# RFID and Its Vulnerability to Faults

Michael Hutter[1], Jörn-Marc Schmidt[1,2], and Thomas Plos[1]

[1] Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
{Michael.Hutter,Joern-Marc.Schmidt,Thomas.Plos}@iaik.tugraz.at
[2] Secure Business Austria (SBA),
Favoritenstraße 16, 1040 Vienna, Austria

**Abstract.** Radio Frequency Identification (RFID) is a rapidly upcoming technology that has become more and more important also in security-related applications. In this article, we discuss the impact of faults on this kind of devices. We have analyzed conventional passive RFID tags from different vendors operating in the High Frequency (HF) and Ultra-High Frequency (UHF) band. First, we consider faults that have been enforced globally affecting the entire RFID chip. We have induced faults caused by temporarily antenna tearing, electromagnetic interferences, and optical inductions. Second, we consider faults that have been caused locally using a focused laser beam. Our experiments have led us to the result that RFID tags are exceedingly vulnerable to faults during the writing of data that is stored into the internal memory. We show that it is possible to prevent the writing of this data as well as to allow the writing of faulty values. In both cases, tags confirm the operation to be successful. We conclude that fault analysis poses a serious threat in this context and has to be considered if cryptographic primitives are embedded into low-cost RFID tags.

**Keywords:** RFID, Fault Analysis, Antenna Tearing, Optical Injections, Electromagnetic Analysis, Implementation Attacks.

## 1 Introduction

Fault analysis is a powerful technique to reveal secret information out of cryptographic devices. Instead of passive techniques where power or electromagnetic side channels are exploited, fault attacks make use of active methods to cause errors during the processing of cryptographic primitives. This article focuses on such active methods that have been applied to RFID, a technology that has become more security related over the last time.

RFID devices consist of a small microchip attached to an antenna. These so-called tags can be powered actively or passively. Actively powered tags use an own power supply, typically a battery. Passive ones are powered by the electromagnetic field generated by a reader. This field is also used for data communication and the transmission of the clock signal. There are numerous types of tags available that can be differentiated depending on the application. They differ in

E. Oswald and P. Rohatgi (Eds.): CHES 2008, LNCS 5154, pp. 363–379, 2008.

their size, shape, functionality, prize, and operating frequency. However, the use of RFID tags is already widespread not only in industry but also in everyday life. They are used in applications such as inventory control, pet identification, e-passports, or in pharmaceutical products. In particular, as RFID is more widely integrated into sensitive areas such as health care or access-control systems, the question of security becomes increasingly important. Currently, there has been much effort to make cryptography applicable to RFID devices. While the integration of cryptographic functions in many typical applications is somewhat straightforward, it is not in the field of RFID. Implementations must have a small footprint not to exceed the costs, and they have to be designed for low power in order to allow a certain reading range. A lot of proposals have been published so far that deal with lightweight cryptography for RFID by using coupon-based signature functions like GPS [23,18], stream ciphers [7,12,9], asymmetric algorithms like ECC [30,4], or symmetric algorithms like AES [10], PRESENT [6], SEA [28], HIGHT [13], or DES variants [22]. At the time, the security features of conventional RFID tags range from simple secure memory-lock functionalities to integrated cryptographic engines like Mifare [19], SecureRF [26], or CryptoRF [2].

Nevertheless, in the last decade, a lot of articles have been published that point out specific physical weaknesses of cryptographic implementations. Initiated by the pioneering work of Kocher et al. [15,16], a lot of attacks have been proposed on different kinds of devices that emphasize the need for hardware and software countermeasures. Especially fault attacks provide a variety of attacking possibilities that can evade effective side-channel countermeasures. Therefore, they are a field of increasing interest. S. Skorobogatov et al. [27] induced optical faults on microcontrollers. J.-J. Quisquater et al. [24] made use of active sensors to inject eddy currents. They have been able to insert permanent faults as well as transient faults into a circuit. Glitch attacks have been performed, for example, by O. Kömmerling et al. [17] or H. Bar-El et al. [3]. In the light of RFID, only a few articles have been published so far that focus on side-channel attacks. In [14], M. Hutter et al. discussed power and EM attacks on passive HF tags. Y. Oren et al. [20] and T. Plos [21] focused on power analysis of UHF tags. However, there is no dedicated article covering the topic of fault injections on RFID so far.

In this article, we introduce fault-analysis attacks performed on different kinds of commonly-used passive RFID tags in the form of adhesive labels. Several tags from various vendors have been examined including HF and UHF tags. The tags include neither cryptographic primitives nor countermeasures against fault-analysis attacks. The main intention of this article is to investigate the susceptibility of faults on RFID devices. This enables the verification whether the threat of faults on such kind of devices is realistic or not. We have focused on the writing of data since this operation is considered critical in respect of power consumption and execution time. Therefore, the target of the analysis has been the time between a reader request and the tag response.

