Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World*

David Oswald and Christof Paar

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

Abstract. With the advent of side-channel analysis, implementations of mathematically secure ciphers face a new threat: by exploiting the physical characteristics of a device, adversaries are able to break algorithms such as AES or Triple-DES (3DES), for which no efficient analytical or brute-force attacks exist. In this paper, we demonstrate practical, non-invasive side-channel attacks on the Mifare DESFire MF3ICD40 contactless smartcard, a 3DES-based alternative to the cryptanalytically weak Mifare Classic [9,25]. We detail on how to recover the complete 112-bit secret key of the employed 3DES algorithm, using non-invasive power analysis and template attacks. Our methods can be put into practice at a low cost with standard equipment, thus posing a severe threat to many real-world applications that employ the DESFire MF3ICD40 smartcard.

Keywords: contactless smartcard, side-channel analyis, templates, DESFire.

1 Introduction

Radio Frequency Identification (RFID) technology has become the basis for numerous large-scale, security-relevant applications, including public transport, wireless payment, access control, or digital identification [39]. The information stored on RFID smartcards, e.g., personal data, or cash balance, is often highly sensitive — however, the access to the air interface and to the device itself is virtually impossible to control. Hence, most modern RFIDs feature cryptographic mechanisms, including encryption and authentication, in order to thwart attacks such as eavesdropping, manipulation, or cloning of a smartcard.

Mifare DESFire MF3ICD40 is a contactless smartcard featuring a cryptographic engine for authentication and encryption based on (Triple-)DES. The smartcard is employed in several large payment and public transport systems around the world, e.g., the Czech railway in-karta [7], the Australian myki card [36], or the Clippercard used in San Francisco [40]. In the course of our

* 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.

B. Preneel and T. Takagi (Eds.): CHES 2011, LNCS 6917, pp. 207–222, 2011.

research, we also noticed many smaller installations, e.g., for mobile payment or access control, that are based on the Mifare DESFire MF3ICD40. From a mathematical point of view, the employed 3DES cipher is secure, because no efficient cryptanalytical attacks are known. Thus, in this paper, we focus on *side-channel attacks*, i.e., methods that target the physical implementation of the cryptographic primitive in soft- or hardware. Using non-invasive and hence non-detectable measurement of the electro-magnetic (EM) emanations of the device, we are able to completely recover the secret 112-bit master key and thus to, for example, read out, manipulate, or duplicate the contents of a Mifare DESFire MF3ICD40 card.

1.1 Related Work

The idea of exploiting physical side-channels to attack hardware implementations of secure ciphers was first put forward in [20] in 1998. Since then, a lot of research has been conducted in this area, with important contributions including the analysis using the EM emanation of a device [1] or the application of the correlation coefficient in Correlation Power Analysis (CPA) to better model the physical behaviour of Integrated Circuits (ICs) [2]. At CHES 2002, the authors of [5] proposed the use of machine learning techniques such as pattern recognition for Side-Channel Analysis (SCA) and coined the notion of "template attacks". Several extensions and improvements for this approach have been suggested in the last few years, cf. [31,33,35].

The susceptibility of ciphers running on RFID devices towards SCA was initially shown in [12,30]: the authors present attacks on a white-box software implementation of the AES executed by a standard, unprotected microcontroller (μC) on a self-made prototype RFID, evaluating techniques to overcome problems such as misaligment of the measured signals.

With respect to the application of SCA to break commercial, *real-world* devices, few papers have been published, as most research in this field is carried out by evaluation labs behind closed doors. The potential impact of SCA in practice was demonstrated by the complete break of the proprietary KeeLoq system presented at CRYPTO 2008 [8]. Results for the black-box analysis of a contactless smartcard are given in [17], proposing a leakage model for RFIDs that forms the basis for our analyses and is outlined in Sect. 2. However, the authors are unable to recover the complete key and do not disclose to which device their attacks apply. In [18], the application of analog demodulation for SCA of RFIDs is presented for the first time. The measurement setup used in the present paper is an extension of the setup described in [18].

1.2 Contribution of this Paper

The work presented in this paper is of practical nature: we highlight the relevance of SCA in the real-world by demonstrating the first full key-recovery attack on the popular Mifare DESFire MF3ICD40 smartcard reported in the literature. Doing so, we point out problems and obstacles that occur when conducting SCA in practice which are often neglected in academic papers. In addition, we

present the — to our knowledge — first application of template attacks to break cryptographic RFIDs, allowing for potentially very fast determination of the secret key. The remainder of this paper is structured as follows: in Sect. 2, we give the signal-theoretical background of our measurement setup for RFID devices, which is presented in Sect. 3. We then practically apply the developed techniques to analyze the smartcard in Sect. 4, detailing on the internal hardware structure of the device. In Sect. 5, we extend our findings and present a successful full key-recovery attack on the 3DES engine. After that, in Sect. 6, we demonstrate a different approach for obtaining the secret key based on template attacks to eavesdrop on the internal databus. Finally, we conclude in Sect. 7, discussing the implications of our findings for commercial applications and giving directions for further research.

2 Demodulation for SCA of Contactless Smartcards

For contactless smartcards, the energy for operation is supplied wirelessly using magnetic coupling. As proposed in [17,18], this gives rise to a different leakage mechanism compared to contact-based devices. In a similar manner as for regular data transmission, the 13.56 MHz field generated by the reader is load-modulated by the power consumption of an RFID[1].

