Chapter 15
Electromagnetic Attacks and Countermeasures

Pankaj Rohatgi

15.1 Introduction and History

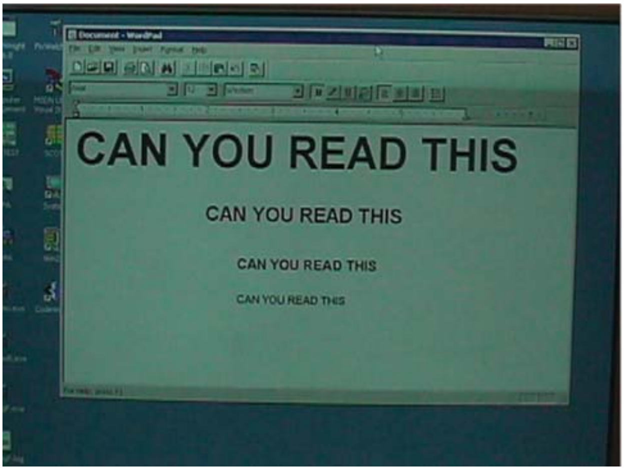
EM is a side-channel with a long history of rumors and leaks associated with its use for espionage. It is well known that defense organizations across the world are paranoid about limiting EM emanations from their equipment and facilities and conduct research on EM attacks and defenses in total secrecy. In the United States, such work is classified under the codename "TEMPEST" which is believed to be an acronym for "transient electromagnetic pulse emanation standard". In January 2001, in response to a Freedom of Information Act (FOIA) request, some documents related to TEMPEST such as *NACSIM 5000 tempest fundamentals*, *NACSEM 5112 NONSTOP evaluation techniques* and *NSTISSI no. 7000 TEMPEST countermeasures for facilities* were released in redacted form and can be downloaded from the website http://www.cryptome.org.

In the public domain, the significance of the EM side-channel was first demonstrated by van Eck in 1985 [11]. He showed that EM emanations from computer monitors could be captured from a distance and used to reconstruct the information being displayed. Figures 15.1 and 15.2 show a modern day recreation of this attack, where the contents of the computer monitor displaying a Word document in Figure 15.1 have been reconstructed in Figure 15.2 using only the EM emanations from that monitor. As a defense against this attack, Kuhn and Anderson in 1998 [8] developed special fonts which have substantially reduced EM leakage characteristics which make them difficult to reconstruct.

The first openly published works on EM analysis of ICs and CPUs performing cryptographic operations by Quisquater and Samyde [9] and by Gandolfi, Mourtel and Olivier [5] in 2001 were quite limited. These attacks were performed on chip cards and required tiny antennas to be placed in very close proximity to the IC being attacked. In fact, the best attacks were semi-invasive, requiring the decapsulation

IBM T. J. Watson Research Center
e-mail: rohatgi@us.ibm.com

Ç.K. Koç (ed.) *Cryptographic Engineering*, DOI 10.1007/978-0-387-71817-0_15,



Document - WordPad

CAN YOU READ THIS

CAN YOU READ THIS

CAN YOU READ THIS

CAN YOU READ THIS

Fig. 15.1 Computer display.

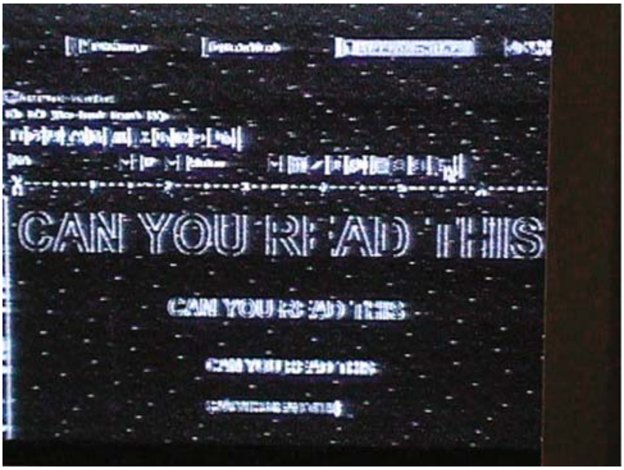


Fig. 15.2 Computer display reconstructed from EM.

of the chip packaging and careful positioning of micro-antennas on the passivation layer of the chip substrate to isolate the signals of interest. The EM signals were used to demonstrate attacks such as simple and differential EM analysis (SEMA/DEMA).

Subsequently the work of Agrawal, Archambeault, Rao and Rohatgi in 2002 [1], which was much closer to the declassified TEMPEST literature, removed these limitations and showed that EM attacks on CPUs and cryptographic devices were possible at a distance and that the EM side-channel leaks information that is not easily available from the power side-channel. This work included a systematic study of EM leakages from computing equipment and peripherals, such as chip cards, CPUs, crypto accelerators, monitors, keyboards and peripherals, comparison of the EM side-channel to other side-channels and a methodology for leakage assessment. This work has appeared in cryptology ePrint archives May 2001, CHES 2002, CHES 2003, RSA Labs CryptoBytes Spring 2003 and forms the basis for this chapter.

15.2 EM Emanations Background

A deep understanding of the different types of EM leakages and the propagation of EM signals are essential in order to conduct EM side-channel attacks and to develop techniques to defend against such attacks.

Some of the earlier published work on EM emanations focused on one particular form of EM leakage, i.e., the *direct emanations* from chip cards and good quality direct EM emanations turned out to be very hard to capture without invasive techniques and careful micro-antenna positioning. In reality, once the different forms of EM emanations are understood, there are usually several possible EM signals that can be easily captured from a device and used for EM analysis. In fact a single EM sensor may be able to multiply EM signals even from a distance. This fact is succinctly captured in the following quote from the NASCIM 5000 Tempest Fundamentals document.

> "The forms in which compromising emanations might appear at an interception point are numerous."

15.2.1 Types of EM Emanations

There are two broad classes of EM emanations:

1. Direct Emanations: These emanations result from *intentional* current flows within circuits. These generate time-varying electric and magnetic fields related by Maxwell's equations. In CMOS circuits, these current flows consist of short bursts of current with sharp rising edges that occur during the switching operation and result in EM emanations observable over a wide frequency band. Often, higher frequency emanations are more useful to the attacker since there is substantial noise and interference in the lower frequency bands. In complex circuits, it may be quite difficult to isolate direct emanations due to interference from other signals. Reducing such interference requires tiny probes positioned very close to the signal source and/or special filters to separate the desired signal from other interfering signals.

The initial published work on EM analysis by Quisquater and Samyde [9] and Gandolfi, Mourtel and Olivier [5] focused exclusively on direct emanations, in particular they focused on using tiny coils to capture the time-varying magnetic fields created by intentional currents.

2. Unintentional Emanations: Most modern devices pack a large number of circuits and components into a very small area and suffer from numerous unintentional electrical and electromagnetic couplings between components, depending on their proximity and geometry. The vast majority of these couplings are minor and are ignored by circuit designers since they do not affect functionality. Such couplings, however, are a rich source of compromising emanations. These emanations manifest themselves as **modulations** *of carrier signals* generated, present or introduced within the device. Depending on the type of coupling, the carrier can be *amplitude modulated* or *angle modulated* by the sensitive signal, or the modulation could be more complex. If a modulated carrier can be captured, the sensitive signal can be recovered by an EM receiver tuned to the carrier frequency and performing the appropriate demodulation.

