Attacking an AES-enabled NFC Tag: Implications from Design to a Real-World Scenario

Thomas Korak, Thomas Plos and Michael Hutter

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{thomas.korak,thomas.plos,michael.hutter}@iaik.tugraz.at

Abstract. Radio-frequency identification (RFID) technology is the enabler for applications like the future internet of things (IoT), where security plays an important role. When integrating security to RFID tags, not only the cryptographic algorithms need to be secure but also their implementation. In this work we present differential power analysis (DPA) and differential electromagnetic analysis (DEMA) attacks on a security-enabled RFID tag. The attacks are conducted on both an ASIC-chip version and on an FPGA-prototype version of the tag. The design of the ASIC version equals that of commercial RFID tags and has analog and digital part integrated on a single chip. Target of the attacks is an implementation of the Advanced Encryption Standard (AES) with 128-bit key length and DPA countermeasures. The countermeasures are shuffling of operations and insertion of dummy rounds. Our results illustrate that the effort for successfully attacking the ASIC chip in a real-world scenario is only 4.5 times higher than for the FPGA prototype in a laboratory environment. This let us come to the conclusion that the effort for attacking contactless devices like RFID tags is only slightly higher than that for contact-based devices. The results further underline that the design of countermeasures like the insertion of dummy rounds has to be done with great care, since the detection of patterns in power or electromagnetic traces can be used to significantly lower the attacking effort.

Keywords: Radio-Frequency Identification (RFID), Advanced Encryption Standard (AES), Side-Channel Analysis (SCA), Differential Power Analysis (DPA), Differential Electromagnetic Analysis (DEMA).

1 Introduction

Radio-frequency identification (RFID) technology has gained a lot of attention during the last decade and is already used in many applications like ticketing, supply-chain management, electronic passports, access-control systems, and immobilizers. The relevance of this technology is underlined by the integration of RFID functionality into the latest generation of smart phones, which uses so-called near-field communication (NFC). With this widespread use of RFID

W. Schindler and S.A. Huss (Eds.): COSADE 2012, LNCS 7275, pp. 17–32, 2012.
The final publication is available at Springer via http://dx.doi.org/10.1007/978-3-642-29912-4_2

technology, new applications like the future internet of things (IoT) will arise where security plays an important role. When integrating security to RFID systems, not only the selected cryptographic algorithms have to be secure, but also their implementation has to be protected against attacks such as side-channel analysis.

An RFID system consists of a reader (e.g. a smart phone) and a tag that communicate contactlessly by means of a radio frequency (RF) field. The tag is a small microchip attached to an antenna. Passive tags also receive their power supply from the RF field, which limits the available power budget of the tags. Especially passive tags that can be produced at low cost will be used in applications like the future IoT, where tags have to be competitive in price. In order to keep the price low, tags have to be produced in high volume and with smallest possible chip size. These limitations make the integration of cryptographic security to RFID tags challenging.

Recent incidents like the reverse engineering of the CRYPTO 1 algorithm in Mifare tags [21], the breaking of the Digital Signature Transponder (DST) [3], or the attacks on the Hitag 2 cipher [5] and the KeeLoq remote entry system [6] have emphasized the need for integrating strong cryptographic security to RFID tags. A lot of effort has been made by the research community to bring strong security to resource-constrained RFID tags. Well-known examples are symmetric-key schemes like the Advanced Encryption Standard (AES) [7,9,20] and PRESENT [25], or public-key schemes like Elliptic Curve Cryptography (ECC) [1,2,10,27] and NTRU [11].

Having a strong cryptographic algorithm alone is not enough, also the implementation of the algorithm has to be secure. Techniques that exploit weaknesses of an implementation are called implementation attacks. A prominent kind of implementation attack is side-channel analysis (SCA). In an SCA attack, side-channel information is measured during the execution of a cryptographic algorithm to deduce secret data like the encryption key. As side-channel information, execution time [17], power consumption [18], or electromagnetic (EM) emissions [8] of a cryptographic device can be used. A very powerful SCA attack is differential power analysis (DPA) introduced by Kocher et al. [18] that reveals even very weak data-dependent information in the power consumption of a device. When using the EM emissions of a device instead of the power consumption, the attack is called differential electromagnetic analysis (DEMA) [26]. In order to make SCA attacks less efficient, so-called countermeasures are integrated.

While there is a large number of published articles about DPA and DEMA attacks on contact-based devices, there is only a handful of them about attacks on RFID devices. Hutter et al. [13,14] have presented several DPA and DEMA attacks on high frequency (HF) RFID prototype devices. Oren and Shamir [22] have inspected the EM emissions of ultra-high frequency (UHF) tags to deduce the secret kill password. Kasper et al. [16] and Oswald [23] have successfully applied DEMA attacks on a contactless smart card that computes Triple DES (3DES).