Let the power consumption of the target device be given as $p(t) = P_{const} + p_{dyn}(t)$, where P_{const} is the constant part and $p_{dyn}(t)$ the fraction caused by internal operations, e.g., intermediate values being manipulated during a cryptographic operation. Usually, the dynamic portion of the power consumption is far weaker than the constant part, i.e., $|p_{dyn}(t)| << P_{const}$. The leakage exploitable for an SCA thus heavily depends on the quality of the isolation and amplification of $p_{dyn}(t)$. As mentioned, in an RFID setting, the amplitude of the reader signal is modulated by $p(t)$, i.e., $s(t) = p(t) \cdot \cos(\omega_r \cdot t) = (P_{const} + p_{dyn}(t)) \cdot \cos(\omega_r \cdot t)$.

where $\omega_r = 2\pi\ f_r$, $f_r = 13.56$ MHz is the standard carrier frequency. Clearly, the extraction of $p(t)$ (and especially of the weak dynamic portion) from $s(t)$ can be done using amplitude demodulation, cf. for instance [34]. In practice, "incoherent" techniques (i.e., for which a separate, unmodulated carrier signal is not necessary) based on rectification (often called envelope detection) are very common, and in this paper, we follow that approach as well. The principle due to which rectification can be used for demodulation is best understood in the frequency domain, following [27]. First note that, as stated above, $|p_{dyn}(t)| << P_{const}$ and hence, $|s(t)| = |P_{const} + p_{dyn}(t)| \cdot |\cos(\omega_r \cdot t)| = (P_{const} + p_{dyn}(t)) \cdot |\cos(\omega_r \cdot t)|$.

Let $P(j\omega) = \mathrm{DFT}\{p(t)\} = \mathrm{DFT}\{P_{const} + p_{dyn}(t)\}$ denote the frequency domain representation of the signal that is to be reconstructed. By expanding $|\cos(\omega_r \cdot t)|$ using its Fourier series, one obtains the spectrum of the rectified signal:

[1] However, for data transmission, the fluctuations of the EM field are intentional and far stronger in magnitude.

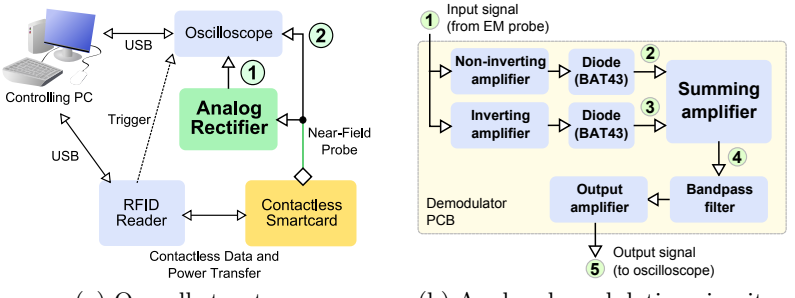
$$\mathrm{DFT}\left\{|s\left(t\right)|\right\} = \mathrm{DFT}\left\{p\left(t\right) \cdot |\cos\left(\omega_r \cdot t\right)|\right\} = \mathrm{DFT}\left\{p\left(t\right) \cdot \frac{2}{\pi} \sum_{\nu=-\infty}^{\infty} \frac{(-1)^{\nu}}{1-4\nu^2} e^{j2\nu\omega_r t}\right\}$$
$$= \frac{2}{\pi} \sum_{\nu=-\infty}^{\infty} \frac{(-1)^{\nu}}{1-4\nu^2} \mathrm{DFT}\left\{p\left(t\right) \cdot e^{j2\nu\omega_r t}\right\} = \frac{2}{\pi} \sum_{\nu=-\infty}^{\infty} \frac{(-1)^{\nu}}{1-4\nu^2} P\left(j\omega - j2\nu\omega_r\right)$$

The rectified signal is essentially formed by the spectrum of $P_{const} + p_{dyn}\left(t\right)$, which, however, is (scaled and) repeated at all even multiples of the carrier frequency $\omega_r = 2\pi$ 13.56 MHz. Thus, the first repetition occurs at 27.12 MHz.

Using a lowpass filter with a cutoff frequency less than 13.56 MHz isolates the desired signal[2] $p\left(t\right)$.

3 Measurement Setup

For the analysis of the DESFire MF3ICD40, we extended the measurement environment of [18]. Fig. 1a gives an overview over the components of our setup. A custom, freely programmable RFID reader [16] compliant to ISO 14443 [13,14] and ISO 15693 [15] supplies the contactless smartcard (from now on occasionally referred to as Device Under Test (DUT)) with power and handles the communication, for instance to trigger an encryption operation.



(a) Overall structure (b) Analog demodulation circuitry

Fig. 1. Measurement setup

A wide-band EM probe with a suitable pre-amplifier [21] captures the magnetic near-field in the proximity of the IC, resulting in a "raw" signal (denoted as ② in Fig. 1a) which is dominated by the 13.56 MHz carrier frequency of the reader. On the one hand, this signal is directly recorded and stored using a Picoscope 5204 Digital Storage Oscilloscope (DSO) [29] at a sample rate of 500 MHz, on the other hand, it is passed to an analog demodulator that performs the operations outlined in Sect. 2 to facilitate SCA, resulting in the signal ① in Fig. 1a. The central PC controls the measurement process, i.e., prepares and sends commands to the DUT via the RFID reader and acquires and stores the resulting side-channel signals ① and ② (from now on referred to as *traces*.

