Attacking ECDSA-Enabled RFID Devices

Michael Hutter, Marcel Medwed, Daniel Hein, and Johannes Wolkerstorfer

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

Abstract. The elliptic curve digital signature algorithm (ECDSA) is used in many devices to provide authentication. In the last few years, more and more ECDSA implementations have been proposed that allow the integration into resource-constrained devices like RFID tags. Their resistance against power-analysis attacks has not been scrutinized so far. In this article, we provide first results of power-analysis attacks on an RFID device that implements ECDSA. To this end, we designed and implemented a passive RFID-tag prototype. The core element of the prototype is a low-power ECDSA implementation realized on 180 nm CMOS technology. We performed power and electromagnetic attacks on that platform and describe an attack that successfully reveals the private-key during signature generation. Our experiments confirm that ECDSA-enabled RFID tags are susceptible to these attacks. Hence, it is important that they implement countermeasures which prevent the forging of digital signatures.

Keywords: Radio-Frequency Identification, RFID, Side-Channel Analysis, ECDSA, Elliptic Curve Cryptography, Implementation Security.

1 Introduction

Radio Frequency Identification (RFID) is an emerging technology that is becoming more and more important in our daily life. There already exist billions of RFID devices and their integration into existing applications seems almost inevitable. Due to the widespread use of this wireless technology, security issues have become a primary concern in the past few years. Especially public-key enabled RFID devices have gained importance because they allow an easier and more secure key management than symmetric solutions. This article focuses on the security of RFID devices that can generate elliptic curve digital signatures.

RFID devices consist of a tiny microchip that is connected to an antenna. These so-called tags are typically powered passively by a reader via an electromagnetic field. This field is also used for the communication between the tags and the reader. Typical security applications of RFID are access-control systems, cashless payment, and the electronic passport. These applications need the devices to make use of cryptographic algorithms to provide required services such as authentication, confidentiality, integrity, and non-repudiation. The cryptographic algorithms have to be light-weight in terms of power and area to

M. Abdalla et al. (Eds.): ACNS 2009, LNCS 5536, pp. 519–534, 2009.

cope with the limited resources in large-scale RFID applications. Due to these constraints, most tags that are now available typically rely on proprietary algorithms or symmetric primitives that have been proven to be suitable for RFID. Large effort has been made in this field to enable resource-constrained implementations of algorithms such as AES [5], DESL [18], PRESENT [3], and HIGHT [9]. Although symmetric algorithms can provide many of the required security assurances, the advantages of facilitated key management offered by asymmetric algorithms would be very desirable for RFID systems. However, they are much more complex to implement. In respect to these facts, many light-weight solutions have been proposed such as NTRU [8], XTR [19], and elliptic-curve based schemes. A typical application that uses asymmetric cryptography is the electronic passport. It comes with an embedded microchip that is used to prove the origin of the passport and to authenticate the owner. This process is referred to as *active authentication* and uses standardized algorithms such as RSA [30], DSA [24], or ECDSA [2].

Besides the growing demand for RFID devices and their widespread integration into existing security applications, there have been many articles published during the last decade that emphasize the vulnerability of such cryptographic devices against implementation attacks. Amongst the most powerful attacks are side-channel attacks that were first introduced by Kocher et al. [16] in 1996. These attacks allow the extraction of the secret key by measuring the power consumption [17], electromagnetic emanation [1,6,29], or timing information [16]. In the context of RFID, Oren and Shamir [27] have shown the first side-channel attack which allows to reveal the *kill* password of ultra-high frequency (UHF) tags, in 2006. They performed a simple power analysis (SPA) attack by observing one power trace that is reflected from the tag to the reader. This backscattered power trace changes depending on the processed data. The first differential power analysis (DPA) attack on RFID devices has been performed by Hutter et al. [10] in 2007. They analyzed hardware and software AES implementations of high frequency (HF) tag prototypes by means of power and electromagnetic analysis. All devices have been successfully attacked using less than 1 000 power traces. Plos [28] demonstrated the susceptibility of UHF tags against DPA attacks in 2008. He analyzed commercially-available RFID tags and determined data-dependent emanations at a distance of up to one meter. However, all available publications describe attacks on either kill-password extraction or symmetric primitives. So far, there exist no article that investigates DPA attacks on public-key enabled RFID tags.

In this article, we provide the first results of side-channel attacks on a public-key enabled RFID device. In order to evaluate the effectiveness of such attacks on RFID tags, we designed a prototype that is able to be powered passively by the field of a reader. The prototype includes a low-power hardware ECDSA implementation fabricated in 180 nm CMOS technology. The implementation is able to authenticate itself to a reader by generating digital signatures. Furthermore, we are the first who provide a DPA attack on a hardware implementation of ECDSA. We show how to reveal the private key during signature generation

by measuring the electromagnetic emanation of the tag. In addition, we describe a useful pre-processing technique for improving side-channel attacks on RFID by applying a trace-decimation technique. All attacks have been successful and led us to the conclusion that public-key enabled RFID devices are as vulnerable as symmetric-based RFID devices. It has been shown that wireless devices are susceptible to these attacks as much as contact-based powered devices.

