On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices

Thomas Plos, Michael Hutter, and Martin Feldhofer

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

Abstract. Security-enabled RFID tags become more and more important and integrated in our daily life. While the tags implement cryptographic algorithms that are secure in a mathematical sense, their implementation is susceptible to attacks. Physical side channels leak information about the processed secrets. This article focuses on practical analysis of electromagnetic (EM) side channels and evaluates different preprocessing techniques to increase the attacking performance. In particular, we have applied filtering and EM trace-integration techniques as well as Differential Frequency Analysis (DFA) to extract the secret key. We have investigated HF and UHF tag prototypes that implement a randomized AES implementation in software. Our experiments prove the applicability of different preprocessing techniques in a practical case study and demonstrate their efficiency on RFID devices. The results clarify that randomization as a countermeasure against side-channel attacks might be an insufficient protection for RFID tags and has to be combined with other proven countermeasure approaches.

Keywords: RFID, Differential Frequency Analysis, Side-Channel Analysis, Electromagnetic Attacks.

1 Introduction

During the last few years, Radio-Frequency Identification (RFID) has emerged from a simple identification technique to the enabler technology for buzzwords like "ambient intelligence" or the "Internet of things". Additional features like sensors and actuators allow applications in many different fields apart from supply-chain management and inventory control. Sarma *et al.* [19] have been the first who addressed the importance of security for passive RFID tags. The introduction of security allows tags to prove their identity by means of cryptographic authentication. Furthermore, privacy issues could be solved and a protected access to the tag's memory becomes possible.

In 2003, it was stated e.g. by Weis *et al.* [20] that strong cryptography is unfeasible on passive tags due to the fierce constraints concerning power consumption and chip area. Since then, many attempts have been made to implement standardized cryptographic algorithms in hardware complying with the

H.Y. Youm and M. Yung (Eds.): WISA 2009, LNCS 5932, pp. 163–177, 2009.
The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-642-10838-9_13

requirements of passive RFID tags. Among the most popular publications on that are realizations of the Advanced Encryption Standard (AES) [6], Elliptic-Curve Cryptography (ECC) [3,8], and GPS [9,15].

Unfortunately, having a crypto module of a secure algorithm in hardware on the tag is not sufficient for a secure RFID system. Due to the fact that an adversary always tries to break the weakest link in a system (and this is the RFID tag that is easily available for attacks), further attacks have to be considered. Side-channel attacks target at the implementation of a cryptographic device. They are very powerful in retrieving the secret key by measuring some physical property like power consumption, electromagnetic emanation, or timing behavior *etc.* Differential power analysis (DPA) [13] attacks and differential electromagnetic analysis (DEMA) [18,1] attacks gained a lot of attention during the last ten years.

In the findings of Hutter *et al.* [11] for HF tags as well as in the work of Oren *et al.* [16] and Plos [17] for the UHF frequency range, it has been shown that passive RFID tags are also susceptible to side-channel attacks. Even in the presence of the strong electromagnetic field of the reader DEMA attacks are possible. Hence, as far as a cryptographic algorithm is implemented on a tag, appropriate countermeasures have to be implemented. According to [14], countermeasures can principally be divided in either hiding or masking.

A very efficient way of implementing hiding, especially for low-resource devices like RFID tags, is to randomize the executing of the algorithm. This means that the performed operations of the algorithm occur at different moments in time in each execution. Randomization can be done by shuffling and by randomly inserting dummy cycles [14]. The reason why randomization is very cost efficient in terms of hardware resources is that the implementation is mainly done in the control logic. Furthermore, in RFID tags where the data rates are low, using the time domain and hence further clock cycles is convenient.

Differential Frequency Analysis (DFA)—not to confuse with differential fault analysis, which uses the same acronym—has been first mentioned by Gebotys *et al.* [7] in 2005. There, the authors successfully applied DFA to attack cryptographic algorithms running on a Personal Digital Assistant (PDA) device. The principle idea of DFA is to transform measured side-channel traces from the time domain to the frequency domain. The Fast Fourier Transform (FFT) is an operation that can be used for this transformation. Since the FFT is time-shift invariant, the time delays introduced by the side-channel analysis countermeasures are removed in the frequency domain. Further advantage of DFA especially for attacking RFID tags is that misaligned traces are of no concern. Misalignments do often occur due to the interfering reader field and difficulties in triggering appropriate events on the tag. Another approach that uses the frequency domain for handling misaligned traces has been presented by Homma *et al.* [10] in 2006. They have been able to diminish the displacement between traces by using a so-called phase-only correlation after transformation to the frequency domain.