The various types of EM emanations are succinctly described in the following quotes from NACSIM 5000 Tempest Fundamentals document:

> “The strongest and most numerous electromagnetic emanations are generated by sharp-rising and current waveforms of short duration $\cdots$. Also, faster rise times generate additional emanations – harmonics – of progressively lower amplitudes from the same pulse source, these harmonics $\cdots$ represent, in effect, a great many compromising signals. These signals can be acquired not only by being correctly tuned to the fundamental frequency, but also at any of the harmonic frequencies $\cdots$. At times, in fact, harmonics are more useful than the fundamental, i.e., Emanations at the fundamental frequency are often lost among other signals of the same frequency, whereas a harmonic might be more easily isolated.”
>
> ...
>
> “Modulated spurious carriers (U). - This type of CE is generated as the modulation of a carrier by RED data. $\cdots$. The carrier is usually amplitude or angle-modulated by the basic red data signal. Or a signal related to the basic RED data signal, which is then radiated into space or coupled into EUT external conductors.”

Exploiting direct emanations requires close physical proximity to be effective. In contrast, unintentional emanations are usually much easier to capture and exploit since some modulated carriers are much stronger and propagate much further than direct emanations. This enables attacks to be carried out at a distance without resorting to any invasive techniques. Rich sources of such carriers include the periodic, harmonic-rich clock signal(s) and signals used for internal and external communication. For example, an ideal, symmetric, “square-wave” clock signal depicted in Figure 15.3, when viewed in the frequency domain in Figure 15.4, consists of a dominant component at the fundamental frequency together with components at all the *odd* harmonics with linearly decreasing amplitude. In practice, the actual clock signal is far from ideal and usually contains a limited number of significant odd harmonics and some even harmonics as well.

15.2.2 EM Propagation

EM emanations can propagate both via radiation and via conduction. Often, EM emanations arrive at an intercept point by a complex combination of radiation and conduction. This phenomenon is well described in the following quotes from NACSIM 5000 Tempest fundamentals:

> Propagation of EM Emanations
>
> “Modulated spurious carriers (U). - This type of CE is generated as the modulation of a carrier by RED data. $\cdots$ The carrier is usually amplitude or angle-modulated by the basic

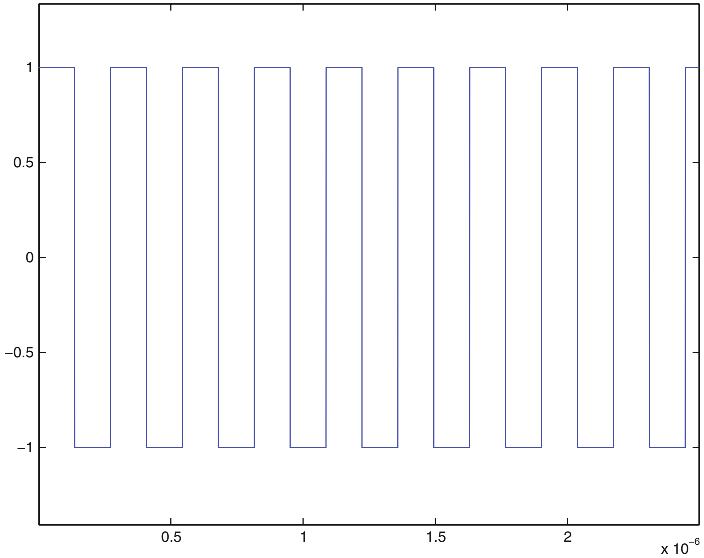


Fig. 15.3 Ideal clock signal.

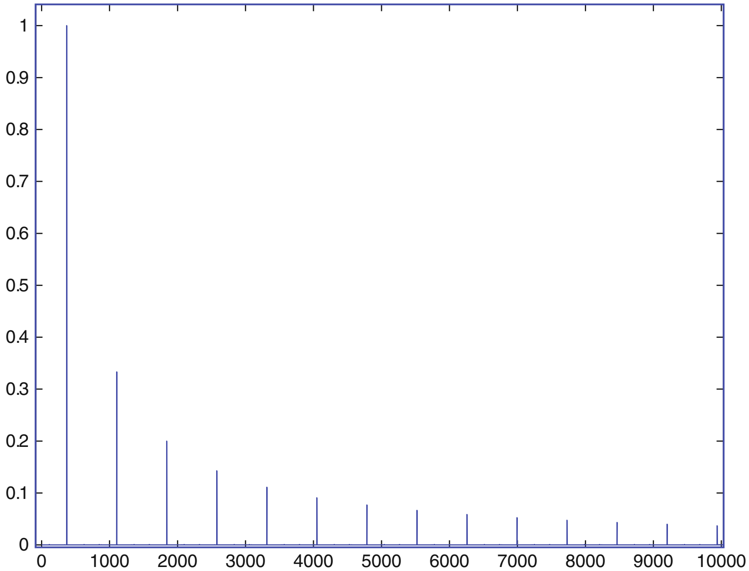


Fig. 15.4 FFT of an ideal clock: $s(t) = \frac{4}{\pi}\Sigma_{n=1,3,5,\ldots,}\frac{1}{n}\sin(n\omega t)$.

red data signal. Or a signal related to the basic RED data signal, which is then radiated into space or coupled into EUT external conductors."

...

"There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics.

> A brief explanation of each follows. a. (C) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation. b. (C) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines. c. (C) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc. d. (C) [Six lines redacted.]"

From an attacker's perspective, conducted emanations are more useful than radiated emanations. Radiated emanations attenuate rapidly with distance and need to be captured close to the device since they obey the inverse square law. Conducted emanations attenuate linearly with distance and thus can be intercepted at greater distances.

The following example illustrates conducted EM emanations. Currents on the power line of smart cards have been well studied in the context of power analysis. For example, Figure 15.5 shows the amplitude of the current flowing on the power line of a smart card while it is performing three rounds of DES. This fact is clearly visible in the power signal which shows a basic signal shape for a DES round that is repeated three times during this time window. Now the power line is also a conductor and therefore is likely to carry conductive EM emanations as well. The faint, AM-modulated EM signals at low carrier frequencies are overwhelmed by larger power-

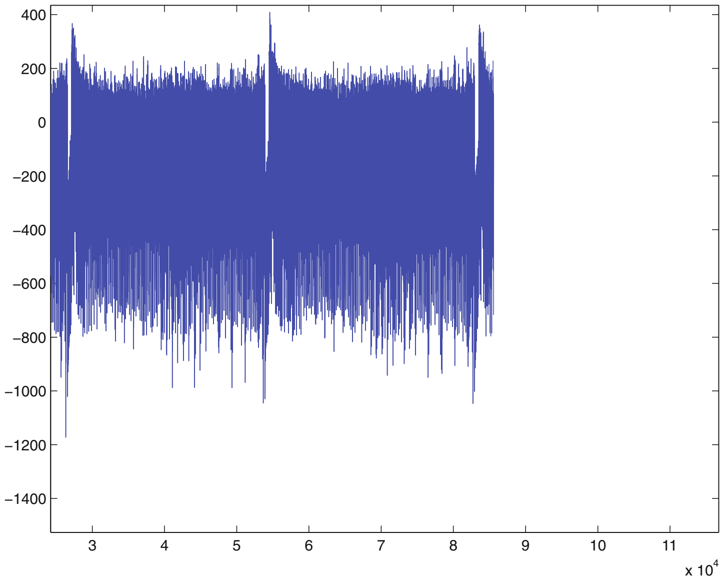


Fig. 15.5 Raw power signal during three rounds of DES.

