Side-channel Issues for Designing Secure Hardware Implementations

Lejla Batina, Nele Mentens, Ingrid Verbauwhede
Katholieke Universiteit Leuven, ESAT/SCD-COSIC
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
{Lejla.Batina,Nele.Mentens,Ingrid.Verbauwhede}@esat.kuleuven.ac.be

Abstract

Selecting a strong cryptographic algorithm makes no sense if the information leaks out of the device through side-channels. Sensitive information, such as secret keys, can be obtained by observing the power consumption, the electromagnetic radiation, etc. This class of attacks are called side-channel attacks. Another type of attacks, namely fault attacks, reveal secret information by inserting faults into the device. Because both side-channel attacks and fault attacks are based on weaknesses in the implementation, they both belong to the category of implementation attacks. This work gives an overview of the state-of-the-art in implementation attacks, reviews the origin of this problem at the CMOS circuit level and discusses countermeasures.

1 Introduction

The security of cryptographic circuits mainly depends on their resistance against all kinds of attacks. While mathematical attacks search for trapdoors in the cryptographic algorithm, implementation attacks focus on weaknesses in the implementation of the algorithm. In this contribution we give an overview of the state-of-the-art in implementation attacks and hardware countermeasures. Implementation attacks can be divided into two categories: side-channel attacks and fault attacks. Side-channel attacks try to extract secret information based on some side-channel. This is a physical quantity such as time, power consumption, electromagnetic radiation or sound. A fault attack is conducted by injecting a fault in a cryptographic implementation, which causes some stored values to change. These incorrect values compromise the security of the system. Section 2 and 3 focus on side-channel and fault attacks, respectively, together with some countermeasures. Conclusions are given in Sect. 4.

2 Side-channel attacks

This section elaborates on the three most commonly exploited side-channel attacks, namely timing, power analysis and electromagnetic radiation attacks. For power analysis attacks, countermeasures at the circuit level are addressed. Other side-channels such as sound and infrared radiation will not be addressed in this contribution.

2.1 Timing attacks

In 1996 Kocher *et al.* introduced the concept of timing attacks by showing that secret information can be extracted through measurements of the execution time of cryptographic algorithms [6]. Timing attacks are applicable to all implementations that have a non-constant execution time which depends on the bits of the secret key.

2.2 Power analysis attacks

Two years later Kocher *et al.* performed successful attacks by measuring the power consumption while the cryptographic circuit is executing the implemented algorithm [7].

Standard CMOS is the most commonly used circuit style to implement digital circuits. Its popularity is the result of its low power consumption and its robust behavior. Yet this is also the source of information leakage. To explain why the power consumption of a circuit can reveal information on the data that are processed inside, we look at the power consumption of a single CMOS inverter. Figure 1 shows the four possible switching events at the output of an inverter.

It is clear that an inverter consumes no power when the output value does not change (of course this is only true to the first order, because in reality there is also leakage power and short-circuit power). On the other hand, a change of value causes supply current to flow and power to be consumed. This fact does not only hold for an inverter, but also for all other logic gates and for registers. Power analysis attacks are based on this observation. More precisely, if the value of a secret key bit determines wether a transition occurs or not, measuring the power consumption reveals the value of this bit.

The most straightforward power analysis, called Simple Power Analysis (SPA), uses a single measurement to reveal

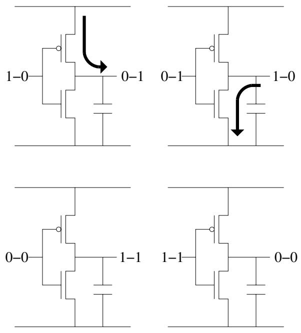

Figure 1. Currents caused by the four different transitions applied of a CMOS inverter.

the secret key by searching for patterns in the power trace. However, implementations that are resistant against SPA attacks, can still be broken by using a more advanced technique, namely Differential Power Analysis (DPA). In this case many power measurements are evaluated using statistical analysis.