In this work we show how DFA can be used to extract the secret key out of RFID devices that implement randomization countermeasures. We compare DFA

with preprocessing techniques such as filtering and trace integration. Commercially-available RFID tags today do not contain cryptographic algorithms with randomization countermeasures implemented. In order to perform and analyze the proposed attacks, we used semi-passive RFID-tag prototypes for HF and UHF frequency as target of evaluation. In these prototypes it is possible to implement e.g. the AES algorithm with randomization countermeasures in software. Our results show that DFA is a powerful technique, especially when analyzing the electromagnetic emanation of RFID devices.

This article is structured as follows. In Section 2, we will describe the HF and the UHF RFID-tag prototypes that have been used throughout the analysis. Section 3 provides insights about different hiding techniques that are applied in practice. Section 5 presents the design of the randomized AES implementation that has been used during the experiments. The measurement setups for the attacks will be shown in Section 6 and results are given in Section 7. The article closes with conclusions in Section 8.

2 RFID-Tag Prototype Implementation

In order to perform side-channel analysis on RFID devices, we have developed two different RFID-tag prototypes. Using prototypes provides many advantages. With the help of a prototype, new applications and protocols can be demonstrated that make an invention more informative and imaginable. Prototypes can also be used to identify weaknesses more easily by modifying and testing the device in real terms. Regarding systems where cryptography is applied, prototypes allow the analysis of side channels by measuring, for example, the electromagnetic emanation. This article focuses on such analyses by using prototypes that implement security mechanisms.

Two RFID-tag prototypes have been designed and developed. One prototype operates in the HF frequency band at 13.56 MHz and one prototype works in the UHF frequency band at 868 MHz. Both devices have been assembled using discrete components. In Figure 1, a picture of the two prototypes is shown. They principally consist of an antenna, an analog front-end, a microcontroller, a clock oscillator, a serial interface, a JTAG interface, and a power-supply connector. Both devices differ in their antenna design, the analog front-end, the clock source, and the software that runs on the microcontroller. The remaining components are the same. As a microcontroller, the ATmega128 [2] has been used, which is responsible for managing reader requests and tag responses by following the specification of the used RF communication protocol. The microcontroller is able to communicate with a PC over a serial interface. It furthermore supports In-System Programming (ISP) and has a JTAG interface for debug control and system programming. Both devices are semi-passive where the microcontroller is powered by an external power source, typically a battery, while the RF communication is done passively without any signal amplification.

In the following sections, the design of the HF and the UHF tag prototype is described in a more detail.

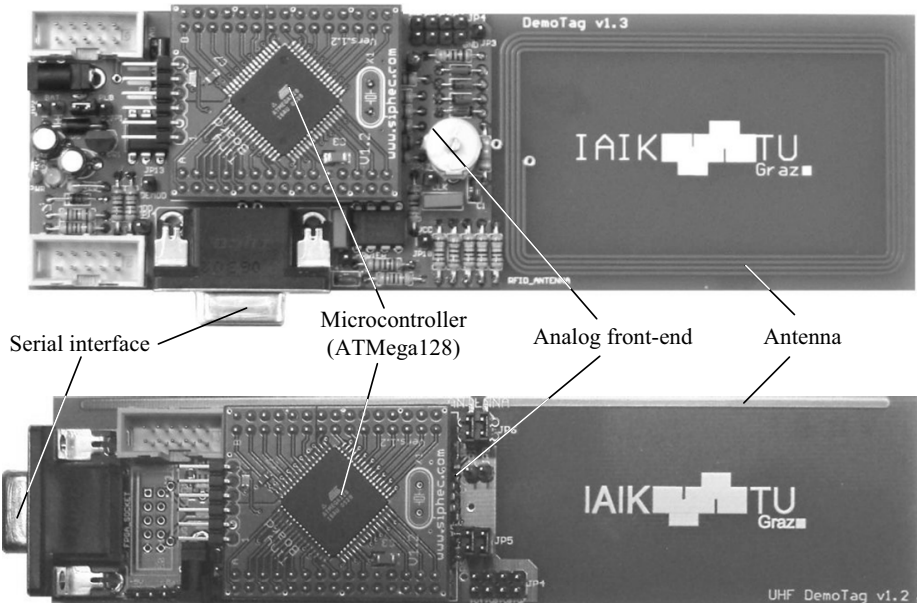

Fig. 1. Picture of the HF (top) and the UHF (bottom) tag prototype.

