A Wireless Covert Channel on Smart Cards (Short Paper)

Geir Olav Dyrkolbotn and Einar Snekkenes

Norwegian Information Security Lab
Department of Computer Science and Media Technology
Gjovik University College
P.O. Box 191 2802 Gjovik, Norway
geirolav.dyrkolbotn@gmail.com, einar.snekkenes@hig.no

Abstract. Microprocessor devices, such as smart cards, are used more and more to store and protect secret information. This development has its advantages, but microprocessor devices are susceptible to various attacks. Much attention has been devoted to side-channel attacks, exploiting unintentional correlation between internal secret information, such as cryptographic keys, and the various side channels. We present a wireless covert channel attack (WCCA) that intentionally correlates secret information with the electromagnetic side channel. WCCA exploits subversive code hidden on all cards during manufacture, to launch an attack, without physical access, when infected cards are used. Experiments on modern smart cards confirm that an insider with the opportunity to hide subversive code can potentially broadcast the card's internal secrets to a nearby receiver. Security features against side-channel attacks will limit the range but not prevent the attack.

Keywords: Smart Cards, EM Side-Channel, Subversion, Wireless Covert Channel.

1 Introduction

Since the birth of modern side channel attack in the 90's there has been an explosion of proposed attacks exploiting side channels to reveal secret information within a smart card. Current research focuses on exploiting unintended correlations between secret information (cryptographic key) and the side channel, tailoring a specific implementation of a cryptographic algorithm. These attacks often require a "lost or stolen" card and experimental results are often obtained on simple cards of older technology, not on modern smart cards equipped with countermeasures.

By combining the efforts of different fields, electromagnetic side channel attacks , covert channels and subversion, we propose a new attack: wireless covert channel attack (WCCA). We believe that hiding subversive code on cards during manufacture can manipulate the energy leakage from a smart card to create a covert broadcast channel. The channel is activated when cards are used in a normal scenario and will give us access to secret information remotely (i.e. wireless),

P. Ning, S. Qing, and N. Li (Eds.): ICICS 2006, LNCS 4307, pp. 249–259, 2006.

without the need for physical access to the target. The attack is tailored the microprocessor architecture rather than the actual cryptographic algorithm and experiments confirm that the attack will work on modern smart cards equipped with countermeasures against side channel attacks.

This article will explain how to collect and analyze electromagnetic emanation from smart cards to build signatures of individual instruction executed by the microprocessor. These signatures will form a symbol alphabet for a covert communication channel. Subversive code hidden on the smart card will create the covert channel and use it to broadcast secret information to a nearby receiver. Practical result obtained on modern smart cards (identity withheld due to a Non Disclosure Agreement) equipped with counter measures will be shown.

2 Previous Work

The basis for side-channel attacks has been available for a long time. It is possible to use the second law of thermodynamics to show that energy must escape from devices in one way or another(e.g. heat) [1]. The laws of physics explain that it is impossible for any operating device not to leak energy. The goal of side-channel attacks is to look for dependencies between this unavoidable energy leakage and the device's secret parameters.

Exploiting this leakage is not new. Military and government organizations have supposedly used them for a long time, with public interest beginning much later. In 1985 Van Eck [2] published the article on how to eavesdrop video display units via radiation from a considerable distance that attracted much attention. In 1996 Anderson and Kuhn published their work, *"Tamper Resistance - A Cautionary Note"* [3], which showed that trusting tamper resistant devices can be problematic. That same year Kocher [4] published his work on exploiting differences in execution time (Timing Attacks). This work was soon followed up and in 1999 Kocher et al. [5] introduced some powerful attacks through measurement of a device's power consumption. Simple Power Analysis (SPA) and Differential Power Analysis (DPA) received some attention from, among others, the banking industry, and countermeasures were publicly announced. In 2000, Quisquater and Samyde [6,7] applied the analysis technique from SPA and DPA to electromagnetic side-channels, thus introducing electromagnetic analysis (EMA).