[2] The constant term P_{const} can be removed with a highpass filter that only blocks the DC and very low-frequency components.

As explained in Sect. 2, analog demodulation is required to separate the actual power consumption signal from the carrier signal and to thereby improve the quality of the (exploitable) side-channel leakage. Accordingly, we developed a custom Printed Circuit Board (PCB) comprising a full-wave rectifier and appropriate filter circuitry to perform the incoherent demodulation approach. Fig. 1b shows the basic structure of the demodulation circuitry. The full schematics are given in an appendix in the extended version of this paper [28]. The full-wave rectifier is formed by two isolated half-wave rectifiers, each employing an BAT43 Schottky diode [38]. To rectify the negative part of the input ①, the signal is first inverted and then rectified by the diode, yielding signal ③ in Fig. 1b. For the positive portion, the buffer amplifier only provides isolation of the input signal and driving of the corresponding diode, but does not perform inversion to produce signal ②. The two resulting parts ② and ③ are then added to form the full-wave rectified output ④.

A third-order LC bandpass filter extracts the baseband part, i.e., the portion of the spectrum centered around 0 Hz. In our case, the -3 dB frequency was specified to 12 Mhz. Additionally, the filter also suppresses frequency components below 10 kHz to remove the constant part of the modulating signal. Finally, the output amplifier adjusts the amplitude of the signal in order to optimally utilize the minimum input range of ± 100 mV of the Picoscope and drives a 50 Ω load, i.e., a suitable coaxial cable.

In the case that a raw signal (i.e., ② in Fig. 1a) is used for SCA, it was shown in [17] that the demodulation has to be performed digitally in order to conduct a successful CPA, i.e., digital pre-processing is mandatory. For the output of the analog demodulator, digitally filtering the output signal ① is optional, however, might help to further reduce the 13.56 MHz frequency component still present due to certain characteristics of the analog circuits. For a more detailed description of the effects of the respective processing techniques, cf. [18].

4 Practical Results: Profiling of Mifare DESFire MF3ICD40

Mifare DESFire MF3ICD40 [26] is a contactless smartcard initially designed by the semicondutor division of Philips, which became the separate company NXP in 2006. The card is compliant to parts 1-4 of the ISO 14443A standard. A communication with the card can be performed in plain, with an appended Message Authentication Code (MAC), or with full data encryption using 3DES. The device offers 4 kByte of storage that can be assigned to up to 28 different applications, whereas each application may hold a maximum of 16 files. Depending on the configuration of the access rights, a mutual authentication protocol has to be carried out before accessing the card, ensuring that the symmetric 3DES keys of the card k_C and of the reader k_R are identical.

According to specifications found on the internet, the smartcard features several functions to thwart physical attacks such as SCA, fault injection, or reverse-engineering: the IC is built using asynchronous circuits and employs a

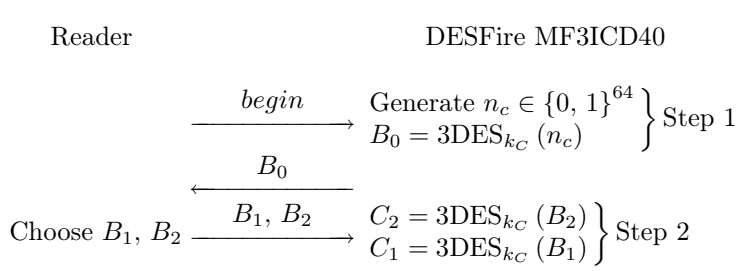


Fig. 2. Exerpt of the Mifare DESFire authentication protocol relevant for SCA

custom, asynchronous μC design based on the 8051 architectures. Besides, all digital units (i.e., control logic, cryptographic engine etc.) are "intermingled" so that no functional block are discernible, a technology called "glue logic" by the vendor. Note that all results in this paper do not directly apply to the newer AES-based variant DESFire EV1. The authentication protocol of the DESFire MF3ICD40 has been disclosed and can for instance be found in [19,4]. For the purpose of SCA, we refer to a simplified version in the following, given in Fig. 2. $k_C = (k_{C,1}, k_{C,2})$ is the 128-bit 3DES master key (including the parity bits) used by the DUT, whereas the two halfs are of size 64 bit each, i.e., $k_{C,1}, k_{C,2} \in \{0, 1\}^{64}$. $3\text{DES}_{k_C}(x) = \text{DES}_{k_{C,1}}\left(\text{DES}^{-1}_{k_{C,2}}\left(\text{DES}_{k_{C,1}}(x)\right)\right)$ denotes a 3DES encryption of a 64-bit value x in Encrypt-Decrypt-Encrypt (EDE) mode. The full command set[3] has been implemented for our custom reader mentioned in Sect. 3.