2.1 HF-Tag Prototype

The HF-tag prototype uses a self-made antenna according to ISO 7810. It consists of a coil with four windings that allows the communication with a reader over the air interface. The antenna is tuned to resonate at a carrier frequency of 13.56 MHz, which is realized by a matching RLC circuit. This circuit narrows the frequency range and can also be considered as a band-pass filter that passes the carrier frequency but attenuates unwanted and spurious frequencies. The matched signals are then preprocessed by an analog front-end that is used to transform the analog signals into the digital world. First, the signals are rectified using a bridge rectifier. Small-signal Shottky diodes have been assembled that provide low voltage drops and low leakage currents. Second, the voltage is regulated by a Zener diode. At the third stage, a comparator is used to identify reader modulations. The output of the comparator is then connected to the microcontroller that rises an interrupt and starts the receiving process. The microcontroller is clocked by a 13.56 MHz quartz crystal that has been assembled on board. For sending data from the tag to the reader, a load modulation circuit is available that consists of a shunt and a transistor. The microcontroller triggers the transistor that switches the shunt and thus modulates the tag response.

The tag prototype can communicate using several protocol standards. It implements ISO 15693, ISO 14443 (type A and B), ISO 14443-4 and ISO 18092. The software is written in C while parts have been implemented in assembly language due to timing constraints. Moreover, it implements a user-command interface that allows easy administration over the serial interface. For our exper-

iments, we have used the ISO 14443-A protocol standard [12] and have included some proprietary commands that implement a simple challenge-response protocol. First, the reader sends 16 bytes of plaintext to the prototype. The prototype encrypts the plaintext using the Advanced Encryption Standard (AES). Second, the reader retrieves the ciphertext and verifies the encrypted result. Furthermore, we have implemented a command to set different randomization parameters for the AES encryption. These parameters are used to randomize the encryption process that is commonly used as a countermeasure for side-channel analysis.

2.2 UHF-Tag Prototype

The second tag prototype operates in the UHF frequency band. Other than the HF-tag prototype it uses a half-wave dipole antenna consisting of two wires directly integrated to the layout of the printed circuit board (PCB). The antenna, whose length is about 150 mm, is optimized for a frequency of 868 MHz and it is connected to the analog front-end. Like for the HF-tag prototype, an adjustable capacitor is placed in parallel to its antenna. This capacitor is used for matching the antenna to the input impedance of the analog front-end. Signals that are received by the antenna are first rectified by a charge-pump rectifier. This rectifier performs demodulation and voltage multiplication all at once. Special detector diodes, which have a low voltage drop and are constructed to operate up to some GHz, are used in the rectifier circuit. Subsequently, signals are filtered and passed to a comparator before feeding them to the microcontroller. For tag-to-reader communication, a backscatter-modulation circuit is provided within the analog front-end. This circuit works similar to the one used by the HF prototype where a transistor is used to switch an impedance (shunt and capacitor) in parallel to the tag antenna. A 16 MHz quartz crystal is assembled on board in order to generate the system clock for the microcontroller.

The UHF-tag prototype supports the ISO 18000-6C standard (EPC Gen2 [5]) which is the most widespread protocol in the UHF frequency range. Implementation of the protocol is done in software on the microcontroller. The software for the UHF-tag prototype is also mainly written in C while time-critical routines are directly realized via assembly language. Also the same challenge-response protocol has been implemented that allows encryption of received data, as well as a dedicated command to adjust the parameters for the AES randomization.

3 Hiding as a Countermeasure Against Side-Channel Analysis

Hiding data-dependent information of a cryptographic device can be achieved by two different approaches. The first approach blurs the data-dependent information by varying the power-consumption characteristic in its amplitude. The second approach randomizes the execution of operations in the time dimension. However, hiding can also occur in an *unintended* manner. There, misaligned traces in the amplitude and also in the time make the analysis of side channels largely infeasible. Measurements on contactless-powered devices like RFID tags

are a typical example for this scenario where the acquired EM traces have to be aligned or preprocessed before the analysis in order to perform a successful attack. In the following, a short description of hiding in the amplitude and hiding in the time dimension is given. A more detailed description is given in [14].

3.1 Hiding in the Amplitude Dimension

In fact, the measurement of side channels that leak from RFID devices is a challenging task. RFID readers emit a very strong field in order to allow a certain reading range. This field is necessary to power the tags, to allow a communication, and in most cases also to provide a clock signal to the tags. However, the field interferes and perturbs the measurement of the weak side-channel emissions. In addition, if the reader field and the clock signal of the tag differ in their frequency, a superposition of signals can be perceived. This results in periodic rises and falls in the amplitude of the measured EM traces. Measurements on HF RFID-tag prototypes, whose clock frequency differ from 13.56 MHz, are a typical example where the reader field interferes the measurement of interesting side-channel emissions. Measurements on UHF tags are another example where they often include their own oscillators. The internal clock allows the communication with multiple reader frequencies such as used in different countries (868 MHz in Europe, 915 MHz in USA, or 950 MHz in Japan).

