On the security of RFID devices against implementation attacks

Michael Hutter*, Thomas Plos and Martin Feldhofer

Institute for Applied Information Processing and Communications,
Graz University of Technology,
Inffeldgasse 16a, 8010 Graz, Austria
Fax: 0043-316-873-5596
E-mail: michael.hutter@iaik.tugraz.at
E-mail: thomas.plos@iaik.tugraz.at
E-mail: martin.feldhofer@iaik.tugraz.at
*Corresponding author

Abstract: Radio-Frequency Identification (RFID) is a wireless technology that already plays an important role in security-related applications. As soon as cryptographic features are integrated into RFID-enabled devices, the issue of implementation security becomes highly important. Implementation attacks exploit potential weaknesses of such devices and allow the extraction of sensitive information like secret keys. In this paper, we evaluate the efficiency of implementation attacks by conducting side-channel attacks and fault analysis on both High Frequency (HF) and Ultra-High Frequency (UHF) RFID tags. The results of our investigations disclose the potential vulnerability of RFID-tag implementations against practical attacks. Furthermore, this paper shows possible countermeasures that are optimised for resource-restricted devices like passive RFID tags.

Keywords: RFID; radio-frequency identification; implementation attacks; power and electromagnetic analysis; side-channel analysis; fault analysis; RFID security.

Reference to this paper should be made as follows: Hutter, M., Plos, T. and Feldhofer, M. (2010) 'On the security of RFID devices against implementation attacks', *Int. J. Security and Networks*, Vol. 5, Nos. 2/3, pp.106–118.

Biographical notes: Michael Hutter received his MSc Degree in Computer Science at Graz University of Technology Austria in 2006. He is currently a Research Assistant and works on his PhD Degree at the Institute for Applied Information Processing and Communications (IAIK). His research interests include applied cryptography, RFID security and privacy, side-channel and fault analyses. Currently, he is working on cryptographic hardware implementations for constrained devices using Elliptic Curve Cryptography.

Thomas Plos received a Master's Degree in Computer Science at Graz University of Technology (TUG), Austria. Since 2007, he is a member of the VLSI and security group at the Institute for Applied Information Processing and Communications (IAIK) at TUG. Currently, he is pursuing his PhD study, which deals with RFID security and implementation attacks. Especially, he is focusing his work there on RFID systems in the Ultra-High Frequency (UHF) range.

Martin Feldhofer is Scientific Member of the research group VLSI and security at the Institute for Applied Information Processing and Communications (IAIK) which is part of the Graz University of Technology in Austria. He has received his Master's Degree in 2003 and his PhD Degree in Information and Communications Technology (ICT) in 2009. His main research topic is the low-power hardware implementation of cryptographic modules. Currently, he is working on the implementation of DPA-secure symmetric and asymmetric crypto algorithms.

1 Introduction

In the last century, digital communication has become a major part of our lives. Information technology is on its move from using autonomous applications like mobile communication and networked computers towards the 'internet of things'. The vision is that every object in the world has the ability to communicate with its environment using a digital identity. RFID is an enabler technology that allows realising this vision.

With the possibility to fabricate low-cost RFID tags in high volume, RFID technology has become very popular. An RFID system mainly consists of a reader device that communicates with a so-called RFID tag. This tag is a small microchip that is attached to an antenna. In a passive RFID system, the tag does not need an internal power source like a battery because it draws the required energy from the RF field of the reader. A bidirectional communication link allows identification and sending of data by applying different interaction techniques depending on the used frequency range. Many applications like supply-chain management, inventory management, and access control already benefit from the use of RFID technology.

The importance of the topic security has been shown by publications of attacks against existing RFID applications. The main threats against RFID systems are cloning of tags, violation of privacy by tracking people that are wearing and carrying tags, and the unauthorised access to the tag's memory. In order to prevent these attacks, we suggest the use of strong cryptographic algorithms and protocols that have been standardised. Proprietary solutions that rely on the secrecy of their methods have often been shown to be insecure.

The research activities that deal with RFID security can be divided into four main categories. The first category are proposals for new security protocols and the invention of cryptographic algorithms. Many different cryptographic primitives are used as underlying building blocks for the protocols. The second category is the development of new applications for RFID systems. In these applications, the main focus lies on the added value that can be achieved when integrating security measures. The third category of research activities are the hardware implementations of cryptographic algorithms. These implementations are optimised for the requirements of passive RFID tags. The last category consists of attacks against RFID systems. The target of the attacks are either currently employed RFID applications, previously proposed protocols, or the implementations on the tags. This last mentioned point is also the main focus of this paper.

Within this paper, we are evaluating different implementation attacks against RFID devices. The two main categories are side-channel attacks and fault analysis. In the former category, unintended leakage of physical properties like power consumption, electromagnetic emanation, or timing behaviour is exploited. Fault analysis targets on exploiting faulty outputs of the device that are caused due to a forced misbehaviour of the circuit. The targets of attack vary depending on the conducted analysis. Because there are nearly no RFID tags available that implement real cryptographic operations, we often have to base our attacks on prototypes or on different operations like the writing of data to the EEPROM of a tag. Even if attacks against real cryptographic hardware would look slightly different, the main principles and the characteristics of the attacks stay the same. The main outcome of all our analyses is that as far as cryptography is implemented on RFID tags the circuits have to be protected against implementation attacks.

There are two main contributions of this paper. First, this is the first paper that gives an overview of different implementation attacks on RFID devices. Practical results are shown and discussed for each attack. Second, we survey countermeasures for these attacks that can be integrated into implementations with low costs. The paper is therefore interesting for both academic research and industrial applications.

The paper is structured as follows. Section 2 describes implementation attacks in general. In Section 3, results of performed side-channel attacks are presented. We analysed the power consumption, electromagnetic emanation, and timing variations of RFID tags. Countermeasures are discussed afterwards. Section 4 presents results of performed fault attacks. We injected faults by inducing over-voltage spikes, electromagnetic interferences, optical light, and by performing tearing attacks. The countermeasures are discussed consecutively. Conclusions are drawn in Section 5.

2 Implementation attacks

Standardised cryptographic algorithms are secure in a mathematical and cryptoanalytical sense. However, when integrating the algorithms into real physical devices like RFID tags, they can become vulnerable to implementation attacks. Principally, implementation attacks can be divided into side-channel analysis attacks and fault analysis attacks.[1] Both techniques aim to reveal secrets stored on the devices. This is achieved by either observing physical properties of the devices or by evaluating their erroneous behaviour. In the following, side-channel analysis and fault analysis are described in a more detail. Afterwards, requirements for integrating countermeasures against implementation attacks on RFID devices are discussed.

2.1 Description of side-channel analysis

Side-channel analyses are related to implementation attacks that work passively by measuring physical properties of a cryptographic device. The attacks exploit the fact that the physical properties are dependent on the data and the operations that are processed and executed by the device. The most promising physical side-channels are timing information, power consumption, and Electromagnetic (EM) emissions of a device. First side-channel analysis results have been published by Kocher (1996). He exploited the execution time of cryptographic algorithms that were running on a standard PC to extract secret information. Three years later, Kocher et al. (1999) have introduced power analysis. Power analysis techniques make use of the fact that the power consumption of a cryptographic device depends on the information it processes. The same relation holds for EM emissions of a device which has been observed by Gandolfi et al. (2001) and by Agrawal et al. (2003).