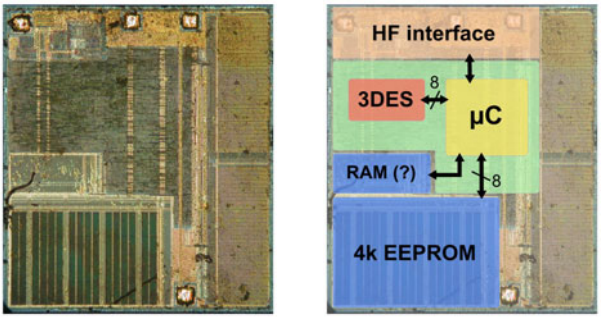
Initially, we are facing a *black-box* scenario, i.e., have (apart from the command set and the specifications in the datasheet) no further knowledge on the inner workings of the device. Hence, *profiling* to map different portions of a power trace to steps of the operation of the DUT (e.g., a data transfer or an encryption operation) is mandatory before attempting to perform real attacks on cryptographic operations. As a first step, we dismantled the IC, took magnified photographs of the silicon die, cf. Fig. 3a, and tried to distinguish the different parts of the circuit. The hypothetical structure depicted in Fig. 3b is a result of this optical inspection and the findings reported in the remainder of this section.

To prepare the actual SCA, we recorded side-channel traces for both steps of the authentication protocol, separately varying either the key of the card k_C or the values for B_1 and B_2 in step 2. To estimate the effect of our analog processing circuitry, we both store the "raw" signals before demodulation (② in Fig. 1a) and the result of the demodulation process (① in Fig. 1a).

We then perform several CPAs to locate the points in time in the power traces at which the known values for k_C, B_1 and B_2 (and the encryption results C_1, C_2[4]) are processed. Employing an 8-bit Hamming weight model, all mentioned

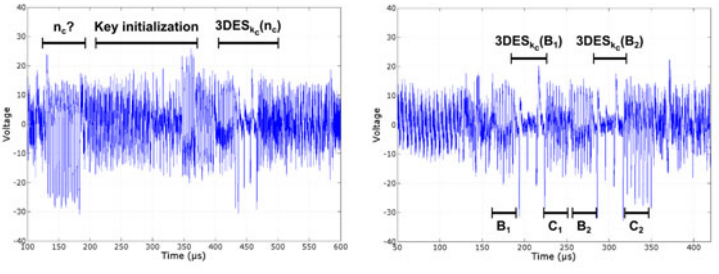
[3] Including the necessary commands for changing the key, performing a full authentication etc.

[4] As we know k_C during the profiling phase, we can predict these values that are never output by the DUT.



(a) IC photo (b) Hypothetical structure

Fig. 3. The DESFire MF3ICD40 IC



(a) Step 1 (b) Step 2

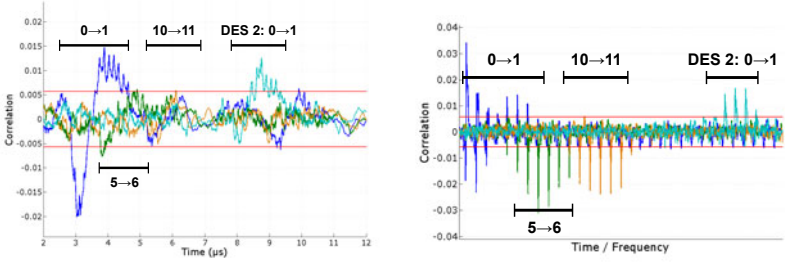
Fig. 4. Annotated traces during the authentication protocol (after analog processing)

values can be precisely pinpointed, cf. Fig. 4. We observed a stable value of ≈ 0.15 for the respective correlation coefficient after around 1,000 traces. This suggests that internally, an 8-bit data bus is used to connect the μC to the memory and the cryptographic engine, yielding the structure of Fig. 3b. For each byte transfered over this bus, a distinct peak appears in the power trace, whereas the distance between two such peaks indicates an internal bus frequency of $f_{bus} \approx 282.5\,\text{kHz} = {}^{13.56}/_{48}\,\text{MHz}$. Note that the peaks for data bus transfers later in a trace, e.g. for B_2 or C_2 in Fig. 4b, are often *misaligned*, i.e., their exact position slightly varies from execution to execution. The reason for this behaviour lies in the non-constant execution time of a 3DES operation, which is further detailed in Sect. 5. Hence, it is necessary to re-align the respective parts (for instance, using standard pattern matching approaches [23]) to obtain a significant correlation.

5 Practical Attack: CPA of the 3DES Engine

Having located the input and output values of the 3DES encryption, we now focus on this part to perform the recovery of the secret key. Comparing this part for several traces, we notice some interesting properties: first, the length of one DES operation varies from execution to execution, even if the input data and the key are kept constant. This hints at a countermeasure based on randomization in time being employed to thwart CPA. We further address this problem in Sect. 5.1. Second, the amplitude of the traces is significantly lower during the supposed encryption, which coincides with the statements in the available DESFire documentation that a dedicated low-power hardware engine performs the cryptographic operation.

To prepare the actual key-recovery, we first attempt to characterize the leakage of the 3DES engine and find a suitable power model by correlating with the full intermediate 64-bit states[5] using a known key. Conducting several experiments, we found the Hamming distance model to yield a significant correlation and were able to locate the first few rounds of the DES, as depicted in Fig. 5 for rounds 0→1, 5→6, 10→11, and 0→1 of the second DES iteration.