In contrast to these *unintended* interferences, variations in the amplitude are also often generated purposely. This has its reason in the fact, that variations in the amplitude dimension essentially lower the signal-to-noise (SNR) ratio and thus make the measurement of side channels harder to perform. This kind of hiding is commonly-used as a countermeasure against such attacks. Devices often integrate noise generators or perform several operations in parallel to increase the overall noise [21].

3.2 Hiding in the Time Dimension

Hiding can also emerge in the time dimension where traces are misaligned either in an unintended or in an intended manner. Unintended time variations often occur due to the absence of adequate trigger signals for measurement. Especially in RFID environments, triggering is often performed on the communication instead of the measured emanation. For example, the end of the last reader command before executing the targeted algorithm can be used to trigger the measurement. This trigger signal does not always appear at the same position in time which leads to misaligned traces and thus to unintended hiding.

Intended time variations are referred to hiding through randomization. There are two possibilities on how execution can be randomized. The first possibility is to insert dummy operations such as additional rounds (or only parts of it). These dummy operations can be processed before or after the execution of the actual algorithm. The second possibility is to shuffle the sequence of operations [4]. In respect of AES, several operations can be randomized such as AddRoundKey, SubBytes, ShiftRows, or MixColumns.

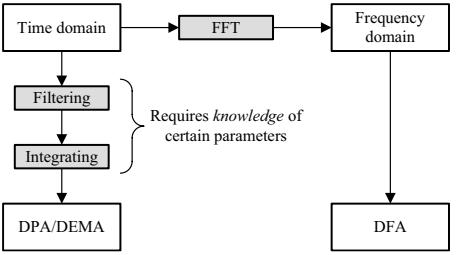

Fig. 2. Overview of the preprocessing steps necessary for DEMA and DPA as well as DFA attacks.

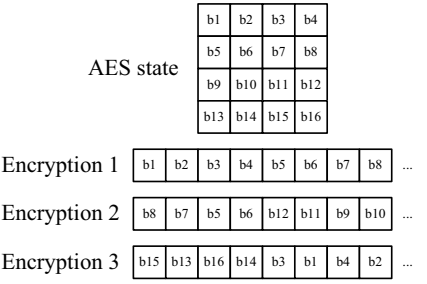

Fig. 3. Principle of shuffling used in the randomized AES implementation.

4 Attacking Techniques on Hiding

There exist techniques that increase the performance of attacks on hiding through trace preprocessing. The most obvious and commonly-used preprocessing technique is filtering. By applying different filters it is possible to reduce noise that originates from narrow-band interferers such as RFID readers. Filtering of these perturbing signals helps to evade hiding in the amplitude dimension. Though this requires knowledge of the appropriate filter parameters to preserve data-dependent information in the traces. In contrast, hiding in the time dimension can be obviated by integration of power or EM traces. Specific points in time are summed up before performing the attack. In practice, only points are chosen that exhibit a high side-channel leakage. These points form a kind of comb or window that can be swept through the trace in order to obtain the highest correlation. This technique is often referred to as *windowing*. However, it is evident that this technique implies the knowledge of certain points in time where the leakage of information is high. If no knowledge of this leakage is available, it shows that the performance of this attack is rather low due to the integration of unimportant points.

Another related technique uses FFT to transform the traces into the frequency domain. Instead of performing differential analysis in the time domain (such as done in standard DPA and DEMA attacks), the analysis is performed in the frequency domain. This allows a time-invariant analysis of side-channel leakages across the overall signal spectrum. This analysis is also referred as Differential Frequency Analysis (DFA) [7]. Figure 2 illustrates the necessary preprocessing steps for conducting DEMA and DPA attacks as well as DFA attacks in presence of hiding. In this article, all three discussed types of preprocessing techniques are analyzed in terms of their efficiency. These preprocessing techniques are applied on EM measurements having increased noise in both amplitude and time dimension. This noise is caused by an interfering RFID reader and by a randomized AES implementation that is described in the following.

5 Description of the Randomized AES Implementation

In our experiments, a 128-bit AES implementation has been used that offers hiding in the time dimension. First, the implementation allows to choose additional rounds that are randomly executed either at the beginning or the end of the actual algorithm. Second, it allows the shuffling of bytes $b1$ to $b16$ within the AES state. There, the sequence of the columns and the sequence of the rows can be randomized as shown in Figure 3. In order to set specific randomization parameters during our experiments, we have implemented a custom command that can be sent over the air interface. These parameters define the number of dummy rounds and the number of shuffling operations. In particular, it is possible to define the sequence of the columns as well as the sequence of the rows within the AES state. If no dummy rounds are inserted and all bytes of the state are shuffled, 16 different positions can be taken over time for one state operation. Regarding side-channel analysis, the correlation coefficient through randomization is then reduced linearly by a factor of 16. The number of necessary traces to succeed an attack increases by a factor of $16^2 = 256$. However, the quadratic influence is only correct when no preprocessing method like windowing or DFA is applied [14].