Experience has shown that the power consumption and the EM emissions of a cryptographic device are the two most powerful side channels. The principle of power and EM attacks is the same. They only differ in the observed physical property. Determining the power consumption of a device is typically achieved by measuring the voltage drop across a resistor that is switched in series to the power-supply line. Gathering the EM emissions of a device is obtained by using special measurement antennas (probes). Antennas of various shapes and sizes are deployed depending on the EM emissions that need to be sensed.

Power analysis in its simplest form requires only a single power trace that is acquired during the execution of the cryptographic algorithm for deducing the secret of the device. This technique is called Simple Power Analysis (SPA) and can be conducted, for example, by visually inspecting the power trace. A more sophisticated approach is Differential Power Analysis (DPA). There, the information of multiple power traces is combined to reveal the device's secret. In the first step of a DPA attack, several input data are fed into the examined device while measuring its power consumption. Next to the physical measurement of the side channel, a model is constructed in software that predicts the consumed power of the cryptographic device. The model predicts intermediate values of the cryptographic algorithm by deploying the known input data and hypothetical values for the unknown secret of the device. After that, these predicted intermediate values are fed into a simplified power-consumption model which results in predicted power-consumption traces. For this power model, the Hamming weight or the Hamming distance of the intermediate values is often calculated. In the last step of the attack, the predicted power-consumption traces are compared to the physically measured power-consumption traces by means of statistical methods. Typically used methods are the Pearson correlation-coefficient or the difference of means. The statistical methods indicate the degree of linear dependency between the predicted power consumption and the measured power consumption. A DPA attack is successful if only the predicted power consumption, which is related to the correctly guessed secret key, shows a significant linear dependency. A more detailed description of power-analysis attacks can be found in Mangard et al. (2007).

When exploiting the EM emissions of a cryptographic device instead of the power consumption, DPA attacks are named Differential Electromagnetic Analysis (DEMA) attacks. Especially DPA and DEMA are typically applied in side-channel analyses and constitute an important and powerful instrument. No detailed knowledge of the device is necessary and the attacks are successful even if the data-dependent leakage is weak or overwhelmed by noise. Moreover, DEMA attacks can be conducted contactlessly and at a distance which makes them potentially difficult to detect.

2.2 *Description of fault analysis*

In contrast to side-channel analysis attacks, which exploit physical properties by means of passive measurements, fault analysis attacks extract secret information through active interferences. By maliciously manipulating the working conditions of a cryptographic device during its operation, erroneous behaviour can be provoked. This erroneous behaviour is then exploited in an attack to reconstruct the secret key consecutively. In general, fault attacks can be divided into non-invasive attacks, semi-invasive attacks, and invasive attacks.

Non-invasive attacks leave no damage of the examined device. Such attacks physically stress the device by applying various methods. Anderson and Kuhn (1996, 1997) injected glitches in the clock signal and induced spikes in the power-supply line of the circuit. Quisquater and Samyde (2002) have applied EM fault attacks that use eddy currents to influence the behaviour of a cryptographic device. Semi-invasive attacks go a step further. They require the decapsulation of the chip from its package. This modification allows to induce faults by exposing the chip to light (optical beams). Skorobogatov and Anderson (2003) have demonstrated that the light of a laser pointer can be utilised to perform successful fault attacks on a cryptographic device after decapsulating the chip. Invasive attacks are by far the most powerful fault attacks. For these attacks, the chip is decapsulated and its surface is electrically contacted with special probes. In that way, secrets stored on the device can be directly modified. In particular, the use of a Focused Ion Beam (FIB) allows to modify the chip layout by cutting and reconnecting specific wires of the circuit. Unlike non-invasive and semi-invasive attacks that can be conducted at moderate costs, invasive attacks require expensive equipment that is only available at special laboratories.

2.3 *Requirements of countermeasure implementations*

The hardware design for passively powered RFID tags faces the difficulty of very fierce constraints. The available silicon area for tags is very small and the power budget is limited. The reasons for these limitations are mainly based on economical and technical issues. In order to allow tagging billions of products with an RFID tag, the production costs have to be low. Due to the linear relationship between silicon area and chip manufacturing costs, limiting the required die size achieves this goal. The hard constraint for the available power consumption has a more technical reason. A passive RFID tag has to be supplied via the RF field of a reader, which strength decreases with the operating distance. Hence, the less power a passive RFID tag consumes the longer is its operation range.

Especially the implementation of cryptographic algorithms in hardware is very costly in terms of chip area and power consumption. This is due to the complex operations and the high amount of memory that is necessary. Hence, the implementations have to be highly optimised to achieve the requirements. The same accounts for the implementation of countermeasures. Many countermeasures that are possible in high-performance devices cannot be realised on passive RFID tags. The most efficient countermeasures are those that work in the time domain because the low data rates of RFID systems allow additional operations and the required hardware resources are minimised. After a description of the specific attacks, we will describe the implementation of several possible countermeasures in the following.

3 Side-channel analysis

Mainly there exist two different types of side channels that can be exploited in practical attacks: side channels that are gained from a contact-based channel, and side channels that are gained contactlessly. Contact-based side channels are typically exploited by measuring the power consumption or by using timing variations in the execution time of the device. Contactless side channels, in contrast, offer information through an emitting electromagnetic field, for example. However, extracting side-channel information out of RFID-based systems is a challenging task due to several reasons. First, passive RFID tags only provide two contact-based antenna connections. These connections are basically used to draw energy from the reader field and furthermore to establish a communication. Hence, power-consumption measurements are only possible in the antenna line of the device. By measuring the power consumption in the antenna line, information of the entire chip is acquired. This information not only holds interesting signals from a cryptographic co-processor, for example, but also contains high noise that is produced by the remaining parts of the chip such as number generators or the analogue front-end. Second, passive RFID tags draw their energy from an electromagnetic field that is generated by the reader. Unfortunately, contactless side channels get interfered by that field which substantially adds a significant amount of noise to the overall side-channel measurement.

In the light of these facts, several pre-processing techniques have to be applied in order to succeed side-channel attacks on RFID devices. For all performed attacks, we therefore applied different filtering techniques to remove the carrier of the reader signal. We calculated the envelope signal of the measured traces by taking the absolute values and by applying a low-pass filter afterwards. Furthermore, we aligned all traces in vertical and horizontal orientation.

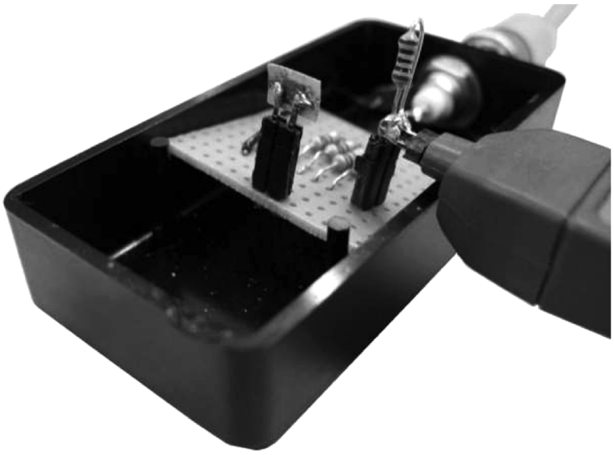
In the following, we describe power-analysis attacks, electromagnetic-analysis attacks, and attacks that exploit the timing behaviour of RFID devices. Countermeasures against these attacks are discussed afterwards.

