Electromagnetic Side Channel Analysis for Embedded Crypto Devices

Dario Carluccio

March, 29th 2005

Diploma Thesis
Ruhr-University Bochum

BOCHVM · RVHR-VNIVERSITÄT

Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

Advised by:
Prof. Dr.-Ing. Christof Paar
Prof. Dr. rer. nat. Jörg Schwenk

Statement

I hereby certify that the work presented in this thesis is my own work and that to the best of my knowledge it is original except where indicated by reference to other authors.

Hiermit versichere ich, dass ich meine Diplomarbeit selber verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie Zitate kenntlich gemacht habe.

Datum   Dario Carluccio

Contents

Statement ii

1 Introduction 1

2 Block Ciphers 2
- 2.1 Data Encryption Standard (DES) 2
  - 2.1.1 DES–Algorithm 2
  - 2.1.2 The Feistel–Function 3
  - 2.1.3 The Round–Keys 4
  - 2.1.4 Triple DES 5
- 2.2 Advanced Encryption Standard (AES) 6
  - 2.2.1 The ByteSub transformation 7
  - 2.2.2 The ShiftRow transformation 7
  - 2.2.3 The MixColumn transformation 7
  - 2.2.4 The Round Key addition 7

3 Side Channel Cryptanalysis 8
- 3.1 Power Analysis 9
- 3.2 Introduction to Differential Power Analysis (DPA) 9
  - 3.2.1 Difference of Means Test 10
  - 3.2.2 T–Test 11
  - 3.2.3 Correlation Method 11

4 Theoretical Electromagnetic (EM) Background 12
- 4.1 Maxwell Equations 12
- 4.2 EM–Radiation 13
- 4.3 Receiving EM–Radiation 14
  - 4.3.1 Electric Field Coupled Antennas 15
  - 4.3.2 Magnetic Field Coupled Antennas 15
- 4.4 Expected Frequency and Bandwidth 16
- 4.5 Impedance and Standing Wave Ratio (SWR) 16
- 4.6 Noise 18

4.7 Using a Receiver . . . 19
4.8 Summary . . . 19

5 Antennas 20
5.1 Electric Field Coupled Antennas . . . 20
5.2 Magnetic Field Coupled Antennas . . . 20
5.3 Near-Field Probes . . . 21

6 AES on Atmel-Microcontroller Based Smartcard 23
6.1 Atmel ATmega–Microcontroller . . . 23
6.2 SOSSE AES-Implementation . . . 26
6.3 Measuring Setup . . . 26
6.4 Results . . . 28

7 RFID Card 32
7.1 RFID Communication Protocol . . . 33
7.2 Authenticate–Command . . . 34
7.3 RFID Measurement Setup . . . 39
7.4 Measurement Improvement . . . 39
7.5 EM Analysis . . . 40
7.6 Further Directions . . . 42

8 Conclusion 43

A Photographies 44

B Bibliography 46

List of Figures

2.1 DES–Algorithm . . . 3
2.2 Feistel–Function . . . 4
2.3 Key Schedule Calculation . . . 5
2.4 AES–Algorithm . . . 6

4.1 E– and H–Field of Elementary–Dipole [1] . . . 14
4.2 Fourier–Transformation of Rectangular Signal . . . 17

5.1 Near–Field–Probe RF U 5–2 . . . 21
5.2 Antennas . . . 22

6.1 Harvard Architecture on Atmel ATmega163 [2] . . . 25
6.2 Side Channel Measurement Setup . . . 27
6.3 DPA and DEMA Results on AES . . . 30
6.4 DEMA Results on AES . . . 31

7.1 RFID-Transmission . . . 32
7.2 RFID-Modulation Codes . . . 33
7.3 Modified Miller Code . . . 34
7.4 Manchester Code . . . 35
7.5 Authentication Protocol $k_c \neq k_r$ . . . 36
7.6 Authentication Protocol . . . 37
7.7 EM Radiation (Near Field Probe) . . . 41

Nomenclature

ADC	Analog–to–Digital Converter
AES	Advanced Encryption Standard
ALU	Arithmetic and Logical Unit
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CBC	Cipher-block chaining
CPU	Central Processing Unit
DCA	Differential CryptAnalysis
DEMA	Differential EM Analysis
DES	Data Encryption Standard
DPA	Differential Power Analysis
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EFF	Electronic Frontier Foundation
EM	ElectroMagnetic
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GF	Galois Fields
I/O	Input / Output
IEC	International Electrotechnical Commission

ISO	International Organization for Standardization
LCA	Linear CryptAnalysis
NASA	National Aeronautics and Space Administration
PWM	Pulse–Width Modulation
RAM	Random Access Memory
RFID	Radio Frequency IDentification
RISC	Reduced Instruction Set Computer
S–Box	Substitution Box
SEMA	Simple EM Analysis
SNR	Signal to Noise Ratio
SOSSE	Simple Operating System for Smartcard Education
SPA	Simple Power Analysis
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
SWR	Standing Wave Ratio
UART	Universal Asynchronous Receiver Transmitter
XOR	Exclusive disjunction

1 Introduction

Low cost cryptographic devices have been a booming market in the past years. These devices are in use for security services such as ticketing, access–control, and electronic payment.The security services often require that the owner of the device is not able to read out or modify the secret data (cryptographic keys and unique IDs) stored.

The interfaces for communication, clock and power supply are either galvanic (contact-based) or radio frequency (RF) based.

Side channel cryptanalysis includes elegant methods to extract cryptographic keys by exploiting the physical leakage of the device. Real hardware has different physical information leakage on the operation it is performing. Such information can be the execution–time, the power consumption, the electromagnetic radiation and other physical observables. An attacker can use this side channel information in addition to the data used for mathematical analysis and could be able to extract secret information, especially the key.

It was reported by Karine Gandolfi at al. [3] that unintended EM radiation is emitted by crypto devices and can be used as side channel information to compromise secret information such as the key. They distinguish SEMA (Simple EM Analysis) and DEMA (Differential EM Analysis) according to previous works of Paul Kocher at al. [4] who introduced the power analysis attacks SPA (Simple Power Analysis) and DPA (Differential Power Analysis). Most EM analysis ([3], [5], [6], [7]) have been done on known hardware, e.g., self programmed microcontrollers and FPGAs.

In this work I give experimental results for an Atmel ATmega–163 smartcard based microcontroller as well as for the Mifare DESFire, which is a state of the art contactless smartcard. The ATmega-163 (contact-based) smartcard was programmed with a known AES implementation. The DESFire card is used by the NASA [8] and the U.S. Department of Interior [9] to secure access to facilities. It is also used by 1. FC Köln [10] for contactless ticketing for FIFA World Cup 2006. I chose this device, because it uses a well established cipher, namely Triple DES.

This work studies the EM leakage that is observable during the computation of a block cipher at these two devices. The EM analysis is of special importance for RF based cryptographic devices, as it is the only possibility for side channel analysis without modifieing the device.

2 Block Ciphers

A cipher is an algorithm designed to encrypt and decrypt data. A block cipher is a type of symmetric key cipher which operates on groups of bits of a fixed length, termed blocks. This contradicts to stream ciphers, which encrypt each bit of the data individually before moving on to the next bit.

Basically a block cipher is composed of two algorithms, one for encryption Enc, and another for decryption $\mathsf{Dec} = \mathsf{Enc}^{-1}$. Both algorithms have two inputs: an N_D-bit data block (d) and an N_K-bit key (k). The result is an N_D-bit output block.

Decryption is the inverse function of encryption, so that for any data block d and key k:

$$\mathsf{Enc}^{-1}(\mathsf{Enc}(d;k);k) = d$$

For each key k, $\mathsf{Enc}(d;k)$ is a one permutation out of $(2^{N_d})!$ possible permutations. Note: The key size and the block size need not to be identical.

2.1 Data Encryption Standard (DES)

The Data Encryption Standard was approved as a federal standard in November 1976 and published in January 1977 as FIPS PUB 46 [11]. It was subsequently reaffirmed as the standard in 1983, 1988 (revised as FIPS-46-1), 1993 (FIPS-46-2) [12], and again in 1998 (FIPS-46-3) [13], where the latter is prescribing "Triple DES".

DES is a widespread and internationally used block cipher algorithm. It is designed to encrypt and decrypt blocks of data consisting of 64 bits with a 56-bit key.

2.1.1 DES–Algorithm

The algorithm's structure is shown in Figure 2.1: There is an initial and final permutation, termed IP and IP^{-1}, which are inverse to each other. They have no cryptographic significance, but were apparently included in order to facilitate loading blocks in and out of mid-1970s hardware.

Between them there are 16 identical stages of processing, termed rounds. The block is splitted into two 32–bit halves and processed alternately; this is known as the Feistel scheme.

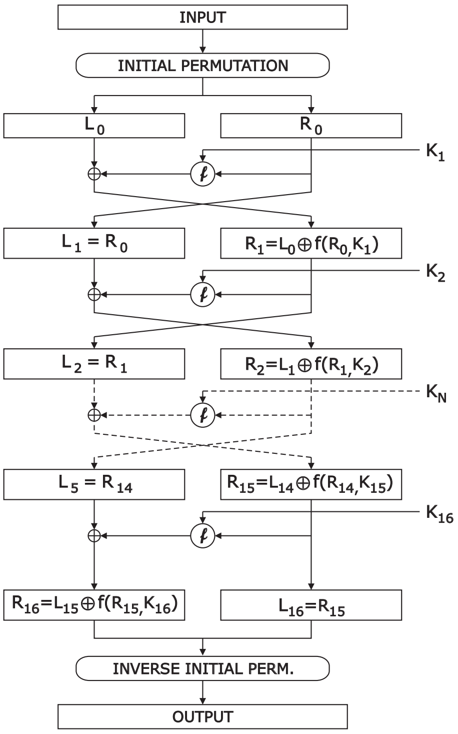


Figure 2.1: DES–Algorithm

2.1.2 The Feistel–Function

The Feistel structure effects that en– and decryption are very similar processes, the only difference is that the subkeys are applied in the reverse order during decryption. Thus there is no need for separate encryption and decryption algorithms.

The Feistel–function processes the right block (R–register, 32-bits) together with the key for the actual round. The output is then combined with the left block (L–register, 32–bits) using an XOR–operation. After that the two registers are swapped before the next round.

The Feistel–function, shown in Figure 2.2, operates on the actual R–register. It consists of four stages:

1. Expansion: the 32–bit input–block is expanded to 48 bits using the expansion function, denoted by E in the diagram, by duplicating some specified bits.

2. Key mixing: the 48-bit result is combined with a 48-bit round–key K_r using an XOR operation.

3. Substitution: the block is divided into eight 6–bit values before processing 8 substitution boxes (S–Boxes). Each of the eight S–Boxes transforms six input bits into four output bits according to a non–linear transformation. The S–Boxes provide the core of the security of DES thus this is the only non–linear operation. Without the S–Boxes, the cipher would be linear, and trivially breakable.

4. Permutation: at the end, the 32 outputs from the eight S–boxes are rearranged according to a fixed permutation (P)

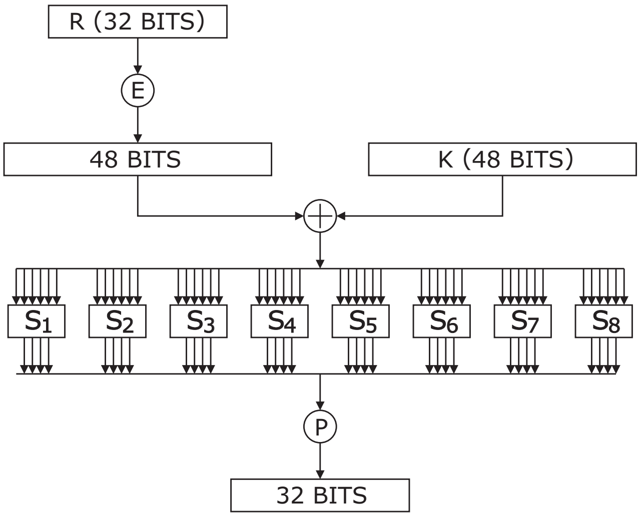


Figure 2.2: Feistel–Function

2.1.3 The Round–Keys

The sixteen 48–bit round–keys, one for each round, are derived from the main key using the schedule algorithm shown in figure 2.3.

Initially, 56 bits of the 64–bit key are selected by the permuted choice 1 (PC-1), the remaining eight bits are discarded. The 56 bits are divided into two halves, that are denotated as the C– and D–register. In the successive rounds, both registers are rotated left as specified for each round, by one or two bits. Then the 48–bit round–key is selected by permuted choice 2 (PC-2). Each bit is used in approximately 14 out of the 16 round–keys.

The key schedule for decryption must generate the keys in the reverse order, and the rotations are to the right.