(a) Time domain (b) Frequency domain

Fig. 5. Correlation coefficients for the Hamming distances between rounds of the 3DES, 500,000 traces

However, as evident from Fig. 5a, this approach only is able to locate the first few rounds (with decreasing correlation), supposedly due to the randomization mentioned above. Statistically analyzing the length of the first DES iteration using 100,000 traces, we observe that one iteration takes 8.2 μs on average. This duration varies in discrete steps of 290 ns over a total range from 6.9 μs to 9.1 μs. This suggests that the cryptographic engine executes up to eight ($\lceil {}^{(9.1-6.9)}/_{0.29} \rceil$) "dummy" rounds based on an internal Random Number Generator (RNG) to impede SCA.

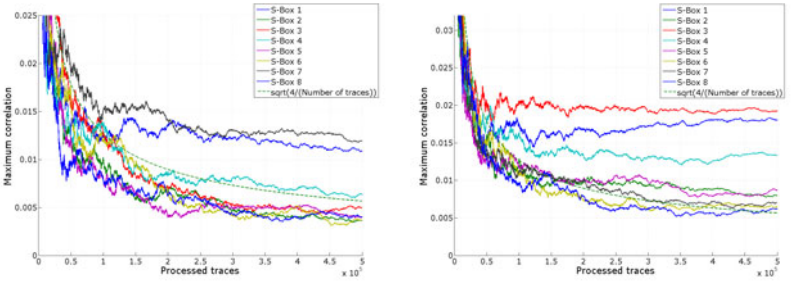
[5] i.e., $\left(L_i^{(n)}, R_i^{(n)}\right)$, $0 \leq i \leq 16$, $n \in \{1, 2, 3\}$, where n denotes the Single-DES iteration within the complete 3DES, for details cf. [24].

To solve this problem, we tried out methods to overcome misalignment suggested in the literature, including comb filtering or windowing [6], Dynamic Time Warping (DTW) [37], and Differential Frequency Analysis (DFA) [10,30]. Our results show DFA to yield the best overall correlation, using the following steps: before correlating with the prediction of the power model, a trace is partitioned into (overlapping) segments, these segments are transformed to the frequency domain with the Discrete Fourier Transform (DFT), and the phase information is discarded by taking the absolute value of the DFT coefficients. The optimal value for the size of each segment was determined to be 1.5 μs, with an overlap of 75 % between adjacent segments. The strongest leakage occurs for low frequencies, hence, we limited the analysed spectral range to 0...16 MHz. Fig. 5b shows the according correlation coefficients for the respective rounds of the cipher — in contrast to the analysis in the time domain, all rounds are clearly distinguishable.

In order to quantify the improvement caused by the employed analog and digital processing methods, we compare the maximum correlation coefficient over the number of traces for the 32-bit Hamming distance $R_0 \rightarrow R_1$ (again, using a known key), with a detailed plot of the respective values given in an appendix in [28]. In all cases, the correlation converges rather quickly to a significant value far greater than $4/\sqrt{\text{No. of traces}}$, yet, a distinct gain due to both analog and digital processing is discernible: while the digitally demodulated traces without re-alignment by DFA result in a stable value of ≈ 0.015, the combination of analog demodulation with DFA yields ≈ 0.032, that is, an improvement by a factor of two. As a result, we utilize these pre-processing techniques for the full key-recovery presented in Sect. 5.1, taking the fact into account that in this case, we have to target each 4-bit S-Box output separately, so smaller overall correlations are to be expected.

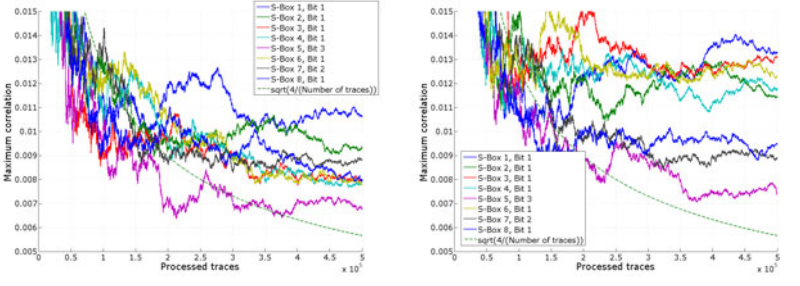
5.1 Full Key-Recovery

Based on the findings of the profiling phase, a CPA can be mounted to obtain the full 3DES key by recovering the 6-bit part of the round key for each S-Box, starting with the first round of the first DES. To make use of all available information, a natural choice is to target the full 4-bit output of each S-Box in the Hamming distance $R_0 \rightarrow R_1$. However, for the case of the DESFire MF3ICD40, this turned out to be problematic: Fig. 6 shows the maximum correlation coefficients for the correct key candidate for a standard CPA in the time domain and DFA in the frequency domain, respectively. Although the complete key is discernible after $\approx$ 450,000 traces in Fig. 6b, the stable value for the correlation significantly differs depending on the S-Box, causing the attack to fail for five S-Boxes when performed without re-alignment by means of DFA, cf. Fig. 6a.Testing other prediction functions, a single-bit CPA (which is equivalent to the classic Differential Power Analysis (DPA)) proved to be the most successful approach. As depicted in Fig. 7, for each S-Box there is at least one bit providing sufficient leakage to allow our attack to succeed after approx. 250,000 traces and 350,000 traces with and without DFA, respectively.