The article is structured as follows. Section 2 describes power-analysis attacks on passive RFID devices in general. Section 3 is dedicated to attacks on ECDSA implementations. We describe the exploitation of different information leakages of ECDSA and propose a DPA attack on the private-key operations during signature generation. Section 4 details our RFID-tag prototype. In Section 5 we describe the measurement setup and side-channel pre-processing techniques that are used in our experiments to perform power-analysis attacks. The results of our experiments are presented in Section 6. Conclusions are drawn in Section 7.

2 Power Analysis of Passive RFID Devices

Side-channel analysis of passive RFID devices is a challenging task due to several reasons. In this section, we give an overview on various issues regarding the acquisition and analysis of side-channel information that are exploited from passive RFID tags.

Passive tags differ from conventional contact-based devices in several ways. First, passive tags only possess two antenna connections. Indeed, there are no dedicated power-supply pins available where a resistor can be placed in series to measure the consumed power. An alternative way of side-channel extraction is the sensing of electromagnetic emanation. The current flow within the microchip of the RFID tag produces an electromagnetic field. This field contains different signals such as the square-wave clock or signals that are caused by data-dependent processing. These signals can be sensed by magnetic near-field probes that are placed directly on the surface of the chip [1]. However, while such attacks will succeed for many contact-based devices, this may not be the case for passive RFID tags. Passive tags have been designed for low-power operation and consume only a few micro Watts of power. Special measurement equipment is therefore necessary to separate and amplify the weak side-channel signals that are emitted from the tags.

In RFID environments, we are actually concerned with another source of electromagnetic emanation. There is not only the weak emanation of the tags but also the emanation of the reader device. This reader field is typically between 40 dB and 80 dB higher than the signals emitted by the tags. As a result, interesting signal emissions of the tags may be unintentionally overwhelmed by the occurring interferences of the reader. The data-acquisition resolution of the measurement equipment is thus inevitably reduced since the weak signals of the tag are superimposed onto the much higher reader field. In addition to the lower acquisition resolution, this reader field is not synchronized with the measurement equipment which causes power-trace misalignments in both the time and

the amplitude dimension. The reader is a high noise source and therefore makes side-channel analysis difficult to perform. The main challenge of electromagnetic measurements in this context is therefore to minimize the impact of this reader signal and to overcome the resulting misalignment of measured power traces.

Another issue which is of major concern in RFID environments is the compression of side-channel traces. Passive RFID tags are powered by the electromagnetic field of a reader. Most of these tags also extract the clock signal out of this field. In order to comply with the low-power requirement, they often use a low clock frequency in the kHz range. The processing of data and especially the computation of asymmetric functions therefore takes a long time (up to several milliseconds). Side-channel attacks on public-key enabled RFID devices require compression techniques to reduce the complexity of storing and subsequent processing of millions of sample points that are acquired throughout the tag computation.

3 Power Analysis Attacks on ECDSA Implementations

ECDSA is the elliptic curve-based variant of the digital signature algorithm (DSA). The DSA has been proposed in 1991 by the National Institute of Standards and Technology (NIST). Since then, many organizations have standardized ECDSA such as ANSI [2], IEEE [11], FIPS [24], and ISO/IEC [14]. In the following, we describe ECDSA in greater detail, discuss various power-analysis attacks that have been performed on different implementations, and present a DPA attack that reveals the private key during signature calculation.

In order to generate a digital signature using ECDSA, a message m is given as an input. By using the domain parameters $D = (q, FR, S, a, b, P, n, h)$, a random number k is first chosen in the interval from 1 to n. This random number is often referred to as ephemeral key. Then, an elliptic-curve point multiplication is performed using k and the base point P. The result is converted to an integer $\bar{x}_1$ in order to compute the intermediate value r. After that, the message m is hashed using the SHA-1 algorithm [26]. The signature generation is then generated within two steps. First, the private key d is multiplied with the intermediate value r. The result is then added to the output of the hashed message $e = h(m)$. Second, the value s is calculated by inverting the ephemeral key k and multiplying it with the output of step one. The generated ECDSA signature that is returned consists of the tuple (r, s). Algorithm 1 shows the signature-generation scheme.

There exist many articles that present power-analysis attacks on elliptic curve-based algorithms. One of the first publications is due to Coron [4] in the year 1999. He showed that the scalar multiplication is highly susceptible to SPA attacks. One way to implement the scalar-multiplication is to use the double-and-add algorithm. By simply inspecting one measured power trace of such implementations, a difference in the power consumption can be observed depending on whether doubling or adding was performed. Several countermeasures have been proposed including scalar blinding techniques [4], unified point operations [15],

Algorithm 1. Signature-generation scheme using ECDSA

Require: Domain parameters $D = (q, FR, S, a, b, P, n, h)$, private key d, message m.
Ensure: Signature (r, s)
1: Select $k \in [1, n-1]$
2: Compute $[k]P = (x_1, y_1)$ and convert x_1 to an integer $\bar{x}_1$
3: Compute $r = \bar{x}_1 \mod n$. If $r = 0$ then go back to step 1.
4: Compute $e = H(m)$.
5: Compute $s = k^{-1}(e + dr) \pmod n$. If $s = 0$ then go back to step 1.
6: Return (r, s)

or the Montgomery point ladder [22]. Nevertheless, recently Medwed et al. [21] have shown attacks on implementations by using template-based SPA attacks. They have been able to successfully reveal the ephemeral key of implementations including SPA countermeasures. However, up to now there neither exist articles describing DPA attacks on ECDSA nor are there publications that reveal the private key directly instead of extracting the ephemeral key to calculate the private key afterwards.