In this work we present DPA as well as DEMA attacks on a security-enabled NFC tag. The novelty of this work is that we have conducted the attacks on two versions of the tag, an ASIC-chip version and an FPGA-prototype version. Both versions implement the same functionality. The ASIC integrates the digital part and the analog part on a single chip, which equals the design structure of commercially available RFID tags. The FPGA prototype on the other hand has the digital part implemented on the FPGA and the analog part is realized via an extra analog front-end built with discrete components. Our work closes the gap of current publications where either prototype tags or commercially available RFID tags are examined separately. Target of the SCA attacks is an AES implementation that has countermeasures integrated. The countermeasures are shuffling of operations and insertion of dummy rounds. Our results show that the effort for attacking the ASIC chip is only 4.5 times higher with our measurement setup than for the FPGA prototype. This clarifies that the effort for attacking commercial RFID tags is only slightly higher than for prototype devices. The results also confirm that countermeasures like the insertion of dummy rounds have to be implemented very carefully, as the detection of patterns in the traces allows to significantly reduce the attacking effort.

The remainder of this work is organized as follows. Section 2 provides an overview of the ASIC chip and the FPGA prototype that we have used for our measurements. In Section 3 we describe the different measurement-setup scenarios. Side-channel analysis results are given in Section 4. Conclusions are drawn in Section 5.

2 Overview of the Analyzed Devices

In this section we give an overview of the attacked hardware devices. For the evaluation we use a security-enabled NFC-tag chip. First the focus is put on the ASIC version of the security-enabled NFC-tag chip and then on the FPGA-prototype version. The latter device is a prototype but with the connected antenna it behaves like a commercial, passive RFID tag. It is an HF tag using a frequency of 13.56 MHz in order to communicate with the reader and the communication protocol is implemented according to the ISO 14443A standard [15]. The chip consists of two main parts as it can be seen in Figure 1: the analog front-end (AFE) and the digital part. The antenna is connected to the AFE that provides the power supply and the clock signal to the digital part. The digital part is responsible for processing the commands to communicate with the reader. This part also contains a crypto unit with an AES implementation to provide symmetric-key cryptography. The AES part is implemented as special-purpose hardware to meet the most important requirements for RFID-tag chips: low power consumption and small chip area. Low power consumption is a requirement because the chip uses the power supply generated from the reader field. Chip area is an important factor concerning the production costs. More implementation details of the chip can be found in [12,24].

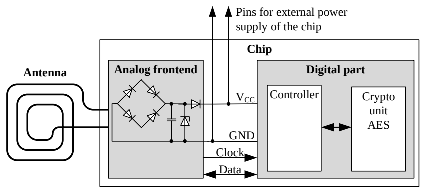

Fig. 1. Architecture of the evaluated chip.

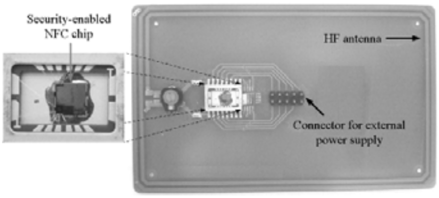

Fig. 2. The development board with the evaluated chip.

There are two countermeasures integrated into the AES implementation in order to increase the resistance against SCA attacks: the insertion of dummy rounds and shuffling. The chip processes in total 25 rounds during an AES encryption/decryption. Ten rounds relate to the real computation of AES and fifteen rounds are dummy rounds that process random data. The dummy rounds are inserted at the beginning and at the end in order to increase the effort for SCA attacks. With shuffling, the processing order of the bytes of the state is randomized. As the AES state consists of sixteen bytes every byte can be processed at sixteen different points in time. For DPA/DEMA attacks it is very important to know at which point in time a specific byte of the state is processed. Because of that fact shuffling increases the attack complexity.

As it can be seen in Figure 2 the prototype chip is mounted on a development board that contains an antenna with four windings. The board also allows to power the chip with an external power supply. If an external power supply with a voltage of 3.3 V or more is connected, the chip does not use the power supply extracted from the reader field. This gave us the ability to measure the power consumption of the chip with a resistor in the ground line.

In addition to the security-enabled NFC-tag chip we also use an FPGA-prototype tag for the evaluation. The implementation of the digital part on the FPGA-prototype tag is equal to the one on the evaluated ASIC chip. For a reader device, the FPGA-prototype tag appears like a regular, passive RFID tag. It uses an external power supply but the reader field is used for communication and for extracting the clock signal. We used the FPGA-prototype tag to show that the DEMA-attack results achieved with this device are comparable with the results from the real tag. Another advantage of the FPGA-prototype tag is that we have more control over this device. We could use, e.g., a debug pin in order to get a precise trigger signal. The FPGA prototype further gives the ability to correct bugs detected on the real chip and evaluate the effects of the modification. It is also important to mention that the FPGA-prototype version enables the chip developers to test the implementation before manufacturing the ASIC chip.