2.3 Countermeasures for side-channel attacks

Security is as strong as the weakest link, therefore protecting cryptographic systems should be done on all levels of abstraction, which are depicted in the security pyramid in Figure 2. Each abstraction layer represents specific modelling, design and implementation issues that must be covered for secure system operation [12]. In this contribution we focus on the circuit level to address countermeasures for side-channel attacks as well as fault attacks.

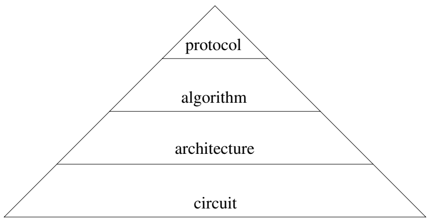

Figure 2. Security pyramid showing the different levels of abstraction.

As explained in Section 2.2, the power consumption of a circuit depends on the output transitions of the gates. If these transitions depend on secret information, the security of the implementation can be compromised. Hence, to make a circuit resistant against power analysis attacks, the power consumption should be independent of the secret information. The circuit-level approaches to achieve this can be divided into two categories: custom logic styles and standard logic styles. Custom logic styles are only applicable to custom ASIC implementations. Standard logic styles combine standard cells from existing libraries into new standard cells. Hence, they can be used for FPGA implementations as well as standard cell ASIC implementations. Tiri *et al.* developed SABL [5], which is a custom logic style, and WDDL [15], which is a logic style consisting of standard cells. In the remainder of this section both SABL and WDDL will be discussed, because they represent the state-of-the-art in logic styles.

2.3.1 Sense-Amplifier Based Logic (SABL)

To make the power consumption of a gate independent of the input values, SABL achieves the following goals: the output switching is independent of the input values and the total load capacitance always sums up to a constant value.

The first goal is achieved by using differential and dynamic logic. Differential logic makes sure that a 1-0 input transition causes the same output transitions as a 0-1 input transition, but it does not hide the difference between a transition (1-0 or 0-1) and no transition. This problem is solved by making the logic dynamic, *i.e.* precharging the output in the first half of every clock cycle and evaluating the correct output value in the second half. In this way, there is a switching event in every clock cycle.

The second goal is achieved by designing a secure cell library in which the load capacitance of a gate is equal for all input values. This library consists of an inverter, a NAND-gate, an XOR-gate and a flip-flop, which should be enough to implement all cryptographic algorithms. To guarantee that the pull-down networks are balanced and completely discharged, design rules for the pull-down network are given in [16].

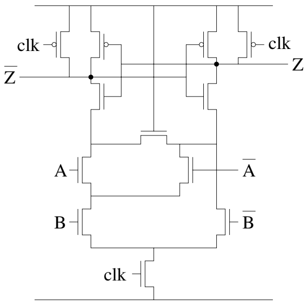

Figure 3. SABL AND gate with $Z = A \cdot B$.

2.3.2 Wave Dynamic Differential Logic (WDDL)

The main drawback of the SABL approach is that it is only suitable for custom ASIC implementations. WDDL achieves the same goals as SABL by using cells from an existing standard cell library. However, to reduce the load on the precharge control signal, WDDL uses a precharge “wave”, *i.e.* the precharge signal ripples through the combinatorial logic. In Figure 4 a cascaded WDDL AND gate and flip-flop are shown. The WDDL gate requires the inputs to be precharged before they are sent to the complementary gates. A precharge circuit after the registers makes sure the next gates receive correct inputs.

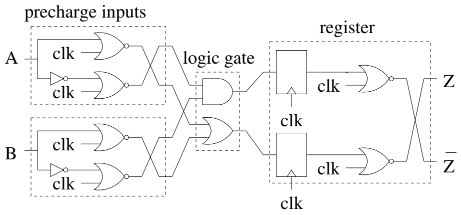

Figure 4. Cascaded WDDL AND gate and flip-flop.

