Enhancing Side-Channel Analysis with Low-Cost Shielding Techniques

Thomas Plos, Michael Hutter, and Christoph Herbst

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{Thomas.Plos, Michael.Hutter, Christoph.Herbst}@iaik.tugraz.at

Abstract

Side-channel analysis (SCA) attacks are a powerful technique to reveal secrets of cryptographic devices due to implementation weaknesses. In order to make SCA less effective, countermeasures are integrated in cryptographic devices. In this work, we have built a low-cost shielding device to enhance SCA measurements. Our objectives have been to reduce the impact of noise that is typically caused by surrounding electromagnetic (EM) radiations. The number of traces in EM measurements that are needed to succeed an attack has been lowered significantly from 70 000 to 17 500. Our shielding device suppresses signals up to several GHz while its development costs lie below 300 €.

Keywords: *Side-Channel Analysis, Differential Power Analysis, Differential Electromagnetic Analysis, Low-Cost Shielding Device, Electromagnetic Radiation*

1 Introduction

The trend of processing and distributing data in electronic form is driven by the rapid advances in microelectronics and network technology. It is clear that with the rising amount of data also the quantity of sensitive data increases. One of the most challenging problems is security. Cryptographic algorithms are an indispensable tool to guarantee authenticity, secrecy, and integrity for digital data. A basic concept of cryptographic algorithms is the fact that their security depends on the secrecy of a so-called key which is only known by entitled parties. Modern cryptographic algorithms are designed in a way so that an attacker can not compromise the key by observing input and output of the algorithm.

In practice, cryptographic algorithms have to be implemented on a physical device which also stores the key. Examples for such devices are PCs, smart cards, embedded systems or microcontrollers. Even if the algorithms themselves are considered to be secure, the implementations could be vulnerable to so-called implementation attacks. Besides fault attacks [2, 3], side-channel attacks are a very important type of implementation attacks. Side-channel attacks exploit that cryptographic devices emit physical information which could depend on the secret data. Such physical side channels are for instance power consumption, electromagnetic emanation, or the time to process the algorithm. First results of using the timing information to extract the key of an RSA [9] implementation have been published in [5]. Power analysis attacks—first introduced by Kocher [6]—have proven to be a very powerful type of side-channel attacks. The same dependency of the emitted information on the secret key as in power analysis attacks, can be observed in the electromagnetic (EM) emanation. This has been shown by Agrawal et al. in [1] and Gandolfi et al. in [4].

The principle of power and EM attacks is the same. They only differ in the observed property. In the following, we will concentrate on EM attacks. To mount a successful attack, an adversary has to measure the electromagnetic emissions while the device performs the cryptographic algorithm with the desired secret key. In Simple Electromagnetic Analysis (SEMA), the attacker extracts the key from a single measurement trace (i.e. by visually inspecting the trace). Whereas, in Differential Electromagnetic Analysis (DEMA) multiple traces are collected to deduce the secret key. In DEMA attacks, intermediate values of the algorithm are predicted by using a known input (plaintext) and a hypothesis for the key. With the help of an emanation model of the device, these predicted intermediate values are then transformed to a predicted emanation. In the last step, the predicted emanation is statistically compared to the measured EM emanation. The predicted emanation, which fits best, indicates the best predicted values and therefore the involved secret key. When talking about power attacks, SEMA is called Simple Power Analysis (SPA) and DEMA is called Differential Power Analysis (DPA).

Besides more sophisticated attacks, the research community also developed countermeasures. There are two basic approaches for countermeasures, namely masking and hiding [7]. The goal of masking is to brake the link between the predicted intermediate values and the values processed by the device. Hiding seeks to minimize the effect of the processed values on the emitted side channel. This means for hiding the Signal-to-Noise Ratio (SNR) is

lowered. Except for more enhanced attacks, which try to reduce the impact of the countermeasures on the attack, an adversary can try to rise the SNR. One method, which helps to rise the SNR, is shielding the measurement setup from the surrounding EM radiation.

In this article, we will show how a low-cost shielding environment can improve side-channel attacks, in particular EM side-channel attacks. We will demonstrate that we can significantly reduce the number of measurements for a successful attack. Moreover, we will present our shielding device and the development in detail.

The rest of this paper is organized as follows. Section 2 will give a basic introduction to side-channel attacks. In Section 3 the development and evaluation of our shielding box is explained. The results of attacks in a shielded versus an unshielded environment are presented in Section 4. Finally conclusions are drawn in Section 5.

