Electromagnetic Analysis of Synchronous and Asynchronous Circuits using Hard Disc Heads

Theo Markettos, Simon Moore

16th UK Asynchronous Forum

September 2004

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Outline

- Introduction to sidechannels and electromagnetic analysis (EMA)
- Construction of different sensors for EMA
- Differential EMA on synchronous and asynchronous processors

Side channels and Security

- Tamperproof security system
- Must interface with the environment
- Side channel: Information leakage through unwanted emanations
  - Power consumption
  - Electromagnetic fields
  - Optics

History of electromagnetic analysis

- Military heritage: Great Seal Bug of 1946

History of electromagnetic analysis

- US Military codename TEMPEST
- Information leakage from wiring, displays, processing equipment, printers etc.
- TEMPEST proof PCs, monitors, telephones available from 1980s
- TEMPEST screening used in government buildings and embassies worldwide

TEMPEST on smartcards

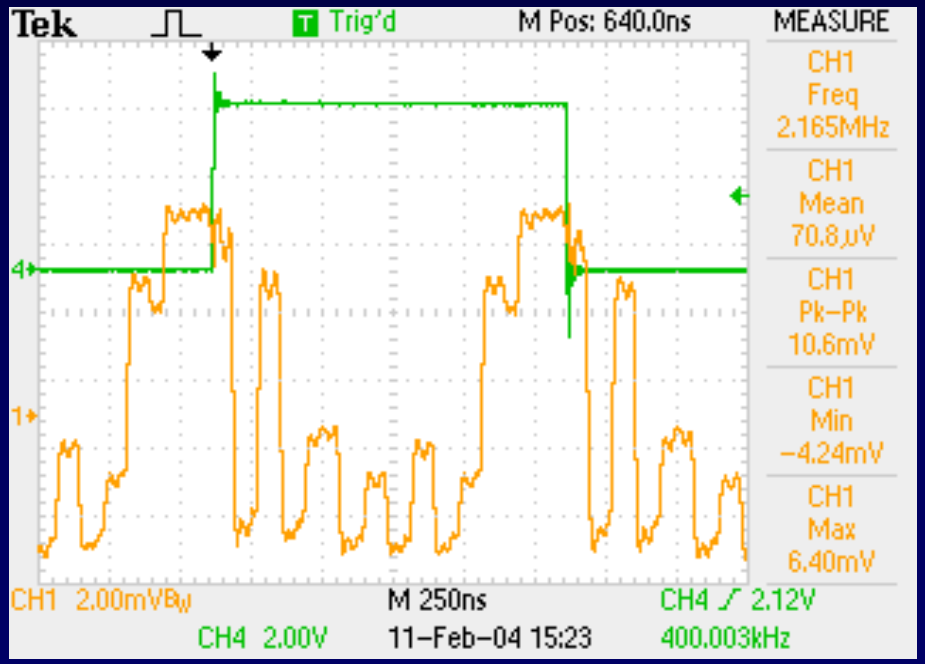
- Smartchips: on credit cards, passports, phone SIMs, pay TV
- Assume smartchip is a tamperproof ‘black box’
- But we have full control over its environment
- Want a cheap, targeted, non-invasive attack

Measuring the E-M field

- Measure the electric field component
  - Electric field probe
- Measure the magnetic field component
  - Inductive hard disc head (circa 1990)
  - Giant magnetoresistive hard disc head (circa 2000)
  - Anisotropic magnetoresistive magnetometer

