HAL open science

Side-Channel Leakage across Borders

Jörn-Marc Schmidt, Thomas Plos, Mario Kirschbaum, Michael Hutter, Marcel Medwed, Christoph Herbst

To cite this version:

Jörn-Marc Schmidt, Thomas Plos, Mario Kirschbaum, Michael Hutter, Marcel Medwed, et al.. Side-Channel Leakage across Borders. 9th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications (CARDIS), Apr 2010, Passau, Germany. pp.36-48, 10.1007/978-3-642-12510-2_4 . hal-01056100

HAL Id: hal-01056100

https://inria.hal.science/hal-01056100v1

Submitted on 14 Aug 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Side-Channel Leakage Across Borders

Jörn-Marc Schmidt, Thomas Plos, Mario Kirschbaum, Michael Hutter, Marcel Medwed and Christoph Herbst

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{joern-marc.schmidt, thomas.plos, mario.kirschbaum, michael.hutter, marcel.medwed, christoph.herbst}@iaik.tugraz.at

Abstract. More and more embedded devices store sensitive information that is protected by means of cryptography. The confidentiality of this data is threatened by information leakage via side channels like the power consumption or the electromagnetic radiation. In this paper, we show that the side-channel leakage in the power consumption is not limited to the power-supply lines and that any input/output (I/O) pin can comprise secret information. The amount of leakage depends on the design and on the state of the I/O pin. All devices that we examined leaked secret information through their I/O pins. This implies that any I/O pin that is accessible for an adversary could be a security hole. Moreover, we demonstrate that the leakage is neither prevented by transmitter/receiver circuits as they are used in serial interfaces, nor by a galvanic isolation of a chip and its output signals via optocouplers. An adversary that is able to manipulate, for example, the pins of a PC's I/O port, can attack any device that is connected to this port without being detected from outside.

Keywords: Power Analysis, I/O Pin, Microcontroller, Optocoupler, Serial Interface

1 Introduction

Security-related devices are an integral part of our everyday life. Typically, it is rather difficult to verify whether a device reaches a certain security level or not. Insufficient security protection remains often unnoticed until a successful attack is found. The security level is basically determined by two factors: the choice of the cryptographic algorithm (including the protocol), and the way the algorithm is implemented.

Even if a cryptographic algorithm is mathematically secure, its implementation in hardware might not be. About one decade ago, Kocher *et al.* published a ground-breaking paper about differential power analysis (DPA) attacks [1]. They showed that analyzing the power consumption of a cryptographic device can reveal secret information that is stored in it, e.g. an encryption key. Since that time, many research groups have gradually improved power-analysis attacks and performed them on a variety of devices, like smart cards [2], field-programmable gate arrays (FPGAs) [3], and radio-frequency identification (RFID) devices [4].

Power-analysis attacks are a very powerful technique that even works in presence of strong noise. In a first step, an adversary generates key hypotheses, which contain all possible values for a small part of the secret key (e.g. one byte). Intermediate values of the attacked algorithm are calculated from the key hypotheses and a set of different input values. Based on the intermediate values, the adversary estimates the power consumption of the device by means of an appropriate power model. During the second step, the power consumption of the device is measured and recorded (leading to the so-called power traces) while it computes the intermediate values. In the third and last step, the power-consumption estimations for each key hypothesis are compared with the measured power traces by means of statistical methods. If the adversary uses an appropriate power model, the analysis leads to the correct key. The adversary has successfully revealed a part of the secret key. This procedure is repeated for the remaining parts. Experience shows that in case of unprotected cryptographic devices, some hundred up to a few thousand input values and corresponding power traces are sufficient to distinctly reveal the whole secret key [5].

Most of the published side-channel attacks measure the power consumption of the target device via a resistor in one of the power-supply lines. Other methods measure, for example, the electromagnetic radiation during the computation of the cryptographic algorithm [6, 7]. In order to prevent the leakage of sensitive information via the power-supply lines, countermeasures are integrated into cryptographic devices. Various countermeasure approaches have been presented in the past, for example, by using special logic styles [8–10], by inserting filters [11], or by decoupling the power consumption with switched capacitors [12, 13].