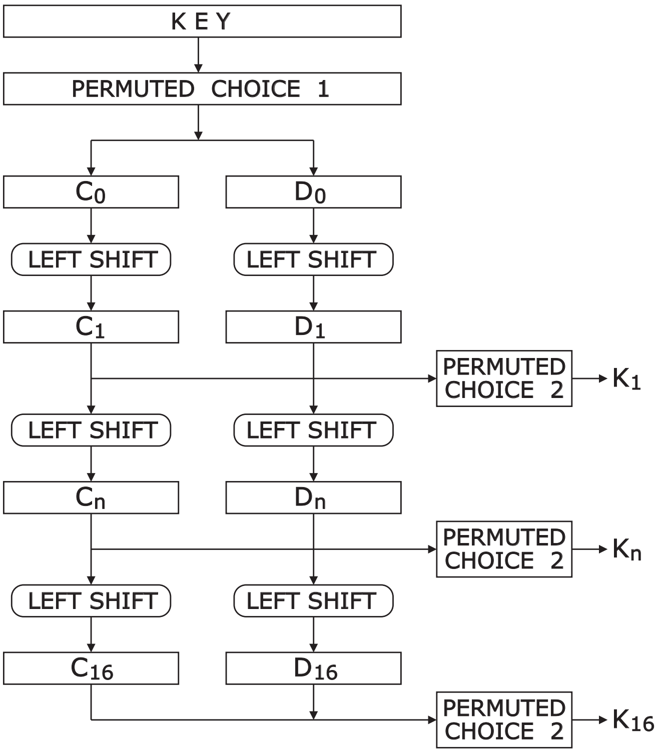


Figure 2.3: Key Schedule Calculation

2.1.4 Triple DES

Due to the very small key size of 56-bit, DES has been broken in July 1998, by the EFF's DES cracker[1] in 56 hours, and in January 1999 by Deep Crack and distributed.net[2] in 22 hours and 15 minutes.

In order to overcome the problems due to the short key size, DES has been reaffirmed as FIPS 46-3, which specifies the preferred use of Triple DES.

Triple DES is, as the name indicates, composed of three consecutive DES operations, which are performed according to the following scheme:

$$C = DES_{K3}\Big(DES_{K2}^{-1}\big(DES_{K1}(P)\big)\Big)$$

Thus Triple DES has a key length of 168-bits (three 56-bit DES keys), but often only two different 56-bit DES keys (112 bits) are used. In this case $K1$ equals $K3$.

[1] http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker

[2] http://www.distributed.net

2.2 Advanced Encryption Standard (AES)

The Advanced Encryption Standard was published in November 2001, as FIPS PUB 197 [14]. This block cipher is also known as Rijndael algorithm. The cipher was developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen.

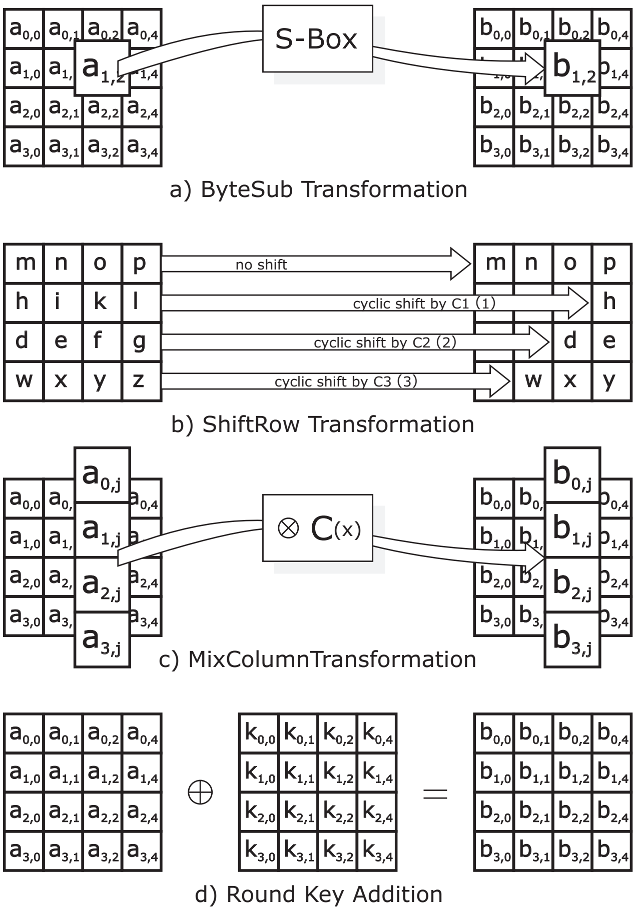


Figure 2.4: AES–Algorithm

AES has a fixed block size of 128 bits and a key size of either 128, 192 or 256 bits. It operates on a 4x4 array of bytes, termed the state. For encryption, each round of AES (besides the last round) consists of four stages:

1. ByteSub transformation: a non-linear substitution step where each byte is replaced with another.
2. ShiftRows: a transposition step where each row of the state is shifted cyclically a certain number of steps.

3. MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.
4. AddRoundKey: each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

2.2.1 The ByteSub transformation

The ByteSub transformation manipulates each byte using a non–linear 8-bit Substitution-Box. The S–Box used is derived from the inverse function over $GF(2^8)$[3], known to have good non-linear properties. To avoid attacks based on simple algebraic properties, the S–Box is constructed by combining an inverse function with an invertible affine transformation.

2.2.2 The ShiftRow transformation

In ShiftRow, the state–rows are cyclically shifted with different offsets. Row 0 is not shifted, Row 1 is shifted over C1 bytes, row 2 over C2 bytes and row 3 over C3 bytes. The shift offsets C1, C2 and C3 depend on the block length which is 128, 196 or 256. For a block size of 128–bit the values are:

$$C1 = 1$$
$$C2 = 2$$
$$C3 = 3$$

For other block sizes refer to [14].

2.2.3 The MixColumn transformation

In the MixColumn step, the bytes of each column are combined using an invertible linear transformation. Together with ShiftRows, this provides the diffusion in the cipher. Each column is treated as a polynomial over $GF(2^8)$ and is then multiplied with a fixed polynomial c(x) modulo $(x^4 + 1)$.

2.2.4 The Round Key addition

In the Round Key addition, the subkey is combined with the state. For each round, a subkey is derived from the main key using the key schedule (see [14]); each subkey is of the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

[3] for further reading about Galois Fields refer to, e.g., [15]

3 Side Channel Cryptanalysis

In this chapter I introduce the origin of side channels and how this information leakage can be used by an attacker to break a crypto device.

To evaluate the security of a cryptographic system against possible attacks, methods like differential cryptanalysis [16] and linear cryptanalysis [17] have been developed. They give assurance that an algorithm is practically secure against all known mathematical attacks.

But cryptographic methods are not restricted to an mathematical object, they are also used in real applications. Many low–cost devices are implemented in an embedded hardware such as smartcards. The advantage is that the user of these cards can use them like a physical key. They can, e.g., be used to authenticate the holder of the smartcard.

The smartcards are used in many environments, e.g., for physical access control, ticketing and electronic payment applications.

Some smartcards are also used together with Personal Computers, because those can not be treated as a secure environment. It is not wise to store secret information or perform secret operations on a computer where malicious software, which is designed to spy out those information, can be executed.

External hardware like smartcards are used to store secret keys and to perform cryptographic operations such as encrypting and decrypting in a secure environment.

The main target of hardware like smartcards is to keep secret keys in a tamper resistant environment, so that an attacker is sufficiently prevented from physical attacks. A typical smartcard solution is a microcontroller embedded in a card which can communicate with a specific protocol. The crypto–algorithm itself can be implemented either in software or in additional hardware, like a co–processor.

The key is stored in the non–volatile memory of the smartcard and there is no function foreseen in the communication protocol to get the key out again. So the card can be used to do the crypto operation, but even if the attacker has physical access to the card it shall not be feasible to extract the key.

3.1 Power Analysis

In 1998 Paul Kocher et al. [4] introduced a method to exploit the power consumption of a crypto device as an information channel.

This Differential Power Analysis (DPA) is a very efficient side channel attack that uses statistical analysis. It is essential for DPA to know the plaintext or the ciphertext of the measurements.

The attacker issues a model for the dependency of the power consumption, on the data and instruction the device is performing. Such a device contains logic gates, which are basically built of transistors. During operation, the gates of the transistors are charged and discharged. A common model is that the power consumption which is the total of all charges and discharges, is related to the Hamming weight[1] and/or the Hamming distance[2] of data, which is computed.

As part of the algorithm the device has to perform non–linear operations, especially the non–linear substitutions which are basic building blocks for encryption of DES and AES. The idea is to test all key hypotheses which affect the output of the selected S–Box. For AES there are 256 hypotheses, and for DES 64 hypotheses, as the DES S–Box maps 6 input bits to 4 output bits.

If random uniformly distributed plaintexts are used as inputs to the algorithm, the inputs of the S–Boxes are also random uniformly distributed. The output of the S–Box will be random uniformly distributed, too. Each bit of the output of the S–Box has the same probability to be set or cleared. But if we make an assumption on parts of the key (subkey), which affects the entry to the S–Box and if this is correct, we can predict the value of this bit.

As mentioned above DPA uses the power consumption of the crypto device as a side channel; if the electromagnetic radiation is used this is called DEMA [5]. DEMA uses the same statistical tests as DPA.

3.2 Introduction to Differential Power Analysis (DPA)

We measure n times the power consumption of the device operating the crypto–algorithm by sampling this values $P(x_n, t)$ with a scope. Then these curves are saved together with either the plaintext or the ciphertext x_n on which the device computes the operation.

[1] The Hamming weight of a string of bits is the number of 1's in it.

[2] Hamming distance is the number of positions in two strings of equal length for which the corresponding elements are different.

For each S–Box we now set up the key hypotheses for all key bits that affect the input of the chosen S–Box.[3]

We choose one bit of the output of the S–Box and predict its value for the known plaintext and the key hypothesis. A selection function $D(x_n, b, k)$ computes the value of the selected bit b according to the plaintext x_n and the key hypothesis k. It returns 1 when b is set and 0 when b is cleared[4].

For each hypothesis we check for statistical dependencies between $P(x_n, t)$ and $D(x_n, b, k)$ at each point of time t.

The output of the statistical test $\Delta_k(t)$ will be:

$$\begin{cases} \Delta(k,t) \overset{n\to\infty}{\longrightarrow} 0 & \text{for all } t \text{ if } k \text{ is wrong} \\ \\ \Delta(k,t) \overset{n\to\infty}{\longrightarrow} C \neq 0 & \text{for some } t \text{ if k is true} \end{cases} \tag{3.1}$$

It is possible that on some wrong key hypotheses $\Delta(k, t) = C_1 \neq 0$ for some t, the criterium for the true key hypothesis is that it has the maximum value for C.

In this work the following statistical tests are used to compute $\Delta_k(t)$.

3.2.1 Difference of Means Test

This test was presented by Paul Kocher et al. [4]. It computes the differences between the average values of two groups:

$$\Delta_{DoM}(ks, t) = \overline{P_{0,k}(t)} - \overline{P_{1,k}(t)} \tag{3.2}$$

The two groups are built by

$$P_{0,k} = \{P(x_n, t) | D(x_n, b, k) = 0\}$$

and

$$P_{1,k} = \{P(x_n, t) | D(x_n, b, k) = 1\}$$

Let $n_{d,k}$ be the number of elements in the corresponding group where $D(x_n, b, k) = d$, then the average value $\overline{P_{d,k}(t)}$ is computed as follows:

$$\overline{P_{d,k}(t)} = \frac{1}{n_{d,k}} \sum_{i=1}^{n_{d,k}} P_{x_i,t}$$

[3] In the case that we know only the ciphertext and this does not effect the input we can swap S–Box Input and Output in the following instructions.

[4] Note, that it might be more appropriate to guess multiple-bits instead of one single bit to enhance the signal to noise ratio.

3.2.2 T–Test

This method was introduced by Manfred Aigner and Elisabeth Oswald in their Power Analysis tutorial [18]. It extends the Difference of Means Test by including the variance of the two sets.

$$\Delta_T(ks,t) = \frac{\overline{P_{0,k}(t)} - \overline{P_{1,k}(t)}}{S_P}\sqrt{\frac{n_{0,k}\cdot n_{1,k}}{n_{0,k}+n_{1,k}}} \tag{3.3}$$

with

$$S_P(k,t) = \sqrt{\frac{(n_{0,k}-1)\ var_0(k,t) + (n_{1,k}-1)\ var_1(k,t)}{n_{0,k}+n_{1,k}-2}} \tag{3.4}$$

where $n_{0,k}$ and $n_{1,k}$ are the number of elements in the corresponding group and

$$var_d(k,t) = \frac{1}{n_{d,k-1}}\sum_n \left(P(x_n,t) - \overline{P_{d,k}(t)}\right)^2 \tag{3.5}$$

This test is preferred, if the variance of the power consumption data varies significantly at different points in time of the measurement.

3.2.3 Correlation Method

This method is also given in the Power Analysis tutorial [18] and also in miscellaneous statistic books.