3 Measurement Setup

The LC584AM oscilloscope from LeCroy was used to record the traces and the recording process was controlled with a computer running MATLAB scripts. In order to establish the communication between computer and tag an RFID reader (Tagnology TagScan) was used. The EM probes to measure the electromagnetic emanation are from 'Langer EMV Technik'. We were able to record 1 trace per second on average. The reason for this rather low recording speed is on the one hand the two-step communication between computer and tag (the reader is in the middle) and on the other hand storing the traces on the computer is also a time-consuming process. Three different measurement setups were used in order to record the traces needed for the SCA attacks: the real-world scenario, the test scenario and the FPGA scenario.

Real-World Scenario The real-world scenario is the most important one because it can be used to attack the real NFC-tag chip without additional requirements like trigger pins or external power supply. In this scenario the electromagnetic emanation of the chip is measured using an EM probe. In order to measure only the electromagnetic emanation and not the reader signal we separated the chip and the antenna. This approach was presented by Hutter et al. [13] as well as by Caluccio et al. [4]. So the chip could be placed outside of the reader field for better measurement results. In our setup the distance between tag chip and antenna was 25 centimeters. The presented modification can be made with every RFID tag. A second EM probe was used in order to get the trigger information. This probe was placed inside the reader field. With these traces the reader commands could be easily identified. The EM traces were recorded with a sampling rate of 2.5 GS/s. A schematic of the measurement setup for this scenario can be seen in Figure 3. There were only small deviations in the duration between the reader command and the start of the AES calculation. With an alignment step these deviations could be removed and satisfying DPA-attack results could be achieved. The least-square matching method was used to align the traces.

Test Scenario The test scenario can only be performed with the development board and is also used to attack the ASIC chip. In that scenario the chip was powered with an external power supply, so the chip does not use the supply voltage extracted from the reader field. We inserted a resistor in the ground line in order to measure the power consumption of the chip. The value of the resistor was 100 Ω. A schematic overview of the measurement setup can be seen in Figure 4. The amplitude of the recorded trace increases significantly when the chip starts an AES calculation. This could be used as trigger information. With that setup the traces were not perfectly aligned so an alignment step was also necessary in order to get satisfying results of the DPA attacks.

FPGA Scenario The FPGA scenario was used to attack the FPGA-prototype tag. In this scenario the electromagnetic emanation of the FPGA was used as side-channel information. We used an EM probe to measure the electromagnetic

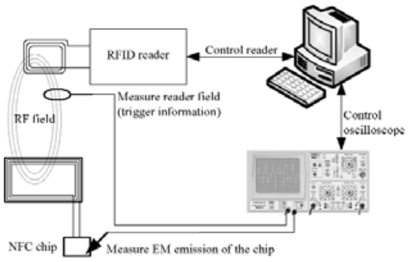

Fig. 3. Measurement setup of the real-world scenario.

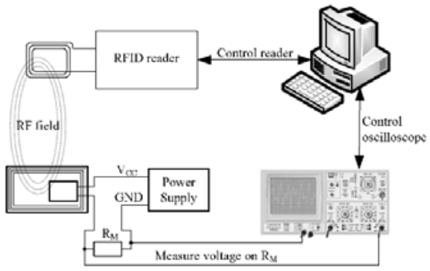

Fig. 4. Measurement setup of the test scenario.

emanation. One advantage of the FPGA-prototype tag for the EM measurements was that the FPGA chip is placed outside of the reader field. Several pins can be used as debug pins on the FPGA-prototype tag. We used one of these pins to indicate when the AES calculation starts. The signal of this pin could be used as trigger information. This trigger information was very accurate so no alignment step was necessary for successful DPA attacks on the FPGA prototype tag.

4 Side-Channel Analysis Results

In order to evaluate the security of the NFC tag we performed DPA and DEMA attacks on the AES implementation on the chip. As intermediate result we used the output of the S-box lookup for the first key byte in the first round of AES. The Hamming-weight model was used as power model to get the hypothetical power values. The Pearson correlation coefficient was used to calculate the correlation between the hypothetical power values and the recorded traces. The equation to calculate the correlation coefficient ρ can be found in [19].

As performance indicator for the attacks we used the number of required traces n to reveal the value of the first key byte. The relationship between the number of traces n and the correlation coefficient ρ is shown in Equation 1 [19]. For further calculations we used $z_{1-\alpha} = 3.719$ with $\alpha = 0.0001$.

$$n = 3 + 8\frac{z_{1-\alpha}^2}{ln^2\frac{1+\rho}{1-\rho}} \tag{1}$$

The results of the performed DPA/DEMA attacks can be split into two main parts: attacks with disabled countermeasures and attacks with enabled countermeasures. The attacks with disabled countermeasures were used to evaluate the performance of the different measurement setups. They equal an attack of an unprotected AES implementation and results can be achieved with a small number of traces. The randomization parameters for the countermeasures were fixed. This means that no dummy rounds are inserted at the beginning. Also shuffling is deactivated, so the first S-box operation always appears at the same point in time for every new AES encryption. With this step we show that the different

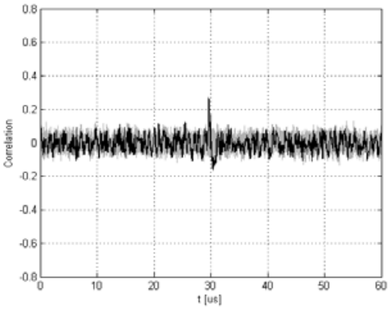

Fig. 5. DEMA-attack result of the real-world scenario with countermeasures disabled. In this case the whole amplitude of the EM trace was recorded.