Fault-injection methods can be divided into two categories dependent on how they are injected: globally and locally. For global fault injections, we have analyzed the impact of temporarily antenna tearing as well as electromagnetic interferences and optical laser-beam inductions. Temporarily antenna tearing has been obtained by simply interconnecting the antenna pins of the RFID chip. Electromagnetic interferences have been caused by a high-voltage generator. Optical faults have been induced by irradiating the chip using a simple laser diode. For local fault injections, a microscope has been used in order to get a focused laser beam. This beam has been concentrated on the control logic of the internal memory. The experiments have led us to several interesting results. At first, all investigated tags are vulnerable to faults during the writing of data. We show that fault-injection methods allow the prevention of writing data into the tag memory and, even worse, to allow the writing of faulty values. In both scenarios, the tags confirm the write operation to be successful. This is the first article that discusses fault analysis on RFID and emphasizes the need of countermeasures against fault-analysis attacks based on practical experiments.

This article is structured as follows. Section 2 gives an overview to the state-of-the-art security mechanisms of common RFID tags. Section 3 focuses on different fault-injection methods that can be applied on RFID tags. In Section 4, the performed analyses are described in detail. Section 5 deals with the measurement setups that are needed for fault analyses. The obtained results are given in Section 6. Section 7 summarizes the results and conclusions are drawn in Section 8.

## 2 State-of-the-Art Security Mechanisms for Passive RFID Tags

It is somehow evident that wireless devices like passive RFID tags require special efforts to reach a comparable security level as contact-based powered devices like smart cards and conventional microcontrollers. While these devices require physical contact to the power supply, passive tags gain their power from the radio frequency (RF) field generated by a reader. This field is rather unstable due to noise and interferences of the proximity. The certainty of the proper tag operation becomes therefore largely infeasible. Thus, conventional tags commonly include protection mechanisms against unintended failures. One of the most sensitive tag operations are the reading and writing of data. This data can be verified by using, for example, cyclic redundancy checks (CRC). The CRC is commonly used to detect failures during RFID-protocol communication but can also be applied to internal memory structures to prevent the storing of faulty values. There also exist so-called anti-tearing mechanisms that provide the verification of data integrity and data consistency when the tag is pulled out of the reader field or if the tag has not enough power to complete a certain operation. These tags may include data backup and shadow-memory techniques that allow the recovery of the data when the tag is powered up the next time after the occurrence of an interruption. In view of intended intervention, tags often

support password protection mechanisms to restrict the reading or writing into the memory. If a transmitted password is valid, the corresponding memory zone becomes accessible as long as the tag is powered up and in active state. The major concern of this weak authentication is the insufficient protection against passive eavesdropping and the potential use of replay attacks. In order to prevent any attempt of impersonalization, one-time passwords or challenge-response protocols are commonly used to proof the origin of the transmitted data from either the tag, the reader, or both. In many cases these protocols implement zero-knowledge concepts or make use of symmetric or asymmetric cryptography to offer strong authentication. There are actually tags available that support the encryption of the transmitted data stream which prevents from skimming attacks or eavesdropping. There are only a few tags available on the market that provide countermeasures against active attacks by using, for example, tamper sensors [2].

## 3 Fault Analysis on RFID Tags

As soon as security becomes a major concern in an application, the perspective of adversaries has to be taken into account. When having physical interaction with the device under attack, a lot of possibilities arise with respect to compromise secret information. Faults pose one of these threats that are caused by either intended or unintended misuse of the system. In the following, we focus on intended fault injections as a method for active attacks. Essentially, faults can be induced globally or locally. Global fault-injection methods influence the entire device and are therefore quite imprecisely. Local fault-injection methods, in contrast, affect only specific parts of the device. There, it is possible to focus on specific regions that are assumed to contain sensitive information. The control of an adversary depends on the fault-injection method which can be non-invasive, semi-invasive, or invasive. While non-invasive methods leave the package of a device untouched, semi-invasive as well as invasive techniques apply a decapsulation procedure to expose the chip surface. Invasive methods also establish direct electrical contact to the chip. In addition to the control of fault injections, the precision of timing constitutes an important factor for an attack. In the following, the structure of an RFID tag is analyzed. After that, the most promising fault-injection methods are described and they are further related to RFID tags.

In general, there are two proven approaches for the manufacturing of an RFID tag. The first one directly mounts the chip onto its antenna. However, this method needs a high precision in the handling and the operating condition and is therefore often outsourced by companies using the second approach. There, a special flip-chip package called *strap* is used which is typically a small Printed Circuit Board (PCB). First, the RFID chip is bonded onto that strap PCB. Second, the strap is mounted onto the antenna. In Figure 1, the cross section of a tag is shown where the chip is interconnected to the antenna circuit. Often, a special ink layer is inserted between the chip and the antenna circuit and a Polyethylene Terephthalate (PET) film is used as a carrier for RFID inlays [11].

