Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation*

Timo Kasper, David Oswald, and Christof Paar

Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
timo.kasper@rub.de, david.oswald@rub.de, christof.paar@rub.de

Abstract. As most modern cryptographic Radio Frequency Identification (RFID) devices are based on ciphers that are secure from a purely theoretical point of view, e.g., (Triple-)DES or AES, adversaries have been adopting new methods to extract secret information and cryptographic keys from contactless smartcards: Side-Channel Analysis (SCA) targets the physical implementation of a cipher and allows to recover secret keys by exploiting a side-channel, for instance, the electro-magnetic (EM) emanation of an Integrated Circuit (IC). In this paper we present an analog demodulator specifically designed for refining the SCA of contactless smartcards. The customized analogue hardware increases the quality of EM measurements, facilitates the processing of the side-channel leakage and can serve as a plug-in component to enhance any existing SCA laboratory. Employing it to obtain power profiles of several real-world cryptographic RFIDs, we demonstrate the effectiveness of our measurement setup and evaluate the improvement of our new analog technique compared to previously proposed approaches. Using the example of the popular Mifare DESFire MF3ICD40 contactless smartcard, we show that commercial RFID devices are susceptible to the proposed SCA methods. The security analyses presented in this paper do not require expensive equipment and demonstrate that SCA poses a severe threat to many real-world systems. This novel attack vector has to be taken into account when employing contactless smartcards in security-sensitive applications, e.g., for wireless payment or identification.

Keywords: contactless smartcards, side-channel analyis, implementation attacks, hardware security, DESFire MF3ICD40

1 Introduction

Contactless smartcards based on RFID technology have become the basis of numerous large-scale, security-relevant applications, including amongst others public transport, wireless payment, access control, and digital identification [36].

* The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

According to NXP, the vendor of the Mifare product line, more than 1 billion Mifare smartcard ICs have been sold [27]. Due to the sensitivity of the stored and transmitted data (e.g., personal information, cash balance, etc.) and the fact that accessing the wireless interface is virtually impossible to control, most RFIDs devices today comprise cryptographic mechanisms, for example to perform a mututal authentication or to encrypt the data sent over the air interface.

As a consequence of the attacks on Mifare Classic following the reverse-engineering of the proprietary cipher Crypto1 [23, 11], many operators of RFID systems have migrated to contactless smartcards based on modern cryptographic primitives, such as (Triple-)DES or AES. As these ciphers are secure from a mathematical point of view and efficient theoretical attacks are currently unknown, the threat scenario is changing:

Instead of performing cryptanalytical attacks on an algorithmic level which are infeasible for modern ciphers, an adversary targets the physical hard- or software implementation. The class of *implementation attacks* includes both passive monitoring of the device during the cryptographic operation via some *side-channel*, and the active manipulation of the target by injecting permanent or transient *faults*. In this paper we focus on *non-invasive*, *passive* SCA exploiting the EM emanation of contactless smartcards while they execute a cryptographic primitive. This class of attacks poses a severe threat to many real-world RFID systems, as SCA may enable an adversary to extract, for instance, the secret key of a Triple-DES (3DES) or AES operation within a few hours of measurement and analysis, whereas an exhaustive search is infeasible with the currently available computational resources.

1.1 Related Work

The concept of SCA was first proposed in [20] in 1998, and the field has since then been an area of extensive research. Notable contributions include the analysis of EM leakage instead of the current consumption [2] and the method of Correlation Power Analysis (CPA) that employs the (linear) correlation coefficient during the evaluation phase to better model the behaviour of real ICs [5]. Apart from that, there is a wide variety of literature both on attack techniques and possible countermeasures — a summary can for instance be found in [22].

For SCA of RFID devices, less research has been conducted, especially with respect to attacks on real-world devices. In [28], a successful side-channel attack against a simple password-based authentication mechanism of an Ultra-High Frequency (UHF) RFID is demonstrated. Precisely monitoring the EM field during the response of the device, the authors are able to predict the password bits. However, due to the different operating principle ("backscatter") of UHF devices, the results cannot be immediately applied to contactless smartcards, which usually follow the ISO 14443 standard [13, 14] employing magnetic coupling at a frequency of 13.56 MHz.

The authors of [12, 31] describe several SCA attacks against a self-made implementation of the AES running on an actively powered microcontroller (μC)-based prototype RFID. As all analyses are performed in a white-box setting,

i.e., with full knowledge and control of the implementation details and in the absence of countermeasures, the results do not imply a direct threat to real-world systems.

At WISA 2009, a key recovery on a commercial contactless smartcard featuring 3DES authentication and encryption was presented [17]. Working in a black-box scenario, the authors were able to profile the device, locate the encryption operation, and mount a successful non-invasive CPA on the 3DES engine. The leakage model for contactless smartcards introduced in this work forms the basis for our analysis and is outlined in Sect. 2. The authors also report that a special analog circuit (subtracting the signal of the oscillator of their reader to dampen the carrier and increase the side-channel amplitude) improves the results of their CPA, however, do not explicitly quantify the actual effect of this approach.

1.2 Contribution of this Paper

As a main contribution, we propose a novel method for isolating and amplifying the SCA leakage of cryptographic RFIDs by means of an analog demodulation circuit. We verify the validity of the leakage model introduced in [17] for real-world products by performing an analyis of the Mifare DESFire MF3ICD40 contactless smartcard. In doing so, we estimate the effectiveness of the developed circuitry by comparing the proposed analog technique to methods that are solely based on digital signal processing.

