EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment

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, cpaar@crypto.rub.de

Abstract. We introduce low-cost hardware for performing non-invasive side-channel attacks on Radio Frequency Identification Devices (RFID) and develop techniques for facilitating a correlation power analysis (CPA) in the presence of the field of an RFID reader. We practically verify the effectiveness of the developed methods by analysing the security of commercial contactless smartcards employing strong cryptography, pinpointing weaknesses in the protocol and revealing a vulnerability towards side-channel attacks. Employing the developed hardware, we present the first successful key-recovery attack on commercially available contactless smartcards based on the Data Encryption Standard (DES) or Triple-DES (3DES) cipher that are widely used for security-sensitive applications, e.g., payment purposes.

1 Introduction

In the past few years, RFID technologies rapidly evolved and are nowadays on the way to become omnipresent. Along with this trend grows the necessity for secure communication and authentification. RFID-based applications such as electronic passport, payment systems, car immobilisers or access control systems require strong cryptographic algorithms and protocols, as privacy and authenticity of the transmitted data are crucial for the system as a whole. Since severe weaknesses have been discovered in the "first generation" of RFIDs that rely on proprietary ciphers [25,8,7,10], such as Mifare Classic contactless smartcards [21] or KeeLoq RFID transponders [20], future systems will tend to employ stronger cryptographic primitives. This trend can already be observed, as several products exist that provide a (3)DES encryption.

The aim of this paper is to practically evaluate the security of these believed (and advertised) to be highly secure contactless smartcard solutions. Since encryption is performed using well-known and carefully reviewed algorithms, cryptanalytical attacks on the algorithmic level are very unlikely to be found. Thus, we aim at performing a *Side-Channel Analysis* which exploits the physical characteristics of the actual hard- or software implementation of the cipher.

H.Y. Youm and M. Yung (Eds.): WISA 2009, LNCS 5932, pp. 79–93, 2009.

1.1 RFID and Contactless Smartcards

The huge variety of applications for RFID implies that products come in a lot of distinct flavors, differing amongst others in the operating frequency, the maximum achievable range for a query, and their computational power [9].

Passive RFIDs draw all energy required for their operation from the field of a reader and are hence severely limited with respect to their maximum power consumption, i.e., the amount of switching transistors during their operation, which has a direct impact on their cryptographic capabilities. For highly demanding applications, the ISO/IEC 14443 standard for *contactless smartcards* [13,14] has proven to be suitable. A strong electromagnetic field combined with a specified reading distance of only approx. 10 cm provides - contrary to most other RFID schemes - a sufficient amount of energy even for public key cryptography, as realised in the electronic passport [1]. In the standard, a contactless smartcard is also referred to as *Proximity Integrated Circuit Card* (PICC), while the reader is called *Proximity Coupling Device* (PCD). The PCD generates an electromagnetic field with a carrier frequency of 13.56 MHz, that supplies the PICC with energy and at the same time serves as a medium for the wireless communication. All communication is initiated by the PCD, while the PICC answers by load-modulating the field of the PCD [13].

Challenge-Response Authentication Protocol. According to its data sheet, the analysed contactless smartcard uses a challenge-response authentication protocol which relies on a symmetric block cipher, involving a 112 bit key k_C that is shared between PCD and PICC. For the cipher, a 3DES using the two 56 bit halves of $k_C = k_1 || k_2$ in EDE mode according to [2] is implemented. After a successful authentication, the subsequent communication is encrypted with a session key. We implemented the whole protocol, but however, focus on the step relevant for our analyses as depicted in Fig. 1, where $\text{3DES}_{k_C}(\cdot) = \text{DES}_{k_1}\left(\text{DES}_{k_2}^{-1}\left(\text{DES}_{k_1}(\cdot)\right)\right)$ denotes a 3DES encryption involving the key $k_C = k_1 || k_2$. The values B_1 and B_2 have a length of 64 bit and are encrypted by the PICC during the mutual authentication. B_2 originates from a random number previously generated by the PICC and is always encrypted by the PICC in order to check the authenticity of the PCD[1]. B_1, a random value chosen by the PCD that serves for authenticating the PICC to the PCD, is mentioned here for completeness only and is not required in the context of our analyses.

1.2 Related Work

Oren and Shamir [22] presented a successful side-channel attack against so-called Class 1 EPC tags operating in the UHF frequency range which can be disabled remotely by sending a secret "kill password". Small fluctuations in the reader

[1] The protocol will abort after the encryption of B_2, in case its verification is not successful.

$$\begin{array}{ccc} \text{PCD} & & \text{PICC} \\ \text{Choose } B_1,\, B_2 & \xrightarrow{B_1,\, B_2} & \text{3DES}_{k_C}\,(B_2) \end{array}$$

Fig. 1. Exerpt of the authentication protocol relevant for an attack

field during the communication with the tag allow to predict the password bits. However, the very limited type of RFID tag does not offer any cryptography.

