New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs

Timo Kasper, David Oswald and Christof Paar

Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
{Timo.Kasper,David.Oswald,Christof.Paar}@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 immobilizers 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 [24, 8, 7, 10], such as Mifare Classic contactless smartcards [20] or KeeLoq RFID transponders [19], 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.

1.1 RFID and Contactless Smartcards

The huge variety of applications for RFID implies that products come in a lot of distinct flavors, differing with respect to the operating frequency, the maximum achievable range for a query, and thereby the energy that can be drawn from the field of a reader for reliable operation [9]. Passive RFIDs are 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 the amount of cryptography that can be put on a passive transponder. 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 realized 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 authentication protocol, but however, focus on the protocol step relevant for our attack as depicted in Fig. 1, where B_1 is a random 64 bit string chosen by the PCD, B_2 is a protocol value that is unconditionally encrypted[1] by the PICC, and $3\mathrm{DES}_{k_C}(\cdot) = \mathrm{DES}_{k_1}\left(\mathrm{DES}_{k_2}^{-1}\left(\mathrm{DES}_{k_1}(\cdot)\right)\right)$ denotes a 3DES encryption involving the key $k_C = k_1||k_2$.

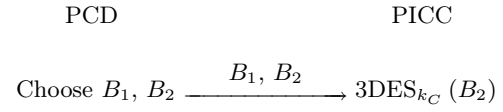

Fig. 1. Exerpt of the authentication protocol relevant for an attack.

[1] This encryption is the first protocol step to verify that the PCD shares the correct key with the PICC and is therefore always executed

1.2 Related Work

Oren and Shamir [21] 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 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. The consequences for real-world systems remain unclear, as the antenna and analogue frontend are separated from the digital circuitry, while on a real RFID tag, these components are intrinsically tied together. Moreover, in their attack, the trigger signal is artificially generated before the S-Box operation, thus ensuring perfect time alignment. Finally, as the clock signal is generated independently from the reader field using a local oscillator, the carrier is uncorrelated with the actual power consumption of the AES hardware and hence easy to remove.

In contrast, we now face the real-world situation, i.e., have no knowledge on the internal implementation details of the contactless smartcard, cannot rely on precise triggering for alignment and analyse a black box with all RFID and cryptographic circuitry closely packed on one silicon die. Therefore, we will describe all relevant steps to analyse an unknown RFID device in practise, starting from the measurement setup and including the extensive profiling that is required to gain insight into the operation of the device, before the actual side-channel attack can take place. First steps towards an EM attack on contactless smartcards were proposed in [6], e.g., an x-ray photograph reveals the position of the chip and antenna inside the plastic packaging.

2 Side-Channel Analysis

Differential Power Analyis (DPA) was originally proposed in [16] 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 RF carrier of the reader that is required for the operation. Anyway, even a successful invasive attack can obviously 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 attack analysing the information contained in the EM emanation of a device is called *Differential Electro-Magnetic Analysis* (DEMA) [3].

The analogue signal, i.e., the EM leakage in case of a DEMA, is digitized and recorded as a discrete and quantized 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* $d(K_s, x_l)$, 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 *Normalized Correlation Coefficient* between the predicted and recorded values for one point in time n and a fixed key K_s:

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

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 analyzing the resulting $\Delta(K_s, 0) \ldots \Delta(K_s, N-1)$, 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

Modelling Power Analysis 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 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.

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

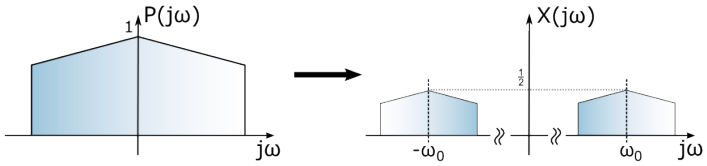

Fig. 2. Frequency spectrum of the carrier signal ω_0 and the assumed information leakage for remote power analysis

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[3].

3 Measurement Equipment

The core of our proposed DEMA measurement setup 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 utilized near-field EM probes are covered in this section.

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 €.

Thus, we were able to implement the authentication protocol that is used by the contactless smartcard under attack. Contrary to commercial RFID readers,

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

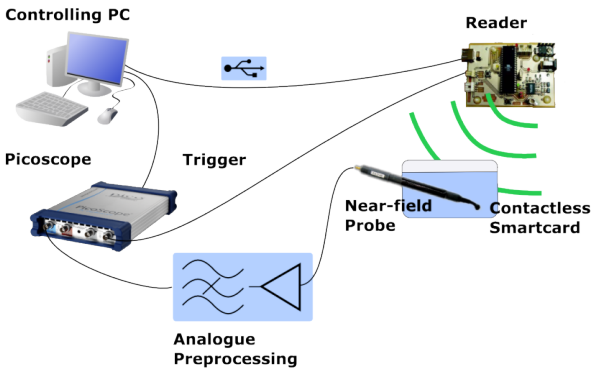

Fig. 3. Measurement setup

our self-built device allows for sending chosen challenges during the authentication and can provide a trigger signal for starting the measurement, thereby facilitating a DEMA.