In recent years several papers have been published in an ongoing effort to systematically investigate electromagnetic side-channel attacks[8,9,10,11,12]. The experiments have been extended to some distance from the target, implying that physical access to the target may not be necessary. It has been shown that EMA is at least as powerful as power analysis, and that EMA could circumvent power analysis countermeasures [10,13]. At USENIX 2002 [14], Quisquater and Samyde described an automatic method to classify instructions, carried out by a simple CISC processor. The power and electromagnetic signature of instructions were captured and then used to train a neural network. The neural network could automatically recognize, and thus reverse engineer, executed code based on stored electromagnetic and power signatures.

Common for previous attacks is that they exploit unintentional correlations between the side-channel and secret information, often a cryptographic key. Taking a more aggressive approach would be to manipulate the side-channel. It is not difficult to imagine a situation were the code on the smart card is manipulated to give specific results for the neural network of Quisquater and Samyde [14].

Covert communication was first introduced by Lampson in 1973 and was then defined as

> A communication channel is covert if it is neither designed nor intended to transfer information at all

An example can be found in an encrypted packet switched network. An adversary can monitor the packet flow, but can not read the encrypted content of each packet. A covert channel can be created if the following is decided beforehand.

- Packet sent from address A to B - interpret as logic 0
- Packet sent from address A to C - interpret as logic 1

This traffic will appear as regular packet switch traffic (at least to the untrained eye) and hopefully not raise any suspicions, therefore it is covert.

Another example of a covert channel can be the running time of a program. This means that the timing attack of Kocher [4] can be seen as exploiting an unintentional covert channel. Unintentional in the way that the secret information was not intentionally correlated with the timing information. Similarly, other side-channel attacks can also be seen as exploiting unintentional covert channels. Side-channels also fit Lampsons definition from 1973 as stated above.

Kuhn and Andersson [15] talk about attacking a system with malicious code that will use a computer's RF emission to transmit stolen information. The possibility to plant a virus to infiltrate a bank or certificate authority and broadcast key material over an improvised radio channel is mentioned. Practical results are shown with hidden messages in a recovered video signal. This can also be categorized as a covert channel where the electromagnetic side channel has been deliberately manipulated. This approach will be used in WCCA. We introduce the term **wireless covert channel** as *a hidden electromagnetic communication channel, detectable outside the system, as a result of intentional manipulation of valid system parameters.*

Creating a wireless covert channel can be viewed as subversion, described by Myers [16] as

> The subversion of computer systems is the covert and methodical undermining of internal and external controls over a systems lifetime to allow unauthorized and undetected access to system resources and/or information.

In the next chapter the wireless covert channel attack (WCCA) is presented.

3 Wireless Covert Channel Attack

The wireless Covert Channel Attack (WCCA) relies on a highly skilled insider to undermine the security mechanisms by hiding subversive code in the smart card's software (SW). This is done during an early stage (design or implementation) of its life cycle (figure 1) and will affect all cards produced. These infected cards may be used e.g. in the banking industry as credit cards, loaded with personal information (cryptographic key, PIN code, account number etc.) when issued to a customer. The adversary is interested in retrieving the secret, personal information and has an accomplice involved at the use stage of the life cycle. This will be somebody with access to a smart card terminal, a store owner or maintenance personnel. When a manipulated card is inserted into any terminal, by the owner, the subversive code exploits characteristic electromagnetic emanation (signatures) from the microprocessor, during execution of instructions, to broadcasting secret information over a wireless covert channel. The success of this attack is ensured by the large number of cards infected. If a whole generation of smart cards to the banking industry is infected, there will be enough cards randomly used in the rigged locations to make the attack worth the effort.

WCCA can be divided into a preparation phase, an implementation phase and an exploitation phase.