At CHES 2007, Hutter et al. [12] performed an EM attack on their own AES implementations on a standard 8-Bit microcontroller and an AES co-processor in an RFID-like setting, i.e., the self-made devices are powered passively and brought into the field of a reader. On their prototype devices the antenna and analogue frontend are separated from the digital circuitry, while on a real RFID tag, these components are intrinsically tied together. An artificially generated trigger signal before the attacked S-Box operation ensures perfect time alignment. Moreover, the clock signal for the digital circuitry is generated independently from the field of the reader using an external oscillator, hence the carrier is uncorrelated with the power consumption of the AES and can be easily removed.

In contrast, we now face the real-world situation, i.e., have no knowledge on the internal implementation details of the unmodified contactless smartcard to be attacked, cannot rely on artificial help like precise triggering for alignment, and analyse a black box with all RFID and cryptographic circuitry closely packed on one silicon die. In the following, after a brief introduction to power analysis in the context of RFID in Sect. 2.1, we will describe all relevant steps to analyse an unknown RFID device in practise, starting from our special low-cost measurement setup in Sect. 2.3 and including the extensive profiling that is required to gain insight into the operation of the smartcard in Sect. 3, before the results of the actual side-channel attack are presented in Sect. 3.2.

2 Power Analysis of RFIDs

Differential Power Analyis (DPA) was originally proposed in [17] and has become one of the most powerful techniques to recover secret information from even small fluctuations in the power leakage of the physical implementation of a cryptographic algorithm. In this paper, we address the popular *Correlation Power Analysis* (CPA), as introduced in [4].

2.1 Traditional vs. RFID Measurement Setup

For a typical power analysis attack [8] the side-channel leakage in terms of the electrical current consumption of the device, while executing a cryptographic operation, is measured via a resistor inserted into the ground path of the target IC. Since the targeted RFID smartcard circuitry including the anntenna is embedded in a plastic case, lacking any electrical contacts, it is difficult to perform a direct on-chip measurement of the power consumption. Invasive attacks, i.e., dissolving the chip from its plastic package and separating it from the antenna, were not successful [6], maybe due to the strong carrier of the reader that is required for the operation. Anyway, even a successful invasive attack is costly and can be easily detected, hence a non-invasive approach becomes very attractive in the context of RFIDs.

Non-Invasive Analysis with DEMA. A possible source of side-channel leakage that can be exploited in a non-invasive attack scenario is the information gathered from fluctuations of the EM field emanated by a device whilst performing a cryptographic operation. The corresponding side-channel information for this so-called *Differential Electro-Magnetic Analysis* (DEMA) [3] is acquired by means of near-field probes that are positioned close to the chip, and typically require no physical contact to the device, i.e., leave no traces. The analogue signal, i.e., the EM leakage in case of a DEMA, is digitised and recorded as a discrete and quantised timeseries called a *trace*. In practice, several traces for varying input data are collected. In the following, let $\boldsymbol{t_l}$ be the l^{th} trace of one attack attempt, where $0 \leq l < L$, with L denoting the number of traces. Likewise, x_l denotes the associated input challenge for the l^{th} measurement. For simplicity, we consider that all traces have the same length N.

2.2 Correlation DPA

For the actual attack, each *key candidate* K_s, $0 \leq s < S$, where the number of candidates S should be small[2], is input to a *prediction function* $d\left(K_s,\, x_l\right)$, establishing a link between given input data x_l and the expected current consumption for each key candidate K_s. Often, d predicts the power consumption of the output of an S-Box after the key addition, modelled either based on the Hamming weight, i.e., the number of ones in a data word, or based on the Hamming distance, i.e., the amount of toggling bits in a data word.

A CPA essentially relies on calculating the *Normalised Correlation Coefficient* between the predicted and recorded values for one point in time n and a fixed key K_s:

$$\Delta\left(K_s,\, n\right) = \frac{\sum_{l=0}^{L-1}\left(\boldsymbol{t_l}\left(n\right) - m_{\boldsymbol{t}(n)}\right)\left(d\left(K_s,\, x_l\right) - m_{d(K_s)}\right)}{\sqrt{\sigma^2_{\boldsymbol{t}(n)}\sigma^2_{d(K_s)}}}$$

with $m_{\boldsymbol{t}(n)}$, $m_{d(K_s)}$ denoting the means of the samples, and $\sigma^2_{\boldsymbol{t}(n)}$, $\sigma^2_{d(K_s)}$ the sample variances of the respective timeseries. Plotting Δ for all n yields a curve indicating the correlation over time that features significant peaks, if K_s is the correct key guess, and has a random distribution otherwise. Thus, by iterating over all K_s and analysing the resulting $\Delta\left(K_s,\, 0\right) \ldots \Delta\left(K_s,\, N-1\right)$, the cryptographic secret can be revealed, given that enough traces have been acquired and that there exists a link between the side-channel leakage and the processed data input.

