Power and EM Attacks on Passive 13.56 MHz RFID Devices

Michael Hutter[1], Stefan Mangard[2,⋆], and Martin Feldhofer[1]

[1] Institute for Applied Information Processing and Communciations (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{Michael.Hutter,Martin.Feldhofer}@iaik.tugraz.at
[2] Infineon Technologies AG
Security Innovation
Am Campeon 1-12, 85579 Neubiberg, Germany
Stefan.Mangard@infineon.com

Abstract. During the last years, more and more security applications have been developed that are based on passive 13.56 MHz RFID devices. Among the most prominent applications are electronic passports and contactless payment systems. This article discusses the effectiveness of power and EM attacks on this kind of devices. It provides an overview of different measurement setups and it presents concrete results of power and EM attacks on two RFID prototype devices. The first device performs AES encryptions in software, while the second one performs AES encryptions in hardware. Both devices have been successfully attacked with less than 1 000 EM traces. These results emphasize the need to include countermeasures into RFID devices.

Keywords: RFID, Power Analysis, EM Attacks, Side-Channel Attacks, DPA, DEMA, AES

1 Introduction

Radio Frequency Identification (RFID) is a rapidly upcoming technology that is used in more and more applications. In 2006, already more than one billion RFID devices have been shipped. These devices range from low-cost passive devices to complex actively powered devices. This article focuses on passive RFID devices for security applications.

Passive RFID devices essentially consist of a tiny microchip that is attached to an antenna. This antenna is used to draw energy from an electromagnetic field of an RFID reader. Passive RFID devices are completely powered by the energy that is provided by this field. Furthermore, this field is used for the communication between the reader and the device. The most prominent application of passive RFID devices in the context of security is the contactless smart card, which is specified in ISO/IEC 14443 [13]. This standard specifies the interface

[⋆] This work was done while the author was with Graz University of Technology.

that is for example used for electronic passports or for contactless payment and access control systems. Contactless smart cards typically implement standardized cryptographic algorithms, like RSA [23], ECC [15], DES [18], or AES [19].

In addition to these cards, there also exist passive RFID devices that implement proprietary cryptographic algorithms. These algorithms have been developed with the goal to provide security at very low implementation costs (power, time, area). However, often these proprietary algorithms do not have the same cryptographic strength as standardized algorithms. This fact has for example been exploited in the attack presented in [3]. In order to avoid these problems, there have recently been several efforts to develop low-cost implementations of ECC and AES for RFID devices (see for example [2], [5], [8], and [14]).

In the light of the fact that contactless smart cards are deployed at a large scale and that more and more cryptography is also added to RFID devices in general, it is almost surprising that so far only very few publications analyze the effectiveness of side-channel attacks on such implementations. Side-channel attacks, like timing [16], power [17], and EM [1, 7, 22] attacks are considered to be the most effective attacks against cryptographic devices in practice. They have been studied extensively in the context of contact-based devices. For RFID devices there only exist three publications so far. In [4], Carluccio *et al.* have tried to perform an EM attack on a contactless smart card. Yet, the secret key could not be revealed by the attack. In [9], Handschuh introduced the term Radio Frequency Analysis (RFA) for attacking contactless devices generating RSA signatures. In [20], Oren and Shamir have successfully revealed passwords of RFID tags using power analysis techniques. This attack has been performed on ultra-high frequency (UHF) tags. The electromagnetic field that is used to power these devices has a frequency of around 900 MHz. However, most RFID devices that use cryptography work in the high frequency (HF) band. Therefore, the results presented in [20] cannot be mapped directly to these devices.

In the current article, we analyze power and EM attacks on RFID tag prototypes that are powered by a field with a frequency of 13.56 MHz. This is the frequency that is used for contactless smart cards and for several other RFID devices that implement cryptography. We present results of different DPA and DEMA attacks on two RFID prototype devices that implement AES. The first one implements AES in software, while the second one implements AES in hardware. We have been able to successfully attack both implementations using several different measurement setups. The current article is therefore novel in two ways. It is the first article that provides an overview of measurement setups for DPA and DEMA attacks on RFID devices. Furthermore, it is the first to report results of successful EM attacks on hardware as well as software implementations of AES on RFID tag prototypes. The results of this article show the importance of countermeasures against side-channel attacks for RFID devices.