The remainder of this paper is structured as follows: in Sect. 2, we briefly summarize the leakage model put forward in [17] and explain the differences between several demodulation approaches in the context of SCA. In Sect. 3, the developed measurement environment is presented, with a focus on the special analog circuitry for extracting side-channel information. The efficiency of the setup is then practically demonstrated by analyzing the DESFire MF3ICD40 smartcard and providing power profiles of several other real-world devices in Sect. 4. Finally, we conclude in Sect. 5, suggesting aspects for future research and outlining open problems.

2 SCA of Contactless Smartcards

In contrast to their contact-based counterpart, the electrical energy for contactless smartcards is supplied wirelessly using magnetic coupling. This results in a leakage model for contactless smartcards as proposed in [17]: the side-channel signal causes an amplitude modulation of the 13.56 MHz field generated by the reader, i.e., it relates to the same physical principle as used for the data transmission from card to reader, termed *load modulation*[1]. In the time domain, an amplitude-modulated signal $s(t)$ may be written as

$$s(t) = (P_{const} + p(t)) \cdot \cos(\omega_{reader} \cdot t)$$

[1] Load modulation causes significantly stronger changes of the EM field compared to the side channel leakage

where $\omega_{reader} = 2\pi\ f_{reader}$, $f_{reader} = 13.56\,\text{MHz}$ denotes the carrier frequency, P_{const} the constant part of the power consumption and $p(t)$ the variation due to the internal operation of a smartcard, e.g., caused by different intermediate values being processed during a cryptographic operation. Note that usually $|p(t)| << P_{const}$, and hence the isolation and amplification of the modulating signal $p(t)$ is a key factor for a successful SCA. The amplitude of the strong field of the reader is several orders of magnitude greater than the side-channel leakage. When digitizing $s(t)$ the input range of the analog-to-digital conversion has to be set large enough to capture the full signal, resulting in a decreased accuracy of the measurements with respect to $p(t)$. In order to maximize the vertical resolution of the measurements and capture all relevant information it is hence beneficial to isolate the side-channel information *before* the digitizing step, so that the input range can be set corresponding to $p(t)$ and the accuracy of the measurements is maximized.

Basically, the problem of extracting the weak signal $p(t)$ from $s(t)$ is equivalent to that of amplitude demodulation, about which extensive research has been carried out in the context of "classical" electronic communication, cf. for instance [32]. In this paper, we focus on the principle of *incoherent* demodulation, which has the advantage that the unmodulated carrier signal is not further required.

Instead, by *rectifying* (i.e., taking the absolute value) of an amplitude-modulated signal and filtering the result, the modulating side-channel information $p(t)$ can directly be retreived.

The rectification may either be achieved by processing the *full wave* to obtain $|s(t)|$ or following the *half wave* approach, i.e., discarding the negative part of $s(t)$[2]. The latter approach is often used in practice, as it can be realized with one diode, whereas full-wave rectification requires more complex circuits. In terms of the achievable bandwidth for receiving the modulating signal $p(t)$, full-wave rectification allows a maximum bandwidth of $B_{full} = f_{reader}$, whereas the half-wave method limits it to $B_{half} = \frac{f_{reader}}{2}$, for details cf. [32].

3 Measurement Setup

In this section, we present the developed measurement environment for the SCA of contactless smartcards. Fig. 1 gives an overview of the components of our setup and their interconnection. An antenna coil establishes the coupling between the contactless smartcard and an RFID reader. The latter supplies the contactless smartcard (from now on occasionally referred to as Device Under Test (DUT)) with power and sends commands by turning the EM field off for a specific amount of time. The DUT transmits its response using load modulation, i.e., it modulates the amplitude of the reader field by increasing its power consumption.

The utilized reader is a custom, freely programmable device based on the design proposed in [16]. This reader allows for sending arbitrary commands to

[2] The remaining half period of the sine-shaped signal can be mathematically expressed as $\frac{1}{2}\ (s(t) + |s(t)|)$

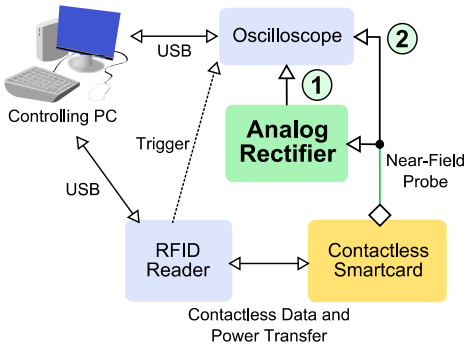


Fig. 1: Overview of measurement environment

an ISO 14443-compliant RFID and can thus be used to implement the protocols of most contactless smartcards in use today. Besides, communication according to ISO 15693 [15] is supported, however, we are not aware of any commercially available RFID complying to this standard that comprises cryptography.

For the purpose of SCA, the 13.56 MHz EM field is captured with a magnetic near-field probe manufactured by Langer EMV [21]. The resulting "raw signal" is on the one hand directly recorded by a Picoscope 5204 Digital Storage Oscilloscope (DSO) [29]. On the other hand, the same signal is further processed using the analog demodulator and filter presented in Sect. 3.2 before being captured by the second input channel of the oscilloscope. The RFID reader generates a trigger event to start a measurement when the last bit of a command has been sent to the DUT.