2 Basics of Side-Channel Analysis

The basic idea of side-channel analysis is to deduce the secret key by observing physical properties of cryptographic devices. The most promising side channels are the power consumption and the electromagnetic emanation of such devices. DPA and DEMA attacks make use of this side channels and exploit that the power consumption of a cryptographic device depends on the data that it processes. In fact, the power characteristic differs when processing different values. By using statistical methods, the extraction of the secret key becomes possible even if the data dependency is very weak or overwhelmed by noise.

The first step in a DPA attack is to feed the cryptographic device with different input values. During the processing of the input data, power traces are measured for each calculation of the algorithm. In order to increase the measurement performance, only a small section in time is recorded. In this time, an intermediate result must be calculated by the device that depends on the secret key. Next to the acquisition of the power traces, a hypothetical model is constructed. This model is fed with the same input data as sent to the cryptographic device. The model calculates all possible intermediate results that can be processed by the device. If, for example, the intermediate result depends on 8 bits of the secret key, the model generates 256 hypothetical results. All hypothetical results are then transformed to hypothetical power-consumption values. A specific power model has to be chosen that fits best to the power consumption characteristics of the "real" device. The *Hamming-weight* or the *Hamming-distance* power model is often used in practice. In the last step of the attack, the output of the power model, which we further denote as H, is compared with the measured power traces P using statistical methods such as the correlation coefficient ρ. The correlation coefficient determines the linear relationship between the two data sets H and P. It is defined as follows:

$$\rho_{H,P} = \frac{cov(H,P)}{\sqrt{Var(H) \cdot Var(P)}}, \tag{1}$$

where cov represents the covariance. The correlation ρ, which is always between -1 and 1, indicates the degree of linear dependency between H and P. If the data dependency is high (i.e. the output of the model using the correct key hypothesis correlates with the measured power traces), the correlation ρ becomes high at a point in time when the intermediate result is processed. This indicates that the correct key hypothesis has been chosen. All other key hypotheses will have low correlations. In this way, all secret-key bytes of the cryptographic device can be revealed [7].

In general, the power consumption P of a cryptographic device is composed of several components. It can be modeled by the sum of an exploitable power consumption P_{exp}, noise P_{noise}, and a constant power consumption part P_{const}:

$$P = P_{exp} + P_{noise} + P_{const}. \tag{2}$$

The exploitable power consumption P_{exp} is caused by the processed data and thus provides side-channel information. Noise and the constant power consumption part, in contrast, do not contain exploitable information.

The SNR is a good measure to characterize the side-channel leakage of a given attack scenario. It relates the exploitable power consumption P_{exp} with the noise P_{noise} by calculating Equation 3:

$$SNR = \frac{Var(P_{exp})}{Var(P_{Noise})}. \tag{3}$$

Next, we further relate the SNR with the correlation coefficient (given in Equation 4) which leads us to the following thoughts.

$$\rho(H,P) = \frac{\rho(H,P_{exp})}{\sqrt{1+\frac{1}{SNR}}} \tag{4}$$

First, the SNR and the correlation are proportional to each other. Increasing the SNR will increase the correlation as well. This is important to succeed an attack especially for devices which have a low exploitable power consumption (e.g. devices which include side-channel countermeasures). Second, in order to increase the SNR, the noise component of the measurement setup has to be decreased. This can be done, for example, by filtering or shielding techniques. In this article, we have focused on such shielding techniques by building a low-cost electromagnetic-shielding box. The box is capable of decreasing the noise of a side-channel measurement setup. It suppresses disturbing signals of the proximity which are typically present in laboratories. We show that the shielded box can be used to drastically reduce the number of needed power traces. The box is described in Section 3 while the deployed measurement setup is described in the following.

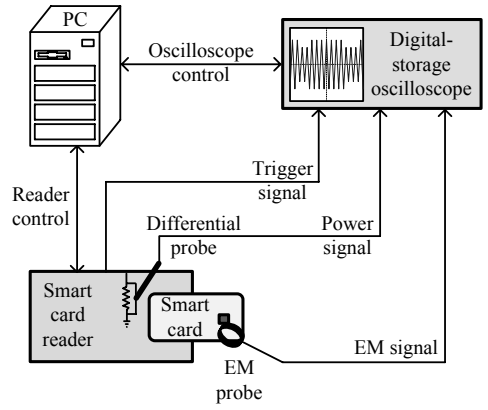

Figure 1. Schematic overview of the measurement setup used for recording power or EM traces.