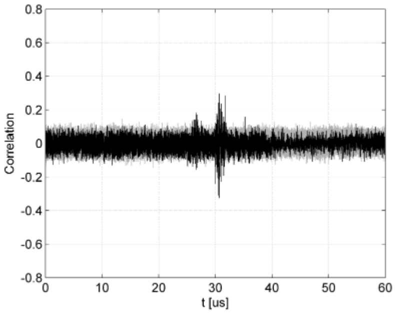

Fig. 6. DEMA-attack result of the real-world scenario with countermeasures disabled. In this case only the positive values of the EM trace were recorded.

approaches to measure the side-channel information as well as the attacks on the different hardware devices lead to comparable results which is a very important observation.

The attacks with enabled countermeasures could only be performed on the FPGA-prototype tag. The reason for this limitation is that the countermeasures on the ASIC version of the chip cannot be enabled because of a bug in the implementation. On the FPGA-prototype version the parameters for the countermeasures are random values. These values are updated for every AES encryption. In that case a random number of dummy rounds is inserted at the beginning and the first S-box operation is shuffled over sixteen positions in time. Before we started with the attacks we did an estimation for the needed effort for successful attacks with enabled countermeasures based on the results with disabled countermeasures.

4.1 Measurements with Disabled Countermeasures

Figure 5 shows the result of the DEMA attack on the security-enabled NFC tag for the real-world scenario. Here the positive as well as the negative part of the EM trace was recorded. The black correlation trace contains a clearly visible peak and belongs to the correct key hypothesis. The maximum correlation value for this attack is 0.267. According to Equation 1, 373 traces are required to obtain the correct value for the first key byte. In order to get a satisfying result two preprocessing steps had to be performed on the recorded traces: filtering and aligning. A lowpass filter with a stop frequency of 8 MHz was used to filter out surrounding noise and the reader signal. The filtered traces had to be aligned because the used trigger signal, the pattern in the communication, was not accurate enough. In order to achieve an even higher correlation value, we performed further measurements where we only recorded the positive values of the EM traces. So we could increase the resolution of the voltage values. As a result we got a higher correlation value of 0.325 and the result can be seen in

Figure 6. According to Equation 1, with 246 traces the correct value for the first key byte could be found. With this improvement we were able to decrease the number of required traces from 373 to 246.

As a second experiment we performed a DPA attack using the test scenario. In this scenario we used an external power supply for the chip and measured the power consumption with a resistor in the ground line. Here we got a correlation value of 0.664 for the correct key hypothesis. About 47 traces are needed in order to reveal the value of the first key byte.

In the FPGA case about 54 traces are needed in order to perform a successful attack. For comparison we have plotted the result of the DEMA attack on the FPGA prototype tag in Figure 7. Here the correlation value for the correct key hypothesis is 0.629. Filtering the recorded traces was the only required preprocessing step for a successful attack. Here a bandpass filter with a lower frequency of 15 MHz and an upper frequency of 25 MHz had to be used in order to get satisfying results. A dedicated pin was used for the trigger information and so the traces did not have to be aligned afterwards.

The test scenario and the FPGA scenario produce similar results. Successful attacks can be performed with low effort, only 47 and 55 traces are needed to reveal the value of the first key byte, respectively. However both of these attacks cannot be performed on a real RFID tag. The real-world scenario that we have used for our measurements can be performed on real RFID tags as well. We were able to perform successful DEMA attacks on the unprotected AES implementation with 246 traces using that scenario, compared to the FPGA scenario the effort increases by a factor of 4.5. This result enables chip designers to evaluate the security of other implementations using the same production process in an early design step. An FPGA implementation of the chip can be used in order to evaluate the resistance of the ASIC against SCA attacks. If there is a redesign of an existing ASIC (e.g. new SCA countermeasures are implemented), the presented approach can be used to evaluate the security of the new ASIC using the results of the SCA attacks on the FPGA implementation. We also use the achieved results from above in the following section in order to evaluate the security of the protected AES implementation.