It was first mentioned by Shamir [12] that side-channel information can also leak through the input/output (I/O) pins of a device. Oren *et al.* [14] presented practical results about analyzing the power consumption of a PC via its universal serial bus (USB) port. In [15], Plos pointed out the problem of side-channel leakage via I/O pins of RFID tags. However, there is no work so far that investigates the effectiveness of side-channel attacks via I/O pins in detail and that compares them with the results from classical attacks in the power-supply lines.

In this paper, we discuss the possibilities to measure the voltage variations at I/O pins. We show that power-analysis attacks are feasible in the same way by using the I/O pins. This presents an alternative attack method whenever a direct measurement in the power-supply lines is not possible. We evaluated the voltage variations at the I/O pins of five devices for different pin-configurations. For each device, we found at least one configuration that leaked information at the I/O pins. The standard microcontrollers, for example, leaked information in any configuration. In addition, we measured a device with capacitors as filters in the power-supply lines, which reduced the leakage in the ground line, but not at the I/O pins. This demonstrates that protecting only the power-supply lines is not sufficient and that additional precautions should be taken to prevent I/O pin leakage. For embedded systems with more than one device integrated onto a board, measuring the voltage variations at an I/O pin can be an improvement

compared to measuring the power consumption of the whole system. We show that information leakage also occurs if the I/O pin is not directly measured, but after passing a signal amplifier. We demonstrate this by successfully performing a DPA attack on a serial interface that uses a receiver/transmitter module. Hence, an adversary can perform attacks without being noticed by the owner of the device, e.g. by manipulating the serial interface of a PC to which the device is connected to. Moreover, we demonstrate that even a galvanic isolation via optocouplers does not totally suppress the information leaking at the I/O pin.

The remaining paper is organized as follows. After giving a brief introduction into I/O pins in Section 2, we present our measurement setup in Section 3. The results of the measurements are given in Section 4. Afterwards, Section 5 discusses some practical scenarios that arise from the presented attacks, including (among others) a DPA measurement on the clock signal as well as DPA measurements of an I/O pin that is separated by an optocoupler. Finally, conclusions are drawn in Section 6.

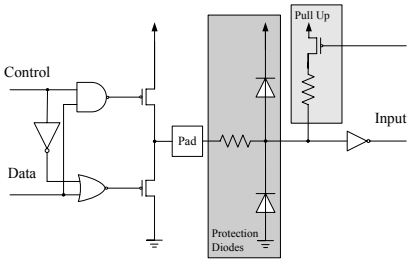

Fig. 1. Schematic of a standard I/O pin. The control signal can switch the pin to tri-state.

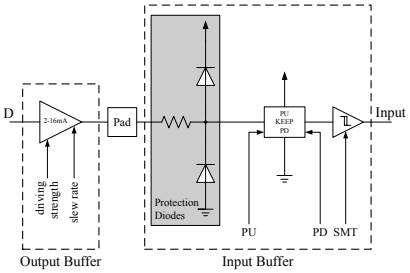

Fig. 2. Schematic of a programmable output and a programmable input buffer of the ASIC prototype chip.

2 I/O Pins

I/O pins are the interface between an integrated circuit and the outside world. They are used to transfer data and control signals. Depending on their design, I/O pins can act in one direction only or they can support both directions: input and output.

Especially input pins require a protection mechanism to prevent damage of the inner circuits caused by an overvoltage. This mechanism is called electrostatic discharge (ESD) protection and typically consists of two diodes that drain off the overvoltage to the positive supply voltage (VDD) or to ground (GND). In addition, a resistor is inserted to limit the current flowing over the diodes. Figure 1 shows an I/O pin that comprises such an ESD-protection circuit.

In contrast to input pins, output pins have a low-resistance connection to VDD or GND. Thus, a dedicated ESD-protection is not necessary for them.

Since output pins have to drive logic signals off-chip, a circuit that is able to provide enough current is required. These circuits are often implemented as parallel transistors of increasing width and length [16].

Pins that can either be configured as input or as output, provide a so-called *tri-state*. This state allows to define the value of the pin externally, i.e. the pin acts as input. Thereby, the output transistors are disabled and the pin is in a high-impedance state. Such an I/O pin is depicted in Figure 1. The schematic features also a pull-up resistor, which holds the input pin in a high state whenever it is not driven externally. This prevents the pin from being in a random or undefined state. Other constructions provide pull-down resistors to put a pin into a low state if no external signal is present.