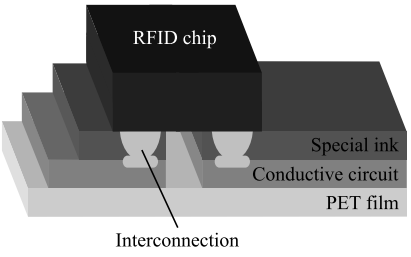


**Fig. 1.** Cross section of a tag where the RFID chip is interconnected to a conductive circuit (antenna)

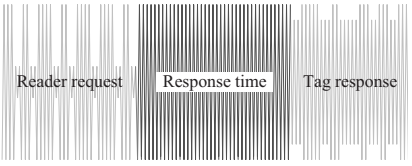


**Fig. 2.** The tag performs computational work in the response time that is located between reader request and tag response

**Temperature Variations.** The heating of cryptographic devices Variations in the operating temperature of cryptographic devices cause faulty computations or random modifications of memory cells. Although CMOS technology is quite resistant to low temperatures, high temperatures lead to variances in the device characteristics like circuit conductance, leakage current, or diode voltage drops [24,3]. Nevertheless, the heating of semiconductors can only be achieved by global means. The adversary has no precise control concerning the timing and the resulting behavior.

In the light of the fact that RFID tags include analog circuits and that these circuits are quite susceptible to temperature variations, tags in high temperature conditions will not be able to communicate with the reader anymore. At a certain temperature, tags are unable to write data into the memory. For common passive RFID tags this is typically around 180 °C. Exceeding higher temperature limits will lead to a complete blackout of tags. In order to avoid the deformation of the tag antenna and the destruction of the inlay label, the chip has to be preferably separated from its antenna before it is stressed with heating.

**Power and Clock Variations.** Sudden changes in power levels or signal clock cycles are called spikes and glitches, respectively. These variations may cause the chip to either misinterpret instructions or to modify the values of internal data-bus lines of semiconductors [1,3]. This form of intervention can only be performed in a global manner but have to be injected very precisely in time.

In the context of RFID, both the power supply and the clock signal are extracted out of the reader field. The RFID tag only possesses two input pads that are normally connected to the tag antenna. By temporarily conducting these input pads, the antenna is bypassed for a certain amount of time. Tearing attacks like on smart cards focus on such supply interruptions and have to be considered especially in contact-less powered devices.

**Electromagnetic Interferences.** A fast-changing electromagnetic field induces current into conductors. Such a field is generated by a fast-changing current that is 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 injection [24,25]. Although there is no need for a chip-decapsulation procedure, a proper probing station is necessary in order to be able to precisely place the probe. Thus, global as well as local fault injections are feasible both with precise timing.

As stated in [5], RFID devices that operate in higher frequencies like UHF tags, are considered to be more sensitive to electromagnetic interferences. Their antenna is largely receptive to high-frequency signals, which are around 900 MHz.

**Optical Inductions.** Light that hits the surface of a chip induces current. This current is often referred to as Optical Beam Induced Current (OBIC) [29]. This optical injection leads transistors to switch and causes faults during the processing of the chip [27]. In order to induce faults, the light beam has to be focused on the chip surface. Thus, it is essential to have intervisibility to regions that are intended to be attacked. As already described in Section 3, many RFID tags are only covered by a transparent PET inlay. Parts of the chip are also hidden by the antenna circuit. Remaining PET layers, adhesive, and dirt can be either removed by carefully scratching off or by using chemicals. Optical faults can be induced very precisely in time and can be applied globally and locally. Moreover, they are semi-invasive and need the decapsulation of the chip. For tags that use transparent inlays, optical inductions are performed innately without further de-packaging. In this context, they are therefore considered to be non-invasive.

## 4 Performed Analyses

There exist many possibilities to induce faults on RFID devices. In this article, we focus on power and clock variations as well as on electromagnetic interferences and optical laser-beam inductions. Power and clock variations have been achieved by temporarily interconnecting the antenna pins of the RFID tag. Electromagnetic injections have been carried out with the help of a self-designed high-voltage generator that is capable of producing sharp-edged EM pulses. Optical laser-beam inductions have been conducted globally by using a simple low-cost laser diode as well as locally by using an additional microscope. In Figure 2, the basic communication process in an RFID system is shown. At first, the reader interrogates the tag by sending a request to the tag. The tag receives and processes the request accordingly and sends the response back to the reader. The time when the tag processes the request of the reader is called the response time. During this time, the tag performs some computational work like writing data into the internal memory or calculating the CRC that is needed and used in the tag response. In our experiments, we have induced faults during this response time in order to disturb the writing of data into the internal memory of the tag. In this time, no RF communication is done neither from reader to tag nor from tag to the reader. The faults have been induced only in the response time after which the tag sends a response back to the reader, if the faults have not caused a reset of the tag actually. Furthermore, the faults have

been induced in a very short period of time that is defined by the trigger width. In addition to the trigger width, we have also varied the point in time at which a fault injection is performed. We have implemented an automatic fault-injection sweep that covers the whole response time from its beginning to its end. The whole response time depends on the memory programming time, the underlying protocol, and the used data rate. In our experiments the response time takes a few milliseconds. The memory programming time, in particular, has taken a few hundred microseconds. We have analyzed tags using the ISO 15693 protocol for HF tags and the ISO 18000-6C (EPC Gen2) protocol for UHF tags. The data rate for HF tags has been 26.48 kbps (fast mode) for both reader to tag and tag to reader communication. For the UHF tags, a data rate of 26.67 kbps for reader to tag communication and 40 kbps for tag to reader communication has been used.