This article is organized as follows. Section 2 provides an overview of the different standards for 13.56 MHz RFID devices. Furthermore, the devices that we have used for the attacks are introduced. Section 3 discusses measurement setups for DPA and DEMA attacks on RFID devices. In Section 4, we discuss results of attacks on the RFID device with the AES software implementation. Section 5 is devoted to the results of the attacks on the device with the AES hardware implementation. Conclusions are provided in Section 6.

2 RFID Devices Running at 13.56 MHz

This article focuses on passive RFID devices that work at a carrier frequency of 13.56 MHz. Two of the most well known standards for RFID devices operating at this frequency are ISO/IEC 14443 [13] for contactless smart cards and ISO/IEC 15693 [11] for RFID tags. There are only minor differences between those two standards in terms of data encoding, modulation indices, and data rates. Another recently upcoming standard for 13.56 MHz RFID devices is called Near Field Communication (NFC) [12]. In NFC, two active devices like mobile phones communicate using the ISO/IEC 14443 interface. Hence, the devices can also be used to communicate with passive RFID devices.

However, although there exist many passive RFID devices that comply to one of the mentioned ISO/IEC standards, it is challenging to find a suitable platform for academic research on side-channel attacks. One of the most important reasons for this is that most contactless smart cards do not only comply to ISO/IEC 14443, but also to confidential standards that specify the communication layers above the ISO/IEC 14443 layer. The most commonly used confidential standard in this context is Mifare [21].

For this article we have not used commercial products, but we have built two RFID prototypes that have properties comparable to commercial passive RFID devices. Both prototypes do not have an internal power supply. They use an antenna to draw energy out of the electromagnetic field of a 13.56 MHz RFID reader. The voltage that is induced in the antenna, is rectified and stabilized in an analog front-end. The output voltage of the analog front-end is then used to power a digital circuit. The difference between the prototype devices and commercially available RFID devices is that our analog front-end is not integrated on the same IC as the digital circuit. It is built using discrete components and therefore it does not work as efficiently as integrated analog front-ends. Furthermore, the discrete components potentially lead to more emissions than an integrated solution. However, the principles of attacks on the prototypes are the same as in case of attacks on commercial productions.

The digital circuits of our RFID devices provide a communication interface and they are also capable of performing AES encryptions. In case of the first prototype, all these operations are implemented in software on a low-power microcontroller, while the second prototype is based on a low-power AES hardware implementation.

2.1 RFID Prototype with a Microcontroller

The main elements of our first prototype are an antenna, an analog front-end, and a microcontroller. All components are discrete and designed for low-power consumption in order to make sure that the device can be powered passively by the electromagnetic field of an RFID reader.

We have used a self-made antenna with four windings according to ISO/IEC 7810 which is connected to the analog front-end using a tuned circuit. This analog front-end is responsible for a stabilized power supply of the microcontroller as well as for the demodulation and modulation of data that is sent over the field. The main parts for the power supply are a simple bridge rectifier with a smoothing capacitor. A Zener diode is used for overvoltage protection. In contrast to commercial RFID devices where the clock signal is recovered from the RF field of the reader, our prototype has a 13.56 MHz oscillator on board. Nevertheless, we have synchronized the clock source with the RF field of the reader. As low-power microcontroller we have used an ATmega168 and we have implemented the communication protocol and AES on it. The total power consumption of this prototype adds up to 3.7 mA at a supply voltage of 1.8 V. The prototype fully complies to ISO/IEC 15693 and cannot be distinguished from a commercial RFID device, except for its larger size due to the discrete electronic components. AES is used in a challenge-response protocol that is performed using custom instructions according to ISO/IEC 15693. The AES software implementation on the microcontroller does not include any countermeasures against power analysis attacks.

2.2 RFID Prototype with an AES Coprocessor

The second prototype is based on an AES coprocessor. The coprocessor consists of an AES core and an 8-bit microcontroller interface. The AES core is very small and has been designed especially for low-power consumption in RFID environments. It has a die size of $0.25\,\text{mm}^2$ using a $0.35\,\mu\text{m}$ CMOS process and needs about $3\,\mu\text{A}$ of current at a frequency of 100 kHz. A detailed description of the chip implementation is presented in [6].

