Low Cost Attacks on Smart Cards
The Electromagnetic Side-Channel

Adam Matthews
adam[at]ngssoftware[dot]com

September 2006

Abstract

This paper documents a successful Electromagnetic Analysis attack implemented using limited technical knowledge and low cost equipment. EM traces were acquired from a sample card and analysis software successfully identified the correct key guesses in proprietary traces.

It is important to note that although this attack was implemented on a smart card running the DES encryption algorithm, that the same kind of attack is possible on other cards, as long as the implementation details of the algorithm are known.

Acknowledgements: Dr. Keith Mayes, Will G. Sirrett, Lishoy Francis, Mike Tunstall, Dr. John Walker, ISG Smart Card Centre - http://www.scc.rhul.ac.uk.

Contents

1 Motivation

When designing a system it is very attractive to base its security around smart cards. They are relatively cheap to produce, small and easily distributed, and are already in wide use. In the event of a security compromise, replacing a smart card is far easier than replacing a set-top box, or a mobile phone handset. When implementing physical crypto-systems, algorithmic complexity is not the only security issue to be taken into consideration. Smart cards are often regarded as tamper-proof devices, where secrets can be physically protected. It should not be forgotten that physical systems have their own vulnerabilities, and that smart cards are not tamper-proof, merely tamper-resistant.

Since Kocher et al. introduced Timing Attacks[1] in 1996, and Differential Power Analysis (DPA)[2] in 1997, it is well know that careless implementation can leak information about the key through the execution time, and power consumption of the card. A more sophisticated attack, Electromagnetic Analysis (EMA) has since been introduced, and can be used to mount an attack when countermeasures prevent the use of the timing or power side-channels, for example when the power supply is filtered.

Large and experienced organisations such as mobile telecommunications providers and satellite television distributors are aware of the cost to their business of security compromises and have taken appropriate measures to prevent them. Emerging industries, due to a lack of experience and technical knowledge or time pressures, may neglect to consider the threat of physical attacks on smart cards, perhaps assuming that they are too expensive, or technically complex.

This paper demonstrates to emerging industries the threat of physical attacks by showing an Electromagnetic Analysis attack on a smart card running a commonly used encryption algorithm, the Data Encryption Standard (DES). The attack was mounted using limited resources, and limited technical knowledge. This paper shows that EM emanations radiating from a smart card chip can be measured using a hand made probe and second hand oscilloscope, and that the cryptographic key can be recovered by differential analysis of these emanations.

2 Attacks on Smart Cards

There are four main classes of attack on smart cards:

- Physical
- Software
- Environmental
- Side-channel

2.1 Physical attacks

Physical attacks are usually invasive, for example rewiring a circuit on the chip. This often involves adding tracks to the chip in order to restore circuitry used in the production process to test the chip before it has been finalized. Once these circuits have been restored, the attack will have access to new functionality, such as being able to dump the contents of the chip's memory. Alternatively, tracks on the chip may be cut, in order to damage circuitry, and interfere with random number generation, which will make it easier to break encryption. Another possibility is to insert probe pins into the chip to monitor data on the chip's buses.

In general, physical attacks are time consuming and destructive. It is likely that a large number of sample chips will be destroyed before an attack is successful. In order to modify the circuitry on a chip, special equipment such as Focused Ion Beam (FIB), and probe stations are required, which are only available to very wealthy attackers.

2.2 Software attacks

Software attacks on smart cards exploit implementation vulnerabilities in the card through its own communication interface. This kind of attack includes exploiting buffer overflows and using trojan horse programs to deliberately inject malicious code into the card.

2.3 Environmental attacks

Environmental attacks involve altering the physical environment around the card, such as temperature, UV radiation, light, or x-ray, in order to induce faults. Inducing faults and causing the chip to behave abnormally can sometimes allow an attacker to bypass security measures, or gain extra information from the behavior of the card which may infer secrets.

2.4 Side-channel attacks

Side-channel attacks exploit information leaked by the physical characteristics of the card during execution of the algorithm. This extra information can be used to infer secrets, and can come in the form of timing, power, or radiation.

A timing attack is based on the principle that the time it takes for the card to execute the cryptographic algorithm depends on the value of the secret data. By measuring and analysing small differences in processing time, an attacker

can infer secret data. Timing attacks can be very effective against carelessly implemented algorithms.