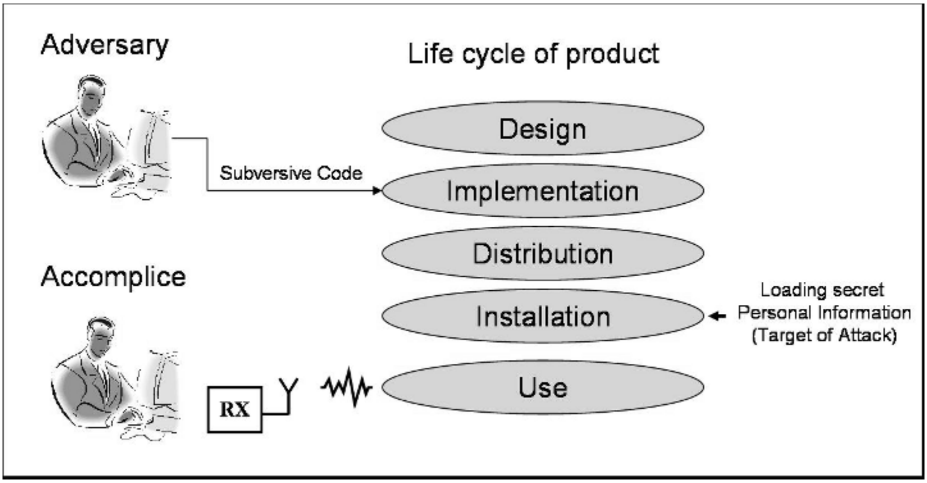

Fig. 1. Scenario: The adversary hides subversive code during an early stage. Later, secret information is loaded to the card. When the card is used, the subversive code is activated and broadcasts secret information to the accomplice.

3.1 Preparation Phase

The preparation phase is used to build a library of characteristic electromagnetic emanation from instructions executed by the microprocessor. WCCA uses the average power spectrum density (PSD) obtained from a spectrum analyzer to characterize an instruction.

For every instruction of interest, a smart card is prepared with a test code. The card inserted into a customized smart card reader will automatically start executing the test code. A small coil is placed on top of the smart card reader, as close as possible to the microprocessor, without any decapsulation. Using a spectrum analyzer, no synchronization between the executed code and the instrument is needed. The average PSD is stored on a computer for further analysis. The test code is written in assembly language and executes one instruction in a loop. The instruction is repeated several times within the loop to reduce the effect of any unwanted instructions, such as ”goto”. Each instruction was measured several times, in random order, to enhance the reliability of the data. The signature of an instruction is the mean of all these repetitions.

3.2 Implementation Phase

The implementation phase is used to design and hide the subversive code needed to create the covert channel. A symbol alphabet for the channel, as well as a carrier frequency, is obtained from analysis of the recorded signatures. The smart card executing the subversive code can be considered a bandpass digital system [17], where a carrier is modulated with binary data. In this work we restrict the discussion to a binary system, and leave M-ary bandpass digital systems for future work.

For two possible messages, m_1 and m_2, two possible waveforms $s_1(t)$ or $s_2(t)$ are transmitted in a bit interval, T_b. The waveforms $s_1(t)$ and $s_2(t)$ cannot be chosen freely, but are a result of emitted energy when executing instructions on the smart card. Since the receiver makes the decision based on received energy, it is natural to look for frequencies where the emitted energy can be controlled by execution of different instructions. Given the right receiver it should be possible to take advantage of the energy difference over a large frequency range, but in order to demonstrate the feasibility of the attack a low cost narrow band receiver was chosen. The approach is therefore to look for one carrier frequency, f_c, with a large difference in emitted energy between execution of two instructions. Exploiting the energy emitted in a larger band is subject to work in progress.

Using the recorded signatures, a carrier frequency is easily found. Let diff(i,j) be the spectral difference between signature i and j. Diff(i,j) is simply the magnitude of the difference at each sample of signature i and j. Calculating diff(i,j) for all combinations of instructions, there will be two signatures i=A and j=B that gives the maximum difference at a specific frequency. This frequency is chosen as the carrier frequency, f_c.

