Test Apparatus for Side-Channel Resistance Compliance Testing

Michael Hutter, Mario Kirschbaum, Thomas Plos, and Jörn-Marc Schmidt

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{mhutter,mkirschbaum,tplos,jschmidt}@iaik.tugraz.at

Abstract. A way to classify the security level of a cryptographic device is to estimate the effort an adversary has to invest in an attack to be successful. While there are metrics and mathematical models to determine the complexity of attacks on cryptographic algorithms and protocols, estimating the security level of an implementation is more complicated. This is because attacks on the implementation depend on a variety of parameters: the expertise of the adversary, the equipment that is available, the knowledge about the implementation, and the individual information leakage of the device. In this paper, we propose a low cost test apparatus that allows amplifying the side-channel leakage by using a second device for noise cancelation. This technique improves the quality of side-channel measurements even without detailed knowledge and control over the reference device. We evaluated our idea by designing and evaluating three different apparatus each using two cryptographic devices. We achieved a side-channel leakage improvement between 20 and 220 % compared to a classical side-channel attack setup using only one device. The number of needed traces is reduced by a factor of 10 which not only minimizes the effort in evaluating the side-channel resistance of countermeasure-enabled devices but also helps in performing efficient attacks in practice.

Keywords: Non-Invasive Attack Setup, Test Methods, Side-Channel Resistance, DPA, SPA, DEMA.

1 Introduction

For security-related applications, it is vital that every part of the system can guarantee a defined security level. This holds especially true for the cryptographic modules of the applications. In order to evaluate the security of those cryptographic modules, the Cryptographic Module Validation Program (CMVP), which has been initiated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE), released the Federal Information Processing Standard (FIPS) 140-2 in 2001 [10]. The standard includes the validation of cryptographic implementations and defines various security requirements regarding physical security, operational environment, key management, electromagnetic interferences, self tests, and design assurance.

NIST (Ed.): The Non-Invasive Attack Testing Workshop – NIAT 2011, 2011.
Online available at http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/

However, side-channel security requirements are not sufficiently covered by the standard so far.

In this paper, we want to contribute to close this gap by proposing a test apparatus for side-channel resistance testing and by describing an evaluation technique for repeatable and reliable side-channel analysis. Our setup is based on the idea of a bridge circuit (Helmholtz arrangement) defined in the ISO/IEC 10373 standard for compliance testing of identification cards [5,6]. The idea is to make use of two equal cryptographic modules and to measure the difference of their physical characteristics (*e.g.* the power consumption or the electromagnetic emanation). If both modules process the same cryptographic operation, their physical characteristics are the same so that the difference of both side-channel measurements becomes theoretically zero. However, if one module processes different data than the other module, a difference in both measurements can be observed at locations in time when data-dependent information is processed. The difference of both side channels therefore provides only data-dependent signals and eliminates uninteresting static and (non data-dependent) dynamic signals (*i.e.* noise). Hence, the quality of the measurements can be significantly improved which helps in further evaluation.

In order to perform side-channel analysis using our test apparatus, we discuss two different scenarios: (1) a test measurement under the assumption that the implementation and the used secret key are known (white-box scenario), and (2) an attack where the implementation is known but the secret key is unknown in which case a black box is used as reference device. For both scenarios, the results show a significant improvement compared to a classical Differential (or Correlation based) Power Analysis (DPA) attack [7,8] setup that uses only one device under attack. To evaluate the performance of our setup, we designed three evaluation boards where each board uses two devices (the AT89S8253 microcontroller, the ATmega128, and a custom 8051 ASIC design). We performed attacks on these devices and achieved a side-channel leakage improvement between 20 and 220 %. Compared to a classical side-channel attack setup, up to 10 % less traces are necessary in order to succeed an attack. The results are especially interesting for evaluating countermeasure implementations where a huge amount of traces is necessary.

The rest of this paper is organized as follows. In Section 2 we describe related work on that topic. Section 3 gives a brief overview on side-channel measurements and describes how to improve the signal-to-noise ratio. Furthermore, we present the new measurement apparatus and present three evaluation boards in Section 4. Section 5 describes the performed attacks. Results are given in Section 6. Conclusions are drawn in Section 7.