Power analysis attacks use information leaked by a card's power consumption. Simple Power Analysis (SPA) attacks rely on detailed knowledge of the cryptographic algorithm being implemented, and visual inspection of the power consumption curve, to extract the cryptographic key. Differential Power Analysis (DPA) is a more powerful attack based on SPA, it adds the power of statistical techniques to separate signal from noise, and requires less detailed knowledge of the implementation of the cryptographic algorithm on the card.

Electromagnetic Analysis (EMA) attacks are very similar to DPA, but they exploit the information leaked in the electromagnetic emanations from the card while it is running. The details of the EMA attack and its advantages over other side-channel attacks are discussed in the next section.

3 Electromagnetic Analysis (EMA)

3.1 Source of EM Emanations

Side-channel leakage is caused due to the electrical characteristics of the technology used in construction of the smart card. Most modern chips are built using Complementary Metal Oxide Semiconductor (CMOS) technology.

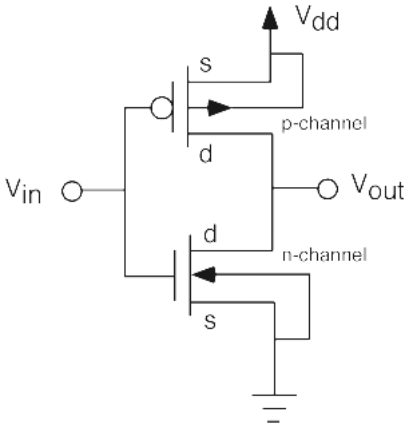

Figure 1: A CMOS inverter

Figure 1 shows a CMOS logic inverter, which forms the basis of all digital CMOS logic. The inverter can be looked upon as a push-pull switch: input at grounded level cuts off the top transistor, producing a high output. A high input does the opposite, pulling output to grounded level.

When a bit is flipped from 0 to 1 or vice-versa, the device's n and p transistors are on for a short period of time. This results in a short current pulse from V_{dd} to V_{ss}. The more circuits change their state, the more power is dissipated. This explains why information leaks when data flips, and why the power curve correlates to the transitions Hamming distance.

This current pulse causes variation in the EM field surrounding the chip, which can be measured by an inductive probe.[3]

3.1.1 Advantages of the EM side-channel

The EM side-channel, although experimentally more complicated, has several advantages over other side-channel attacks. Despite being more noisy, the measurements have a higher signal to noise ratio than those collected from the power side-channel, and therefore give better differential curves.[3, 4] making the correct key guess easier to identify, and requiring fewer samples.

Another advantage is that EMA does not suffer from the problem of 'false alarms'. In a DPA attack it is expected that the differential curve with the highest peaks will represent the correct subkey guess, however, experimentally this is not always the case; large peaks can sometimes be observed for incorrect guesses. This 'false alarm' problem can be attributed to the fact the power consumption relates to the power consumption of all the components of the chip, and not just those processing the algorithm, it may be due to the way the algorithm is implemented in code. EMA is less prone to these 'false alarms' since the data collected is better correlated to the processing of secret information, as it is possible to isolate the various components of the chip for individual analysis.

EMA can also bypass countermeasures that protect against DPA attacks, such as current smoothers, shields, and randomized logic.

3.1.2 The Attack

Following[2, 5]

There are several requirements that must be first met in order to carry out a successful EMA attack. The attacker must be able to take precise EM measurements, they must have detailed knowledge of the algorithm being computed, and they must also have knowledge of the plain-text corresponding to each encryption operation captured.

The first step is to capture EM measurements of the first round of N DES encryption operations, and represent the data as an array S_{ij}. The corresponding plain-texts are also collected and are represented as an array P_i. Optionally, the cipher-texts may be collected, and represented as array C_i. The EM signal S_{ij} is a sampled version of the EM emanations from the target area of the chip during the first round of DES execution. The i index corresponds to the plain-text P_i that produced the signal and the j index corresponds to the time of the sample.

Next, a selection function $D(\cdot, \cdot, \cdot)$ is chosen:

$$S_0 = \{S_{ij} | D(\cdot, \cdot, \cdot) = 0\}$$
$$S_1 = \{S_{ij} | D(\cdot, \cdot, \cdot) = 1\}$$

Then an average power trace is constructed from each set:

$$A_0[j] = \frac{1}{|S_0|} \sum_{S_{ij} \epsilon S_0} S_{ij}$$
$$A_1[j] = \frac{1}{|S_1|} \sum_{S_{ij} \epsilon S_1} S_{ij}$$

where $|S_0| + |S_1| = N$. The EMA bias signal is obtained by calculating the differential trace:

$$T[j] = A_0[j] - A_1[j]$$

The selection function D will result in an EMA bias signal that can be used to verify the correct key guess:

$$D(P_1, P_6, K_1) = P_1 \oplus SBOX_1(P_6 \oplus K_1)$$

where
P_1 = the 1 bit of plain-text input that is XOR'ed with bit 1 of S-Box 1.
P_6 = the 6 bits of plain-text that are XOR'ed with subkey K_1.
K_1 = 6 bits of the 1st round subkey feeding into S-box 1.