6 Measurement Setups

The measurement setup used for our experiments is shown in Figure 4. It comprises different devices such as a PC, a standard RFID reader, a digital-storage oscilloscope, the tag prototype, and a measurement probe. The RFID reader and the digital-storage oscilloscope are directly connected to the PC that controls the overall measurement process. Matlab is running on the PC and is used to apply the preprocessing techniques and to conduct the side-channel analysis. The RFID reader communicates with the tag prototype via the air interface. For the HF-tag prototype, the ISO 14443-A protocol has been used while the ISO 18000-6C protocol has been used for the UHF-tag prototype. The HF-tag prototype has been placed directly upon the reader antenna. The UHF-tag prototype has been placed 30 cm in front of the UHF reader. Two channels of the digital-storage oscilloscope (*LeCroy LC584AM*) are used in our experiments. One channel is connected to the trigger pin of the tag prototype, the other channel is connected to the measurement probe. Signals have been sampled with 2 GS/s. Both tag prototypes have been programmed to release a trigger event whenever a new AES encryption is started. This trigger event causes the oscilloscope to record the EM emissions of the tag prototype using magnetic near-field probes. We have used two probes from *EMV Langer* which is the RF R 400 for the HF measurements and the RF B 3-2 for the UHF measurements. Figure 5 shows a picture of the measurement setup for the HF and one for the UHF-tag prototype.

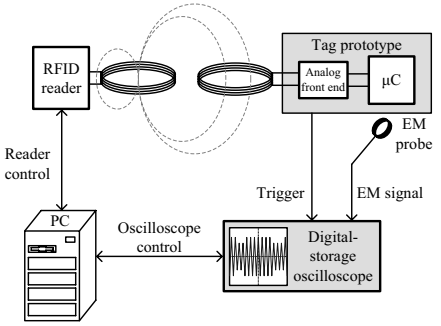

Fig. 4. Schematic view of the general measurement setup used to gather the EM emissions of the tag prototypes.

Fig. 5. Picture of the measurement setup using UHF (upper left) and HF (lower right) RFID-tag prototypes.

7 Results

In this section, the results of the performed side-channel attacks on our RFID-tag prototypes are presented. Attacks have been performed on the electromagnetic emissions of the HF and the UHF-tag prototype. The target of all attacks has been the first byte of the first round of AES. As a power model, the hamming weight has been used.

First, we have analyzed the impact of misaligned traces in the amplitude dimension. For this, we have measured EM emissions of our prototypes that are interfered by unsynchronized reader signals. Note that no randomization of the AES state is enabled in this experiment. In order to perform attacks on such kind of hiding, we investigated two different preprocessing approaches. The first approach applies filtering techniques to suppress the interfering noise of the reader. The second approach applies an FFT before performing the DFA attack. We compare both techniques in their practical efficiency and performance. Second, we show results of attacks that have been performed on misaligned traces in both amplitude and in the time dimension. For this experiment, we have enabled the randomization of the AES implementation which is commonly-used in practice to counteract against side-channel attacks. For this scenario, we have applied trace-integration techniques by windowing. We also compare the results with the results obtained by DFA.

7.1 Attacks on Hiding in the Amplitude Dimension

At first, we focus on typical measurements in RFID environments. The misalignment of EM traces is often caused by readers that interfere the EM measurement of RFID devices. In our experiment, we consider the scenario where the clock signal of our prototype and the reader carrier are desynchronized. This is already the case for our UHF-tag prototype which operates at 16 MHz and which communicates with an 868 MHz reader. For the HF prototype, we have used a 13.56 MHz quartz crystal that is assembled on board. This quartz crystal is also

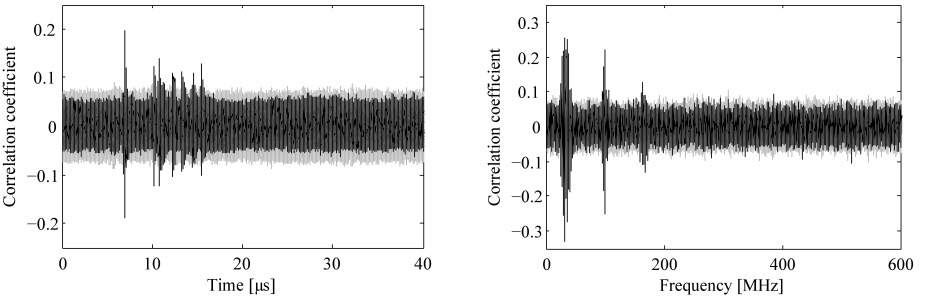

Fig. 6. Result of the filtered DEMA attack (a) and DFA attack (b) on the HF-tag prototype when using hiding in the amplitude domain.