2 Related Work

There exist several side-channel analysis (SCA) measurement boards as well as SCA simulation tools and evaluation setups. SCA measurement boards aim to provide a common attack platform that eases the comparison of measurement re-

sults. Well-known attack platforms for SCA evaluation are the INSTAC boards from the Tamper-resistance Standardization Research Committee (TSRC) [9] and the SASEBO boards from the Research Center for Information Security (RCIS) and Tohoku University [15]. The TSRC has released two boards, the INSTAC-8 with an 8-bit microcontroller and the INSTAC-32 with a 32-bit microcontroller and an FPGA. From the SASEBO boards there exist a variety of different evaluation platforms that contain Xilinx (SASEBO, SASEBO-G, SASEBO-GII) or Altera (SASEBO-B) FPGAs. The boards contain two FPGAs, one for the implementation of the cryptographic algorithm and one for handling control tasks. Since the FPGAs have processor cores integrated (powerPC processor cores), both hardware and software implementations can be evaluated with theses boards.

An SCA simulation tool has been presented by the Eindhoven University of Technology. The tool is called PINPAS and allows analyzing the vulnerability of software algorithms against SCA attacks [4]. PINPAS consists of two parts: a simulator and an analyzer. The simulator executes the assembler program that contains the algorithm implementation and generates simulated power traces. The analyzer is used to conduct SCA attacks on the simulated power traces. The advantage of simulated power traces is that they require no physical devices and that they are free from surrounding noise.

SCA evaluation setups are provided by companies like Cryptography Research (DPA Workstation [3]), Riscure (Inspector [14]), and Brightsight (Sideways [2]). The setups allow analyzing the vulnerability of cryptographic devices against SCA attacks in a comprehensive and reliable manner. All steps that are necessary for an SCA attack are covered by the evaluation setups, such as measuring the side-channel data (power consumption or EM emissions), performing filtering and preprocessing steps, and analyzing the gathered data. Often, special measurement hardware is included that speeds up the data collection [3], or micropositioners are provided to determine the optimal attack location of a device [14].

3 The Measurement of Side-Channel Information

The measurement of side-channel information involves various signals. Besides signals that are caused by the execution of an operation or due to data-dependent variations, there exist signals that are caused due to different kinds of noise. Noise is produced by the equipment itself (e.g. quantization noise of the digital oscilloscope, an unstable clock generator, glitches and variations in the power supply, etc.), by the device (switching noise or noise due to leakage currents), or by the proximity (radiated or conducted emissions, cosmic radiation, etc.). The higher the noise, the lower the measured side-channel leakage will be and the more traces have to be acquired to perform a successful side-channel attack. The signal-to-noise ratio is an ideal measure to characterize the side-channel leakage of cryptographic devices. It is the ratio between the (data-dependent) signal and the noise component of a measurement [8].

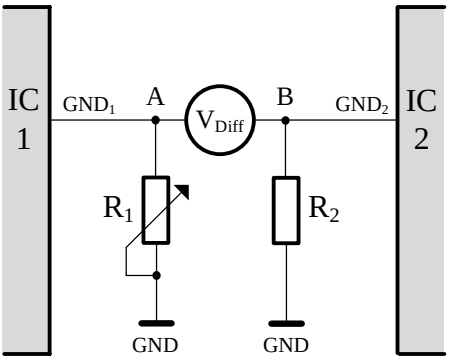

Fig. 1. Schematic of proposed apparatus.

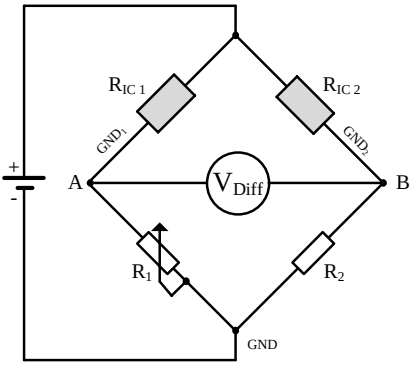

Fig. 2. Schematic of a Wheatstone bridge.

In the following, we propose a side-channel measurement apparatus that can be used to increase the signal-to-noise ratio of side-channel measurements. The idea is to exploit the side-channel information of two cryptographic devices at once by subtracting the obtained side-channel information. This significantly reduces the noise factor and increases the sensitivity of the performed measurements.

3.1 The Proposed Measurement Apparatus

Figure 1 shows the schematic of the proposed apparatus. It consists of two cryptographic Integrated Circuits (ICs) (IC_1 on the left side and IC_2 on the right side of the figure). In the ground line of each IC (GND_1 and GND_2) a resistor is placed that allows the measurement of the voltage drop across the resistors (which is typically the case in classical side-channel attack setups).

