The EM Side-Channel(s)

Dakshi Agrawal
Bruce Archambeault
Josyula R Rao
Pankaj Rohatgi
IBM

EM History

- Classified TEMPEST standards. Some parts declassified Jan '01, http://www.cryptome.org.
- Published work
  - EM Leakages from Peripherals, E.g., Monitors: Van Eck, Anderson & Kuhn.
  - EM Leakage from smart-cards during Computation.
    - J.-J. Quisquater & David Samyde, E-smart 2001,
    - Gemplus Team [GMO '01], CHES '01.
      - SEMA/DEMA attacks.
    - Best results require "decapsulation" of chip packaging and/or precise micro-antennas positioning on chip surface

Our Work

- Deeper understanding of the EM leakages.
  - Similar to declassified TEMPEST literature.
- Key Insights/Results
  - Plenty of EM signals are available, provided you know what to look for and where.
    - Superior signals and attacks possible without micro-antennas or decapsulation.
    - Some attacks possible from a distance.
  - EM side-channel(s) >> Power side-channel
    - EM can break DPA-resistant implementations.

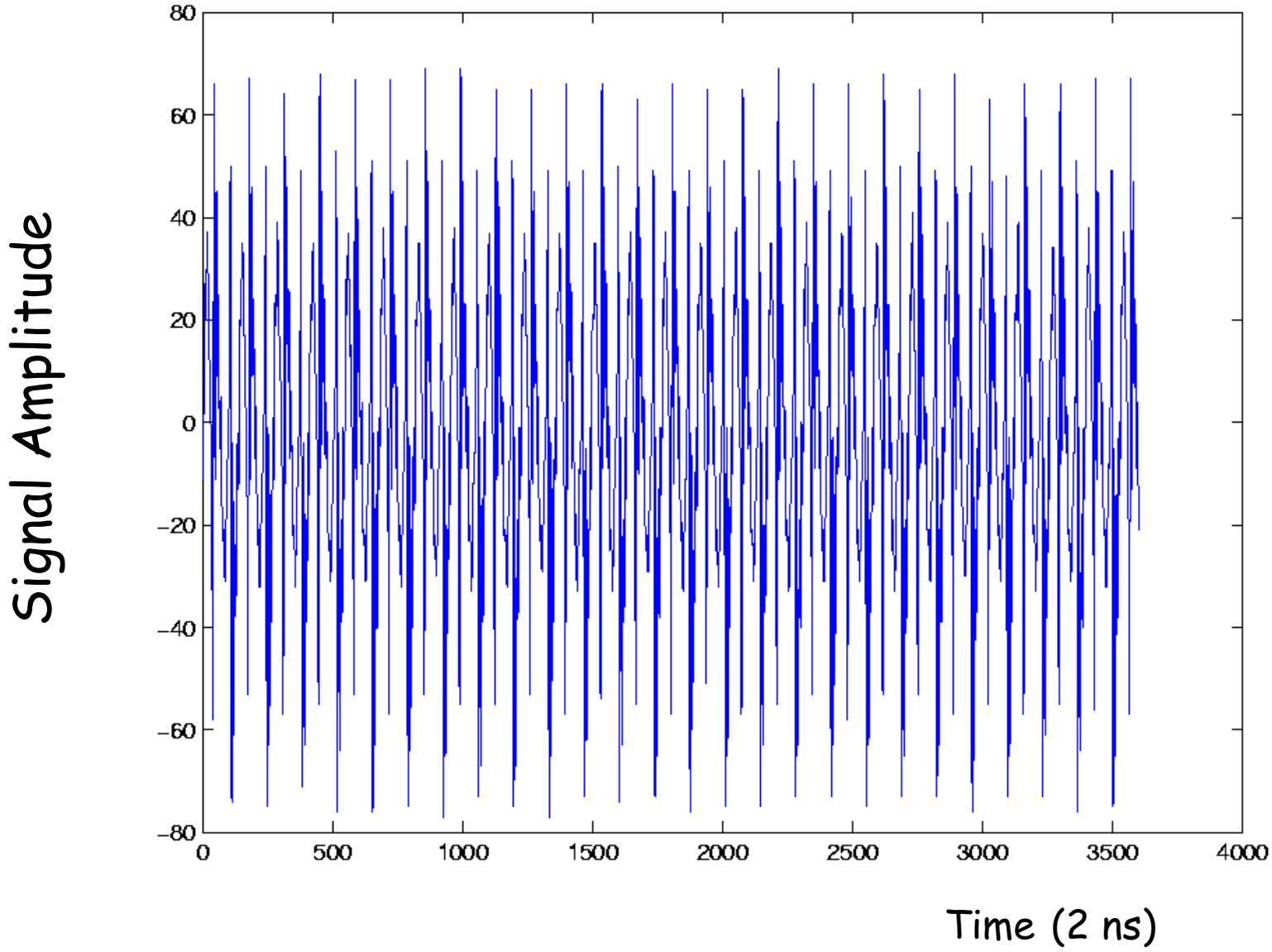
EM Emanations Background

- Origin/Types of EM Emanations
  - Direct emanations from intended currents.
    - Maxwell's equations, Ampere's and Faraday's laws.
  - Unintentional emanations from coupling effects.
    - Depend on physical factors, e.g., circuit geometry.
    - Most couplings ignored by circuit designers.
    - Manifest as modulation of carriers (e.g. clock harmonics) present/generated/introduced in device.
      - AM or Angle (FM/Phase) Modulation.
    - Compromising signals available via demodulation.
- Propagation of EM
  - Radiation, Conduction, Combination of both.
    - E.g., Faint EM signals riding on power line.