## 5 Measurement Setups

In order to perform fault injections, various measurement setups have been used in our experiments. All measurement setups use a PC, a standard RFID reader, a tag emulator, and the device under attack. The PC controls the devices using appropriate measurement scripts. Therefore, Matlab has been used which provides serial-connection options as well as useful functionalities like plotting and post-processing facilities. For both HF and UHF frequencies, a tag emulator has been used that is capable of eavesdropping the reader-to-tag communication. The emulators include an antenna, an analog front-end, and a programmable microcontroller. They are used to provide a trigger event that gets activated at the beginning of the response time. The trigger offset is then increased by steps of about 300 ns until the end of the response time is reached and the modulation of the tag response starts. Thus, a precise event is provided in order to trigger the antenna tearing, electromagnetic injection, and the optical induction performed by using the setups described in the following. First, the measurement setups for global fault injections are described. Second, the measurement setup for the local fault injections is described.

### 5.1 Setups for Global Fault Injections

The setups for global fault injections and the setup for local fault injections differ in several ways. One of the major advantages of global injections is the fact that no sophisticated equipment like probing stations or microscopes are required. The location of the fault induction is therefore fairly imprecise. Faults affect the entire chip and make an accurate knowledge of the chip circuit unessential. In fact, global faults can be performed using low-cost equipment and are rather versatile compared to immotile equipment.

**Temporarily Antenna Tearing.** For this setup, we have separated the chip from the tag antenna in a similar way as done by [8]. Between the chip and the

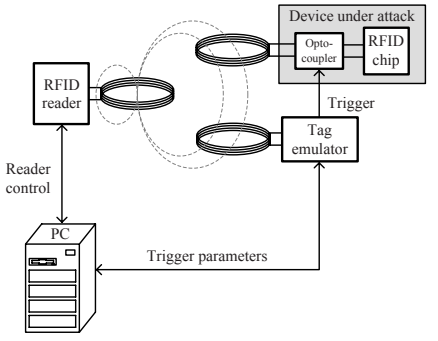


**Fig. 3.** Schematic view of the measurement setup for performing antenna-tearing attacks using an optocoupler that is placed between tag antenna and chip

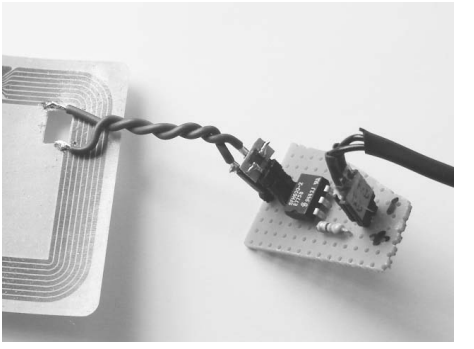

**Fig. 4.** Picture of the antenna-tearing setup where the chip has been separated from its antenna

antenna an optocoupler has been placed 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. On the one hand, this is useful to protect the tag emulator against high-voltage interferences. On the other hand, it prevents against additional capacitive coupling through the galvanic isolation. This is especially necessary for antenna circuits that are matched for higher frequencies as it is used in UHF tags. In Figure 3, the used measurement setup is shown. A PC is used to control the overall measurement process. The PC is connected to an RFID reader and to the tag emulator. For UHF measurements, a reader has been used that has a field strength of about 60 mW. The distance between the reader and the device under attack and the tag emulator has been about 10 cm. For HF measurements, a field strength of about 400 mW was chosen and the device under attack and the tag emulator have been placed directly upon the reader antenna. However, the PC has been used to send write commands to the reader and to set trigger parameters to the tag emulator which has been programmed to perform the triggering. The tag emulator has therefore been placed inside the reader field to identify the beginning of the response time. Furthermore, it is connected to the optocoupler which allows us to interconnect the antenna of the chip for a user-defined interval. In Figure 4, a picture is given that shows the detachment of the tag antenna and the integration of an optocoupler.

**Electromagnetic Interferences.** A high-voltage generator has been built to achieve electromagnetic fault injections (see Figure 5). This device is capable of generating up to 18 kV. 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. However, the Electrostatic Discharge (ESD) of the high voltage generates electromagnetic interferences that can influence or damage electronic devices in the proximity. So as to protect all