In contrast to classical setups, we propose to measure the voltage difference of both ICs, *i.e.* V_{Diff} in Figure 1. This can be simply done by using a differential probe which in fact implicitly subtracts the side-channel leakage of both devices and allows the efficient acquisition of their side-channel leakage difference.

In view of electrical metrology, the apparatus actually equals to a bridge circuit which can be used to accurately measure very small variations of two circuit branches. Figure 2 shows the schematic of a Wheatstone bridge. The dynamic resistance R_{IC_1} of IC_1 and R_1 form one branch and the resistance R_{IC_2} of IC_2 and R_2 represent the other branch of the bridge circuit. Both branches are connected over a "measurement bridge" between the points A and B.

The bridge can be manually balanced by varying the resistor R_1. It is balanced if a zero value is measured at V_{Diff} which means that the same amount of current flows through the branch $R_{IC_1} + R_1$ and through the second branch $R_{IC_2} + R_2$. Note that the voltage at point A is proportional to the ratio $\frac{R_{IC_1}}{R_1}$ and it is $\frac{R_{IC_2}}{R_2}$ at the point B.

If both ICs process different data, the apparatus becomes unbalanced. Then, the measured voltage difference (or offset) V_{Diff} is proportional to the side-channel leakage which is of interest for an evaluator or an attacker.

3.2 What are the Advantages of the Proposed Apparatus?

Compared to a classical power-analysis attack setup where the power consumption is measured over a resistor of a single device, the proposed apparatus provides two major advantages:

1. **Higher measurement sensitivity.** Since only the difference of both side-channel information is measured, a higher measurement sensitivity is obtained. This results in a higher y-coordinate resolution during signal acquisition. We achieved a signal amplification by a factor of up to 5.5 in our experiments, cf. Section 6.
2. **Reduction of noise.** Constant and static power consumption (*e.g.* the clock signal or non data-dependent operations) are canceled out by the apparatus. Furthermore, noise from the proximity is canceled out since both devices are exposed to the same noise level of the environment. This results in a higher signal-to-noise ratio of the measurement.

3.3 Measurement Procedure

In order to perform side-channel measurements using the apparatus, we propose the following three steps:

Step 1: Calibrate the apparatus. Both ICs have to execute the same operations and the same data has to be processed (*e.g.* zero values). The resistor R_1 has to be adjusted to balance the apparatus until a minimum voltage offset V_{Diff} is measured using a differential probe connected to a digital oscilloscope. Figure 3 shows the result of the calibration step. In the upper plot of the figure, the power-consumption of IC_1 (drawn in black) and IC_2 (drawn in gray) is shown processing the same operation. For this, we measured the voltage drop over the resistors R_1 and R_2 in parallel. The lower plot shows the difference signal of both devices captured at the differential point V_{Diff}. Note that the power level is much lower (up to a factor of 5.5 in our experiments) and that the same signals (*e.g.* the clock signal or the signal between 200 and 300 ns) are nearly canceled out due to the signal subtraction.

Step 2: Identify the highest signal difference. One IC has to be fed with zero input values and the other IC with the highest possible Hamming weight[1]. This causes the bridge to become unbalanced and a significant voltage difference V_{Diff} can be measured using a digital oscilloscope. Adjust the

[1] For simplicity reasons we assume a cryptographic device that provides a side-channel leakage according to the Hamming-weight power model.

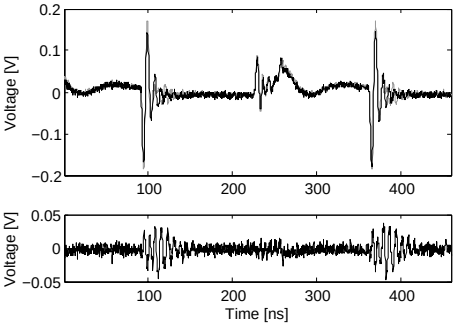

Fig. 3. Subtraction of nearly equal side-channel leakage signals.