The correlation coefficient $c(k,t)$ is a function of plaintext x_n at the time t. It correlates the selection function $D(x_n,b,k)$ depending on the key hypothesis k and the power consumption $P_{x_n,t}$ of each measurement.

$$c(k,t) = \frac{\sum_n \left(D(x_n,b,k) - \overline{D(x_n,b,k)}\right)\ \left(P(x_n,t) - \overline{P(x_n,t)}\right)}{\sqrt{\sum_n \left(D(x_n,b,k) - \overline{D(x_n,b,k)}\right)^2}\ \sqrt{\sum_n \left(P(x_n,t) - \overline{P(x_n,t)}\right)^2}}$$

In case of complete positive correlation of the two signals $D(x_n,k)$ and $P(x_n,t_0)$ at one point of time, the correlation coefficient is 1.0. It is $c(k,t)=0$ if the signals are uncorrelated. The minimum value for the correlation coefficient is -1.0, in this case the key–hypothesis is true, but the model for the relation between the power consumption and the observed bit–state is anti–proportional.

4 Theoretical Electromagnetic (EM) Background

As this work studies the EM–side channels, I will give an introduction to the origin of EM emissions and the behavior of the electric and magnetic components of the generated radiation. Furthermore, I will introduce some basics of high frequency measurement techniques which are important for this setup.

Some basic antenna types are discussed and finally I will explain the expected frequency and bandwidth of the radiation and the importance of noise.

4.1 Maxwell Equations

The EM–theory is completely described by Maxwell's equations. They build a set of four equations, that describe the behavior of the electric and magnetic fields, and their interactions. For one single frequency ω Maxwell equations can be written introducing the phasor quantities (time factor $e^{j\omega t}$) [19] of the electromagnetic field as:

$$\vec{\nabla} \cdot \vec{D} = \rho \tag{4.1}$$

$$\vec{\nabla} \cdot \vec{B} = 0 \tag{4.2}$$

$$\vec{\nabla} \times \vec{E} = -j\omega\vec{B} \tag{4.3}$$

$$\vec{\nabla} \times \vec{H} = \vec{J} + j\omega\vec{D} \tag{4.4}$$

The first equation (4.1) is called Gauss' law and gives the relation between the electric flux flowing out a closed surface and the charge enclosed in the surface.

The second equation (4.2) is the same for the magnetic flux, with the difference, that a magnetic charge does not exist, therefore the magnetic flux flowing out a closed surface must be 0.

The third equation (4.3) is called Faraday's law of induction and gives the relation between the rate of change of the magnetic flux through the area enclosed by a closed loop and the electric field induced along the loop.

The last equation (4.4) is called Ampère's law with Maxwell's extension. It is the magnetic equivalent of Gauss' law, it relates the circulating magnetic field in a closed loop to the electric current passing through the loop.

The first two equations describe the static portion of the electromagnetic field and the other two the dynamic behavior[1].

4.2 EM–Radiation

A wire which is short according to the wavelength λ_0, ($dl \ll \lambda_0$), and which is thin against his length dl is a model for an elementary radiator also called elementary dipole or Hertz–dipole.

For convenience the current shall be considered constant $\widehat{I}$ along the wire.

The emitted field for the geometry shown in figure 4.1 is calculated by solving Maxwell's equations, as described in many books, e.g., [1].

The solution (Hertz–solution) for this case is done in polar coordinates and gives the following results for the tangential (ϑ) and radial components (φ) of the magnetic (H) and electric (E) field components:

$$\begin{aligned} H_\varphi &= j\,\widehat{I}\,\beta_0\,dl\,\frac{sin\,\vartheta}{4\pi r}\left(1+\frac{1}{j\beta_0 r}\right)e^{-j\beta_0 r} && (4.5)\\ E_\vartheta &= j\,Z_0\,\widehat{I}\,\beta_0\,dl\,\frac{sin\,\vartheta}{4\pi r}\left(1+\frac{1}{j\beta_0 r}+\frac{1}{(j\beta_0 r)^2}\right)e^{-j\beta_0 r} && (4.6)\\ E_r &= j\,Z_0\,\widehat{I}\,\beta_0\,dl\,\frac{cos\,\vartheta}{2\pi r}\left(\frac{1}{j\beta_0 r}+\frac{1}{(j\beta_0 r)^2}\right)e^{-j\beta_0 r} && (4.7)\\ H_r &= H_\vartheta = E_\varphi = 0 && (4.8) \end{aligned}$$

with $Z_0 = \sqrt{\mu_0/\varepsilon_0}$ and $\beta_0 = 2\pi/\lambda_0 = \omega/c$

As it can be seen, there is only a magnetic component in φ direction and the electric field has no φ component, so the two fields are orthogonal to each other.

In the near-field, where $r \ll \lambda_0$ the biggest part of the electric field does not emit energy, but it is charged and discharged by the dipole with energy.

In the far-field, where $r \gg \lambda_0$ the radiation field is built of the components H_φ and E_ϑ which are in phase and orthogonal to each other and to the radiation vector $\vec{r}$:

[1] for further reading refer to [19]

$$E_\vartheta = Z_0\, H_\varphi = j\, Z_0\, \widehat{I}\, \beta_0\, dl\, \frac{sin\,\vartheta}{4\pi}\, \frac{e^{-j\beta_0 r)}}{r} \tag{4.9}$$

This is the energy which is radiated as an electromagnetic wave. Notice that the radiation of electric and magnetic field varies due to the polar angle ϑ according to $sin\vartheta$ and in radial direction. It falls off with $1/r$.

The pointing–vector $\vec{S} = \vec{E} \times \vec{H}$ describes the direction of the power–flux. The time averaged power–flux is given by:

$$S_r = \frac{1}{2} Re(E_\vartheta H_\varphi^*) = \frac{Z_0}{2}\, (\widehat{I}\, \beta_0\, dl)^2\, \frac{sin^2\,\vartheta}{(4\pi r)^2} \tag{4.10}$$

The energy–flux-density is related to the distance r with $1/r^2$ and to the polar angle ϑ with $sin^2\vartheta$. Obviously there is no energy transported in axial direction of the dipole.

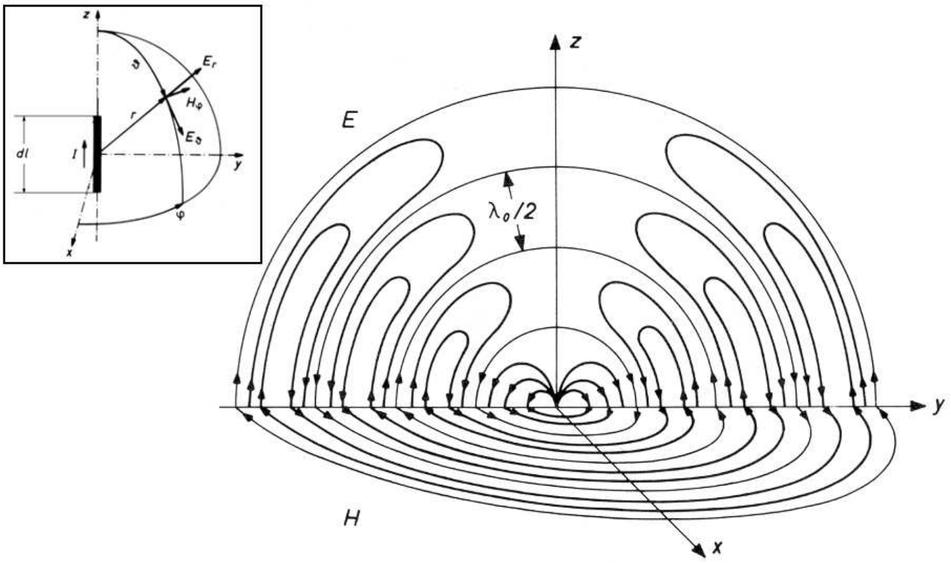


Figure 4.1: E– and H–Field of Elementary–Dipole [1]

4.3 Receiving EM–Radiation

To receive EM–radiation an antenna couples the energy from the EM–field into an electric wire. Two elementary types of antennas are used here.

The first type couples to the electric field of an electromagnetic wave, usually using a wire in which an electric charge moves back and forth, like the previously discussed dipole.

The second couples to the magnetic field of an electromagnetic wave, this is in general a coil of wire, forming an electromagnet.

Typically, antennas are designed to operate in a relatively narrow frequency range, this means that they have the best efficiency in this range, for other frequencies the gain of the antenna is reduced.

4.3.1 Electric Field Coupled Antennas

Most antennas which couple to the electric field are built of one simple beam, they are called dipole antennas. They have the same characteristics as the dipole shown in 4.2.

One of the main variables when designing an antenna is the frequency, respectively the wave length of the radiation to be received. The optimal length of dipole antenna is half of the wavelength, and such an antenna is called $\lambda/2$ – dipole.

4.3.2 Magnetic Field Coupled Antennas

Antennas which couple to the magnetic field are mainly coils. They receive the field according to Faraday's law of electromagnetic induction:

$$\oint \vec{E} \cdot ds = -j\omega\Phi_B \tag{4.11}$$

where $\vec{E}$ is the induced electric field, $\vec{ds}$ is an infinitesimal element of the closed loop and $j\omega\Phi_B$ is the rate of change of the magnetic flux.

For a coil with n windings the formula is:

$$V = -n\, j\omega\Phi_B \tag{4.12}$$

where V is the induced voltage.

Notice: we will only receive a signal, if $j\omega\Phi_B \neq 0$; this means, if the magnetic field is static we will not receive a signal at all, because we receive only the derivative of the magnetic field.

4.4 Expected Frequency and Bandwidth

The frequency of the signal which is emitted by the device is related to the frequency on which the device is operating. This frequency controls the processing steps of the device and thereby the transistors which are switched on and off are synchronous to this clock–cycle.

The first assumption could be, that the frequency of the radiated electromagnetic field from the device would be of the same frequency as the clock. But by analyzing the device it is possible that during one clock–cycle more than one operation is going on. For example a RISC–CPU based on a Harvard architecture fetches one opcode and executes another earlier fetched opcode in one clock–cycle.

The other point is that the gates of the transistors are switching, and the current of that is not related to a *sin*–function as described in chapter 4.2. We assume that the electromagnetic field generated from the circuit is caused by the current of the switching gates of the device, which has a rectangular characteristic. Also we assume that the radiation is correlated to the power consumption of the circuit. This has been measured during other DPA–attacks.

To understand the bandwidth of such a signal, we can exemplary perform a Fourier–transformation of a rectangular signal:

$$f(t) = \begin{cases} \sqrt{\frac{\pi}{2}} & for \quad (-1 < t < 1) \\ 0 & for \quad (t < -1), (t > 1) \end{cases} \tag{4.13}$$

this is :

$$F(\omega) = \frac{1}{\sqrt{2\pi}} \int\limits_{-1}^{1} \sqrt{\frac{\pi}{2}}\, e^{-i\omega t}\, dt = \begin{cases} \frac{sin\omega}{\omega} & for \quad (\omega \neq 0) \\ 1 & for \quad (\omega = 0) \end{cases} \tag{4.14}$$

As result there is no ω_0 for which $F(\omega > \omega_0) = 0$. This means that a signal with a high slope is not frequency delimited.

Thus if a transistor switches with a frequency of ω the radiated signal is not a narrow band signal, it contains frequencies that are much higher, than the clock signal.

4.5 Impedance and Standing Wave Ratio (SWR)

To connect the antenna to the scope we have to use an electrical transmission line.

For high frequencies conditions, the electrical behavior of the line is more complex than that of a low-frequency transmission line.

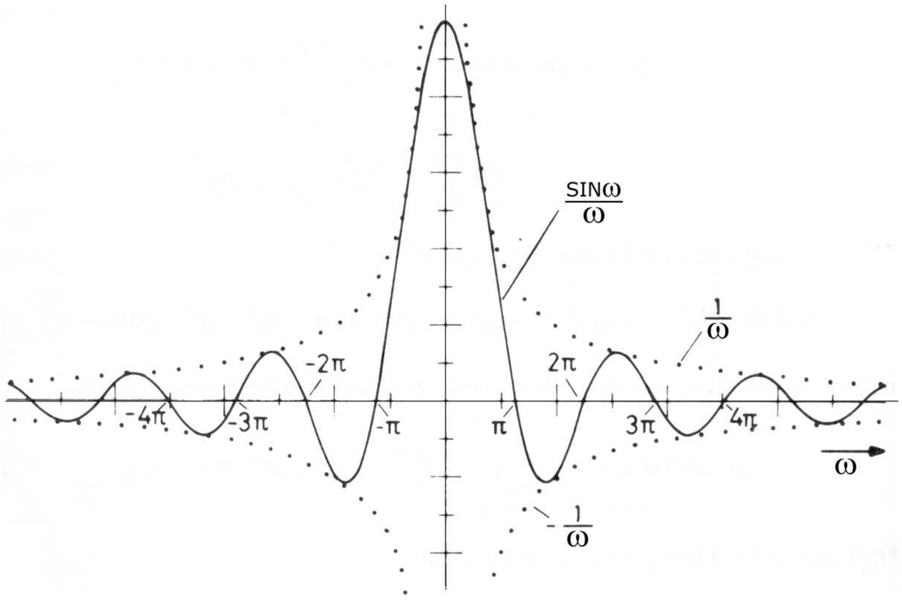


Figure 4.2: Fourier–Transformation of Rectangular Signal

I used a coaxial–cable to connect the antennas with the scope. The impedance of a coaxial–cable is fixed by its geometry according to:

$$Z_0 = \frac{120}{\sqrt{\varepsilon_r}} \cdot ln\left(\frac{D}{d}\right)$$

where D is the outer and d the inner diameter. The used cable is a RG–58 with an impedance of:

$$Z_0 = 50\Omega$$

This is important, because if two cables with different impedances are connected, reflection occurs at the connection point. If the wave is coming from the cable with the impedance Z_1 at the connection with the media with the impedance Z_2 the reflection factor is:

$$\Gamma = \left|\frac{Z_1 - Z_2}{Z_1 + Z_2}\right|$$

This describes the ratio of the amplitude of the reflected wave and the amplitude of the incident wave.

