fitting parameters [14]:

$$a = p \cdot P_{laser}^2 + q \cdot P_{laser} \tag{2}$$

$$b = s \cdot P_{laser} \tag{3}$$

The parameter ρ is used to take into account the distance between the PN junction and the laser spot, as expressed in equation 4.

$$\rho = \beta \cdot exp(-\frac{d^2}{c_1}) + \gamma \cdot exp(-\frac{d^2}{c_2}), \tag{4}$$

where β and γ are the fitting parameters [14] and c_1 and c_2 express the influence of optical lens.

Note that the equations above contain parameters specific for each PN junction: the *p-sub/n-well* junction use different parameters to express the photocurrent than *p+/n-well* or *p-sub/n+*. The parameters are reported in the referenced papers.

IV. Technology and Experiment Replicability

Sarafianos et al. [14], [15], [16] used the STM 90nm technology for their experiments. As the STM's technology details (SPICE models, cell libraries), are not publicly available, we decided to mount their models to publicly available technology node to increase the experiment replicability.

For simulations, we used primarily TSMC models for 180nm technology. The TSMC 180nm technology advantage is the availability of open-source standard cell library and SPICE models provided by Oklahoma State University (OSU)[1]. Thanks the availability of open-source SPICE models and standard cell library, it is possible to perform the simulation of a manufacturable circuit layout.

First of all, we replicated SPICE models and simulations presented by Sarafianos et al. by using TSMC transistor models[2]. By comparing our simulation outcomes with Sarafianos et al., we have confirmed that using different transistor models does not lead to unrealistic results. As the model parameters used for experiments in this paper were compiled from a number of publications, these are available for further experiments[3].

For real layout simulation, shrinking transistor sizes in the model are necessary. For scaling to lower transistor dimensions, we simply used equation 1 following Roscian and Sarafianos et al. [19]. We used PN junction sizes coming from the layout under simulation.

[1] https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS

[2] Note, that all parasitic parameters were not set precisely in our models, thus transients are poorly represented in simulation outputs

[3] http://ddd.fit.cvut.cz/prj/MajVoterPLS

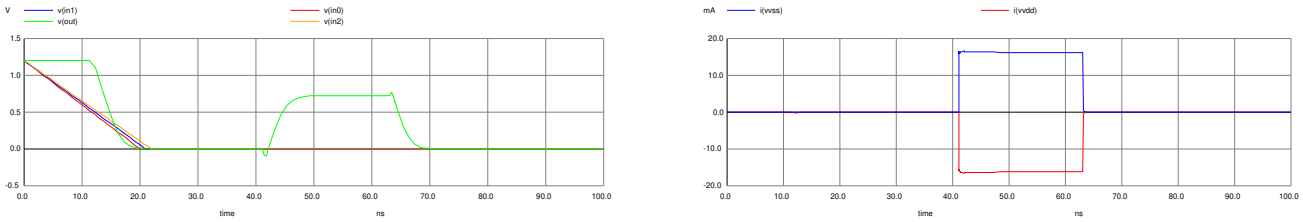


Fig. 4. Voltage and current waveforms –the output of ngSPICE simulation. The wider laser beam (strongly influencing 3 central NAND gates) is directed to the middle of the voter for 20ns starting at t = 40ns; for all-0 voter inputs, the induced current is 16.2 mA; for all-1 inputs, the current peak is ≈1mA lower

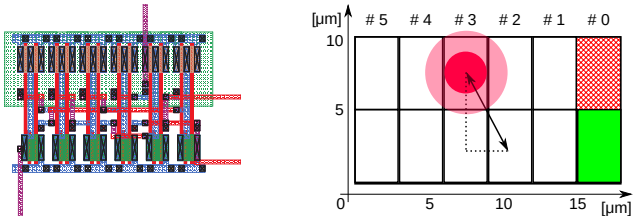
A. *Voter Layout Synthesis*

For the experiment replicability reasons, we choose a completely open toolchain to synthesize the voter layout for experiments. The used available open *digital synthesis flow* is called *Qflow*[4]. Qflow incorporates well known open-source tools for different digital flow stages, notably *GrayWolf*[5] for place&route and *Magic*[6] as a VLSI layout tool.