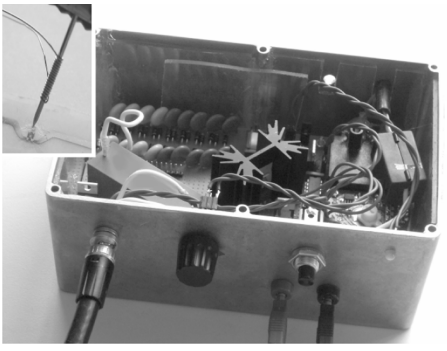

**Fig. 5.** High-voltage generator that produces fast-changing discharges through a probe needle (upper left)

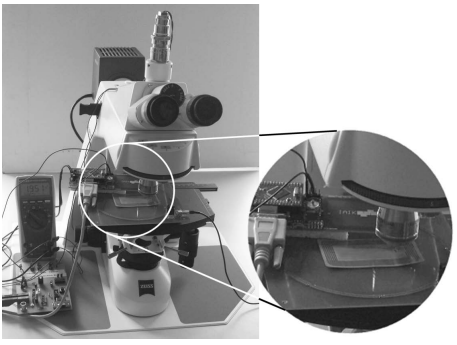

**Fig. 6.** Measurement setup for local fault injections on RFID tags using a microscope to focus the light of a laser diode

involved measurement devices and to produce electromagnetic injections only at a dedicated location, which is the top layer of the RFID tag, we have shielded the circuit using an aluminium case. The case has been connected to the earth ground. The output of the high-voltage generator is connected to a probe coil using a high-voltage shielded cable. As soon as the current flows through the coil, an eddy current is induced into the chip that influences the processing of operations. Electromagnetic fault injections using high-voltage pulses are more dangerous but offer a non-invasive technique as opposed to antenna tearing.

**Optical Inductions.** Like electromagnetic interferences, optical inductions on RFID tags with transparent inlays provide a non-invasive injection technique. We have placed a simple laser diode directly upon the chip surface. The diode emits an optical output power of 100 mW with a wavelength of 785 nm. In fact, the light of the laser diode illuminates the whole chip surface at once. Since RFID chips are typically mounted between a metallic thin-film antenna circuit and the transparent PET layer, no decapsulation procedure has to be performed. In our experiments, not all but a few regions of the chip die have been susceptive to the light beam.

### 5.2 Setup for Local Fault Injections

For local fault injections, we have used an optical microscope. The microscope has an integrated incident illumination device as well as a camera port. Instead of a camera, a laser diode has been used and mounted on top of the port. A collimator lens is used to parallelize the laser beam. Furthermore, the beam is focused using an optical objective which has a magnification of 50 diameters. Using the microscope it is possible to explore the device under attack very accurately. It allows the injection of focused laser beams into specific chip-circuit locations. In addition to that, it is possible to interfere data and control lines as well as memory blocks and driver circuits. Figure 6 shows the measurement setup

for our local fault-injection experiments. The focused laser beam illuminates an RFID tag that lies upon an HF RFID-reader antenna. The tag emulator has also been placed inside the reader field in order to determine the beginning of the response time. The reader and the tag emulator are connected to the PC using a serial interface.

## 6 Results

In our experiments, different kinds of passive tags have been analyzed. Various faults have occurred that are described in the following.

Generally, five fault types have emerged during the injection of faults and are listed in Table 1. Each tag has its own behavior pattern such as the writing time, the duration of writing, and the writing strategy, for example, erasing the memory before writing. There are tags that are more sensitive to certain classes of faults while there exist other tags that are less sensitive. Once the offset and the length of the fault-injection trigger is adjusted accordingly, all examined tags show the same faulty behavior and the same results have been obtained during all our tests. Note that the microchips of the tags are different and are definitely not the same. Two types of faults occurred that are also defined in common RFID-protocol standards. We have denoted these faults by *Unconfirmed Lazy Write* and by *Unconfirmed Successful Write*. *Unconfirmed Lazy Write* indicates an unsuccessful write operation where the tag does not confirm the write-operation request. The value of the tag memory remains untouched. *Unconfirmed Successful Write*, in contrast, represents a successful write operation but the tag does not confirm the operation. Though, the new value is stored into the memory. In case of errors, protocol standards provide a certain waiting time in which tags can send an error response like *insufficient power*.

However, our experiments have shown also other tag behaviors when they are stressed within a write operation. *Unconfirmed Faulty Write* indicates the behavior where the tag does not confirm the reader request but different values are stored into the memory. These values are not random and depend on the trigger delay, the trigger width, the original memory value, the value that has to be written, and the type of fault injection. Another interesting fault that has occurred has been denoted by *Confirmed Lazy Write*. Thereby, the tag did not perform the memory writing but confirms the operation to be successful. At last,

**Table 1.** Overview of the specified fault types and the resulting EEPROM values

| **Fault type** | **EEPROM value** |
|---|---|
| Unconfirmed Lazy Write | old |
| Unconfirmed Successful Write | new |
| Unconfirmed Faulty Write | influenced by adversary |
| Confirmed Lazy Write | old |
| Confirmed Faulty Write | influenced by adversary |

we have observed the case where the tag writes different values to the memory but confirms the operation to be successful. This case is denoted by *Confirmed Faulty Write* and is one of the most critical type of faults.

### 6.1 Global Fault Injections

For all global injection methods, the same results have been obtained. We have induced faults by temporarily antenna tearing, electromagnetic interferences, and optical inductions. By using an automatic sweep, faults have been induced during the response time of a tag as already described in Section 5. Thus, the width as well as the offset of the trigger signal have been varied. First, we discuss the impact of the trigger-width variation. Second, results are given that have been obtained by varying the trigger offset.