Figure 2 shows a programmable output and a programmable input buffer of the application-specific integrated circuit (ASIC) prototype chip that we used for some of our measurements. The ASIC input buffer contains ESD protection structures similar to the one described above. The input buffer can be programmed to work as pull up, as pull down, or as keeper[1]. Additionally, the input buffer can be programmed to work as a Schmitt trigger to switch the input value only if a clearly different signal is applied. Also the output buffer can be programmed to some degree. The driving strength can vary between 2 mA and 16 mA, and the slew rate of the output buffer can be either set to *slow* or to *fast*. On our prototype chip, the input buffers are programmed as pull down with Schmitt-trigger functionality disabled. The output buffers are configured to have a driving strength of 2 mA with the slew rate set to *fast*.

3 Measurement Setup

For a general characterization of the I/O pin leakage of the devices, we compare the leakage in the GND supply line to the information that leaves the device via the I/O pins in different configurations. We test five devices, an Atmel ATMega163 8-bit microcontroller on a smart card, an 8-bit 8051 microcontroller AT89S8253 from Atmel, a 32-bit ARM7 microcontroller LPC2148 from NXP, a Virtex-II Pro XC2VP7 FPGA, and an ASIC chip. Each of them contains an implementation of the Advanced Encryption Standard (AES) that uses a key length of 128 bits. None of these implementations include side-channel countermeasures.

For each measurement, we perform a Differential Power Analysis (DPA) attack. The goal of our DPA attacks on the AES implementations is to reveal the secret key. During the last years, several approaches for DPA attacks on AES implementations have been proposed ([17–19]). Our DPA attacks are based on the Hamming distance of two intermediate byte values. The target of the attack is the result of the SubBytes transformation in the first round of the AES algorithm. We use the Pearson correlation coefficient for matching our power estimations with the measurements.

[1] The input value does not change when the signal is disconnected from the pin if the buffer is programmed as keeper.

Our measurement setup mainly consists of a PC, an oscilloscope, measurement probes, and the device under test. A Matlab script running on the PC controls the whole measurement. It sends the plaintexts to the device via a serial interface and reads the power traces from the oscilloscope that measures the voltage on the I/O pin and the voltage drop across a resistor in the ground line of the device.

A classical measurement in the GND line is performed in parallel to the measurement at the I/O pin. The power measurement delivers a basis for comparison with the results from I/O pin measurements. For each device, the pin configurations output high, output low, and input (with 10 kΩ pull-down resistor) are measured. Each measurement uses the same fixed AES key and the same input plaintexts.

Since no side-channel countermeasures are included in our implementations, a DPA attack was possible with some hundred to a few thousand traces. Our measurements show that the same attacks are possible when measuring the I/O pins instead of the power-supply lines.

4 Practical Results

This section shows the practical outcomes of our measurements. We describe the special properties of all five devices, present the analysis results, and discuss them.

4.1 Atmel ATMega163 8-bit Microcontroller on a Smart Card

In the first experiment, we measured a programmable smart card with an integrated 8-bit microcontroller. The microcontroller is an ATMega163 from Atmel, which has a reduced instruction set (RISC) architecture. The ATMega163 comprises various features, including internal EEPROM, a serial interface, a serial peripheral interface, and an analog comparator. A self-made smart-card reader, which is depicted in Figure 3, was used to establish the communication between the PC and the smart card. Since the smart card only provides an 8-pin connector, the number of pins of the microcontroller that are accessible is strongly limited. However, there is one unused I/O pin that we measured in our experiments.

We conducted four DPA attacks on the smart card and compared them with respect to the maximum achievable correlation. The first attack measured the power consumption of the smart card in the GND line of the power supply. The remaining three attacks targeted the voltage variations at the unused I/O pin with different configurations: pin defined as output and logic high, pin defined as output and logic low, and pin defined as input (tri-state).

All attacks were successful. The reference measurement in the GND supply line led to a maximum correlation of 0.57. The voltage variations at the I/O pin defined as output delivered similar values: 0.64 for logic high and 0.56 for logic low. Defining the I/O pin as input reduced the maximum correlation to about 0.11.