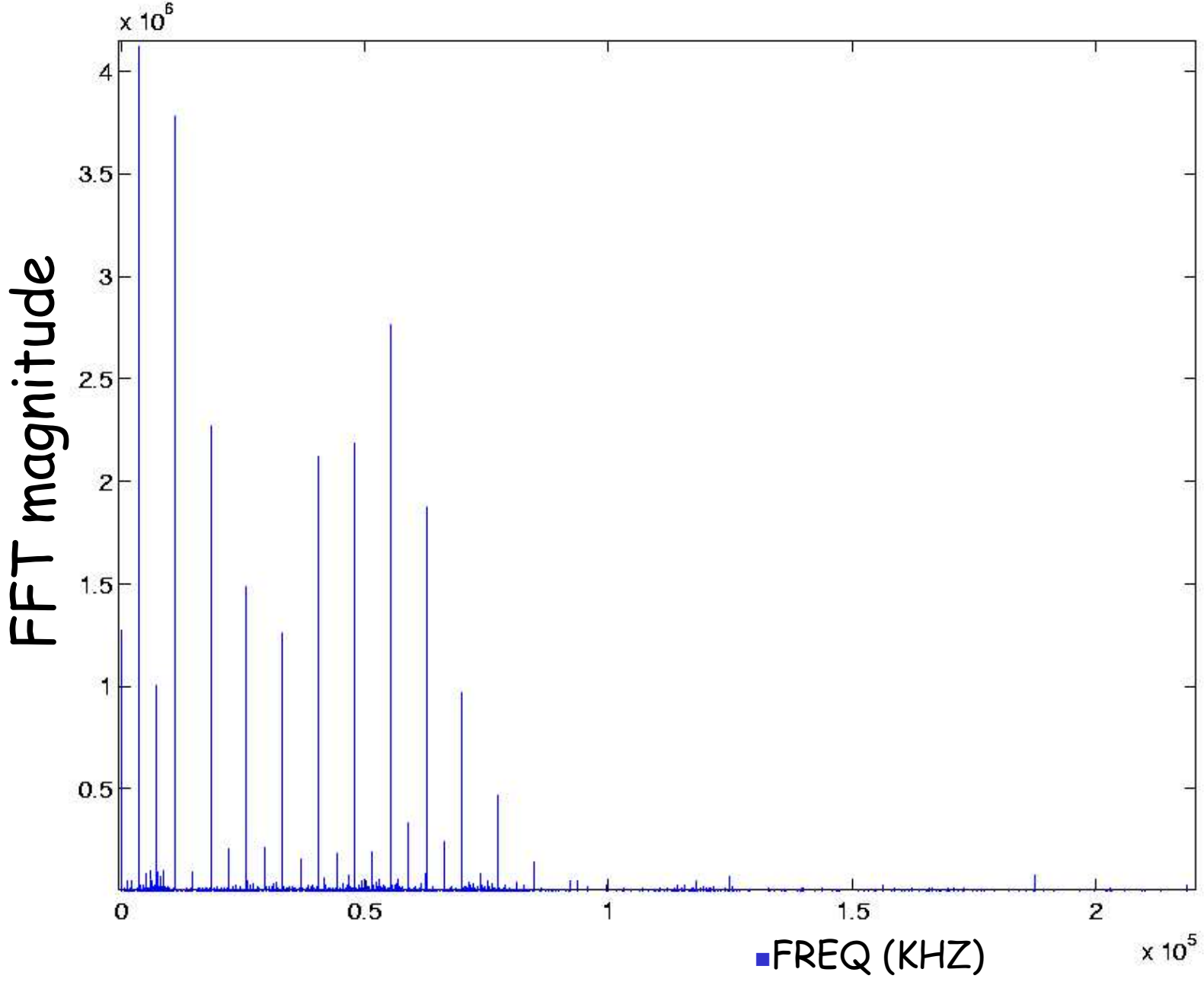
EXAMPLE 1

- 6805-based smart-card using external 3.68Mhz clock.
- 3 instruction, 13 cycle loop:
  - Access RAM containing a value B (5 cycles)
  - Check for external condition (5 cycles)
  - Jump back to start of loop (3 cycles)

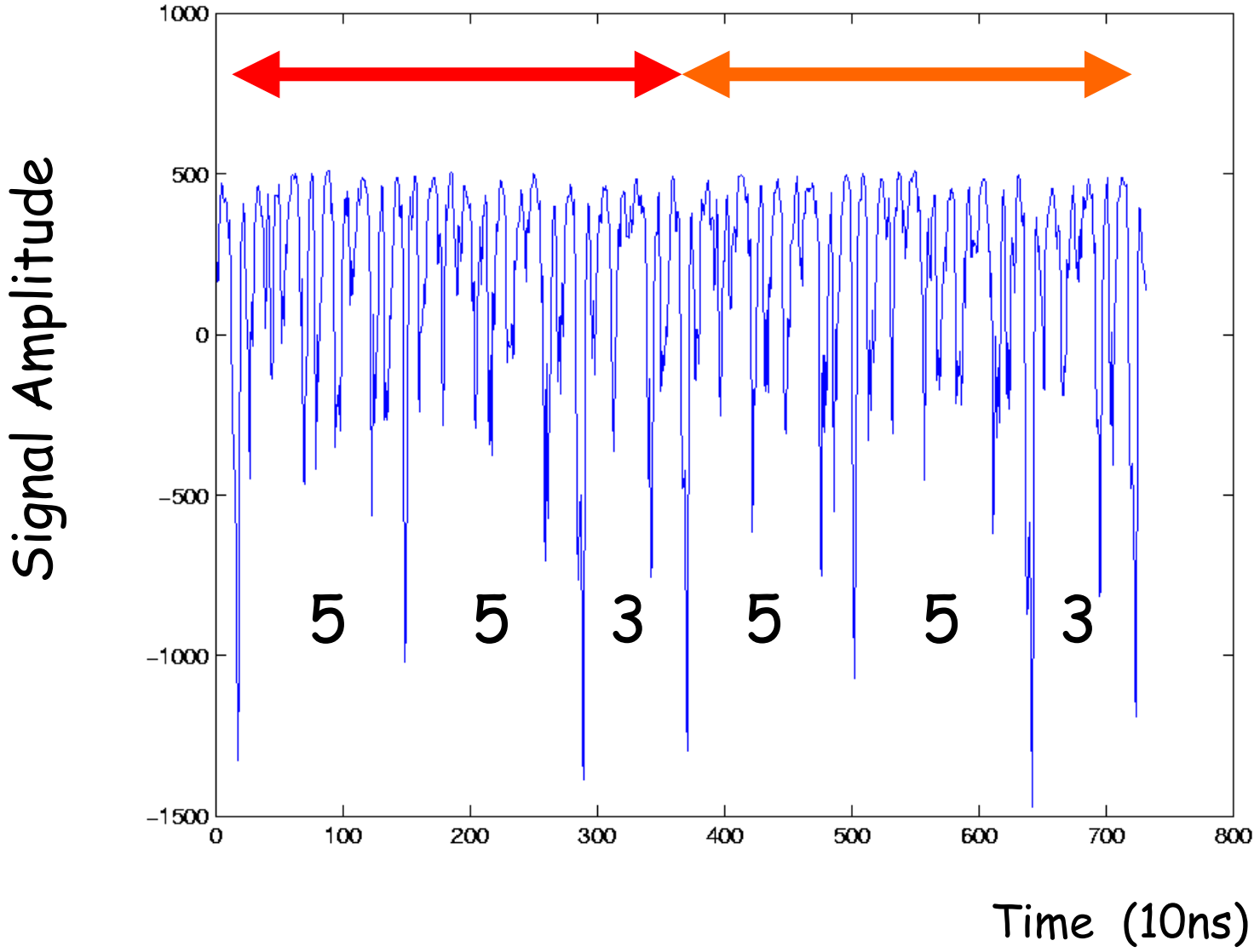
Raw signal from near-field sensor during 2 iterations of loop (26 cycles)