2.4 Electromagnetic radiation attacks

A third side-channel is the electromagnetic radiation [4, 9]. An ElectroMagnetic Analysis (EMA) attack can be done by using the same methods as for power attacks. Therefore, the terms Simple EMA (SEMA) and Differential EMA (DEMA) are commonly used. However, EMA attacks can extract much more information than power attacks. The reason is that the latter measure the complete power consumption, while EMA attacks can zoom in on smaller parts of the circuit.

3 Fault attacks

The second kind of implementation attacks are fault attacks. They are based on hardware faults, which are usually caused by some unexpected condition or defect. However, they can also be applied deliberately by the use of fault insertion techniques. The damage they can cause was first elaborated by Boneh *et al.* [3]. Their target application was RSA with CRT. Biham and Shamir introduced differential fault attacks (DFAs) on the DES algorithm [2] and they showed that DFAs are applicable to any secret key cryptosystem. In the research community two types of investigations are being performed. The first type is investigating the actual ways to induce faults in a cryptosystem *i.e.* it deals with so-called physical security and the other one is examining vulnerabilities in cryptographic algorithms with the assumption that some faulty computation happened. In this paper we consider only the former one.

Usual sources of faults are glitches (voltage, clock, temperature, radiations *i.e.* “microwave attacks”) or beams (UV light, X-rays, laser, camera flash, *etc.*). They can be semi-invasive or invasive. For the former type of fault insertions the best results were achieved by depackaging the chip (as for invasive attacks), but the passivation layer of the chip *i.e.* the shield covering the chip remains intact. More precisely, unlike invasive attacks they do not require electrical contact to the metal surface. As an example of a cheap semi-invasive attack optical fault induction attacks were introduced by Skorobogatov and Anderson [14]. They showed that it is possible to change the state of any individual bit in a microcontroller by using a camera flash and a laser pointer. Their target was an SRAM cell but this type of attacks is applicable to any other kind of memory as well. Another type of semi-invasive attacks are done by electromagnetic induction *i.e.* eddy currents [10]. The follow-up work of Samyde *et al.* [11] summarizes all kinds of possibilities to read secret data from memories. They compare the effects caused by optical induction on one side and eddy currents on the other side. The conclusion was that for the latter resolution is not so precise as for optical fault attacks. Skorobogatov and Anderson suggested to use self-timed dual-rail logic as a countermeasure. The idea behind this approach is not just to have a logical 0 or 1 encoded as HL and LH (or vice versa), but also to prohibit the HH state. Namely, this combination signals an alarm, which will typically reset the processor. This property is also present in WDDL logic (Sect. 2.3.2). If the circuit is read before the output is ready, the outputs Z and $\overline{Z}$ of Figure 4, will not yet be differential. As WDDL is glitch-free, only one transition can occur during evaluation from the precharge state to a differential state (01 or 10).

Considering glitches-based attacks, the first practical result was given by Aumüller *et al.* in [1]. They introduced a *spike*, *i.e.* a certain deviation from a standard interval for a smart card parameter *e.g.* the supply voltage. They performed two attacks on a smart card with an RSA coprocessor and proved that these type of attacks are feasible even if some countermeasure [13] is deployed.

Most of the techniques for fault insertion target the secret data that are manipulated during the execution of a cryptographic algorithm, but some are directed on faults on memories. An overview paper dealing with several ideas about these issues for memories and their secure use is the work of Neve *et al.* [8]. The authors also mention a number of countermeasures to prevent those threats, such as: dual rail precharged logic, sensors, *etc.* Sensors are supposed to monitor sudden changes in temperature, voltage or similar and act accordingly. By their function they can be active or passive.

All attacks mentioned above are considered to be semi-invasive. Invasive fault induction includes probing the circuit with active or energy probes [17]. Other options mentioned are electron or ion beams.

As for countermeasures, [11] mentions the importance of hardware countermeasures and lists the necessary requirements for the protection of modern smart cards. Means to achieve minimal physical security include: implementing the CPU using random place-and-route to avoid the visibility of the registers, memory encryption, use of self-timed logic with built-in alarm propagation and alarm sensors for temperature, X-rays, *etc*. It is up to the manufacturers to investigate the risks and decide about the best combination of countermeasures.