The selection function D is chosen because at some point during the DES implementation, the software must calculate the value of this bit. When this calculation occurs, or whenever this bit is manipulated, there will be a slight difference in the amount of power dissipated by the chip, depending on whether this bit is a zero or a one. If this difference is ε, and the instructions manipulating the D bit occur at times j^*, the following expected difference in power equation results:

$$E\left[S_{ij}|D(\cdot,\cdot,\cdot) = 0\right] - E\left[S_{ij}|D(\cdot,\cdot,\cdot) = 1\right] = \varepsilon$$
$$\text{for } j = j^*$$

When j is not equal to j^*, the smart card is manipulating bits other than the selection bit D, and the power consumption is independent of D:

$$\begin{aligned} &E\left[S_{ij}|(D(\cdot,\cdot,\cdot) = 0)\right] - E\left[S_{ij}|D(\cdot,\cdot,\cdot) = 1\right] \\ &= E\left[S_{ij}\right] - E\left[S_{ij}\right] = 0 \end{aligned}$$
$$\text{for } j \neq j^*$$

As the number N of P inputs increases, the differential trace converges to the expectation equation:

$$\begin{aligned} \lim_{N\to\infty} T[j] = &E\left[S_{ij}|(D(\cdot,\cdot,\cdot) = 0)\right] \\ &-E\left[S_{ij}|(D(\cdot,\cdot,\cdot) = 1)\right] \\ &= E\left[S_{ij}\right] - E\left[S_{ij}\right] = 0 \\ &\forall j \end{aligned}$$

Therefore, if enough P samples are used, $T[j]$ will show EM biases of ε at times j^*, and will converge to zero at all other times. Due to small statistical biases in the outputs of the S-boxes, $T[j]$ will not always converge to zero in practice, however the largest biases will occur at times j^*.

One of the inputs to the selection function D was K_1. These bits are not available to the attacker, so all 2^6 possible subkey bits must be guessed. For each guess, a new partition is created for the power signatures, and a new differential trace $T[j]$ is calculated. The trace for the correct guess will show biases wherever the selection bit was manipulated. If the wrong guess was made, then the differential trace will show no biases. With this approach the attacker can determine the six subkey inputs to S-box 1 in the first round of DES. By repeating these steps he can find the seven other S-box inputs, which gives him the entire round one subkey. This gives 48 bits of the secret key, and the remaining 8 bits can be found by brute force. Using the extra information leaked by the EM side-channel, and breaking the encryption algorithm in this way takes far less time than a brute force attack on the entire 56-bit key.

4 Method

4.1 Equipment

The attack was carried out using inexpensive equipment. This included an oscilloscope capable of 2GS/s, amplifier, personal computer, hand made probe coils, and a decapsulated DES smartcard.

4.1.1 Probe design

The layout of standard smart card chips consists of blocks of a few hundred microns. In order to isolate the different components, such as the CPU, RAM, and EEPROM, and collect traces for analysis, the probe must be very small.

Although similar experiments have been successfully carried out using hard disk heads, small metal plates[6], and various other types of probe, a hand made coil, was chosen for these experiments. A coil should give superior EM traces.[3]

4.2 Signal Location

4.2.1 Vertical Probe Positioning

If we approximate the source as a long linear wire, then according to the Biot-Savart law B the magnitude of the field is inversely proportional to the distance r between the wire and the probe:

$$B = \frac{\mu_0 I}{2\pi r}$$

This means that the probe's coil must be placed as close as possible to the chip in order to get the best EM traces.

The standard thickness of a smart card is 800 microns, which means that placing the probe on the back of the card leaves it up to 500 microns away from the source of the emanations. In order to capture the strongest possible signals, the chip was decapsulated, and the probe's coil was lowered onto the surface of the chip. Decapsulation of the chip also allowed the structure of the chip to be viewed under a microscope, which allowed the various blocks of the chip to be identified, and isolated for analysis.[3].