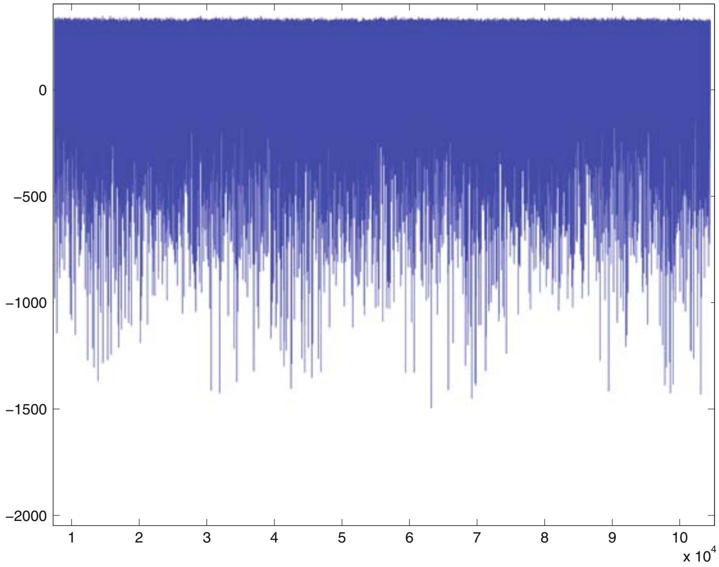


Fig. 15.6 Conducted EM signal on the power line during three rounds of DES.

consuming currents, but the faint, AM-modulated EM signals at higher carrier frequencies can be easily separated and demodulated to yield compromising information. Figure 15.6 shows the demodulated EM signal obtained from the power line, which also displays a (different) basic shape for a DES round repeated three times.

15.3 EM Capturing Equipment

Like power analysis, an EM attack system requires sample collection equipment such as a digital oscilloscope or a sampling board as well as software for controlling device operations, triggering and controlling data collection and for signal processing and analysis.

Radiated EM signals in the near field can be captured using near-field probes. Signals in the far field can be captured by antennas appropriate for the band being considered. Antennas and probes are not expensive and can even be constructed at low cost. Conducted emanations on the power or ground lines are best captured using LISNs (line impedance stabilization networks) and signals from fortuitous conductors can be processed directly.

The *critical* piece of equipment for performing EM attacks is a tunable receiver/demodulator which can be tuned to various modulated carriers and can perform demodulation to extract the sensitive signal. High-end receivers such as the Dynamic Sciences R-1550 (see [4]) are ideal for this purpose since they cover a wide band and offer a large selection of bandwidths and demodulation options. However, wideband/wide-bandwidth receivers tend to be quite expensive even when

Fig. 15.7 A second-hand wideband, wide-bandwidth receiver.

Fig. 15.8 ICOM 7000 receiver.

purchased second-hand (see Figure 15.7). Another option is to use certain wideband radio receivers that provide a large bandwidth intermediate frequency (IF) output in addition to the audio output. One such receiver is the ICOM 7000 (see Figure 15.8) which can be purchased second-hand for less than $1000. The IF output can be sampled and demodulated by software to extract the signal. However, such receivers introduce significant noise into the captured signals and are not suitable for capturing very faint signals that are close to the thermal noise floor. In addition, these receivers only provide a few MHz of bandwidth which is not enough to capture the internals of devices operating at high frequencies. Those on low budgets can construct their own low-noise receiver for under $1000 by using commonly available low-noise electronic components (see Figure 15.9), common lab equipment and demodulation software, but this approach can become inconvenient due to the need for frequent calibration. However, once the best signal to attack is identified, a custom, non-tunable receiver/demodulator for the attack can be built quite cheaply.

Common laboratory equipment such as spectrum analyzers are also very useful for quickly assessing the available EM signals to identify potentially useful carriers.

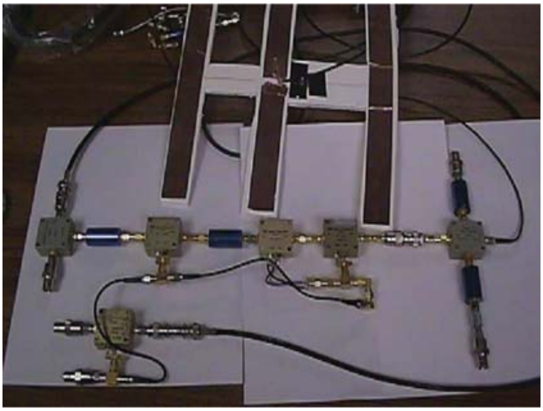


Fig. 15.9 Low-cost, low-noise receiver built from components.

15.4 EM Leakage Examples

In this section we will describe several experiments which illustrate the types of EM signals and EM side-channels available from several different devices and describe possible avenues for attack.

15.4.1 Examples: Amplitude Modulation

In our first set of experiments, we will explore EM side-channels available via amplitude demodulation of a carrier signal. Our first example is a 6805-based smart card operating on a 3.68 MHz external clock and performing the following set of three instructions continuously in a 13-cycle loop:

1. Access RAM containing a value B (5 cycles)
2. Check for external condition (5 cycles)
3. Jump back to start of loop (3 cycles)

Figure 15.10 shows the raw signal obtained by a near-field EM sensor placed behind the smart card during a time interval in which the card executed around 26 cycles or 2 iterations of the loop. The figure shows a very regular signal structure repeated 26 times. On closer examination, this regular structure turns out to be the differential of the clock signal. This is not surprising since the clock is the most dominant signal and *direct emanation* within the card. From the raw signal, it is not possible to discern the fact that the smart card is operating in a loop or to know the nature of the operations being performed. This figure also highlights the problem of working with *direct emanations*. In this case, the clock signal is so dominant that information about other currents within the smart card have been washed out. Extracting these smaller signals will require careful micro-antenna positioning in close proximity to these signal sources.

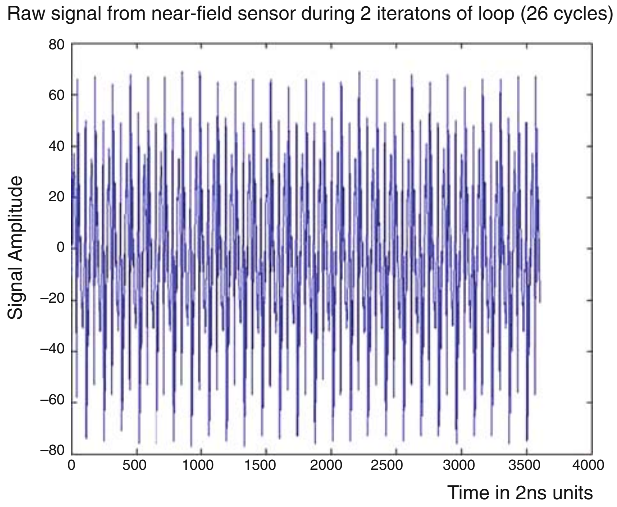


Fig. 15.10 Raw EM signal from 6805 smart card during 26 clock cycles.

This situation becomes clearer once the FFT of the raw signal is examined as shown in Figure 15.11. Here the dominant signal is the clock signal, which consists of strong components at the fundamental frequency and at odd harmonics as well as some components at even harmonics. Information about the internal operations of the smart card, such as the fact that it is operating in a loop with a frequency that is 1/13th the clock frequency, is not readily apparent in the FFT; these signals have very low amplitude and appear as noise in between the clock harmonics.