FFT OF RAW SIGNAL FROM EXPERIMENT 1 (0-250MHZ)



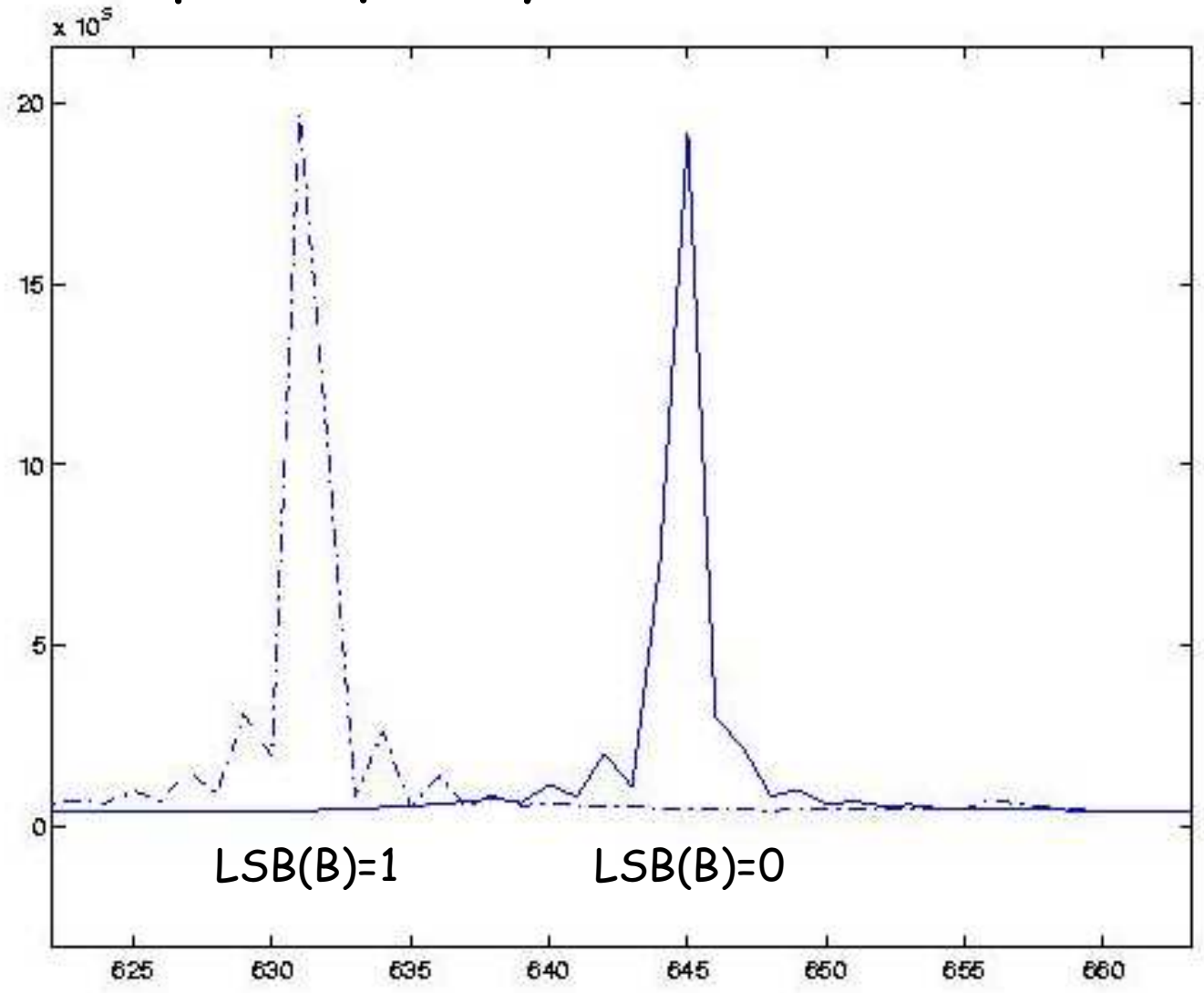
AM Demodulated signal (150Mhz carrier, 50Mhz band) showing 2 iterations of Loop



EXAMPLE 2: Angle Modulation

- Same 6805-based smart-card executing same loop, running on variable internal clock (a DPA countermeasure).
- 3 instructions.
  - Check RAM containing value B (5 cycles)
  - Check for external condition (5 cycles)
  - Jump back (3 cycles)
- Varied B and looked at loop frequency.