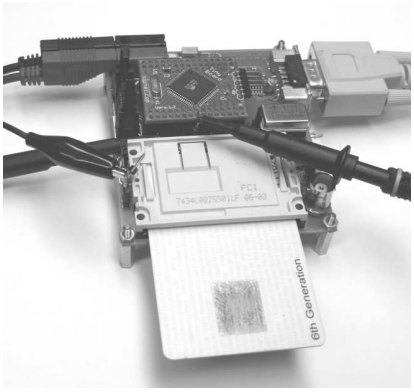

Fig. 3. Measurement setup for the Atmel ATMega163 smart card. One probe measures the trigger signal, the other probe measures the voltage variation of a fix programmed I/O pin.

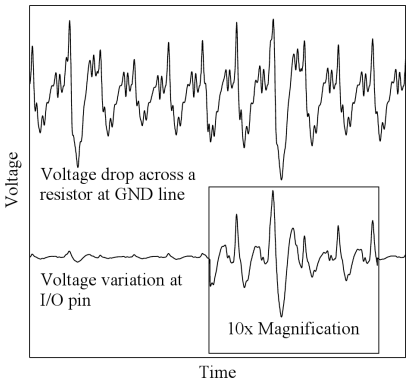

Fig. 4. Comparison between the power consumption measured in the GND line and the voltage variations at an I/O pin of the AT89S8253. The I/O pin was set to logic low for the measurement.

4.2 Virtex-II Pro FPGA XC2VP7

For testing the leakage at an I/O pin of an FPGA, we targeted a Xilinx XC2VP7 of a SASEBO board[2]. Our AES implementation for the FPGA includes one extra pin for the measurements, which varied between input and output. A measurement in the GND line resulted in a correlation of 0.06, setting the output pin to low reduced the correlation to 0.03. A correlation of 0.01 was achieved for the pin configured as input. For a pin that was set to high, no correlation was measured by using up to 300 000 power traces.

In order to characterize further details of the leakage, we added area constrains to the implementation that forced the place and route utilities to concentrate on one half of the chip and leave the second half unprogrammed. In addition, two wires were routed through the device to an output pin, one straight through the programmed logic, and one through the *empty* part. The measurements revealed no difference between the information leakage of the two pins.

4.3 ARM 32-bit RISC Processor

The LPC2148 from NXP is an ARM7TDMI-S based microcontroller with a 32-bit architecture. Our device under test features a wide range of peripherals like USB, analog-to-digital converters, and several bus standards. None of those peripherals was turned off during the measurements. Thus, the noise level was comparable to an unprotected real-world application.

[2] The control FPGA of the SASEBO board was programmed to forward the serial interface.

Our development board gave access to the I/O pins of the microcontroller. The measurement at the I/O pins was threefold: output pin set to one, output pin set to zero, and input pin pulled down to GND. For the correct AES key, the power measurements in the GND line achieved a correlation of 0.56. The traces acquired at the high output pin still yielded a correlation of 0.44. The voltages at the low output pin and at the input pin correlated with 0.15 and 0.12, respectively.

4.4 Atmel 8051 Microcontroller

The data-dependent I/O leakage of an 8051 8-bit microcontroller was investigated on an AT89S8253 from Atmel. The microcontroller is shipped with 32 programmable I/O pins that can be accessed by four 8-bit bi-directional ports. One port provides eight open-drain pins, which can be configured to logic low (actively sinking current) or to a high impedance state. The pins of the three remaining ports can be configured as sink or source input/output that are equipped with internal pull-up resistors.

We performed four attacks. First, we measured the power consumption in the GND line of the prototyping board and obtained a correlation of 0.59 for the correct key hypothesis. Next, we performed attacks on 20 different I/O pins, which where configured to logic low. All attacks were successful and led to nearly the same correlation of 0.56. This demonstrates that the leakage does not depend on the measured I/O pin (the standard deviation of the correlation was 0.01). A comparison between two power traces, one measured at the GND line and one at the I/O pin configured to output logic low is given in Figure 4. After that experiment, we performed an attack on a pin that was configured to logic high. The attack was successful with a correlation of 0.30. Our last attack on this device targeted the open-drain port, which was configured as a high-impedance output. The attack was also successful and led to a correlation of 0.22.

4.5 180 nm CMOS ASIC Prototype Chip

The ASIC prototype chip for testing the leakage of I/O pins was produced in a 180 nm CMOS process technology from UMC [20] and uses the standard cell library from Faraday [21]. The chip contains an AES crypto module with a size of 0.1 mm^2, which equals approximately 10 770 GEs.