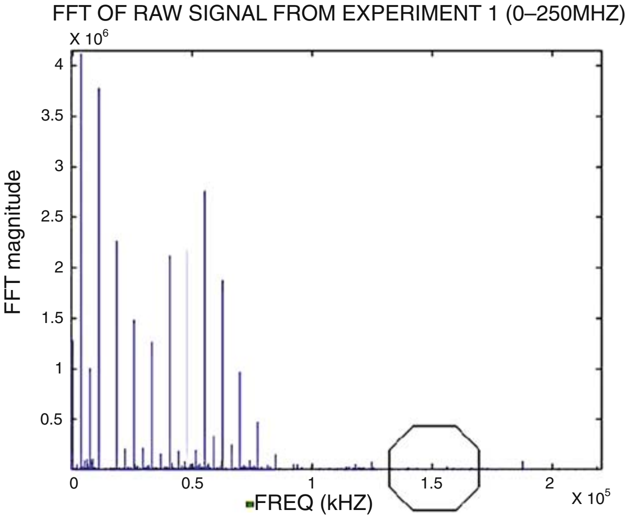


Fig. 15.11 FFT of raw EM signal from 6805 smart card.

However, at higher frequencies, say beyond 100 MHz, the amplitude of the clock harmonics have been significantly reduced and these smaller signals can be extracted via AM demodulation by tuning a receiver at one of these clock harmonics. Figure 15.12 shows the result of AM demodulating the raw signal at the 41st clock harmonic with a center frequency of around 150 MHz. The demodulated signal, which again covers around 26 cycles, shows the structure of the computation quite clearly. It is easy to see that these 26 cycles consist of a basic signal repeated twice, i.e., a loop of 13 cycles, and the internals of this basic signal show three different substructures of 5 cycles, 5 cycles and 3 cycles which represents the three instructions in the loop.

Just like the power side-channel, once the compromising EM signals are extracted, they provide details about the computation. For example using the same AM demodulating technique, if one looks at the same smart card performing DES, at a large time scale (see Figure 15.13) one can discern the 16 rounds of DES; at an intermediate time scale (see Figure 15.14) one can discern the internals of the computation during two rounds of DES; and at a very fine time scale (see Figure 15.15) one can get information at the clock cycle level.

Our second example is a Palm Pilot which has been loaded with software developed by Feng Zhu of Northeastern University to perform elliptic curve cryptography. In particular it has been programmed to perform the point multiplication operation kP where P is a point on a Koblitz curve over GF[2^{163}]. The multiplication operation is performed using Solinas's technique which replaces the traditional point doubling operation by the highly efficient Frobenius map (τ) computation as follows:

- First the secret k is decomposed into its τ-adic NAF (non-adjacent form), i.e., $k = \Sigma s_i \tau^i$ where $s_i \in 0, 1, -1$ and no two adjacent s_i's can be nonzero.

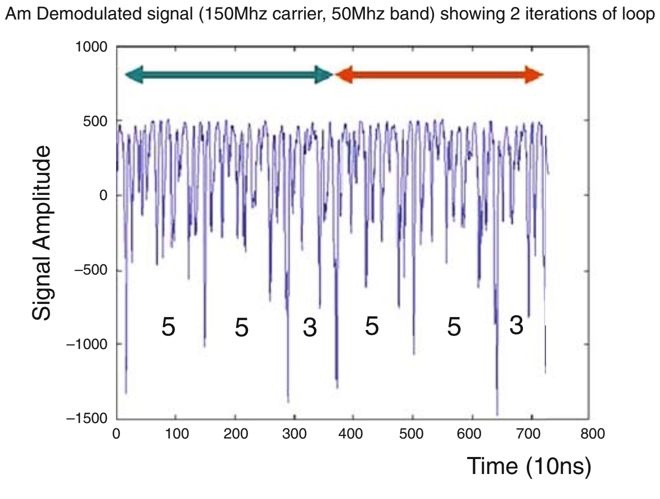


Fig. 15.12 Demodulated EM signal from 6805 smart card during 26 clock cycles.

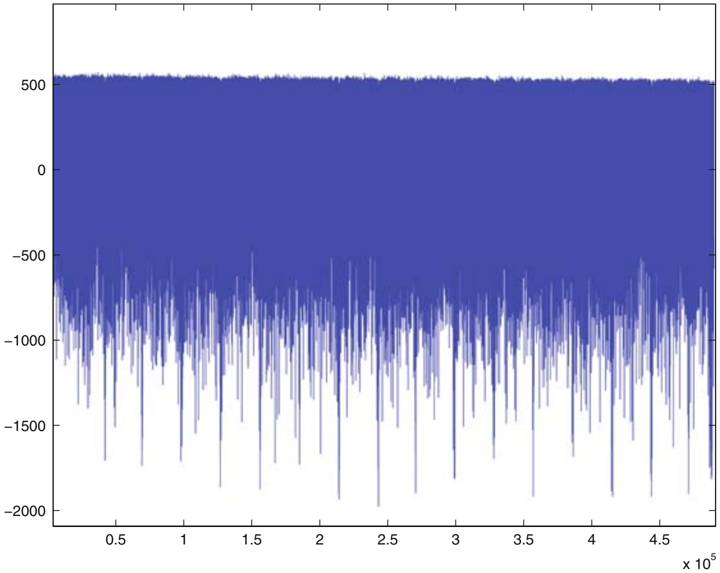


Fig. 15.13 Demodulated EM signal (100 MHz bandwidth) from smart card performing 16 rounds of DES.

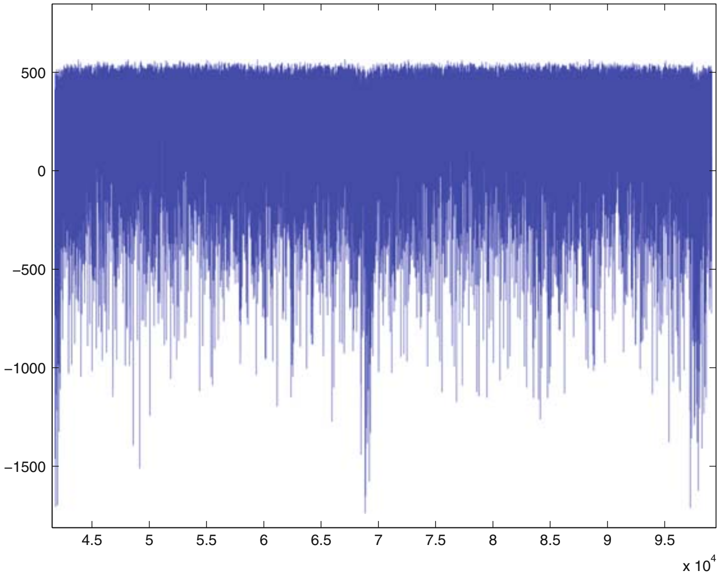


Fig. 15.14 Demodulated EM signal showing two rounds of DES (100 MHz bandwidth).

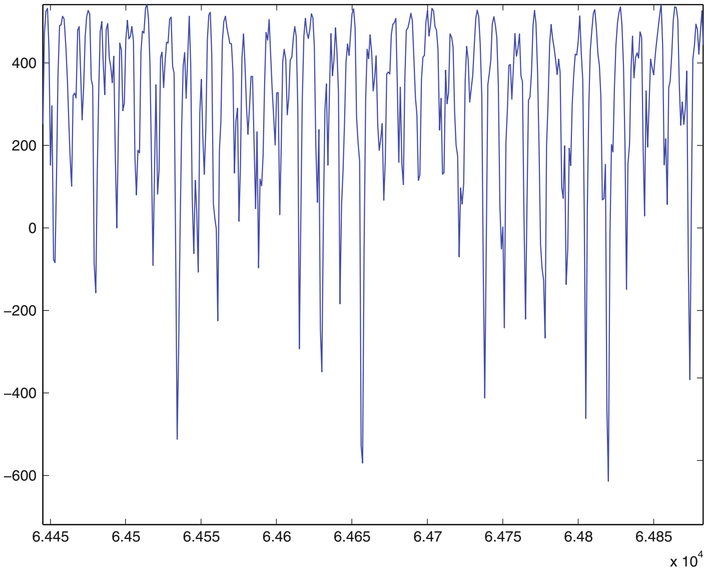


Fig. 15.15 Demodulated EM signal: clock cycle level details within a DES round.