unsynchronized with the communicating 13.56 MHz reader. Both devices have been placed inside the reader field, which interfered the measurement due to additional noise. After the acquisition of 2 000 traces, we have performed filtering techniques to circumvent the interferer and to decrease the noise at this juncture. For the HF prototype, a bandstop filter has been designed using Matlab that filters the 13.56 MHz carrier. For the UHF prototype, a low-pass filter has been used that passes all frequencies below 200 MHz. We have performed a filtered DEMA attack and a DFA attack using FFT.

In Figure 6(a), the result of the filtered DEMA attack for the HF-tag prototype is shown. The correct key hypothesis is plotted in black while all other key hypotheses are plotted in gray. The correct key hypothesis leads to a correlation coefficient of 0.20. Figure 6(b) shows the result of the DFA attack. Three peaks in the electromagnetic spectrum are clearly discernable, which represent high data-dependent frequency emissions. The highest absolute correlation coefficient has been 0.33 and occurred at a frequency of around 33 MHz.

In Figure 7(a), the result of the filtered DEMA attack is presented that has been performed on the UHF-tag prototype. A maximum absolute correlation coefficient of 0.63 has been obtained for the correct key hypothesis. Figure 7(b) shows the result of the DFA attack. As opposed to the results of the HF-tag prototype, many peaks occurred up to a frequency of about 600 MHz. The highest correlation that has been obtained is 0.28.

For the UHF-tag prototype, the results show a higher correlation coefficient compared to the results of the HF prototype. This is explained by the fact that our UHF measurement setup provides a higher SNR. On the one hand, a different EM probe has been used for the measurement that allows the probe to be drawn nearer to the surface of the chip. On the other hand, our experiments have shown that the UHF reader produces lower noise compared to the HF reader. However, when the result of the filtering technique and the result of the DFA are compared to each other, it shows that the DFA attack leads to a higher correlation in noisier

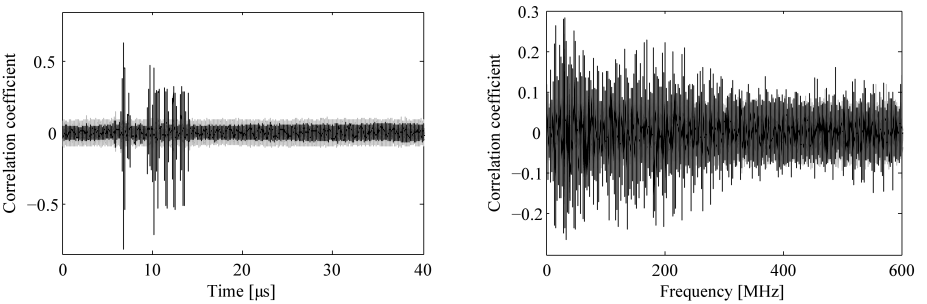

Fig. 7. Result of the filtered DEMA attack (a) and DFA attack (b) on the UHF-tag prototype when using hiding in the amplitude domain.

environments while it is less effective in measurements where a low noise source is present.

7.2 Attacks on Hiding in the Amplitude and Time Dimension

Next, we consider the scenario where a side-channel countermeasure is enabled on the tag side. In addition to the noise of the reader, we have activated the hiding mechanism using AES randomization. As stated in Section 5, we are able to shuffle all bytes within the AES state. This leads to 16 different positions in time where a byte may be processed during one round. Nonetheless, the results of our experiments have shown that for the HF tag no significant correlation has been obtained for the case where we have preprocessed the traces using the trace integration (windowing) technique. By performing the attack in the frequency domain using DFA, we successfully revealed the correct key byte. However, we decided to reduce the number of shuffling bytes to 8 for the HF-measurement scenario in order to succeed the attack in both cases. For the UHF measurements, in contrast, the attacks have been successful when randomizing all 16 bytes of the AES state. For the DEMA attacks in the time domain, we performed software filtering as described in the section above to reduce the noise of the RFID reader. Moreover, for each experiment 10 000 traces have been captured.