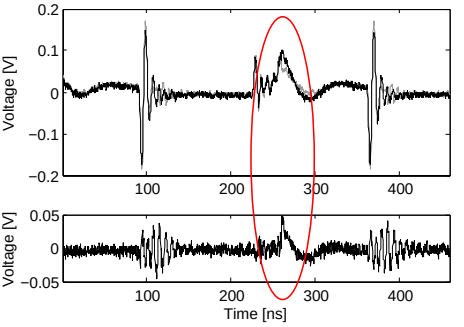

Fig. 4. Subtraction of different side-channel leakage signals.

y-coordinate resolution of the oscilloscope to an optimum, *i.e.* the difference of both side-channel signals should be measured with highest possible resolution. Figure 4 shows the result of Step 2. The different power traces are shown in the upper plot. In the lower plot, a peak can be discerned at the location in time when different data is processed by the devices.

Step 3: Perform a white-box or black-box analysis. The description of the proposed analyses is given in Section 5.

3.4 The ISO/IEC 10373-6/7 Test Apparatus

The proposed apparatus is similar to the test-method setup for compliance testing of identification cards specified in the ISO/IEC 10373-6 [5] (for proximity cards) or 10373-7 [6] (for vicinity cards) standard. Figure 5 shows a picture of the apparatus. It consists of a Radio-Frequency Identification (RFID) reader antenna in the middle of the setup and two so-called sense coils. The sense coils have the same distance to the reader antenna so that they measure the same signals emitted by the reader. Both sense coils are connected such that the signal from one coil is in phase opposition to the other coil. This theoretically cancels out the signal of the reader and allows the detection of load modulation signals of contactless identification cards (which are in fact much weaker than the RFID reader field).

4 Evaluation Boards

In the following, we describe three different evaluation boards that have been used to evaluate the efficiency of our proposed apparatus. Each board contains two equal ICs that allow the measurement of side-channel leakage differences. We used the following processors: an 8051-compatible microcontroller (the AT89S8253 from Atmel), the ATmega128, and an 8051 microcontroller that has

Fig. 5. The test apparatus according to the ISO/IEC 10373-6 standard [5].

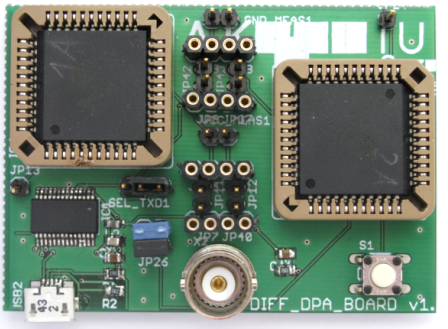

Fig. 6. The AT89S8253 evaluation board.

been incorporated in an ASIC design fabricated as a prototype chip presented in [11,12].

Figure 6 shows a picture of the AT89S8253 board. It consists of two 8051 microcontrollers, a USB connector, an FTDI controller, a BNC clock connector, a reset switch, debug pins, and sockets for measurement resistors (for the VDD as well as the GND line) and for a differential probe. Both ICs are connected to the same clock source and the wires have been routed in a way so that both wires provide the same length to avoid timing differences. The ICs are connected to an USB-to-serial FTDI controller to allow the control using a PC. The receive (RX) line of the serial FTDI interface is connected to both devices. The transmit (TX) line can be chosen by setting a jumper, *i.e.* either IC_1 or IC_2 transmits data.

Figure 7 shows the ATmega128 evaluation board using two ATmega128 microcontrollers. The schematic and layout are similar to the AT89S8253 board but assemble also two JTAG interfaces in order to allow the programming and debugging of both devices.

Figure 8 shows the evaluation board operating two of our ASIC prototype chips. The prototype chip is the result of an Austrian Government funded project called GRANDESCA[2]. Similar to our other two boards, this board contains the same basic components, *i.e.* an FTDI controller and some I/O pins for communicating with the devices. The board additionally contains voltage regulators for providing the appropriate I/O and core voltages for the chips. The board allows to measure the core power consumption over a measurement resistor either in the VDD or in the GND line.

Each GRANDESCA prototype chip contains an 8051-compatible microcontroller with an AES coprocessor implemented in CMOS logic and in an improved version of the Masked Dual-Rail Precharge Logic (iMDPL) as presented

[2] The GRANDESCA project has been supported by the Austrian research program FIT-IT Trust in IT Systems (project number 813434).