[2] This is always the case when attacking single S-Boxes with few in- and outputs.

Efficiently Implementing a CPA. Straightforward implementations of a CPA read all L traces, each with a length of N samples, into memory before calculating the correlation coefficient $\Delta(K_s, n)$ (see Sect. 2.2).

This may become problematic for long traces and/or a large amount of measurements, e.g., $L = 10\,\text{k}$ traces with $N = 350\,\text{k}$ data points (stored as 4 byte single precision values) consume $\approx 13\,\text{GByte}$ of memory. Therefore, a *recursive* computation of $\Delta(K_s, n)$ becomes attractive. Instead of first reading and then processing all data, existing values of the correlation coefficient can be updated with every new trace. This approach makes use of an algorithm given in [16], originally proposed by Welford. The update equations are

$$m_{i+1} = m_i + \frac{t_{i+1} - m_i}{i+1}, \ M2_{i+1} = M2_i + (t_{i+1} - m_i)(t_{i+1} - m_{i+1}).$$

where the initial values are $m_0 = 0$, $M2_0 = 0$, t_i denotes the data points, m_i is the mean and $\sigma_i^2 = \frac{M2_i}{i-1}$ the variance after i samples. Applying this idea for computing the correlation coefficient of a key candidate, it suffices to keep track of N trace means $m_{\boldsymbol{t}(n)}$ and $M2_{\boldsymbol{t}(n)}$. Analogously, $m_{d(K_s)}$ and $M2_{d(K_s)}$ are updated, however, these are independent of n and thus need to be stored only once.

Besides, for evaluating Eq. 2.2, $c(K_s, n) = \frac{\sum_{l=0}^{L-1} \boldsymbol{t_l}(n) d(K_s, x_l)}{L-1}$ is stored for N points in time and updated[3] according to

$$c_{i+1} = c_i + \frac{\boldsymbol{t}_{i+1} \cdot d(x_{i+1}) - c_i}{i}$$

with initial values $c_0 = \boldsymbol{t_0} \cdot d(x_0)$, $c_1 = \boldsymbol{t_0} \cdot d(x_0) + \boldsymbol{t_1}\cdot$. $\Delta(K_s, n)$ after L traces is

$$\Delta(K_s, n) = \frac{(L-1) \cdot c_L(K_s, n) - L \cdot m_{\boldsymbol{t}(n)} \cdot m_{d(K_s)}}{\sqrt{M2_{\boldsymbol{t}(n)} M2_{d(K_s)}}}$$

The application of the recursive approach requires the storage of $\mathcal{O}(N)$ values for each key candidate K_s. In contrast, the traditional two-pass method (read all, then process) needs $\mathcal{O}(L \cdot N)$ memory. Thus, for large L, the memory footprint of the above described computations remains *constant*, while a straightforward algorithm becomes infeasible.

Modelling the Power Consumption of RFID Devices. For a simple model of the frequencies where we would expect the EM leakage to occur, consider a band-limited power consumption $p(t)$ that directly affects the amplitude of the $\omega_0 = 2\pi \cdot 13.56$ MHz carrier, i.e., the amplitude of the field will be slightly smaller in an instant when the chip requires more energy than in an instant when no energy is consumed. This results in possibly detectable frequency components

[3] Note that n and K_s have been omitted for readability.

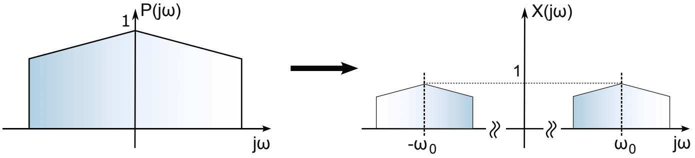

Fig. 2. Frequency spectrum of the carrier signal ω_0 and the assumed information leakage for remote power analysis

in the side bands of the carrier, as depicted in Fig. 2. Equation 1 describes this model more precisely, where $\circ\!\!-\!\!\bullet$ denotes the Fourier transform[4].

$$p(t)\cos(\omega_0 t) \circ\!\!-\!\!\bullet X(j\omega) = \frac{1}{2}\left(P(j\omega - j\omega_0) + P(j\omega + j\omega_0)\right) \tag{1}$$

We refer to this approach as *Remote Power Analysis*, as the fluctuations in the power consumption of the device are modulated onto the strong carrier signal of the PCD and may thus be visible even in the far-field[5].