The attack using windowing as a preprocessing technique has been performed as follows. We summed up 100 points in time which showed the highest correlation in a previously performed standard DEMA attack. This defines an integration window that involves points with high data-dependent information. For a better visualization of the window matching, we have further implemented an automatic sweep that slides the window from the beginning of the trace to its end. At each position in time, all points of the window are summed up and a DEMA attack has been performed afterwards. This results in a correlation trace where a peak occurs in time when the window fits best the specified data-dependent locations. In Figure 8(a), the result of the attack on the HF-tag prototype is shown where we have zoomed only into the interesting region in

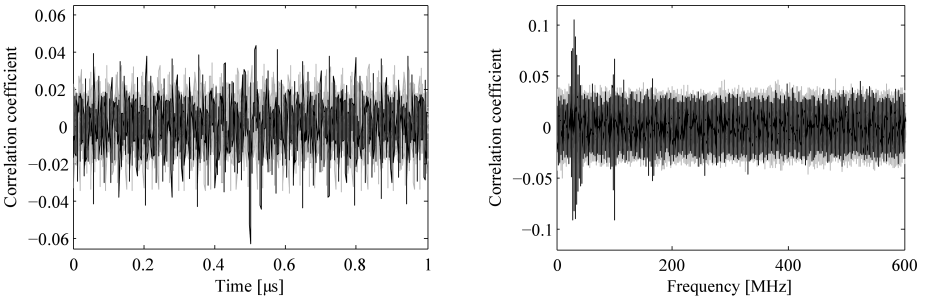

Fig. 8. Result of the windowing attack (a) and DFA attack (b) on the HF-tag prototype when using hiding in the amplitude domain and shuffling 8 bytes of the AES state.

time. A peak is observable which has a maximum absolute correlation coefficient of 0.06. In Figure 8(b), the result of the performed DFA attack is given. Note that neither filtering nor other trace-alignment techniques have been applied before. Two peaks are discernable that arise at about 30 MHz and 100 MHz. These data-dependent frequencies are the same as those we have already obtained in the previous experiment (see Figure 6(b)). The highest correlation coefficient is 0.10.

After that, we have focused on our UHF-tag prototype. We have applied the same integration technique as used for the HF-tag prototype. In contrast to the attack on the HF-tag prototype where 8 bytes have been randomized, now 16 bytes have been shuffled within the AES state. Figure 9(a) shows the trace-integration result of the UHF-tag prototype. A maximum absolute correlation coefficient of 0.23 has been obtained. In Figure 9(b), the result of the performed DFA attack is shown again without using any filtering or trace-alignment techniques. There, a maximum correlation coefficient of 0.14 is obtained.

By taking a closer look at our results, it becomes clear that DFA poses a powerful and easy preprocessing technique that is able to reveal the secret key of our RFID-tag prototypes. DFA provides not only high correlation even in noisy environments but can also be successfully applied against randomization countermeasures without having any knowledge of either interfering frequencies nor data-dependent locations.

8 Conclusions

In this article, we present results of performed DEMA and DFA attacks on HF and UHF RFID-tag prototypes. We addressed the issue of misaligned traces that are captured during EM measurements. These traces are interfered by the reader field, which results in a lower SNR within the amplitude dimension. In addition to that, we have investigated a randomized AES implementation in software

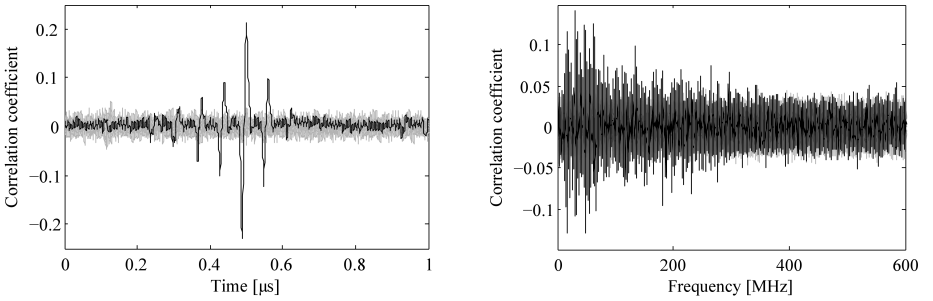

Fig. 9. Result of the windowing attack (a) and DFA attack (b) on the UHF-tag prototype when using hiding in the amplitude domain and shuffling 16 bytes of the AES state.