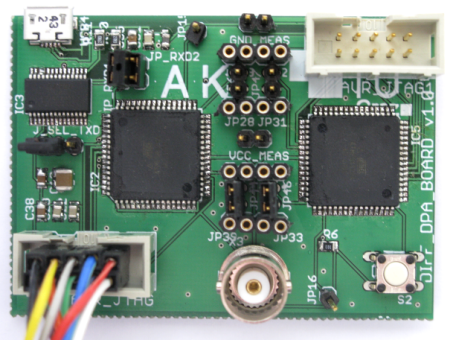

Fig. 7. The ATmega128 evaluation board.

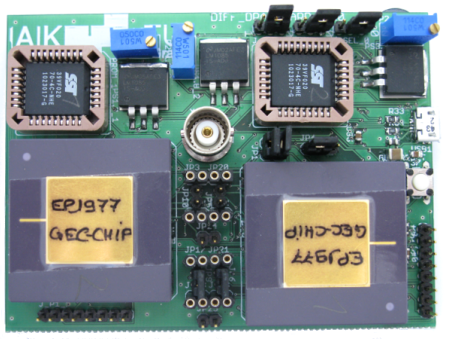

Fig. 8. The GRANDESCA-chip evaluation board.

in [12,13]. The board contains two ROMs for storing the programs executed in the microcontroller cores and jumpers for selecting the active core on the chip.

5 Description of the Attacks

We consider two attack scenarios: a *white-box* scenario and a *black-box* scenario. In the white-box scenario, the targeted intermediate value is known by the attacker. This scenario is, for example, realistic in side-channel resistance evaluation or compliance testing of cryptographic implementations. For both devices, the input and the secret key can be chosen by the attacker. In the black-box scenario, the targeted intermediate value is not known by the attacker. This scenario is given, for example, in the case where an adversary tries to reveal secret-key information from a cryptographic device. In this case the implementation of one device is unknown, whereas the other device can be fully controlled and programmed by the attacker.

As a target of the attacks within the white-box scenario, we considered the output of a `MOV` operation (the input byte is moved from memory to a working register of the CPU). Note that this or similar memory operations are also performed in implementations of cryptographic algorithms such as DES or AES, *e.g.* moving the S-box output byte after the first round of AES from a register to the RAM. For the black-box scenario, we targeted an AES hardware implementation.

All boards have been connected to a PC that runs Matlab [16] in order to control the entire measurement setup. The PC transmits three bytes over the serial connection to both ICs that are assembled on each board. IC_1 listens to the first byte, IC_2 listens to the second byte, and the last byte starts the operation on both ICs.

The power consumption of the ICs has been measured using the 2.5 GHz LeCroy WavePro 725Zi 8-bit digital-storage oscilloscope. For all experiments, we used a sampling rate of 5 GS/s. Each IC has been further programmed to pull

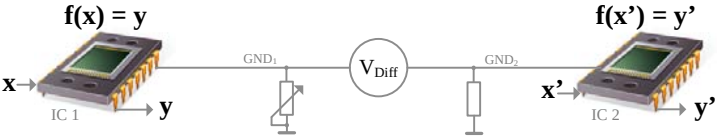

Fig. 9. The processing of different input data x and x' causes a voltage difference between both ICs which can be exploited in a side-channel attack.

a debug pin to high which triggers the oscilloscope and starts the measurement process.

5.1 The White-Box Scenario

For each board, we performed two attacks. The first attack performs a classical CPA attack on one cryptographic device. The result of the attack is used as a reference for the following investigations. The second attack subtracts the side-channel leakage of two devices. This results in a higher signal-to-noise ratio.

1. Reference attack. As a first attack, we performed a classical Correlation Power Analysis (CPA) attack [1] on one IC of each apparatus. In this scenario, the measured power consumption consists of a operation-dependent part P_{op}, a data-dependent part P_{data}, noise from the proximity $P_{prox.noise}$, and noise caused by the device itself, *i.e.* $P_{dev.noise}$ (see [8] for a detailed description of power-trace characterization). The measured power consumption P_{meas} can therefore be modeled as a sum of those components, *i.e.*

$$P_{meas} = P_{op} + P_{data} + P_{prox.noise} + P_{dev.noise}. \tag{1}$$

For the side-channel measurement, the second IC of the board has been disabled using a jumper in the power-supply lines. For the AT89S8253 and ATmega128, we used a 3.9 Ω resistor in the ground line of IC_1 and IC_2 and measured the voltage drop across that resistor. The measurements of the prototype GRANDESCA chips were performed using a 15 Ω resistor in the VDD line of each chip.