3.1 Our Contribution and Description of the Attack

In the following, we describe a DPA attack that reveals the private key during signature generation. The target of the attack is an intermediate value that depends on the private key on the one hand and that depends on some random value on the other hand. Regarding the ECDSA scheme described in Algorithm 1, the private key d is multiplied with the output of the scalar multiplication r. The private key is static and the output of the scalar multiplication is random since the ephemeral key k is chosen randomly for each signature generation. Furthermore, r is publicly known because it is part of the signature. In the light of these facts, we are able to perform a DPA attack on intermediate values that are processed during the calculation of the multi-precision integer multiplication $d * r$.

Common hardware implementations for multi-precision multiplication are the operand scanning and the product scanning (Comba) algorithm which are depicted in Figure 1. Both algorithms multiply the words of two n-word long operands. In our case, those are r_i (the input) and d_j (the key). The resulting partial products are then added to a cumulative sum p. This results in n^2 partial products. Note that one word of the private key is processed n times during the whole integer multiplication.

What seems obvious at first glance turns out to be more complex in practice. The integer multiplication is a linear function that multiplies a constant value with a random input value. That means that shifted bit combinations of a key word have a linear impact to the multiplication result. When the key is shifted x times, the result is also shifted x times. Therefore, it is evident that in power-analysis attacks, one or more correlation peaks occur for only one key word. This is due to the fact that all bit combinations of the key word will result in

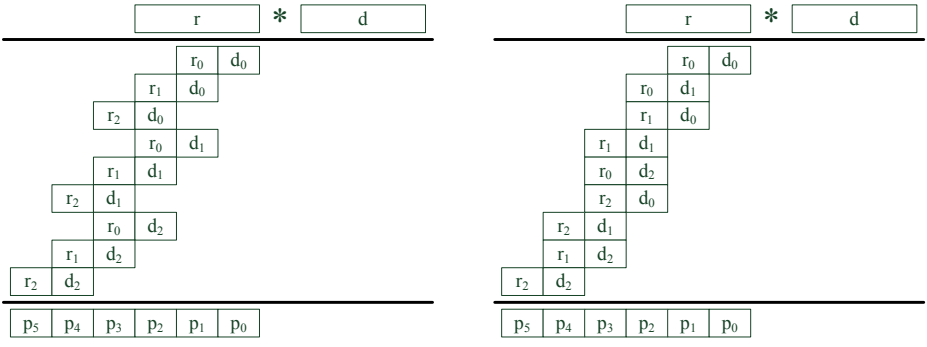

Fig. 1. Operand scanning form (left) and product scanning form (right)

the same Hamming-weight[1] value of the multiplication output. The number of possible shifts s of the key word d_i can be calculated as follows:

$$s(d_i, l) = log_2(gcd(d_i, 2^l)) + l - \lfloor log_2(d_i) + 1 \rfloor, \tag{1}$$

where l represents the word size. Note that the maximum number of key shifts is equal to the word size, i.e. 16 for a device using 16 bit operands (in this case the key word has a Hamming weight of one and the value of the shifted key combinations are a multiple of 2^x where $x = 0..15$). Due to these facts, the decision of which hypothetical key is the correct one and which are incorrect keys seems therefore infeasible. It is clear that this makes a DPA attack much more inefficient compared to attacks on intermediate values that occur after non-linear functions such as the S-box in DES [23] or AES [25].

Our attack can be separated into two steps. In the first step, we target the output of all partial products and perform a DPA attack on that intermediate value. For each partial product, we obtain one or more promising key candidates due to the reasons described above. For a device with a 16 bit word size, for example, we obtain up to 16 promising key candidates. Hence, we get up to 16 key candidates for each private-key word d_i. In the second step, we target the output of the final multiplication product p. Each word of this product depends on one or more different key words. Thus, we can use the information obtained from the first step and use all obtained key candidates d_i to perform an attack on the final product words p_i. After revealing the key candidates for d_0 and d_1, for example, we can attack the second product word p_1 to obtain the correct key word d_0. Incorrect key hypotheses will show low correlation peaks so that they can be eliminated from the correct key hypothesis that causes a higher correlation. By following this way, a DPA attack on each of these product words p_i will yield all private-key words d_i successively.

[1] The Hamming weight power model is often used in practice and is further used in order to describe the attack.

