Electromagnetic-based Side Channel Attacks

Yasmine Badr

10/28/2015

What is Side Channel Attack

- Any attack based on information gained from the **physical implementation** of a cryptosystem, <u>rather</u> than **brute force or theoretical weaknesses** in the **algorithms**. [Wikipedia]
  - Example: using timing information, power consumption, electromagnetic leaks or even sound
- EM side channels are easier because usually there is no direct access to power line

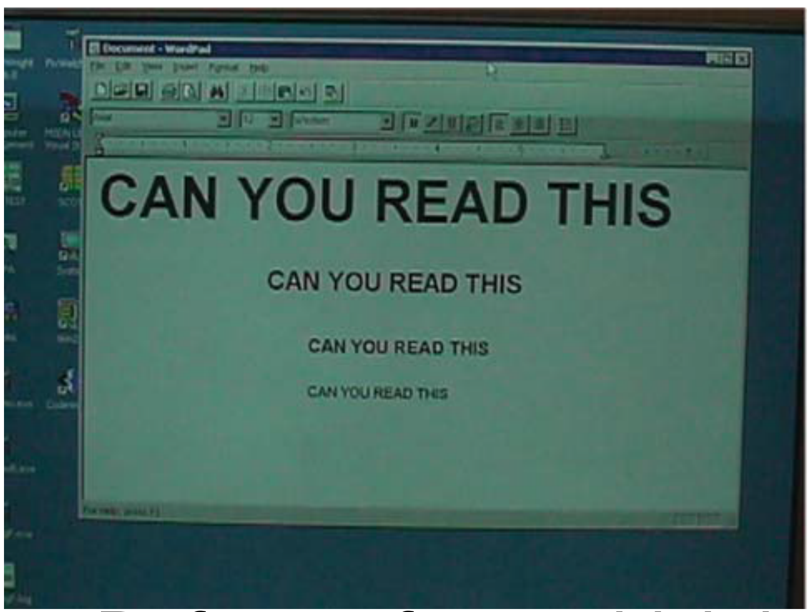
Defense

- These attacks depend on information from physical behavior and secret data.
- Countermeasures:
  - make the leaked physical info and the secret date uncorrelated or
  - eliminate/reduce the leak of the physical information

Examples

Electromagnetic Side Channel Attack [1]

- Using EM emanation from devices to recover info
- First demonstrated in 1985
  - EM emanations from monitor captured from a distance and used to reconstruct the display



  - Defense: fonts which have reduced EM leakage characteristic→ hard to recover

Types of EM emanations [1]

- **Direct (Intentional):**
  - Result from intentional current flows
  - Simple example: using coils to capture the time-varying magnetic fields created by current
  - Usually difficult to isolate direct emanations due to interference from other signals

Types of EM emanations [1]

- **Unintentional:**
  - Minor Electrical and Electromagnetic couplings between components in a device
  - These emanations act as **modulations of carrier signals** (already present or injected into device)
    - Amplitude or angle or more complex modulation
  - EM receiver, tuned to the carrier frequency, demodulates the signal (if captured)

Exploiting Emanations

- Strongest EM emanations are generated by sharp-rising waveforms of short duration
- Exploiting **direct emanations** requires **close proximity**
- **Unintentional emanations** can be captured from distance without invasive techniques
  - Modulated carriers are stronger and can travel longer than direct emanations
  - Carrier can be the **clock**

EM Capturing Equipment

- A tunable receiver/demodulator which can be tuned to various modulated carriers and can perform demodulation to extract the sensitive signa