- The traditional double/add algorithm is replaced by an algorithm that performs a sequence of τ-transforms followed by add/subtract based on the value of s_i.

The advantage of this technique is that the computational cost of the kP operation is approximately $|k|/3 \approx 54$ point additions/subtractions, since the τ-transform operation is very efficient.

The EM emanations from the Palm Pilot can be picked up even a few centimeters away from the device. A fairly good signal showing internal operations is available via AM demodulation at 241 MHz. The signal shown in Figure 15.16 immediately provides the sequence of τ-transforms (where s_i is 0) and the add/subtract operations (where s_i is $+1$ or -1). Recovering the key k further requires distinguishing between the add and subtract operations, but as Figure 15.17 shows, under intermediate level of resolution these operations are distinct. Thus we have a simple electromagnetic attack (SEMA) against this implementation.

Our final example for AM demodulation is a PCI bus-based RSA accelerator S inside a Intel/Linux server. Multiple AM-modulated carriers are available from that device, mostly at odd harmonics of the PCI clock of 33 MHz. Several carriers from this device propagate upto 50 feet and through walls enabling precise RSA timing to be measurable from around 50 feet. This precise timing could be used to perform better timing attacks than via remote interaction with the server. In addition to high-energy carriers at multiples of the PCI clock frequency, there were also several intermediate strength *intermodulated* carriers at other frequencies. These intermodulated carriers arise due to nonlinear interactions among the various carriers present within the accelerator's operating environment. These carriers provided more details

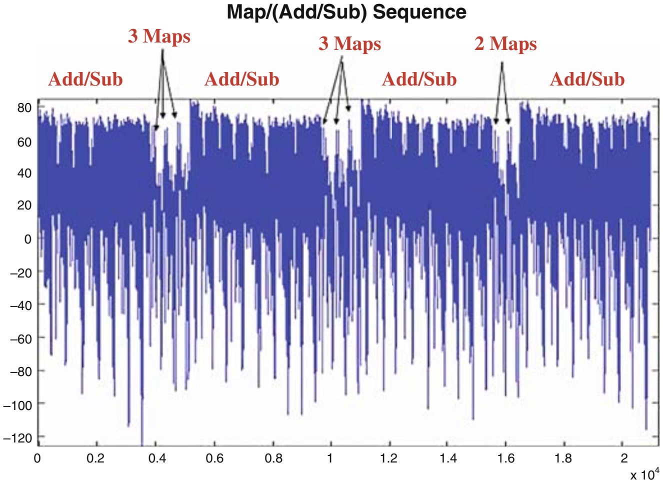


Fig. 15.16 EM signal from Palm Pilot showing elliptic curve operation sequence.

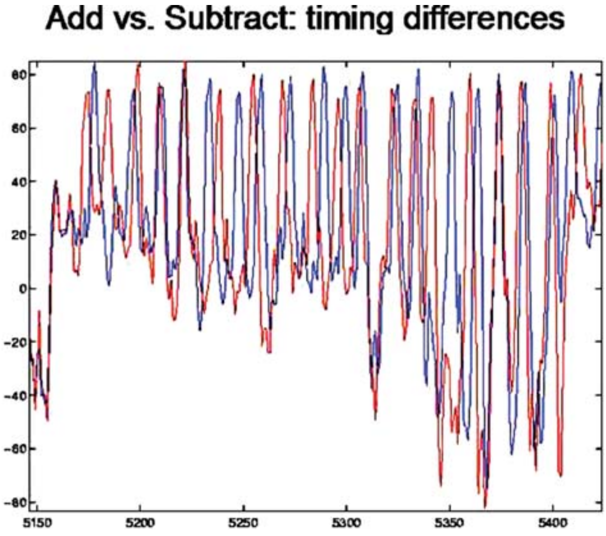


Fig. 15.17 EM signal from Palm Pilot: add vs. subtract.

of the internals of the RSA operation in S. For example, AM demodulating an intermodulated carrier at 461.4 MHz provided detailed information even from 3 to 4 feet away.

Figure 15.18 shows the signal obtained by AM demodulating the 461.46 MHz intermodulated carrier with a band of 150 KHz for a period of 2.5 ms during which S computes two successive and identical 2048-bit modular exponentiations with a 12-bit exponent. For clarity, the figure shows an average taken over 10 signal samples. One can clearly see a basic signal shape repeated twice, with each repetition

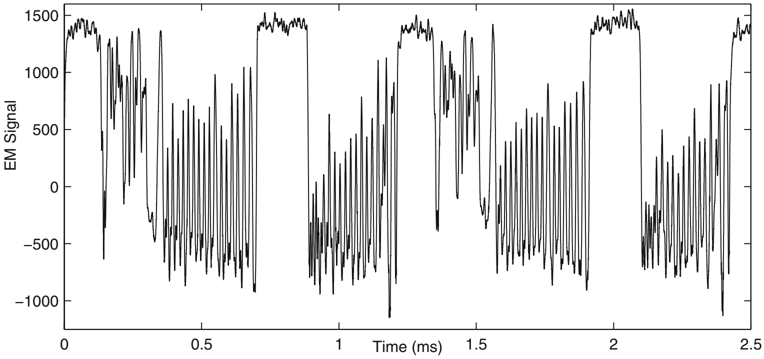


Fig. 15.18 EM signal from SSL accelerator S.

corresponding to a modular exponentiation. The first repetition spans the time interval from 0 to 1.2 ms and the second from 1.2 to 2.4 ms. The signal also shows the internal structure of the exponentiation operation. From time 0 to 0.9 ms, S receives the exponentiation request and performs some precomputation to initialize itself to exponentiate using the Montgomery method. The actual 12-bit exponentiation takes place approximately from time 0.9 to 1.2 ms. A closer inspection of this region reveals substantial information leakage which is beneficial to an adversary. Figure 15.19 plots an expanded view of this region for two different exponentiation requests which have the same modulus and exponent but different data. The two signals are plotted in different line styles (solid and broken). From the start, one can see that the two signals go in and out of alignment due to data-dependent timing of the Montgomery multiplications employed by this implementation. This data dependence of the Montgomery multiplication operation provides the basis for most of the attacks against S (see [2], [10] and [12]).

At intermediate distances of 10–15 feet, the level of noise increases significantly, but simple statistical attacks on S are still feasible and require a few thousand

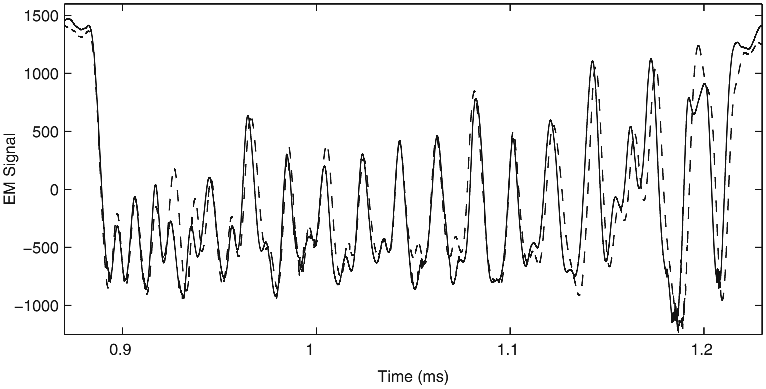


Fig. 15.19 Two EM signals, different data, same modulus, same exponent.

samples. However, attacks that are limited to one or a few samples become much harder and quickly start approaching the limits of even the advanced signal analysis techniques such as template attacks that will be described in another chapter.