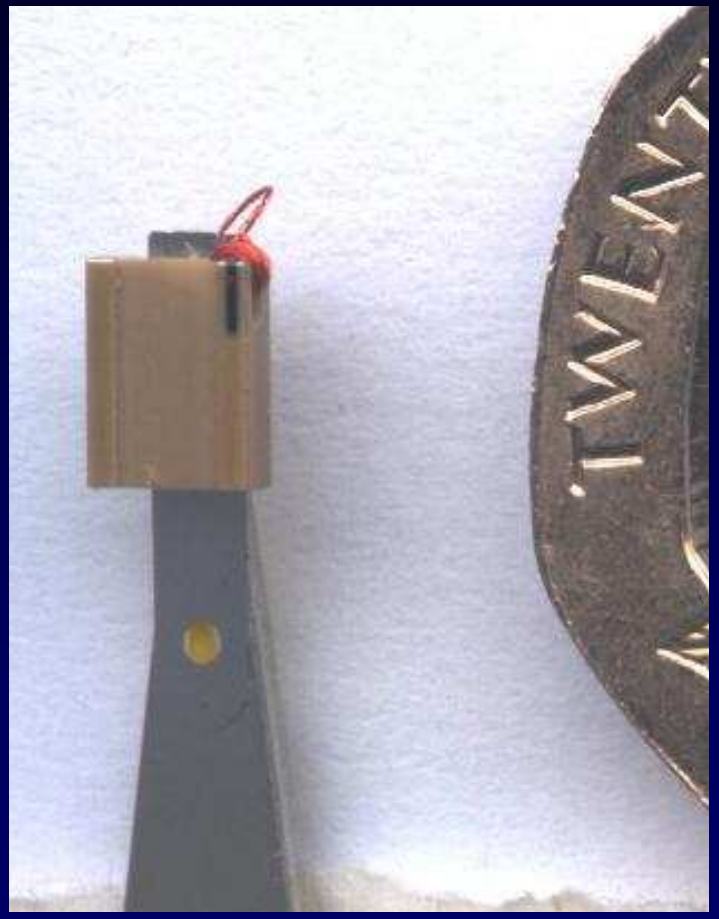
Electric field probe

- Coaxial cable direct to ‘scope
- Couldn’t detect ALU activity, only bus traffic and clock on bond wires



Inductive hard disc head

- From Western Digital 80MB drive, circa 1990
  - based on coil around ferrite core
- Measures derivative of field:
  - $V \propto dI/dt$
- Surface mount gain 400 amplifier, then to scope
- Plausible results: see later

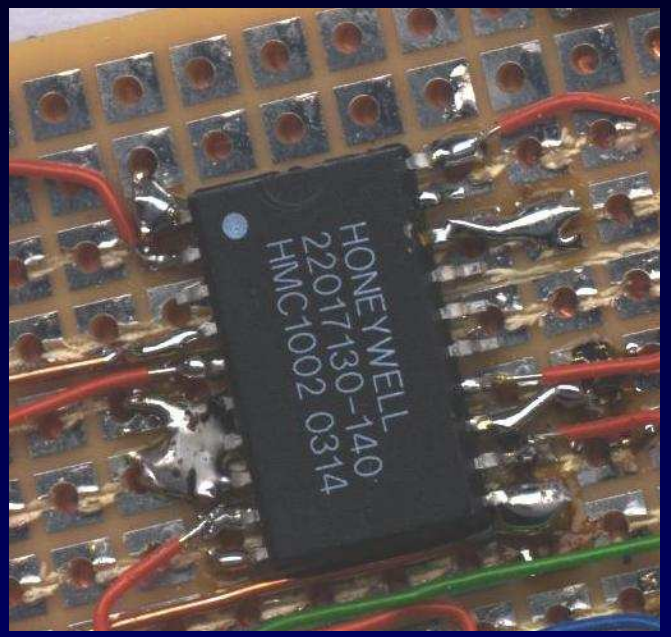


Giant Magnetoresistive (GMR) head

- From IBM 45GB drive, circa 2000
- $V \propto I$
- Buffer → gain 400 amp → scope
- Couldn’t distinguish any non-noise emanations from test chip
- Conclusion: GMR head isn’t sensitive enough
  - HDDs fix this by flying head nm from disc surface