The overall control of the measurement process presented in Sect. 3.1 is performed by a central standard PC, which is connected to the RFID reader and the oscilloscope via a USB link. The PC prepares the commands to be sent to the DUT, transmits them to the RFID reader and initiates the acquistion of side-channel measurements. The resulting waveforms (from now on referred to as *traces*) captured by the oscilloscope are stored on the harddrive along with additional information, e.g., the input and/or output of a cryptographic operation performed by a contactless smartcard.

3.1 Measurement Process

We implemented the authentication protocols of a wide range of contactless smartcards, including Mifare Classic, Mifare DESFire MF3ICD40, Mifare DESFire EV1, Mifare Ultralight C, and the Basic Access Control (BAC) of the German electronic passport. All these protocols involve the execution of one or several cryptographic operations on the DUT, for which we can either control the input or obtain the output an unlimited number of times.

A side-channel trace is acquired as follows: First, the DUT is reset by switching off the field of the reader for a device-specific duration. Then, all initializa-

tions according to ISO 14443 are performed, and finally, a cryptographic operation is started by sending the appropriate command. The input data (challenge) for this operation is stored in a file so that it can be used to predict intermediate values in the analysis phase. While the device is executing this operation, side-channel traces are recorded simultaneously both for the raw field of the reader (i.e., without analog preprocessing) and for the processed signal (i.e., demodulated using the analog rectifier and filter). In case the DUT returns a relevant response (e.g., the result of an encryption), this value is also stored along with the trace. For all experiments presented in this paper, we use a sample rate of 500 MHz for digitizing the signals, which turns out to be sufficient considering the band-limiting operations performed by the analog and digital processing. This process is repeated several thousand times, depending on the characteristics of the DUT and the target for the SCA[3].

3.2 Analog Processing

According to the assumed leakage model for contactless smartcards explained in Sect. 2, the power consumption of the smartcard causes a (very weak) amplitude modulation of the field generated by the RFID reader. Hence, demodulation of this signal and isolating it from the strong carrier field of the reader can reveal the side-channel leakage and enable further analysis, e.g., key recovery by means of Simple Power Analysis (SPA) or CPA. In [17] the amplitude of the modulating signal is increased by subtracting the known, constant reader signal using analog circuity. The actual demodulation is then performed digitally during the analysis phase. In this paper we implement a new different method by realizing the complete demodulation process with analog components, which allows to isolate and *directly* obtain the power consumption signal of an RFID smartcard.

For this purpose, we designed a custom Printed Circuit Board (PCB) comprising circuitry for amplification, rectification, and filtering of the raw analog signal. The complete schematics are given in Appendix A. The signal acquired by the EM probe is first amplified using an AD8058 Operational Amplifier (opamp) [4] and then rectified by a BAT48 Schottky diode [35]. The result is filtered using an active low-pass filter[4] with a -3 dB frequency of 6.25 MHz. The output stage is designed to drive a standard 50 Ω load, e.g., connected via a suitable coaxial cable.

In our practical experiments, it turned out that the filtering and amplification performed on the demodulation board can be further improved: the carrier signal was not suppressed as strong as desired and a slight drift of the DC component of the signal occurred during long-term measurements (e.g., due to temperature variations). Thus, we extended the demodulator with a bandpass filter circuit that further reduces the amplitude of the 13.56 MHz signal and besides provides

[3] For example, it turns out that a transfer on the internal data bus of a smartcard results in stronger leakage than a register update within an encryption, and hence, SCA of the latter requires significantly more traces

[4] The filter is built with a Sallen-Key topology using an AD8045 opamp [3]

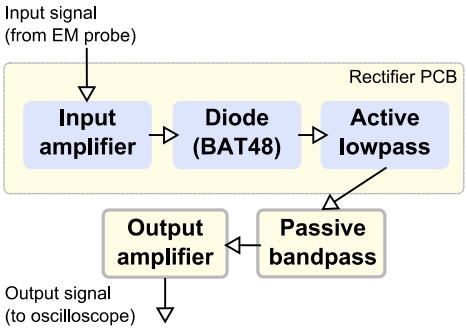


Fig. 2: Structure of the analog demodulation circuitry

a highpass characteristic to remove the DC shift. This second-order filter is built using passive components only (i.e., inductors and capacitors) and has a passband between 100 kHz and 7 MHz. Finally, the filter output is amplified to utilize the full input range of ± 100 mV of the oscilloscope. The overall structure of the demodulation system, used for the analyses presented in Sect. 4, is depicted in Fig. 2. To minimize the complexity of the board we implemented a half-wave rectification, i.e., discard the negative part of the signal. As explained in Sect. 2, this approach limits the bandwidth of the receivable signal to $\frac{13.56}{2}$ MHz.

3.3 Digital Processing

As mentioned in Sect. 3.1, side-channel traces (of the same operation) are acquired both before (raw trace, ② in Fig. 1) and after the demodulation circuitry (① in Fig. 1). For analysing the improvement provided by the analog hardware, the demodulation process thus has to be reproduced in the digital domain. For that purpose, we developed respective functions that perform half- or full-wave rectification and the necessary filtering of the raw traces. Besides, additional filtering in the evaluation phase may also be beneficial for the output of the analog demodulator, for instance, to further suppress the 13.56 MHz signal with a digital Finite Impulse Response (FIR) filter. The concrete effects of the digital processing techniques are practically evaluated in Sect. 4.1.