The emitted energy at carrier frequency f_c can now be controlled by designing a subversive code that transmits secret information using

- Instruction A - logic 0 - small energy emission at f_c
- Instruction B - logic 1 - large energy emission at f_c

Once the subversive code is designed, the task is to make sure it is hidden on every card produced, undetectable. It is beyond the scope of this article to describe this in detail. However, if third party compilers and library files have less stringent security requirements than the developed SW, and commercial interest prohibits full insight into the source code of them, it could serve as an excellent opportunity for the adversary.

3.3 Exploitation Phase

The success of the attack relies on the adversary or his accomplice placing a receiver in the vicinity of where infected cards are used. The subversive code will be executed during normal use and secret information broadcasted to any receiver in the vicinity.

The range of the covert channel will have a great impact on how difficult this will be. Given a range of several meters, the receiver can be placed somewhere in the room and maybe in an adjacent room. It may also be possible to carry a concealed receiver and stand nearby or be in the line behind the victim. If the range is in order of cm, the probe of the receiver must be placed close to the terminal. This may be possible if the accomplice is the store owner or maintenance personnel with access to the terminal.

The receiver can be optimized to cost, range, channel capacity, probability of error, size etc, but even a cheap commercial receiver used in this experiments gives promising results. Due to the relative long exposure time, when the card is used in a terminal (up to 30 sec) the bit rate does not need to be high. Assuming that the covert channel use only 1% of the processor time, reduces the risk of detection, and still gives 0.3 sec for the attack. Sending 1024 bits in 0.3 sec requires a channel capacity of only 3.5 kbits/s.

4 Experiment

The experiments have been carried out on a modern smart card with several security features against side channel attacks. The identity of the card and the details about the security features are withheld due to a Non Disclosure Agreement (NDA).

In the preparation phase, the electromagnetic signature of 25 instructions were collected. None of the instructions activated the I/O interface of the smart card. Signatures were collected with and without security features against side channel attacks activated. Spectrum analyzer Advantest 3641 was used. Measurements were done from DC to 60 MHz, with 100 averages, providing signatures of 4206 samples. Typical signatures can be seen in figure 2.

The object of the implementation phase is to analyze the 25 signatures collected and to identify frequencies where the emitted energy can be controlled by toggling between two instructions. Therefore, the spectral difference diff(i,j) is of more importance than the shape of the signature, this is shown in figure 3. The maximum amplitude difference for all combinations of instructions, when security features are activated, has been plotted in figure 4.

These are potential carrier frequencies for the covert channel and the corresponding instructions are used to create the subversive code. As an example,

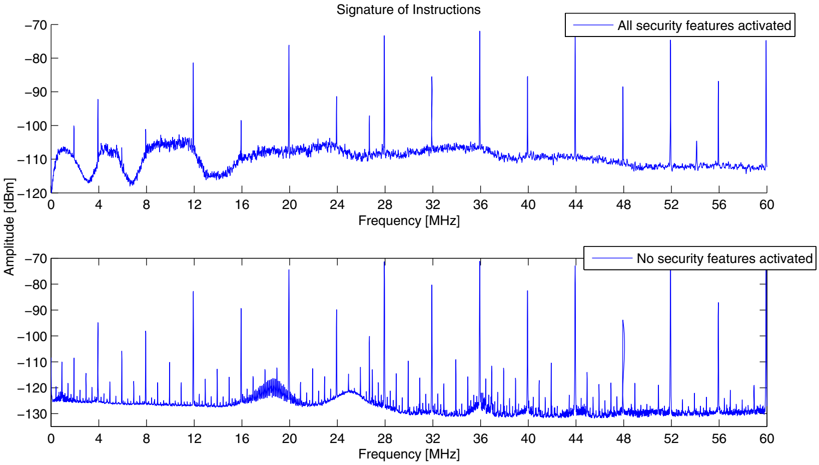

Fig. 2. Average power spectrum density as signatures of instructions. Instructions executed on card with and without security features activated.

using instruction A and B at frequency f_c=11.5 MHz provides an amplitude difference of 10.5 dB. It may be interesting to notice that the peaks around 53 to 57 MHz are introduced by one of the security features.