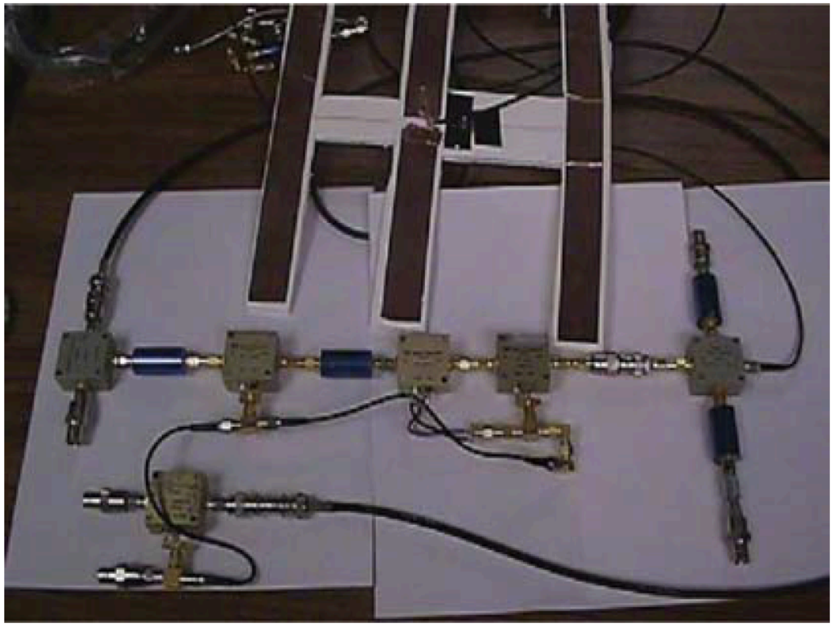
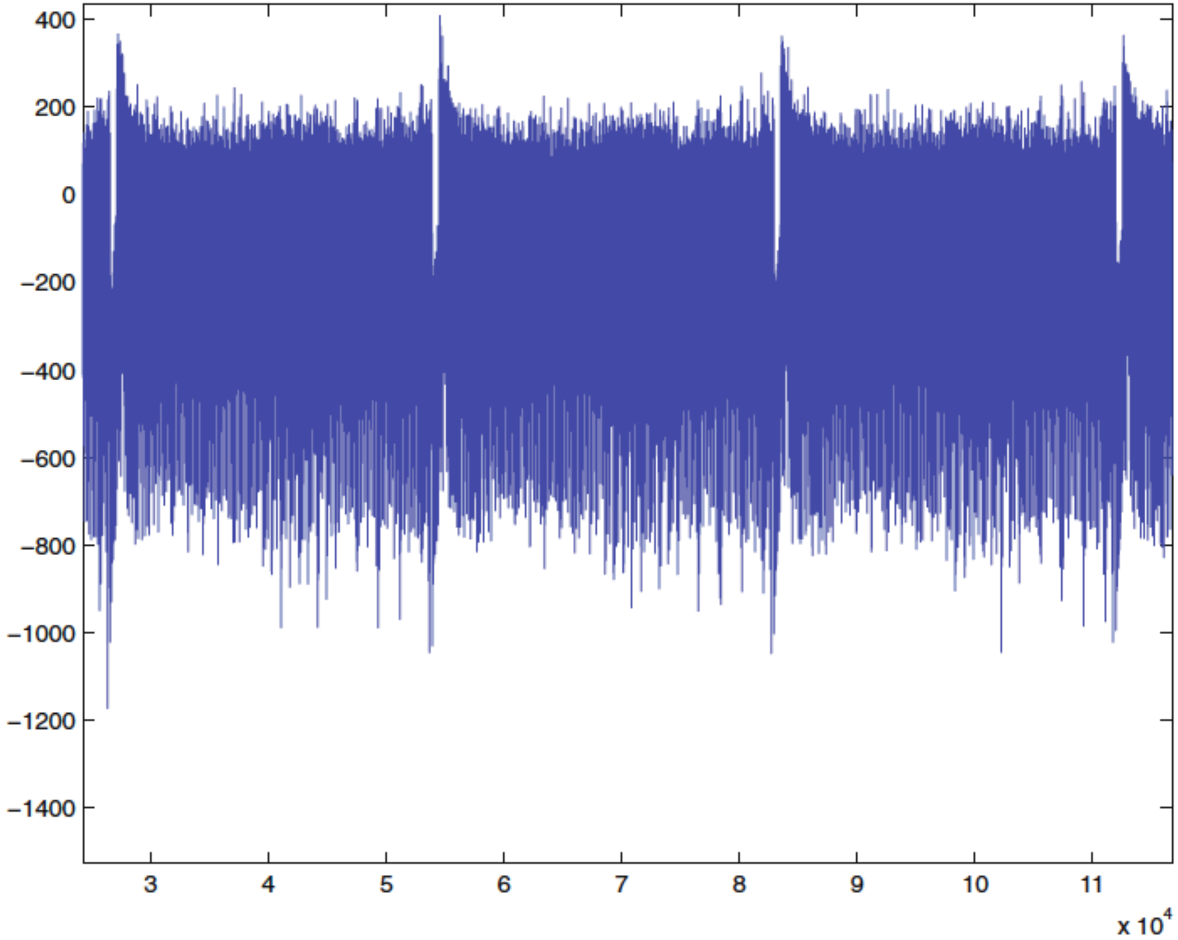