4.2 Measurements with Enabled Countermeasures

Before we started with the attack on the protected AES implementation, we did some estimations on the effort needed for a successful attack. These estimations can be found in Table 1. The dummy-round countermeasure increases the number of traces needed for a successful attack by a factor of 256 and also shuffling increases the number of traces needed for a successful attack by a factor of 256. As a result the total number of traces required for a successful attack increases by a factor of $256^2 = 65\,536$. For a successful attack on the unprotected implementation 55 traces were needed and this value multiplied with 65 536 gives nearly four million traces. With our recording speed of one trace per second this would lead to a recording time of about 42 days! For the real-world scenario this would lead to a recording time of 189 days (using the factor of 4.5 from above). This effort is rather high so we tried to find a way to reduce the impact of the

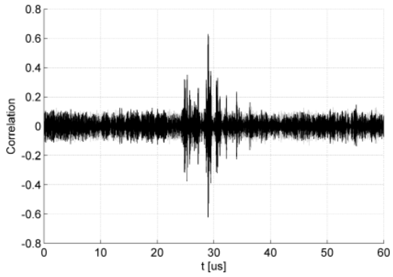

Fig. 7. DEMA-attack result of the FPGA scenario with countermeasures disabled.

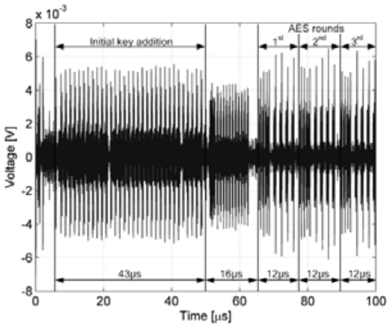

Fig. 8. Filtered EM trace of the initial key addition and the first three rounds of AES.

Table 1. Estimate of the required number of traces for a successful DPA attack with enabled countermeasures.

	Estimated number of traces		
Countermeasures	**FPGA scenario**	**Test scenario**	**Real-world scenario**
No active countermeasures	55	47	246
Shuffling	14 080	12 032	62 976
Shuffling and dummy rounds	$> 3\,600\,000$	$> 3\,000\,000$	$> 16\,100\,000$

countermeasures. In many applications the number of encryptions is also limited to a specific value, so a DPA/DEMA attack can only be successful if the number of required traces is below this value.

The approach we used for reducing the impact of the countermeasures was to get some information about the random value defining the number of dummy rounds inserted at the beginning. For that purpose we recorded a set of 100 traces containing the initial key addition and the first AES round. A plot showing one trace of this set can be found in Figure 8. Our observations showed that delay cycles are also inserted during the initial key addition. After some analysis of the traces we found a pattern during the initial key addition. When calculating the difference of two traces, peaks appear at different points in time depending on the random variable defining the number of dummy rounds inserted at the beginning. For the set of 100 traces we have calculated the difference for every single pair of traces and could observe three different cases which are illustrated in Figure 9:

– In the first case no significant peak can be identified.
– In the second case four significant peaks can be identified which have nearly the same amplitude.
– In the third case again four peaks in the difference trace can be identified but one of these four peaks has a significantly higher amplitude.

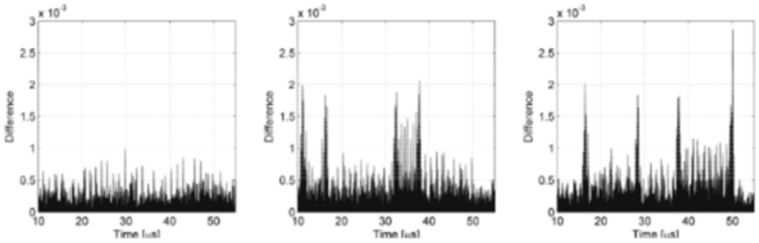

Fig. 9. The left plot shows the difference of two traces without significant peaks (first case). The plot in the middle shows the difference of two traces with four peaks with comparable amplitude (second case). The plot on the right side shows the difference of two traces with one significant peak (third case). Traces recorded with the FPGA scenario have been used to generate these plots.

Following the upper observation we made the following assumptions: If the difference of two traces leads to the first case, the same random value was used for the dummy-round countermeasure of both encryptions. If the difference of two traces leads to the second case different random values were used for the dummy-round countermeasure for the two encryptions. Finally, if the difference leads to the third case a specific value was used for the countermeasure during one of the two encryptions.

In a first attack scenario we used the third case to filter out the traces with one specific number of dummy rounds inserted at the beginning. First we recorded a set of traces including the first 16 rounds (there are 25 rounds in total, 15 dummy rounds and ten real AES rounds). In a next step we created a new set of traces containing only these traces where the specific number of dummy rounds were inserted at the beginning. In order to visualize our approach to filter out the traces we have plotted the difference matrix for 100 traces which can be seen in Figure 10. This matrix contains the absolute maximum value of the difference of the two traces corresponding to the row number and column number. It is clearly visible that for some traces this value is higher (darker points) compared to other traces. In order to build the reduced set of traces we have selected only these traces corresponding to a row number with a high value (dark points). As we assume a unique distribution of the random value the size of this new set is about 1/16 of the size of the original set. On the reduced set we performed a DEMA attack. In order to conduct the first attack scenario we recorded a set of 320 000 traces. After filtering out the dummy rounds with the approach presented above the size of the set reduced by a factor of 16 to 20 000 traces. The reduced set only contains traces with a specific number of dummy rounds at the beginning followed by the first real AES round processing the attacked intermediate value. On this reduced set we performed a DEMA attack and were able to reveal the value of the first key byte. It figured out that 15 dummy rounds are inserted at the beginning when the special pattern appears in the difference traces. Figure 11 shows the result of this attack. Compared to the results in Figure 5, Figure 6 and Figure 7 no single correlation peak can be identified.