2. Difference attack. In this attack, we subtract the power-consumption of two ICs. For this, both ICs perform the same operation f but they are fed with different input values x and x'. Figure 9 shows a schematic of that setup. IC_1 processes random input values x and IC_2 processes input values x' such that the targeted intermediate value y' provides the maximum Hamming distance to y. This actually corresponds to flipping all bits of the intermediate value y or to perform a XOR operation of y with 255. For example, if the output byte y of IC_1 is 3 (0x03), the output byte y' of IC_2 is 252 (0xFC).

The measured power consumption can then be modeled as follows:

$$\begin{aligned} P_{meas} &= P_{op1} + P_{data1} + P_{prox.noise1} + P_{dev.noise1} - \\ &\quad (P_{op2} + P_{data2} + P_{prox.noise2} + P_{dev.noise2}) \\ &= (P_{data1} - P_{data2}) + (P_{dev.noise1} - P_{dev.noise2}). \end{aligned} \tag{2}$$

Since both devices process the same operation, P_{op1} and P_{op2} are equal and are therefore canceled out by the apparatus. The same holds true for the noise $P_{prox.noise1}$ and $P_{prox.noise2}$ that is caused by the proximity and that influences both devices with the same signal strength. Thus, the remaining power consumption consists of the difference of their data-dependent components $P_{data1} - P_{data2}$ as well as the difference of their electronic noise, *i.e.* $P_{dev.noise1} - P_{dev.noise2}$.

For the side-channel measurement, we used an active differential probe to measure the difference of both side channels. For this, we used the LeCroy D320 WaveLink Differential probe with 3.5 GHz bandwidth.

Processor Synchronization. In practice, both ICs are usually not synchronized and their trigger signals occur at different points in time. This is because both ICs are not powered up perfectly in parallel which causes one IC to get clocked earlier or later than the other IC. In addition, both ICs provide slightly different characteristics (power consumption, timing, etc.) which is due to variations in the fabrication process of the ICs. In order to minimize the differences, we recommend to use only ICs which provide at least the same revision number, production line, and year/month of fabrication.

In order to synchronize the two ICs, we need to reset and power up the boards until they are synchronized (try and error). For example, for the 8051 microcontroller AT89S8253 the probability of synchronization is 1/24 since the processor requires 12 clock cycles (so-called T-states) to execute a single machine cycle.

5.2 The Black-Box Scenario

We also performed a black-box attack on the AES coprocessor implemented in CMOS logic on our GRANDESCA prototype chip. For this scenario, we assume an attacker knows the implementation but does not possess the secret key used by the device. Similar to the white-box scenario, we first performed a reference attack and then we performed an attack that exploits the side-channel difference of two devices.

1. Reference attack. For the reference attack, we measured the power consumption of a single chip (IC_1) during the execution of AES encryptions of a known plaintext. We performed a standard CPA attack on the AES coprocessor based on the Hamming distance (HD) of two consecutively processed S-box outputs in the IC_1. Note that the device leaks the Hamming distance (HD) instead of the Hamming weight of the intermediate values.

Table 1. Correlation coefficient of performed attacks for every measurement apparatus.

	AT89S8253	**ATmega128**	**8051 GRANDESCA**	
			CMOS	**iMDPL**
Reference Attack	0.83	0.67	0.11	0.05
Difference Attack	0.99	0.96	0.22	0.16
Improvement	**0.16**	**0.29**	**0.11**	**0.11**
Improvement [%]	**20**	**43**	**100**	**220**

2. Difference attack. For the second attack, the power consumption of IC_1 and IC_2 is subtracted. IC_1 performs the same operation as in the reference attack, *i.e.* AES encryptions of known random plaintext. IC_2, in contrast, is fed with a constant plaintext. In our case, we set all bytes of the secret key stored in IC_2 to the value 82 (0x52). Moreover, the plaintext of IC_2 was chosen to be a zero value (0x00). This way, the output of the S-box transformation in the first round of AES was constantly 0. Also in this case, our CPA attack was based on the HD of two S-box outputs processed by IC_1.

6 Results

This section presents the results of the performed attacks. First, we present the results of the white-box scenario targeting a simple `MOV` operation. Second, we present the result of a black-box scenario targeting an AES implementation of the GRANDESCA chip. All boards have been clocked at a frequency of 3.6864 MHz. As a side-channel distinguisher, we have chosen the Pearson correlation coefficient.