(a) Time domain (b) Frequency domain

Fig. 6. Maximum correlation coefficient for the correct key, 4-bit model, Hamming distance $R_0 \rightarrow R_1$ for all S-Boxes



(a) Time domain (b) Frequency domain

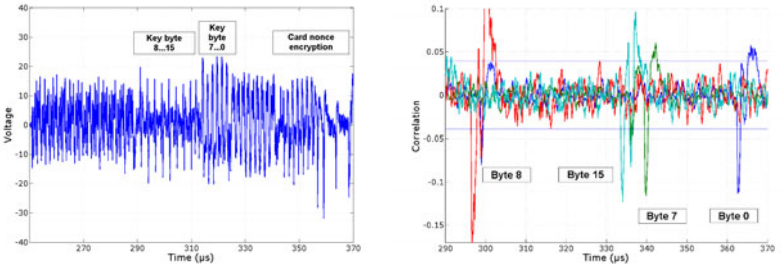
Fig. 7. Maximum correlation coefficient for the correct key, 1-bit model, Hamming distance $R_0 \rightarrow R_1$ for all S-Boxes

For the sake of optical clarity, the maximum correlation for *wrong* key candidates has been omitted in the above figures. Yet, we performed the actual key-recovery computing these correlations as well and verified that in all cases, the correlation for the wrong candidates is below $4/\sqrt{\text{No. of traces}}$, i.e., there are no "ghost peaks" that might interfere with the retreival of the correct key. Besides, the results are not limited to the first round of the first DES: the analysis equivalently works for other rounds of the first DES (to recover the remaining eight bit of $k_{C,1}$) and for the second DES iteration[6] (to obtain $k_{C,2}$). In summary, as a result of this section, we conclude that the extraction of the complete secret 3DES key from a Mifare DESFire MF3ICD40 can be carried out with approx. 250,000 traces, which can be collected in approx. seven hours using our current measurement setup.

[6] In this case, alignment to the start pattern of this operation is necessary.

6 Practical Attack: Template Attack on the Key Transfer

As observed during the profiling phase described in Sect. 4, the internal databus of the DUT seems to be completely unprotected and exhibits a far stronger Hamming weight leakage than the cryptographic engine analyzed in Sect. 5. Thus, *template attacks* to obtain information on internal values transfered over this bus can be expected to work with a far lower number of traces compared to a CPA. Of special interest is the initialization of the cryptographic engine before the start of the actual 3DES operation: our analyses shows that the transfer of the *secret key* can be identified in the power trace of the DUT after the reader has sent the initial `begin` command in the authentication protocol (that is, during Step 1 in Fig. 2). Fig. 8a depicts a trace for the loading of the key and indicates



(a) Side-channel trace (b) Correlation

Fig. 8. Transfer of the 3DES key over the internal databus

the internal order of operation: by repeatedly changing the key and performing a CPA using the Hamming weight of each key byte, we found out that the 3DES key is initialized in two steps. First, the upper eight byte ($k_{C,2}$) are transfered, starting with the least significant byte. After that, the lower half $k_{C,1}$ (i.e., byte 0 ... 7) is transmitted, this time in reverse byte order. In both cases, the (redundant) parity bits are not removed prior to the key transfer, suggesting that they are discarded internally by the cryptographic engine. Fig. 8b exemplarily shows the corresponding correlation peaks for the key bytes 0 (blue), 7 (green), 8 (red) and 15 (cyan), allowing to exactly pinpoint the time instants at which information on a specific byte is leaking.

In contrast to CPA, template attacks require a profiling phase, i.e., a step during which the DUT is under full control of the adversary to estimate the statistical relation between the observable random variables — in our case the respective points in time of a trace — and the internal states that are to be distinguished (here, the value of a key byte). The resulting *training set* is then used to recover the desired values from a *test set*, i.e., traces for which the value of the key byte is considered unknown.

To systematically evaluate the success rate of template attacks for the case of the transfer of the key on the Mifare DESFire MF3ICD40, we obtain 8,000

traces for each possible value of a targeted key byte[7]. Here, we only address byte 0 and 15, however, our results hold for all other bytes as well. 4,000 traces are used for the training set, while the other 4,000 form the test set — in total, to cover all 256 possible values for a byte, we acquired $2 \cdot 256 \cdot 4{,}000 = 2{,}048{,}000$ traces. Again, we also compare the quality of analog demodulation compared to its digital equivalent and hence recorded traces both before and after the analog circuitry. Let $\mathcal{S}_b^{training} = \{\boldsymbol{t}_{b,0}, \ldots, \boldsymbol{t}_{b,3999}\}$ be the training set and $\mathcal{S}_b^{test} = \{\boldsymbol{t}_{b,4000}, \ldots, \boldsymbol{t}_{b,7999}\}$ the test set , where $\boldsymbol{t}_{b,n}$ denotes the n'th trace for a specific byte $0 \leq b < 256$, i.e., a $K \times 1$ vector of measured values. Given $\mathcal{S}^{test}$ for a fixed but unknown key — in our case, the test set for some key byte value b — the comparision to the training data is carried out as outlined in Alg. 1.