3.1 Analysis of the power consumption

In order to perform power analysis on RFID devices, corresponding measurement setups are necessary. These setups are typically more complex than power-measurement setups for contact-based devices. The reason for this is that RFID devices are powered via the electromagnetic field of an RFID reader and not directly via a power-supply unit. The classical method to measure the power consumption of a device is to insert a resistor into one of its power supply lines. The voltage drop over this resistor, which is proportional to the consumed power of the device, can then be measured by a digital storage oscilloscope.

In practice, the insertion of a resistor into the power-supply line of an RFID device is often not possible. RFID devices are usually integrated on a single die providing only two connections for the antenna. It is obvious that the power consumption of such a device can only be measured via these two antenna connections. An example of a power-consumption measurement setup is given in Figure 1. The setup is composed of an RFID chip, a reader, a matching resistor, and a measurement resistor. The RFID chip is first separated from its antenna and soldered on a two-pin strip. This strip is then directly connected to the interface of an RFID reader which is terminated by a 50 Ohm matching resistor. A measurement resistor is placed between the chip and the reader interface. The power consumption of the tag is then measured over that resistor.

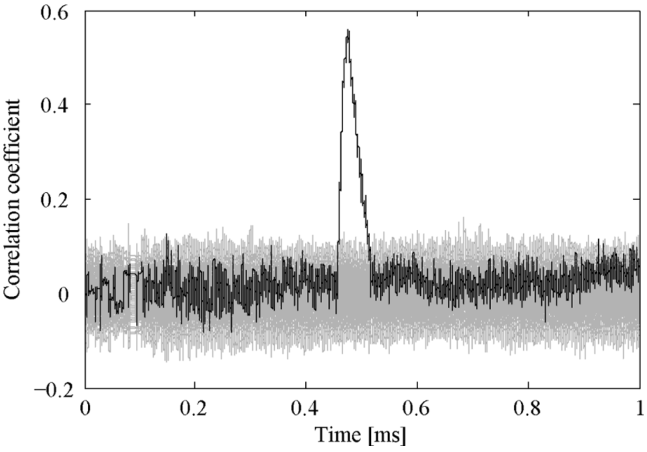
Figure 1 Setup for power-consumption measurements on a passive RFID tag



Another possibility to measure the power consumption of RFID tags is the insertion of a measurement resistor into the internal power-supply lines of an RFID chip. One way to achieve this measurement is to use a probing station. The probing station allows the monitoring of the power consumption of the tag by penetrating a tiny needle through the top-level substrate of the chip. The power consumption can then be easily acquired by an oscilloscope.

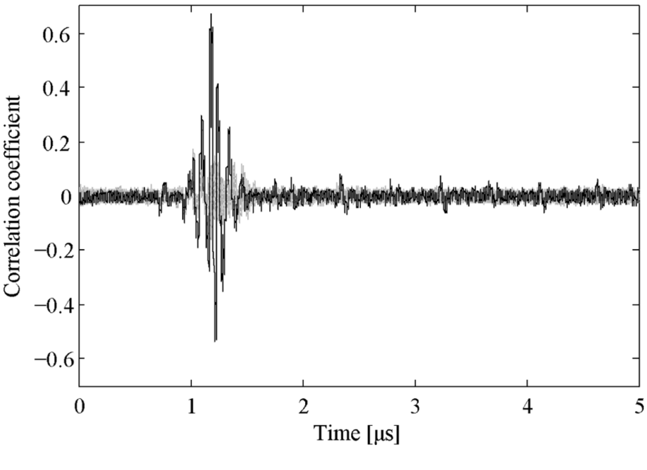
In Hutter et al. (2007), a measurement resistor was placed between the analogue front-end and the microcontroller of an RFID-tag prototype. The prototype was used to demonstrate the susceptibility of RFID tags against power analysis. Figure 2 shows a picture of the prototype. It mainly consists of an antenna, an analogue front-end, and a microcontroller. All components are designed for low-power consumption to make sure that the device can be powered passively by the field of an RFID reader. The target of the attacks has been an AES software implementation that runs on the microcontroller.

Figure 2 Result of a power-analysis attack on a commercially available RFID tag



In Figure 3, the result of a power-analysis attack on a commercially-available RFID tag is shown. The x-axis represents the acquisition time. The time interval between a reader request and the tag response has been measured. The y-axis shows the result of the attack as an output of the Pearson correlation coefficient. The target of the attack has been the writing of data into the internal tag memory. For the attack, 1 000 power traces have been used and a dedicated power model has been applied.

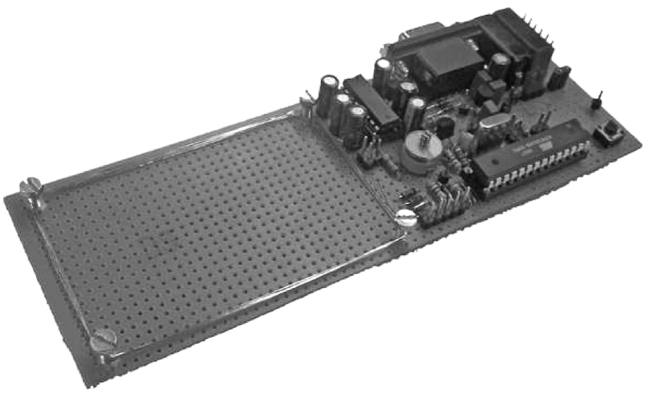
Figure 3 Result of a power-analysis attack on a passively-powered RFID-tag prototype



The correct hypothesis (drawn in black) led to a high correlation coefficient of about 0.56. Incorrect hypotheses are drawn in grey and led to no significant correlation.

Figure 4 shows the result of a power-analysis attack on the RFID-tag prototype. The target of the attack has been the first S-box output of the first round of AES. 10,000 power traces have been measured and the Hamming-weight power model has been used. The correct hypothesis for the first AES key-byte led to a correlation coefficient of 0.67. All other hypotheses led to no significant correlation.

Figure 4 A passively powered RFID-tag prototype operating at a frequency of 13.56 MHz



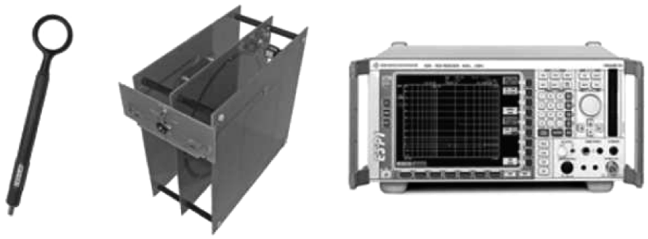
The performed power-analysis attacks on the commercially-available RFID tag and the tag prototype have been successful. The attacks demonstrate the susceptibility of RFID tags against these kind of attack. Nearly the same correlation coefficient has been obtained for both scenarios.