Loop Frequency for LSB(B) = 0/1

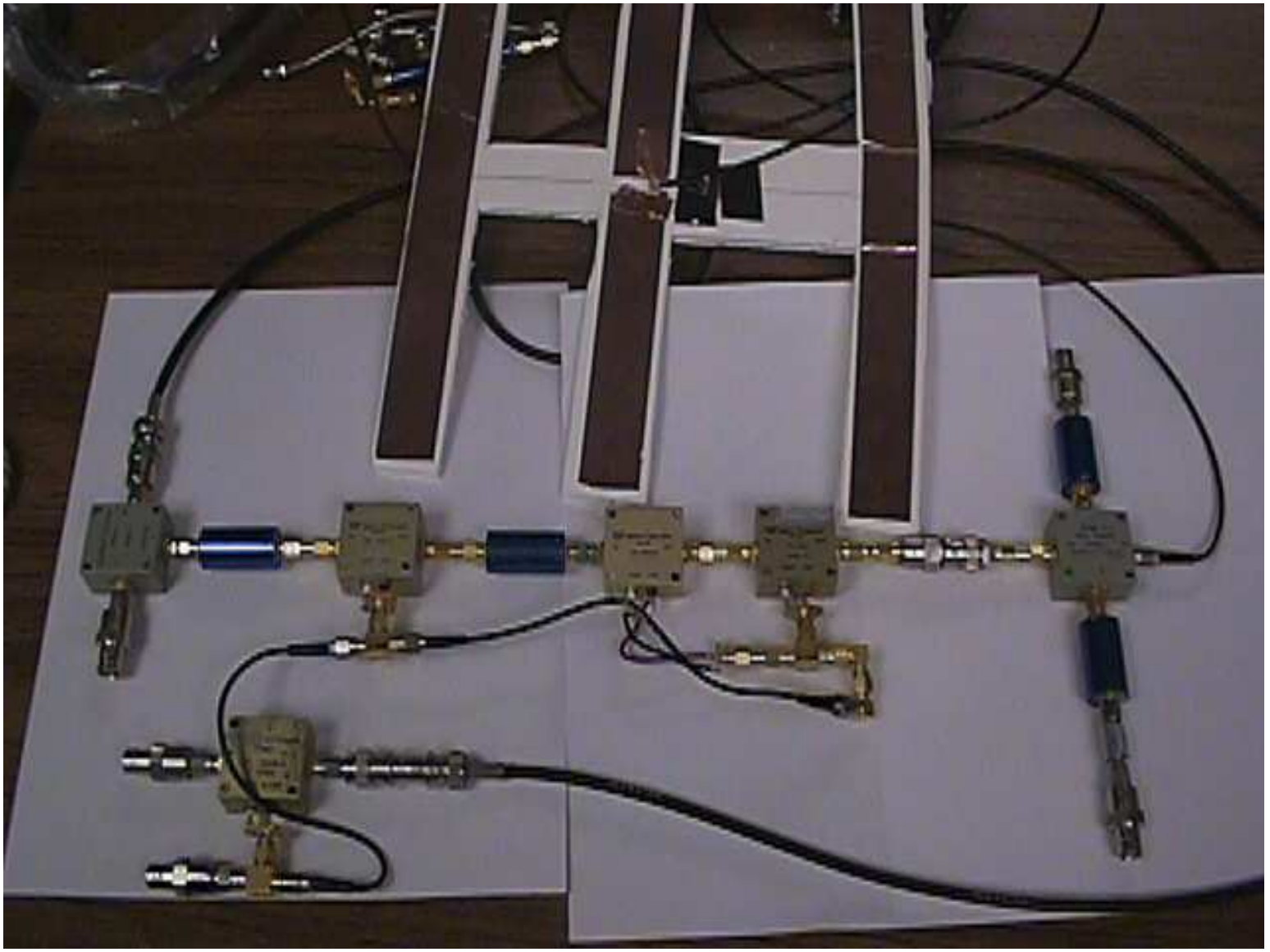


EM Capturing Equipment

- Antennas (Far-field) and Near-field probes
- Current probes.
- Analog processing: Filters/Amplifiers, Tunable wideband receiver or equivalent $$
- Digital sampling hardware.