4.2.2 Horizontal Probe Positioning

In order to extract the secret key, the signals captured must be data dependant. This means that the probe must be positioned near an area of the chip that leaks EM radiation while the algorithm is running. It is expected that the most data dependent signals will be emanating from the CPU as this is where the execution of the algorithm is taking place. I believe that signals from the RAM of the chip may have some relevance to the crytographic key, as data is read to and written from RAM during the execution of the DES encryption algorithm. I believe that traces from the vicinity of the EEPROM and ROM will not yield any information relating to the cryptographic key.

5 Results

Signal Location

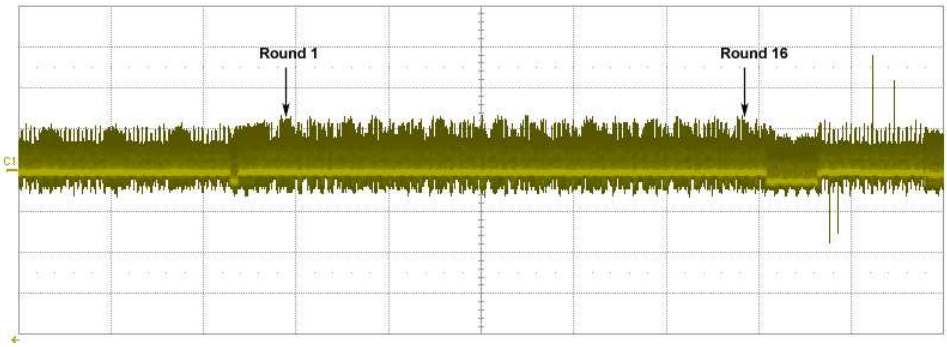

Figure 2: Power consumption during DES 16 rounds

The power trace shown in Figure 2 shows 16 distinct peaks, which correspond to the 16 rounds of DES.

In order to position the probe to capture a data dependent EM trace it was very useful to identify the different components of the chip. Figure 3 shows the surface of the chip as seen under the computer microscope. Since the chip has been decapsulated, it is possible to identify the various components, and avoid scanning the surface of the chip manually.

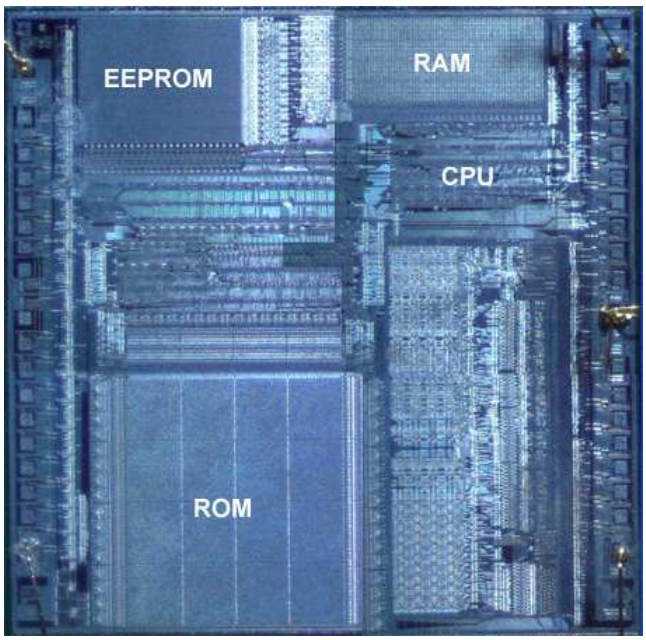

Figure 3: The surface of the chip

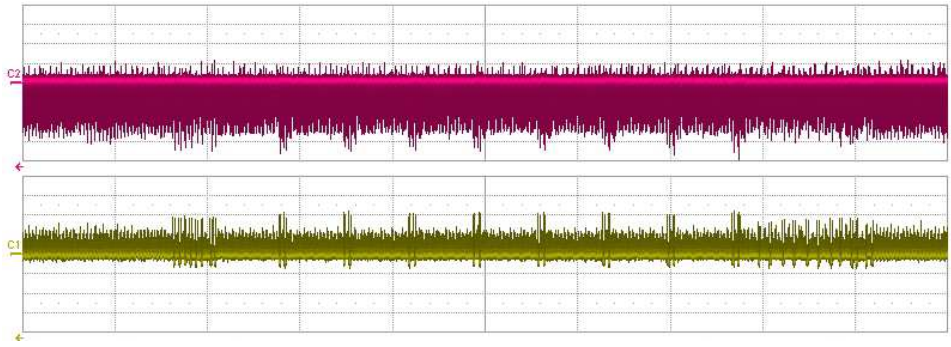

Figure 4: EM emanations from CPU during DES first round

Figure 4 shows EM emanations in the upper trace with power in the lower trace for comparison. The CPU gives a lot of signal, as this is where the DES execution takes place.