3.2 Analysis of the electromagnetic emanation

Another approach to measure the power consumption of RFID devices is to measure it indirectly via the electromagnetic field. This can, for example, be done by a magnetic near-field probe (see left picture in Figure 5). For this, the probe is placed on top of the chip surface. The current flow within the chip produces an electromagnetic field that is sensed by the probe. This field contains different signals such as the square-wave clock or signals that are caused by data-dependent processing. There exist several publications that discuss how this method can be used to attack contact-based devices (see for example Agrawal et al. (2003), Gandolfi et al. (2001), and Quisquater and Samyde (2001)).

However, in view of electromagnetic attacks on RFID devices, the measured signals become very weak in their amplitude. Passive RFID devices have been designed for low-power operation and consume only a few microwatts of power as opposed to contact-based devices that consume some milliwatts of power. In addition to this fact, there also exists the problem of the interfering reader field. This field is typically between 40 dB to 80 dB higher than the signals emitted by the tag. As a result, interesting signals are 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. Next to the lower acquisition resolution, this reader field is not synchronised with the measurement equipment which causes power-trace misalignments in both the time and the amplitude dimension. The reader is a strong noise source and makes the acquisition of side-channel information difficult. The main challenge of electromagnetic measurements in this context is therefore to minimise the impact of the reader signal and to overcome the resulting misalignment of measured power traces.

Figure 5 Different EM measurement setups: a magnetic near-field probe (left), a Helmholtz assembly (middle), and a receiver (right)



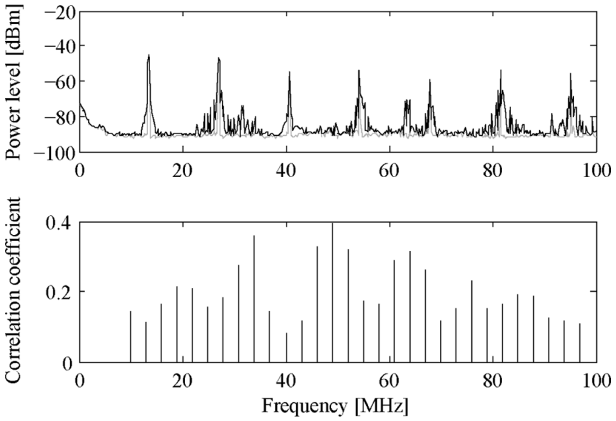
One way to overcome the problem of the interfering reader signal is the use of the test setup described in ISO/IEC 10373-6 (International Organization for Standardization (ISO), 2001). In this standard, a so-called Helmholtz assembly (see middle picture of Figure 5) is specified for compliance testing. This assembly essentially consists of two sense coils that are arranged in parallel to a reader antenna. The two sense coils are connected with in-phase opposition. Consequently, the induced voltage becomes zero at the point where the two coils are connected to each other (differential point). When a passively powered device draws energy out of the field, this measuring bridge becomes unbalanced and an offset voltage can be observed at the differential point. This voltage offset can be measured using a digital oscilloscope and it contains information about the power consumption of the RFID device. The carrier signal of the RFID reader is typically attenuated by 40 dB by a Helmholtz assembly.

Another way to avoid the interfering reader field is to separate the chip of the RFID device from its antenna. The basic idea of this method is to place an antenna in the field of the reader and to use wires to supply an RFID device that is placed outside the field. This approach has first been presented in Carluccio et al. (2005). The alternative to this approach is to filter the signal that is measured by the EM probe. This can for example be done by a receiver.

The first publication that discusses the use of a receiver to perform EM attacks on cryptographic devices is Agrawal et al. (2003). In this publication, a receiver is used to find the side-channel leakage of devices in different parts of the EM spectrum. A very similar approach can of course also be used for RFID devices. In this case, the basic idea is to scan the EM spectrum of the device between the harmonics of the 13.56 MHz carrier. The leakage in between the harmonics can easily be exploited as there is no interference of the harmonics of the carrier.

In Figure 6, the result of an electromagnetic-analysis attack on an RFID device is shown. As an attacking platform, the RFID-tag prototype has been used that is described in the power-analysis measurement scenario. The attack is split into two phases: a profiling phase and an attacking phase. In the profiling phase, the device was first separated from the reader field and characterised afterwards in terms of its side-channel leakage. Therefore, we connected a 3 GHz wideband receiver to the magnetic near-field probe. The receiver was programmed to sweep across the EM spectrum of the tag prototype while it performed AES encryptions for different plaintexts. The sweep was performed using a filter bandwidth of 3 MHz. We have used the receiver for mixing down the HF signals to an intermediate frequency of 20.4 MHz which was sampled with the digital oscilloscope. We recorded 1000 traces for different plaintexts for each 3 MHz interval between 10 MHz and 100 MHz. Subsequently, an electromagnetic-analysis attack was performed for each of the 30 frequency intervals. The upper plot in Figure 6 shows the EM spectrum from 0 MHz to 100 MHz. The clock harmonics, which are a multiple of 13.56 MHz, can be clearly identified as peaks in the spectrum. The lower plot shows the correlation coefficient at each frequency interval. It can be observed that there are high data-dependent emissions in the sidebands of several clock harmonics. The highest obtained correlation coefficient is 0.39 at a frequency of 49 MHz.

Figure 6 Correlation across the EM spectrum of the passively powered RFID-tag prototype



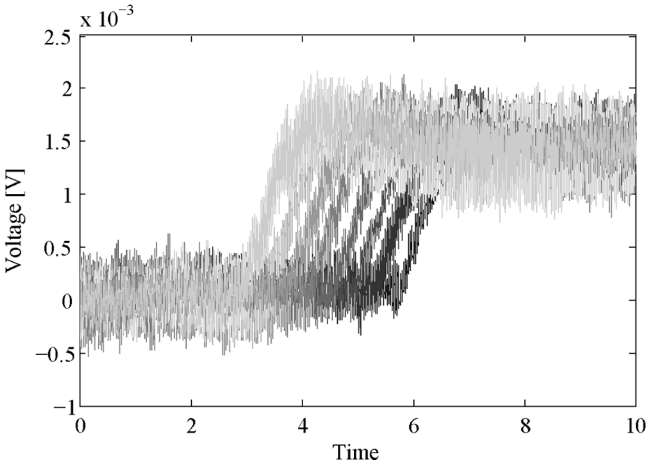
After the profiling phase, we conducted an electromagnetic-analysis attack in presence of the reader field. In this phase, the receiver has been used as a simple filter that separates the highest data-dependent frequency interval from the rest of the interfering signals. Thus, we adjusted the receiver to 49 MHz and performed an attack using the 3 MHz-filtered sideband signals of the tag prototype. Using this method, each secret key-byte of our AES implementation could be successfully revealed.

3.3 Exploiting timing variations

Exploiting timing variations of cryptographic devices was one of the first published side-channel attacks. Paul Kocher, who also introduced the differential power analysis, showed that it is possible to extract secret information out of various cryptographic systems such as RSA, Diffie-Hellman, and the Digital Signature Standard (DSS) in Kocher (1996). He showed that the cryptographic operations vary in the time depending on the processed data. An attack can exploit this data-dependent execution times and allows the extraction of the used secret key.

However, the same device behaviour that was shown in the mid 1990s can also be observed on RFID devices. Figure 7 shows the time variation during the writing of different data into the EEPROM of an RFID tag. It can be clearly observed that the power consumption raises earlier for certain input values. The power-consumption traces of different input values are drawn in different grey-scale colours. Depending on the processed data, the tag pulls the energy sooner or later from the reader field.