The measurement setup for power and electromagnetic analysis is shown in Figure 1. It includes: a digital-storage oscilloscope, a differential probe, a self-made loop antenna, a PC, a smart card reader, and the device under attack (smart card). For DPA, a differential probe ($AP034$ from LeCroy) is placed in series to the ground line of a reader circuit to measure the power consumption of a smart card using a digital-storage oscilloscope (LeCroy $LC584AM$). For DEMA, a loop antenna is placed directly upon the reader. A standard PC controls the overall measurement process. The device under attack is a smart card including a microcontroller (ATmega163) that implements the Advanced Encryption Standard (AES) (see [8] for more details) as a cryptographic algorithm.

3 Building a Low-Cost Shielding Device

In order to lower the noise component of the measurement setup and thus to increase the SNR of the measurements, we have built an electromagnetic-shielding box. Keeping the costs of the box and the accessory materials low was an important requirement. However, the shielding box was not created within a single step but its construction was divided into several phases. After each phase, the EM spectrum was analyzed to evaluate the influence of the individual shielding steps. The EM spectrum was sensed from 150 kHz to 3 GHz by using a self-made loop antenna interlinked to a spectrum analyzer (Rhode & Schwarz *ESPI3*) via a double-shielded cable. The antenna consists of two rectangular wire loops of different size connected in parallel to make the antenna receptive for a wider frequency range. Lower parts of the EM spectrum are absorbed by the large wire loop (80 cm by 34 cm), higher parts by the small wire loop (13 cm by 5.5 cm). The DEMA attacks described in Section 2 have been performed using this antenna.

As mentioned above, the construction process of the electromagnetic-shielding box was divided into multiple phases. Altogether we decided to introduce four phases, beginning with the evaluation of the unmodified box and improving it step by step within each phase. Starting point was a metal box with a plate thickness of 2 mm, measuring 84 cm by 47 cm by 33 cm. The box has a metal cover that can be reliably closed via two spring locks. In the first phase, the box has been equipped with a BNC feed through, allowing the self-made loop antenna to be placed inside the box while the cover is actually closed. Plugging the loop antenna to the spectrum analyzer via the feed through makes it possible to compare the EM spectrum outside the box with the spectrum recorded inside the box, regardless whether the cover of the box is opened or closed. When the loop antenna is positioned on the bottom inside the box, interfering signals in the lower frequency band (up to 50 MHz) are mostly suppressed even if the cover is left open. The signals of the radio stations around 100 MHz are already attenuated by about 30 dB. Closing the cover has the effect that the radio signals are stronger suppressed and the amplitudes of the television signals around 500 MHz are lowered as well. Higher frequencies are not influenced by this first shielding step.

In the second phase, areas of the metal box that seemed to be leaky for EM signals (e.g. splices) have been abraded and sealed with adhesive copper tape. The cover of the box remained untouched. Now, if the cover of the box is closed, both radio and television signals are completely suppressed. Significant influence on signals with higher frequencies such as mobile phones was not observed.

Goal of the third phase was to improve the shielding capability of the box to get rid of further interfering signals at high frequencies. This improvement has been achieved by also abrading and sealing the cover of the box with adhesive copper tape. Additionally, a conductive sealing was glued onto the contact area between the box and the cover. The conductive sealing gets compressed when the cover is closed via the two spring locks and turns the cover and the box into a persistent conducting unit. Eliminating the last remaining source of leakage for interfering EM signals prevents them from entering the inner area of the box. Measuring the spectrum of the so finally shielded box confirms that all interfering EM signals (up to our measurement limit of 3 GHz) are now entirely suppressed. Figure 2 shows a comparison of the EM spectrum which was acquired outside the box (gray trace) and inside the box (black trace). It shows a quite good shielding property in a large frequency range. The two steps in the traces at 30 MHz and 1 GHz result from switching between different filters inside the spectrum analyzer.

Since our shielding box is used for SCA of cryptographic devices, several signals like power supply for the DUT, RS232 interface, and trigger signal have to be provided inside the box. Thus, depending on the utilized DUT and the used SCA-measurement technique (DPA attack or DEMA attack), different numbers and kinds of connectors are required. In order to remain as flexible as possible and to have only as many signal feed throughs as necessary (each additional feed through is a potential source of leakage), we added *plug panels* in the fourth

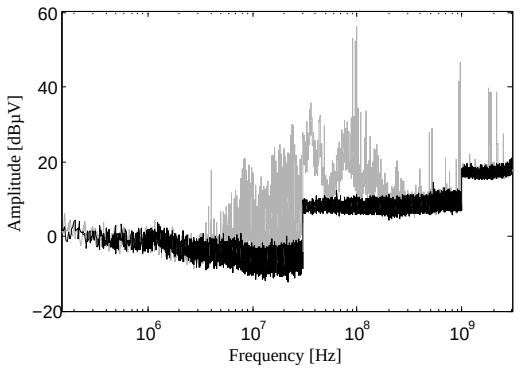

Figure 2. Comparison of the spectrum outside the shielding box (gray trace) and inside the shielding box (black trace).