2.3 Measurement Setup

The core of our proposed DEMA measurement equipment for RFIDs, illustrated in Fig. 3, is a standard PC that controls an oscilloscope and a self-built, freely programmable reader for contactless smartcards. These components, a specially developed circuit for analogue preprocessing of the signal and the utilised near-field EM probes are covered in this section.

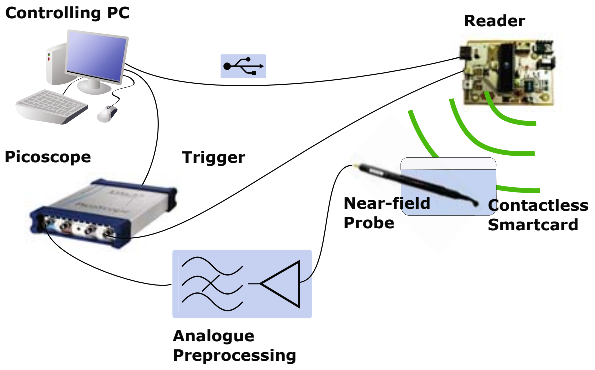

Fig. 3. Measurement setup

[4] The Fourier transform is commonly used to transform signals from the time domain into the frequency domain.

[5] For a frequency of 13.56 MHz the far-field begins at approx. 22 m [15].

RFID Reader. The RFID-interface is a custom embedded system both capable of acting as a reader and a transponder [15], whereas in the context of DEMA only the reader functionality is used. The device is controlled by a freely programmable Atmel ATMega32 microcontroller and provides an ISO 14443-compliant analogue front-end at a cost of less than 40 €. Contrary to commercial RFID readers, our self-built device allows for sending chosen challenges during the authentication.

Scope. The *Picoscope 5204* is a dual-channel storage USB-oscilloscope [23], featuring a maximum sample-rate of 1 GHz, an 8 bit analogue-to-digital converter (ADC), a huge 128 MSamples waveform memory and an external trigger input. These conditions are extremely good for side-channel analysis[6], alone the minimum input range of ± 100 mV might pose a problem in the context of DEMA attacks, where small voltage changes need to be detected with a high accuracy.

Probes. For measurements of the EM-field emanated by the contactless smartcard, a *RF-U 5-2* probe [18] is suitable, because it captures the near H-field that is proportional to the flow of the electric current in the horizontal plane. Note that, if no commercial EM probes are at hand, a self-wound coil can be a suitable replacement [5]. The small signal amplitudes (max. 10 mV) delivered by the probe are preamplified with the *PA-303* amplifier [18] by 30 dB over a wide frequency range of 3 GHz.

Analogue Signal Processing. Although to our knowledge there exist no reliable estimations about the exact amplitude of the EM emanations caused by digital circuitry — especially when attacking an unknown implementation — the unintented emanations of the chip are clearly orders of magnitude smaller than the strong field generated by the reader to ensure the energy supply of a PICC. The quantisation error induced by the ADC of the oscilloscope constitutes a minimum boundary for the achievable *Signal-to-Noise Ratio* (SNR), depending on the number of bits used for digitising an analogue value. Following [11], each bit improves the SNR by about 6 dB. Thus, for the best SNR the full input scale should be utilised for the signal of interest, implying that a maximum suppression of the carrier frequency and a subsequent amplification of the small side-channel information must already take place in the analogue domain, before the digitising step.

For minimising the disturbing influence of the carrier frequency on the measurements, we have built and tested several types of active and passive analogue filters. We here present our most straightforward and most unexpensive idea which in fact turned out to be the most effective approach in order to bypass the influence of the field of the reader. A part of the analogue front-end of the reader is a crystal-oscillator generating an almost pure sine wave with a frequency of 13.56 MHz that serves as the source for the field transmitted to the contactless

[6] In fact, for a typical side-channel attack such a large memory will never be fully used.

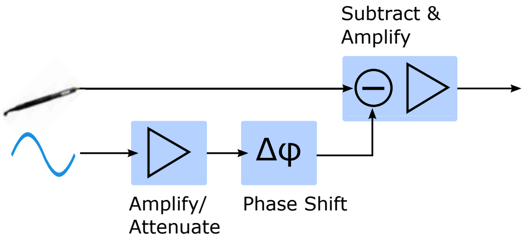

Fig. 4. Block diagram for removing the unwanted carrier frequency of the reader

smartcard. The straightforward principle introduced in the following is to tap the oscillator of the reader and subtract its signal from the output of the EM probe. The sine signal has a constant amplitude and a constant shift in time, compared to the field acquired with the EM probes. Hence, as shown in Fig. 4, the developed analogue circuitry is capable of delaying and scaling the sine wave of the crystal, in order to match its amplitude and phase to that of the EM measurements, before substracting the pure sine from the EM measurements. This approach, based on low-cost circuits employing operational amplifiers, allows to suppress the unwanted signal component while keeping all possibly interesting variations. The analoque preprocessing unit can also be used for other types of RFIDs, such as 125 kHz transponders in car immobilisers.