In order to power the AES core, the same antenna and analog front-end have been used as in case of the first prototype. However, in contrast to the first prototype, the communication between the RFID reader and the coprocessor is not performed via the air interface. The communication is done using an FPGA board. This communication interface has been separated from the power supply of the AES core in order to make sure that the core is only powered by the field of the reader. The coprocessor is clocked with a 40 MHz signal.

3 Measurement Setups

In order to perform DPA and DEMA attacks on passive RFID devices it is necessary to build corresponding measurement setups. These setups are typically more complex than power measurement setups for contact-based devices. The reason for this is that the RFID devices are powered via the electromagnetic field of an RFID reader and not directly via a power supply unit. In the following subsections, we provide a brief overview of different methods that can be used to measure the power consumption of passive RFID devices.

Fig. 1. Magnetic near-field probe

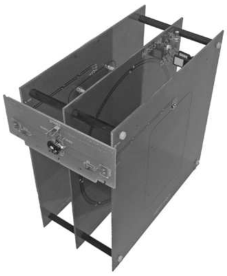

Fig. 2. Helmholtz assembly according to ISO/IEC 10373-6

3.1 Power Measurements Based on a Resistor

The simplest method to measure the power consumption of a device is to insert a resistor into one of its power supply lines. For DPA attacks, this resistor should ideally be placed into one of the power supply lines of the module that performs the encryption operation. In case of an RFID device, this means that the resistor should be placed between the analog front-end and the digital circuit that performs the encryption.

Obviously, this is not possible in practice because RFID devices are usually integrated on one piece of silicon. However, in case of the two prototype devices we are analyzing in this article, we have access to the power supply lines that connect the analog front-end and the chip performing the AES encryptions. Hence, we can directly measure the power consumption of the digital circuit. We use this method as a reference for the contactless measurement setups.

3.2 Power Measurements Based on an EM Probe

Another approach to measure the power consumption is to measure the power consumption indirectly via the electromagnetic field of the device. This can for example be done by a magnetic near-field probe (see Figure 1). There are several publications that discuss how this method can be used to attack contact-based devices (see for example [7] and [22]). However, in the case of RFID devices, the electromagnetic field of the device cannot be measured so easily. The problem is that the 13.56 MHz carrier of the reader is much stronger than the field of the RFID device. Therefore, it is necessary to suppress this carrier.

Essentially, there exist two methods to do this. The first method is to separate the chip of the RFID device from the antenna. The basic idea of this method is to place an antenna in the field of the reader and to use wires to supply an RFID device that is placed outside the field. This approach has first been presented in [4]. The alternative to this approach is to filter the signal that is measured by the EM probe. This can for example be done by a receiver.

3.3 Power Measurements Based on an EM Probe and a Receiver

The first publication that discusses the use of a receiver to perform EM attacks on cryptographic devices is [1]. In this publication, a receiver is used to find the side-channel leakage of devices in different parts of the EM spectrum. A very similar approach can of course also be used for RFID devices. In this case, the basic idea is to scan the EM spectrum of the device between the harmonics of the 13.56 MHz carrier. The leakage in between the harmonics can be easily be exploited as there is no interference of the harmonics of the carrier.

Another approach to attack an RFID device with a receiver has been presented in [20]. In this publication an UHF tag has been attacked that operates at around 900 MHz. For the attack, an antenna has been placed in such a way that it only records the backscattered signal of the tag. This signal has been demodulated by a receiver and it turned out that this signal carries exploitable information about the power consumption of the tag.

3.4 Power Measurements Based on a Helmholtz Assembly

Another possibility to measure a signal that is proportional to the power consumption of a 13.56 MHz RFID device is to use the test setup described in ISO/IEC 10373-6 [10]. In this standard a so-called Helmholtz assembly (see Figure 2) is specified for compliance testing. This assembly essentially consists of two sense coils that are arranged in parallel to a reader antenna. The two sense coils are connected with in-phase opposition. Consequently, the induced voltage becomes zero at the point where the two coils are connected to each other (differential point). When a passively powered device draws energy out of the field, this measuring bridge becomes unbalanced and an offset voltage can be observed at the differential point. This voltage offset can be measured using a digital oscilloscope and it contains information about the power consumption of the RFID device. The carrier signal of the RFID reader is typically attenuated by 40 dB by a Helmholtz assembly.