If $\Gamma \neq 0$ then a portion of the wave is reflected back to the source, interferes with the arriving signal and results in a standing wave.

The value for the standing wave on a transmission line is the standing wave ratio (SWR) If a is the amplitude of the forward wave and b the amplitude of the reflected wave then the standing wave ratio is defined as:

$$\mathrm{SWR} = \frac{a+b}{a-b}$$

For $a = b$ (total reflection) the SWR becomes infinite and in case of a matching connection, where $Z_1 = Z_2$ there is no reflection ($b = 0$) and $SWR = 1$.

The standing wave ratio expressed in terms of the reflection factor Γ is:

$$\mathrm{SWR} = \frac{1+|\Gamma|}{1-|\Gamma|}$$

In HF–applications it is normally intended to minimize Γ, such as the whole energy passes the connection and nothing will be reflected back to the source, this can be realized by choosing $Z_1 = Z_2$.

The above is only valid for the connection of two cables of the same type. If the cables are from different types (e.g., a coaxial– and two–wire cable) this calculation is more complex and it is very difficult to get the antenna matched to the cable so that $SWR = 1$.

It is important to know that the signal received by the antenna is reflected at the connection to the coaxial–cable back to the antenna, if $\Gamma \neq 0$. Then it is reflected back by the antenna itself, so that a single signal is multiplied.

4.6 Noise

It is desired that the antennas I use obtain only the emitted radiation from the crypto device. But the antenna also receives radiation from other sources.

The characteristic value is the signal–noise–ratio (SNR). It describes the ratio from the effective signal amplitude ($U_{eff,S}$) and the power (P_S) to the effective noise amplitude ($U_{eff,N}$) and the power (P_N):

$$\mathrm{SNR} = \frac{P_S}{P_N} = \frac{U_{eff,S}^2}{U_{eff,N}^2}$$

Signal noise ratios cannot be improved by linear signal processing. Systems, which try to improve the signal noise ratio by a noise suppressor always contain non–linear elements.

It is desired to have a maximum SNR, this can be realized by placing the antenna near to the device, so that the amplitude from the radiation generated by the device is high compared to the background noise.

4.7 Using a Receiver

Some publications like [6] and [7] consider the usage of a receiver, but I think that this is not applicable for DEMA like it is for SEMA.

A receiver demodulates the received signal and so periodic events can be detected as patterns of the demodulated EM signal, as they can be treated like the modulating signal. But it is essential, that the bandwidth of the modulating signal is lower than the signal which is modulated.

DEMA is based on a statistic test at one point in time. It is not possible to detect e single event using a receiver, as the modulating signal which is one discrete event is not limited in bandwidth.

4.8 Summary

A chip can be treated as an x/y–plane, it has nearly no z–dimension. Therefore, the currents that flow in a chip have no components normal to the chip. The resulting EM–field is calculated by superposing the EM–field components of all single flows. The direction of the maximum resulting field measured directly above the chip is normal to the chip layer for the electric– as well as for the magnetic–field.

To have the best SNR it is preferred to place the antenna as near as possible to the chip. If the impedances form the antenna and the coaxial–cable don't match, a standing–wave occurs. In case of too much disturbance due to a high SWR an active amplifier may be used to match the impedances of antenna and coaxial–cable.

5 Antennas

During this work I have constructed some antennas. For electric coupling antennas small copperplates were used and for magnetic coupled antennas coils of a thin wire have been winded. All those self made antennas do not have the same impedance as the attached coaxial–cable.

It can be expected that not the entire power received from the antenna is coupled in the coaxial–cable. The scope used for sampling has a built–in amplifier, therefore the power of the signal has no evidence for the measurements.

But the standing wave which occurs due to the mismatched antenna can cause reflections.

5.1 Electric Field Coupled Antennas

Two antennas are built of copper plates that are solded to the core of a coaxial–cable with an impedance of 50Ω. The energy that can be received with such an antenna is calculated by integrating the electric field $\vec{E}(\vec{r})$ to be received, over the surface of the antenna.

When the field is constant a larger surface results in higher output. The direction of the electric field to be received must be normal to the plate orientation. So these antennas are placed parallel to the surface of the chip, whose radiation will be measured.

A plate of 4×4 mm is used for the first antenna and a larger plate with the dimension 13.5×14.5 mm is used for the second antenna.

5.2 Magnetic Field Coupled Antennas

As previously explained, antennas that couple to the magnetic field are mainly coils. During this work some antennas of this type have been built.

An isolated copper wire with a thickness of 0.2 mm has been turned around a small cylinder with a diameter of 2 mm used as a shaft. Afterwards the shaft was removed and so the air-core coil was constructed. The two ends of the coils did been sold to a copper core of a RG-58 coaxial–cable with an impedance of 50Ω.

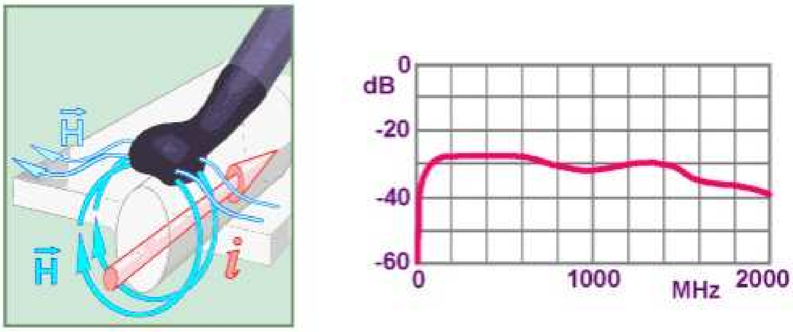


Figure 5.1: Near–Field–Probe RF U 5–2

I have made some different coils with the same wire and the same inner diameter, but with different winding numbers from 40 up to 800. Also a coil with an inner diameter of 30 mm has been compounded with 50 windings.

These antenna types receive the magnetic portion of the field, depending on the number of windings and the magnetic field which passes the area enclosed by the ring. It can be calculated by integrating the magnetic field $\vec{H}(\vec{r})$ over the enclosed area multiplied by the number of windings. The received power will increase due to a bigger diameter and more windings.

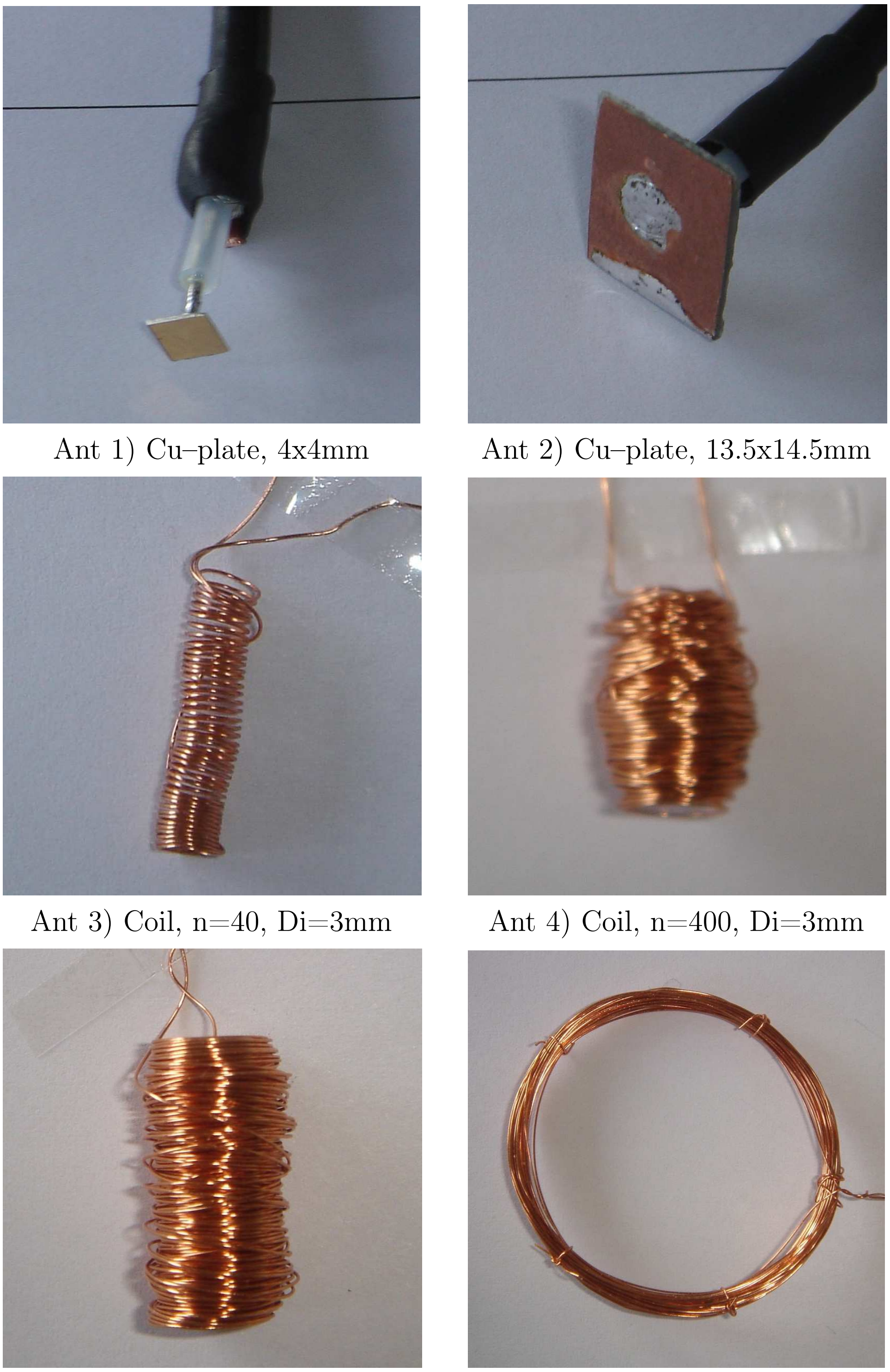
The antennas are shown in figure 5.2

5.3 Near-Field Probes

Some companies are specialized on near field probes, which are used to measure the electromagnetic field generated by wires on electronic circuit boards. These probes operate on the same principle as the probes built during this work with the difference, that they are much smaller and so they can be used to get a higher resolution of the place where the field is generated.

In this work I used the RF U–2 near field probe, from the company *LANGER EMV-Technik GmbH, Bannewitz, Germany*[1]. A drawing from the probe and the frequency characteristics is shown in figure 5.1.

[1] `http://www.langer-emv.de`



Ant 1) Cu–plate, 4x4mm

Ant 2) Cu–plate, 13.5x14.5mm

Ant 3) Coil, n=40, Di=3mm

Ant 4) Coil, n=400, Di=3mm

Ant 5) Coil, n=800, Di=3mm

Ant 6) Coil, n=50, Di=30mm

Figure 5.2: Antennas

6 AES on Atmel-Microcontroller Based Smartcard

To evaluate the antennas constructed in chapter 5, a known device with a well known cryptographic implementation is selected.

Previous work on power analysis at the Chair for Communication Security has been done on a smartcard containing an Atmel ATmega RISC–CPU. For this microcontroller an AES software implementation was developed and tested.

This hardware is also usable for electromagnetic side channel analysis and as the results for power analysis are known, they can be compared with the results of this work.

This work uses known input data and the outcomes of the S–Boxes in the first round as the selection function. It is also possible to analyze the S–Boxes of the last round with known output values.

As this controller is based on an Harvard–architecture (which will be explained in chapter 6.1) the S–Box output byte has to be sent on the data bus to get stored in the internal RAM or register. This transfer causes electromagnetic emissions, as the bus–drivers have to be charged according to that.

6.1 Atmel ATmega–Microcontroller

The controller which is embedded in this smartcard is an Atmel ATmega 163 RISC–CPU. This device is based on the AVR–core and it additionally has many functions, which are not used for the crypto function. The smartcard also comprises an 8 kbyte EEPROM, which has not been used during this work.

The main features of this controller are:

- 130 instructions; most single clock cycle execution
- 32 x 8–bit General Purpose Working Registers
- Program–Memory: 16 kilobytes nonvolatile Flash

- Nonvolatile Data–Memory: 512 bytes EEPROM
- Data–Memory: 1024 bytes Internal SRAM
- Timer/Counters: two 8-bit and one 16-bit with separate prescaler, compare mode and capture mode for the 16-bit timer/counter
- Real–Time–Clock with separate oscillator and counter mode
- Three PWM–Channels
- 8–channel, 10-bit Analog–Digital–Converter
- Two–wire Serial Interface
- Programmable Serial UART
- Master/Slave SPI Serial Interface
- Programmable Watchdog Timer with Separate On-chip Oscillator
- Analog Comparator
- Four Sleep Modes: Idle, ADC Noise Reduction, Power-save, and Power-down
- 32 Programmable I/O Lines

In this smartcard application the most peripheral equipment of the controller is not used.