Anisotropic magnetoresistive (AMR) magnetometer

- Honeywell HMC1002, 2 axis magnetometer, resolution 27μGauss (2mA/m) at DC. Freq up to 5MHz specified
- $V \propto I$
- One die per axis, no data on offset between them
- No data on frequency rolloff
- Buffer → gain 400 amp → scope
- Plausible results: see later

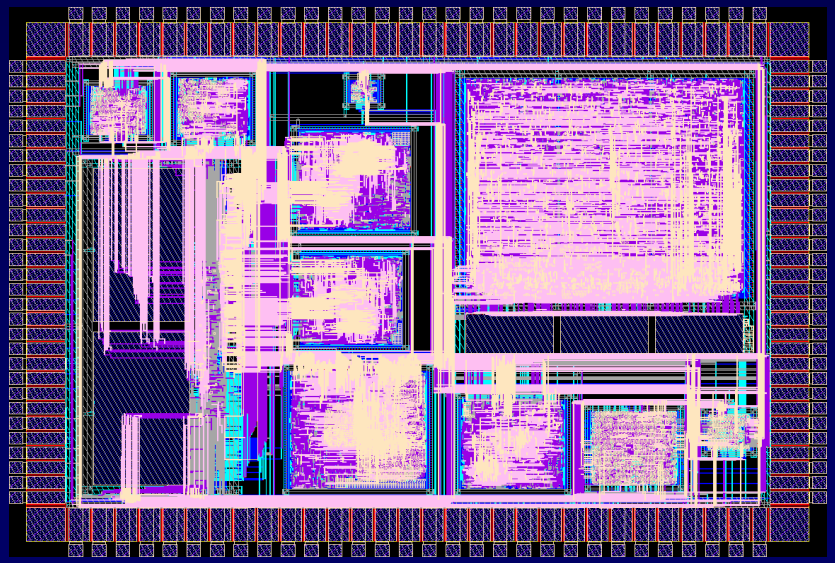


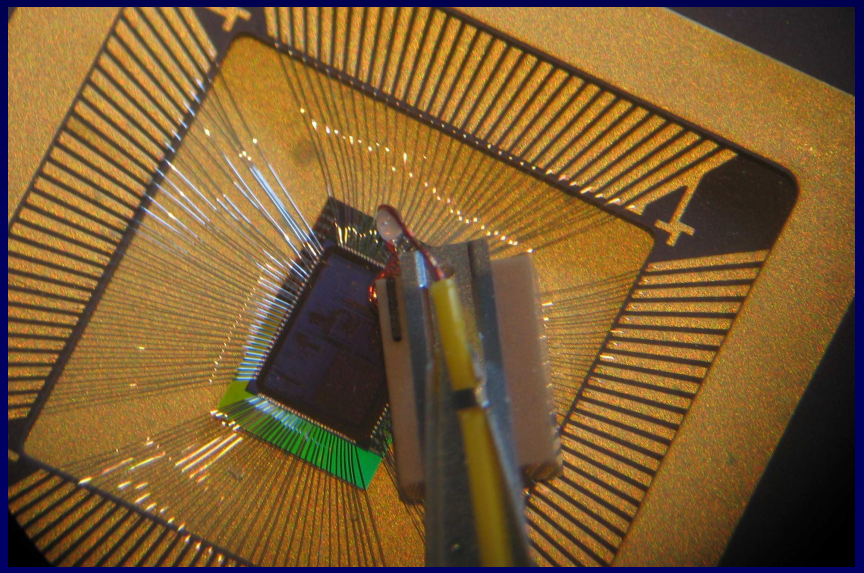
Differential electromagnetic analysis (DEMA)

- Basis of EM attacks:
  - Subtract EM traces of smartcard performing different operations, or on different data
  - If they differ, we might infer the operation that took place
  - We might then deduce secret information (eg key bits)

Test subject

- Springbank chip (Cambridge, 2002)
- Five 16-bit XAP processors, SRAM, bus crypto, modular exponentiator
- We tested synchronous XAP, and secure dual-rail asynchronous XAP