Figure 5a presents the resulting voter layout in the TSMC 180nm technology (provided by OSU), which is distributed with Qflow. The SPICE netlist of the circuit layout (generated by Magic) was used for simulation, while the layout itself was used to obtain dimensions of PN junction areas.

V. Experimental Evaluation

The area of the voter produced in TSMC 180nm technology by Qflow was 10 x 18μm. For experimental purposes, this area was divided into 12 rectangular areas (5 x 3μm), each containing half of a NAND gate (PMOS (n-well) or NMOS part).



(a) Voter layout produced by *Magic*

(b) PMOS – top/red and NMOS – bottom/green and laser position calculation

Fig. 5. Voter layout (a) and voter area partitioning (b). Gate numbers (#0 – #5) are used for reference

In our experimental setup, we assume that a 1250mW laser beam is focused to one of the 12 rectangular areas affecting all PN junctions in this area directly (the distance is equal to 0) – see Equation (4) – the beam distance for PN junctions in other 11 areas is computed based on the actual laser beam position (Figure 5b). To be as close to our assumptions as possible, we choose equation parameters for 20X lens, which results in 3.25μm laser beam diameter, as reported in [16].

In the SPICE netlist produced by Qflow, the PMOS/NMOS transistor models were replaced by the sub-circuit representing the transistor under PLS, while preserving the geometry of the layout and other parameters like parasitics originating in the circuit layout. For the purpose of the simulation, the voter output is connected to a 10fF capacitance node.

For the final netlist, we performed the transient simulation with VDD at 1.2V and room temperature in *ngSPICE*[7] for all 12 rectangular areas twice – for all-1 and for all-0 voter input. VDD and VSS current traces and gate-output voltage waveforms were recorded – as in Figure 4.

The average values of current peaks induced by the laser beam are shown in Figure 6a. For the NMOS part, the current is lower than for the PMOS part. This is caused by the presence of two PN junctions in the PMOS transistor (n-well/p-sub and P+/n-well), not by any difference the in parallel/serial geometry. The cause was confirmed by modified netlist resimulation.

The simulation has additionally shown (Figure 6a) that the induced current reaches its maximum, as the laser beam moves to the center of the circuit, where it influences most of the circuit area.

The most important lecture however comes from the difference for all-1 and all-0 input cases as shown in Figure 6b: the current peak for all-0 voter inputs is, independently of the laser beam position, significantly higher than the current peak for all-1 inputs, thus allowing determination of the voter state from the power trace.

Last but not least: we extended the diameter of the laser while fixing the laser beam position to the center of the majority voter. The power traces obtained from such simulation provided about 1mA difference in power peaks allowing to distinguish both voter states – see Figure 4.

VI. Discussion

The current peak difference for all laser positions in Section V is in the order of hundreds of micro amps or even in milliamps, which **supports the voter vulnerability statement.**

The laser beam may cause the voltage drop at affected gate outputs, which is amplified by the subsequent logic. Thanks to the circuit nature, the absolute value of the induced current is lower for gates closer to the voter output (Figure 6a), but this behavior will differ in real circuits, where the voter output is connected to the subsequent logic.

The feasibility of the measurement in practice may be limited due to the presence of additional sources of photocurrent coming from voter-surrounding logic or simply by noise.

[4]http://opencircuitdesign.com/

[5]https://github.com/rubund/graywolf

[6]http://opencircuitdesign.com/magic/

[7]http://ngspice.sourceforge.net/

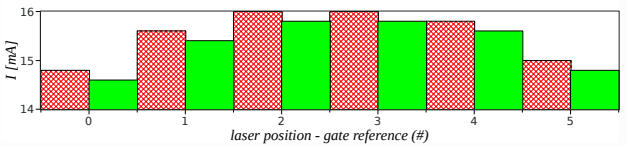


Fig. 6. (a) The current peaks induced by a PLS in a voter circuit depending on the laser beam position: average for voter all-1 and all-0 inputs is shown

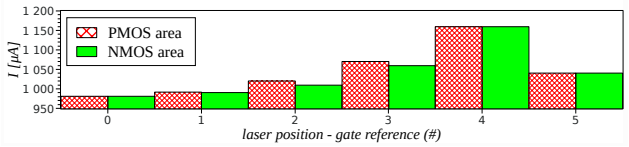


Fig. 6. (b) The difference in current peaks induced by PLS targeting the voter with all-1 and all-0 inputs depending on the laser beam position

Although the simulations were currently not confirmed by real measurements, we believe that due to the significant difference in simulated currents, the presented threat requires attention.