4 Attacks on the RFID Prototype with a Microcontroller

In this section, we discuss results of different power and EM attacks on our first RFID prototype. This prototype is based on a low-power microcontroller that performs AES encryptions in software. In order to attack this device, we have essentially used the measurement setups described in Section 3. Hence, the discussed attacks range from classical DPA attacks that are based on the insertion of a resistor to DEMA attacks that are based on a Helmholtz assembly.

All attacks that we have performed have been successful. Hence, the results are very relevant for contactless smart cards, which are typically based on a low-power microcontroller. The attacks that we discuss in this section have used the output of the first S-box operation in round one of AES to reveal one byte of the secret key. As a trigger signal, an output pin of the microcontroller has

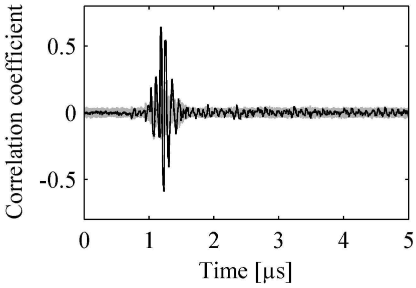

Fig. 3. Result of a DPA attack on the actively powered prototype outside the reader field.

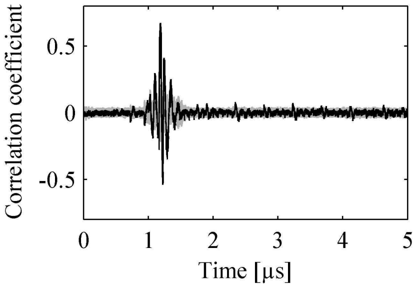

Fig. 4. Result of a DPA attack on the passively powered prototype inside the reader field.

been programmed to pull high right before the S-box operation. The power consumption has been recorded for 5 μs with a sampling rate of 2 GS/s. For each attack, 10 000 traces have been recorded and the Hamming weight model has been used.

4.1 Power Analysis Attacks

For the first attack, the microcontroller has been powered actively by a DC power supply. Furthermore, we have placed our prototype outside the field of the RFID reader. In order to provide a communication link between the prototype and the RFID reader, we have designed an additional antenna with the same dimensions and properties as the original antenna of the prototype. We have placed this additional antenna on top of the reader and connected it with the prototype using a one meter cable. The power consumption of the microcontroller has been measured by inserting a 1 Ω resistor into the ground line of the power supply. Hence, this attack corresponds to a classical power analysis attack on a contact-based device. The only difference to a classical attack is that the device communicates via an RFID interface. We have performed this attack as a reference for all following attacks.

Figure 3 shows the result of the DPA attack on the output of the first S-box operation in round one of AES. The correct key hypothesis is plotted in black, while all other 255 key hypotheses are plotted in gray. The correct key hypothesis leads to a clear peak with a correlation coefficient of 0.64. Hence, the secret key has been revealed successfully.

After this first DPA attack, we have performed another DPA attack. For this second attack, we have removed the additional antenna and we have placed our prototype directly on top of the RFID reader. Furthermore, we have removed the active power supply. Hence, the device was passively powered. Nevertheless, the power consumption was still measured using a resistor. Figure 4 shows the result of this attack. Just like before, a peak for the correct key hypothesis is clearly visible. The maximum correlation coefficient is 0.67. Hence, there is

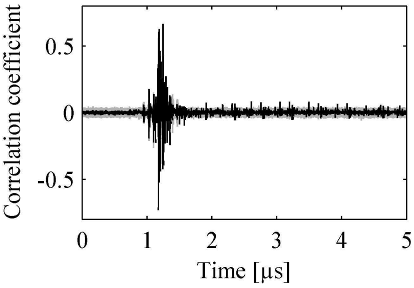

Fig. 5. Result of a DEMA attack on the actively powered prototype outside the reader field.

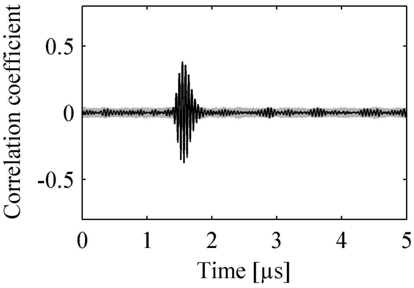

Fig. 6. Result of a DEMA attack on the passively powered prototype inside the reader field.

no substantial difference between a conventional DPA attack on our actively powered prototype and a DPA attack on the passively powered prototype.