Scope The *Picoscope 5204* is a dual-channel storage USB-oscilloscope [22], 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, alone the minimum input range of $\pm$ 100 mV might pose a problem in the context of DEMA attacks, where small voltage changes need to be detected with a high resolution.

Probes For measurements of the EM-field emanated by the contactless smartcard, a *RF-U 5-2* probe [17] 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 [17] 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. Consequently, the carrier frequency has to be suppressed as much as possible to increase the resolution available for the side-channel information.

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 digitizing 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 utilized for the signal of interest, requiring removal of the carrier and amplification of the small side-channel information in the analogue domain, before digitizing.

For minimizing 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 smartcard. The self-evident 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 immobilizers. In the following, we detail on our realization of the phase shifter and the subtraction by means of a standard active adder, passing one signal shifted in phase by 180°.

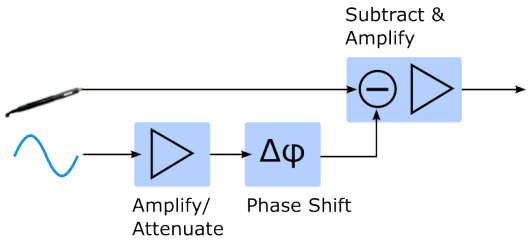

Fig. 4. Block diagram for removing the unwanted carrier frequency of the reader

Phase Shifter The phase-shift is performed by an adjustable *allpass filter* (Fig. 5) which ideally does not alter the amplitude but only the phase, depending on the center frequency ω_g. Its transfer function is:

$$H_{allpass}(s) = \frac{\omega_g - s}{\omega_g + s}$$

with $\omega_g = \frac{1}{RC}$. The magnitude response $|H_{allpass}(s)| = 1$ is constant for all frequencies, while the phase is given as $\varphi(\omega) = \arctan \frac{-2\omega\omega_g}{\omega_g^2 - \omega^2}$. This phase response is plotted for different values of $f_g = \frac{\omega_g}{2\pi}$ in Fig. 6.

By varying the value of C (or R) and thus shifting ω_g, a fixed-frequency sine can be delayed by a specifiable amount. Around the center frequency, the phase shift is almost linear, so that frequency components in this range are subject to the same time shift - the *group delay* $\tau_g = -\frac{\partial\varphi}{\partial\omega}$ then remains almost constant.

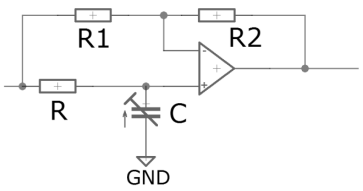

Fig. 5. Active allpass filter circuit

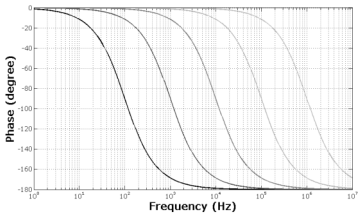

Fig. 6. Phase response for $f_0 = 100\,\text{Hz}$, 1 kHz, 10 kHz, 100 kHz, 1 MHz

4 Practical Results

By performing a full authentication and reproducing the responses[4] of the cryptographically enabled contactless smartcard under attack on the PC, we can verify that a standard (3)DES [2] is used for the encryption of the challenge according to Fig. 1. As mentioned in Sect. 1.1, we also observed that the card unconditionally encrypts any plaintext sent to it.

On the basis of these observations, the analysis of the contactless smartcard is further detailed in this section. It will turn out that digitally preprocessing the recorded traces is vital to achieve meaningful results by means of CPA.

4.1 Trace Preprocessing

As the recorded raw traces do not expose any distinctive pattern, digital preprocessing is applied in order to identify interesting patterns useful for the precise alignment of the traces before conducting a CPA attack.

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 spectral analysis and the well-known fact that

[4] Note that the secret key of the implementation can be changed by us and is hence known.

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 (Figure 7, following [25]). The raw trace is first rectified, then low-passed FIR-filtered. An additional high-pass IIR filter removes the DC offset and low-frequency noise. Good values for the filter cutoff frequencies $f_{lowpass}$ and $f_{highpass}$ were determined experimentally and are given in Sect. 4.2.