Figure 7 Data-dependent time variations in the execution time of a write operation of an RFID tag



In Table 1, an overview of the presented side-channel analysis attacks is given. The table lists the advantages and disadvantages of each method to characterise their properties and performance efficiency.

3.4 Implementation of countermeasures against SCA attacks

Power and EM analysis attacks work because the power consumption of the target depends on the intermediate values of the cryptographic algorithm. The two best known principles of SCA countermeasures are masking and hiding.

Masking tries to randomise the intermediate values that are processed on the device. On the architectural level, Boolean masks are typically applied to all intermediate values. This causes a relatively high overhead (especially in non-linear functions like the S-boxes), which is not acceptable for a passive RFID tag. Also masking countermeasures on the cell level require high additional costs. For example, the logic style Masked Dual-Rail Precharge Logic (MDPL) proposed by Popp and Mangard (2005) that has been invented to protect circuits at the cell level requires 4.5 times more chip area as standard Complementary Metal Oxide Semiconductor (CMOS) logic.

In contrast to masking, hiding countermeasures try to break the link between the processed data and the power consumption. The goal is to consume either random power in each clock cycle or to consume equal power in all clock cycles. In the amplitude dimension this is achieved by increasing the noise or by reducing the data-dependent signal. However, increasing the noise also means to increase the power consumption, which is very limited in passive RFID tags. Reducing the data-dependent signal is typically achieved by using a Dual-Rail Precharge (DRP) logic style like Sense Amplifier Based Logic (SABL) proposed by Tiri et al. (2002). As already explained, secure logic styles require a significantly higher chip area and have a high power consumption.

The most efficient hiding countermeasures for RFID tags work in the time dimension. In these methods, the attacked operations of the cryptographic algorithm are executed at different moments in time during each execution. This can be implemented by shuffling or by randomly inserting dummy operations. The basic idea of shuffling is to randomly change the sequence of the operations such that in each execution the attacked

Table 1 Efficiency of the described SCA methods performed on RFID devices

	Advantages	*Disadvantages*
Power	• Higher reproducibility due to a contact-based measurement setup	• Insertion of a measurement resistor
	• Direct contact to the chip necessary	
		• No selective measurement of chip components
EM	• (remote) attacks at a distance (undetectable)	• Weak signals in remote attacks (amplifiers)
	• Non destructive	• Noise of the proximity
	• Selective measurement of chip components	• Accurate positioning of probes required
Time	• RFID devices often process data serially	• Higher sampling rates required

intermediate result occurs at a different time location. Unfortunately, this measure only works to a certain extend because the different possibilities are limited depending on the executed algorithm. In case of AES this works on byte level, 16 different positions are feasible.

An alternative and an extension of the randomisation degree is the insertion of dummy cycles. In this method, so-called dummy operations are inserted before, during and after the execution of the actual operation. It is important that the total number of dummy cycles is constant to not allow an attacker to get any information about how many dummy cycles have been introduced. Before the execution, a random source decides at which positions the additional operations are inserted.

The advantages of countermeasures that work in the time domain are that the additional hardware resources are very low and the power consumption is nearly not increased. Only the controlling effort of the cryptographic module is higher. The additional runtime of the algorithm is for RFID tags, which have very low data rates, typically no problem. This makes randomisation in time to the best solution for low-cost countermeasures in passive RFID tags. An interesting solution has been presented in Feldhofer and Popp (2008). This paper shows the application of several low-cost countermeasures that have been optimised for the use in hardware modules for passive RFID tags.

4 Fault analysis

In the following, we describe four fault-analysis attacks on RFID devices. All attacks are non-invasive[2] and do not leave any damage of the chip. We performed spike and glitch attacks, electromagnetic fault-injections, optical fault-injections, and attacks by tearing off the reader field. Countermeasures to thwart these attacks are discussed afterwards.

4.1 Spike and glitch attacks

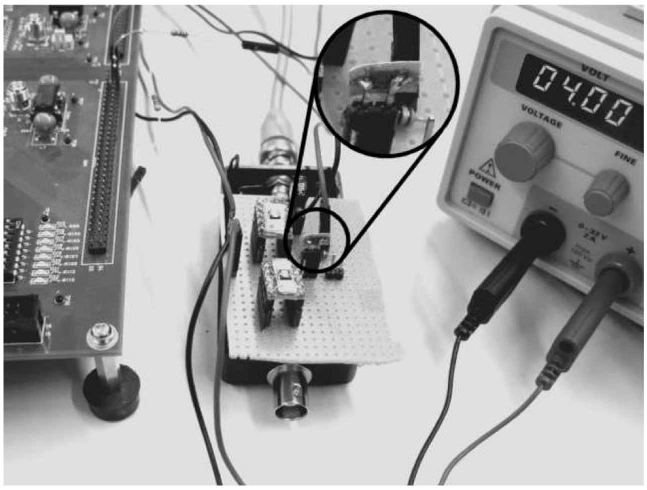
Among the most popular fault attacks against cryptographic devices are spike attacks and glitch attacks. The main difference of these two kinds is which external supply line of a device is interfered by the attack. Spike attacks basically affect the power-supply line of a device while glitch attacks interfere the clock-signal line.

Essentially, integrated circuits are designed to operate within a certain supply-voltage range. For CMOS devices, this range covers typically 1.2 V to 5 V. If the supply voltage exceeds the power-supply deviation tolerance of the device, the device might produce faults during the execution of algorithms. So-called induced over-voltage spikes can cause the chip to perform erroneous computations and can modify the execution path of the device. Glitch attacks, in contrast, modify the clock signal that is fed into the device. Like over-voltage spikes, variations in the clock signal might cause faulty computations.

One of the first publications that have demonstrated the effectiveness of spike and glitch attacks, have been published by Anderson and Kuhn (1997). They injected spikes and glitches in the power-supply line of a smart card and performed successful attacks on the Data Encryption Standard (DES) and the RSA cryptosystem. Boneh et al. (1997), and Biham and Shamir (1997) presented theoretical fault attacks on DES and RSA implementations. Practical experiments on smart cards are described by Kömmerling and Kuhn (1999). They showed various techniques for extracting protected data from smart-card processors.

In order to perform spike and glitch attacks on RFID devices, an appropriate setup is needed to inject the faults. In our experiments, we used a setup that is similar to the power-consumption measurement setup for RFID. First, the chip has been separated from its antenna and the antenna pins were directly connected to the reader. Between this connection, a switch has been placed in series that is able to switch the connection between the reader-to-chip line and an external DC power supply. This power supply is used to induce a fast over-voltage spike into the antenna interface of the RFID chip. The switch is further controlled by a trigger device that is composed of an 8-bit microcontroller and a Xilinx VirtexTM-II Pro Field Programmable Gate Array (FPGA). The trigger device is fully programmable to perform different trigger delays and trigger widths in order to vary the fault-injection time and period for the fault attack on the RFID chip. Note that the trigger device is also connected to the reader and listens to the communication. It starts a trigger event at an adjusted point in time between the reader request and the chip response. A picture of the RFID chip and the surrounding components such as the FPGA board and the DC power supply is depicted in Figure 8.