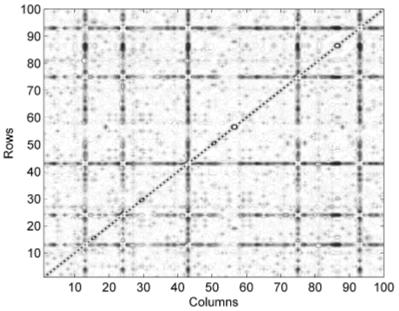

Fig. 10. Visualization of the difference matrix for 100 traces.

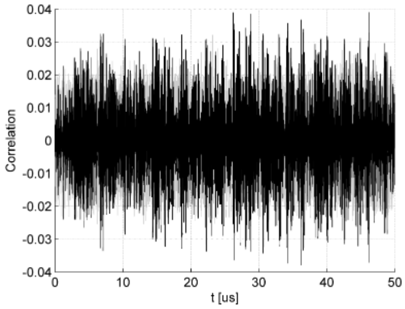

Fig. 11. DEMA-attack result of the FPGA scenario with active countermeasures.

This is because shuffling spreads the single peak on 16 different points in time. With a bigger set of traces the 16 peaks in the correlation trace of the correct key hypothesis could be identified better. The maximum correlation value of the attack is 0.03931.

In a second attack scenario we used the first case of our observations above to split the recorded traces into 16 groups. As we had the ability to read out the random value used for the randomization for every encryption by a small change in the FPGA implementation we were able to verify the performance of the clustering approach. All the traces in one group belong to encryptions where the same random value for the dummy rounds was used. In order to perform the clustering we used the K-means clustering function provided by MATLAB with the squared euclidian distance as distance measure. We also did a performance analysis where we performed the group building for 100 to 500 traces. There is a linear relationship between runtime of the group building algorithm and the number of traces used. The amount of correctly classified traces is between 96% and 98%. The building of the groups takes about 0.25s per trace. It has to be mentioned that for an attack the group building step has to be conducted only for e.g. the first 100 traces. The huge remaining part of the traces can be clustered by just comparing with the groups. We achieved similar results by comparing with one single trace of each group and by comparing with the mean trace of each group. Here we were able to decrease the time to group one trace to 0.1s. The length of the traces used for the mentioned experiment was 250 000 samples. The runtime strongly depends on the length of the used traces.

With the clustering approach it is now possible to decrease the number of required traces for a successful DEMA attack on the secret AES key. First of all we recorded a set of 320 000 traces containing the initial key XOR and the first three rounds. Next we applied the clustering algorithm to group the traces into 16 groups. The clustering step for 320 000 traces takes about 9 hours on a standard desktop computer. Every group contains on average 20 000 traces as the random value defining the number of dummy rounds at the beginning follows a uniform distribution. Now there are more possibilities to conduct the attack. One way is to put the focus just on the first round and perform a DEMA attack on each of the 16 groups separately. The result of the attack using one specific group (the one where no dummy rounds are inserted at the beginning) leads to a significantly higher correlation value for the correct key byte. The shuffling countermeasure is still active but Table 1 shows that 20 000 traces are sufficient to find the correct key value even in the presence of shuffling. A second way is to combine the first and the second round and trying out all different combinations of two groups. That means to pick out the first round of group A and the second round of group B and preform a DPA attack on this combination. If group A is the group where no dummy rounds are inserted at the beginning and group B is the group containing traces where one dummy round is inserted at the beginning the DPA attack leads to a correct result. This approach leads to a higher computational effort because there are 256 possible combinations. The number of required traces decreases because only 10 000 traces are needed in each group. So the total number of traces decreases to 160 000. The runtime for the DEMA attacks increases to nearly 15 hours in that case. Furthermore we estimated the complexity for the focus on three rounds and the combination of three groups. As the number of possible combinations increases to 4 096 the runtime for the DEMA attacks increases to nearly 6.5 days. The positive effect is that the number of required traces decreases again. A summary of the upper scenarios can be found in Table 2.

Table 2. The influence of the clustering approach on the number of traces needed for a successful DPA attack as well as on the calculation time for the attack.

Groups used	**Comb.**	**Required traces per group**	**Required traces overall**	**Time for DPA attack on one group**	**Total time**
				[s]	[s]
1	16	20 000	320 000	400	6 400
2	256	10 000	160 000	200	51 200
3	4 096	6 666	106 666	133	544 768

In a last experiment we used another preprocessing step called windowing in order to reduce the impact of shuffling on the attack complexity. This approach is presented in the book of Mangard et al. [19]. It should be possible to decrease the attack complexity by a factor of four with windowing. A key factor for this step is to find a good window pattern. In our attacks it was very hard to find such a pattern and so we could only achieve a complexity reduction of 1.4.