3 A Real-World EM Attack on Contactless Smartcards

By performing a full authentication and reproducing the responses[7] of the cryptographically enabled contactless smartcard under attack on the PC, we verify that a standard (3)DES [2] is used for the encryption of the challenge according to Fig. 1. We further observe that the card unconditionally encrypts any value B_2 (cf. Sect. 1.1 sent to it, hence we can freely choose the plaintext. For the CPA described in the following, we will send random, uniformly distributed plaintexts for B_2 and attack the first DES round.

3.1 Trace Preprocessing

The raw traces recorded between the last bit of the command sent by the reader and the first bit of the answer of the card do not expose any distinctive pattern, hence, digital preprocessing is applied in order to identify interesting patterns useful for a precise alignment of the traces. On the basis of the RFID power model introduced in Sect. 2.2, we assume that the power consumption of the smartcard modulates the amplitude of the carrier wave at frequencies much lower than the 13.56 MHz carrier frequency, which is justified by a preliminary

[7] Note that in this context the secret key of the implementation can be changed by us and is hence known.

spectral analysis and the well-known fact that the on-chip components (such as capacitances, resistors, inductances) typically imply a strong low-pass filter characteristic.

Digital Amplitude Demodulation. In order obtain the relevant side-channel information, we record raw (undemodulated) traces and perform the demodulation digitally, using a straightforward incoherent demodulation approach (Fig. 5, following [26]). The raw trace is first rectified, then low-passed filtered using a *Finite Impulse Response* (FIR) filter. An additional high-pass *Infinite Impulse Response* (IIR) filter removes the constant amplitude offset resulting from the demodulation principle and low-frequency noise. Good values for the filter cutoff frequencies $f_{lowpass}$ and $f_{highpass}$ were determined experimentally and are given in Sect. 3.2.

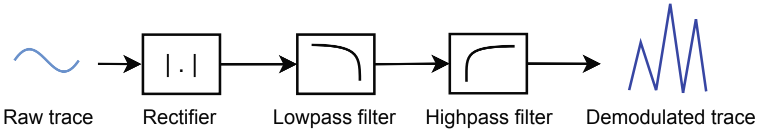

Fig. 5. Digital amplitude demodulator

Fig. 7 displays a demodulated trace ($f_{lowpass} = 2\,\text{MHz}$, $f_{highpass} = 50\,\text{kHz}$) in which distinct patterns are visible, especially two shapes at 240000 ns and 340000 ns preceded and followed by a number of equally spaced peaks. For comparision, Fig. 6 shows a zoomed part of the same trace without demodulation. Fig. 8 and Fig. 9 originate from a trace recorded without the analogue prefilter described in Sect. 2.3 and demonstrate that our filter circuit effectively increases the amplitude of the signal of interest and reduces the noise level of the demodulated signal.

Trace Alignment For precise alignment during the digital processing, we select a short reference pattern in a demodulated *reference trace*. This pattern is then located in all subsequent traces by finding the shift that minimises the squared difference between the reference and the trace to align, i.e., we apply a least-squares approach.

For devices with a synchronous clock, the alignment with respect to one distinct pattern is usually sufficient to align the whole trace. However, in our measurements we found that the analysed smartcard performs the operations in an asynchronous manner, i.e., the alignment may be wrong in portions not belonging to the reference pattern. The alignment has thus to be performed with respect to the part of the trace we aim to examine by means of CPA.

3.2 Results of DEMA

The process to perform a DEMA of the 3DES implementation can be split up into the following steps, of which we will detail the latter two in this section:

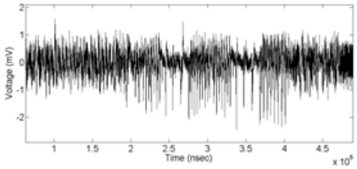

Fig. 6. Demodulated trace (50 kHz - 2 MHz) with analogue filter

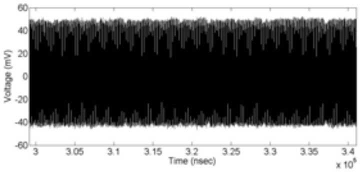

Fig. 7. Raw trace with analogue filter (zoomed)