Three different subversive codes have been designed to test the covert channel and serves to illustrate the potential. It is assumed that the highly skilled insider will be able to create more sophisticated codes. The first code was designed to demonstrate that subversive code can manipulate the energy emitted and that the channel is detectable by a receiver. For this purpose two instructions are executed n times alternately, to create a pulse train with fundamental frequency dependent on n. With $1\mu s$ execution time of each instruction, choosing $n = 500,\ 250\ and\ 125$ results in a fundamental frequency of 1,2 and 4 kHz respectively. This is in the audible range and serves well for a demonstration with an AM receiver. The second code was designed to demonstrate that messages can be transmitted. A short or a long audible tone is used to send morse code (SOS) to the receiver. The third code broadcasts the memory contents of a smart card in an attempt to demonstrate how secret information can be compromised.

Using the ICOM IR-20 receiver with the extendable rod antenna, the audible tones and the morse code are easily detected. On a simple card the tone has been detected 10 meter from the terminal. The modern card is detectable within 1 meter even with security features activated. The covert channel is also detectable on the peaks introduced by one of the security features at 53-57 MHz. The same procedure as with morse code can be used to broadcast the memory content of a smart card to the AM receiver. This is a low rate transmission and work is in progress to improve the transmission rate.

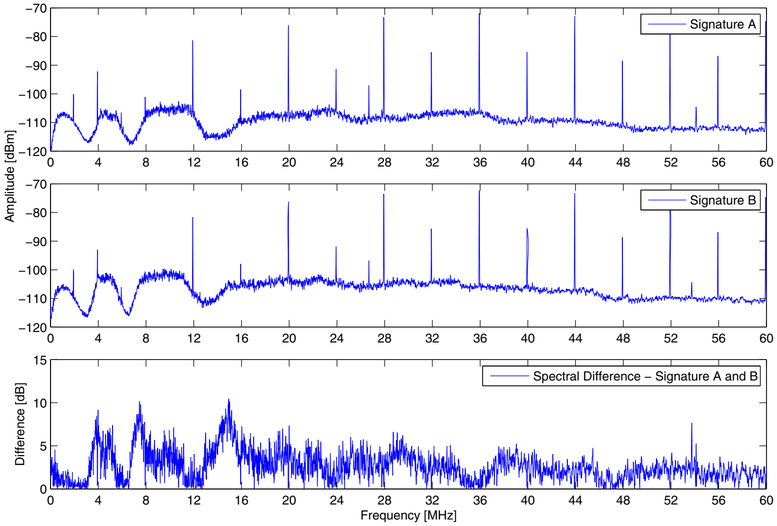

Fig. 3. Individual signatures of two instructions, with all security features activated, are shown above. In a covert channel context the spectral difference between them shown in the lower figure, illustrates our ability to manipulate the emitted energy for various frequencies.

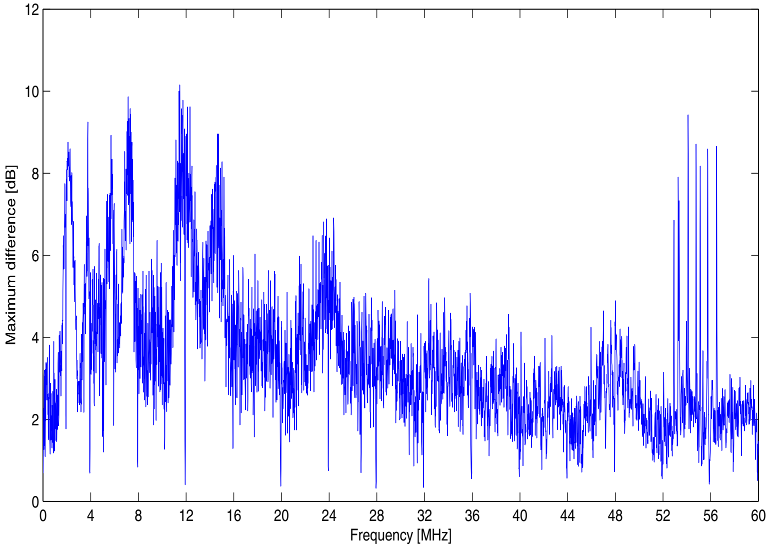

Fig. 4. The largest spectral difference for all combinations of instructions, illustrates the overall covert channel potential