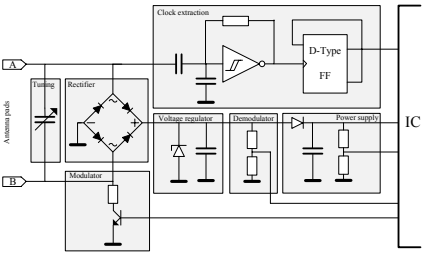

Fig. 2. Schematic of the analog front-end of our passively powered RFID-tag prototype

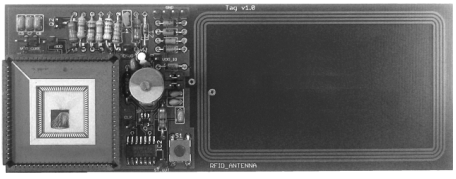

Fig. 3. A passively powered RFID-tag prototype that is capable of generating digital signatures using ECDSA

4 A Passive ECDSA-Enabled RFID-Tag Prototype

In this section, we present the design and implementation of the passively powered RFID-tag prototype that has been used throughout our experiments. The prototype consists of an antenna, an analog front-end, and a low-power digital controller. The antenna has four windings and has been designed according to ISO 7816 [12]. The antenna is connected to an analog front-end that transforms the received analog signals of the reader to the digital world of the digital controller. The controller includes a digital RFID front-end and a low-power hardware implementation of ECDSA. In the following, we describe the analog front-end and the digital controller in a more detail.

4.1 The Analog Front-End

The analog front-end is composed of the seven parts shown in the schematic view in Figure 2. In the first stage, the antenna is connected to a matching circuit which tunes the antenna to the 13.56 MHz carrier frequency of the reader. After that, a bridge rectifier has been assembled using low-voltage drop schottky diodes. The rectified signal is then smoothed and fed into a slow envelope detector to provide a stable power supply for the digital controller.

In order to comply with many commercial RFID tags, we designed a clock extraction circuit that is able to regenerate a system clock out of the 13.56 MHz reader signal. For this, a relaxation oscillator has been implemented using an inverting Schmitt trigger, one resistor, and a capacitor which produce a stable 13.56 MHz square-wave clock. The clock is then divided by two using a d-type flip-flop to provide a 6.78 MHz clock frequency that is needed for the controller.

For receiving and sending of data, both a modulation and a demodulation circuit have been integrated. For data modulation, a resistor is used that can be connected and disconnected to the antenna by the controller. After switching the resistor, a significant amount of additional power is drawn out of the reader field. This so-called load modulation is then detected and demodulated by the reader.

4.2 The Digital ECDSA-Enabled RFID Controller

The digital controller is an elliptic-curve point multiplication device with an ISO 15693 [13] compatible digital RFID front-end. It is capable of computing the multiplication of a scalar value with a point on the NIST standardized elliptic curve B-163 [24]. The B-163 curve is defined on the binary extension field $\mathbb{F}_{2^{163}}$. The controller was fabricated by the UMC L180 GII 1P/6M 1.8V/3.3V CMOS process. The controller has a total area of 15 630 Gate Equivalents (GE) while an overhead of 654 GE is incurred by components for production testing. The digital RFID front-end requires 1 726 GE and the ECC core 13 250 GE. This includes 1 346 GE for a memory slot to enable the separate setting of the ephemeral key k.

The controller must be operated at a fixed frequency of 6.78 MHz. This is half of the carrier frequency. Internally, this frequency supplies two different clock domains. One of them is used for the RFID interface and has a frequency of 106 kHz. The other one clocks the ECC core at 847.5 kHz. The whole chip has an estimated power consumption of about 176 µW.

5 The Measurement Setup

The measurement setup is composed of several parts. We used a PC, an RFID reader, the RFID-tag prototype, a digital sampling oscilloscope (DSO), a differential probe, and a near-field measurement probe. The PC controls the overall measurement process. It is connected to the DSO and the RFID reader. An 8-bit oscilloscope is used that offers an acquisition bandwidth of up to 1 GHz. As a reference measurement, an active differential probe has been connected in parallel to a 1 Ω resistor that is placed in series to the *VDD* core power supply. For electromagnetic measurements, we used a tiny magnetic near-field probe that allows the sensing of signals only up to a few millimeters. This already reduces the noisy reader signal in an early stage of the acquisition process. The sensed signals are then amplified by a 30 dB pre-amplifier before they are sampled by the oscilloscope. The sampling rate has been set to 1 GS/s for all measurements. Figure 4 shows the RFID measurement setup involving our tag prototype that lies on the antenna of a reader.

We have used a standard RFID reader that supports mandatory ISO 15693 commands such as *Inventory* or *Select*. It is also able to send custom commands that are needed to start the ECDSA signature generation. We defined three custom commands. The first command (0xE0) performs a hardware reset and loads initial data (like the base point) from Read Only Memory (ROM) into the internal Static Random Access Memory (SRAM) of the tag controller. The second command (0xE1) starts the scalar multiplication and the third command (0xE2) evaluates the signing equation given in Algorithm 1.

The communication flow between the reader and our tag prototype is shown in Figure 6. First, a reset command (0xE0) is sent to the tag. The tag responds with its unique ID (UID) number. Instead of calculating the scalar multiplication in each power trace acquisition, we pre-calculated the value r and loaded it into

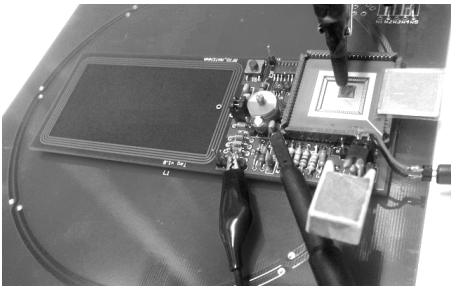

Fig. 4. RFID measurement setup involving our tag prototype lying on the reader antenna