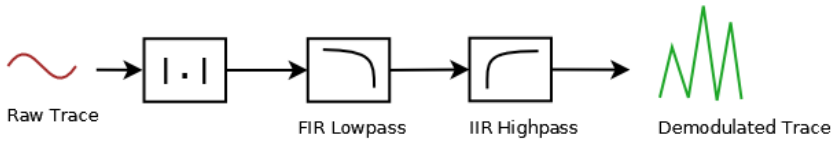

Fig. 7. Digital amplitude demodulator

Figure 8 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, Figure 9 shows the same trace without demodulation.

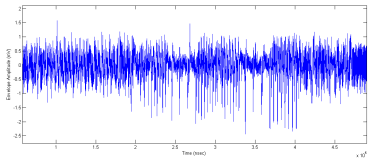

Fig. 8. Demodulated trace (50 kHz - 2 MHz)

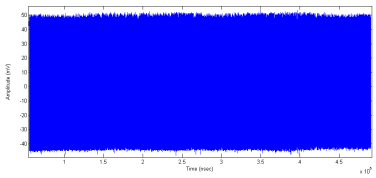

Fig. 9. Raw oscilloscope trace

Trace Alignment Correct alignment of traces is of particular importance for performing a CPA on time-domain signals. We therefore select a short reference pattern in a demodulated *reference trace* and locate it in all other traces by finding the shift that minimizes 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.

4.2 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:

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 Figure 10 and 11.

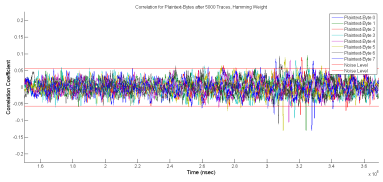

Fig. 10. Correlation coefficients for plaintext bytes (second block, before 3DES encryption)

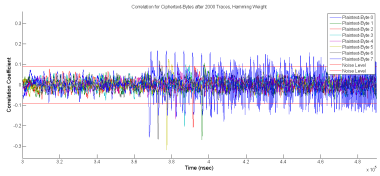

Fig. 11. Correlation coefficients for ciphertext bytes (after 3DES encryption)

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

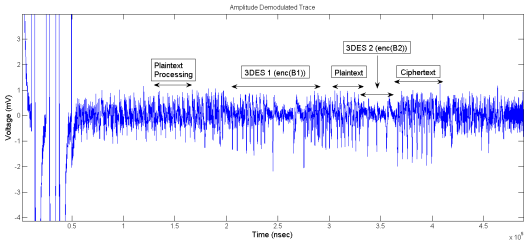

Fig. 12. Overview over operations in amplitude-demodulated trace

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. Figure 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[5].

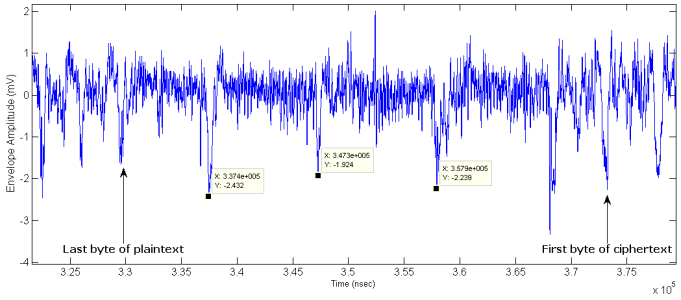

Fig. 13. Part of trace with 3DES encryption, filtered with $f_{lowpass} = 8$ MHz, $f_{highpass} = 50$ kHz

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. Figure 14 shows the correlation for all eight DES 4-bit S-Box outputs for $L = 150000$ traces, where the correlation coefficient for the correct subkey is highlighted and the horizontal lines indicate the theoretical noise level $\frac{4}{\sqrt{L}}$ (cf. [18]). For S-Box 1

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

and 3, correlation peaks with maximum amplitude for the correct key candidate occur at a position which we consider as the start point of the first DES. This result allows us to reduce the number of possible candidates for the complete key k_1 from 56 bit to 44 bit.

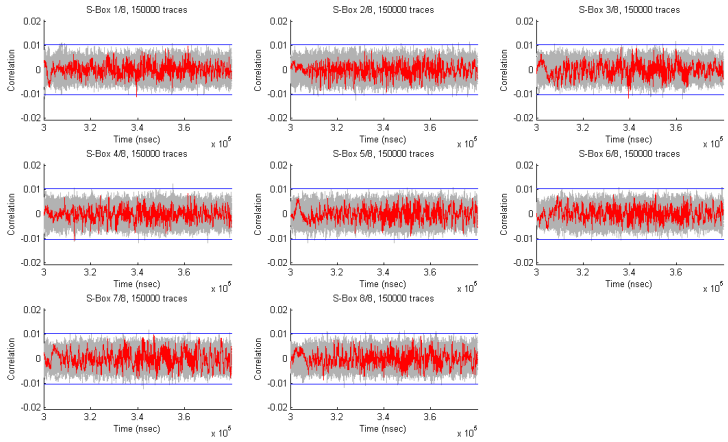

Fig. 14. Correlation coefficients for CPA with alignment to second peak after 150000 traces, $f_{lowpass} = 8$ MHz, $f_{highpass} = 50$ kHz

As the attack works for a subset of S-Boxes, we conclude that no masking scheme ([18]) 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 Figure 13 vary[6].