Fig. 15.9 Low-cost, low-noise receiver built from components.

Current Amplitude: 3 rounds of DES on power line of smart card



Example: Amplitude Modulation [1]

- Smart Card operating on a 3.68MHz external clock, performing these instructions (13 cycles)
  - Read specific value from Ram (5 cycles)
  - Check for external condition (5 cycles)
  - Jump back to start of loop (3 cycles)

Raw Signal

- Raw signal obtained by a near-field EM sensor placed behind the smart card for 26 clock cycles

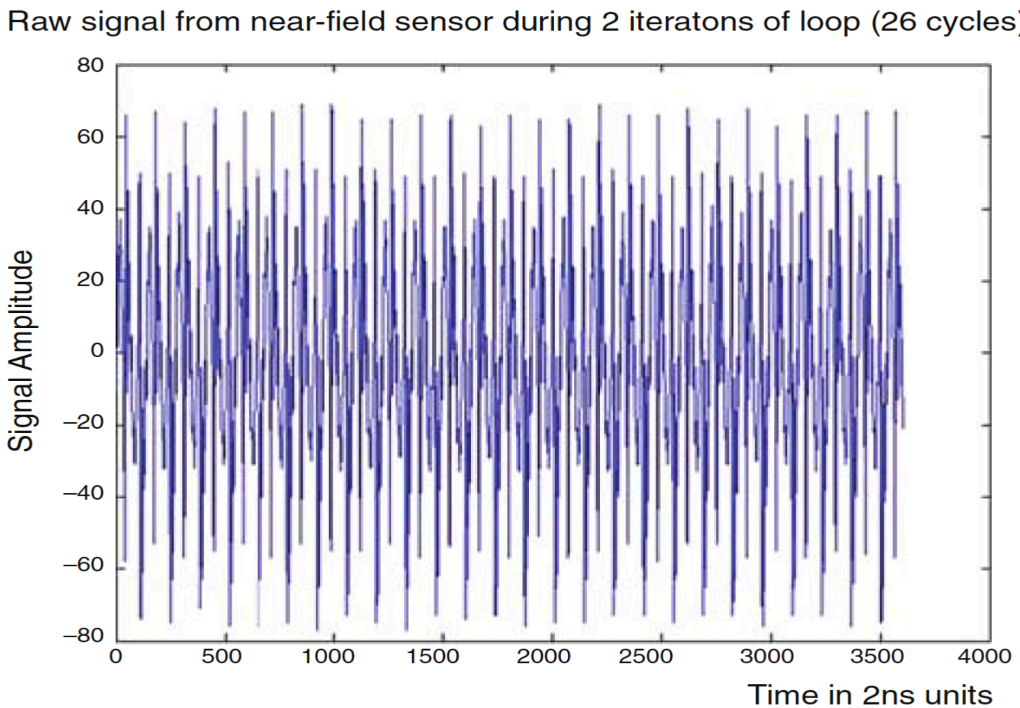


Fig. 15.10 Raw EM signal from 6805 smart card during 26 clock cycles.