5.1 Analysis

A sample of 1000 traces were collected, and analysed.

5.1.1 Differential Curves

Figure 5 shows the differential curve calculated by the analysis software for an incorrect guess of the 6-bit S-Box input.

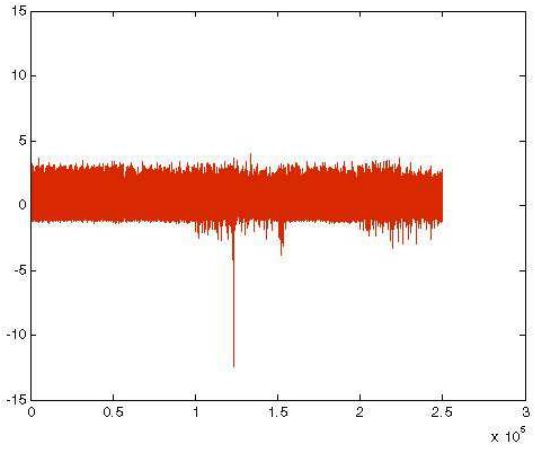

Figure 5: Differential curve for incorrect guess

Figure 6 shows the differential curve for the correct guess of the 6-bit S-box input.

It can be clearly seen that the differential curve for the correct guess has much higher peaks than the curve for the incorrect guess. Similar traces were

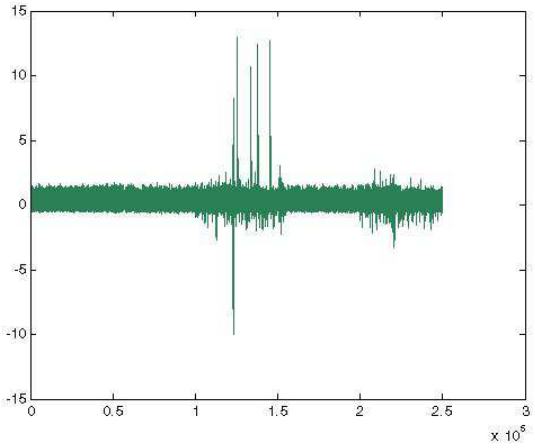

Figure 6: Differential curve for correct guess

calculated for the remaining seven S-boxes, and the correct 6-bit input guesses were identified.

6 Conclusion

This paper demonstrates that it is possible to perform an Electromagnetic Analysis attack using limited technical knowledge, and inexpensive equipment. EM traces were successfully acquired from the sample card, and the analysis software successfully identified the correct key guesses in proprietary traces.

It is important to note that although this attack was implemented on a smart card running the DES encryption algorithm, that the same kind of attack is possible on other cards as long as the implementation details of the algorithm are known.

Although this paper demonstrates an EMA attack on a decapsulated card, it is possible to perform the same kind of attack on a fully packaged smart card when using an alternative probe design[6]. Also, for industrially equipped attackers it may be possible to repackage the chip after the attack has been performed, and return it to its rightful owner without any evidence of the attack having been performed.

7 Countermeasures

With careful design and implementation, it is possible to incorporate countermeasures that defend against side-channel attacks such as EMA. Some of these countermeasures will now be outlined.

Hardware countermeasures to protect chips against EM attack include adding a metal layer to the chip, to contain the radiation, and placing an active grid on top of the chip to introduce more noise into the EM field, blurring the emanations. Radiation can also be reduced by shrinking the technology, and using smaller transistors in the construction of the chip.[3] All of these measures will reduce the leakage of useful information via the EM side-channel, which will greatly increase the amount of samples needed to perform a successful attack, possibly making the attack infeasible. An attacker with infinite samples however would still be able to perform an EMA attack on the reduced signal. It is also possible that in the future, alternatives to semiconductor technology will be developed that do not leak information, and semiconductors will no longer be used. Adding photosensitive circuitry to the chip, so that it will cease to function when exposed to light, would complicate the decapsulation process, as well as the acquisition phase.