Figure 8 Setup of the fault attack to induce an over-voltage spike into the antenna interface of an RFID chip



By using the setup described above, we conducted an over-voltage spike attack on a commercially-available RFID tag. The target of the attack has been the writing of data into the internal memory of the tag. The attacking process is as follows. First, the tag receives the data from the reader and deletes the content of the current memory block. Second, it writes the received data into that memory block. After each write operation, the tag sends an acknowledge message to the reader or returns an error message if the writing was not succeeded. Hence, we injected a spike during the time between the last write-command sequence (end of frame) of the reader and the sending of the tag response. This time period can take some 100 μs depending on the tag manufacturer. By using the trigger device, we have been able to sweep over this time and accurately inject spikes in steps of only a few nanoseconds. The experiments have shown that RFID tags are vulnerable to such attacks and cause faults during the writing of data. After a fault injection, the tag performs a reset during the writing of data. This reset results in a faulty memory-value block because the tag was not able to finish the write operation. In addition, by using our setup, we have been even able to influence the value that is written into the memory. By varying the fault-injection time, the write operation is interrupted at different moments in time. Thereafter, the memory holds only that value which bits have been already written successfully.

4.2 *Electromagnetic fault-injections*

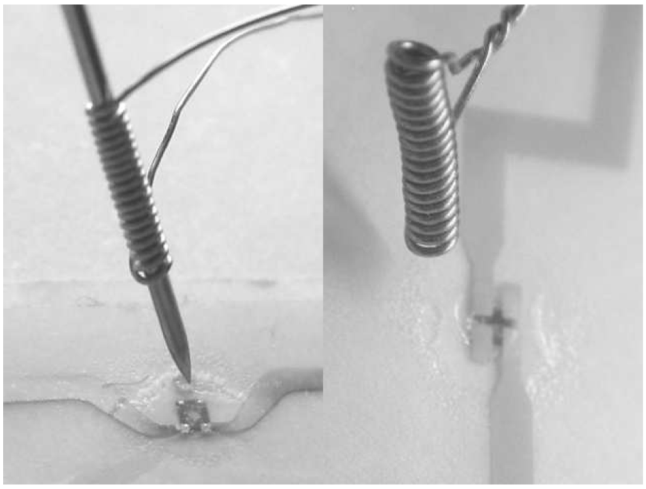
A fast-changing electromagnetic field induces current into conductors. Such a field is generated by a fast-changing current that is, for example, flowing through a coil. The characteristic of the coil, its windings, and the distance from the coil to the chip surface define the pulse strength and efficiency of the electromagnetic fault-injection.

Electromagnetic attacks are non- or at least semi-invasive attacks and allow fault injections to be performed without direct contact to the device. No chip-decapsulation procedure has to be applied in practice. However, the position of the probe often requires the accuracy of an appropriate probing station. Depending on the position and distance of the probe, globally as well as locally injected faults can be achieved.

Quisquater and Samyde (2002) have been one of the first who published results of electromagnetic fault-attacks on smart cards. They used a probe coil with several hundred windings and induced eddy currents inside the chip. They have been able to insert transient as well as permanent faults in the memory of the chip.

Electromagnetic fault injections in RFID tags have been first presented by Hutter et al. (2008). A high-voltage generator has been used to inject faults during the writing of data into the tag memory. The device is capable of generating electromagnetic sparks of high intensity. The circuit consists of a digital part that is used to produce a pulsating square wave of about 100 V. This pulse is then amplified using a DC voltage converter and a charge-pump circuit. Using this setup, the injection voltage could be raised up to 18 kV. The injection is controlled by a high-voltage relay. The output of the generator is then connected to a probe coil. As soon as the current flows through the coil, a current is induced into the RFID chip which influences the processing of operations. In Figure 9, two probe coils are shown that have been placed on top of RFID chips.

Figure 9 Electromagnetic fault-injections using tiny probe coils



Although fault injections could only be performed very inaccurately because of the used relay, RFID tags could be effectively influenced in their operation. The same chip behaviour has been observed that has been discerned by injecting spike attacks. Note that the Electrostatic Discharge (ESD) of the high voltages generates strong electromagnetic interferences that might influence or even damage electronic devices in the proximity. This kind of fault-injection is therefore more complex in term of EM shielding, fault-injection handling, and human security.

4.3 *Optical fault-injections*

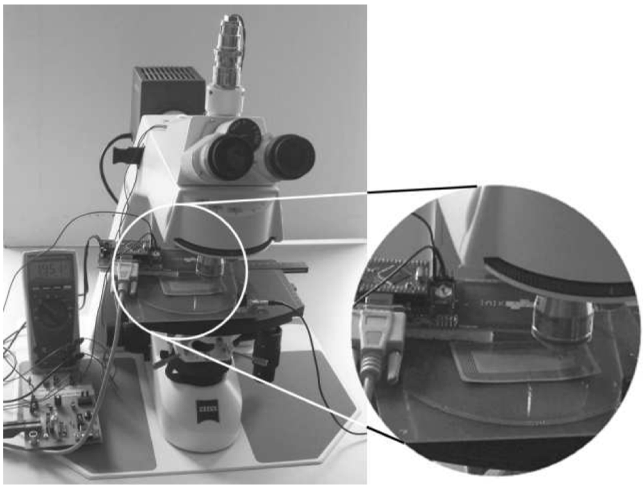
Light that hits special regions of a chip induces a current.[3] This current is often referred to as Optical Beam Induced Current (OBIC). Internal transistors get switched by the light and cause faults during the processing of data (Tan et al., 1997).

Fault attacks using optical fault injections basically need an intervisibility to regions of the chip that are being attacked. The package of the chip has therefore to be opened and decapsulated. For RFID chips, which are often only covered by a transparent smart label, direct sight to the chip die might already exist. These kind of attacks are therefore either non-invasive or semi-invasive. Similar to the electromagnetic injections, the region of the fault occurrence can be adjusted by the focus and the size of the light beam.

Skorobogatov and Anderson (2003) have first demonstrated the potential of optical fault-injections on secure microcontrollers and smart cards. They showed that it is possible to cause simple transistors to conduct by illuminating the chip with a focused laser beam. Blömer and Seifert (2003) presented optical as well as electromagnetic fault-attacks on AES. The attack allows the extraction of the complete 128-bit secret key of a sealed tamper-proof smart card.

In order to inject faults into RFID devices, we have used a microscope to focus a light beam to specific regions of the chip. The microscope has an integrated camera port where a camera can be connected to take pictures of enlarged chip regions. Instead of the camera, we connected a laser diode which provides an optical output power of about 100 mW. The emitted light has a wavelength of 785 nm. Furthermore, a collimator lens is used to parallelise the laser beam. The focus has been realised through an optical objective which offers a magnification of 50 diameters. In Figure 10, the setup for the optical fault-injection attack is given. The focused laser beam illuminates an RFID tag that lies upon an RFID-reader antenna. The communication of the reader is eavesdropped by a trigger device. The trigger device listens to reader requests and starts the illumination of the chip by turning on the laser diode. For the experiments, we have varied the illumination starting time as well as the illumination duration for different RFID devices. The target of the attacks has been the writing of data into the tag memory.