- Regular Signal structure repeated 26 times

Raw Signal (cont'd)

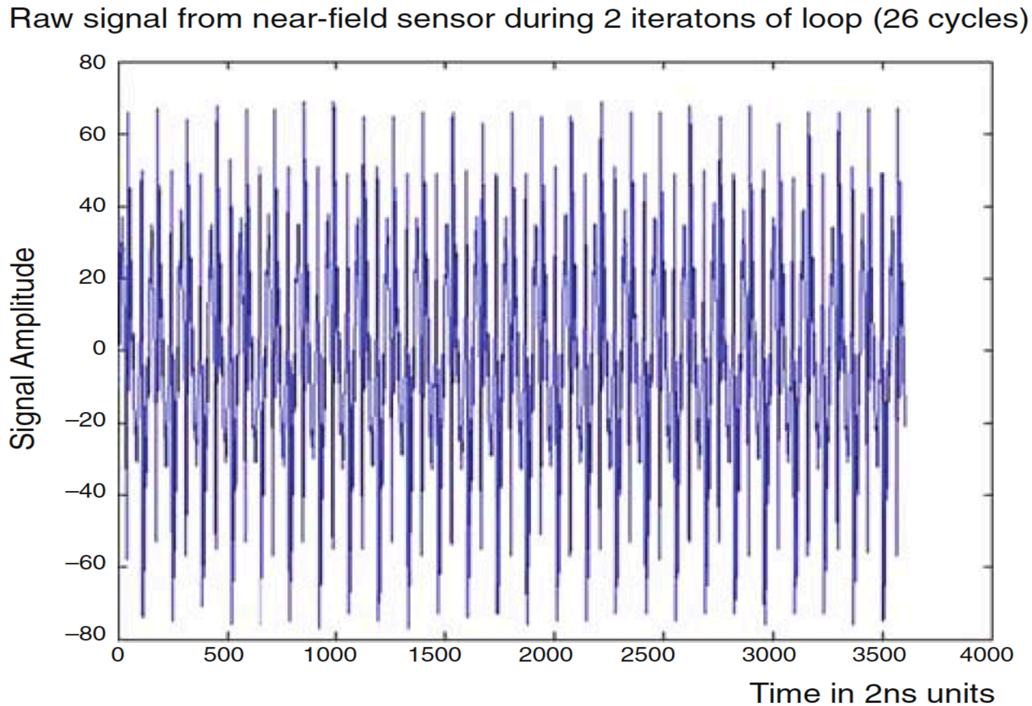
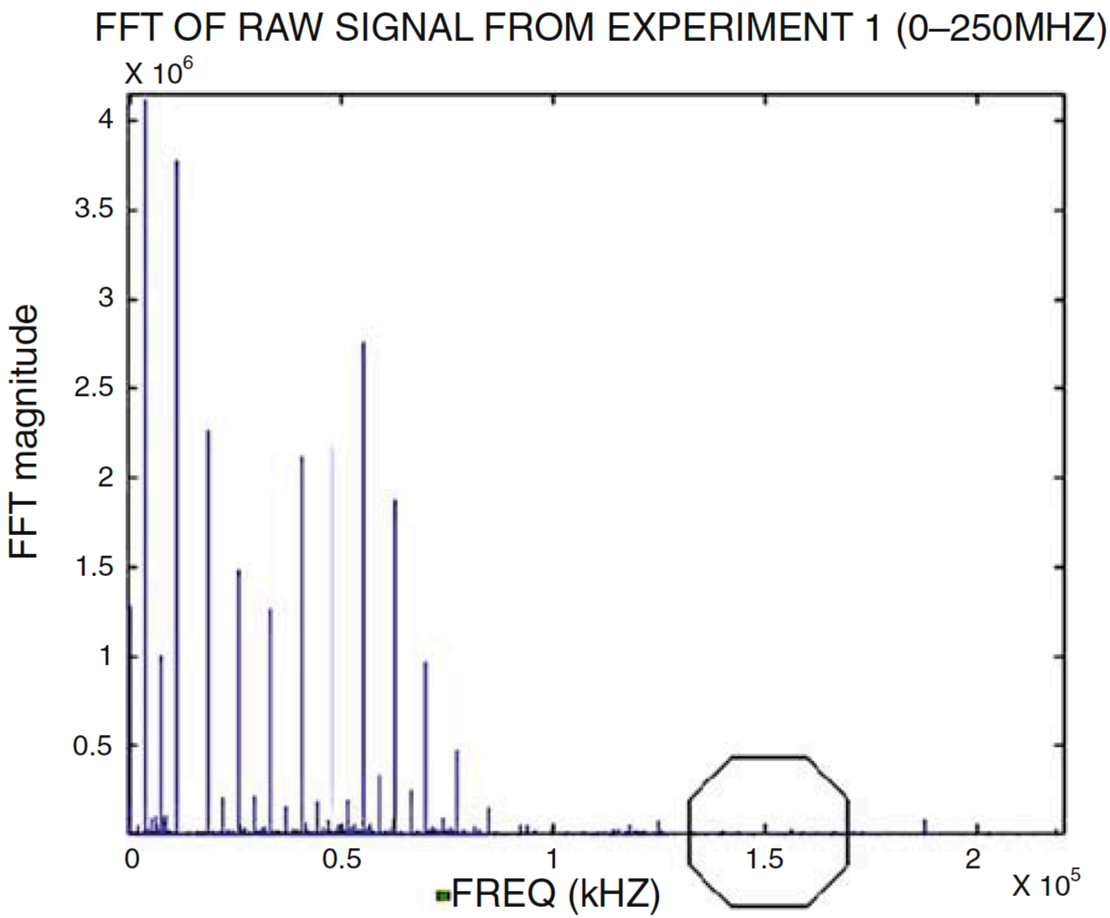