4.2 EM Attacks

In addition to DPA attacks, we have also performed DEMA attacks. For these attacks, we have placed a magnetic near-field probe with a diameter of 22 mm (see Figure 1) directly on the microcontroller. It has a frequency range from 30 MHz to 3 GHz. The goal of the first DEMA attack has been to verify that the field of our RFID prototype indeed leaks side-channel information. For this purpose, we have performed an attack that was very similar to the first DPA attack. This means that we have powered the prototype actively by a DC power supply and that we have placed the prototype outside the field of the reader. Just like in the DPA attack, an antenna with a one meter cable has been used to provide a communication link between the prototype and the reader. Hence, there has been almost no interference between the field of the reader and the field of the microcontroller. The magnetic probe has essentially measured the field of the microcontroller. Figure 5 shows the result of a DEMA attack that has been performed using this setup. The hypothesis for the correct key leads to a correlation coefficient of 0.73. Hence, this attack is even slightly more efficient than the power analysis attacks discussed in the previous section.

The next step has been to perform DEMA attacks by using a wideband receiver. As pointed out in Section 3, receivers can be used to perform DEMA attacks inside the field of a reader. However, before we have placed our RFID prototype directly on top of the reader, we have characterized the side-channel leakage of our prototype. For this purpose we have kept the prototype outside the field of the reader and we have connected a 3 GHz wideband receiver to the magnetic probe. We have programmed the receiver to sweep across the EM spectrum of the microcontroller while it has performed AES encryptions for different plaintexts. The sweep has been performed with a bandwidth of 3 MHz. We have used the receiver for mixing down the HF signals to an intermediate

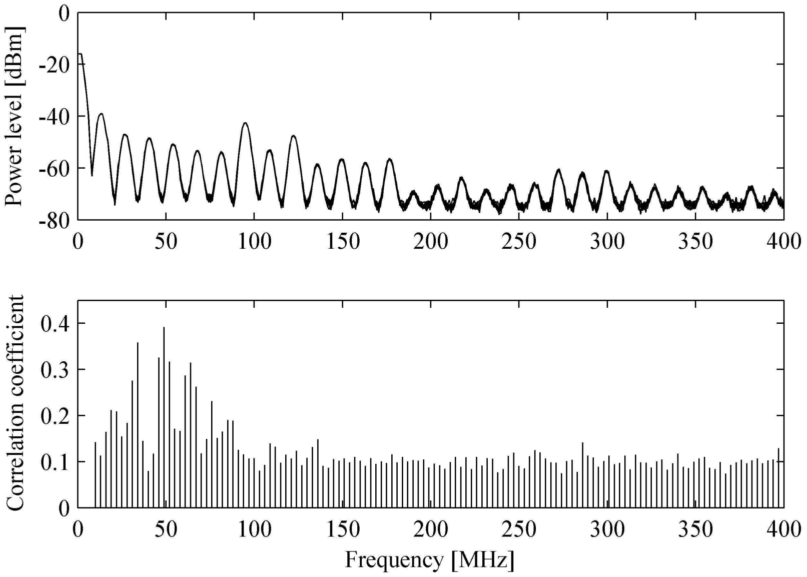

Fig. 7. Correlation coefficients for the correct key hypothesis in DEMA attacks that have been conducted at different frequencies.

frequency of 20.4 MHz which has been sampled with the digital oscilloscope. We have recorded 1 000 traces for different plaintexts for each 3 MHz interval between 10 MHz and 400 MHz. Subsequently, a DEMA attack has been performed for each of the 130 intervals.

The result of the attacks is shown in the lower plot of Figure 7. The x-axis shows the frequency and the y-axis shows the correlation coefficients of the correct key hypothesis. It can be seen that there are several data-dependent emissions below 90 MHz. The highest correlation coefficient is 0.39 at a frequency of 49 MHz. As a reference, the upper plot shows the spectrum of the microcontroller in the same frequency range. The clock harmonics, which are a multiple of 13.56 MHz, can easily be identified.