that hides the leakage of side channels in the time dimension. We performed several attacks by applying filtering, trace integration, and DFA preprocessing techniques. Our experiments prove that DFA is a powerful technique that allows a fast and time-invariant analysis even in environments where traces are misaligned due to noise and randomization. Filtering techniques, in contrast, need the knowledge of the noise-source frequency and might also suppress interesting leakages. Applying integration techniques is a time-consuming task that requires the knowledge of data-dependent locations to design an appropriate integration window. Moreover, if the degree of randomization is increased, the number of windowing points has to be increased as well. We conclude that DFA offers many advantages especially when neither knowledge of the device nor possibilities of noise reduction are given. All side-channel attacks performed on the RFID-tag prototypes with the randomized AES implemented in software have been successful by applying DFA. This also clarifies that RFID devices that are using randomization as a countermeasure suffer from this kind of attack. The effort for attacking commercially-available RFID tags is assumed to be higher, since they will have their cryptographic algorithm and the countermeasure realized in dedicated hardware. Nevertheless, combining randomization with other countermeasure approaches as proposed in [14] might be a good approach to provide a higher degree of security.

Acknowledgements. This work has been supported by the Austrian Government through the research program FIT-IT Trust in IT Systems (Project POWER-TRUST under the Project Number 816151 and Project CRYPTA under the Project Number 820843).

References

1. 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, 4th International Workshop, Redwood Shores, CA, USA, August 13-15. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003)
2. Atmel Corporation: 8-bit AVR Microcontroller with 128K Bytes In-System Programmable Flash. http://www.atmel.com/dyn/resources/prod_documents/doc2467.pdf (August 2007)
3. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-Key Cryptography for RFID-Tags. In: Workshop on RFID Security – RFIDSec, July 12-14, Graz, Austria. pp. 1–16 (2006)
4. Clavier, C., Coron, J.S., Dabbous, N.: Differential Power Analysis in the Presence of Hardware Countermeasures. In: Koç, Ç.K., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems – CHES, Second International Workshop, Worcester, MA, USA, August 17-18. LNCS, vol. 1965, pp. 252–263. Springer, Heidelberg (2000)
5. EPCglobal: EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9 (January 2005), http://www.epcglobalinc.org/
6. Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems using the AES Algorithm. 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. 357–370. Springer, Heidelberg (August 2004)
7. Gebotys, C.H., Ho, S., Tiu, C.C.: EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. 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. 250–264. Springer, Heidelberg (2005)
8. Hein, D., Wolkerstorfer, J., Felber, N.: ECC is Ready for RFID – A Proof in Silicon. In: Selected Areas in Cryptography – SAC, 15th International Workshop, Sackville, Canada, August 14-15. pp. 401–413. LNCS (September 2008)
9. Hofferek, G., Wolkerstorfer, J.: Coupon Recalculation for the GPS Authentication Scheme. In: Grimaud, G., Standaert, F.X. (eds.) Smart Card Research and Advanced Application Conference – CARDIS, September 8-11, 2008, London, UK. LNCS, vol. 5189, pp. 162–175. Springer, Heidelberg (September 2008)
10. Homma, N., Nagashima, S., Imai, Y., Aoki, T., Satoh, A.: High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching. In: Goubin, L., Matsui, M. (eds.) Cryptographic Hardware and Embedded Systems – CHES, 8th International Workshop, Yokohama, Japan, October 10-13. LNCS, vol. 4249, pp. 187–200. Springer, Heidelberg (October 2006)
11. 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, 9th International Workshop, Vienna, Austria, September 10-13. LNCS, vol. 4727, pp. 320–333. Springer, Heidelberg (September 2007)
12. International Organization for Standardization (ISO): ISO/IEC 14443: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards (2000)
13. 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)

14. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
15. McLoone, M., Robshaw, M.J.B.: New Architectures for Low-Cost Public Key Cryptography on RFID Tags. In: IEEE International Symposium on Circuits and Systems (ISCAS 2007), New Orleans, USA, May 27-30. pp. 1827–1830. IEEE (May 2007)
16. Oren, Y., Shamir, A.: Remote Password Extraction from RFID Tags. IEEE Transactions on Computers 56(9), 1292–1296 (September 2007)
17. Plos, T.: Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In: Malkin, T. (ed.) Topics in Cryptology – CT-RSA, San Francisco, CA, USA, April 8-11. LNCS, vol. 4964, pp. 288–300. Springer, Heidelberg (April 2008)
18. Quisquater, J.J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In: Attali, I., Jensen, T.P. (eds.) International Conference on Research in Smart Cards – E-smart, Cannes, France, September 19-21. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)
19. Sarma, S.E., Weis, S.A., Engels, D.W.: RFID Systems and Security and Privacy Implications. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems – CHES, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002. LNCS, vol. 2523, pp. 454–470. Springer, Heidelberg (August 2003)
20. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) 1st Annual Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (March 2003)
21. Witteman, M.: Advances in Smartcard Security. Information Security Bulletin 7, 11–22 (July 2002)