Figure 6.1 shows the core of an AVR ATmega163. It points out, that all results of the ALU have to pass the data–bus to be transported to their destination which can be the internal RAM or EEPROM or the different registers.

Whereas the command instructions, which control the operation of the CPU, have a separate bus, they don't pass the data–bus. A special case is the internal RAM. The data from and towards the RAM passes the data–bus, while there is a separate bus for the address data.

Recapitulating: The Atmel AVR Core uses different memories and buses for program and data. Most instructions take a single clock cycle to be executed.

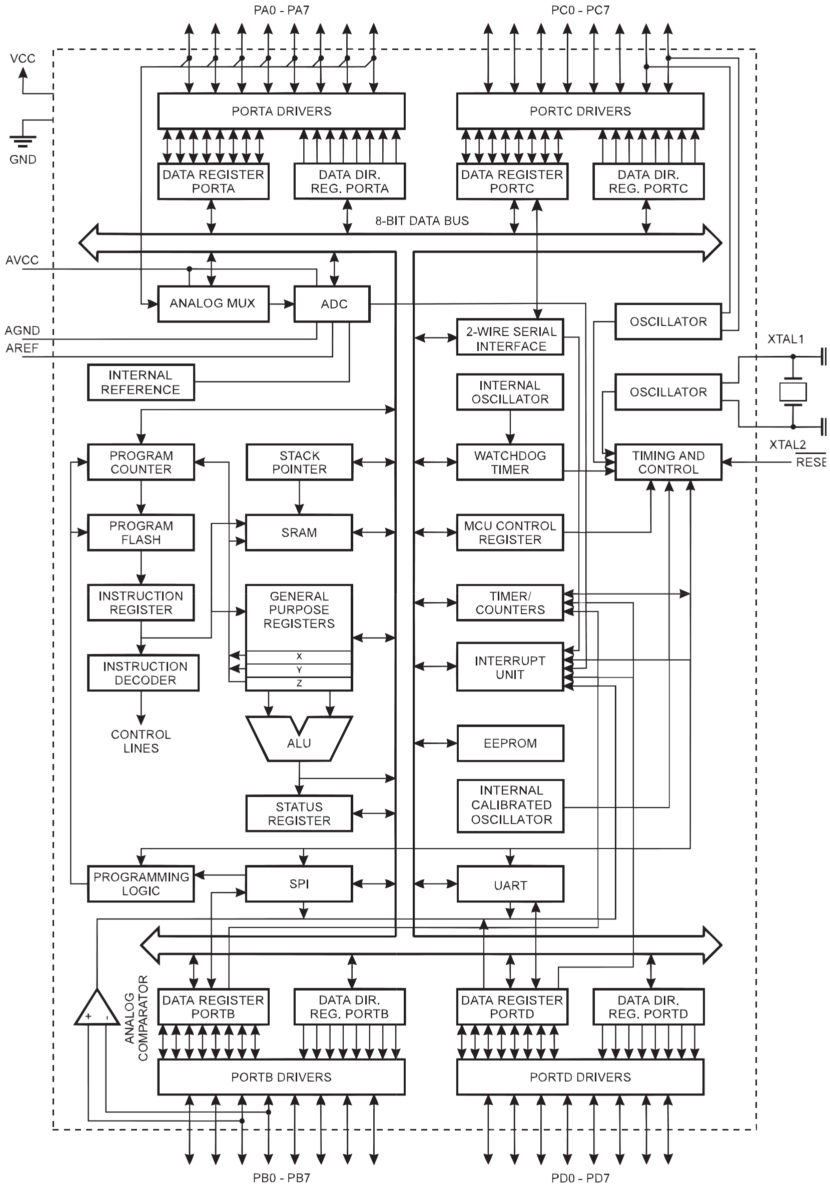


Figure 6.1: Harvard Architecture on Atmel ATmega163 [2]

6.2 SOSSE AES-Implementation

The goal is to analyze a cryptographic AES–128 algorithm on this smartcard. Here a straight-forward implementation of the AES–128 was programmed in assembly.

For the communication between the smartcard and the PC which controls the measurement setup a communication protocol is needed. The smartcard needs an operating system which supplies such a protocol, interprets the commands and executes the implemented functions.

Such a communication protocol is described in ISO/IEC 7816-3. The AES encryption function was integrated in the *Open-Source Simple Operating System for Smartcard Education* [20](SOSSE). It provides the protocol in this way, that a standard card reader [1] can be used to access the cryptographic functions of the smartcard by using a standard Windows API.

6.3 Measuring Setup

We remember, the goal is to gather information about the secret key by measuring and analyzing the electromagnetic emission that the smartcard generates while it computes the AES algorithm.

We also know from chapter 4 that it is advantageous to place the antenna near to the device, so that it receives the field components normal to the device.

Therefore, the card reader which communicates with the smartcard has been modified to give a possibility to access the chip with the EM-Probe as near as possible. The card reader has been disassembled, instead of using the internal contacts a standard smartcard–connector has been wired to it. A hole has been milled in this connector, so that it gives access to the inserted smartcard at the backside of the position where the pins are. This gives the possibility to place the antenna touching the smartcard.

It is essential that the measurements are synchronous to each other, so that the point in time on which the device computes the observed operation is at the same sampling–point $P(x_n, t_0)$ in each measure. If the measurements are not triggered to ensure this requirement the DEMA might fail, respectively it will be much more costly.

Thus the AES implementation includes a built-in trigger by pulling the I/O signal low for a few clock cycles, before it starts the first AES round. On real devices, as we see in chapter 7 it is much more difficult to obtain a reliable trigger signal that is close to the interesting operation.

I programmed a software to perform the measurements. This software includes the following steps:

[1] e.g.,: Chipdrive `http://www.chipdrive.de`

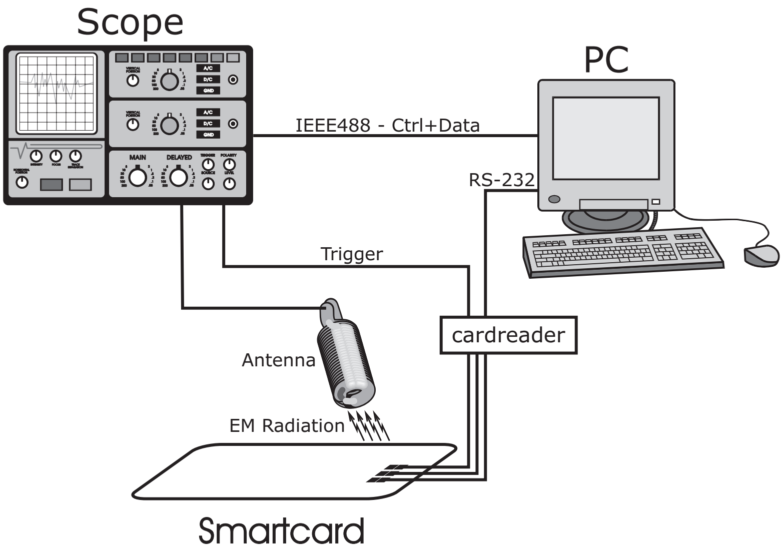


Figure 6.2: Side Channel Measurement Setup

1. Set up the scope over the IEEE488–Interface.
2. Self–calibrate the amplitude of the scope–input to fit the attached antenna.
3. Arm the scope to wait for trigger condition.
4. Send random data to the smartcard to be encrypted;
   the smartcard computes the AES–Algorythm (including the generation of the trigger signal).
5. Read out the scope data.
6. Store the data on the harddisk.
7. If sufficient measurements measures are done finish, else repeat at Point 2.

The scope[2] used in this work has an 8–Bit Analog–Digital–Converter. It is important that the measured signal does not clip, which means that the signal exceeds the limits of the converter. Furthermore, it is designated that the range of the signal is as high as possible. Therefore a self–calibration–routine has been programmed which computes the gain and the offset for scope to maximize the dynamic as much as possible without clipping for the actual attached antenna. The calibration values are stored and can be used for further analysis.

[2] Agilent infiniium 5432D MSO

Each measurement is stored in a binary file to the harddisk, where the first 16 bytes contains the plaintext–block which has been encrypted by the smartcard and the other bytes contains the measuring data recorded by the scope. For the first five measurements of a set this data is also stored in plain ASCII–Data, so that is possible to use gnuplot[3] to visualize the received signal.

6.4 Results

For each antenna 1000 measurements at 200 MS[4] per second have been done. The different antennas have been positioned touching the backside of the smartcard directly on top of the chip, which is located centered under the contacts.

The measured data has been processed with the statistic tests from chapter 3.2. The selection function has been applied on the output of the first S–Box after the first round.

As shown in figure 6.3 and 6.4, the side channel information received by all antennas could be used to extract the secret key, which was used during the operation. The figures show the correlation signal for the correct key hypothesis, depending on antenna and position.

The outer dimensions of the small antennas have been so small, that it was possible to do the measurements at different positions. The best correlation signal is received near to the contact pin 5. The information leakage is emitted from this area of the chip. Thus the rest of the chip emits non key dependent information, this can be treated as noise. If an antenna receives this radiation, too, the SNR is getting smaller. This condition is displayed in the figure for the antennas with $n = 400$ and $n = 800$. These antennas have been positioned in the center of the chip.

If the antenna is located so that it does not receive the normal component of the field that is caused by the device, the SNR is getting lower, as the signal is weaker but the background noise is the same. As anticipated, in this case there is nearly no correlation, between the received signal and the key hypothesis.

Furthermore we see in figure 6.4c), that the antenna 6 causes a standing wave while receiving the signal. Thus the point in time, where key dependent emission occurs is multiplied like an echo. There are many points, where the signal correlates. Figure 6.4d) shows, that there is no correlation when a wrong key hypothesis is chosen. This demonstrates, that an antenna which doesn't match the cable is not inevitable a bad configuration for side channel analysis.

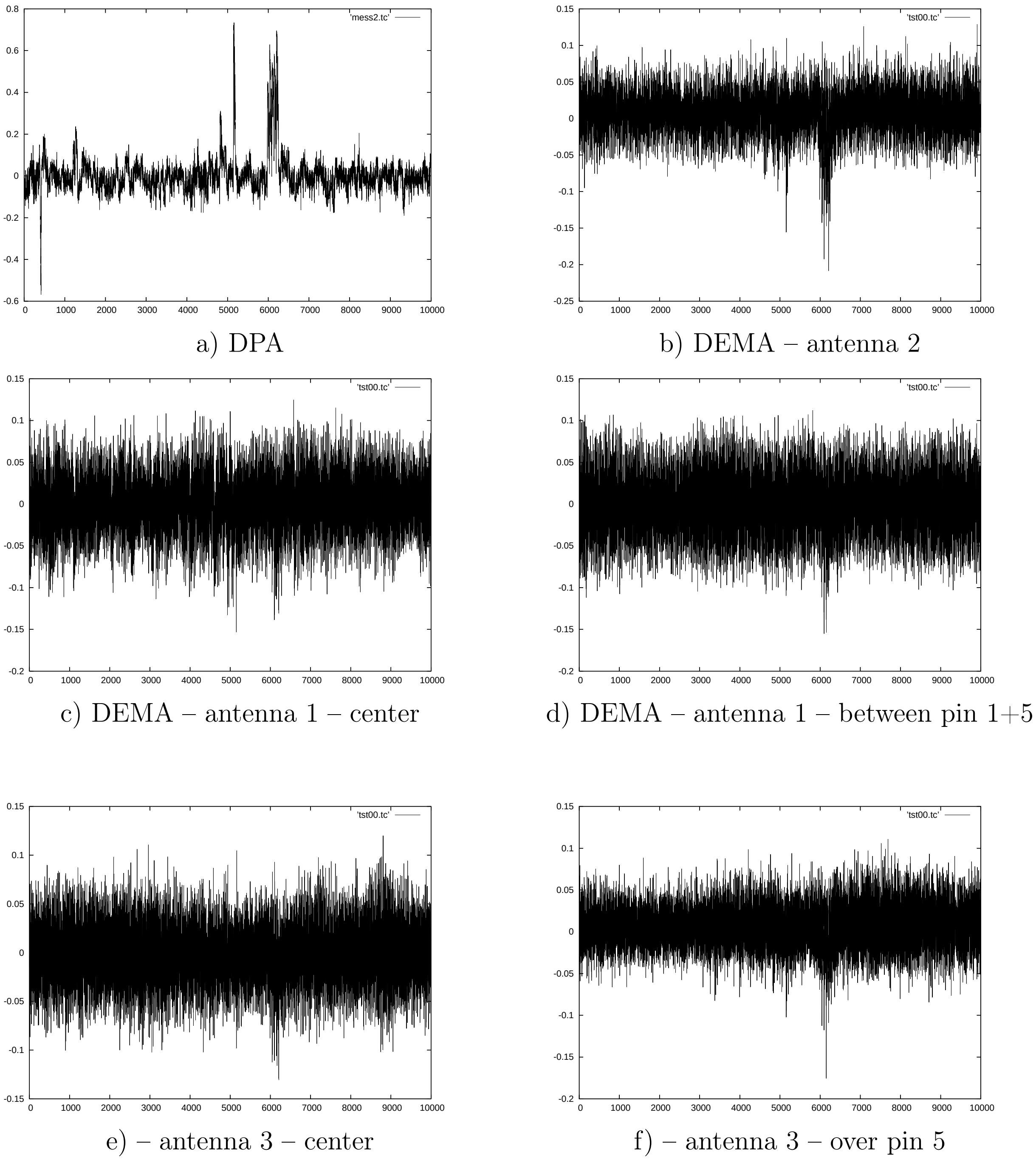
[3] Gnuplot is a portable command-line driven interactive data and function plotting utility for UNIX, IBM OS/2, MS Windows, DOS, Macintosh, VMS, Atari and many other platforms see `http://www.gnuplot.info`

[4] 200.000.000$Samples$

The near field probe RF U 5–2 from *LANGER EMV* was used with the corresponding amplifier PA 203. Figure 6.4e) and f) displays that the correlation is better, if the probe is located to receive the components standing normal to the chip.