Fig. 15.10 Raw EM signal from 6805 smart card during 26 clock cycles.

- Can't tell that smart card is operating in a loop or to know of the operations being performed
- Shown signal is the differential of the clock
  - Clock signal is so dominant such that all other info about other currents is washed out
- Clock is Direct Emanation

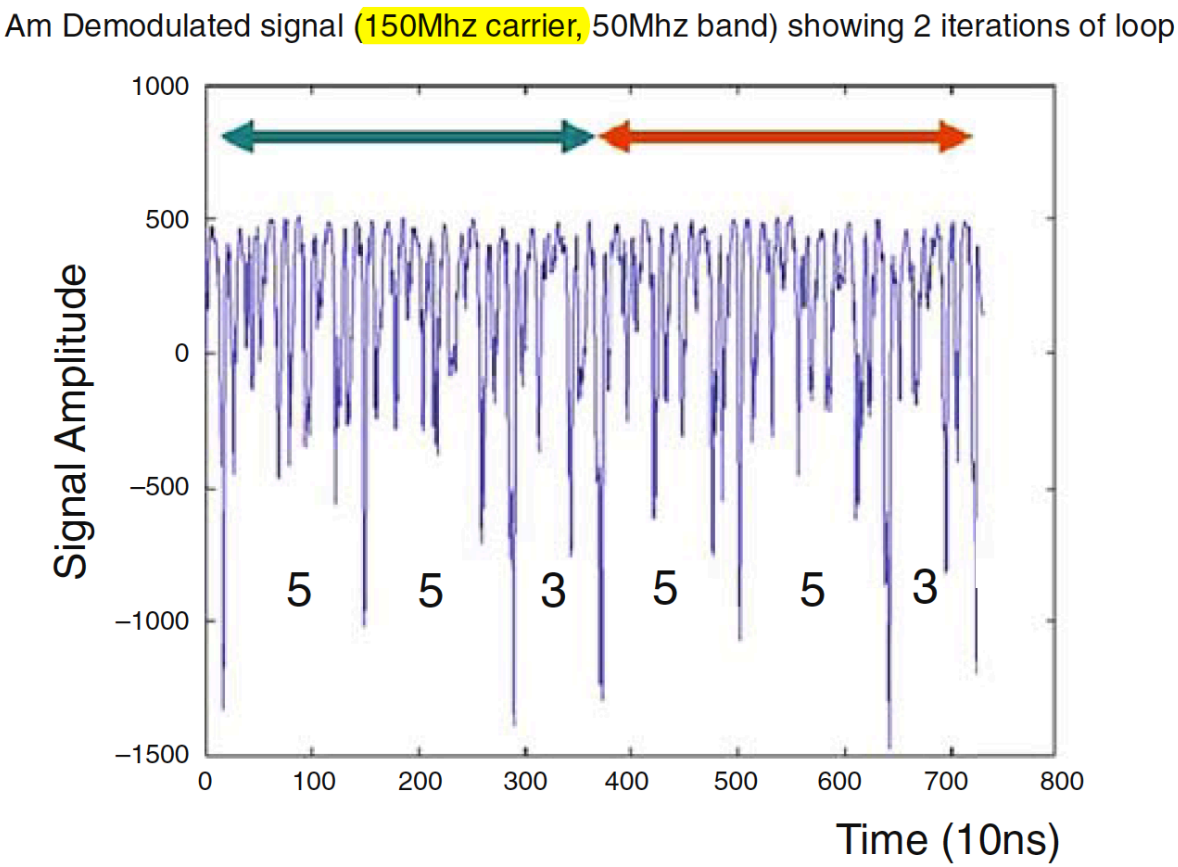
With FFT→ anything discerned?