Figure 3. Shielding box with utilized spectrum analyzer and DEMA/DPA measurement setup.

and last phase. For various measurement setups, specific *plug panels* have been built that contain all the required connectors. According to a specific measurement setup, the appropriate *plug panel* is selected and attached to the box. The *plug panel* is placed above a cut in the box and it is fixed with two stable metal frames and several screws. Only electromagnetic-shielded cables are used to be connected to a specific *plug panel*. Moreover, the cables are equipped with filters to prevent contact-based interferences from entering the shielded area inside the box. Analysis of the box with an attached *plug panel* pointed out that no noticeable degradation of the box's shielding capabilities compared to the third phase was detected.

We have tested the shielding effectiveness of the final box by using three explicit noise sources. The noise sources are located at: 13.56 MHz, 868 MHz, and 2.4 GHz. Comparing the spectrum measured outside the box with the one measured inside the box shows that the 13.56 MHz signal is attenuated by more than 60 dB, the 868 MHz signal by about 50 dB, and the 2.4 GHz signal by approximately 30 dB. A picture of the final box with the utilized spectrum analyzer and the DPA measurement setup, which is described in Section 2, is presented in Figure 3. Summing up all costs for building such a shielding device (the *plug panels*, the cables, the shielding material, and various consumable material), brings us to an amount of about 300 €.

4 Side-Channel Analysis Results in Shielded and Unshielded Environments

After building the measurement box and evaluating its shielding capabilities, we have tested its effectiveness for improving SCA attacks. Using the measurement setup described in Section 2, we have conducted DEMA and DPA attacks inside the shielding box and compared them against measurements outside the box in an unshielded environment. First, DEMA attacks have been carried out utilizing the self-made loop antenna to gather the emissions from the smart card. As mentioned above, the correlation coefficient ρ given by Equation 1 has been used to detect linear dependencies between the intermediate results computed by the smart card during an AES encryption, and the recorded EM traces. Since the observed intermediate results are 8-bits long, 256 hypothetical outputs are possible, whereas only one hypothesis is assumed to be correct. For all attacks, the *Hamming-weight* power model has been selected to estimate the power consumption of the smart card.

Using more measurements for computing the correlation coefficient ρ, lowers the noise and brings ρ closer to its expectation. We have acquired 100 000 EM traces for each experiment to obtain sufficiently accurate results. For the DEMA attack in an unshielded environment, the maximum absolute value of the correlation coefficient ρ for the correct hypothesis converges on 0.02. Conducting the same measurement inside the shielding box leads to a maximum absolute correlation coefficient of 0.04 which is twice as high than before. Figure 4 shows the evolution of ρ as a function of the number of recorded EM traces outside the shielding box, whereas Figure 5 illustrates the evolution of ρ when measuring inside the shielding box. In both figures the correlation coefficient associated with the correct hypothesis is printed in black, the remaining 255 incorrect hypotheses are printed in gray. It is clearly visible that ρ of the incorrect hypotheses is continuously lowered as the number of recorded EM traces increases. Consequently, after a certain number of measurements, the correlation coefficient of the correct hypothesis sticks out and is clearly distinguishable from all the incorrect hypotheses. The number of traces that needs to be acquired for such a successful attack depends on the value of ρ. As depicted in [7] a rule of thumb can be used to determine the number of traces that is approximately required for a successful attack with high probability (> 99.99%). Equation 5 illustrates the simplified relation between the required number of measurements n and the correlation coefficient ρ. This simplification only holds for small values of ρ (< 0.2) which is applicable in our case.

$$n \approx \frac{28}{\rho^2}, \quad \rho \leq 0.2 \tag{5}$$

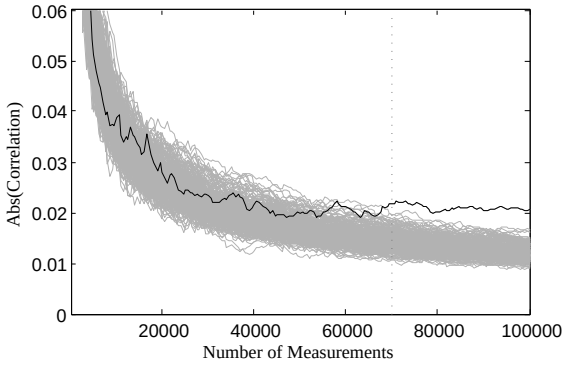

Figure 4. Evolution of the correlation coefficient as a function of the number of measurements outside the shielding box.