Recapitulating:

- Electric as well as magnetic antennas can be used to receive the side channel information for DEMA.
- The best magnetic antennas are small coils, placed near to the device, like antenna 2 and the near field probe RF U 5–2.
- The best electic coupling antenna was a cu–plate which is as big as the chip (antenna 2).
- It is essential to place the antenna in such a way, that it receives the components normal to the chip layer.
- If an antenna is small enough it is promising to scan the device to find the area, where the best signal for DEMA occurs.
- In certain cases it can be good, if the antenna is not matched well to the cable, like antenna 6 in this case, but this is depending on the frequency.



a) DPA

b) DEMA – antenna 2

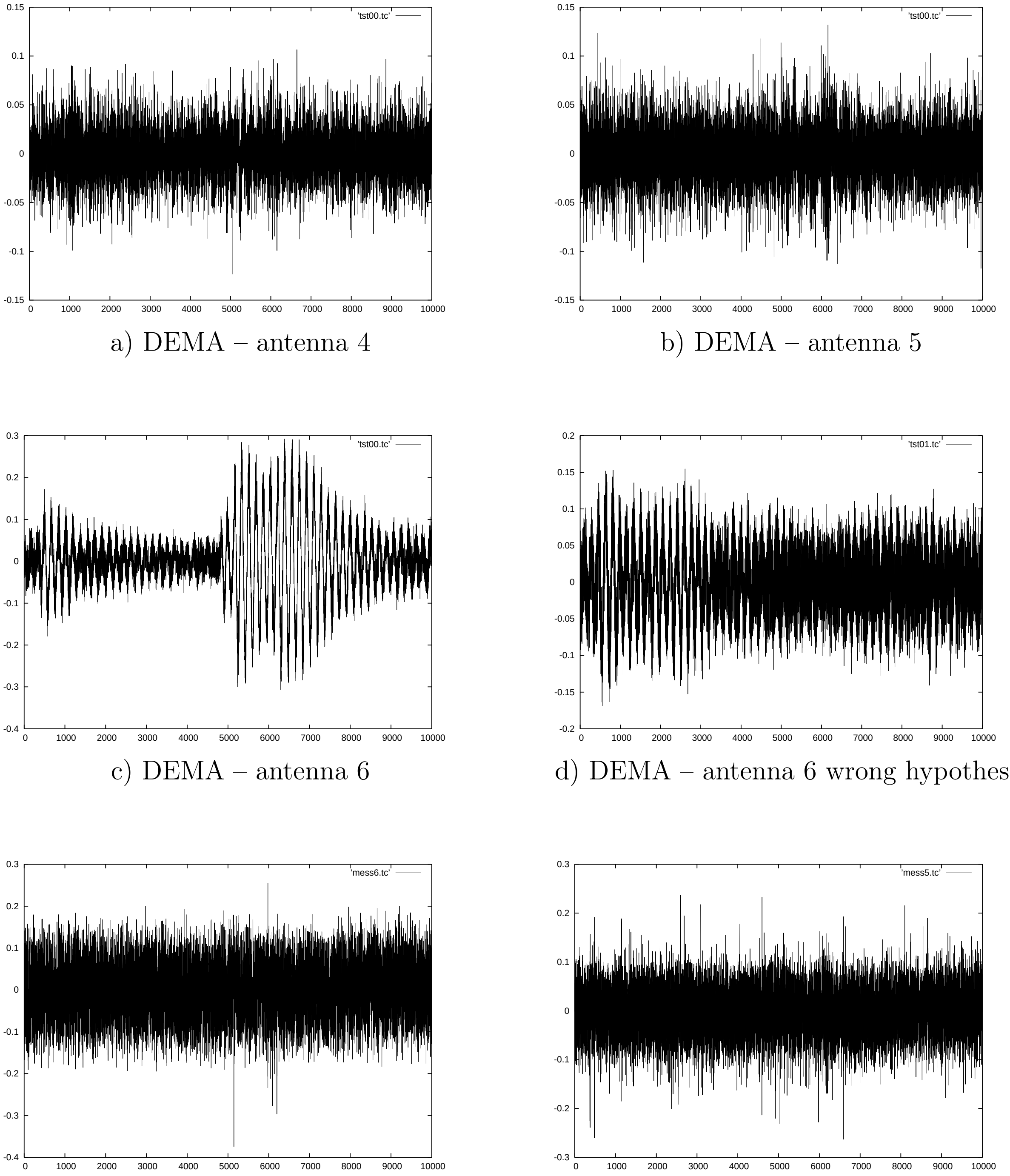
c) DEMA – antenna 1 – center

d) DEMA – antenna 1 – between pin 1+5

e) – antenna 3 – center

f) – antenna 3 – over pin 5

Figure 6.3: DPA and DEMA Results on AES



a) DEMA – antenna 4

b) DEMA – antenna 5

c) DEMA – antenna 6

d) DEMA – antenna 6 wrong hypothesis

e) DEMA – RF U 5–2 – normal

f) DEMA – RF U 5–2 – tangential

Figure 6.4: DEMA Results on AES

7 RFID Card

The second part of this work deals with a commercial Radio Frequency Identification (RFID) DESFire smartcard, which – according to its name – computes the DES–algorithm.

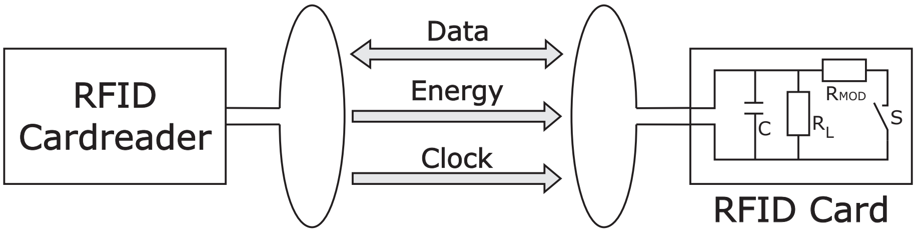


Figure 7.1: RFID-Transmission

A card reader device has been bought together with some Mifare DESFire cards[1]. ACG[2], the distributor of the card reader delivered the reader together with a Windows API and a documentation how this API can be used to access the functions provided by the DESFire card.

The DESFire Short Form Specification [21] says that the device uses a mutual three pass authentication employing either DES or Triple DES. This procedure not only confirms that the card reader and the card possess the same secret, it furthermore creates a session key which is used to keep the further communication path secure.

It is not shown in the public available documentation how this authentication is implemented exactly. The whole communication with the card is encapsulated by the card reader. Only the commands that have to be sent to the reader are described in the readers API.

First this protocol has to be examined, to get the required plaintext or ciphertext that is needed for the DEMA.

[1] for further infomation refer to [21]

[2] ACG Identification Technologies GmbH, Walluf, `http://www.acg.de`

7.1 RFID Communication Protocol

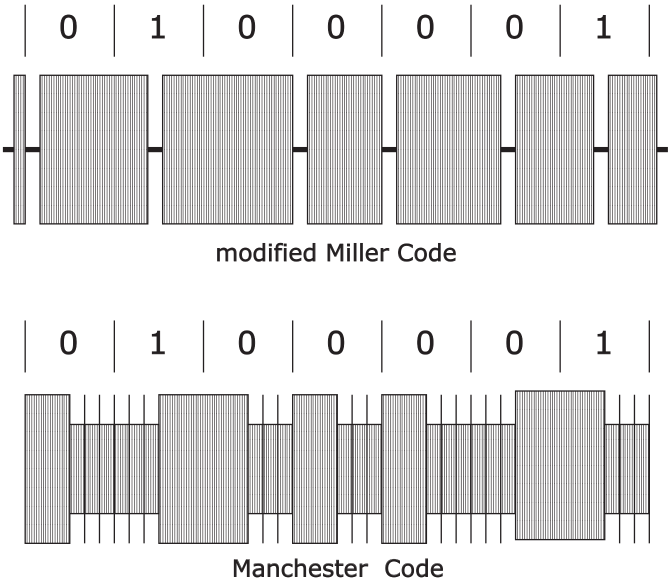


Figure 7.2: RFID-Modulation Codes

To examine the protocol which the card reader and the DESFire Card use, it is necessary to log the data transfer between both devices.

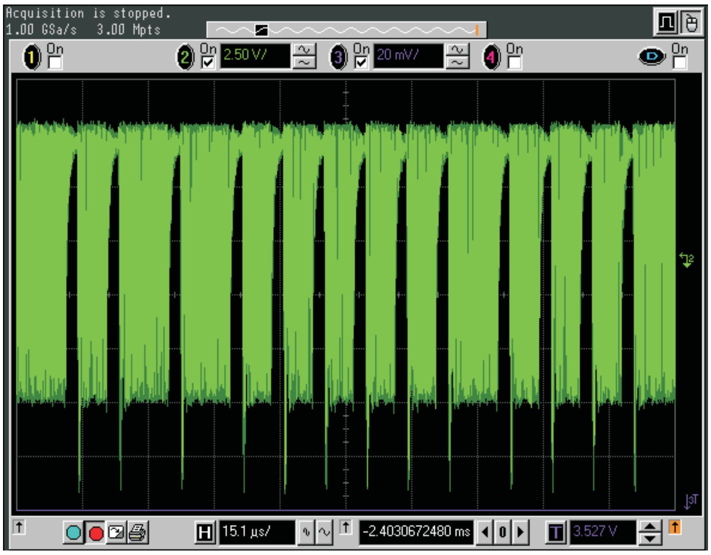
The card reader communicates with the DESFire card using a well known standard protocol ISO 14443 A described in [22].

The reader generates a *sin*–signal with the frequency of 13.56 MHz. This is used to transfer energy to the card and to provide the device with a system clock. Thus, the device clock is synchronous to the signal generated from the reader.

The downlink–data–transfer from the reader to the card is defined by the modified Miller–Code shown in figure 7.2. The blanking gap takes only $2 - 3\mu s$, this ensures that the device is continuously powered during the transmission. Figure 7.3 shows a scope signal while the reader is sending to the card.

The uplink–data–transfer from the card back to the reader is defined by the Manchester–Code shown in figure 7.2. The card transmits this signal by modulating the load applied to the signal the reader sends. This is done by switching on an additional load R_{MOD}.

The reader can detect this load–modulation and demodulates this to get the information the card sends to it. The Manchester–Code provides a simple collision detection ability, thus if two devices are sending simultaneously different data – and their serial numbers are different – the reader gets an invalid signal. In this case the reader uses a binary search tree to select the cards until no collision occurs. A scope signal during response from the card to ther raeder is shown in figure 7.4.



Acquisition is stopped.
1.00 GSa/s 3.00 Mpts

Figure 7.3: Modified Miller Code

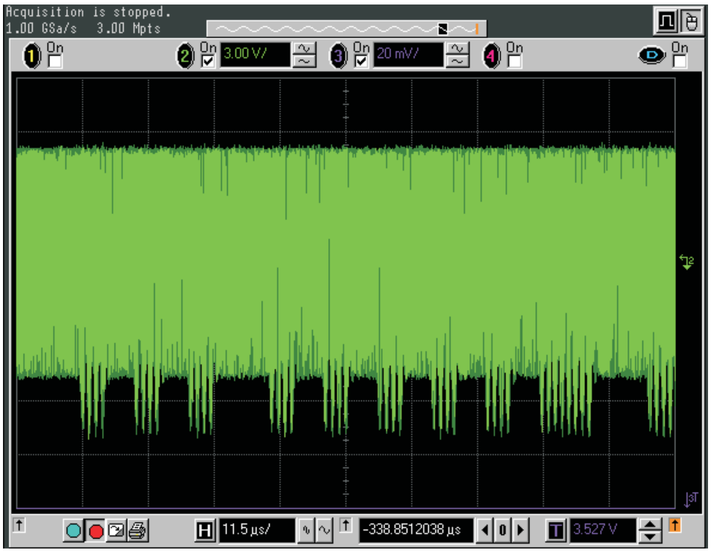
To monitor this communication a scope was attached to the reader's antenna output signal, so that the antenna signal could be recorded during the operation. I wrote a program that issues a command to the reader, which causes the reader to perform the communication with the card. The scope was configured to capture this data. After that, the program analyzed the stored data and shows the bitstreams that reader and the card have sent each other.