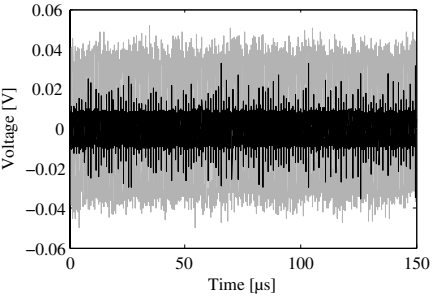

Fig. 5. Power trace (black) and (30-times magnified) EM trace (gray) during the calculation of the private-key multiplication

the SRAM before starting the power acquisition of the integer multiplication. This is done by sending the mandatory Write-Single-Block (WSB) command (0x21) of ISO 15693. After that, the reader sends the ECDSASign command (0xE2) to start the calculation of the digital signature (r, s). As a trigger signal, the oscilloscope was set to listen on the End-of-Frame (EOF) sequence of the Write-Single-Block command.

The RFID controller inverts the ephemeral key k in about 11.8 ms. The private-key multiplication needs about 150 µs, the hash-value addition and the final multiplication need around 600 µs. In our setup, the power consumption as well as the electromagnetic emanation of our device were acquired simultaneously throughout the private-key multiplication. Figure 5 shows one measured power trace (drawn in black) and a 30-times magnified electromagnetic trace (drawn in gray).

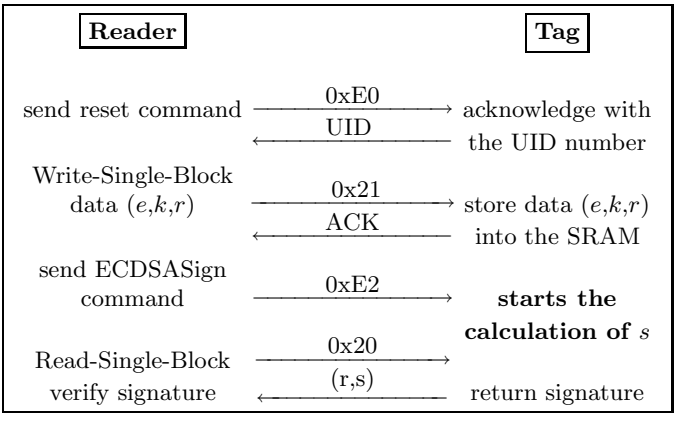

Fig. 6. RF communication between the reader and the tag

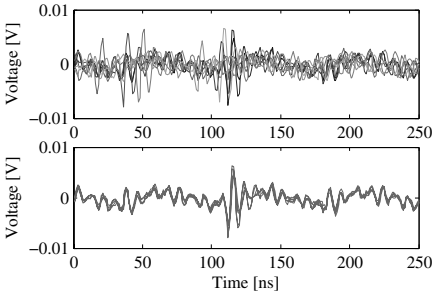

Fig. 7. Misaligned traces (upper plot) and aligned traces (lower plot) of electromagnetic measurements

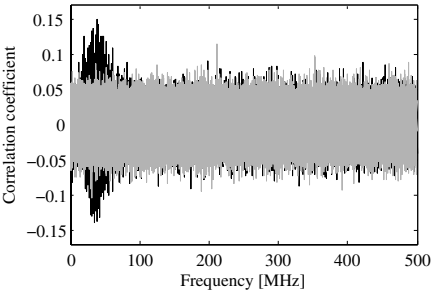

Fig. 8. Correct (black) and incorrect (gray) correlation traces of the frequency-based DPA attack using 2 000 power traces

5.1 Pre-processing RFID Power Traces

As we already stated in Section 2, measurements in RFID environments are very noisy due to the high energy signal of the reader device. We therefore applied two pre-processing techniques: trace alignment and trace decimation.

First, we aligned all measured traces in both horizontal and vertical orientation. We determined a specific trace pattern which was used to align the remaining traces using the least-mean-square (LMS) algorithm. The misaligned traces are shown in the upper plot of Figure 7. The lower plot demonstrates the traces after alignment. Our experiments have shown that without alignment or even poor alignment, successful attacks become largely infeasible due to the high noise of the measurement setup.

Second, we applied a trace-decimation technique that has been proven to be very useful throughout our experiments. Decimation is a technique typically used in signal processing. It performs two actions: filtering and re-sampling. First, the measured power traces are applied to an appropriate low-pass filter. This filter attenuates all frequency signals above a certain cut-off frequency. Second, it re-samples the smoothed traces at a lower rate. Decimation has therefore two major advantages. On the one hand, misalignment are compensated due to the averaging of filtering. On the other hand, all measured traces become shorted in their length. Both properties are a major concern for successful attacks in RFID environments as stated in Section 2.