15.4.2 Examples: Angle Modulation

Next we look at EM emanations that manifest as angle modulations of a carrier signal. Our first example is the same 6805-based smart card as before running the same 13-cycle loop, i.e.,

1. Access RAM containing a value B (5 cycles)
2. Check for external condition (5 cycles)
3. Jump back to start of loop (3 cycles)

but now the smart card is run on its internally generated, variable clock. In this case, as a DPA countermeasure, the clock is designed to run freely with its frequency changing with time. The smart card was tested with different values of the byte B and the following behavior was observed (see Figure 15.20): When the byte B had an LSB of 0, the loop ran faster, when it was 1 the loop ran slower. This means that the internally generated clock signal is being angle modulated by the least significant bit on the bus! The clock signal being the strongest EM signal can be captured from a distance and by angle demodulating this signal one gets information about the LSB on the bus.

The second example is another PCI-based RSA/Crypto Accelerator R inside an Intel/Linux server. After AM demodulating a 99 MHz carrier (clock harmonic) some

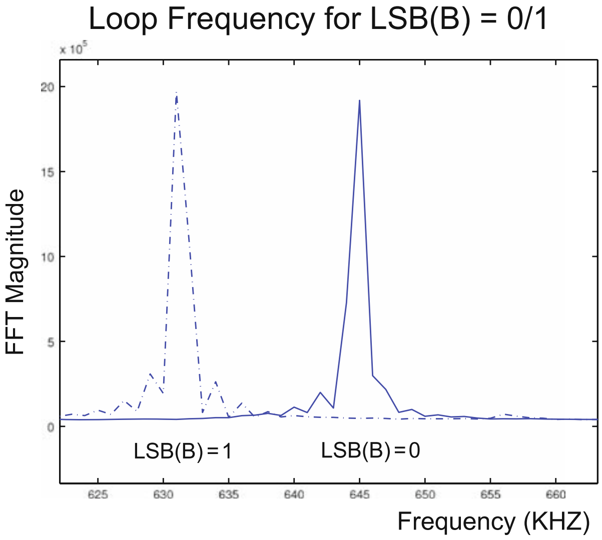


Fig. 15.20 Loop frequency related to LSB(B)!

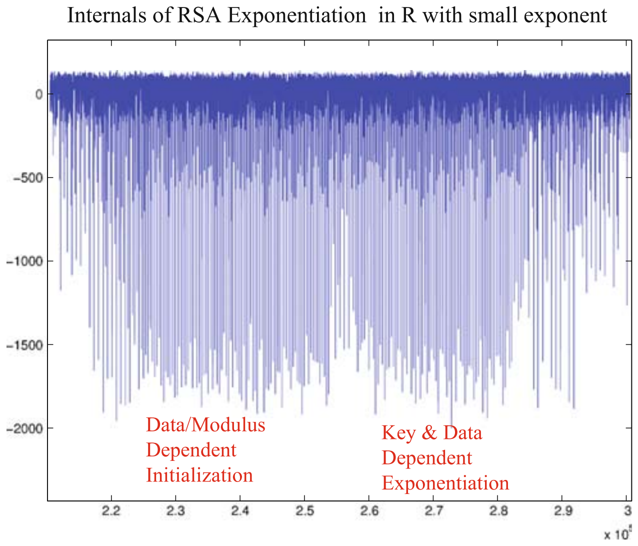

Internals of RSA Exponentiation in R with small exponent

Fig. 15.21 Macro view of internal operations within Crypto Accelerator R.

information about the internal operations of R is available as shown in Figure 15.21, where the RSA operation is seen to consist of two stages: an initialization stage followed by an exponentiation stage. However, at finer time scales, the information about the internal operations of R is obscured by another, asynchronous signal G as shown in Figure 15.22. Due to this interference it appears that one may not be able to reconstruct the internals of the RSA operation to attack this device.

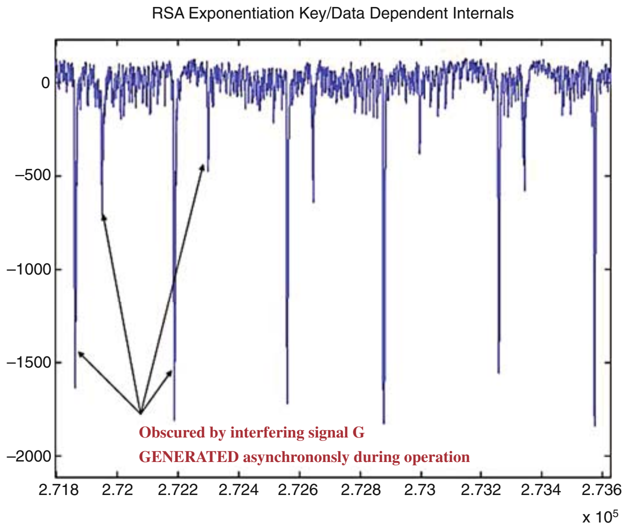

RSA Exponentiation Key/Data Dependent Internals

Fig. 15.22 Signal G obscures details of internals of R.

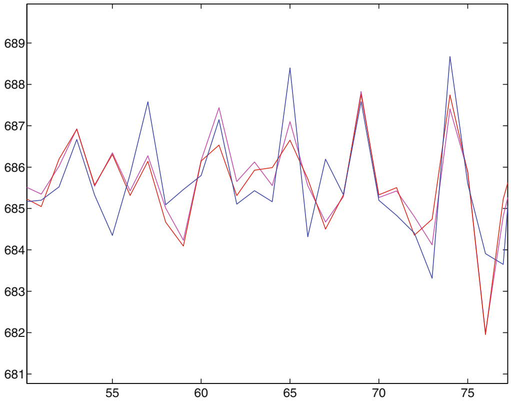


Fig. 15.23 Timing characteristics of G for three keys (two same).

But, as mentioned earlier, due to coupling effects, the timing of asynchronously generated signals is usually affected by the operations being performed within a device. This turns out to be the case for the signal G as well. Timing statistics of G (using 1000 samples) gives information about internals as can be seen in Figure 15.23, which shows the timing characteristics of G in three independent runs with three exponents, two of which are the same. This figure shows the average inter-peak time between the different peaks in G. As seen from this figure, when the keys are the same, the timing characteristics are very similar and quite different from the timing characteristics for a dissimilar key. An attacker who can get around 1000 EM samples from one device R1 can use the timing statistics of G to determine the key used by R1 if he can get access to an identical test device R2. The attacker would reconstruct the key bit-by-bit by comparing the timing statistics of the signal G for different test keys in R2 with the timing characteristics of the signal G obtained from R1. Moreover, since the signal G is strong enough to be captured even at a distance of 10–15 feet, the attack may be quite practical.

15.5 Multiplicity of EM Channels and Comparison with Power Channel

Based on the experiments described above, it is clear that there are multiple EM side-channels based on amplitude or angle demodulating different carriers which may be generated within the device, present in the environment or deliberately introduced within the device. We have also seen that often higher frequency, low-energy carriers may be more useful and leak more information than lower frequency, high-energy carriers. Also in many situation, such as attacking cryptographic tokens, PDAs and SSL accelerators, the EM side-channel is the only powerful side-channel available since the power side-channel is not accessible.

Next we illustrate that different EM carriers carry different information and leakages via some EM side-channels are different from and incomparable to power side-channel leakage and therefore the EM side-channel can sometimes be more powerful than the power side-channel.