4 Practical Results

In this section, we demonstrate the effectiveness of our approach by analysing the side-channel leakage of several commercial contactless smartcards. As our main example we use the Mifare DESFire MF3ICD40, an ISO 14443-compliant smartcard. We briefly present the power profile of this smartcard and then compare our analog and digital processing techniques by quantifying their impact on real-world measurements. Subsequently, we perform several attacks on the 3DES encryption of the Mifare DESFire MF3ICD40 and show that the success rate of

the SCA can be improved using the developed analog demodulator. Finally, we consider other contactless smartcards, including the German electronic passport and the new DESFire EV1, and present side-channel traces of these devices.

4.1 Example: Mifare DESFire MF3ICD40

Mifare DESFire MF3ICD40 [24] contactless cards feature an implementation of 3DES that can be used both for establishing a mutual authentication between the smartcard and a reader and to ensure the confidentiality of the information exchanged over the wireless interface. In our experiments, the device turned out to be susceptible to SCA, and hence, we utilize it as an example to demonstrate and evaluate the capabilities of our measurement setup. Note that all results given in this section refer to the DESFire MF3ICD40 and do not apply to the newer AES-based variant DESFire EV1.

Profiling When performing an SCA in a black-box scenario (i.e., when no information about the internals of the DUT is available), the first step is usually a profiling phase during which one attempts to map different parts of the power trace to steps of the operation of the DUT (e.g., a data transfer or an encryption operation). We target the step in the DESFire authentication protocol (for details on the protocol, cf. [19, 9]) during which the reader sends its response (denoted as B_2) to the challenge of the card transmits its own challenge (B_1). To verify the response of the reader and compute its own response, the smartcard encrypts both B_1 and B_2 using 3DES with its secret symmetric key k_C, as shown in Fig. 3.

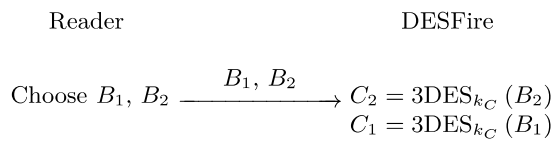


Fig. 3: Excerpt of the Mifare DESFire authentication protocol relevant for SCA

Figure 4 shows the power trace during this operation. The depicted waveform is the result of the analog demodulation (using the hardware proposed in Sect. 3.2) and digital filtering (using an FIR bandpass filter from 50 kHz to 8 MHz, as described in Sect. 3.3).

We performed a CPA on the plain- and ciphertext of both encryption operations using an 8-Bit hamming weight model. Note that during the profiling stage, we are able to set the secret key k_C of the card, and can thus predict intermediate values that are not directly output by the DUT, e.g., the resulting ciphertexts C_1 and C_2 of the encryption of B_1 and B_2. As suggested by the findings of [18], we were able to obtain a significant correlation result at the

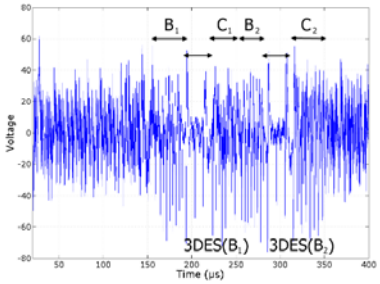
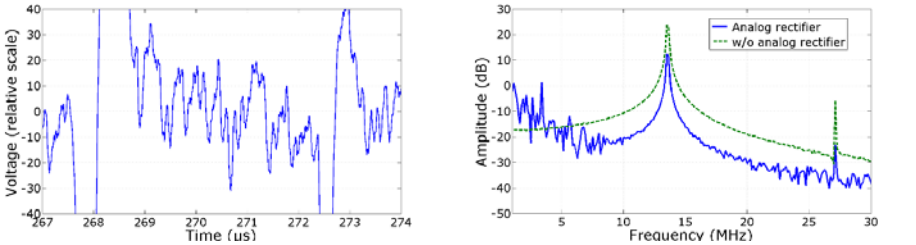


Fig. 4: Power profile of the Mifare DESFire MF3ICD40 (after analog processing)

correct points in time[5] using less than 1000 traces (this result is further detailed in Sect. 4.1).



(a) Power profile in the time domain

(b) Spectrum before (dashed) and after (solid) analog processing

Fig. 5: DES encryption on the Mifare DESFire MF3ICD40

The part of the power trace that belongs to the actual 3DES encryption, which is presumably performed by a dedicated (and protected) hardware engine on the DUT, is illustrated in Fig. 5a. In order to optimize the evaluation, we set up our environment to yield maximum amplitude for this part, and again digitally band-limited the trace with an FIR bandpass from 50 kHz to 8 MHz.