Figure 10 Optical fault injections on an RFID chip using a focused laser beam



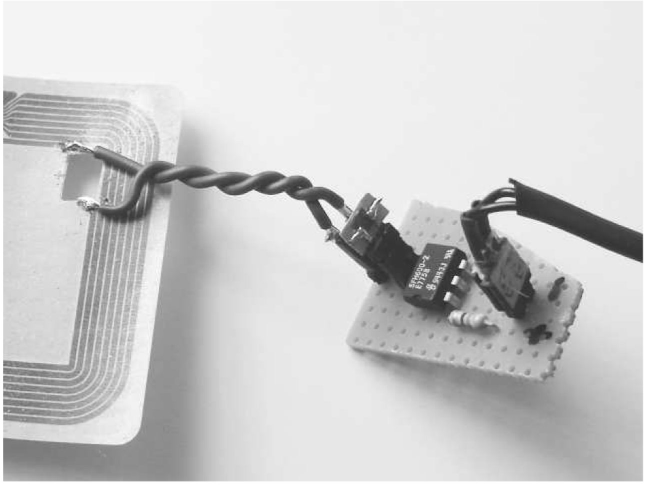
Our investigations have led us to the following results. First, they have shown that RFID devices are vulnerable to optical fault-attacks. By illuminating larger parts of the chip, the same results could be achieved as with spike attacks or electromagnetic fault-attacks. If the light of the laser is chosen very intense, the tag performs a reset as it was in the case of the other performed attacks. Faulty values remained in their EEPROM memory. Second, it has shown that if the laser beam is focused on specific regions on the chip, a faulty value is written into the memory whereas no reset is performed. After fault injection, the tag sends a successful write-operation response to the reader while a faulty value was written into the memory. Due to the large opportunities and options for different fault-injection possibilities, optical fault-attacks constitute one of the most powerful attacks that can be conducted in practice.

4.4 Tearing attacks

Another possibility to cause faults on RFID devices is to tear-off the antenna during the execution of a sensitive operation. So-called tearing attacks are usually known from contactless smart-card applications, where smart-card implementations have to take care of sudden power losses during sensitive computations (see for example the work of Hubbers et al. (2006)). In view of RFID, tearing attacks can be similarly performed by temporarily conducting the input pads of the chip as it was shown by Hutter et al. (2008). This bypasses the antenna connection for a certain amount of time which may cause the chip to perform erroneous computation results.

We have performed tearing attacks on RFID devices by following the next described process. First, we have separated the chip from the antenna. Between the chip and the antenna, we have placed an optocoupler that is used to temporarily interconnect the antenna pins of the RFID chip. Optocouplers, in general, use a short optical transmission path that allows the transmission of signals without having electric contact. This optocoupler is controlled by the same trigger device that was also used for the other fault-attack experiments. In Figure 11, the setup of the tearing attack on an HF RFID tag is shown.

Figure 11 Setup of a tearing attack on an HF RFID tag



In the next step, a write command is sent by the reader that causes a trigger event during the writing of data into the memory. This trigger event switches the optocoupler which interconnects the antenna pins of the chip. Accordingly, faulty values were written into the memory due to an unexpected power-loss of the tag.

In Table 2, the efficiency of the performed fault-injection methods is characterised. The table lists the advantages and disadvantages of each method to describe their performance.

Table 2 Efficiency of the described fault-injection methods performed on RFID devices

	Advantages	*Disadvantages*
Spikes/Glitches	• Modification of data and programme flow	• Direct contact to the chip (destructive) • Accurate fault-injection equipment needed
EM	• Non invasive • Allow (remote) attacks at a distance	• High voltages (dangerous) • Appropriate equipment required • Can lead to a destruction of the chip
Optical	• Selective location of fault injection • Allow attacks at low distance	• Decapsulation maybe necessary • More expensive equipment needed
Antenna tearing	• Low cost	• Removing chip from antenna (destructive) • Global fault injections

4.5 Implementation of countermeasures against fault attacks

Countermeasures for RFID devices against fault attacks are very similar to those which have been integrated on (contactless) smart cards. Basically, there exist three different concepts for such countermeasures. The first concept is to prevent the injection of faults. This can be realised for example through passive or active shielding. A mesh of power lines is placed on top of the chip surface. This countermeasure makes electromagnetic attacks much more difficult to perform. Another way to prevent the injection is to integrate different sensors that check the power supply and the clock signal for critical modifications. An alarm might be triggered in case of an injection that causes the chip to jump into a specific safe state. There also exist detectors for optical light and temperature variations that look for deviant operating conditions. In security-related applications, some devices also include a self-destruction capability in case of an external intrusion detection. In view of passive RFID tags, these kind of countermeasures are quite effective but need a high amount of overhead in respect of power consumption and chip size. They are therefore often omitted in practical implementations.

The second concept is to distribute computations of sensitive data over a certain period of time. In fact, this does not prevent the fault injection itself but reduces the exploitation of sensitive information. For RFID devices, this countermeasure offers a potential and effective way to prevent the extent of information extraction by requiring an inessential amount of implementation costs.

The third concept makes use of redundant computations. This is indeed one of the most intuitive and usable ways in practice. Intermediate values and results are computed twice and checked at the end of both computations. The computation can be calculated consecutively on the same hardware unit or it can be calculated in parallel. The implementation of the parallel version obviously needs twice the area which often discourages the use of concurrent executions. Especially for RFID implementations, the consecutive computation is attractive due to two reasons. First, time is typically not a critical factor in RFID applications. The recalculation of results is therefore possible without any functional constraints. Second, the additional overhead in terms of chip area is only marginal compared to its fault-protection capability. Alternatively, error-detecting codes can be applied. The codes calculate the signature of sensitive data and they concurrently check the values by using for instance parity bits.

While there exist many proposals and solutions for fault protection in practice, there will be no effective and satisfying protection against powerful adversaries. The history already illustrated the difficulty of preventing attacks and intrusion techniques also on security-related devices. Countermeasures may not provide complete and perfect protection for a given system but they can make attacks considerably harder to perform in practice.

5 Conclusions

This paper surveys different implementation attacks on RFID devices. We performed practical attacks using both side-channel analysis and fault analysis. The results of our experiments demonstrate the susceptibility of tags and the potential of practical implementation attacks against these kind of devices. We successfully extracted secret information out of passively-powered RFID tags. Furthermore, we show the vulnerability of tags against active fault injections during the writing of data. In addition to these findings, we give an overview of various countermeasures to thwart these attacks. The countermeasures can be applied with low cost and provide an adjustable degree of security. We suggest the integration of appropriate countermeasures into RFID devices especially in the case where they are applied in security-related applications.

Acknowledgements

The authors would like to thank Jörn-Marc Schmidt for his active collaboration in this work. The research described in this paper has been supported by the European Commission funded project *Collaboration at Rural* under the grant number 034921 (project C@R) and the FIT-IT initiative of the Austrian Federal Ministry of Transport, Innovation, and Technology (project CRYPTA) under the grant number 820843. The information in this document reflects only the authors' views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

Agrawal, D., Archambeault, B., Rao, J.R. and Rohatgi, P. (2003) 'The EM side-channel(s)', in Kaliski Jr., B.S., Kaya Koç, Ç. and Paar, C. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop*, Redwood Shores, CA, USA, 13–15 August, Revised Papers, Volume 2523 of Lecture Notes in Computer Science, Springer, pp.29–45.

Anderson, R.J. and Kuhn, M.G. (1996) 'Tamper resistance – a cautionary note', *Proceedings of the 2nd Usenix Workshop on Electronic Commerce*, Oakland, California, 18–21 November, pp.1–11.