Table 3 compares the FPGA scenario and the real-world scenario. Based on the correlation values of the attacks using the FPGA scenario the number of required traces n using Equation 1 are calculated. With the number of traces the attack duration can be calculated as our recording speed is one trace per second. With the knowledge that the attack complexity for the real-world scenario increases by a factor of 4.5 the number of required traces to perform a successful attack as well as the attack duration can be given.

Table 3. Comparison of the number of needed traces and the duration for recording the required amount of traces for the FPGA scenario and the real-world scenario. Also the influence of the used preprocessing techniques is illustrated. With windowing the impact of shuffling can be decreased. With our clustering approach the impact of the dummy rounds can be decreased. The number in the brackets denotes the number of used groups for the DPA attack.

		FPGA scenario		**Real-world scenario**	
Countermeasures	**Preprocessing**	**n**	**Time**	**n**	**Time**
No countermeasures	-	55	< 1 min	246	< 5 min
Shuffling	-	17 886	5 hours	80 000	23 hours
	Windowing	9 119	2.5 hours	41 036	11.4 hours
Shuffling, dummy rounds	-	4 571 000	53 days	20 480 000	246 days
	Clustering(1)	320 000	3.7 days	1 440 000	17 days
	Clustering(2)	160 000	1.9 days	720 000	8.5 days
	Clustering(3)	106 666	30 hours	480 000	5.6 days

4.3 Summary of the Results

As we have shown with the DPA/DEMA attacks performed on the unprotected AES implementation the effort (needed number of traces) for a successful attack for the real-world scenario is 4.5 times higher compared to the FPGA scenario. Table 3 draws a comparison between the effort for a successful DPA attack using the FPGA scenario and the real-world scenario. Attacks on the protected AES implementation could only be performed in the FPGA scenario because of a bug in the ASIC chip. The effort for the real-world scenario can be estimated based on the results for the attacks on the unprotected AES implementation.

A successful attack on an unprotected AES implementation using the FPGA scenario can be performed in less than one minute. With the real-world scenario the value of a key byte can be revealed within five minutes. This result emphasises again that it is possible to successfully attack an unprotected AES implementation on an RFID tag with very low effort and that countermeasures have to be implemented.

If the AES implementation is protected with countermeasures against SCA attacks (insertion of dummy rounds and shuffling) as it is done on the FPGA-prototype tag the attack complexity increases significantly. If no patterns can be found to decrease the influence of the countermeasures 53 days are required in order to record the amount of traces needed for a successful DEMA attack on the FPGA-prototype tag. For the real-world scenario the duration has to be multiplied by a factor of 4.5, so the duration for a successful attack increases to 246 days.

If the attacker can find a pattern to mitigate the influence of the used countermeasures the effort for a successful attack can be decreased. As we have shown with the FPGA scenario we could find 2 different ways to decrease the attack complexity. We were able to reveal some information about the number of dummy rounds inserted before the first real AES round. Furthermore we could show that with our approach it is possible to scale down the number of required traces by adding more computational effort afterwards. This can be an important step if the number of encryptions is limited to a fixed value (e.g. 200 000).

5 Conclusion

In this work we presented DPA and DEMA attacks on the AES implementation of a security-enabled NFC tag. For the attacks we used an FPGA-prototype version as well as a manufactured ASIC chip. Three different measurement setups were used: a real-world scenario, a test scenario and an FPGA scenario. We could show that the results of the attacks on the ASIC chip using the real-world scenario are comparable with the attack results on the FPGA prototype. The effort for the attack on the ASIC chip is 4.5 times higher compared to the attack on the FPGA prototype. The attacks on the ASIC chip were performed using a real-world scenario without a dedicated trigger pin or an external power supply of the chip. The attacks on the FPGA prototype were performed under laboratory conditions. The attacked AES implementation also has countermeasures against SCA attacks integrated which are the insertion of dummy rounds and shuffling. We were able to enable and disable the countermeasures and so we found a pattern to mitigate the impact of the dummy-round countermeasure. This pattern gave us the ability to group the recorded traces according to the number of dummy rounds inserted before the first real AES round. As a consequence the attack complexity decreased. Only some knowledge (usage of the dummy-round countermeasure) about the AES implementation was needed in order to find this pattern so the presented approach is a serious thread for implementations with countermeasures against SCA attacks. We could show that with the presented approach it is possible to decrease the number of needed traces for a successful DPA attack. In our special case the number of traces could be reduced from 320 000 to less than 110 000 traces. As a side-effect the computational effort increases but within acceptable limits.

Acknowledgements.

The work presented in this article has been supported by the European Commission through the ICT programs TAMPRES (under contract ICT-SEC-2009-5-258754) and ECRYPT II (under contract ICT-2007-216676).