In order to apply the decimation technique to our power traces, we determined a proper cut-off frequency. This frequency has to be chosen in a way so that signals are eliminated that do not carry data-dependent information. Agrawal et al. [1] have shown that there exist data-dependent information in the lower frequency spectrum. The higher the frequency, the weaker will be the signals that carry interesting information. Due to this fact, we have performed a frequency-based DPA attack that was first introduced by Gebotys [7]. All measured power traces are transformed into the frequency domain using the Fast Fourier Transformation (FFT). Instead of correlating the sample points in the time domain, the sample points are correlated in the frequency domain. As a target of the

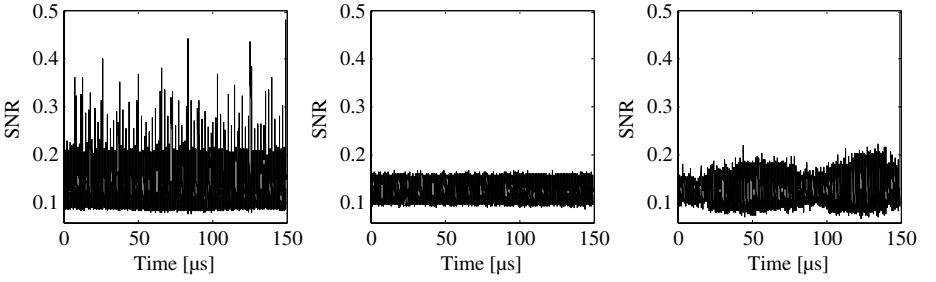

Fig. 9. SNR of the power traces (left), SNR of the EM traces without pre-processing (middle), and SNR of the pre-processed EM traces (right)

attack, we have chosen the same intermediate value used in the attack described in Section 3. Figure 8 shows the result of the attack using 2 000 power traces. The correct key hypothesis is drawn in black and the incorrect key hypotheses are drawn in gray. It can be clearly seen that there is a high correlation below 50 MHz. Above this frequency, no significant correlation can be discerned. On this account, we applied an 8th-order Chebyshev (Type 1) low-pass filter with a cutoff frequency at 50 MHz and down-sampled the traces accordingly. All traces have been decimated from 300 000 sampling points to only 32 500 samples.

5.2 Device Characterization and Pre-processing Evaluation

Next, we characterize our tag prototype concerning side-channel information leakage. First, the noise of the measurement setup is characterized. Second, the data-dependent signal that is leaked by the device is determined. After that, we calculate the signal-to-noise (SNR) ratio of the power and the electromagnetic measurements and compare them. Furthermore, we evaluate the pre-processing techniques by comparing measurements with and without trace alignment and trace decimation.

The noise of the measurement setup has been characterized by calculating the mean of all traces that were captured by processing constant data. This avoids data-dependent power variations and allows the determination of the measurement noise. Data-dependent signals, in contrast, have been characterized within two steps: First, the mean of those traces that process the same input data is calculated. Second, the variance of these mean traces is calculated. The SNR can now be calculated by dividing the variance of the obtained mean-signal trace from the variance of the calculated noise trace [20]. For the SNR calculation, 2 000 traces have been used.

Figure 9 shows the result of the characterization and performance evaluation. The left plot in the figure shows the SNR of the power traces. A maximum SNR of 0.45 has been obtained. In the middle plot of the figure, the result of the EM traces is given which have not been pre-processed. It can be seen that the signal components are below the noise floor. With this number of traces, an attack would fail due to the low SNR. The right plot of the figure shows the SNR

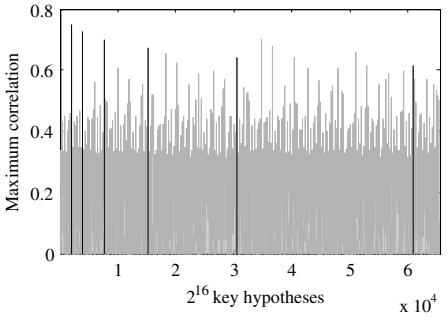

Fig. 10. Maximum correlation coefficient of all 2^{16} key hypotheses for the first private-key word d_0 using 2 000 power traces

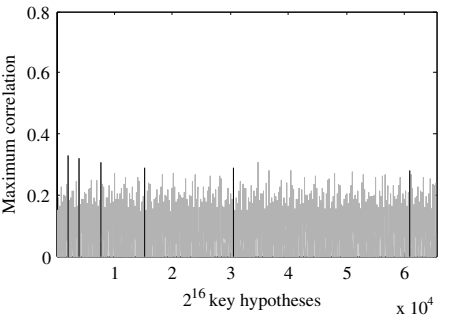

Fig. 11. Maximum correlation coefficient of all 2^{16} key hypotheses for the first private-key word d_0 using 2 000 EM traces

of the pre-processed EM traces. Due to the pre-processing, the SNR could be significantly increased to a maximum of 0.22. The signal components are much weaker as compared to the power traces but an attack will still succeed as shown in the next section.

6 Results

This section presents results of power and electromagnetic (EM) analysis attacks on our ECDSA-enabled RFID-tag prototype. First, we perform a reference attack using a contact-based power analysis. The power consumption of the RFID-tag prototype is measured over a resistor that has been placed in series to the integrated RFID controller and the analog front-end. Second, we perform a contact-less attack using EM analysis by using a magnetic near-field probe. In both scenarios, the tag was powered passively by the field.

The first attack targets the first partial product of the multi-precision multiplication unit of our RFID controller. The controller implements a 16-bit Comba-multiplication unit so that we have to test 2^{16} key hypotheses that are multiplied with the known intermediate value r. The target has been the 32-bit output of the multiplication. However, our experiments have shown that our device does not leak all bits of this 32-bit output with same amount. Hence, we have modeled the power consumption by weighting the Hamming weight of the higher 16 bits and the lower 16 bits differently to obtain the highest correlation.