Algorithm 1. Template creation and matching procedure

for $b = 0 \ldots 255$ **do**
  $(\boldsymbol{\mu}_b,\ \Sigma_b) \leftarrow \text{estimate}\left(\mathcal{S}_b^{training}\right)$
end for
$\overline{\Sigma} \leftarrow \frac{1}{256}\sum_{b=0}^{255} \Sigma_b$
$(\boldsymbol{\mu}',\ \Sigma') \leftarrow \text{estimate}\left(\mathcal{S}^{test}\right)$
for $b = 0 \ldots 255$ **do**
  $\delta_b \leftarrow \text{distance}\left(\boldsymbol{\mu}_b,\ \Sigma_b,\ \overline{\Sigma},\ \boldsymbol{\mu}',\ \Sigma'\right)$
end for
return $\underset{b}{\text{argmin}}\, \delta_b$

estimate $(\cdot)$ is an algorithm that estimates the (pointwise) sample mean and covariance matrix from the respective set of traces, e.g., using the standard empirical formulae [41]. distance $(\cdot)$ is a suitable distance measure based on the previously estimated statistical parameters. The value for the key byte b that minimizes the chosen distance measure is then returned as the most probable candidate for the given test traces. We exemplarily selected the following distance measures:

Difference of means. The simplest case only evaluates the norm of the pointwise difference of the class means, i.e., $\sum_{k=1}^{K} \left(\boldsymbol{\mu}_b(k) - \boldsymbol{\mu}'(k)\right)^2$, discarding any information on the (co-)variances

Euclidean. Assuming that the covariance matrix is diagonal, one obtains the Euclidean distance, $\sum_{k=1}^{K} \left(\boldsymbol{\mu}_b(k) - \boldsymbol{\mu}'(k)\right)^2 / \Sigma_b(k,k)$, for which the differences are normalized using the pointwise variance

Mahalanobis. Taking all parameters of the distribution into account, the Mahalanobis distance [22] is given as $\left(\boldsymbol{\mu}_b(k) - \boldsymbol{\mu}'(k)\right)^T \overline{\Sigma^{-1}} \left(\boldsymbol{\mu}_b(k) - \boldsymbol{\mu}'(k)\right)$

Table 1 summarizes the results of our template analysis both with (Table 1a) and without analog preprocessing (Table 1b). The average bit error rates were

[7] The training and test sets were acquired in separate measurement campaigns to rule out effects due to slightly varying environmental conditions.

Table 1. Average bit error rates for the key recovery based on templates using 4,000 traces

(a) With analog processing

Keybyte	Distance	Bit error rate
0 ($k_{C,1}$)	DiffMeans	2.07
	Euclidean	2.14
	Mahalanobis	**1.77**
15 ($k_{C,2}$)	DiffMeans	0.55
	Euclidean	**0.51**
	Mahalanobis	0.64

(b) Without analog processing

Keybyte	Distance	Bit error rate
0 ($k_{C,1}$)	DiffMeans	2.89
	Euclidean	2.66
	Mahalanobis	**2.4**
15 ($k_{C,2}$)	DiffMeans	1.55
	Euclidean	**0.71**
	Mahalanobis	1.22

estimated by applying Alg. 1 for each byte, using the corresponding test set $\mathcal{S}_b^{test}$ and computing the Hamming distance between the detected and the actual value b. Evidently, the upper half $k_{C,2}$ can be recovered with significantly less error than $k_{C,1}$, which interestingly admits a rather different leakage characteristic. In either case, the remaining uncertainty can be accounted for using exhaustive search over the key candidates, starting with the ones having the smallest distance to the training set.

Limitations. Compared to the CPA presented in Sect. 5, the key recovery by means of templates might be carried out with far less traces and hence within a very short time[8], thus potentially posing a severe security threat in a scenario in which an adversary either has to extract many different keys (e.g., due to a key distribution mechanism) or faces a constant risk of being detected. However, due to the necessity for a profiling phase, implementing the approach in practice turns out to be highly problematic: for the results given in Table 1, we could employ the same DUT, whereas in a real-world attack, the profiling and the attack device are different. In our experiments with different cards, we observed significantly differing leakage characteristics, even if the measurement setup (i.e., the positions of the EM probe and the DUT on the antenna) was kept exactly fixed. At present, we are therefore not able to apply the profiling data to a different card, however, we are currently evaluating calibration approaches and improved classifiers (e.g., using Principal Component Analysis (PCA) [35]). We were already able to obtain correct matchings at least for a subset of all possible key values.

7 Conclusion

We show several SCA attacks to fully recover the 3DES key of the Mifare DESFire MF3ICD40, employing standard equipment in an academic measurement setup that can be built for approx. 3000 $. As we figured out the details of the

[8] In our current setup, recording 4,000 traces is a matter of minutes.

implementation of the DUT, the attacks can be realized within a few hours (e.g., to collect approx. 250,000 traces for a CPA), and hence pose a severe threat to the security of DESFire-based real-world systems.

System integrators should be aware of the new security risks that arise from the presented attacks and can no longer rely on the mathematical security of the used 3DES cipher. Hence, in order to avoid, e.g., manipulation or cloning of smartcards used in payment or access control solutions, proper actions have to be taken: on the one hand, multi-level countermeasures in the backend allow to minimize the threat even if the underlying RFID platform is insecure, cf. [32]. For long-term security and when developing new systems, we recommend to use certified smartcards, e.g., the AES-based Mifare DESFire EV1, which passed an EAL-4+ evaluation [3] and which comprises SCA countermeasures that thwart the attacks presented in this paper.