After having characterized the EM spectrum of our microcontroller, we have performed a DEMA attack in presence of the reader field. We have placed the prototype inside the field of the reader and the prototype has been powered passively by this field. The frequency of the wideband receiver has been adjusted to 49 MHz and the bandwidth has been set to 3 MHz. Figure 6 shows the result of a DEMA attack that has been performed using this setup. The attack has successfully revealed the secret key. The correlation of the correct key hypothesis is 0.19.

After this attack, we have also performed a DEMA attack using the Helmholtz assembly. Thus, we have placed the microcontroller in front of one sense coil and we have connected the oscilloscope to the differential point of the measuring

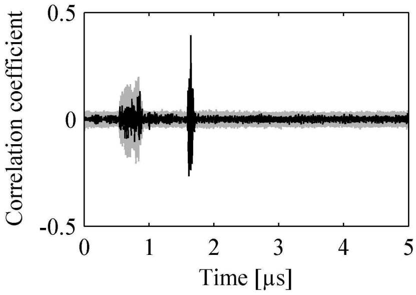

Fig. 8. Result of a DPA attack on the actively powered AES coprocessor outside the reader field.

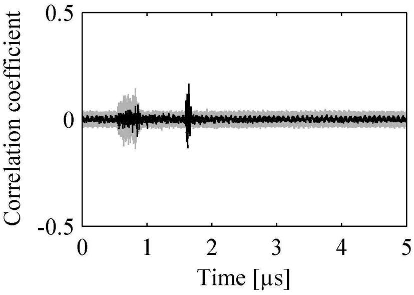

Fig. 9. Result of a DPA attack on the passively powered AES coprocessor inside the reader field.

bridge. The offset voltage has been measured while the prototype has performed AES encryptions. Based on the recorded traces, an attack has been performed successfully. However, the correlation for the correct key hypothesis has only been around 0.058.

In summary, we have hence made the following observations. The DPA attacks have shown that it does not make a substantial difference whether this prototype is powered actively or passively. The DEMA attack outside the reader field has led to slightly better results than the DPA attacks. However, all these attacks have lead to correlation coefficients above 0.6, which can be exploited with less than 100 traces. Inside the reader field the correlation was reduced due to the filtering that was necessary to suppress the interference of the carrier of the reader. Nevertheless, this attack has lead to a correlation of 0.19, which is still quite high and which can be exploited with about 700 traces. The correlation coefficients that we have observed with the Helmholtz assembly have been significantly lower than all other correlation coefficients. About 8000 traces have been necessary to distinguish the correlation of 0.058 for the correct key hypothesis from the other key hypotheses. All in all the experiments have shown that EM attacks are highly relevant for RFID devices like cryptographic smart cards.

5 Attacks on the RFID Prototype with an AES Coprocessor

This section presents results of power and EM attacks on our second RFID prototype. This prototype consists of a low-power hardware implementation of AES. Like in case of the software implementation, we have used the measurement setups described in Section 3. Furthermore, we have also used the Hamming weight model to attack the power consumption of the first S-box output in round one of AES based on 10 000 traces. The measuring window for each trace covers again 5 µs and the traces have been sampled with 2 GS/s.

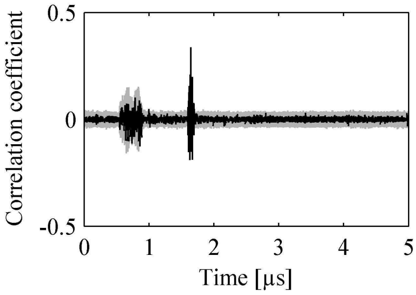

Fig. 10. Result of a DEMA attack on the actively powered prototype outside the reader field.

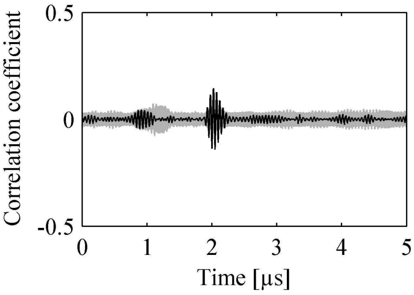

Fig. 11. Result of a DEMA attack on the passively powered prototype inside the reader field.

5.1 Power Analysis Attacks

For the first attack, no RFID reader has been used. The prototype has been powered actively and the plaintexts have been provided by the FPGA. For the power measurements, a 1 Ω resistor has been inserted into the ground line of the AES core. Hence, this is again a classical DPA attack that serves as a reference. The result of this attack is shown in Figure 8. For the correct key hypothesis, a peak with a correlation of 0.39 occurs after 1.64 µs. The low correlation peaks between 0.3 µs and 1 µs are caused by the loading of the plaintexts and are not relevant for this attack.