The duration of an injected fault is an important factor for an attack. If it is chosen too short, it does not have an impact on the device under attack. If the fault duration is chosen too long, the tag performs a reset due to the absence of power supply and will not answer to reader requests anymore. The time when the tag actually causes a reset due to these induced faults depends on several factors. These factors are, for example, the field strength of the reader device and the distance between the tag and the reader, respectively, or the fault-injection technique (antenna tearing, optical inductions, or electromagnetic interferences). If the distance between the tag and the reader is chosen short, the duration of the fault has to be longer as compared to the scenario where the distance between the tag and the reader is chosen long. In general, the more power is available for the tag, the longer must be the fault-injection duration to cause the chip to fail. However, while the duration of the fault is important for antenna tearing and optical inductions, it is not for electromagnetic injections. The high-voltage generator produces EM pulses which have a fixed pulse width of only a few nanoseconds. Our experiments have shown that even one pulse is sufficient to force a reset of the tag. For antenna tearing, the trigger width constitutes the time in which the tag is not supplied by the field anymore. For optical inductions, the trigger width defines the period of time when the laser diode is illuminating the chip. During our experiments on antenna tearing and optical inductions, we finally have chosen a fault-injection period (trigger width) of about 100 µs which essentially causes the tags to force a reset.

Next, we have varied the trigger offset by starting at the beginning of the response time. Figure 7 shows different types of occurred faults. Depending on the offset value, we observed the occurrence of three different fault types: *Unconfirmed Lazy Write*, *Unconfirmed Faulty Write*, and *Confirmed Successful Write*. In fact, if the offset is chosen small, the reset is performed before the writing of data. Thus, the tag does not send an answer anymore and the content of the memory keeps the same. If the offset is chosen very high, the tag performs a reset after the writing of data. The tag is able to write the new memory content but is disturbed before sending the answer. However, if the offset of the fault trigger is chosen to occur during the writing of data, the content of the memory becomes modified. In addition, varying the offset very slightly leads to different

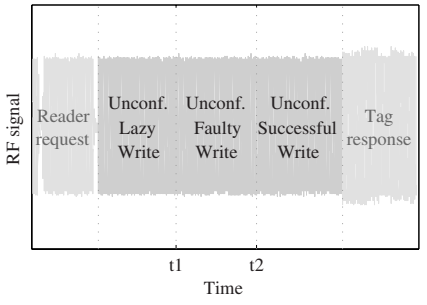


**Fig. 7.** Types of faults occurred at different points in time within the response time

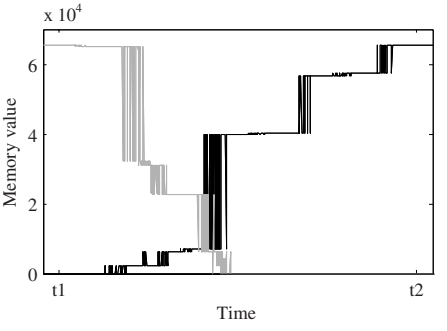


**Fig. 8.** Memory value during *Unconfirmed Faulty Write* after writing two different values (black curve: $0x$FFFF; gray curve: $0x0000$) by varying the delay of the fault injection

memory contents. In Figure 8, the memory values are depicted as a function of the trigger offset. The black curve has been achieved by initializing two bytes of the memory with zero and setting all bits of them to one during an *Unconfirmed Faulty Write* operation. The gray curve describes the same for writing zeros to the memory that was first initialized with ones. It can be observed that the data bits are serially written into the memory and that different bits are flipped at different positions in time. The more time is proceeded the more bits are actually written. In fact, 16 bits are written while the Most-Significant Bit (MSB) makes the highest value step. The Least-Significant Bits (LSB) have only a small impact on the written value and thus cause only small value steps which are not clearly discernable in the given figure. Nevertheless, note that we have influenced the bits not sequentially (i.e. from the LSB to the MSB) but we have rather influenced specific bits at specific points in time.

With the help of an automatic sweep, we are able to detect the writing of data into the memory within a few minutes. It is possible to determine the time when the writing of data starts and how long it takes. It is further possible to detect if the memory content is cleared before the real writing of data. This allows fingerprinting of tags by identifying device-specific patterns for operations like writing to the memory.

While the same results have been obtained for all three injection methods, optical inductions have led us to further interesting findings. Besides *Unconfirmed Faulty Write* faults, we have been able to produce *Confirmed Lazy Write* and even *Confirmed Faulty Write* faults. This has been achieved by accurately adjusting the trigger width of the fault to a limit where the tag has barely enough power to confirm the write operation but it is not able to write the exact value. The tag either keeps the old value or it stores a different one. However, by choosing the right trigger width and by varying the trigger delay we have been able to roughly influence the modification of individual bits that have to

be written. Following these facts, it appears that this allows the modification of memory content at several points in time during one tag operation. Hence, it is possible to bypass common security features which make use of backup facilities or memory-shading techniques. It is further possible to skip the increasing or decreasing of counter values. Counters are commonly used in cashing applications or they are used to limit the number of authentication steps to avoid differential side-channel attacks.