6.1 White-Box Evaluation Results

Table 1 shows the correlation coefficient for each measurement apparatus and for each attacking scenario. For the AT89S8253 and ATmega128, we used 1 000 traces to perform the analysis. 5 000 traces have been measured for the CMOS core of the GRANDESCA chip and 10 000 traces have been measured for the iMDPL core.

For the AT89S8253, the apparatus provided an improvement of about 20 % compared to a classical CPA-attack setup. The correlation coefficient increased from 0.83 to 0.99 in our experiment. The y-coordinate resolution of the oscilloscope was increased from 55 mV/DIV (for the reference attack) to 10 mV/DIV (for the difference attack) which is a factor of 5.5.

Figure 10 presents the results of a CPA attack that has been performed on one ATmega128 microcontroller (reference attack). It shows two correlation peaks (two because the intermediate value has been moved two times in our implementation). The peaks occur between the second and fourth microsecond after the

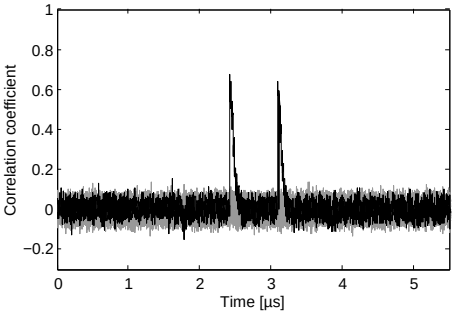

Fig. 10. Result of a classical CPA attack on one ATmega128 device (reference attack).

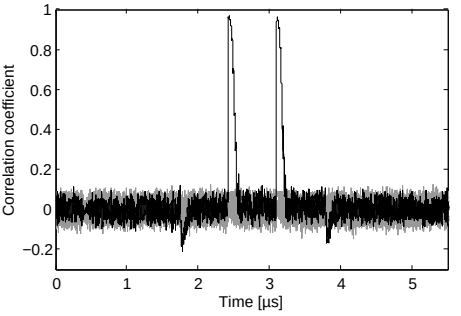

Fig. 11. Result of a CPA attack that exploits the difference of two side channels (difference attack).

trigger signal. The maximum absolute correlation coefficient is 0.67 for the correct intermediate value guess (trace plotted in black). All other incorrect guesses show no significant correlation (traces plotted in gray). Figure 11 shows the result of the CPA attack performed on the difference signal of both side channels. For the correct intermediate guess, a correlation of 0.96 has been obtained while no significant correlation can be discerned for incorrect guesses. Compared to the reference attack, this is an improvement of about 40 % (in terms of correlation coefficient). In view of acquisition resolution, an improvement of factor 5 could be achieved (from 50 mV/DIV to 10 mV/DIV). The number of needed traces to succeed an attack is therefore decreased from about 2 300 traces to only 580 (factor 8).

The attacks on the GRANDESCA chip also resulted in a higher correlation coefficient. For both the CMOS and the iMDPL implementation, an improvement of 0.11 could be achieved. The improvement for the CMOS core is 100 % (0.22 instead of 0.11) and 220 % (0.16 instead of 0.05) compared to the reference attack. The acquisition resolution increased by a factor of 1.9 for the CMOS (from 19 mV/DIV to 10 mV/DIV) and by 2.8 for the iMDPL core (from 28 mV/DIV to 10 mV/DIV). The number of needed traces to succeed an attack on this device is therefore decreased from 10 000 traces to only 1 000 (factor 10).

6.2 Black-Box Evaluation Results

An excerpt of the results of the black-box CPA attacks on the GRANDESCA AES coprocessor implemented in CMOS logic are shown in Table 2. The table compares the results of the reference CPA attack on one single AES coprocessor (reference attack) with the CPA results obtained from measuring the difference of the side-channel leakages in case the second chip always computes 0 (0x00) at the S-box output in the first round of the AES encryption. We targeted 8 byte transitions in the AES State and measured 200 000 power traces for the analyses.

Table 2. Summary of the CPA attacks on the AES coprocessor in the prototype chip implemented in CMOS logic; Hamming-distance power model.