5 Analysis

The feasibility of the attack has been confirmed through the use of a cheap AM receiver. An important issue left is the rate of information leakage from the smart card, the channel capacity of the covert channel.

The source rate, R, how fast the smart card (source) can transmit information, is given by [18]:

$$R = \frac{H}{T}\, bits/sec \tag{1}$$

where H is the average information (entropy) of the source , given by Shannon [19], and T is the time required to send each message. For a binary system with equal probability of sending zero and one, the entropy is H=1. Since each message, m_1 or m_2, is represented with the waveform resulting from execution of instructions, the execution speed of the microprocessor will set a lower limit on T. Assume a microprocessor architecture that requires multiple of 4 clock cycles per instruction. Choosing two, single cycle, instructions with clock frequency of 4 MHz gives $T = 1\mu s$. Using (1) a source rate of $R = 1\ Mbit/s$ is found. This is an upper limit and not very realistic as it e.g. does not take into consideration fetching the next message before sending it. By analyzing the flow chart of the test code, designed to read and broadcast the memory contents of a smart card, an average of 37 clock cycles ($T = 9.25\ \mu s$) is required to send each message. The source rate is then $R = 1/9.25\ \mu s \approx 108\ kbit/s$.

The source rate , R, is important when designing a communication channel. Shannon [19] has shown that, for the case of signal plus white gaussian noise, it is theoretically possible to have the probability of error approach zero for a channel capacity of C bits/sec, as long as $R < C$. The equation for C is then

$$C = B \log_2(1 + \frac{S}{N}) \tag{2}$$

where B is the channel bandwidth in hertz (Hz) and S/N is the signal-to-noise power ratio (watts/watts) at the input to the receiver.

Using the recorded signature we can estimate B and S/N. B should be the lowest bandwidth in the communication chain. In our experiment this is the receiver with B=15 kHz. Using the amplitude difference in dB from diff(i,j) as the value for S/N can be justified since one of the signatures is close to the noise floor at the chosen frequency. The experiment suggested a pair of instructions with 10.5 dB difference. With a receiver bandwidth of 15 kHz this gives C=32 kb/s. This is an upper limit for error free communication that may be approached using efficient coding. The adversary is limited to the waveforms emitted when executing instructions and cannot hope to achieve this capacity. However, a transmission rate of one tenth of C is realistic and can be sufficient. A key of 1024 bits is transmitted in 32 ms at 3,2 kb/s. Assuming 1 % processor load for the covert channel requires the card to be turned on for 32 seconds, which is not unreasonable in e.g. a bank terminal.

Care must be taken if the requirement of $R < C$ is violated. This is not a problem if handled properly, R can be decreased or C increased. Reducing the rate of transmission is not a problem and can be solved with different coding techniques. A simple approach can be to represent each message m_1 and m_2 with n execution of an instruction, where n is chosen such that $R < C$. The drawback is that the risk of exposing the subversive code increases as the size and execution time of the code increases. Increasing C can be done by increasing the bandwidth of the receiver or the S/N ratio at the receiver. An interesting approach would be to exploit differences between signatures at several different frequencies as opposed to one frequency.

The results in this experiment are believed to be moderate, as many improvements are possible. One obvious improvement would be to use a receiver with larger bandwidth. Work is in progress to calculate the potential channel capacity when the transmitter and not the receiver is the limiting factor for bandwidth.