Having demonstrated the susceptibility of the DESFire MF3ICD40 towards SCA, there are several interesting directions for further research to consider: first, the SCA could be improved in order to work with a smaller number of traces, for instance, employing different alignment methods or model-independent distinguishers like Mutual Information Analyis (MIA) [11]. Apart from that, extensions of the proposed template attack may allow to reduce the error rate or to utilize the templates generated with a profiling device to recover the unknown key of another DESFire MF3ICD40 card. Also, a combination of CPA and templates could further reduce the required number of traces. Finally, the developed techniques can be applied in order to attempt attacks on different cryptographic RFIDs, possibly including (certified) high-security smartcards.

References

1. 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)
2. 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)
3. BSI – German Ministry of Security. Mifare DESFire8 MF3ICD81 Public Evaluation Documentation. Electronic resource (October 2008)
4. Carluccio, D.: Electromagnetic Side Channel Analysis for Embedded Crypto Devices. Master's thesis, Ruhr-University Bochum (2005)
5. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Kaliski Jr., B.S., Koç, Ç.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2003)
6. Clavier, C., Coron, J.-S., Dabbous, N.: Differential Power Analysis in the Presence of Hardware Countermeasures. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 13–48. Springer, Heidelberg (2000)
7. Czech Railways. In-karta (March 2011), `http://www.inkarta.cz/`
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. 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., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 97–114. Springer, Heidelberg (2008)
10. Gebotys, C.H., Ho, S., Tiu, C.C.: EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 250–264. Springer, Heidelberg (2005)
11. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual Information Analysis – A Generic Side-Channel Distinguisher. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)
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. 320–333. Springer, Heidelberg (2007)
13. ISO. ISO/IEC 14443-3: Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 3: Initialization and Anticollision (February 2001)
14. ISO. ISO/IEC 14443-4: Identification cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 4: Transmission Protocol (February 2001)
15. ISO. ISO/IEC 15693-3: Identification Cards – Contactless Integrated Circuit Cards – Vicinity Cards – Part 3: Anticollision and Transmission Protocol (April 2009)
16. 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)
17. Kasper, T., Oswald, D., Paar, C.: EM Side-Channel Attacks on Commercial Contactless Smartcards Using Low-Cost Equipment. In: Youm, H.Y., Yung, M. (eds.) WISA 2009. LNCS, vol. 5932, pp. 79–93. Springer, Heidelberg (2009)
18. Kasper, T., Oswald, D., Paar, C.: Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation. Springer LNCS Proceedings of RFIDSec 2011, Northampton, USA (to appear)
19. Kasper, T., von Maurich, I., Oswald, D., Paar, C.: Chameleon: A versatile emulator for contactless smartcards. In: Rhee, K.-H. (ed.) ICISC 2010. LNCS, vol. 6829, pp. 189–206. Springer, Heidelberg (to appear)
20. 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)
21. Langer EMV-Technik. Details of Near Field Probe Set RF 2. Website
22. Mahalanobis, P.C.: On the Generalised Distance in Statistics. In: Proceedings National Institute of Science, India, vol. 2, pp. 49–55 (April 1936)
23. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
24. NIST. FIPS 46-3 Data Encryption Standard (DES), `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`
25. Nohl, K., Evans, D., Plötz, H.: Reverse-Engineering a Cryptographic RFID Tag. In: USENIX Security Symposium, pp. 185–194. USENIX Association (2008)
26. NXP. Mifare DESFire Contactless Multi-Application IC with DES and 3DES Security MF3ICD40 (April 2004)
27. Ochs, K.: Transmission of Digital Signals. Lecture notes (2006)
28. Oswald, D., Paar, C.: Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World — Extended Version (2011), `http://www.emsec.rub.de/research/publications/`
29. Pico Technology. PicoScope 5200 USB PC Oscilloscopes (2008)

30. 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)
31. Rechberger, C., Oswald, E.: Practical Template Attacks. In: Lim, C.H., Yung, M. (eds.) WISA 2004. LNCS, vol. 3325, pp. 443–457. Springer, Heidelberg (2005)
32. Rohr, A., Nohl, K., Plötz, H.: Establishing Security Best Practices in Access Control (September 2010), http://www.srlabs.de/pub/acs
33. Schindler, W., Lemke, K., Paar, C.: A Stochastic Model for Differential Side Channel Cryptanalysis. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 30–46. Springer, Heidelberg (2005)
34. Schwartz, M., Bennett, W.R., Stein, S.: Communication Systems and Techniques. Wiley, Chichester (1966)
35. Standaert, F.-X., Archambeau, C.: Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 411–425. Springer, Heidelberg (2008)
36. State Government Victoria. myki (March 2011), http://www.myki.com.au/
37. van Woudenberg, J.G.J., Witteman, M.F., Bakker, B.: Improving Differential Power Analysis by Elastic Alignment. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 104–119. Springer, Heidelberg (2011)
38. Vishay Semiconductors, Inc. BAT43 Schottky Diode Datasheet
39. Wikipedia. Contactless Smart Card — Wikipedia, The Free Encyclopedia (2011) (accessed March 5, 2011)
40. Wikipedia. MIFARE — Wikipedia, The Free Encyclopedia (2011) (accessed March 25, 2011)
41. Wikipedia. Sample Mean and Sample Covariance — Wikipedia, The Free Encyclopedia (2011) (accessed April 1, 2011)