	GRANDESCA AES COPROCESSOR CMOS							
Byte transition[a]	$2 \rightarrow 1$	$3 \rightarrow 2$	$4 \rightarrow 3$	$16 \rightarrow 4$	$1 \rightarrow 5$	$11 \rightarrow 6$	$3 \rightarrow 7$	$4 \rightarrow 8$
Reference attack	0.0174	0.0163	0.0164	0.0315	0.0133	0.0170	0.0155	0.0292
Difference attack	0.0226	0.0239	0.0278	0.0436	0.0223	0.0293	0.0267	0.0466
Improvement	**0.0052**	**0.0076**	**0.0114**	**0.0121**	**0.009**	**0.0123**	**0.0112**	**0.0174**
Improvement [%]	**30**	**46**	**69**	**38**	**67**	**72**	**72**	**59**

[a] The byte transitions of the AES State implemented in the GRANDESCA chip (see [12,13] for a detailed description of the hardware architecture).

The result shows that the apparatus is able to improve the correlation coefficients between 30 % and 72 %. In five of the eight attacks, the correlation coefficient could be increased by more than 50 %. For the best attack, this means that 33 000 traces instead of about 97 000 traces have to be measured to succeed the attack which corresponds to a trace reduction of nearly 3.

7 Conclusion

This paper presents a new test setup for side-channel measurements. It is based on using a second device for noise reduction by measuring the difference between the two devices. If both devices perform the same operation with different data, the static and the data-independent dynamic power leakage cancel out. In the resulting power trace, only the data-dependent part is left. This effect can be amplified by choosing the intermediates of the two devices to have a large Hamming distance. Compared to a classical CPA-attack setup using only one device, up to a factor of 10 less power traces are necessary to perform a successful side-channel attack.

Acknowledgements. The work has been supported by the European Commission through the ICT program under contract ICT-SEC-2009-5-258754 (Tamper Resistant Sensor Node - TAMPRES) and by Austrian Science Fund (FWF) under grant number P22241-N23.

References

1. 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, 6th International Workshop, Cambridge, MA, USA, August 11-13. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
2. Brightsight: Unique Tools from the Security Lab. http://www.brightsight.com/documents/marcom-materials/Brightsight_Tools.pdf

3. Cryptography Research: DPA Workstation. http://www.cryptography.com/technology/dpa-workstation.html
4. den Hartog, J., Verschuren, de Vink, E., de Vos, J., Wiersma, W.: PINPAS: A Tool for Power Analysis of Smartcards. In: International Conference on Information Security – SEC, Athens, Greece, May 26-28. pp. 453–457. LNCS, Springer, Heidelberg (2003)
5. International Organisation for Standardization (ISO): ISO/IEC 10373-6: Identification cards - Test methods – Part 6: Proximity cards (2001)
6. International Organisation for Standardization (ISO): ISO/IEC 10373-7: Identification cards - Test methods – Part 7: Vicinity cards (2001)
7. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) 19th Annual International Cryptology Conference – CRYPTO, Santa Barbara, CA, USA, August 15-19. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
8. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
9. Matsumoto, T., Kawamura, S., Fujisaki, K., Torii, N., Ishida, S., Tsunoo, Y., Saeki, M., Yamagishi, A.: Tamper-Resistance Standardization Research Committee Report. The 2006 Symposium on Cryptography and Information Security
10. National Institute of Standards and Technology (NIST): FIPS PUB 140-2: Security Requirements for Cryptographic Modules (2001), http://www.itl.nist.gov/fipspubs/
11. Popp, T., Kirschbaum, M., Mangard, S.: Practical Attacks on Masked Hardware. In: Fischlin, M. (ed.) Topics in Cryptology – CT-RSA, San Francisco, CA, USA, April 20-24. LNCS, vol. 5473, pp. 211–225. Springer, Heidelberg (April 2009)
12. Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In: Paillier, P., Verbauwhede, I. (eds.) Cryptographic Hardware and Embedded Systems – CHES, 9th International Workshop, Vienna, Austria, September 10-13. LNCS, vol. 4727, pp. 81–94. Springer, Heidelberg (September 2007)
13. 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, 7th International Workshop, Edinburgh, UK, August 29 - September 1. LNCS, vol. 3659, pp. 172–186. Springer, Heidelberg (2005)
14. Riscure: Inspector – The Side-Channel Test Tool. http://www.riscure.com/fileadmin/images/Docs/Inspector_brochure.pdf
15. Side-Channel Attack Standard Evaluation Board: The SASEBO Website. http://staff.aist.go.jp/akashi.satoh/SASEBO/en/index.html
16. The Mathworks: MATLAB - The Language of Technical Computing. http://www.mathworks.com/products/matlab/