- Again, dominant signal is the clock signal, which consists of strong components at the fundamental frequency and at odd harmonics as well as some even harmonics.
- Nothing yet about the smart card operations

At higher frequency..

- But clock harmonics die at higher frequency
- AM demodulating the raw signal with a center frequency of around 150MHz



Demodulated Signal from Smart card doing 16 rounds of DES

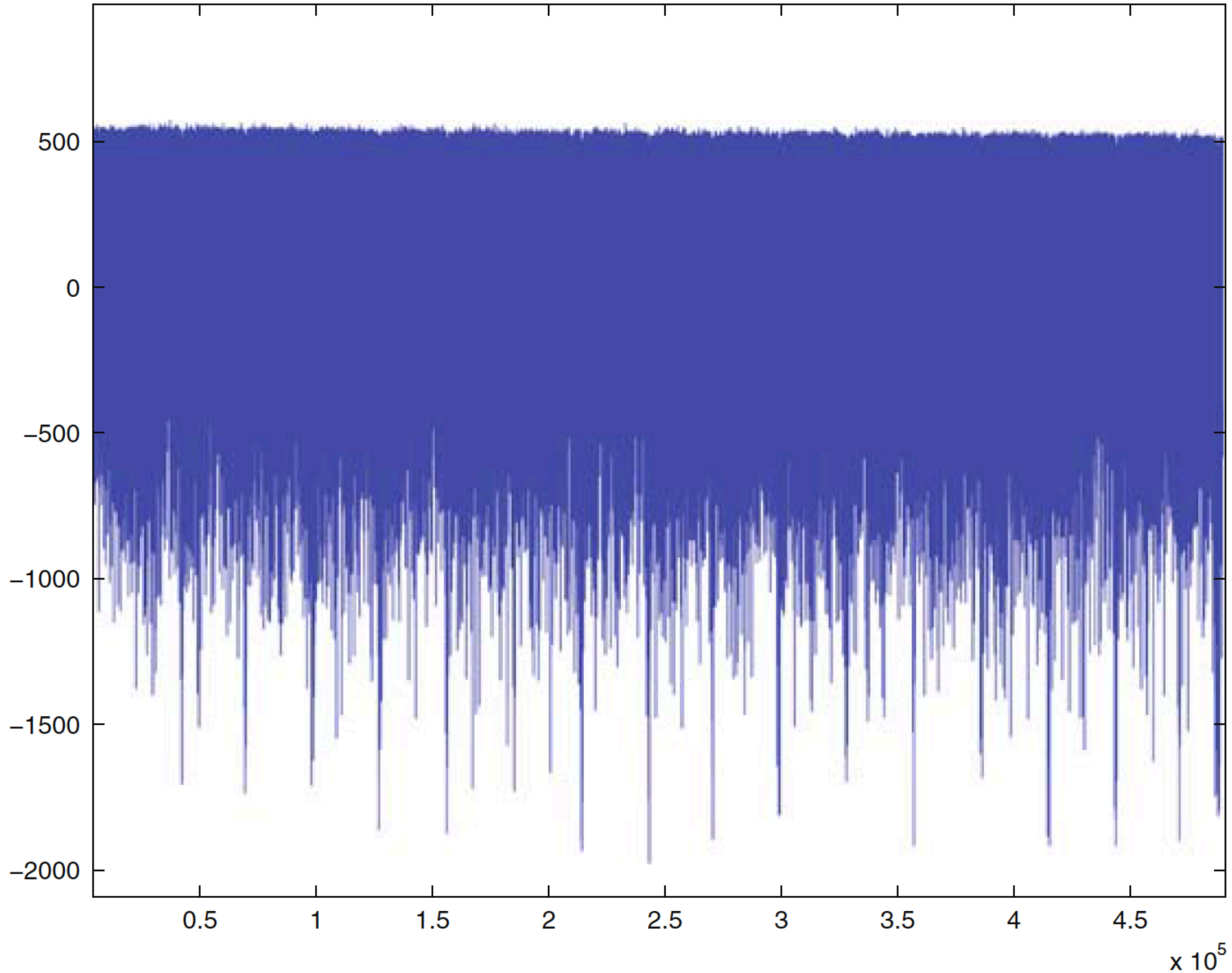


Fig. 15.13 Demodulated EM signal (100 MHz bandwidth) from smart card performing 16 rounds of DES.