Since EMA requires the attacker to know the time at which a certain bit is manipulated, inserting random time delays in the execution of the algorithm would help prevent against the attack. An even more effective measure would be to introduce random clock-cycles, which would mean the EM traces were not synchronized, and calculating average and differential traces would be far more difficult.[7]

Other measures such as nonlinear key updates can help prevent attackers from being able to correlate power traces with encryption operations. Also key use counters can be used to prevent attackers collecting the large samples necessary in order to perform the attack.[2]

8 About

About NGSSoftware

NGSSoftware is the trusted supplier of specialist security software and hi-tech consulting services to large enterprise environments and governments throughout the world. Voted "best in the world" for vulnerability research and discovery in 2003, the company focuses its energies on advanced security solutions to combat today's threats. In this capacity NGSSoftware act as adviser on vulnerability issues to the National Infrastructure Security Co-ordination Centre (NISCC). NGSSoftware maintains the largest penetration testing and security cleared CHECK team in EMEA. Founded in 2001, NGSSoftware is headquartered in Sutton, Surrey, with research offices in Scotland, and works with clients on a truly international level.

About NGSSoftware Insight Security Research (NISR)

The NGSSoftware Insight Security Research team are actively researching and helping to fix security flaws in popular off-the-shelf products. As the world leaders in vulnerability discovery, NISR release more security advisories than any other commercial security research group in the world.

References

[1] Paul C. Kocher: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, Advances in Cryptology-Crypto 96, Lecture Notes in Computer Science # 1109, pp 104113.

[2] Paul Kocher, Joshua Jaffe, and Benjamin Jun: *Differential Power Analysis*, `http://www.cryptography.com/dpa/technical/index.html`.

[3] Karine Gandolfi, Christophe Mourtel, and Francis Olivier: *Electromagnetic Analysis: Concrete Results*, In the Proceedings of theWorkshop on Cryptographic Hardware and Embedded Systems 2001 (CHES 2001), LNCS 2162 Paris, France, May 2001, pp 251261.

[4] Micheal Tunstall: *Attacks on smartcards*, Smart Card Lecture Notes, Royal Holloway Information Security Group, 2005.

[5] Thomas S. Messerges Ezzy A. Dabish and Robert H. Sloan: *Investigations of Power Analysis Attacks on Smartcards*, In Proc. of the usenixWorkshop on Smartcard Technology (Smartcard'99). usenix Association, 1999.

[6] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi: "The EM Side-Channel(s):Attacks and Assessment Methodologies"

[7] Oliver Kömmerling, Markus G. Kuhn: *Design Principles for Tamper-Resistant Smartcard Processors*, In USENIX Workshop on Smart Card Technology, 9-20, 1999.

[8] Elke De Mulder, Pieter Buysschaert, Siddika Bera Örs: *Electromagnetic Analysis*, `www.informatik.uni-hamburg.de/SVS/teaching/ss2005/oberseminar/`.

[9] Stefan Mangard: *Exploiting Radiated Emissions EM Attacks on Cryptographic ICs*, Proceedings of Austrochip 2003, October 3, 2003, Linz, Austria.

[10] Vincent Carlier, Hervé Chabanne, Emmanuell Dottax and Hervé Pelletier: *Electromagnetic Side Channels of an FPGA Implemenation of AES*, `eprint.iacr.org/2004/145.pdf`.

[11] J-J. Quisquater and D. Samyde: "A new tool for non-intrusive attacks of smart cards based on elctro-magnetic emissions, the SEMA and DEMA methods"

[12] Pankaj Rohatgi, Dakshi Agrawal, Bruce Archambeault, Suresh Chari, and Josyula R Rao: *Power, EM and all that: Is your crypto device really secure?*, `http://www.cacr.math.uwaterloo.ca/conferences/2003/ecc2003/`.

[13] Paul Kocher, Joshua Jaffe, and Benjamin Jun: *Introduction to Differential Power Analysis and Related Attacks*, `http://www.cryptography.com/dpa/technical/index.html`.

[14] Manfred Aigner and Elisabeth Oswald: *Power Analysis Tutorial*, `www.iaik.tugraz.at/aboutus/people/oswald/papers/`.

[15] Mathieu Ciet, Francesco Sica, and Jean-Jacques Quisquater: *On The Security of Certain DPA Countermeasures*, Proceedings of the 25 th Symposium on Information Theory in the Benelux, R. Pellikaan Ed., published by Werkgemeenschap voor Informatie-en Communicatietheorie Eindhoven, 2004.