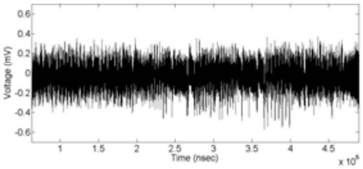

Fig. 8. Demodulated trace (50 kHz - 2 MHz) without analogue filter

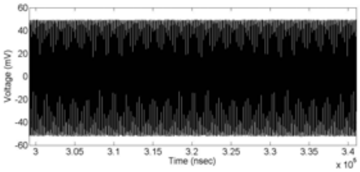

Fig. 9. Raw trace without analogue filter (zoomed)

1. Find a suitable trigger point.
2. Align the traces.
3. Locate the DES encryption.
4. Perform the EM analysis.

Data Bus Transfer of Plain- and Ciphertext. As the plaintext for the targeted 3DES operation is known and the ciphertext can be computed in a known-key scenario, we are able to isolate the location of the 3DES encryption by correlating on these values. From the profiling phase with a known key it turns out that the smartcard uses an 8 bit data bus to transfer plain- and ciphertexts. The corresponding values can be clearly identified from 2000 - 5000 traces using a Hamming weight model, as depicted in Fig. 10 and 11.

This first result suggests that the smartcard logic is implemented on a microcontroller which communicates with a separate 3DES hardware engine over

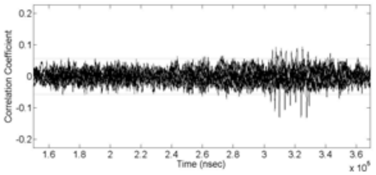

Fig. 10. Correlation coefficients for plaintext bytes (before targeted 3DES encryption) after 5000 traces, Hamming Weight

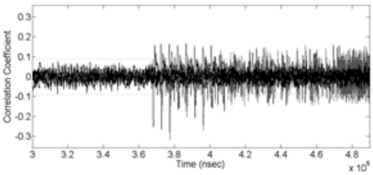

Fig. 11. Correlation coefficients for ciphertext bytes (after targeted 3DES encryption) after 2000 traces, Hamming Weight

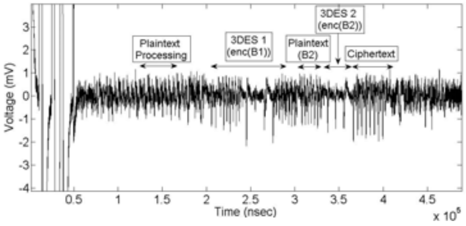

Fig. 12. Overview over operations in amplitude-demodulated trace

a data bus using precharged wires. This assumption is further supported by the fact that correlation with the plaintext bytes can be observed twice, but with reversed byte order. The microcontroller probably first receives the plaintext bytes via the RF module, byte-reverses it and transmits it over the internal bus to the encryption engine later. The ciphertext is then sent back using the same byte order as for the second appearance of the plaintext.

From the profiling observations, Fig. 12 was compiled, with the shape of the 3DES operation marked. The first 3DES encryption (3DES 1) results from a prior protocol step, the correlation with the correct ciphertext appears after the second 3DES shape only (labeled 3DES 2).

3DES Engine. After having localised the interval of the 3DES operation from the position of the corresponding plain- and ciphertexts, we now focus on this part of the trace. Fig. 13 shows a zoomed view of the targeted 3DES operation, filtered with $f_{lowpass} = 8\,\text{MHz}$ and $f_{highpass} = 50\,\text{kHz}$. The short duration of the encryption suggests that the 3DES is implemented in a special, separate hardware module, hence we assume a Hamming distance model[8].

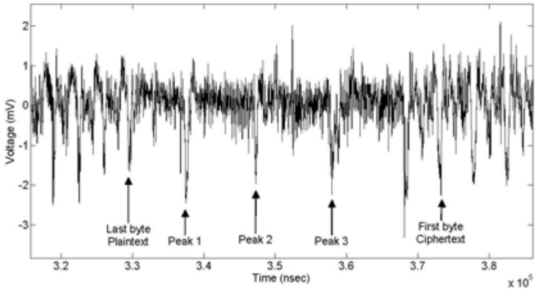

Fig. 13. Part of trace with 3DES encryption, filtered with $f_{lowpass}$ = 8 MHz, $f_{highpass}$ = 50 kHz

[8] We also considered a Hamming weight model, however, did not reach conclusive results with it.