As a simple countermeasure against these attacks, a comparison of the value that has to be written and the actually written value becomes reasonable. However, if the register that stores the new value is modified by faults before the writing into non-volatile memory, a comparison does not help to detect the failure, obviously. This article focuses only on the modification of writing into the non-volatile memory and does not analyze the susceptibility of faults on register-values. This point keeps unclear at this stage but is marked for future work.

### 6.2 Local Fault Injections

Next, we focus on local fault injections using an optical laser beam. In fact, the injection of local faults offers more control for an adversary. Depending on the position of the light beam, different components of the integrated circuit are affected. The occurred faults range from simple resets to definite modifications of tag memory contents. We have been able to generate all kinds of faults that have been described in the section above.

By increasing the power of the light or by broadening the beam of the laser, simple resets have been enforced. As soon as the laser beam has been focused on the memory control logic, various faults are initiated such as they have been obtained by global fault injections. All in all, for local fault injections the timing of faults is not that relevant as the issue of fault-injection location. Once the laser beam has been focused to a specific position, injecting faults is rather easy. The fault type *Confirmed Faulty Write* has been achieved without accurately adjusting the illumination time to a certain period. However, this convenience is compensated by higher costs for the equipment.

## 7 Summary of the Results

In Table 2, a summary of the occurred fault types and their fault-reproducibility rate is given for different fault-injection techniques. For the antenna tearing, which has a global fault-injection scope, *Unconfirmed Lazy Write*, *Unconfirmed Successful Write*, and also *Unconfirmed Faulty Write* types have been obtained. All faults occurred with a reproducibility rate of more than 95 %. Note that especially in UHF measurements the distance between the tag and the reader antenna constitutes an important factor for a successful attack. If the tag is placed very close to the reader antenna, the tag-antenna de-tuning becomes ineffective due to parasitic inductions that inhibit further power losses on the tag side. The reproducibility of electromagnetic interferences, in contrast, is rather

**Table 2.** Summary of the occurred fault types and their fault-reproducibility rate

| | **Antenna tearing** | **Electromagnetic interferences** | **Optical inductions** | |
|---|---|---|---|---|
| **Fault type** | *global* | *global* | *global* | *local*[1] |
| Unconfirmed Lazy Write | $> 95\,\%$ | $< 10\,\%$ | $> 95\,\%$ | $> 95\,\%$ |
| Unconfirmed Successful Write | $> 95\,\%$ | $< 10\,\%$ | $> 95\,\%$ | $> 95\,\%$ |
| Unconfirmed Faulty Write | $> 95\,\%$ | $< 10\,\%$ | $> 95\,\%$ | $> 95\,\%$ |
| Confirmed Lazy Write | — | — | $> 90\,\%$ | $> 95\,\%$ |
| Confirmed Faulty Write | — | — | $> 90\,\%$ | $> 95\,\%$ |

low ($< 10\,\%$) for our experiments. This has its reason in the imprecise timing of our EM fault-injection setup. Nevertheless, we have obtained the same fault types as obtained by antenna tearing.

For optical inductions, we have to distinguish between global as well as local fault injections. Both fault-injection techniques led to all types of faults. However, the laser beam has to be adjusted accordingly before the attacks. After the adjustment, each kind of fault type is reproducible with high probability ($> 90\,\%$) depending on the time and duration of the fault injection.

## 8 Conclusions

This article presents fundamental observations about the vulnerability of commonly-used passive RFID tags. It is the first work that provides concrete results of practical experiments in the context of fault analysis on RFID devices. We have demonstrated global as well as local fault-injection methods on HF and UHF tags. Global fault-induction methods affect the whole chip at once, local-fault induction methods apply only to dedicated parts of the chip. Beside temporarily antenna tearing, we have analyzed the impact of electromagnetic interferences as well as optical inductions. In particular, optical inductions pointed out to be a very convenient fault-injection method because of its non-invasive and effective manner. The main intention of this article is to investigate the susceptibility of faults on RFID devices and to identify potential weaknesses. Thus, we have only examined tags that do not include any countermeasures against fault-analysis attacks at this stage. Instead, we have focused on write operations which are considered critical in respect of power consumption and execution time. We have shown that fault-injection methods allow the prevention of writing data into the tag memory and, even worse, to allow the writing of faulty values. In both scenarios, the tag confirms the write operation to be successful. Hence, countermeasures have to be integrated that have to contend with limited resources as well as limited power supply and their price has to be

[1] For local optical inductions, the focus and position of the laser beam has to be adjusted accordingly to achieve high reproducibility.

competitive for a large deployment. This article demonstrates potential weaknesses of RFID tags to faults and provides a basis for future work like analysis of the susceptibility of cryptographic-enabled RFID tags to faults. We conclude that countermeasures against fault analysis have to be considered especially in applications where security is of increasing interest.

## Acknowledgements

We would like to thank Kerstin Lemke-Rust for improving the editorial quality of this article. This work has been funded by the European Commission under the Sixth Framework Programme (Project BRIDGE, Contract Number IST-FP6-033546), by the Secure Business Austria (SBA) research center, and by the Austrian Science Found (FWF) under the grant number P18321.