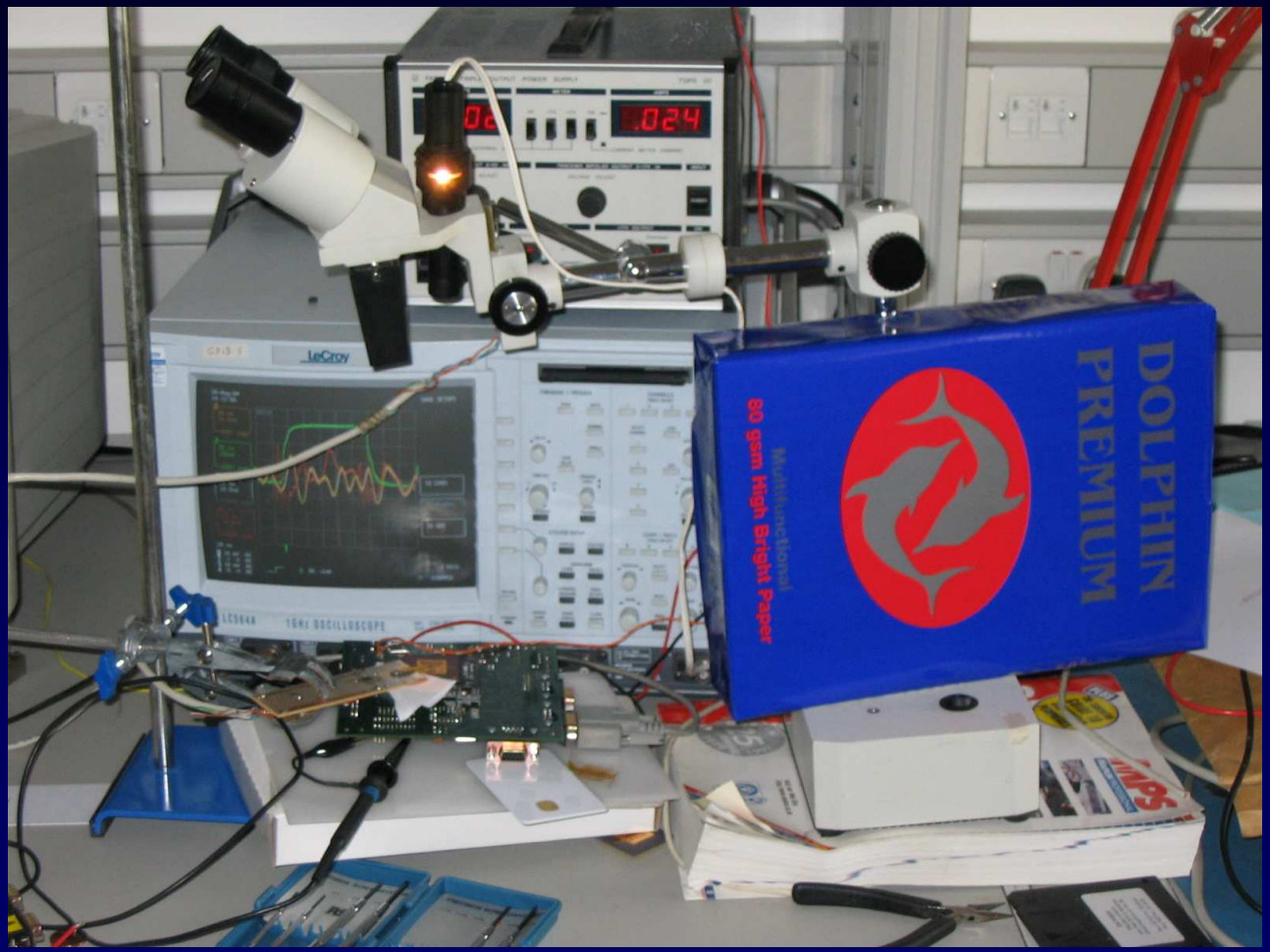




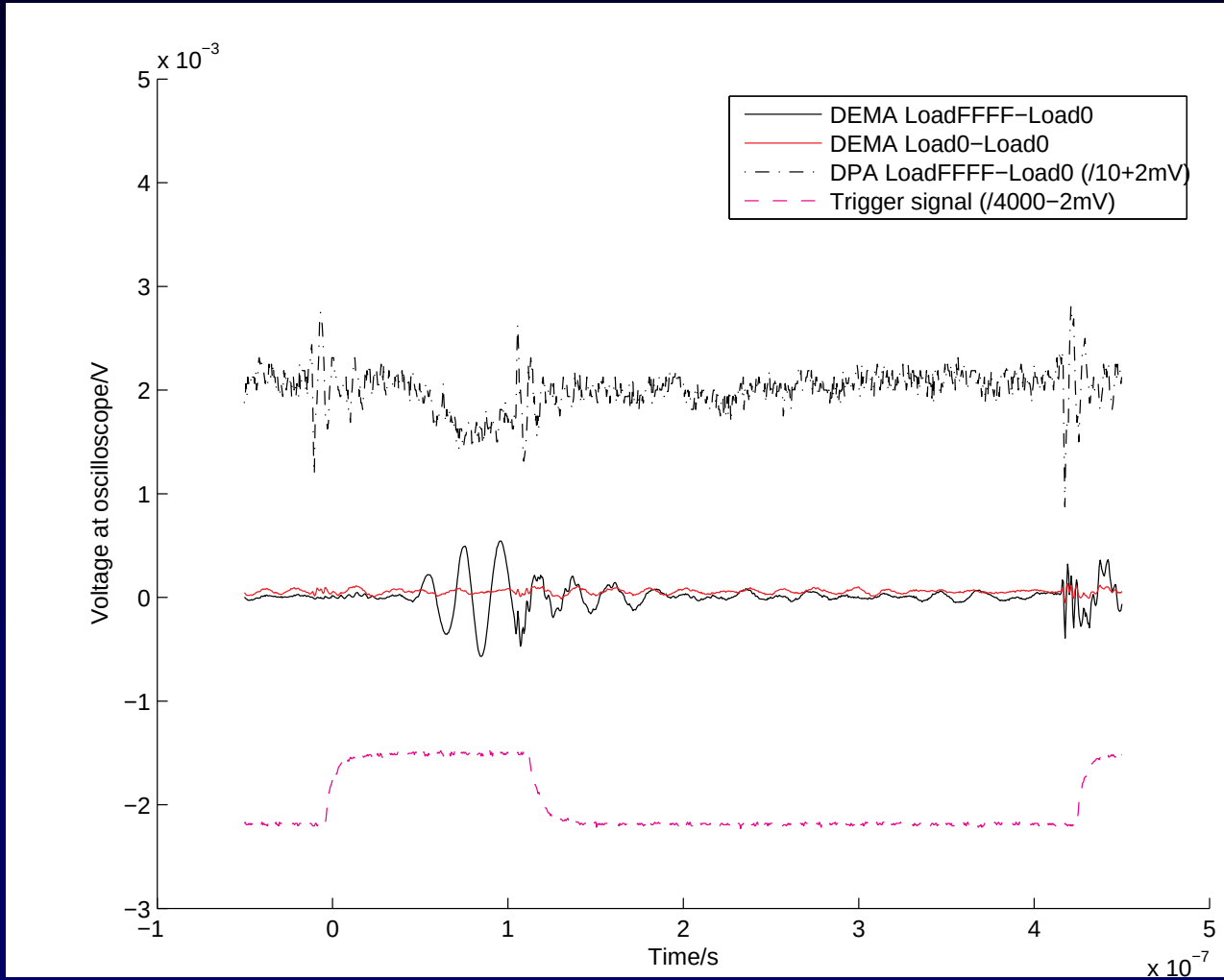
Test apparatus

- Springbank chip on test board
- 10Ω resistor in series with 1.8V Vcore, measures current consumed
- Run test program: load 0x0000 or 0xFFFF from SRAM. Average EMA over 5000 sweeps.
- Align head over chip by hand (and microscope!)
- Control: compare loads of same value to ensure no experimental variations