To evaluate the configuration first the SELECT–Command described in [22, chapter 9.2.2.3.1] has been monitored. It showed that the communication was exactly as specified. The communication starts with a start bit and ends with an end bit. Except the REQUEST–Command which is 7 bit long each byte consists of 8 bits. An odd parity bit is added to every byte and at the end of the block a CRC16–Checksum[3] is added.

7.2 Authenticate–Command

With the setup built in chapter 7.1 the communication during the Authenticate(AUTH)-command was monitored several times. The command was issued using different keys

[3] Cyclic redundancy check, for further information refer to [22, chapter 7]



Acquisition is stopped.
1.00 GSa/s 3.00 Mpts

Figure 7.4: Manchester Code

on card and reader, such that the authentication failed. A sample data–block with

$$\begin{aligned} k_r &= 112233445566778899\mathrm{AABBCCDDEEFF00} \\ k_c &= 00000000000000000000000000000000 \end{aligned}$$

is shown in table 7.1

By comparing the stored data to each other it was possible to discover the protocol data as follows:

1. To initiate the procedure the card reader sends the AUTH-Command to the card.

2. The card generates a 64–bit random number R_C and encrypts this number with its own secret key k_C. This encrypted block 0; $B_0 = \mathsf{Enc}(R_C; k_C)$ is sent to the reader.

3. The reader generates 64–bit random data R_R and decrypts this with its secret key which becomes block 1; $B_1 = \mathsf{Dec}(R_R; k_R)$.

   Afterwards, the reader decrypts the 8 byte block 0 received from the card with its key k_R. This results is $R_{C1} = \mathsf{Dec}(B_0; k_R)$ (which becomes R_C if $k_C = k_R$). Now the reader rotates R_{C1} by 8 bits left and decrypts this again with its key.

   The result of this operation is XORed with block 1, which becomes block 2. This is like the CBC-Mode[4]. Finally, the reader sends these two 64-bit blocks back to

[4] Cipher-block chaining, for further information refer to [23]

the card:

$$\begin{aligned} B_1 :&\quad \mathsf{Dec}(R_R; k_R) \\ B_2 :&\quad \mathsf{Dec}(\mathsf{RotLeft}(\mathsf{Dec}(B_0; k_R), 8); k_R) \oplus B_1) \end{aligned}$$

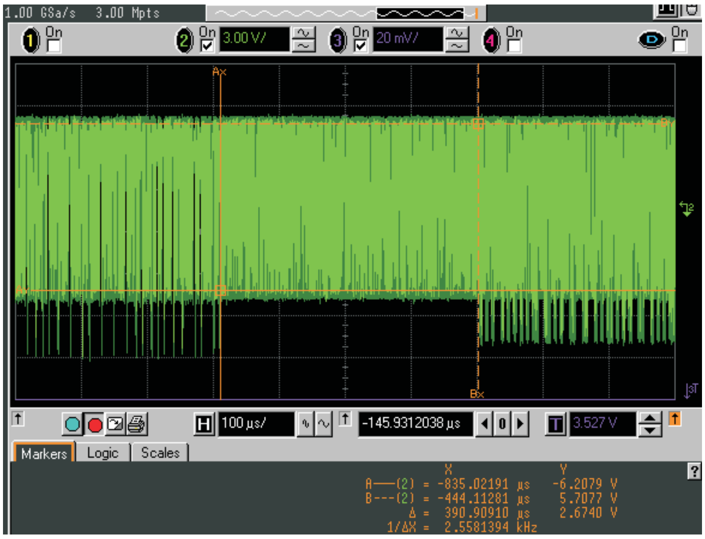
4. Now the card examines if the card reader works with the same key by performing the following algorithm:

$$R'_C = \mathsf{RotRight}((\mathsf{Enc}(B_2; K_C) \oplus B_1), 8)$$

   If this results in R_C, the card has successfully verified the cryptogram. If $R'_C \neq R_C$ then the card sends a failure response to the reader.

5. If the keys on the card and the reader have been chosen different, at this point the communication terminates. If $R'_C = R_C$ the card encrypts block 1 and rotates the result by 8 bits. Then it encrypts the rotated block with its key and sends it back to the reader, so that also the reader can validate the key stored in the card, like the card did before.

Note that the card reader does only perform DES decryption whereas the card only computes DES encryption. Remark: Further analysis is not needed here as the goal is to attack the authentication protocol.



```
            X                  Y
A——(2) = -835.02191 µs   -6.2079 V
B---(2) = -444.11281 µs   5.7077 V
     Δ =  390.90910 µs    2.6740 V
  1/ΔX =  2.5581394 kHz
```

Figure 7.5: Authentication Protocol $k_c \neq k_r$

Figure 7.5 shows a sample antenna signal recorded during the authentication procedure in the case that $k_c \neq k_r$. The left side shows the last bits of the data send from the reader containing block B_2 and B_2. On the right side the authentication failure response is shown.

From the point of which the card receives B_1 and B_2 to the time it sends the response depends on the fact if card and reader possesses the same key. If the keys don't match, as shown in figure 7.5, then the duration is 390μs. If $k_r = k_c$ then the card responds after 690μs.

The clock frequency of the DESFire card is 13.56 MHz, thus in 690μs it performs 9356 cycles. The duration for each 3 Triple DES encryptions is less than 3100 clock cycles, therefore it is probable, that the DESFire chip has an integrated DES hardware coprocessor.

$$\begin{array}{rcl}
\text{cardreader} & & \text{DESFire card} \\
& \xrightarrow{\hspace{2em}'AUTH'\hspace{2em}} & \\
& & R_C = \mathsf{GenRand}(64bit) \\
& & B_0 = \mathsf{Enc}(R_C; k_C) \\
& \xleftarrow{\hspace{3em}B_0\hspace{3em}} & \\
R_R = \mathsf{GenRand}(64bit) & & \\
B_1 = \mathsf{Dec}(R_R; k_R) & & \\
R_{C1} = \mathsf{Dec}(B_0; k_R) & & \\
R_{C2} = \mathsf{RotLeft}(R_{C1}; 8) & & \\
R_{C3} = \mathsf{Dec}(R_{C2}; k_R) & & \\
B_2 = R_{C3} \oplus B_1 & & \\
& \xrightarrow{\hspace{2em}B_1, B_2\hspace{2em}} & \\
& & R_{C4} = \mathsf{Enc}(B_2; k_C) \\
& & R_{C5} = R_{C4} \oplus B_1 \\
& & R'_C = \mathsf{RotRight}(R_{C5}; 8) \\
& \xleftarrow{\hspace{1em}\text{'ERROR'}\hspace{1em}} & \text{check if } R'_C \neq R_C? \\
& & \text{else} \\
& & R_{R1} = \mathsf{Enc}(B_1; k_C) \\
& & R_{R2} = \mathsf{RotLeft}(R_{R1}; 8) \\
& & R_{R3} = \mathsf{Enc}(R_R2; k_C) \\
& & \vdots \\
& & \vdots
\end{array}$$

Figure 7.6: Authentication Protocol

Reader → DESFire card			DESFire card → Reader		
Bits	Hex	Description	Bits	Hex	Description
0100 0000 0	02h	DESFire Cmd			
0101 0000 1	0Ah	AUTH			
0000 0000 0	00h	KeyNo			
0011 1011 0	DCh	CRC 16_L			
1011 0111 1	EDh	CRC 16_H			
			0100 0000 0	02h	DESFire Cmd
			1111 0101 1	AFh	Challange
			0000 1111 1	F0h	byte 0 (B_0)
			1100 1010 1	53h	byte 1 (B_0)
			0000 1000 0	10h	byte 2 (B_0)
			0101 1000 0	1Ah	byte 3 (B_0)
			0111 1100 0	3Eh	byte 4 (B_0)
			0101 1000 0	1Ah	byte 5 (B_0)
			1101 0001 1	8Bh	byte 6 (B_0)
			0001 1111 0	F8h	byte 7 (B_0)
			0011 0111 0	ECh	CRC 16_L
			1110 1001 0	97h	CRC 16_H
0100 0000 0	02h	DESFire Cmd			
1111 0101 1	AFh	Response			
0100 0101 0	A2h	byte 0 (B_1)			
0010 0101 0	A4h	byte 1 (B_1)			
1001 1000 0	19h	byte 2 (B_1)			
0111 0100 1	2Eh	byte 3 (B_1)			
0110 0111 0	E6h	byte 4 (B_1)			
1011 1001 0	9Dh	byte 5 (B_1)			
1000 0101 0	A1h	byte 6 (B_1)			
0001 1101 1	B8h	byte 7 (B_1)			
1101 1100 0	3Bh	byte 0 (B_2)			
1010 0011 1	C5h	byte 1 (B_2)			
1110 0010 1	47h	byte 2 (B_2)			
1100 1000 0	13h	byte 3 (B_2)			
0100 1010 0	52h	byte 4 (B_2)			
1100 1101 0	B3h	byte 5 (B_2)			
1000 0000 0	01h	byte 6 (B_2)			
0011 1001 1	9Ch	byte 7 (B_2)			
1010 1111 1	F5h	CRC 16_L			
0101 0000 1	0Ah	CRC 16_H			
			1100 0000 1	03h	
			0111 0101 0	AEh	
			0011 1101 0	BCh	
			0001 1110 1	78h	

Table 7.1: Sample Authentication Protocol Data

7.3 RFID Measurement Setup

With the information about the authentication protocol it is now possible to extract the input data, which is essentially needed for the DEMA.

To trigger the scope the voltage from the built–in red LED[5] was used. This LED flashes immediately after an unsuccessful authentication attempt, the signal is imprecisely to be used for the DEMA measurement[6], but it is sufficient to trigger the scope, that stores the whole procedure.

This measurement becomes much more difficult as the measurement on the smartcard in chapter 6 because the whole authentication procedure must be sampled together with the EM radiation received by the antenna.

So I built a program which performs n–times the following steps:

1. Arm the scope to wait for trigger condition.
2. Issue the AUTH–Command.
3. Read out the channel data of the scope, which is connected to the card reader's antenna.
4. Extract $Block1$ and $Block2$ which the reader sends to the card and the absolute point of time, when the last bit has been sent.
5. From this point read 500μs out from the channel which is connected to the antenna, containing the side channel information.
6. Store the side channel information together with the two plaintext blocks on a file.

Up to 10.000 measurements have been done using the antenna 2 and the near field probe RF U 5–2. As the clock frequency of the DESFire card is 13.56 MHz is four times higher than the frequency of the smartcard used in chapter 6 the sampling rate has been raised to 1 GS[7].

7.4 Measurement Improvement

To get the best results and the smallest SNR the antenna must be placed exactly on top of the chip. As the chip is embedded in the smartcard it is not possible to see where the

[5] Light-emitting diode

[6] The trigger offset for DEMA is evaluated in software

[7] 1.000.000.000 Samples per second

chip is located. The magnetic antenna and the chip are sealed inside the card material. The card material is not transparent to strong light neither the chip can be palpated.

In the first attempt I made an X–Ray photograph (see picture 3). On this X–Ray we see the exact position of the coil and the chip. According to this the antenna has been placed on top of the chip to get the best results.

Later on I dissolved the card using Trichloroethylene $C_2\ H\ Cl_3$ at a temperature of 100°C. Trichloroethylene dissolves the outer layers from the card and the chip was removed without damage. I built an antenna according to the geometry of the antenna that is visible on the X-Ray of the DESFire card. Additionally I elongated the cable to connect the chip by a distance of 30 cm.

After soldering the chip to the antenna, the chip was placed away from the reader's field, so that the emitted field does not disturb the measurements anymore. This results in two benefits: first it is possible to position the antenna more accurate at the chip, second the antenna is placed closer to the chip and so the signal amplitude increases, which results in a better SNR.

7.5 EM Analysis

On the measured data the side channel analysis according to section 3 has been computed. This analysis has been performed on the output of the S–Box at the first round. The result of this analysis shows no correlation to the correct key hypothesis.