References

1. Auer, A.: Scaling Hardware for Electronic Signatures to a Minimum. Master thesis, University of Technology Graz (October 2008)
2. 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)

3. Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., Szydlo, M.: Security Analysis of a Cryptographically-Enabled RFID Device. In: USENIX Security Symposium, Baltimore, Maryland, USA, July-August. pp. 1–16. USENIX (2005)
4. Carluccio, D., Lemke, K., Paar, C.: Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. In: Oswald, E. (ed.) Workshop on RFID and Lightweight Crypto – RFIDSec, July 13-15, Graz, Austria. pp. 44–51 (2005)
5. Courtois, N.T., O'Neil, S., Quisquater, J.J.: Practical Algebraic Attacks on the HITAG2 Stream Cipher. In: Samarati, P., Yung, M., Martinelli, F., Ardagna, C.A. (eds.) Information Security Conference – ISC. LNCS, vol. 5735, pp. 167–176. Springer, Heidelberg, Pisa, Italy (September 2009)
6. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.T.M.: On the Power of Power Analysis in the Real World: A Complete Break of the KEELOQ Code Hopping Scheme. In: Wagner, D. (ed.) Advances in Cryptology – CRYPTO, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21. pp. 203–220. No. 5157 in LNCS, Springer, Heidelberg (2008)
7. 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)
8. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) Cryptographic Hardware and Embedded Systems – CHES, Third International Workshop, Paris, France, May 14-16. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001)
9. Hämäläinen, P., Alho, T., Hännikäinen, M., Hämäläinen, T.D.: 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, Dubrovnik, Croatia, 30. August-1 September. pp. 577–583. IEEE Computer Society (September 2006)
10. 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 (LNCS) (September 2008)
11. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. In: Buhler, J. (ed.) Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
12. Hutter, M., Feldhofer, M., Wolkerstorfer, J.: A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES like Sardines. In: Ardagna, C.A., Zhou, J. (eds.) Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems – WISTP, Fifth International Workshop, Heraklion, Crete, Greece, June 1-3. LNCS, vol. 6633, pp. 144–159. Springer, Heidelberg (2011)
13. 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)
14. Hutter, M., Medwed, M., Hein, D., Wolkerstorfer, J.: Attacking ECDSA-Enabled RFID Devices. In: Abdalla, M., Pointcheval, D., Fouque, P.A., Vergnaud, D. (eds.)

Applied Cryptography and Network Security – ACNS 2009, 7th International Conference, Paris-Rocquencourt, France, June 2-5. LNCS, vol. 5536, pp. 519–534. Springer, Heidelberg (May 2009)

15. International Organization for Standardization (ISO): ISO/IEC 14443: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards (2000)
16. Kasper, T., Oswald, D., Paar, C.: EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. In: Youm, H.Y., Yung, M. (eds.) Information Security Applications – WISA, 10th International Workshop, Busan, Korea, August 25-27. LNCS, vol. 5932, pp. 79–93. Springer, Heidelberg (2009)
17. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) 16th Annual International Cryptology Conference – CRYPTO, Santa Barbara, CA, USA, August 18-22. pp. 104–113. No. 1109 in LNCS, Springer, Heidelberg (1996)
18. 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)
19. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
20. Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H.: Pushing the Limits: A Very Compact and a Threshold Implementation of AES. In: Paterson, K.G. (ed.) Advances in Cryptology – EUROCRYPT, 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19. LNCS, vol. 6632, pp. 69–88. Springer, Heidelberg (2011)
21. Nohl, K.: Cryptanalysis of Crypto-1. Computer Science Department University of Virginia, White Paper (2008)
22. Oren, Y., Shamir, A.: Remote Password Extraction from RFID Tags. IEEE Transactions on Computers 56(9), 1292–1296 (September 2007)
23. Oswald, D., Paar, C.: Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In: Cryptographic Hardware and Embedded Systems – CHES, 13th International Workshop, Nara, Japan, September 28 - October 1. LNCS, vol. 6917/2011, pp. 207–222. Springer, Heidelberg, Berlin, Heidelberg (2011)
24. Plos, T., Feldhofer, M.: Hardware Implementation of a Flexible Tag Platform for Passive RFID Devices. In: 14th Euromicro Conference on Digital System Design Architectures, Methods and Tools – DSD, Oulu, Finland, August. pp. 293–300. IEEE Computer Society (August 2011)
25. Poschmann, A.Y.: Lightweight Cryptography - Cryptographic Engineering for a Pervasive World. Ph.D. thesis, Faculty of Electrical Engineering and Information Technology, Ruhr-University Bochum,Germany (Februrary 2009)
26. Quisquater, J.J., Samyde, D.: A new Tool for Non-Intrusive Analysis of Smart Cards Based on Electro-Magnetic Emissions, the SEMA and DEMA Methods,. Presented at the rump session of EUROCRYPT 2000 (2000)
27. Tuyls, P., Batina, L.: RFID-Tags for Anti-counterfeiting. In: Pointcheval, D. (ed.) Topics in Cryptology – CT-RSA, San Jose, CA, USA, February 13-17. LNCS, vol. 3860, pp. 115–131. Springer, Heidelberg (2006)