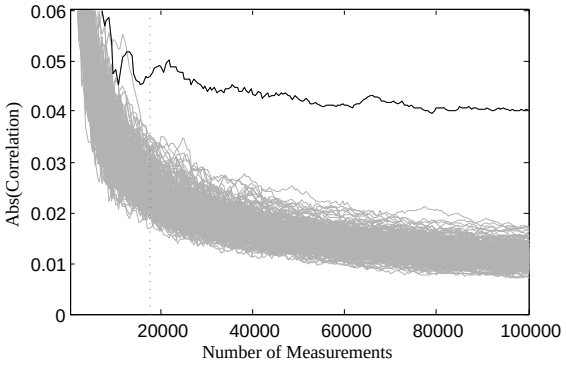

Figure 5. Evolution of the correlation coefficient as a function of the number of measurements inside the shielding box.

Entering the two correlation coefficients $\rho = 0.02$ and $\rho = 0.04$ determined during the previous DEMA attacks, leads to an estimation of the required number of measurements n of 70 000 and 17 500. The quadratic relation between ρ and n clarifies that doubling the correlation coefficient when measuring inside the shielded environment quarters the number of EM traces that needs to be recorded. Hence, the effectiveness of the DEMA attack is improved by a factor of 4. The estimated value for the required number of measurements is marked with a vertical dotted line in Figure 4 and Figure 5, illustrating that the estimations coincide quite well with the practical results.

Subsequently to the DEMA attacks, the influence of the shielding box on DPA attacks has been examined. Also for DPA attacks, the achievable correlation coefficient ρ has been increased when performing the attack inside the shielding box compared to measurements outside the shielding box (by approximately 0.01). Since for the deployed smart card, the correlation coefficient obtained via the DPA attack is much higher than with the DEMA attack, the impact of the shielding box is more or less negligible. In order to demonstrate that the shielding offers a significant benefit for DPA attacks, the usage of a cryptographic device with an integrated DPA countermeasure would be required. The correlation coefficient of such devices is innately low, effectuating that even a slight increase of ρ dramatically reduces the number of required measurements for a successful attack.

Besides a higher correlation coefficient, measuring inside a shielded environment increases the reproducibility of DEMA and DPA attacks. Reproducibility is especially a concern, if EM-noise producing equipment like switching power supplies or PCs are located in close proximity to the measurement setup. If so, DEMA or DPA attacks can be successful in one case and unsuccessful in another case. Deploying our shielding box also solves this issue.

5 Conclusion

In this work, we have shown how to build a low-cost shielding device for less than 300 € and how it can be used to enhance SCA attacks. The shielding capability of our device was evaluated up to 3 GHz, pointing out that noise sources above 2 GHz were still attenuated by more then 30 dB. Subsequently, DEMA and DPA attacks were carried out inside the shielded environment and compared against measurements outside the shielded environment. In all cases, the correlation coefficient ρ was increased by deploying our shielding device. Especially for the DEMA attacks, where the achievable correlation coefficient was innately low, the required number of EM traces for a successful attack was decreased dramatically from 70 000 to 17 500. We conclude that our low-cost shielding device is highly suitable not only for improving the effectiveness of DEMA attacks, but also for enhancing DPA attacks that are applied to cryptographic devices with integrated DPA countermeasures.

Acknowledgements.

This work has been funded by the European Commission through the IST Programme under Contract IST-FP6-033546 BRIDGE and Contract IST-FP6-034921 Collaboration@Rural, and by the Austrian Science Found (FWF) under the grant number P18321.

References

[1] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-channel(s). In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *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*, pages 29–45. Springer, 2003.

[2] Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer, 1997.

[3] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract). In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceedings*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer, 1997.

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In Çetin Kaya Koç, David Naccache, and Christof Paar, editors, *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*, pages 251–261. Springer, 2001.

[5] Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, number 1109 in Lecture Notes in Computer Science, pages 104–113. Springer, 1996.

[6] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *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*, pages 388–397. Springer, 1999.

[7] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks – Revealing the Secrets of Smart Cards*. Springer, 2007. ISBN 978-0-387-30857-9.

[8] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001. Available online at `http://www.itl.nist.gov/fipspubs/`.

[9] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. ISSN 0001-0782.