4 Conclusions

This contribution gives an overview of the state-of-the art in side-channel and fault attacks. Implementing cryptographic circuits is always a trade-off between security and performance. This work focuses on the most efficient, but also the most costly type of countermeasures, namely countermeasures at the circuit level. However, for security-crucial applications these kind of countermeasures might be unavoidable.

5 Acknowledgements

Lejla Batina and Nele Mentens are funded by research grants of the Katholieke Universiteit Leuven, Belgium. This work was supported by FWO project G.0450.04 and by the EU IST FP6 projects SCARD and ECRYPT. The work on SABL and WDDL is done by Kris Tiri and Ingrid Verbauwhede at UCLA. It was funded by NSF project CCR-0098361.

References

[1] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J.-P. Seifert. Fault attacks on RSA with CRT: Concrete results and practical countermeasures. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proceedings of 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, number 2523 in Lecture Notes in Computer Science, pages 260–275, Redwood Shores, CA, USA, August 13-15 2002. Springer-Verlag.

[2] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In B. S. Kaliski Jr., editor, *Advances in Cryptology: Proceedings of CRYPTO'97*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer-Verlag, 1997.

[3] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults (extended abstract). In W. Fumy, editor, *Advances in Cryptology: Proceedings of EUROCRYPT'97*, number 1233 in Lecture Notes in Computer Science, pages 37–51, Konstanz, Germany, May 11-15 1997. Springer-Verlag.

[4] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Proceedings of 3rd International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, number 2162 in Lecture Notes in Computer Science, pages 255–265. Springer-Verlag, 2001.

[5] M. A. K. Tiri and I. Verbauwhede. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Proceedings of 28th European Solid-State Circuits Conference (ESSCIRC)*, pages 403–406, 2002.

[6] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. In N. Koblitz, editor, *Advances in Cryptology: Proceedings of CRYPTO'96*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer-Verlag, 1996.

[7] P. Kocher, J. Jaffe, and B. Jun. Introduction to differential power analysis and related attacks. `http://www.cryptography.com/dpa/technical`, 1998.

[8] M. Neve, E. Peeters, and J. J. Quisquater. Memories: A survey of their secure uses in smart cards. In *Second International IEEE Security in Storage Workshop - Proceedings of SISW 2003*, 2003.

[9] J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and couter-measures for smard cards. In I. Attali and T. P. Jensen, editors, *Smart Card Programming and Security (E-smart 2001)*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer-Verlag, 2001.

[10] D. Samyde and J.-J. Quisquater. Eddy current for magnetic analysis with active sensors. In *Smart Card Programming and Security (E-smart 2002)*, pages 185–194, 2002.

[11] D. Samyde, S. Skorobogatov, R. Anderson, and J.-J. Quisquater. On a new way to read data from memory. In *First International IEEE Security in Storage Workshop, Greenbelt Marriott, Maryland, USA*, 2002.

[12] P. Schaumont and I. Verbauwhede. Domain-specific codesign for embedded security. *IEEE Computer Magazine*, 36(4):68–74, April 2003.

[13] A. Shamir. Method and apparatus for protecting public key schemes from timing and fault attacks. US patent number 5,991,415, November 1999.

[14] S. P. Skorobogatov and R. J. Anderson. Optical fault induction attacks. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer-Verlag, 2002.

[15] K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings of Design, Automation and Test in Europe Conference (DATE)*, pages 246–251, February 2004.

[16] K. Tiri and I. Verbauwhede. Design method for constant power consumption of differential logic circuits. In *Proceedings of Design, Automation and Test in Europe Conference (DATE)*, pages 628–633, March 2005.

[17] S. H. Weingart. Physical security devices for computer subsystems: A survey of attacks and defenses. In Ç. K. Koç and C. Paar, editors, *Proceedings of 2nd International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, number 1965 in Lecture Notes in Computer Science, pages 302–317, Worcester, Massachusetts, USA, August 17-18 2000. Springer-Verlag.