First, a DPA attack based on the power consumption measured in the GND line of the prototype chip was performed. The result of this attack served as a reference for the other DPA attacks that targeted the voltage variations at I/O pins. The other DPA attacks were performed on an output pin with logic level low, on an output pin with logic level high, and on an input pin with logic level low (programmed as pull-down, see Section 2).

All attacks on the AES crypto module on the ASIC prototype chip were successful. The reference attack based on the power measurement in the GND line led to a maximum correlation of 0.0119. The other DPA attacks led to quite

similar results: 0.0124 for the low output pin, 0.011 for the high output pin, and 0.0121 for the low input pin.

Table 1. Summary of the Results.

Device	Corr. in GND	Correlation (Percentage of GND) Output High	Output Low	Input
ATMega163 (Smart Card)	0.57	0.64 (112%)	0.56 (98%)	0.11 (19%)
LPC2148 (ARM7)	0.56	0.44 (79%)	0.15 (27%)	0.12 (21%)
AT89S8253 (8051)	0.59	0.30 (54%)	0.56 (95%)	0.22 (37%)
XC2VP7 (FPGA)	0.06		0.03 (50%)	0.01 (17%)
ASIC Prototype (180 nm)	0.0119	0.011(92%)	0.0124(104%)	0.0121(101%)

4.6 Summary of the Practical Results

Table 1 summarizes the results of our DPA attacks on the five different devices. It can clearly be seen that DPA attacks based on voltage variations at I/O pins can successfully be mounted on many devices even if the VDD line or GND line are not directly accessible. Furthermore, regardless of the configuration of the I/O pin, a successful DPA attack is possible. The fact that conventional DPA attacks can easily be performed by measuring the voltage variations at I/O pins opens new possibilities for adversaries to attack cryptographic devices, even if the accessibility of the target is limited. Some practical scenarios demonstrating new attack variants are discussed in the following section.

5 Practical Scenarios

In order to transfer our results into a more practical context, we performed additional experiments, which demonstrate the relevance of our research. Since the AT89S8253 shows the strongest information leakage of all tested devices, we focus on this device in the following experiments. Considering the results presented in the previous section, it is very likely that the following scenarios work with the other devices alike.

5.1 Signal Filter

Throughout this paper, our experiments assumed that the power-supply lines of the device under test are not accessible for an adversary and hence a direct measurement of the consumed power is not possible. This can be the case, for example, if a filter suppresses the leakage in the power supply lines. We used a cascade of capacitors as filter to reduce the data-dependent signal. Although our filter significantly reduced the data dependency in the GND line, we were not able to eliminate it totally. However, our approach did not influence the leakage

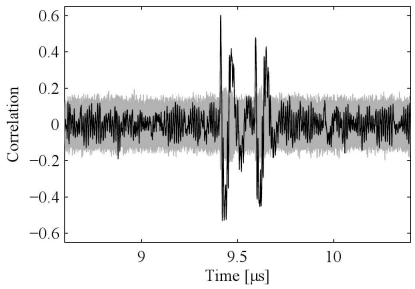

Fig. 5. Correlation plot of AT89S8253 measured with a passive probe in the GND line of the power supply. The measurement serves as reference.

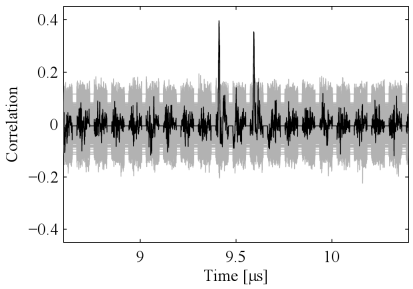

Fig. 6. Correlation plot of AT89S8253 measured with a passive probe at the clock interface, supplied with an on-board crystal oscillator.

in the I/O pins. The experiment demonstrates that the information leakage via the I/O pins does not depend on the information leakage in the power-supply lines.