ICOM wideband radio receiver with IF output

MAKE YOUR OWN



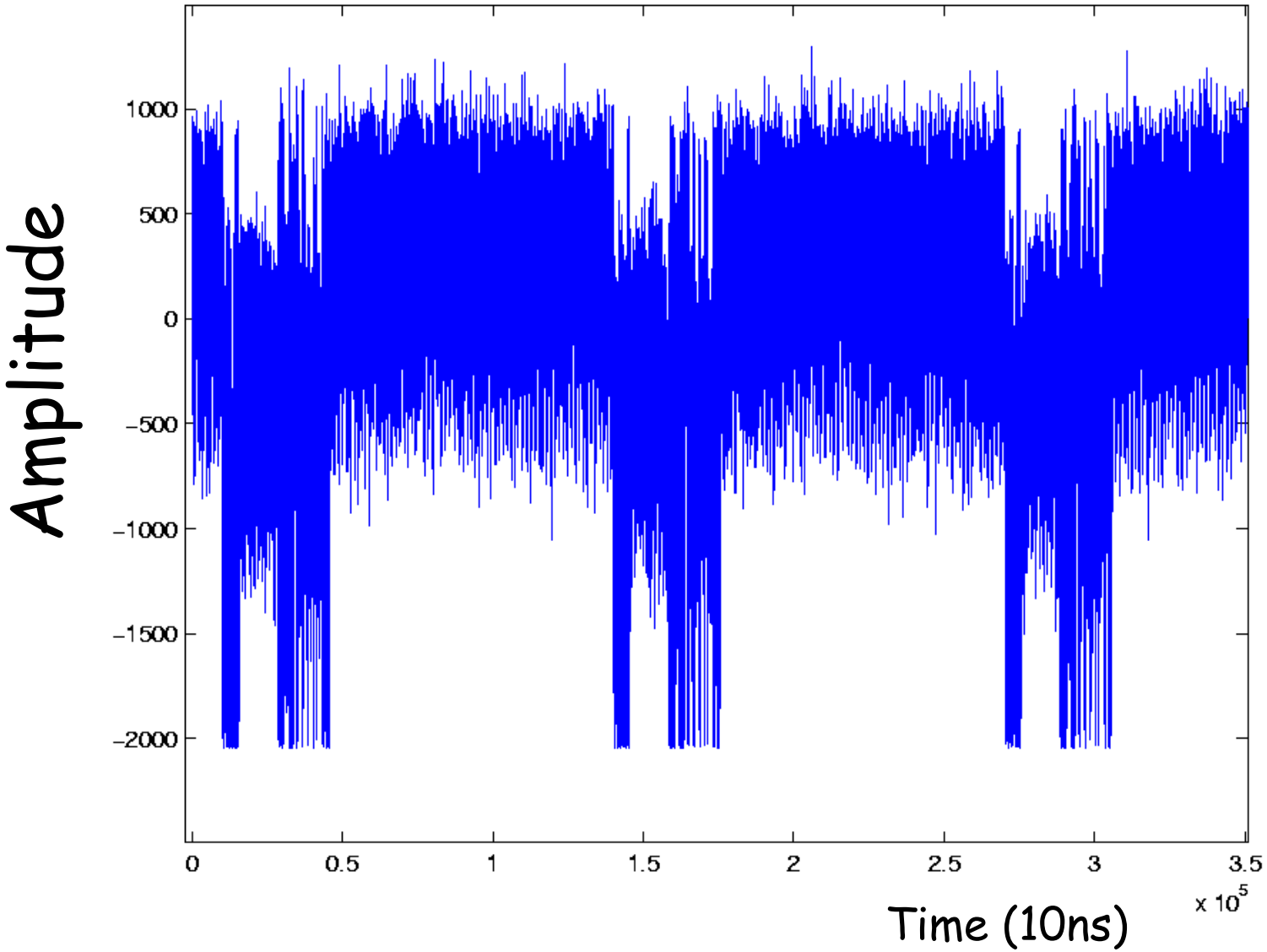
EM vs. Power

- Sometimes, EM is the only side-channel available.
  - Filtered power supplies, restricted access…
  - E.g. Crypto Tokens, SSL Accelerators,...

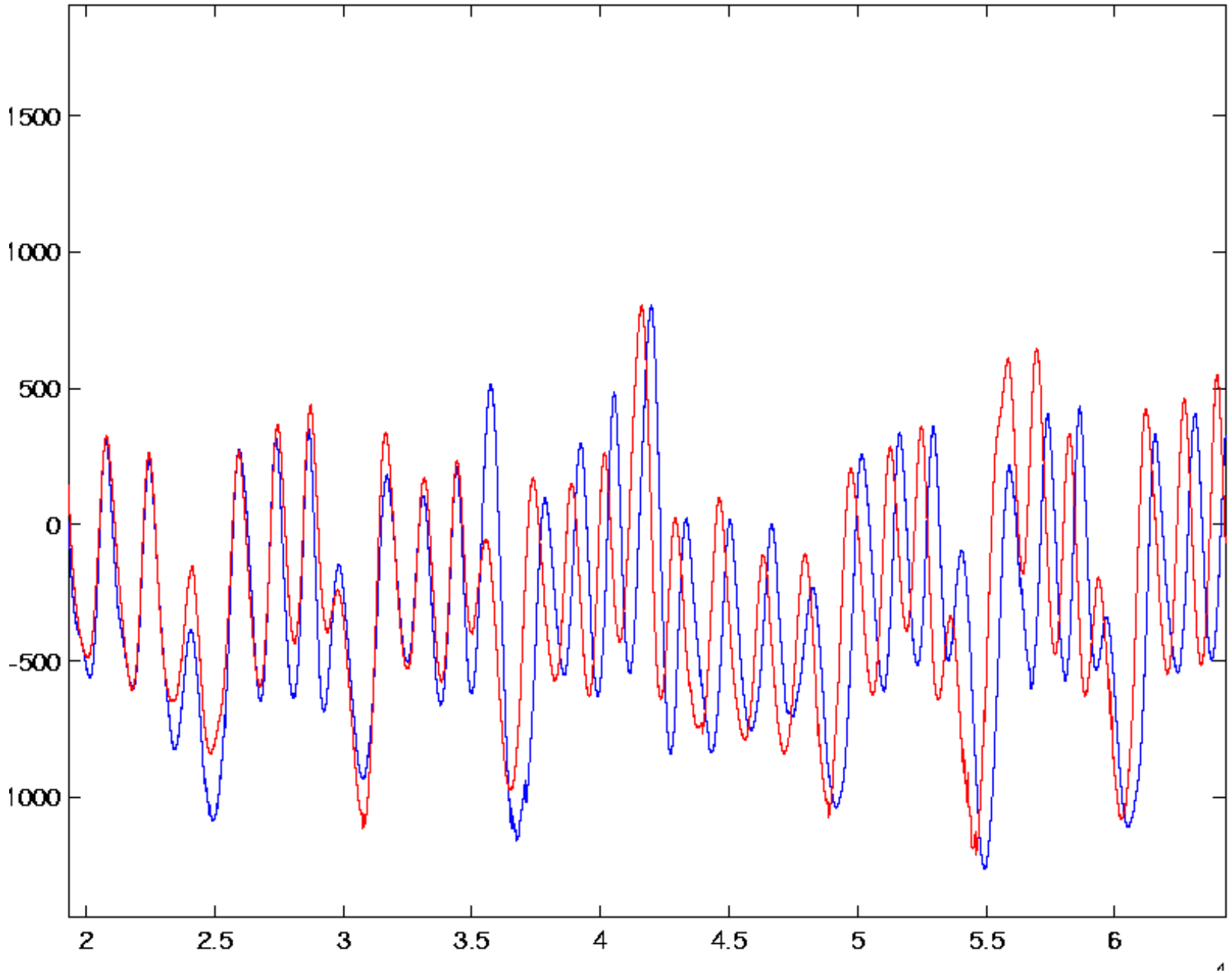
SSL Accelerator Music

- SSL Accelerator S, looping with ~3s each of
  - 512-bit RSA
  - 1024-bit RSA
  - 2048-bit RSA
  - 4096-bit RSA
- Can be heard on a Radio Receiver 40 feet away.