In order to improve the alignment, we extract local maxima and minima from the trace part belonging to the first DES operation, assign them to equally spaced *bins* and perform the CPA *binwise*. The correlation coefficients for this experiment are given in Figure 15, where the y-axis has been normalized to the theoretical noise level, 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, 2, 3, 4 and 8, recovering 30 bits of k_1 and leaving only 26 bit which can be easily recovered by exhaustive search.

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

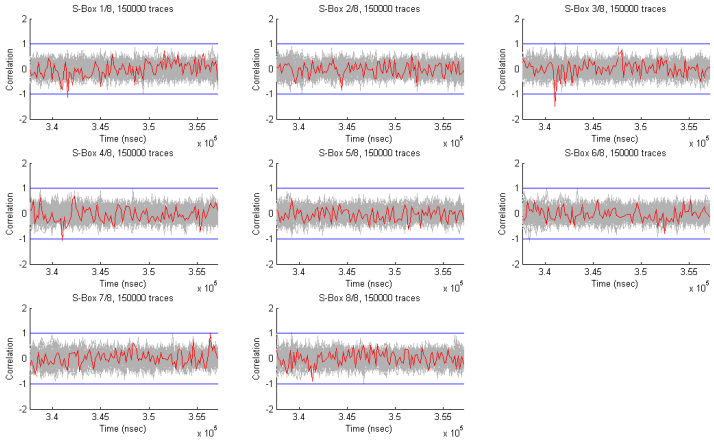

Fig. 15. Correlation coefficients for binwise CPA with peak extraction after 150000 traces, $f_{lowpass} = 8$ MHz, $f_{highpass} = 50$ kHz

5 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 ([26], [23]), on the other hand, we optimize 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 quantizes a full scale of 100 mV. Hence, only approx. 100 out of 256 values are currently used for digitizing 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.

6 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, realized 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. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM Side-Channel(s). In *CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, pages 29–45, London, UK, 2003. Springer-Verlag.
4. 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 *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.
5. D. Carluccio. Electromagnetic Side Channel Analysis for Embedded Crypto Devices. Master's thesis, Ruhr Universität Bochum, 2005.
6. D. Carluccio, K. Lemke, and C. Paar. Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. RFIDSec05 Workshop on RFID and Lightweight Crypto, July 2005. `http://events.iaik.tugraz.at/RFIDandLightweightCrypto05/RFID-SlidesandProceedings/Carluccio-EMSideChannel.pdf`.
7. N. T. Courtois, K. Nohl, and S. O'Neil. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166, 2008.
8. T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer, 2008.

9. K. Finkenzeller. *RFID-Handbuch*. Hanser Fachbuchverlag, Third edition, October 2002.
10. F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. Dismantling MIFARE Classic. In S. Jajodia and J. López, editors, *ESORICS 2008*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114. Springer, 2008.
11. S. Haykin. *Communications Systems*, chapter 8. Wiley, 2nd edition, 1983.
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*, 1st edition, 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 edition, February 2001.
15. 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.
16. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 388–397, London, UK, 1999. Springer-Verlag.
17. Langer EMV-Technik. Details of Near Field Probe Set RF 2. Web resource. `http://www.langer-emv.de/en/produkte/prod_rf2.htm`.
18. S. Mangard, E. Oswald, and T. Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Springer-Verlag, Secaucus, NJ, USA, 2007.
19. Microchip. HCS410, KeeLoq Code Hopping Encoder and Transponder Data Sheet. `http://ww1.microchip.com/downloads/en/DeviceDoc/40158e.pdf`.
20. NXP. *Data Sheet of Mifare Classic 4k chip MF1ICS70*, 2008.
21. 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`.
22. Pico Technology. PicoScope 5200 USB PC Oscilloscopes, 2008.
23. 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.
24. H. Plötz. Mifare Classic - Eine Analyse der Implementierung. Master's thesis, Humboldt-Universität zu Berlin, 2008.
25. K. S. Shanmugam. *Digital & Analog Communication Systems*, chapter 8.3.2. Wiley-India, 2006.
26. C. C. Tiu. A New Frequency-Based Side Channel Attack for Embedded Systems. Master's thesis, University of Waterloo, 2005.