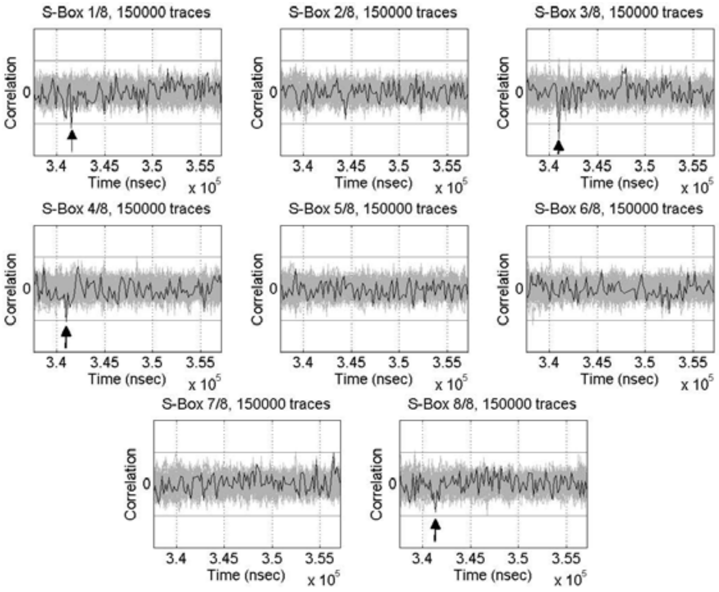

Fig. 14. Correlation coefficients for binwise CPA with peak extraction after 150000 traces, $f_{lowpass} = 8$ MHz, $f_{highpass} = 50$ kHz

The three marked peaks seemingly appear at the end of one complete Single-DES and are thus promising candidates as alignment patterns. Consequently, we conduct a CPA on demodulated traces aligned to each of these peaks, where we consider the Hamming distance between the DES registers (L_0, R_0) and (L_1, R_1), i.e, the state before and after the first round of the first Single-DES. It turns out that for the second peak, results are generally most conclusive. When performing a standard CPA with $L = 150000$ traces, correlation peaks with maximum amplitude for the correct key candidate for S-Box 1 and 3 occur at a position which we consider as the start point of the first DES.

As the attack works for a subset of S-Boxes, we conclude that no masking scheme ([19]) is used to protect the hardware engine. Rather than, we conjecture that hiding in time dimension is used, i.e., dummy cycles with no computation taking place or similar measures might be inserted to prevent correct alignment of the traces. This assumption is strengthened by the fact that even when repeatedly sending the same plaintext B_2 to the smartcard, the shape of the DES operation and the position of the peaks depicted in Fig. 13 vary[9].

In order to improve the alignment, we extract local maxima and minima from the trace part belonging to the first DES operation. The resulting data points (composed of time position and amplitude) are then grouped on the basis of their time coordinate by dividing the time axis into equal intervals or *bins*. Thus, extrema which occur at slightly different points in different traces are assigned

[9] This misalignment also hinders improving the SNR by means of averaging.

to the same bin, correcting for timing jitter up to a certain extent. The CPA is performed *binwise*, i.e., the correlation coefficient for each bin is computed from all extrema lying within the corresponding time interval.

The correlation coefficients for this experiment are given in Fig. 14, where the y-axis has been normalised to the theoretical noise level $\frac{4}{\sqrt{L}}$ (cf. [19]), accounting for the different number of data points per bin. It can be seen that using this method, the correct subkey can be identified for S-Box 1, 3, 4 and 8.

4 Future Work

To further improve the attack and to both reduce the number of traces and increase the correlation, we investigate suitable methods for precise alignment within the DES operation and for the detection of dummy operations. For this purpose we are currently evaluating two approaches. On the one hand, we plan to apply CPA in the (short-time) frequency domain ([27], [24]), on the other hand, we optimise our measurement environment to gain more information on the details of the internal operation of the RFID smartcard.

The maximum amplitude of the measurements for our DEMA in the oscilloscope has been approx. 40 mV, while the 8 Bit ADC in the oscilloscope quantises a full scale of 100 mV. Hence, only approx. 100 out of 256 values are currently used for digitising the analogue signal. Accordingly, we expect to carry out an EM analysis with 2.5 times less measurements than before when exploiting the full scale. Besides, the amplitude demodulation that has already has proven its effectiveness when implemented digitally can also be performed in the analogue domain, allowing for a significantly better amplification of the side-channel information contained in the carrier envelope.

It is also promising to further investigate a remote power analysis as described in Sect. 2.2, i.e., whether an EM attack from a distance of several meters is conductable. Since the side-channel signal is contained in the envelope of the carrier wave, it can be expected to be receivable from distant locations in the far field using analogue receiver equipment and suitable antennae.