## References

1. Anderson, R.J., Kuhn, M.G.: Tamper Resistance - a Cautionary Note. In: Second Usenix Workshop on Electronic Commerce, pp. 1–11 (November 1996)
2. Atmel Corporation. Website atmel.com - Secure RFID: CryptoRF, `http://www.atmel.com/products/SecureRF`
3. Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C.: The Sorcerer's Apprentice Guide to Fault Attacks. Cryptology ePrint Archive Report 2004/100 (2004), `http://eprint.iacr.org/`
4. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-Key Cryptography for RFID-Tags. In: Workshop on RFID Security 2006 (RFIDSec 2006), Graz, Austria, July 12-14 (2006)
5. Blitshteyn, M.: Mastering RFID Label Converting: Where Understanding Static Control Can Help Prevent RFID Transponder Failures. Technical report, Ion Industrial (2005)
6. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurinand, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, Springer, Heidelberg (2007)
7. Canniére, C.D., Preneel, B.: TRIVIUM Specifications. eSTREAM, ECRYPT Stream Cipher Project Report 2005/030 (April 2005), `http://www.ecrypt.eu.org/stream`
8. Carluccio, D., Lemke, K., Paar, C.: Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. In: Oswald, E. (ed.) Workshop on RFID and Lightweight Crypto (RFIDSec 2005), Graz, Austria, July 13-15 (2005)
9. Feldhofer, M.: Comparing the Stream Ciphers Trivium and Grain for their Feasibility on RFID Tags. In: Posch, K.C., Wolkerstorfer, J. (eds.) Proceedings of Austrochip 2007, Graz, Austria, October 11, 2007, pp. 69–75. Verlag der Technischen Universität Graz (2007) ISBN 978-3-902465-87-0
10. 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)

11. God, R.: Lean Manufacturing of RFID Products - Put the Chip on the Box. In: Electronics Systeminteg ration Technology Conference, Proceedings of IEEE Conference, September 2006, pp. 1118–1121. IEEE Computer Society, Los Alamitos (2006)
12. Hell, M., Johansson, T., Meier, W.: Grain - A Stream Cipher for Constrained Environments. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/010 (revised version 2005) (2006), http://www.ecrypt.eu.org/stream
13. 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)
14. 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)
15. 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)
16. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
17. Kömmerling, O., Kuhn, M.G.: Design Principles for Tamper-Resistant Smartcard Processors. In: USENIX Workshop on Smartcard Technology (Smartcard 1999), pp. 9–20 (May 1999)
18. McLoone, M., Robshaw, M.J.B.: Public Key Cryptography and RFID Tags. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, pp. 372–384. Springer, Heidelberg (2007)
19. NXP Austria GmbH. Website mifare.net - contactless smart cards, http://www.mifare.net
20. Oren, Y., Shamir, A.: Remote Password Extraction from RFID Tags. IEEE Transactions on Computers 56(9), 1292–1296 (2007)
21. Plos, T.: Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In: Malkin, T. (ed.) Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008, San Francisco, CA, USA, April 8-11, 2008. LNCS, vol. 4964, pp. 288–300. Springer, Heidelberg (2008)
22. Poschmann, A., Leander, G., Schramm, K., Paar, C.: A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications. In: Workshop on RFID Security 2006 (RFIDSec 2006), Graz, Austria, July 12-14 (2006)
23. Poupard, G., Stern, J.: Security Analysis of a Practical "on the fly" Authentication and Signature Generation. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 422–436. Springer, Heidelberg (1998)
24. Quisquater, J.-J., Samyde, D.: Eddy Current for Magnetic Analysis with Active Sensor. In: Proceedings of Esmart, pp. 185–194 (2002)
25. Schmidt, J.-M., Hutter, M.: Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results. In: Posch, K.C., Wolkerstorfer, J. (eds.) Proceedings of the Austrochip 2007, October 2007, pp. 61–67. Verlag der Technischen Universität Graz (2007) ISBN 978-3-902465-87-0
26. SecureRF. SecureRF - Secure RFID Solutions, http://www.securerf.com
27. Skorobogatov, S.P., Anderson, R.J.: Optical Fault Induction Attacks. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 2–12. Springer, Heidelberg (2003)

28. Standaert, F.-X., Piret, G., Gershenfeld, N., Quisquater, J.-J.: SEA: a Scalable Encryption Algorithm for Small Embedded Applications. In: Domingo-Ferrer, J., Posegga, J., Schreckling, D. (eds.) CARDIS 2006. LNCS, vol. 3928, pp. 222–236. Springer, Heidelberg (2006)
29. Tan, K., Tan, S., Ong, S.: Functional failure analysis on analog device by optical beam induced current technique. In: Proceedings of the 1997 6th International Symposium on Physical & Failure Analysis of Integrated Circuits, 1997, pp. 296–301. IEEExplore (July 1997)
30. Tuyls, P., Batina, L.: RFID-Tags for Anti-counterfeiting. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, Heidelberg (2006)