Next, we have conducted a DPA attack in presence of the field of an RFID reader. We have placed the prototype on top of the reader antenna and we have used an antenna with an analog front-end to power the AES core passively. The power consumption has been measured with a 1 Ω resistor in the ground line between the analog front-end and the power-supply pin of the AES core. Figure 9 shows the result of this attack. A peak with a correlation coefficient of 0.17 has been obtained. In contrast to the software implementation, the hardware implementation is obviously more affected by the fact whether the device is powered actively or passively.

5.2 EM Attacks

The next experiments have focused on EM attacks. Like for the DPA attacks, the prototype has first been powered actively. Instead of the power measurements with a resistor, a magnetic near-field probe (see Figure 1) has been placed directly on the AES chip. Again, no reader has been necessary. The result of the performed DEMA attack can be seen in Figure 10. A correlation coefficient of 0.34 has been obtained, which nearly corresponds to the previous result.

Subsequently, we have characterized the EM spectrum of the AES coprocessor using the same procedure as for the microcontroller in Section 4. The upper plot of Figure 12 shows the spectrum of the AES coprocessor. The 40 MHz clock

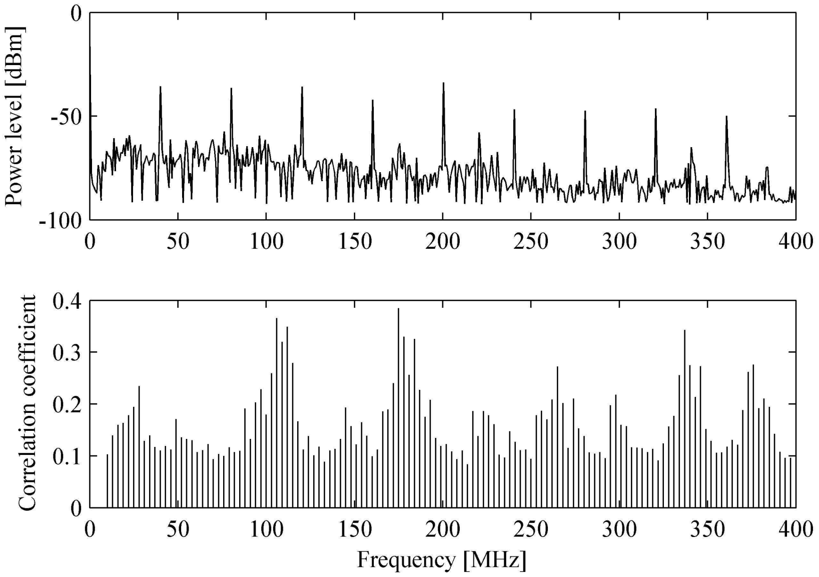

Fig. 12. Correlation coefficients for the correct key hypothesis in DEMA attacks that have been conducted at different frequencies.

harmonics are clearly visible as peaks. We have again programmed a wideband receiver to sweep from 10 MHz to 400 MHz using a 3 MHz filter resolution. Like before, 130 DEMA attacks have been performed. The results are shown in the lower plot of Figure 12. The EM side-channel leakage is more spread across the spectrum as opposed to our first prototype. Note that the leakage occurs between the sidebands of higher-order clock harmonics. High correlation coefficients have been obtained in frequency bands between 100 MHz and 120 MHz, 170 MHz and 180 MHz or between 330 MHz and 350 MHz. We have also performed a more detailed analysis with higher filter resolutions up to 100 kHz. In this way, we have identified highly data-dependent emissions at 106.4 MHz.

We have performed a DEMA attack that exploits this leakage inside the reader field. Thus, the AES coprocessor has been powered passively by the field. We have filtered the 106.4 MHz frequency band with a 3 MHz filter. Figure 11 shows the result of the attack. The attack has successfully revealed the secret key. The correlation for the correct key hypothesis has been 0.15.