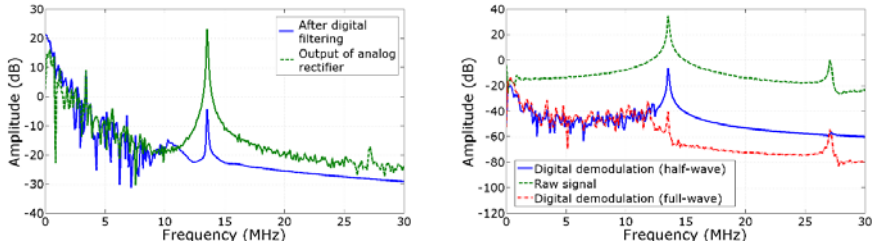
Influence of Analog Processing To estimate the increase of the amplitude of the side-channel signal due to the analog demodulator, we focus on the part of the power trace belonging to the encryption operation and compare the power spectrum[6] before and after the analog processing.

[5] i.e., for which eight subsequent peaks are visible in the power profile

[6] i.e., the squared magnitude $|DFT(s(k))|^2$ of the Discrete Fourier Transform (DFT) [33] of a signal $s(k)$

Figure 5b compares the respective spectra (with the y-axis logarithmically scaled) for frequencies from 0 MHz to 30 MHz. For the unprocessed traces, no clear side-channel signal can be identified in the frequency domain. In contrast, the result of the analog demodulation clearly shows the spectrum of the side-channel information between 0 MHz and approx. 7 MHz.

Influence of Digital Processing As mentioned in Sect. 3.3, further digital processing of the acquired signals is mandatory for signals recorded without analog processing to perform the demodulation. For traces already demodulated using the proposed analog rectifier, additional digital filtering is not required — however, it can help to further improve the results of subsequent analyses. To illustrate the effect of the digital processing, Fig. 6a compares the power spectra for the filtered (blue, solid) and unfiltered (green, dashed) output of the analog demodulator. The raw signal (green, dashed) without analog filtering and its digitally demodulated variants using half-wave (blue, solid) and full-wave (red, dashed-dotted) rectification are depicted in Fig. 6b.

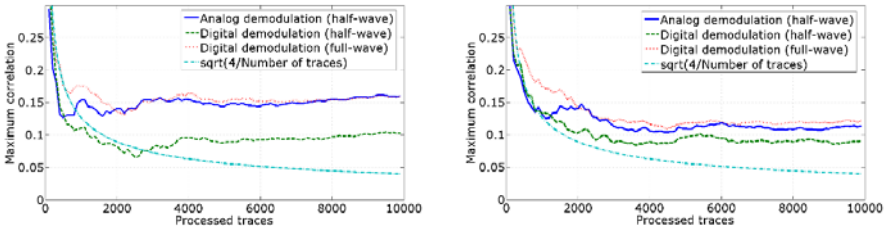


(a) Output of analog rectifier (b) Raw signal before analog rectifier

Fig. 6: Power spectrum during DES encryption, before (dashed) and after (solid and dashed-dotted) digital processing

SCA Results In this section, we move forward and evaluate the effect of our proposed signal processing techniques in terms of CPA results. To this end, we compare the magnitude of correlation coefficients for the analog and the digital demodulation approaches. We target the transfers on the databus of the DUT during the profiling, as detailed in Sect. 4.1. Furthermore, some CPA-relevant results of the actual hardware encryption engine are provided.

As mentioned in Sect. 4.1, a significant correlation for the bytes of the plaintext of the encryption operation can already be obtained from a small number of traces. We thus recorded 10,000 measurements and computed the correlation coefficients after (a) analog demodulation using half-wave rectification, (b) digital demodulation using half-wave rectification, and (c) digital demodulation using full-wave rectification.



(a) Byte 5 (b) Byte 7

Fig. 7: Maximum correlation coefficient for plaintext bytes (Hamming weight) for (1) analog (blue, solid) and digital demodulation using (2) half-wave (green, dashed) and (3) full-wave rectification (red, dotted)

The maximum value of the correlation coefficient over the number of processed traces is shown in Fig. 7 exemplarily for the fifth and the seventh byte of the plaintext B_2. To provide a measure for the significance of the correlation values, we also included the expected "noise level" of $4/\sqrt{\text{No. of traces}}$ in the diagrams (turquoise, dashed-dotted). The analog rectifier yields correlation results that are clearly distinguishable from noise after approx. 900 traces. In contrast, the digital (half-wave) equivalent of our analog processing circuit exhibits an inferior performance and displays a lower overall value for the correlation, i.e., cannot exploit the full side-channel leakage present in the measured signals. Comparing these cases using the same demodulation principle, i.e., (1) and (2) in Fig. 7, the developed analog circuitry clearly outperforms the standard digital approach. For reference, curve (3) in Fig. 7 further illustrates the results obtained for a digital full-wave rectifier, yielding almost equivalent correlation results compared to the half-wave analog rectifier, which indicates that realizing an analog full-wave rectifier is promising to further improve the efficiency of the measurement setup.