Finally, some remarks about countermeasures. It is beyond the scope of this article to suggest new or improved countermeasures, but maybe it will serve as a reminder that countermeasures should be considered for the entire life cycle of the product and for the entire system, including third party SW, terminals and locations of use. It is also important to remember that in a complex system, introducing new functionality may have unwanted side effects. This has been demonstrated in this experiment as one security measure against side-channel attacks introduced a peak that could be exploited as a covert channel.

6 Conclusion and Future Work

This article presents a new attack on smart cards. The wireless covert channel attack (WCCA) combines theory from subversion and covert channels with side channel attack.

Experiments have shown that by manipulating the energy leakage from a smart card can create a covert channel that will give access to secret information when the card is used and that the attack will work on modern smart cards equipped with countermeasures against side channel attacks. It has been estimated that transmitting secret information at a rate of 108 kb/s is possible from the tested card.

Work in progress include designing a receiver to match this transmission rate by exploiting energy differences in a larger frequency range.

Acknowledgements. We would like to thank Arne Wold, at Gjovik University College, for helpful discussion and guidance related to the analysis of the results.

References

1. D. C. Giancoli. *Physics for Scientists and Engineers.* Prentice Hall, 1989.
2. W. van Eck. Electromagnetic radiation from video display units: An eavesdropping risk. *Computers & Security*, 4:269–286, 1985.
3. R. Anderson and M. Kuhn. Tamper resistance-a cautionary note. In *USENIX E-Commerce Workshop*, USENIX Press, pages 1–11, 1996. ISBN 1-880446-83-9.

4. P. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in Cryptology-Crypto 96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer-Verlag, 1996.
5. P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in Cryptography - Crypto 99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.
6. J-J. Quisquater and D. Samyde. A new tool for non-intrusive analysis of smart cards based on electromagnetic emissions:the sema and dema methods. *Eurocrypt rump session*, 2000.
7. J-J. Quisquater and D. Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *Esmart 01*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer-Verlag, 2001.
8. S. Chari, J.R. Rao, and P. Rohatgi. Template attack. In *CHES'02*, volume 2523 of *Lecture Notes in Computer Science*, pages 13–28. Springer-Verlag, 2003.
9. D. Agrawal, B. Archambeault, J.R. Rao, , and P. Rohatgi. The em side-channel(s):attacks and assessment methodologies. In *CHES'03*, Lecture Notes in Computer Science. Springer-Verlag, 2003.
10. D. Agrawal, B. Archambeault, J.R. Rao, and P. Rohatgi. The em side-channel(s). In *Cryptographic Hardware and Embedded Systems - CHES'02*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer-Verlag, 2003.
11. D. Agrawal, B. Archambeault, S. Chari, J.R. Rao, and P. Rohatgi. Advances in side-channel cryptanalysis, electromagnetic analysis and template attacks. *CryptoBytes*, 6(1):20–32, Spring 2003.
12. D. Agrawal, J.R. Rao, and P. Rohatgi. Multi-channel attack. In *CHES'03*, volume 2779 of *Lecture Notes in Computer Science*, pages 2–16. Springer-Verlag, 2003.
13. J.R. Rao and P. Rohatgi. Empowering side-channel attacks. volume 037 of *IACR ePrint*, 2001.
14. J-J. Quisquater and D. Samyde. Automatic code recognition for smart cards using a kohonen neural network. In *5th Smart Card Research and Advanced Application Conference*. USENIX, 2002.
15. R. Anderson and M. Kuhn. Soft tempest: Hidden data transmission using electromagnetic emanations. In *2nd Workshop on Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 124–142. Springer-Verlag, 1998.
16. P.A. Myers. Subversion: The neglected aspect of computer security. Master's thesis, Naval Postgraduate School, 1980.
17. Jr. P.Z. Peebles. *Digital Communication Systems.* Prentice Hall, 1987.
18. L.W. Couch II. *Digital and Analog Communication Systems.* Macmillan, 1993.
19. C.E. Shannon and W. Weaver. *The Mathematical Theory of Communication.* University of Illinois Press, 1998.