Just like the power side-channel, the EM side-channel signals can be used to perform attacks like simple/differential electromagnetic attacks (SEMA/DEMA) which are the analogues of SPA and DPA. This is because, like power signals, EM emanations are correlated to each active bit in the state of device at an instant in time. Also, by comparing the correlation plots of DEMA/DPA for a particular algorithmic bit using different EM channels as well as the power side-channel, one can compare how a particular bit leaks in the various side-channels. Figures 15.24 and 15.25 show the correlation plots for the correct hypothesis for the DES algorithm running on a smart card using three different EM channels (AM demodulation done at different carrier frequencies) as well as the power side-channel. These correlation plots are aligned in time for all the channels with the power side-channel being the solid line and the different EM channels being different styles of broken lines. These plots show the extent to which the algorithmic bit (an S-box output bit in this case) leaks into different side-channels. Figure 15.24 shows that the bit leaks differently at different times in these channels. Figure 15.25 shows the case where the bit leaks substantially in two of the EM channels, somewhat less prominently in the third EM channel and hardly leaks within the power side-channel. In smart cards, this is a common occurrence for several ALU-oriented instructions since power leakages are biased toward instructions that access memory and consume more energy. We term these instructions “bad instructions”, i.e., instructions where information leakage in an EM channel is significantly greater than the corresponding leakage in the power side-channel. In the 6805-based smart card, several bit-test instructions turned out to

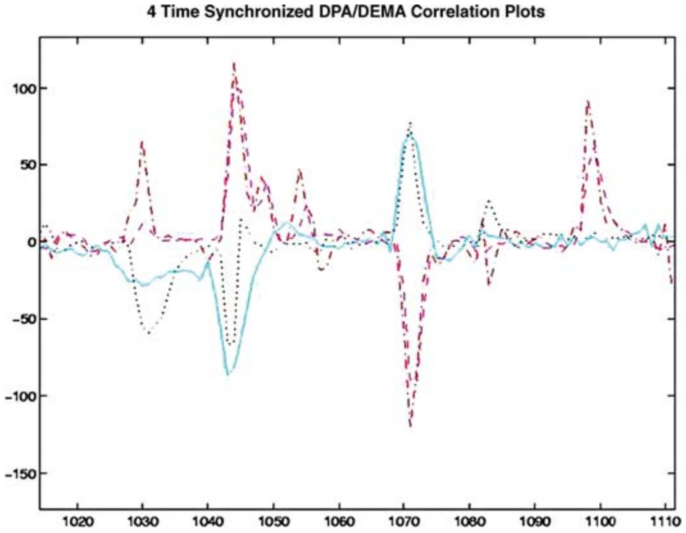


Fig. 15.24 DPA and three DEMA correlation curves (aligned).

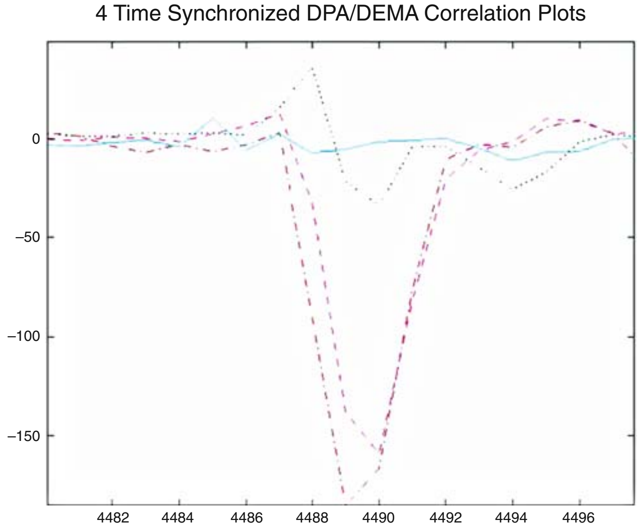


Fig. 15.25 DPA and three DEMA correlation curves (aligned) where the bit leaks substantially.

be bad instructions: the value of the bit being tested leaked into the EM side-channel but not in the power side-channel. Figures 15.26 and 15.27 shows two traces where the tested bit is different and same, respectively, and the highlighted portion of the signal is significantly different in these two cases, thus directly leaking the bit. The power side-channel on the other hand did not carry this information.

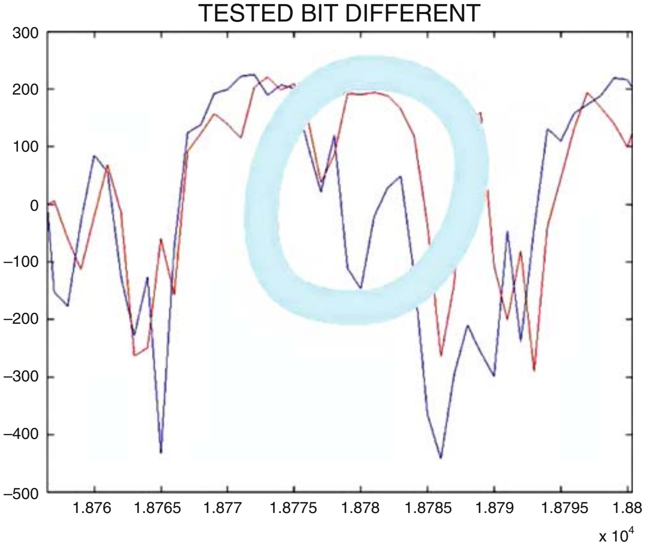


Fig. 15.26 Two EM signals for a bit-test operation: bits different.

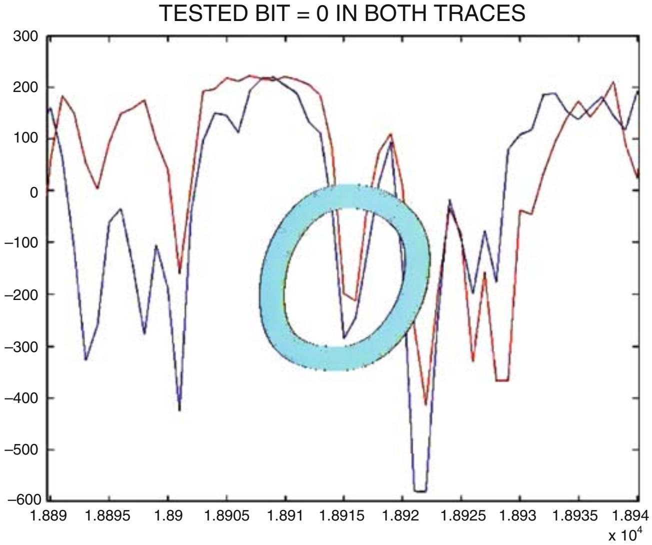


Fig. 15.27 Two EM signals for a bit-test operation: bits same.

15.6 Using EM to Bypass Power Analysis Countermeasures

In general all architectures have bad instructions and typically, in smart cards, these tend to be the ALU-intensive instructions rather than bus-intensive instructions. These bad instructions provide an avenue to break power analysis-resistant implementations.

A common assumption behind many power analysis countermeasures is that once the basic execution sequence is free from simple power analysis (SPA) attacks, there is enough noise/uncertainty in each power trace to prevent direct recovery of sensitive information. Then various techniques such as masking [3, 6] and nonlinear key update [7] can be used to further amplify this uncertainty to prevent the adversary from learning information from multiple samples. If bad instructions are used in a DPA-resistant implementation, then this assumption of limited leakage from a single sample is violated and vulnerabilities get created. For example, if the EM leakage is very large, then the DPA-resistant implementation may be vulnerable to SEMA. If the EM leakage is moderate then higher-order EM attacks on masking DPA countermeasures become possible as was shown in [1].