5 Conclusion

As the main result attained in this paper, we give practical contributions for analysing the security of RFIDs via non-invasive side-channel attacks. We presented a new approach for performing effective EM analyses, realised a corresponding analogue hardware and describe our resulting low-cost measurement environment. We detail on the relevant steps of performing practical real-world EM attacks on commercial contactless smartcards in a black-box scenario and thereby demonstrated the potency of our findings.

This paper pinpoints several weaknesses in the protocol and the actual implementation of widespread cryptographic contactless smartcards, including a vulnerability to DEMA. We investigated the leakage model applicable for the data bus and described a CPA on the 3DES hardware implementation running on the targeted commercial smartcard. We demonstrated the effectiveness of our developed methods, that are generally applicable for analysing all kinds of RFID devices and contactless smartcards, by detailing and performing a full key-recovery attack, leaving no traces, on a black box device.

References

1. Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)., `http://www.bsi.de/english/publications/techguidelines/tr03110/TR-03110_v200.pdf`
2. FIPS 46-3 Data Encryption Standard (DES), `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
3. Agrawal, D., Archambeault, B., Rao, J.R., Rohatgi, P.: The EM Side-Channel(s). In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 29–45. Springer, Heidelberg (2003)
4. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
5. Carluccio, D.: Electromagnetic Side Channel Analysis for Embedded Crypto Devices. Master's thesis, Ruhr Universität Bochum (2005)
6. Carluccio, D., Lemke, K., Paar, C.: Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. In: RFIDSec 2005 Workshop on RFID and Lightweight Crypto (July 2005), `http://events.iaik.tugraz.at/RFIDandLightweightCrypto05/RFID-SlidesandProceedings/Carluccio-EMSideChannel.pdf`
7. Courtois, N.T., Nohl, K., O'Neil, S.: Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166 (2008)
8. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M.T.M.: On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 203–220. Springer, Heidelberg (2008)
9. Finkenzeller, K.: RFID-Handbuch, 3rd edn. Hanser Fachbuchverlag (October 2002)
10. Garcia, F.D., de Koning Gans, G., Muijrers, R., van Rossum, P., Verdult, R., Schreur, R.W., Jacobs, B.: Dismantling MIFARE Classic. In: Jajodia, S., López, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 97–114. Springer, Heidelberg (2008)
11. Haykin, S.: Communications Systems, 2nd edn., ch. 8. Wiley, Chichester (1983)
12. 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. 320–330. Springer, Heidelberg (2007)
13. International Organization for Standardization. ISO/IEC 14443-3: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialization and anticollision, 1st edn. (February 2001)
14. International Organization for Standardization. ISO/IEC 14443-4: Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol, 1st edn. (February 2001)

15. Kasper, T., Carluccio, D., Paar, C.: An Embedded System for Practical Security Analysis of Contactless Smartcards. In: Sauveron, D., Markantonakis, K., Bilas, A., Quisquater, J.-J. (eds.) WISTP 2007. LNCS, vol. 4462, pp. 150–160. Springer, Heidelberg (2007)
16. Knuth, D.E.: The Art of Computer Programming, 3rd edn., ch. 2. Seminumerical Algorithms. Addison-Wesley, Boston (1998)
17. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
18. Langer EMV-Technik. Details of Near Field Probe Set RF 2, `http://www.langer-emv.de/en/produkte/prod_rf2.htm`
19. Mangard, S., Oswald, E., Popp, T.: Power analysis attacks: Revealing the secrets of smart cards. Springer, Secaucus (2007)
20. Microchip. HCS410, KeeLoq Code Hopping Encoder and Transponder Data Sheet, `http://ww1.microchip.com/downloads/en/DeviceDoc/40158e.pdf`
21. NXP. Data Sheet of Mifare Classic 4k chip MF1ICS70 (2008)
22. Oren, Y., Shamir, A.: Remote Password Extraction from RFID Tags. IEEE Transactions on Computers 56(9), 1292–1296 (2007), `http://iss.oy.ne.ro/RemotePowerAnalysisOfRFIDTags`
23. Pico Technology. PicoScope 5200 USB PC Oscilloscopes (2008)
24. Plos, T., Hutter, M., Feldhofer, M.: Evaluation of Side-Channel Preprocessing Techniques on Cryptographic-Enabled HF and UHF RFID-Tag Prototypes. In: Dominikus, S. (ed.) Workshop on RFID Security 2008, pp. 114–127 (2008)
25. Plötz, H.: Mifare Classic - Eine Analyse der Implementierung. Master's thesis, Humboldt-Universität zu Berlin (2008)
26. Shanmugam, K.S.: Digital & Analog Communication Systems, ch. 8.3.2. Wiley-India, Chichester (2006)
27. Tiu, C.C.: A New Frequency-Based Side Channel Attack for Embedded Systems. Master's thesis, University of Waterloo (2005)