EM Signal from SSL Accelerator S at 15 feet



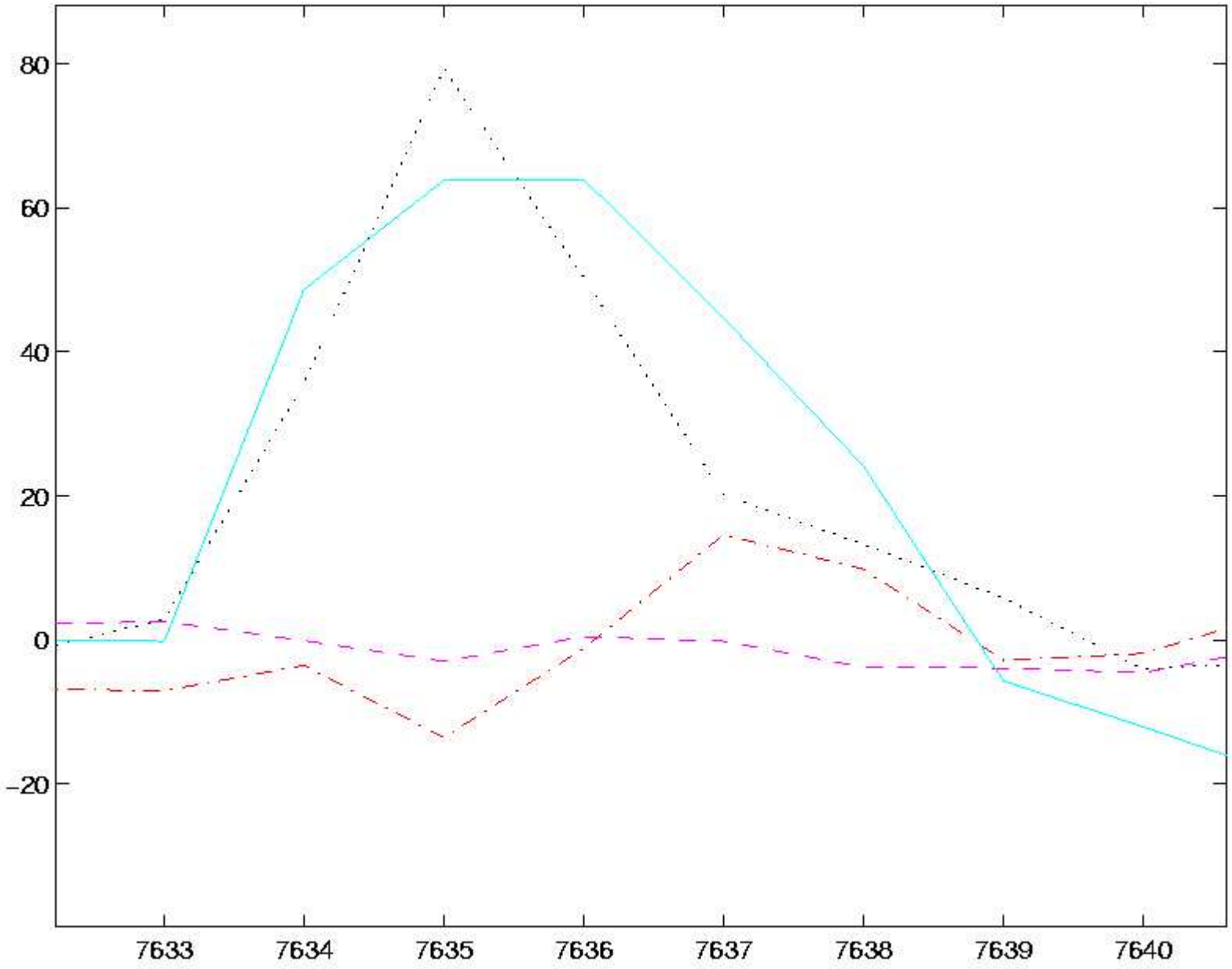
Conditional operations within montgomery multiplication in S