In summary, the performed experiments have provided the following observations. The DPA and DEMA attacks on the actively powered device have led to correlation coefficients of about 0.35. In order to detect the correct key hypothesis hence about 200 traces are necessary in this case. For the passively powered prototype the correlation has been significantly lower. The DPA attack as well as the DEMA attack has led to a correlation coefficient of 0.15 for the correct key hypothesis. For a successful attack, about 2 000 traces are necessary in this case.

All in all, the side-channel leakage of the second prototype is slightly different than the one of the first prototype. Nevertheless, the attacks on both prototypes have been successful. Therefore, it is necessary to implement countermeasures against these attacks.

6 Conclusions

In this article, we have presented results of several successful DPA and DEMA attacks on two RFID prototypes that operate at 13.56 MHz. The results show that attacks on contactless devices are not significantly less effective than attacks on contact-based devices. In fact, we have only needed about 700 traces to attack a software implementation of AES on an RFID device that has been passively powered and that has been located in the field of the reader. Similar results have also been obtained for an attack on an RFID device with a hardware implementation of AES. The experimental results of this article show that countermeasures need to be included into implementations of cryptographic algorithms on RFID devices.

Acknowledgements.

This work origins from the Austrian Government funded project *SNAP* established under the embedded system program FIT-IT.

References

1. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM Side-channel(s). In B. S. K. Jr., Çetin Kaya Koç, and C. 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. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. Public-Key Cryptography for RFID-Tags. In *Workshop on RFID Security 2006 (RFIDSec06), July 12-14, Graz, Austria*, 2006.
3. S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium, Baltimore, Maryland, USA, July-August, 2005, Proceedings*, pages 1–16. USENIX, 2005.
4. D. Carluccio, K. Lemke, and C. Paar. Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. In E. Oswald, editor, *Workshop on RFID and Lightweight Crypto (RFIDSec05), July 13-15, Graz, Austria*, 2005.
5. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems – CHES 2004, 6th International Workshop, Cambridge, MA, USA, August 11-13, 2004, Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370. Springer, August 2004.

6. M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings on Information Security*, 152(1):13–20, October 2005.
7. K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic Analysis: Concrete Results. In Çetin Kaya Koç, D. Naccache, and C. 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.
8. P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen. Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core. In *9th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools (DSD 2006), Dubrovnik, Croatia, 30. August-1 September, 2006. Proceedings*, pages 577–583. IEEE Computer Society, September 2006.
9. H. Handschuh. Contactless technology security issues. `http://www.chi-publishing.com/samples/ISB0903HH.pdf`, April 2004.
10. International Organisation for Standardization (ISO). ISO/IEC 10373-6: Identification cards - Test methods – Part 6: Proximity cards, 2001.
11. International Organisation for Standardization (ISO). ISO/IEC 15693-3: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards – Part 3: Anticollision and transmission protocol, 2001.
12. International Organisation for Standardization (ISO). ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol, April 2004.
13. International Organization for Standardization (ISO). ISO/IEC 14443: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards, 2000.
14. J.-P. Kaps and B. Sunar. Energy comparison of AES and SHA-1 for ubiquitous computing. In X. Zhou, O. Sokolsky, LuYan, E.-S. Jung, Z. Shao, Y. Mu, D.-C. Lee, D. K. Y.-S. Jeong, and C.-Z. Xu, editors, *2nd IFIP International Symposium on Network Centric Ubiquitous Systems (NCUS 2006), Seoul, Korea, August 1-4, 2006, Proceedings*, volume 4097 of *Lecture Notes in Computer Science*, pages 372–381. Springer, 2006.
15. N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.
16. P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In N. 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.
17. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In M. 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.
18. National Institute of Standards and Technology (NIST). FIPS-46-3: Data Encryption Standard, October 1999. Available online at `http://www.itl.nist.gov/fipspubs/`.
19. National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001. Available online at `http://www.itl.nist.gov/fipspubs/`.
20. Y. Oren and A. Shamir. Power Analysis of RFID Tags. `http://www.wisdom.weizmann.ac.il/~yossio/rfid/`, February 2006.
21. Philips Austria GmbH. Website mifare.net - contactless smart cards. `http://www.mifare.net`.

22. J.-J. Quisquater and D. Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In I. Attali and T. P. Jensen, editors, *Smart Card Programming and Security, International Conference on Research in Smart Cards, E-smart 2001, Cannes, France, September 19-21, 2001, Proceedings*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer, 2001.
23. R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. ISSN 0001-0782.