2 Rounds only.. Better look

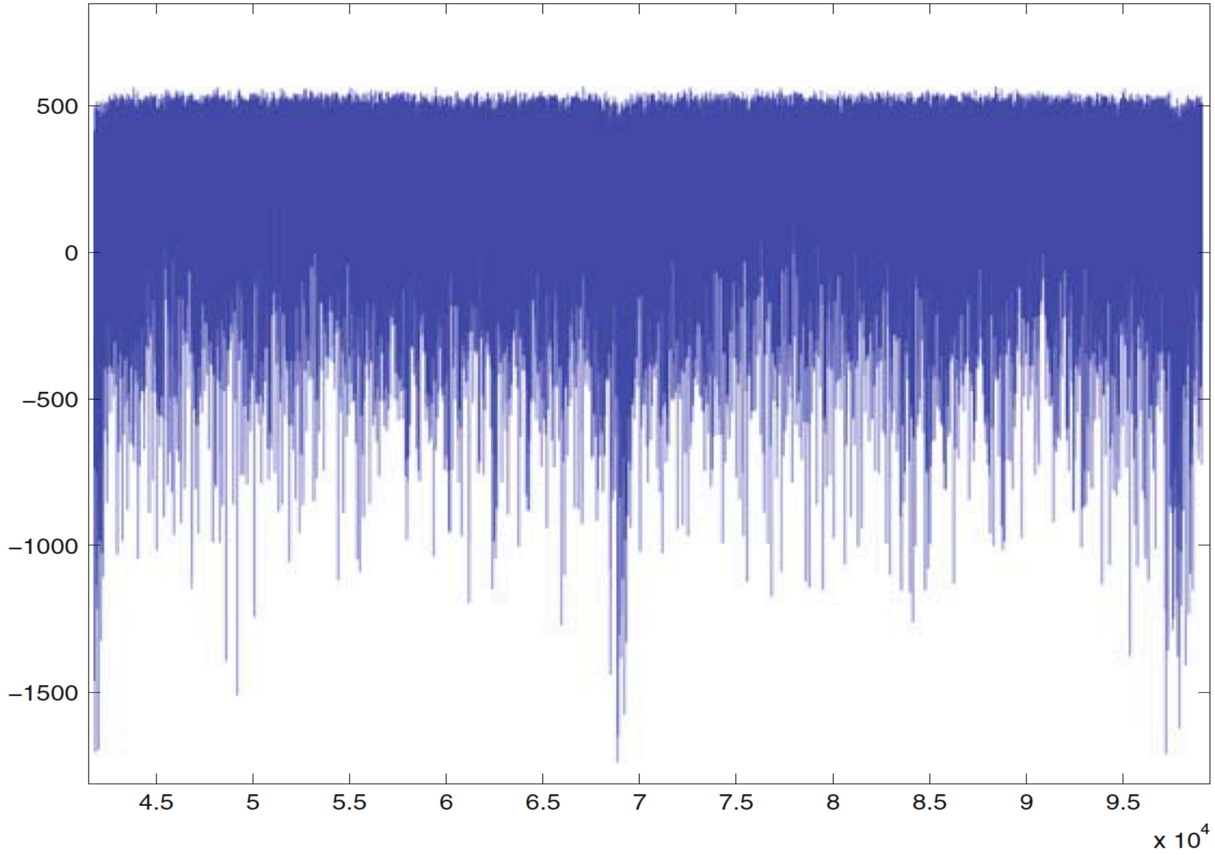


Fig. 15.14 Demodulated EM signal showing two rounds of DES (100 MHz bandwidth).

DES on smart card: EM signal with two different and same bit values (one output bit of an S-box)

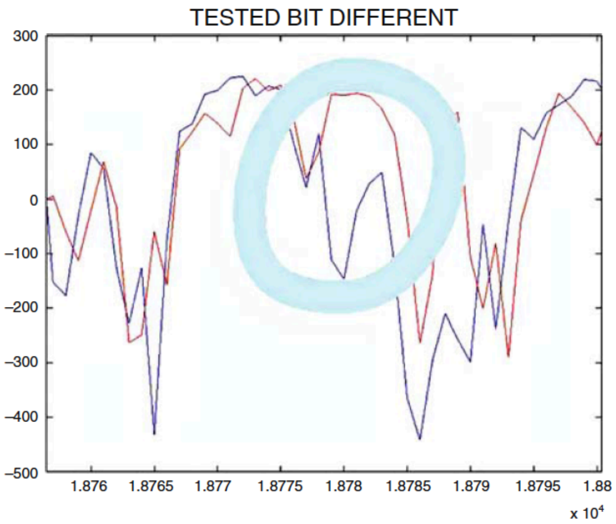


Fig. 15.26 Two EM signals for a bit-test operation: bits different.