Skorobogatov and Anderson have shown, that it is possible to perform optical attacks with very cheap equipment [17]. However, environment stability and replicability of the experiment may require relative costly equipment.

If the voter occupies a compact space, it is simple to target the laser beam on the voter logic only (even for sub-100nm process). In the case where the voter logic is dissolved in the other logic, precise fault injection will be more challenging, but still possible (for above 100nm process) – the fault injection into the voter subpart (gate) may still disclose the voter state.

VII. Conclusions and Future Work

In this paper, we reported a novel potential threat endangering the security of digital circuits employing voters. The threat enables direct bit-value reading from the circuit.

We described the properties of a majority voter, that make this kind of circuit a source of the threat. SPICE simulations were used to demonstrate the potentially dangerous behaviour.

As only simulations were provided, measurements should be performed to confirm the severity of the reported threat. We used conventional voter design for demonstration, the influence of voter architectures should be studied.

Acknowledgment

The authors acknowledge the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics" and grants GA16-05179S of the Czech Grant Agency and the CTU grant SGS17/213/OHK3/3T/18.

References

[1] T. Snyder and G. Byrd, "The Internet of Everything," *Computer*, vol. 50, no. 6, pp. 8–9, 2017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/MC.2017.179

[2] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 3, pp. 461–491, 2004.

[3] I. Koren and C. M. Krishna, *Fault-Tolerant Systems*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2007.

[4] T. M. Austin, "DIVA: A reliable substrate for deep submicron microarchitecture design," in *Microarchitecture, 1999. MICRO-32. Proceedings. 32nd annual international symposium on*. IEEE, 1999, pp. 196–207.

[5] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." *IACR Cryptology ePrint Archive*, vol. 2005, p. 388, 2005.

[6] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The sorcerer's apprentice guide to fault attacks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 370–382, 2006.

[7] S. Bhasin, J. L. Danger, F. Flament, T. Graba, S. Guilley, Y. Mathieu, M. Nassar, L. Sauvage, and N. Selmane, "Combined SCA and DFA Countermeasures Integrable in a FPGA Design Flow," in *2009 International Conference on Reconfigurable Computing and FPGAs*, Dec 2009, pp. 213–218.

[8] D. Karaklajić, J. Schmidt, and I. Verbauwhede, "Hardware Designer's Guide to Fault Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 12, pp. 2295–2306, Dec 2013.

[9] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Annual international cryptology conference*. Springer, 1997, pp. 513–525.

[10] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 320–334.

[11] S.-M. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," *IEEE Transactions on Computers*, vol. 49, no. 9, pp. 967–970, Sep 2000.

[12] F. Amiel, K. Villegas, B. Feix, and L. Marcel, "Passive and active combined attacks: Combining fault attacks and side channel analysis," in *Fault Diagnosis and Tolerance in Cryptography, 2007. FDTC 2007. Workshop on*, Sept 2007, pp. 92–102.

[13] D. H. Habing, "The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, 1965.

[14] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J.-M. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology," in *IEEE International Reliability Physics Symposium (IRPS), 2013*. IEEE, 2013, pp. 5B–5.

[15] A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart *et al.*, "Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology," in *38th International Symposium for Testing and Failure Analysis, (ISTFA) 2012*, 2012, pp. 5B–5.

[16] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J. Dutertre, and A. Tria, "Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology," in *Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, July 2013, pp. 22–27.

[17] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[18] S. Skorobogatov, "Optically enhanced position-locked power analysis," in *Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2006, pp. 61–75.

[19] C. Roscian, A. Sarafianos, J. Dutertre, and A. Tria, "Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells," in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Aug 2013, pp. 89–98.

[20] R. Llido, A. Sarafianos, O. Gagliano, V. Serradeil, V. Goubier, M. Lisart, G. Haller, V. Pouget, D. Lewis, J.-M. Dutertre *et al.*, "Characterization and TCAD simulation of 90 nm technology transistors under continous photoelectric laser stimulation for failure analysis improvement," in *19th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA) 2012*. IEEE, 2012, pp. 1–6.

[21] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 4th ed. USA: Addison-Wesley Publishing Company, 2010.