Figure 10 and Figure 11 show the result of the power and EM attack. For both attacks, 2 000 traces have been used. The x-axis represents all possible key hypotheses and the y-axis represents the maximum absolute correlation of each resulting correlation trace. It is clearly discernable that the results obtained from the EM traces reach only half the correlation value as they have been obtained from the power traces. The reason for this is the lower SNR of the EM measurement calculated in the previous section. Furthermore, it can be observed that the highest peak has been obtained for the key word 1901 and reached a correlation coefficient of 0.75 for the power traces and 0.33 for the EM

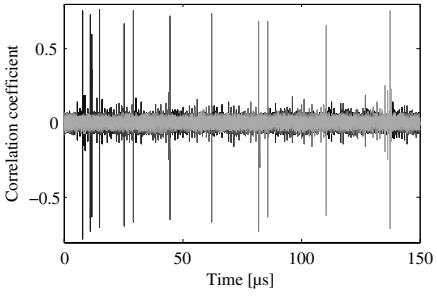

Fig. 12. Correlation traces of all partial products $r_i * d_0$ using 2 000 power traces

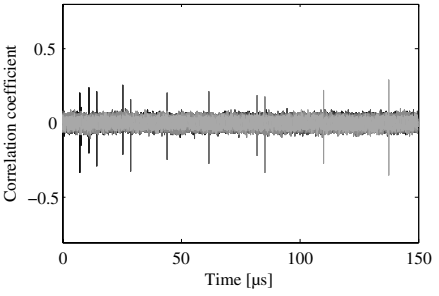

Fig. 13. Correlation traces of all partial products $r_i * d_0$ using 2 000 EM traces

traces. However, there exist also five other key hypotheses which result in a high correlation[2]. These are 3802, 7604, 15208, 30416, and 60832 (marked as black lines in the figures). Obviously, these values have the same bit representation as 1901 but are gradually shifted to the left. This is due to the fact that integer multiplication is a linear function where shifted bit combinations of the correct key have a linear impact to the multiplication result.

Next, we perform the same attacks on all other partial products that involve the first private-key word d_0. Figure 12 and Figure 13 show the result of the attacks. The correlation results of the correct key-hypothesis d_0 of all partial products are plotted on top of each other. Eleven peaks are observable that occur at locations in time when the output of the partial products is stored into the internal registers of the controller. Due to the structure of the Comba multiplication-unit, the distance between these results becomes larger the more partial products are calculated. The first partial product is calculated after about 10 μs and the last one after about 140 μs. The power-analysis attacks lead to a mean correlation of 0.72. The EM attacks yielded a mean correlation of 0.22.

After revealing the promising key candidates of the first private-key word d_0, we performed attacks on all partial products that involve the second private-key word d_1. The attacks led us to two promising key candidates: 24027 and 48054. Now we perform an attack on the second result of the final multiplication product p_1. This product word involves the calculation of the first and the second private-key word. Thus, we have to test 12 promising key hypotheses. A high correlation will occur when both hypotheses are correct. Incorrect hypotheses will show no peak. In Figure 14, the result of the power-analysis attack is given using 2 000 power traces. The correct key hypotheses (drawn in black) 1901 for d_0 and 48054 for d_1 yield a high correlation while all other key hypotheses (drawn in gray) show no peak in time when the final product is stored into the internal register of the controller. Figure 15 shows the result of the EM attack using 10 000 traces. It provides a much smaller correlation as compared to the result of the power-analysis attack. Nevertheless, the correct key can be easily discovered from the incorrect ones.

[2] The peaks do not have the same correlation value since our power model weighted the lower and higher bits of the 32-bit multiplication output differently.

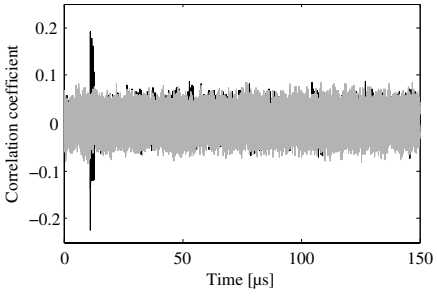

Fig. 14. Result of the power-analysis attack on the final multiplication product p_1 using 2 000 traces

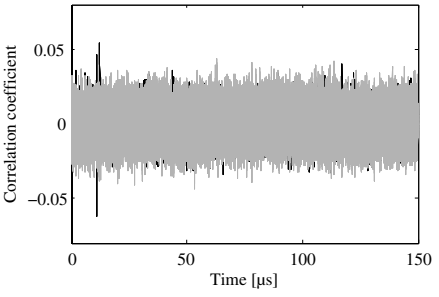

Fig. 15. Result of the EM attack on the final multiplication product p_1 using 10 000 traces

All other private-key words have been extracted by following the same strategy. Both power and electromagnetic attacks have been successful. The attacks revealed the entire private key of the ECDSA implementation which enables us to forge digital signatures and therefore to impersonate any entity and person by cloning the extracted key.