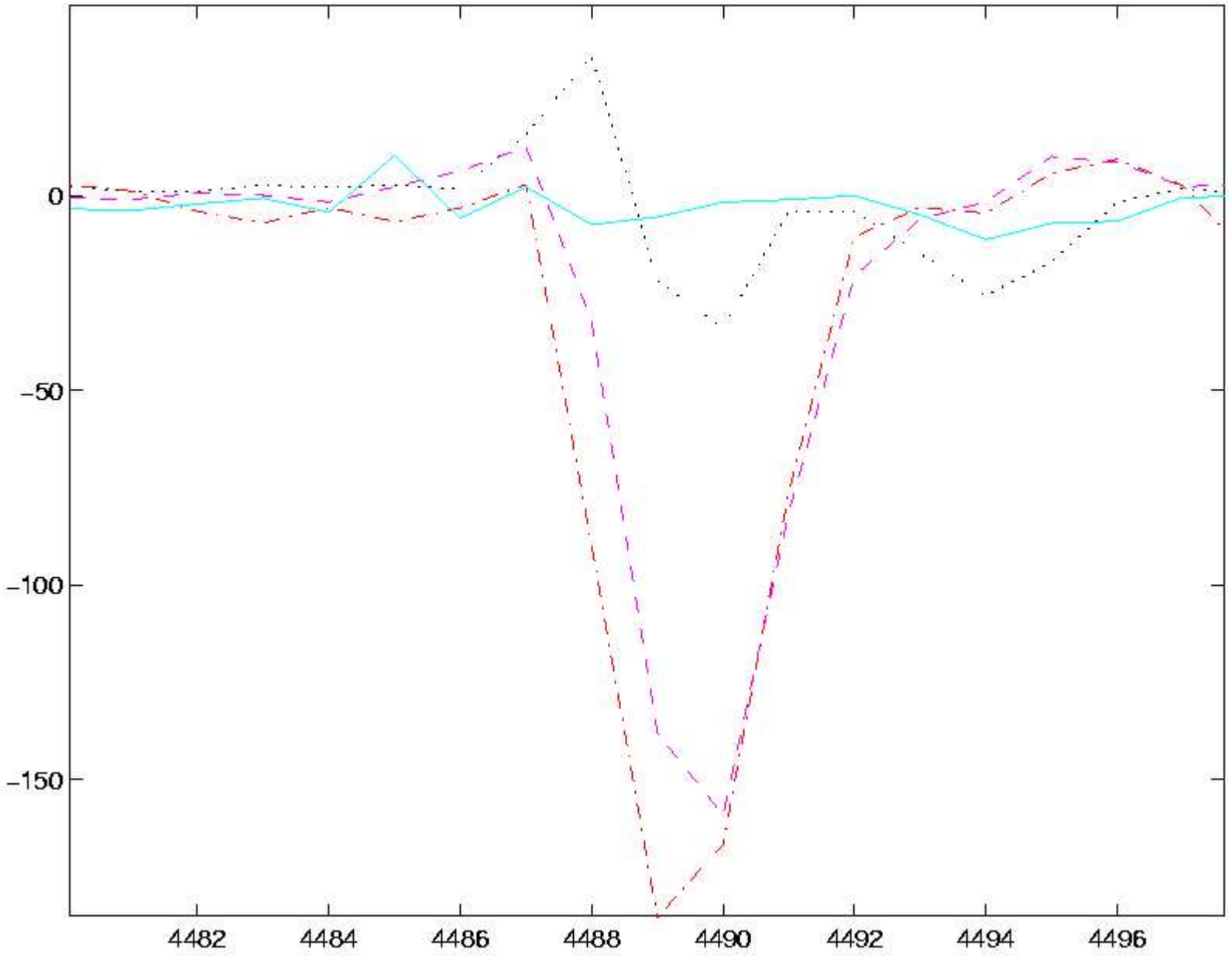
EM vs. Power

- Is EM useful in the presence of power?
- Yes, several EM carriers: Generated, Ambient, Introduced…
  - Experimentally verified:
    - Different carriers carry different information.
    - Some EM leakages substantially different from Power leakages.
  - Experiment: Use DEMA/DPA correlation plots to judge extent of leakage from different EM carriers & compared with power signal.

4 Time Synchronized DPA/DEMA Correlation Plots



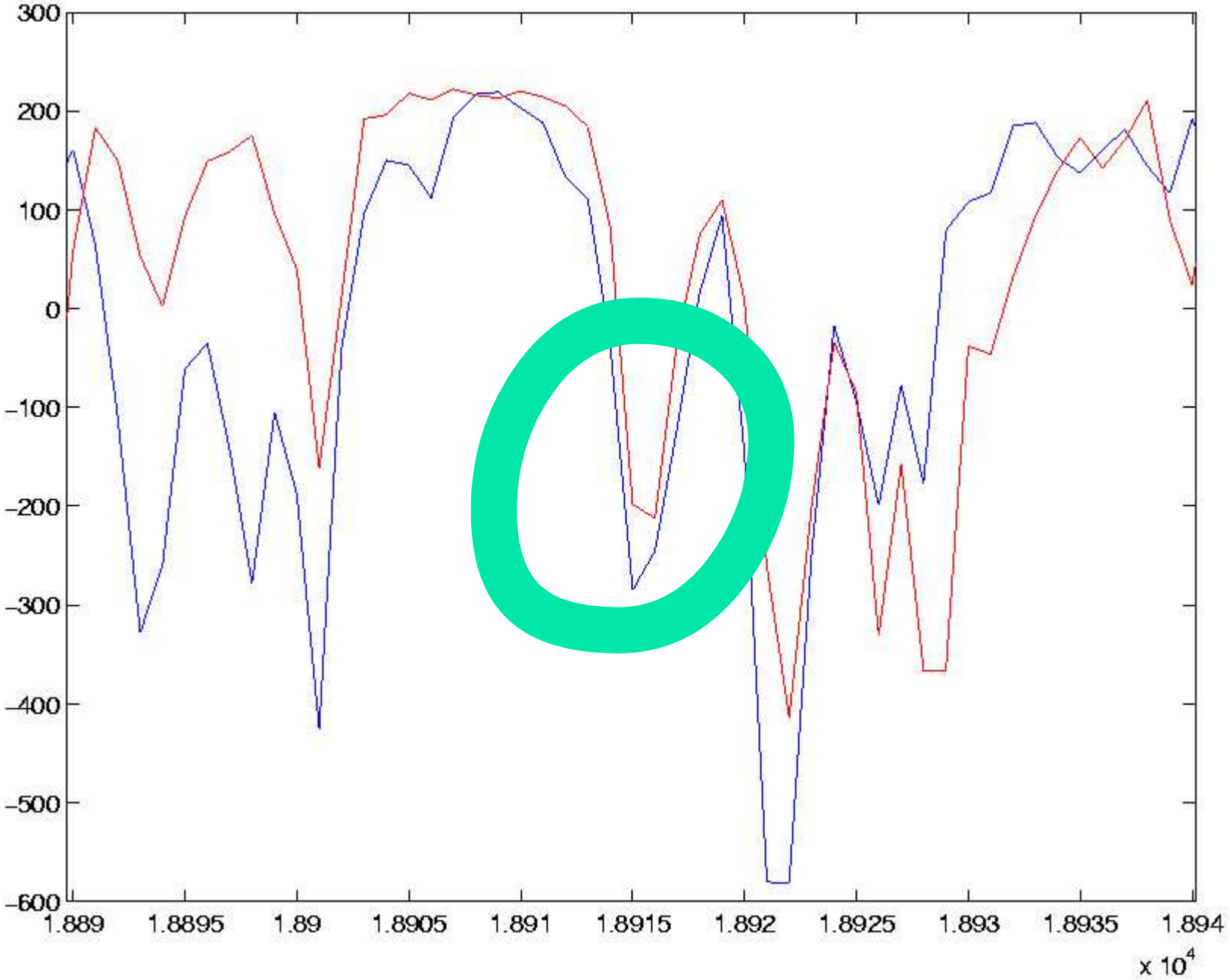
4 Time Synchronized DPA/DEMA Correlation Plots