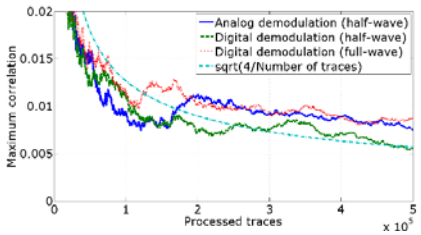


Fig. 8: Maximum correlation coefficient (8-bit Hamming distance $R_0 \rightarrow R_1$) for (a) analog (blue, solid) and digital demodulation using (b) half-wave (green, dashed) and (c) full-wave rectification (red, dotted)

Focusing on the actual encryption process, beginning at approx. 270 μs when the last byte of B_2 has been sent, one can correlate on an intermediate value of the cipher, for instance, the output of the first round of the first DES iteration[7]. Figure 8 shows the maximum correlation coefficient for the Hamming distance between the lower 8 bit of the DES state register R before and after the first round [1]: the correlation after the analog rectification converges to a value of approx. 0.09 after 160,000 traces, while for the digital counterpart after more than 250,000 traces the correlation coefficient is just marginally distinguishable from the noise floor. Note that this analysis targets the internal cryptographic hardware and hence, as expected [22], requires more traces to detect the side-channel leakage, compared to the data bus.

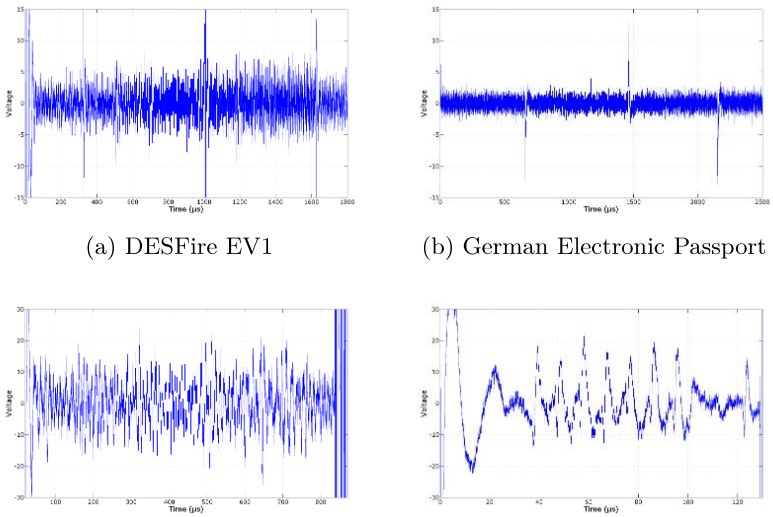
4.2 Power Profiles of Different Contactless Smartcards

In order to further illustrate the capabilities of our setup and to show the general validity of the RFID leakage model used throughout this paper, we analyzed several other contactless smartcards. The selection primarily focuses on modern high-security ICs (including the new DESFire EV1 and the German electronic passport), but also comprises devices for low-cost applications, i.e., Mifare Classic and Ultralight C. Note that the results presented in this paper are not specific to RFIDs devices manufactured by NXP — in fact, we were able to reproduce similar results with products made by other vendors, but cannot disclose the results for legal reasons. In this section, we do not perform a detailed analysis of the considered DUTs as done for Mifare DESFire MF3ICD40 in Sect. 4.1, but summarize the characteristics of the respective smartcards and provide some observations made during our experiments.

Figure 9 depicts exemplary power profiles of each DUTs in this section, recorded with the analog demodulator during a particular cryptographic operation. The following paragraphs introduce the devices and give a short description of the cryptographic operations for which the side-channel traces were obtained. We highlight some particular features evident in the power profiles and try to relate them to the internal operation of the DUT.

Mifare DESFire EV1 Mifare DESFire EV1 [26] is the successor of Mifare DESFire MF3ICD40 and was announced in 2006. Apart from authentication and encryption with 3DES, the smartcard also provides support for AES with a 128-bit key. The device is certified according to Common Criteria EAL-4+ [7] and implements special hardware countermeasures against SCA, which are, however, not further characterized in the publicly available datasheets. The authentication protocol of the DESFire EV1 is similar to that of the DESFire MF3ICD40 and was disclosed in [19]. The power profile in Fig. 9a has been recorded during the second step of the protocol which involves two AES encryptions. The noticeable peaks in the signal arise from significant shifts in the DC component that might be caused by a countermeasure involving a switching of the internal power

[7] Knowing the key we can compute all intermediate values within the DES



(a) DESFire EV1 (b) German Electronic Passport

(c) Ultralight C (d) Mifare Classic

Fig. 9: Power profiles of various contactless smartcards

supply of the DUT [30]. Another interesting feature is the increase in the signal amplitude from 500 μs to 1600 μs, which might result from the AES encryption.

German Electronic Passport The German electronic passport [6] is based on a high-security contactless smartcard either manufactured by Infineon or NXP. It comprises several levels of security and is protected by different authentication mechanisms. We implemented the BAC protocol [8] which ensures that the device can only be read with the approval of the owner by performing a 3DES-based mutual authentication based on a key derived from information printed inside the passport. SCA of the protocol itself would not provide a significant gain for an adversary (as the key is printed inside the document), however, it provides a starting point for the analysis of the DUT and allows to trigger a 3DES operation on the smartcard. As for the DESFire EV1, distinct offsets of the DC component can be observed, that again might stem from some protection mechanism.

Mifare Ultralight C This contactless smartcard was introduced by NXP in 2009 [25] and targets cost-sensitive segments, e.g., paper tickets for public transport systems. Its cryptographic capabilities are limited, and the device only offers an authentication mechanism with 3DES (but no data encryption). Initially, we assumed that the DUT is based on a similar architecture as the Mifare DESFire MF3ICD40 analyzed in Sect. 4, however, this appears not to be the case: neither does the power profile resemble that of DESFire, nor are we currently able to reproduce the correlation results of Sect. 4.1.