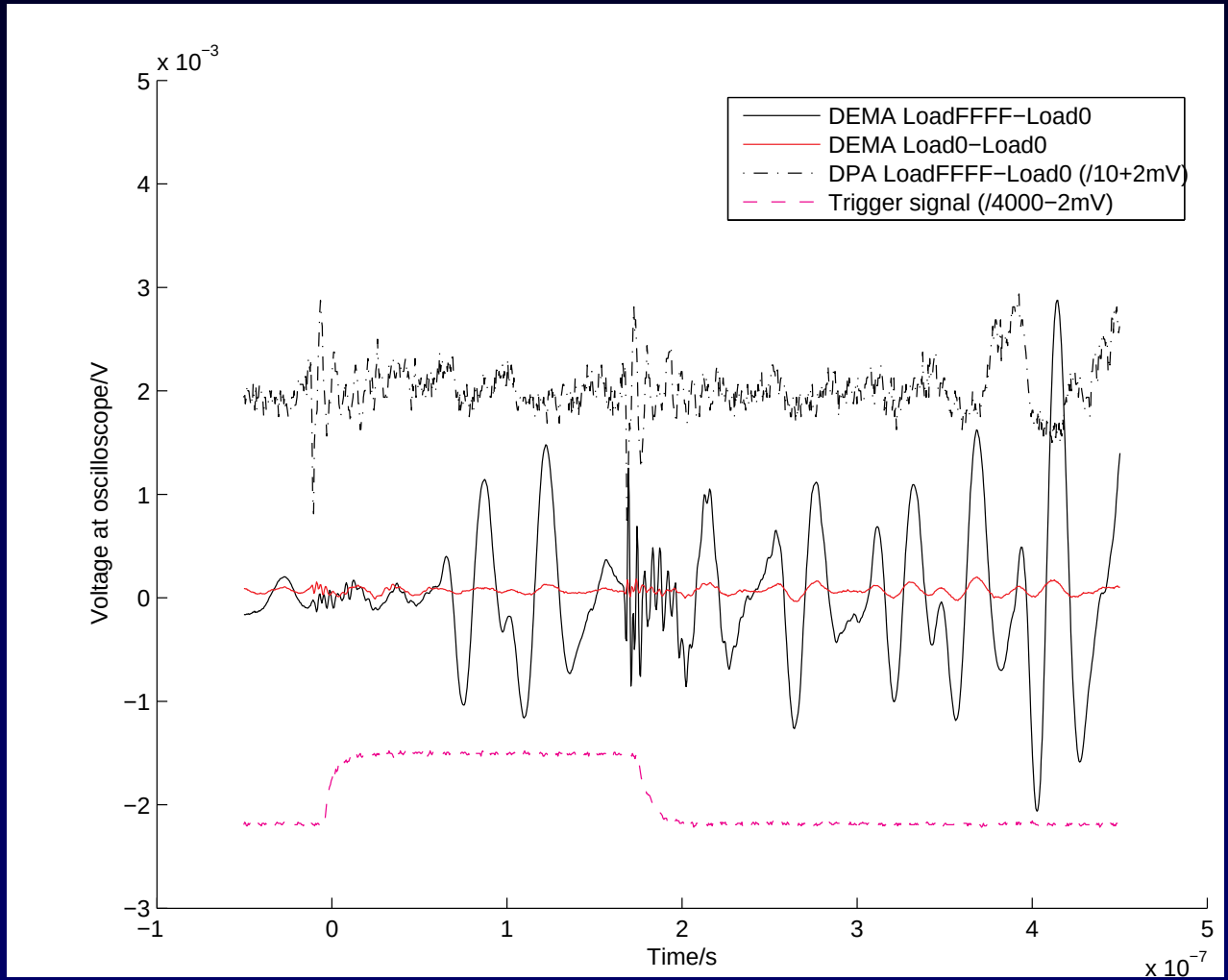
Experimental apparatus