5.2 Clock Supply

A special case of an I/O pin is the clock interface. While capacitors can filter the power-supply lines to prevent information leakage, this approach is not applicable in the same simple way to the clock supply. We tried two different scenarios. First, an on-board crystal oscillator generated the clock signal. For the measurement, we concentrated on the positive part of the signal and cut the negative part off to get a better measurement resolution. Our attack was successful with a correlation of 0.4, which is about two third of the correlation in the GND line, as depicted in Figure 5 and Figure 6. Second, an external signal generator provided the signal. We achieved a correlation of 0.5. Hence, whenever the clock signal is accessible, it is a potential threat to the security of the device.

5.3 Serial Interface

A very common way to transfer data between devices is a serial port. The results from the previous section showed that I/O pins leak information. This includes the pins of the serial interface. However, in an embedded system, the device is often supplied by a lower voltage than the one required for the serial connection (+/- 12 V). Hence, a signal amplifier converts the logical signals from the device to the voltage range required for the serial connection. An adversary may only have access to those signals, not to I/O pins directly. Fortunately for an adversary, the information is not suppressed by the amplifier. We measured the receive (RX) and transmission (TX) line of a signal converter (MAX232) directly on the board and achieved a correlation of 0.1 in the TX line and in the RX line, compared to a correlation of 0.6 for a direct measurement in the GND line.

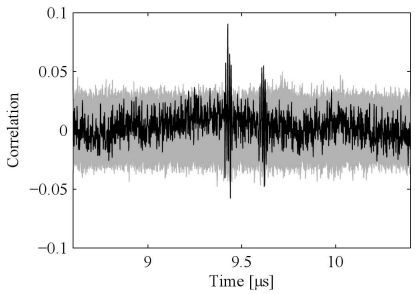

Fig. 7. Correlation plot of AT89S8253 measured with a passive probe at the serial interface on the transmission line after the signal converter (MAX232) directly on the test board.

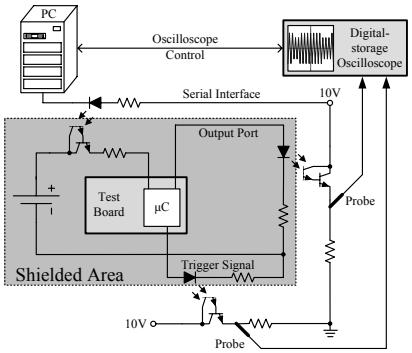

Fig. 8. Measurement setup with galvanically isolated circuits. The measurement signal, the trigger, as well as the transmission line of the serial interface are transferred via optocouplers.

A correlation plot for the TX line is given in Figure 7. Using a 1 m cable that is connected to a computer and measuring at the input port of the PC reduced the correlation to 0.05. Hence, an adversary that is able to modify the serial port of a computer can successfully attack devices without the device owners' knowledge who connects the device to a PC.

5.4 Device and Measurement Circuit Separated via Optocoupler

A common idea when talking about information leakage via power lines is to separate the circuit in which the computation takes place from the *outside world*. In order to transfer information between the device and the outside world, it is possible to use optocouplers. These small devices consist of a light-emitting diode and a phototransistor. Thus, they allow data transfer without an electric connection. We performed two different measurements. In the first one, only the trigger signal and the signal of the I/O pin were separated via optocouplers. In the second experiment, the two circuits were galvanically isolated.

In the setup for the first measurement, one optocoupler provides the trigger signal, another one was connected to a high output pin. The influence of the pin on the second circuit was measured via an oscilloscope. We could successfully perform a DPA and achieved a correlation of 0.02. The corresponding correlation plot is given in Figure 9.

However, this measurement setup still has a common ground connection since the PC is connected to the oscilloscope and to the device. Thus, the measurement circuit and the target circuit are not galvanically isolated. In order to achieve a galvanic isolation, the device was powered by a battery and the transmission line of the serial connection was established via an optocoupler[3] in the setup

[3] The setup did not use the RX line of the serial interface.

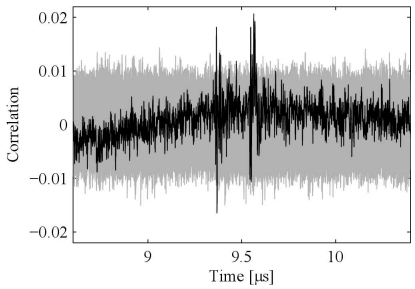

Fig. 9. Correlation plot of AT89S8253 measured with a passive probe at the separated circuit with common ground.