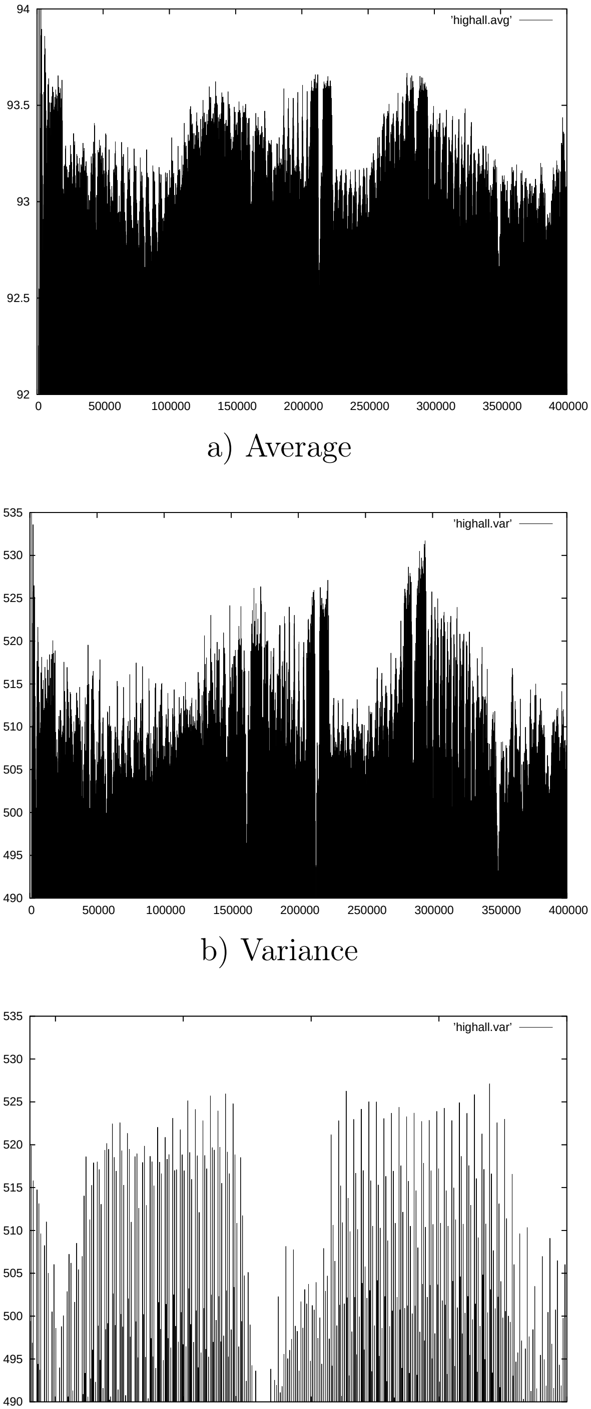
Due to that fact I tried to find a correlation between the measured signal and the plaintext. This would show the point of time, where the data is transmitted to the DES algorithm, but even this is not correlated to the received signal.

Another attempt is, that the variance[8] of the signal shall be high at the point of time, where the device is computing the DES operation. Furthermore the average value of the EM radiation might be different at the point of time where the DES is been computed. Figure 7.7 a) shows the average values over 1300 measurements. It shows two significant patterns starting at timepoint 206.000 and 277.000. The same pattern appears in the variance shown in figure 7.7 b).

A detailed view of the variance is shown in figure 7.7 c). This operation takes 20.000 sampling points, which is equal to 270 clock cycles. It is possible, that this is the signal originated by the triple DES operation done in hardware.

I observed two distinct execution times, one is about 390μs, the other about 460μs. This shows, that all the measurements are synchronous to each other. As the DES operation is implemented in hardware, the noise generated by the output of the not observed S–Boxes is quite high according to the signal from the observed S–Box.

[8] see formula 3.5



a) Average

b) Variance

c) Variance (Zoomed)

Figure 7.7: EM Radiation (Near Field Probe)

7.6 Further Directions

The current efforts are actually not sufficient to extract the DES key by DEMA. The following directions are suggested to improve the analysis.

For the suppression of external environmental noise a Faraday–cage can be used. Otherwise it is important to remove extra noise sources such as cellular phones. In this work I decided not to build a Faraday cage, as the SNR was obviously big enough. For further work it could be interesting to analyze if the correlation signals can be improved by using a self made or commercial Faraday cage.

During this work I was able to get the chip out off the card, see pictures 2 and 5 in appendix A. Another attempt is to scan the field with a smaller antenna using an opened chip (as shown in picture 4).

All measurements done during this work have been stored, thus it is possible to use these data for further examination. The measurements have been triggered at the end of the transmission from the reader to the DESFire card.

As the protocol of the DESFire card has been discovered, it is possible to construct a reader device which communicates with the card in the way, that the random numbers used are provided by the reader afterwards. Such an attack saves the measurement time needed for the extraction of the communication data. The time needed with the current set–up to perform 1500 measurements is 10 hours, the most portion is needed to extract B_1 and B_2 sent from the reader. If this extraction of the data can be avoided, in the same time more measurements could be done and so the number of measurements could be increased.

8 Conclusion

EM radiation is a side channel alternative if it is not practicable to measure the power consumption of a crypto device, e.g., at RFID devices or FPGAs.

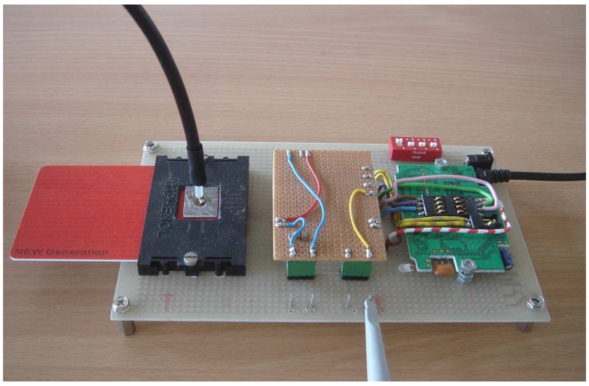
In this work I gave a theoretic introduction to the origin of EM radiation and antenna types that can be used to receive this radiation. Furthermore I explained the relevancy of the bandwidth, noise and the standing wave ratio for the side channel measurements.

I built some electric as well as magnetic antennas and showed that it is possible to perform a DEMA on a well known straight forward AES implementation on an ATMEL ATmega smartcard. The direction of the EM radiation has been verified and I showed that a standing wave can cause a significant correlation signal.

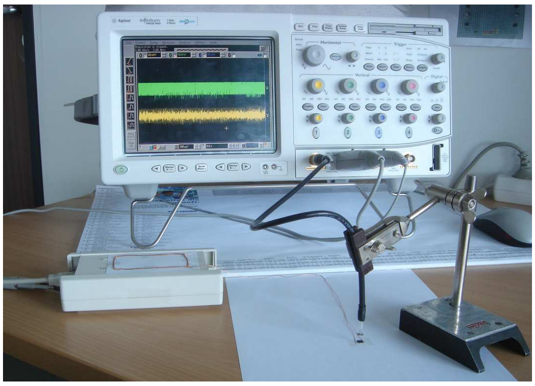
The measuremets set–up for the DESFire card was done and I discovered the authentication procedure of the DESFire card thus it is possible to perform measurements for DEMA as well as chosen plaintext analysis.

By using the efforts described in this work DEMA was not successful to compromise the cryptographic key of a DESFire card. In section 7.6 I give further directions that yield to more powerful conditions for applying DEMA. Nevertheless, due to the fact that the DESFire card is used by institutes like NASA it can be presumed that it has been evaluated to be secure due to side channel analysis, even if it is a low cost device.

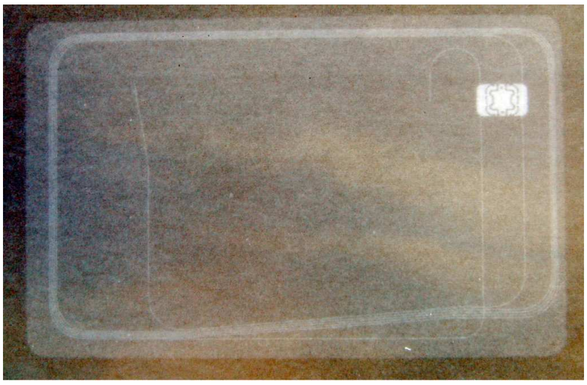
A Photographies



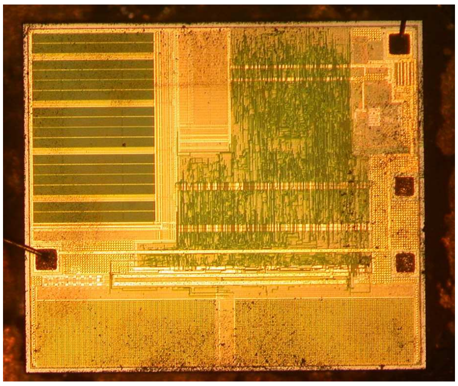
Pic 1: Modified Smartcard Reader



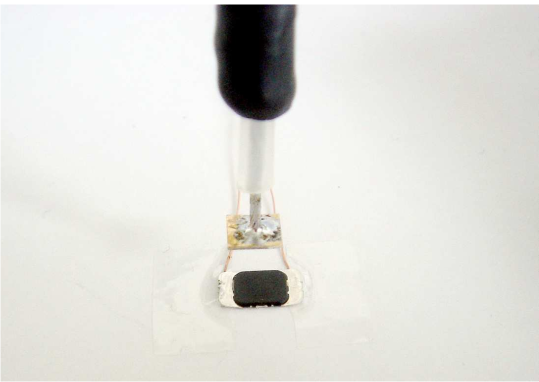
Pic 2: Scope with RFID-Reader



Pic 3: X-Ray of DESFire Chipcard



Pic 4: DESFire Chip



Pic 5: External DESFire Chip

Pic 6: Near Field Probe

B Bibliography

[1] E. Meyer and R. Pottel. Physikalische Grundlagen der Hochfrequenztechnik, 1969.

[2] Atmel. ATmega163 ATmega163L, 8-bit AVR Microcontroller with 16K Bytes In-System Programmable Flash. Rev. 1142E-AVR-02/03, Available at `www.atmel.com`.

[3] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic Analysis: Concrete Results. In Ç. K. Koç, D. Naccache and C. Paar, editor, *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2001*, volume LNCS 2162, pages 251–261, Paris, France, May 2001. Springer-Verlag.

[4] P. Kocher, J. Jaffe, and B. Jun. Introduction to Differential Power Analysis and Related Attacks, 1998. Manuscript, Cryptography Research, Inc., Available at `www.cryptography.com/dpa/technical`.

[5] J.-J. Quisquater and D. Samyde. Electro Magnetic Analysis (EMA): Measures and Countermeasures for Smart Cards. In *International Conference on Research in Smart Cards, E-smart 2001*, pages 200 – 210, Cannes, France, September 2001.

[6] S. Mangard. Exploiting Radiated Emissions – EM Attacks on Cryptographic ICs. In *Proceedings of Austrochip 2003*, Linz, Austria, October 3 2003. Springer-Verlag.

[7] D. Agrawal, B. Archambeault, J.R. Rao, and P. Rohatgi. The EM Side–Channel(s): Attacks and Assessment Methodologies. IBM Watson Research Center `http://www.cs.jhu.edu/~astubble/600.412/s-c-papers/em.pdf`.

[8] Royal Philips Electronics of the Netherlands. NASA selects PhilipsŠ advanced MIFARE DESFire contactless smart card chip technology to meet its secure facility access needs, July 27 2004. Available at `www.newscenter.philips.com/about/news/press/section-13267/article-3387.html`.

[9] Royal Philips Electronics of the Netherlands. U.S. Department of Interior selects Philips' advanced contactless smart card chip technology to heighten secure access to national facilities, December 6 2004.

[10] Royal Philips Electronics of the Netherlands. 1. FC Köln implements Philips chip technology for contactless ticketing, December 16 2004. Available at `www.semiconductors.philips.com/news/content/file_1116.html`.

[11] U.S. Department of Commerce/National Institute of Standards and Technology, National Bureau of Standards, U.S. Department of Commerce. *NIST FIPS PUB 46, Data Encryption Standard*, January 1977.

[12] U.S. Department of Commerce/National Institute of Standards and Technology, National Bureau of Standards, U.S. Department of Commerce. *NIST FIPS PUB 46-2, Announcing the Standard for Data Encryption Standard (DES)*, December 30 1993. Available at `http://www.itl.nist.gov/fipspubs/fip46-2.htm`.

[13] U.S. Department of Commerce/National Institute of Standards and Technology, National Bureau of Standards, U.S. Department of Commerce. *NIST FIPS PUB 46-3, Specification for the Data Encryption Standard (DES)*, October 25 1999. Available at `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[14] U.S. Department of Commerce/National Institute of Standard and Technology. *NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES)*, November 26 2001. Available at `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

[15] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, Great Britain, Second edition, 1997.

[16] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, 1993.

[17] M. Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard, 1994. Advances in Cryptology: Proceedings of CRYPTO '94.

[18] M. Aigner and E. Oswald. Power Analysis Tutorial. Available at `www.iaik.tu-graz.ac.at/aboutus/people/oswald/papers/dpa_tutorial.pdf`.

[19] S. Blume. *Theorie elektromagnetischer Felder*. Hüthig Verlag, Fourth edition, 1994.

[20] M. Brüstle et al. SOSSE: Simple Operating System for Smartcard Education. Available at `www.mbsks.franken.de/sosse`.

[21] Philips Semiconductors. Short Form Specification Mifare DESFire, Contactless Multi-Application IC with DES and 3DES security MF3 ICD 40, April 2004. Available at `http://www.semiconductors.philips.com/acrobat/other/identification/SFS075530.pdf`.

[22] K. Finkenzeller. *RFID-Handbuch*. Hanser Fachbuchverlag, Third edition, October 2002.

[23] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, Florida, USA, 1997.