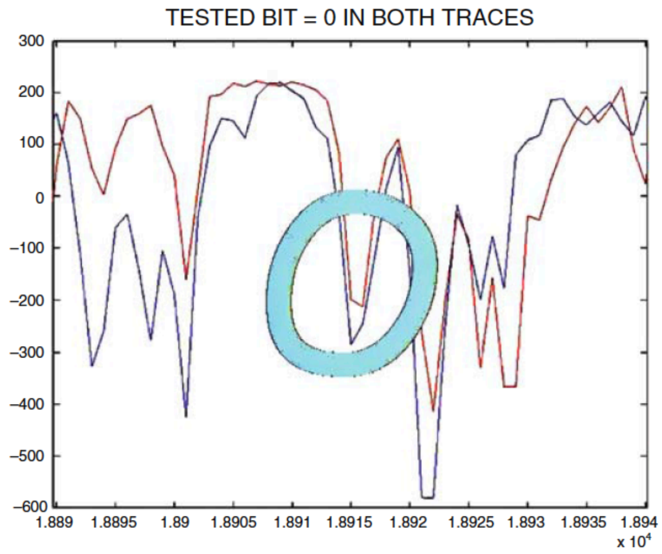


Fig. 15.27 Two EM signals for a bit-test operation: bits same.

References

[1] Rohatgi, Pankaj. "Electromagnetic attacks and countermeasures." *Cryptographic Engineering*. Springer US, 2009. 407-430.

[2] Longo, Jake, et al. "SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip." *Cryptographic Hardware and Embedded Systems--CHES 2015*. Springer, 2015.