Anderson, R.J. and Kuhn, M.G. (1997) 'Low cost attacks on tamper resistant devices', in Christianson, B., Crispo, B., Lomas, M. and Roe, M. (Eds.): *Security Protocols, 5th International Workshop*, Volume 1361 of Lecture Notes in Computer Science, Springer, pp.125–136.

Biham, E. and Shamir, A. (1997) 'Differential fault analysis of secret key cryptosystems', in Kaliski Jr., B.S. (Ed.): *Proceedings of the 17th Annual International Cryptology Conference Advances in Cryptology – CRYPTO'97*, Santa Barbara, California, USA, 17–21 August, Volume 1294 of Lecture Notes in Computer Science, Springer, pp.513–525.

Blömer, J. and Seifert, J-P. (2003) 'Fault based cryptoanalysis of the advanced encryption standard (AES)', in Wright, R.N. (Ed.): *Financial Cryptography, 7th International Conference, FC 2003*, Guadeloupe, French West Indies, 27–30 January, Revised Papers, Volume 2742 of Lecture Notes in Computer Science, Springer, pp.162–181.

Boneh, D., DeMillo, R.A. and Lipton, R.J. (1997) 'On the importance of checking cryptographic protocols for faults (extended abstract)', in Fumy, W. (Ed.): *Proceedings of the Advances in Cryptology – EUROCRYPT'97, International Conference on the Theory and Application of Cryptographic Techniques*, Konstanz, Germany, 11–15 May, Volume 1233 of Lecture Notes in Computer Science, Springer, pp.37–51.

Carluccio, D., Lemke, K. and Paar, C. (2005) 'Electromagnetic side channel analysis of a contactless smart card: first results', in Oswald, E. (Ed.): *Workshop on RFID and Lightweight Crypto (RFIDSec05)*, 13–15 July, Graz, Austria, pp.44–51.

Feldhofer, M. and Popp, T. (2008) 'Power analysis resistant AES implementation for passive RFID tags', in Lackner, C., Ostermann, T., Sams, M. and Spilka, R. (Eds.): *Proceedings of Austrochip 2008*, 8 October, Linz, Austria, pp.1–6, ISBN: 978-3-200-01330-8.

Gandolfi, K., Mourtel, C. and Olivier, F. (2001) 'Electromagnetic analysis: concrete results', in Kaya Koç, Ç., Naccache, D. and Paar, C. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2001, Proceedings of the Third International Workshop*, Paris, France, 14–16 May, Volume 2162 of Lecture Notes in Computer Science, Springer, pp.251–261.

Hubbers, E., Mostowski, W. and Poll, E. (2006) 'Tearing Java cards', *Proceedings of the 7th Edition of e-smart Conference and Demos*, 20–22 September, Sophia Antipolis, French Riviera, France.

Hutter, M., Mangard, S. and Feldhofer, M. (2007) 'Power and EM attacks on passive 13.56 MHz RFID devices', in Paillier, P. and Verbauwhede, I. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2007, Proceedings of the 9th International Workshop*, Vienna, Austria, 10–13 September, Volume 4727 of Lecture Notes in Computer Science, Springer, pp.320–333.

Hutter, M., Schmidt, J-M. and Plos, T. (2008) 'RFID and its vulnerability to faults', in Oswald, E. and Rohatgi, P. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2008, Proceedings of the 10th International Workshop*, Washington DC, USA, 10–13 August, Volume 5154 of Lecture Notes in Computer Science, Springer, pp.363—379.

International Organisation for Standardization (ISO) (2001) *ISO/IEC 10373-6: Identification Cards – Test Methods – Part 6: Proximity Cards*, Geneva, Switzerland, 15 May.

Kocher, P.C. (1996) 'Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems', in Koblitz, N. (Ed.): *Advances in Cryptology – CRYPTO'96, Proceedings of the 16th Annual International Cryptology Conference*, Santa Barbara, California, USA, 18–22 August, Number 1109 in Lecture Notes in Computer Science, Springer, pp.104–113.

Kocher, P.C., Jaffe, J. and Jun, B. (1999) 'Differential power analysis', in Wiener, M. (Ed.): *Advances in Cryptology – CRYPTO '99, Proceedings of the 19th Annual International Cryptology Conference*, Santa Barbara, California, USA, 15–19 August, Volume 1666 of Lecture Notes in Computer Science, Springer, pp.388–397.

Kömmerling, O. and Kuhn, M.G. (1999) 'Design principles for tamper-resistant smartcard processors', *Proceedings of the 1st USENIX Workshop on Smartcard Technology (Smartcard'99)*, Chicago, Illinois, USA, 10–11 May, pp.9–20.

Mangard, S., Oswald, E. and Popp, T. (2007) *Power Analysis Attacks – Revealing the Secrets of Smart Cards*, Springer, Berlin, 11 April, ISBN 978-0-387-30857-9.

Popp, T. and Mangard, S. (2005) 'Masked dual-rail pre-charge logic: DPA-resistance without routing constraints', in Rao, J.R. and Sunar, B. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2005, Proceedings of the 7th International Workshop*, Edinburgh, UK, 29 August – 1 September, Volume 3659 of Lecture Notes in Computer Science, Springer, pp.172–186.

Quisquater, J-J. and Samyde, D. (2001) 'ElectroMagnetic analysis (EMA): measures and counter-measures for smart cards', in Attali, I. and Jensen, T.P. (Eds.): *Smart Card Programming and Security, Proceedings of the International Conference on Research in Smart Cards, E-smart 2001*, Cannes, France, 19–21 September, Volume 2140 of Lecture Notes in Computer Science, Springer, pp.200–210.

Quisquater, J-J. and Samyde, D. (2002) 'Eddy current for magnetic analysis with active sensor', *Proceedings of the 3rd International Conference on Research in SmartCards (E-Smart'02)*, September, Nice, France, pp.185–194.

Skorobogatov, S.P. and Anderson, R.J. (2003) 'Optical fault induction attacks', in Kaliski Jr., B.S. Kaya Koç, Ç. and Paar, C. (Eds.): *Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop*, Redwood Shores, CA, USA, 13–15 August, Revised Papers, Volume 2523 of Lecture Notes in Computer Science, Springer, pp.2–12.

Tan, K., Tan, S. and Ong, S. (1997) 'Functional failure analysis on analog device by optical beam induced current technique', in Radhakrishnan, M.K., Ho, P. and Kin, C.W. (Eds.): *Proceedings of the 6th International Symposium on Physical and Failure Analysis of Integrated Circuits (IPFA'97)*, 21–25 July, Raffles City Convention Centre, IEEE, Singapore, pp.296–301.

Tiri, K., Akmal, M. and Verbauwhede, I. (2002) 'A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards', *Proceedings of the 28th European Solid-State Circuits Conference – ESSCIRC 2002*, 24–26 September, IEEE, Florence, Italy, pp.403–406.

Notes

[1] Another kind of implementation attacks that is not addressed within this paper is the passive probing of inner states of a circuit by using a proper probing station (probing attacks).

[2] Our attacks do not modify the chip layout but only the RFID-tag inlay.

[3] A line-of-sight to the NP junction of the target transistor is required to cause an electron reaction.