Mifare Classic Finally, we also examined the Mifare Classic, even though a successful key recovery by means of SCA would, in the light of the powerful cryptanalytical attacks [10] that allow to extract the secret key in minutes, pose little additional threat. Thus, we only performed some superficial experiments, which, however, suggest that SCA could be utilized for practical key recovery as well. The trace depicted in Fig. 9d was acquired during the verification of the reader response in the Mifare Classic authentication protocol [11]. The power profile exhibits eight characteristic peaks that appear to correspond to the eight bytes sent by the reader: in fact, we can observe a correlation with some bits of these values. Nevertheless, we will not further investigate the susceptibility of Mifare Classic to SCA in the context of this paper.

5 Conclusion

To summarize the impact of our work, we briefly outline the used methods and the results of our analyses in this section, focussing on the implications for real-world systems. We finally pinpoint directions for further improvements and research.

Summary We present an analog demodulation circuit that is specifically designed for improving the SCA of contactless smartcards and that can be integrated into any existing EM SCA setup at a very low cost. We verify the benefits of our new methods by comparing it with a fully digital approach and practically demonstrate the effectiveness of our findings at hand of real-world targets. The developed hardware allows to directly and instantly isolate the side-channel leakage from the reader signal, before the digitizing step, and hence significantly facilitates the alignment and further profiling of SCA measurements of RFID devices.

We illustrate that modern cryptographic RFIDs devices are susceptible to (non-invasive) implementation attacks based on monitoring of the EM field. By evaluating the number of traces required for a successful CPA of the popular Mifare DESFire MF3ICD40 smartcard we quantify the advantages of using an analog demodulator compared to a digital demodulation performed in software. We identify several weaknesses in the implementation of the DESFire MF3ICD40 that enable corresponding SCA attacks to extract the secret key. Our work has severe implications for real-world systems: operators and vendors of commercial RFID systems can no longer rely on the mathematical security of the employed cryptographic algorithms, but also have to take into account that an adversary may be able to obtain secret keys by means of SCA. Thus, appropriate protective measures on the system level, e.g., ensuring that each smartcard has a unique secret key and storing sensitive data in a separate database in the backend whenever possible, are mandatory to guarantee maximum security.

Future Work The described analog circuitry for half-wave rectification has the disadvantage that it discards half of the side-channel information, contained

in the part of the reader's signal with a negative amplitude, and limits the available bandwidth of the side-channel signal. Our results indicate that using the information present in the full-wave rectified signal may enhance SCA attacks, hence a corresponding circuit is currently under development. In this context, experiments with other demodulation techniques, e.g., employing a coherent approach based on a Phase-Locked Loop (PLL), would be interesting in order to determine which method yields the best performance.

Apart from that, the technique of analog demodulation enables — due to the clear isolation of the side-channel signal from the reader signal and the noise — other signal processing methods such as resynchronization [34] that can increase the success rate of, e.g., CPA. In the context of real-world systems and especially for some of the highly protected and certified smartcards briefly presented in Sect. 4.2, these and other techniques might enable an adversary to extract secret information even in the presence of hardware countermeasures.

References

1. FIPS 46-3 Data Encryption Standard (DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.
2. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM Side-Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002*, LNCS, pages 29–45. Springer, 2003.
3. Analog Devices, Inc. *AD8045 Voltage Feedback High Speed Amplifier Datasheet*, 2004.
4. Analog Devices, Inc. *AD8058 Dual, High Performance Voltage Feedback 325 MHz Amplifier Datasheet*, 2009.
5. E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *LNCS*, pages 16–29. Springer, 2004.
6. BSI - German Ministry of Security. Security mechanisms in electronic ID documents. http://www.bsi.de/fachthem/epass/.
7. BSI - German Ministry of Security. Mifare DESFire8 MF3ICD81 Public Evaluation Documentation. Electronic resource, October 2008.
8. BSI - German Ministry of Security. Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents. Electronic resource, October 2010. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/TR-03110_v205_pdf.pdf?__blob=publicationFile.
9. D. Carluccio. Electromagnetic Side Channel Analysis for Embedded Crypto Devices. Master's thesis, Ruhr-University Bochum, 2005.
10. N. Courtois. The Dark Side of Security by Obscurity and Cloning Mifare Classic Rail and Building Passes, Anywhere, Anytime. In *SECRYPT 2009*, pages 331–338. INSTICC Press.
11. F. D. Garcia, G. Koning Gans, R. Muijrers, P. Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. Dismantling MIFARE Classic. In *Proceedings of the 13th European Symposium on Research in Computer Security - ESORICS 2008*, LNCS, pages 97–114. Springer, 2008.
12. M. Hutter, S. Mangard, and M. Feldhofer. Power and EM Attacks on Passive 13.56 MHz RFID Devices. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, LNCS 4727, pages 320 – 330. Springer, 2007.
13. International Organization for Standardization. ISO/IEC 14443-3: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards - Part 3: Initialization and Anticollision, February 2001.
14. International Organization for Standardization. ISO/IEC 14443-4: Identification cards - Contactless Integrated Circuit(s) Cards - Proximity Cards - Part 4: Transmission Protocol, February 2001.
15. International Organization for Standardization. ISO/IEC 15693-3: Identification Cards - Contactless Integrated Circuit Cards - Vicinity Cards - Part 3: Anticollision and Transmission Protocol, April 2009.
16. T. Kasper, D. Carluccio, and C. Paar. An Embedded System for Practical Security Analysis of Contactless Smartcards. In *WISTP*, volume 4462 of *LNCS*, pages 150–160. Springer, 2007.