15.7 Quantifying EM Exposure

In order to assess vulnerability of a device to EM and other side-channels it is imperative that there be an assessment methodology in place to determine the extent of the leakage and the effectiveness of the countermeasures. In the case of EM, this assessment can be quite complex since there are several possible interception points and at each interception point multiple EM signals are available by considering different carriers and demodulations. One has to consider different adversaries and classes of attacks including low-cost attacks by limited adversaries who can capture only one signal at a time, to more powerful adversaries that can capture multiple signals and perform complex signal processing operations, as well as unbounded adversaries that can capture as many signals as they wish from a bounded set of sensors and perform any feasible processing on these signals.

In some cases a sound methodology to assess EM vulnerabilities in these cases is feasible. This will be covered in the chapter on improved techniques for side-channel analysis.

15.8 Countermeasures

EM analysis countermeasures include circuit redesign to reduce unintentional emanations and techniques to reduce the S/N ratio observed by the adversary. For example, EM shielding and/or the introduction of additional noise can reduce the S/N ratio. Another option is to set up physically secure zones where entry is restricted, to prevent the adversary from capturing a strong EM signal.

A systematic way to minimize EM exposure is outlined in the following quote from the NACSIM 5000 TEMPEST Fundamentals document:

> “The prevention of TEMPEST problems can best be accomplished by being attentive to the problem throughout every stage of the equipment or system design and development. Due to the many ways that information is processed in an equipment, there are many ways that compromising emanations can be generated. It is nearly impossible to completely prevent the generation of such compromising emanations. Therefore, the TEMPEST design objectives should be to (a) keep the amplitude and frequency spectrum of compromising emanations as low as possible (i.e., below the appheable limit); (b) prevent RED signals from coupling from RED to BLACK lines or circuits; and (c) to prevent emanations from escaping from the equipment through electromagnetic or acoustical radiation or through line conduction. When involved in retrofitting non-TEMPEST designed equipments, many of the methods identified herein, in addition to encapsulation techniques, may be useful in meeting design objectives.”

However, the following cautionary quote from NACSIM 5000 also outlines why, from a practical perspective, such EM attack resistance is unlikely to be present in most systems.

> “In typical baseband communication or data processing circuit designs, minimum attention is given to suppression of unintentional emanations. Design engineers do not realize the importance of component selection, interconnections, or layout in minimizing signal emanations. Draftspersons, who are unfamiliar with electrical engineering fundamentals, are frequently employed in the design of PC boards and interconnecting leads. Occasionally, this chore is delegated to a computer, which follows a minimal number of rules governing circuit applications and circuit interconnections. As a result, undesired signal emanations will probably be detected when the equipment must be proven TEMPEST hazard-free.”

Once the basic EM leakage is minimized to prevent SEMA-style attacks, then other randomization-based countermeasures that have been used in the context of DPA, such as random masking or computing with shares or nonlinear updates of sensitive information, may be used as countermeasures against DEMA attacks.

15.9 Projects

Pre-requisite: A wideband radio and embedded device, e.g., a cellphone or PDA

1. Using a wideband radio how can you determine the clock frequency and harmonics of the processor? Verify by checking the device specifications. What professional equipment can be used to quickly determine the clock signals within the device?
2. *(Advanced: Assuming that You Can Program the PDA.)* Use your knowledge of the processor clock frequency and instruction set to write a program that loops with a frequency of around 1000 Hz or any other frequency in the audible range, till a key/button is pressed. Execute the program on the PDA. Then, slowly scan the parts of the spectrum that are covered by your radio (using AM or FM demodulation). If the processor clock and harmonics are within a band covered by the radio, you should be able to hear the 1000 Hz tone at several different center frequencies. Each of these bands represents a potential EM side-channel that leaks information about the computation occurring within the processor.
3. Now that you have determined the EM bands where there is leakage from the CPU, how would you use this information to set up EM capturing equipment and carry out a SEMA/DEMA attack on the device?
4. *Locating Compromising Emanations from Device Display:* While manipulating the information displayed by the device (e.g., either by running an application that regularly updates the screen or manually updating what is displayed), slowly scan the parts of the spectrum (either AM or FM demodulation) that your radio covers. At several frequencies you should be able to hear audible sounds whenever the screen changes. These are frequencies at which information about the contents of the screen can leak. Actual attacks to capture the screen will depend on the specifics of how the display is being refreshed.
5. *EM Propagation (Advanced):* First conduct experiment in exercise 2 to obtain the 1000 Hz tone indicating EM leakage from the device. Place the device with the running program inside a completely enclosed metal box (or a cardboard box covered with aluminum foil). Can your receiver still capture the 1000 Hz tone outside the metal box? Why not? Now place the device on a metal box that has one or a few small openings (e.g., by creating a small opening within the foil-covered cardboard box). Again, try to obtain the 1000 Hz tone with your receiver. Move the receiver around the box to locate where the signal is strongest. Where is the signal the strongest? Why?

References

1. D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. The EM side-channel(s). In B. Kaliski, Ç. K. Koç, and C. Paar editors, *Proceedings of CHES 2002*, Lecture Notes in Computer Science, vol. 2523, pp. 29–45, Springer, 2002.
2. A. V. Borovik and C. D. Walter. A Side Channel Attack on Montgomery Multiplication. Private technical report, Datacard platform seven, July 1999.
3. S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi. Towards sound approaches to counteract power-analysis attacks. In M. Wiener editor, *Proceedings of Advances in Cryptology, CRYPTO '99* Lecture Notes in Computer Science, vol. 1666, pp. 398–412, Springer, 1999.
4. Dynamic R1550. Dynamic Sciences International Inc, R 1550 Receiver. Specifications available at http://www.dynamic-sciences.com/r1550.html.
5. K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar editors, *Proceedings of CHES 2001*, Lecture Notes in Computer Science, vol. 2162, pp. 251–261, Springer, 2001.
6. L. Goubin and J. Patarin. DES and Differential power analysis (The "Duplication" method). In Ç. K. Koç and C. Paar editors, *Proceedings of CHES 1999*, Lecture Notes in Computer Science, vol. 1717, pp. 158–172. Springer, 1999.
7. P. C. Kocher and J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener editor, *Proceedings of Advances in Cryptology CRYPTO '99*, Lecture Notes in Computer Science, vol. 1666, pp. 388–397, Springer-Verlag, 1999.
8. M. G. Kuhn and R. J. Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In D. Aucsmith editor, *Information Hiding 1998*, Lecture Notes in Computer Science 1525, pp. 124–143, Springer-Verlag, 1998.
9. J.-J. Quisquater and D. Samyde. Electromagnetic analysis (EMA): Measures and countermeasures for smart cards. In *Proceedings of e-Smart 2001*, Lectures Notes in Computer Science (LNCS), vol. 2140, pp. 200–210, Springer, 2001.
10. W. Schindler. A Timing attack against RSA with chinese remainder theorem. In Ç. K. Koç and C. Paar (eds.) *Proceedings of CHES 2000*, Lecture Notes in Computer Science, vol. 1965, pp. 109–124, Springer, 2000.
11. W. van Eck. Electromagnetic radiation from video display units: An evesdropping risk? *Computers & Security*, vol. 4, pp. 269–286, 1985.
12. C. D. Walter and S. Thompson. Distinguishing exponent digits by observing modular subtractions. In D. Naccache editor, *Proceedings of CT-RSA 2001*, Lecture Notes in Computer Science, vol. 2020, pp. 192–207, 2001.