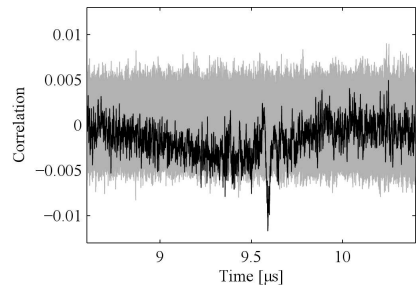

Fig. 10. Correlation plot of AT89S8253 measured with a passive probe at the galvanically isolated circuit.

for our second measurement. The whole measurement circuit was put into a shielding box to suppress possible coupling between the measurement circuit and the target circuit. Figure 8 sketches the measurement setup. Even with the galvanic isolation, we achieved a correlation of 0.01. Figure 10 shows the corresponding plot.

5.5 Summery of Practical Scenarios

Table 2 summarizes the results of the practical scenarios provided in this section. In addition to the achieved correlation, the table provides the estimated number of traces required to succeed with an attack. The numbers were calculated with the rule of thumb from [5]: $n = 3 + 8\frac{z_{1-\alpha}^2}{ln^2\frac{1+\rho}{1-\rho}}$, with n the number of required traces, ρ the correlation coefficient for the correct hypothesis, and α the confidence. For $\alpha = 0.0001$ we get a value $z_{0.9999} = 3.719$.

Table 2. Summary of the Results of the Practical Scenarios.

Scenario	Correlation	Required Samples
Reference in GND	0.6	61
Clock with Signal Generator	0.5	95
Clock with Crystal Oscillator	0.4	158
Serial Interface (RX and TX)	0.1	2 751
Serial Interface at a Distance of 1 m	0.05	11 050
Optocouplers with Common Ground	0.02	69 140
Galvanic Isolation via Optocouplers	0.01	276 604

6 Conclusion

In this paper we demonstrate that side-channel information not only leaks via the power supply lines but also via I/O pins. We performed DPA attacks on five different devices that have integrated a hardware or a software implementation of the AES-128. Our investigations show that DPA attacks can be mounted even if the access to the examined device is severely limited. For example, if the power supply lines are not at an adversary's disposal, or if the adversary wants to attack a device that consists of several chips but has only access to the chip of interest by some sort of interface. Moreover, our results make clear that even in the presence of filtering techniques, signal converters, or optocouplers, successful DPA attacks are possible.

Acknowledgement

The work described in this paper has been supported through Austrian Government funded project *PowerTrust* established under the Trust in IT Systems program FIT-IT.

The authors want to thank Akashi Satoh (National Institute of Advanced Industrial Science and Technology, Japan) and designers of SASEBO for the board we used for the FPGA measurements.

The information in this document reflects only the authors' views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In Wiener, M., ed.: Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings. Volume 1666 of Lecture Notes in Computer Science., Springer (1999) 388–397
2. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Investigations of Power Analysis Attacks on Smartcards. In: USENIX Workshop on Smartcard Technology (Smartcard '99). (May 1999) 151–162
3. Örs, S.B., Oswald, E., Preneel, B.: Power-Analysis Attacks on FPGAs – First Experimental Results. In Walter, C.D., Koç, Ç.K., Paar, C., eds.: Cryptographic Hardware and Embedded Systems – CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings. Volume 2779 of Lecture Notes in Computer Science., Springer (2003) 35–50
4. Hutter, M., Mangard, S., Feldhofer, M.: Power and EM Attacks on Passive 13.56 MHz RFID Devices. In Paillier, P., Verbauwhede, I., eds.: Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings. Volume 4727 of Lecture Notes in Computer Science., Springer (September 2007) 320–333
5. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer (2007) ISBN 978-0-387-30857-9.

6. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P.: The EM Side-channel(s). In Kaliski Jr., B.S., Koç, Ç.K., Paar, C., eds.: Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers. Volume 2523 of Lecture Notes in Computer Science., Springer (2003) 29–45
7. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. In Koç, Ç.K., Naccache, D., Paar, C., eds.: Cryptographic Hardware and Embedded Systems – CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings. Volume 2162 of Lecture Notes in Computer Science., Springer (2001) 251–261
8. Tiri, K., Akmal, M., Verbauwhede, I.: A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. In: 28th European Solid-State Circuits Conference - ESSCIRC 2002, Florence, Italy, September 24-26, 2002, Proceedings, IEEE (September 2002) 403–406
9. Tiri, K., Verbauwhede, I.: A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In: 2004 Design, Automation and Test in Europe Conference and Exposition (DATE 2004), 16-20 February 2004, Paris, France. Volume 1., IEEE Computer Society (February 2004) 246–251 ISBN 0-7695-2085-5.
10. Popp, T., Mangard, S.: Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints. In Rao, J.R., Sunar, B., eds.: Cryptographic Hardware and Embedded Systems – CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings. Volume 3659 of Lecture Notes in Computer Science., Springer (2005) 172–186
11. Coron, J.S., Kocher, P.C., Naccache, D.: Statistics and Secret Leakage. In Frankel, Y., ed.: Financial Cryptography, 4th International Conference, FC 2000 Anguilla, British West Indies, February 20-24, 2000, Proceedings. Volume 1962 of Lecture Notes in Computer Science., Springer (2001) 157–173
12. Shamir, A.: Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies. In Koç, Ç.K., Paar, C., eds.: Cryptographic Hardware and Embedded Systems – CHES 2000, Second International Workshop, Worcester, MA, USA, August 17-18, 2000, Proceedings. Volume 1965 of Lecture Notes in Computer Science., Springer (2000) 71–77
13. Corsonello, P., Perri, S., Margala, M.: A New Charge-Pump Based Countermeasure Against Differential Power Analysis. In: Proceedings of the 6th International Conference on ASIC (ASICON 2005). Volume 1., IEEE (2005) 66–69
14. Oren, Y., Shamir, A.: How not to protect pcs from power analysis. Rump Session, Crypto 2006 (August 2006) Available online at `http://iss.oy.ne.ro/HowNotToProtectPCsFromPowerAnalysis.pdf`.
15. Plos, T.: Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags. In Fischlin, M., ed.: Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009, Proceedings. Volume 5473 of Lecture Notes in Computer Science., Springer (April 2009) 444–458
16. Weste, N.H.E., Eshraghian, K.: Principles of CMOS VLSI Design - A Systems Perspective. 2nd edn. VLSI Systems Series. Addison-Wesley (1993) ISBN 0-201-53376-6, reprinted with corrections October 1994.
17. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In Joye, M., Quisquater, J.J., eds.: Cryptographic Hardware and Embedded

Systems – CHES 2004, 6th International Workshop, Cambridge, MA, USA, August 11-13, 2004, Proceedings. Volume 3156 of Lecture Notes in Computer Science., Springer (2004) 16–29

18. Örs, S.B., Gürkaynak, F.K., Oswald, E., Preneel, B.: Power-Analysis Attack on an ASIC AES Implementation. In: International Conference on Information Technology: Coding and Computing (ITCC 2004), April 5-7, 2004, Las Vegas, Nevada, USA, Proceedings. Volume 2., IEEE Computer Society (April 2004) 546–552 ISBN 0-7695-2108-8.
19. Schramm, K., Leander, G., Felke, P., Paar, C.: A Collision-Attack on AES: Combining Side Channel- and Differential-Attack. In Joye, M., Quisquater, J.J., eds.: Cryptographic Hardware and Embedded Systems – CHES 2004, 6th International Workshop, Cambridge, MA, USA, August 11-13, 2004, Proceedings. Volume 3156 of Lecture Notes in Computer Science., Springer (2004) 163–175
20. United Microelectronics Corporation: The United Microelectronics Corporation Website. `http://www.umc.com/`
21. Faraday Technology Corporation: Faraday FSA0A_C 0.18 μm ASIC Standard Cell Library (2004) Details available online at `http://www.faraday-tech.com`.
22. Mangard, S., Aigner, M., Dominikus, S.: A Highly Regular and Scalable AES Hardware Architecture. IEEE Transactions on Computers **52**(4) (April 2003) 483–491
23. Wolkerstorfer, J., Oswald, E., Lamberger, M.: An ASIC implementation of the AES SBoxes. In Preneel, B., ed.: Topics in Cryptology - CT-RSA 2002, The Cryptographers' Track at the RSA Conference 2002, San Jose, CA, USA, February 18-22, 2002, Proceedings. Volume 2271 of Lecture Notes in Computer Science., Springer (2002) 67–78