17. T. Kasper, D. Oswald, and C. Paar. EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. In H. Y. Youm and M. Yung, editors, *10th International Workshop on Information Security Applications - WISA 2009*, LNCS, pages 79–93. Springer, 2009.
18. T. Kasper, D. Oswald, and C. Paar. A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices. In M. Gavrilova, C. Tan, and E. Moreno, editors, *Transactions on Computational Science X*, volume 6340 of *LNCS*, pages 100–130. Springer, 2010.
19. T. Kasper, D. Oswald, and C. Paar. Chameleon: A Versatile Emulator for Contactless Smartcards. To appear in the Springer LNCS proceedings of ICISC 2010, Seoul, Korea, 2010.
20. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *19th Annual International Cryptology Conference on Advances in Cryptology - CRYPTO'99*, pages 388–397. Springer, 1999.
21. Langer EMV-Technik. Details of Near Field Probe Set RF 2. Website.
22. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, Secaucus, NJ, USA, 2007.
23. K. Nohl, D. Evans, Starbug, and H. Plötz. Reverse-Engineering a Cryptographic RFID Tag. In *USENIX Security Symposium*, pages 185–194. USENIX Association, 2008.
24. NXP. *Mifare DESFire Contactless Multi-Application IC with DES and 3DES Security MF3ICD40*, April 2004.
25. NXP. *Mifare Ultralight C Product Short Datasheet*, May 2009.
26. NXP. *Mifare DESFire EV1 Contactless Multi-Application IC Datasheet*, December 2010.
27. NXP. Mifare Smart Card ICs. Website, March 2011. `http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/index.html`.
28. Y. Oren and A. Shamir. Remote Password Extraction from RFID Tags. *IEEE Transactions on Computers*, 56(9):1292–1296, 2007. `http://iss.oy.ne.ro/RemotePowerAnalysisOfRFIDTags`.
29. Pico Technology. PicoScope 5200 USB PC Oscilloscopes, 2008.
30. T. Plos. Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags. In M. Fischlin, editor, *Topics in Cryptology - CT-RSA 2009*, volume 5473 of *LNCS*, pages 444–458. Springer, 2009.
31. T. Plos, M. Hutter, and M. Feldhofer. Evaluation of Side-Channel Preprocessing Techniques on Cryptographic-Enabled HF and UHF RFID-Tag Prototypes. In S. Dominikus, editor, *Workshop on RFID Security 2008*, pages 114 – 127, 2008.
32. M. Schwartz, W. R. Bennett, and S. Stein. *Communication Systems and Techniques*. Wiley, 1966.
33. P. S. W. Smith. *The Scientist and Engineer's Guide to Digital Signal Processing*. California Technical Publishing, 1st edition, 1997.
34. J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker. Improving Differential Power Analysis by Elastic Alignment. In *Topics in Cryptology - CT-RSA 2011*, volume 6558 of *LNCS*, pages 104–119. Springer, 2011.
35. Vishay Semiconductors, Inc. *BAT48 Schottky Diode Datasheet*.
36. Wikipedia. Contactless Smart Card — Wikipedia, The Free Encyclopedia, 2011. [Online; accessed 5-March-2011].

A Schematics

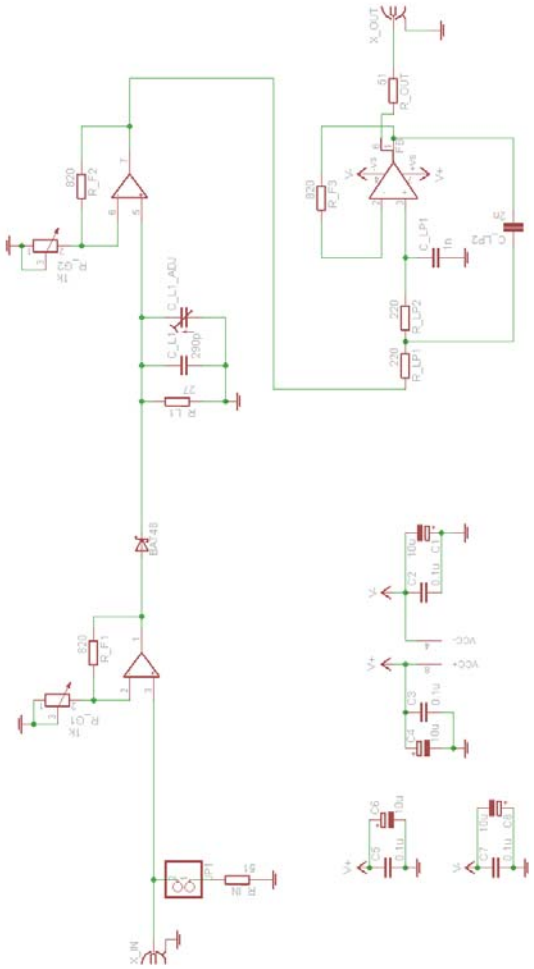


Fig. 10: Schematics of analog rectifier circuit