7 Conclusions

In this article, we presented the first results of DPA attacks on a hardware ECDSA implementation in a passively powered RFID device. We have designed and implemented a low-power RFID-tag prototype which consists of a 180 nm CMOS implementation of ECDSA which allows authentication by generating digital signatures. In order to evaluate the effectiveness of side-channel attacks on such devices, we performed power analysis and electromagnetic analysis. Furthermore, we propose the application of a decimation filter to reduce the complexity of the analysis on RFID devices. For both power analysis and electromagnetic analysis, the private-key could be revealed successfully. Opposed to other proposed attacks that try to reveal the ephemeral key of ECDSA, we extract the private key during signature generation. Hence, our attack is unaffected by common countermeasures that avoid the extraction of the ephemeral key. In addition, it is independent of the underlying elliptic curve representation. The significant points of our findings are as follows: First, public-key enabled RFID devices are as vulnerable to side-channel attacks as conventional contact-based devices. Second, it is not sufficient to protect the ephemeral key during scalar multiplication. It is also imperative to secure the private-key multiplication during the signature generation. This article is the first to provide results of power-analysis attacks on passive RFID devices that generate digital signatures using ECDSA. It further presents the first results of attacks on a hardware ECDSA implementation revealing the private-key during signature generation.

Future work will be to evaluate the effectiveness of this attack on existing RFID devices such as the electronic passport. The International Civil Aviation

Organization (ICAO) has published the technical specifications of e-passports in Europe and defined ECDSA as a standardized algorithm for *active authentication*. This feature allows the verification of whether the passport is authentic or not. We will evaluate the side-channel leakage of such a device to answer the question of how e-passports are effected by these attacks.

Acknowledgements

The authors would like to thank Thomas Popp and Stefan Tillich for their valuable inputs and helpful discussions. The research described in this paper has been supported by the European Commission funded project *Collaboration at Rural* under grant number 034921 (Project *C@R*) and the Austrian government funded project *CRYPTA* established under the *Trust in IT-Systems* program FIT-IT.

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.) CHES 2002. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003)
2. American National Standards Institute (ANSI). American National Standard X9.62-2005. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm, ECDSA (2005)
3. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
4. Coron, J.-S.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302. Springer, Heidelberg (1999)
5. Feldhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems using the AES Algorithm. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 357–370. Springer, Heidelberg (2004)
6. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 251–261. Springer, Heidelberg (2001)
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.) CHES 2005. LNCS, vol. 3659, pp. 250–264. Springer, Heidelberg (2005)
8. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A Ring-Based Public Key Cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998)
9. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer, Heidelberg (2006)
10. Hutter, M., Mangard, S., Feldhofer, M.: Power and EM Attacks on Passive 13.56 MHz RFID Devices. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 320–333. Springer, Heidelberg (2007)

11. IEEE. IEEE Standard 1363a-2004: IEEE Standard Specifications for Public-Key Cryptography, Amendment 1: Additional Techniques (September 2004), http://ieeexplore.ieee.org/servlet/opac?punumber=9276
12. International Organisation for Standardization (ISO). ISO/IEC 7816: Identification cards - Integrated circuit(s) cards with contacts (1989)
13. 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)
14. International Organisation for Standardization (ISO). ISO/IEC 14888-3: Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms (2006)
15. Joye, M.: Defences Against Side-Channel Analysis. In: Advances In Elliptic Curve Cryptography. London Mathematical Society Lecture Note Series, vol. 317, pp. 87–100. Cambridge University Press, Cambridge (2005)
16. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)
17. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
18. Leander, G., Paar, C., Poschmann, A., Schramm, K.: New Lightweight DES Variants. In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 196–210. Springer, Heidelberg (2007)
19. Lenstra, A.K., Verheul, E.R.: The XTR Public Key System. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 1–19. Springer, Heidelberg (2000)
20. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks – Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
21. Medwed, M., Oswald, E.: Template Attacks on ECDSA. In: Chung, K.-I., Yung, M., Sohn, K. (eds.) 9th International Workshop on Information Security Applications (WISA 2008), Korea, Jeju Island, September 23-25, 2008, Pre-Proceedings (2008)
22. Montgomery, P.L.: Speeding the Pollard and Elliptic Curve Methods of Factorization. Mathematics of Computation 48(177), 243–264 (1987)
23. National Institute of Standards and Technology (NIST). FIPS-46-3: Data Encryption Standard (October 1999), http://www.itl.nist.gov/fipspubs/
24. National Institute of Standards and Technology (NIST). FIPS-186-2: Digital Signature Standard (DSS) (January 2000), http://www.itl.nist.gov/fipspubs/
25. National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard (November 2001), http://www.itl.nist.gov/fipspubs/
26. National Institute of Standards and Technology (NIST). FIPS-180-2: Secure Hash Standard (August. 2002), http://www.itl.nist.gov/fipspubs/
27. Oren, Y., Shamir, A.: Remote Power Analysis of RFID Tags. Master's thesis, Weizmann Institute of Science, Rehovot, Israel (August 2006), http://www.wisdom.weizmann.ac.il/~yossio/rfid/
28. Plos, T.: Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 288–300. Springer, Heidelberg (2008)
29. Quisquater, J.-J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In: Attali, S., Jensen, T. (eds.) E-smart 2001. LNCS, vol. 2140, pp. 200–210. Springer, Heidelberg (2001)
30. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21(2), 120–126 (1978)