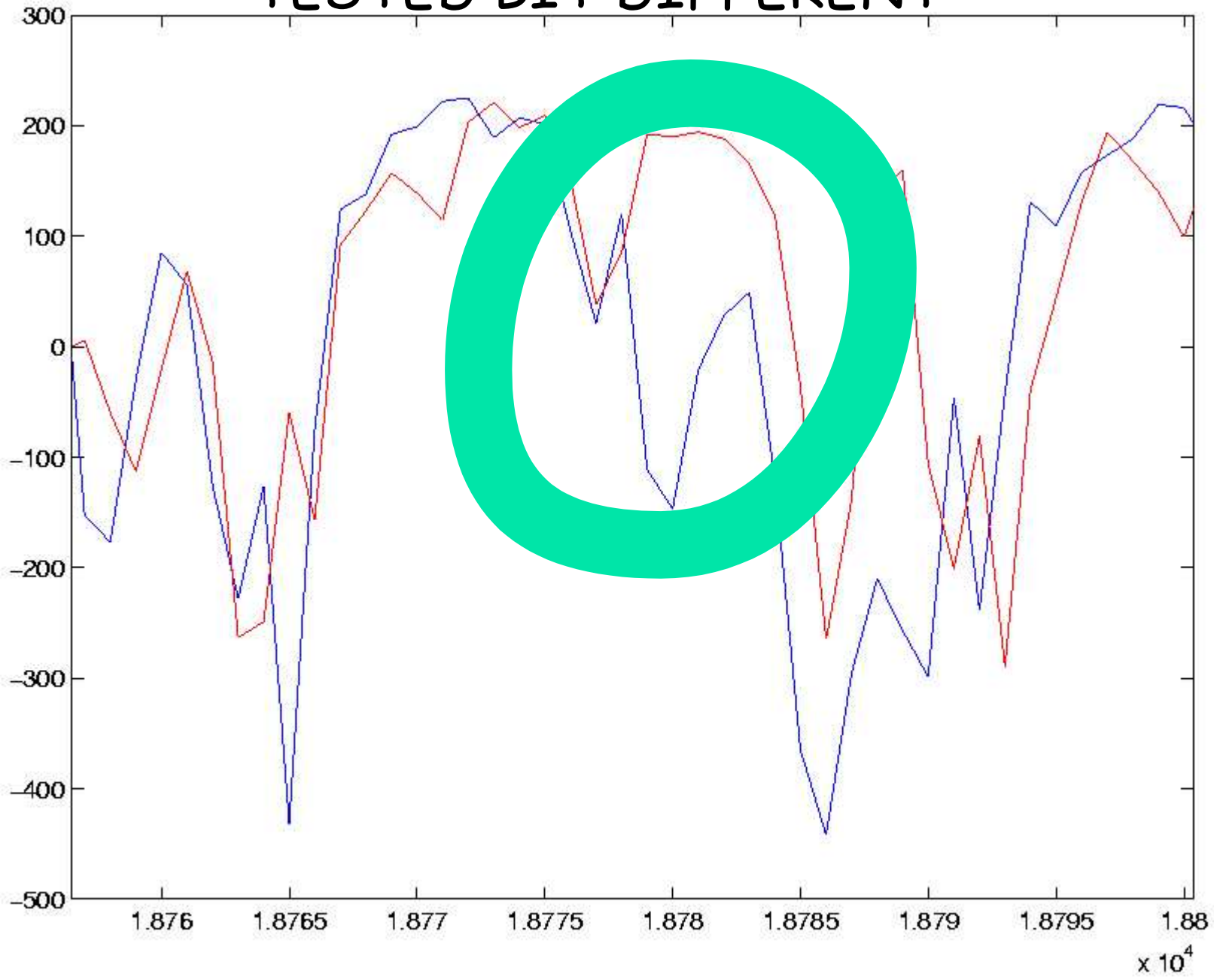
Bad Instructions

- Instructions where some EM leakage >> Power leakage.
- Typically CPU intensive rather than bus intensive.
- All architectures have BAD Instructions.
- Example: Bit-test on several 6805 based systems leaks tested bit.

TESTED BIT = 0 IN BOTH TRACES



TESTED BIT DIFFERENT



Bad instructions can break power analysis countermeasures

- Assumption behind power analysis countermeasures
  - Minimize information leakage (from power) from each execution sequence.
    - Additional techniques[KJJ, C et al, GP] can amplify uncertainty.
- Bad instructions in DPA-resistant implementations violate the assumption and create vulnerabilities.
  - Large EM leakage → SEMA.
  - Moderate EM leakage →Higher-order EM attacks on share-based DPA countermeasures [C et al, GP].
    - Some attacks work even when code unknown!
    - Example given in paper.

Results and Further Work

- Attacks
  - Commercially deployed smart cards
    - Identification of compromising AM/Phase modulated carriers and bad instructions for several cards.
    - DES, RSA, DPA-resistant DES
    - COMP-128 on GSM SIM cards
  - RSA on SSL Accelerators.
- Further Work
  - Multi EM-channel attack techniques
  - EM vulnerability assessment
  - http://www.research.ibm.com/intsec/

Countermeasures

- Require sound vulnerability assessment.
- Countermeasures include:
  - Circuit redesign to reduce unintentional emanations.
  - Reducing S/N ratio
    - EM Shielding
    - Noise introduction
    - Physically secure zones.
  - Randomization based software countermeasures similar to DPA countermeasures.