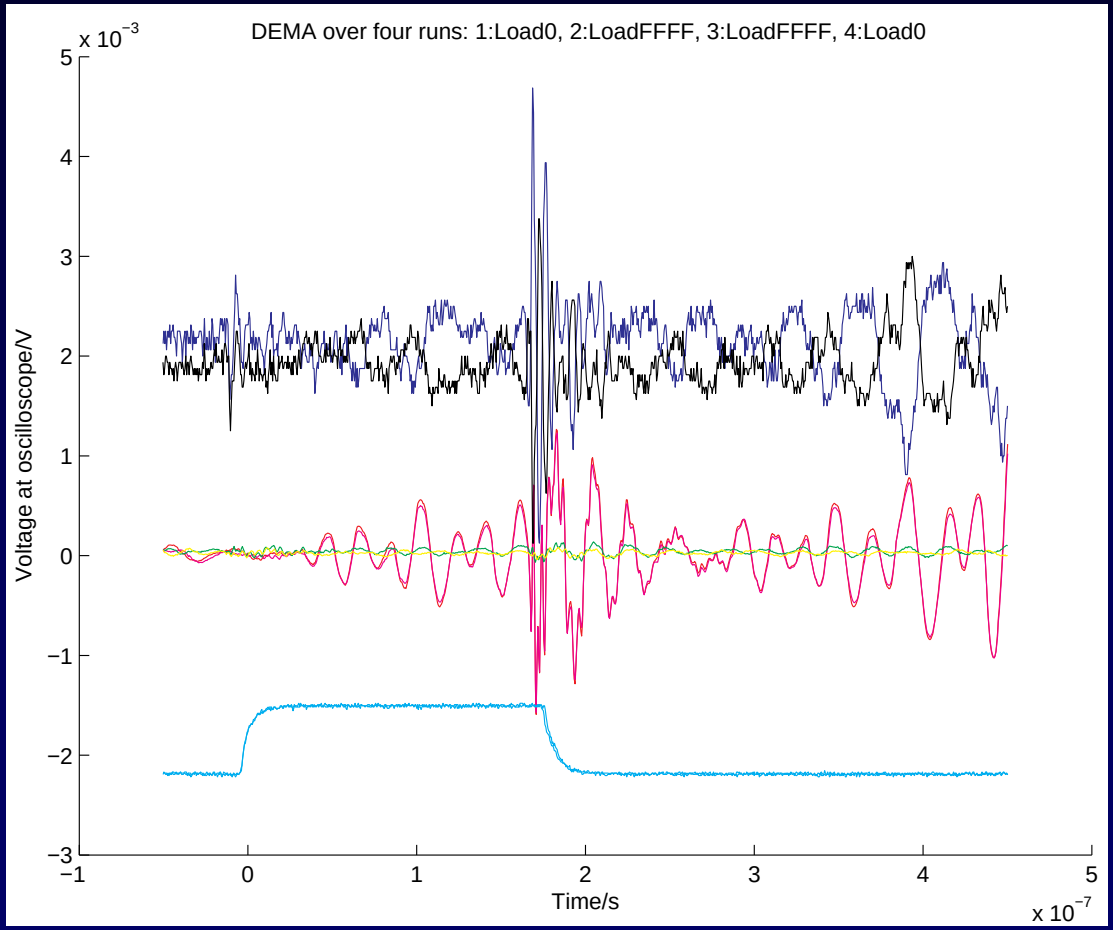
DEMA with inductive sensor: Synchronous XAP



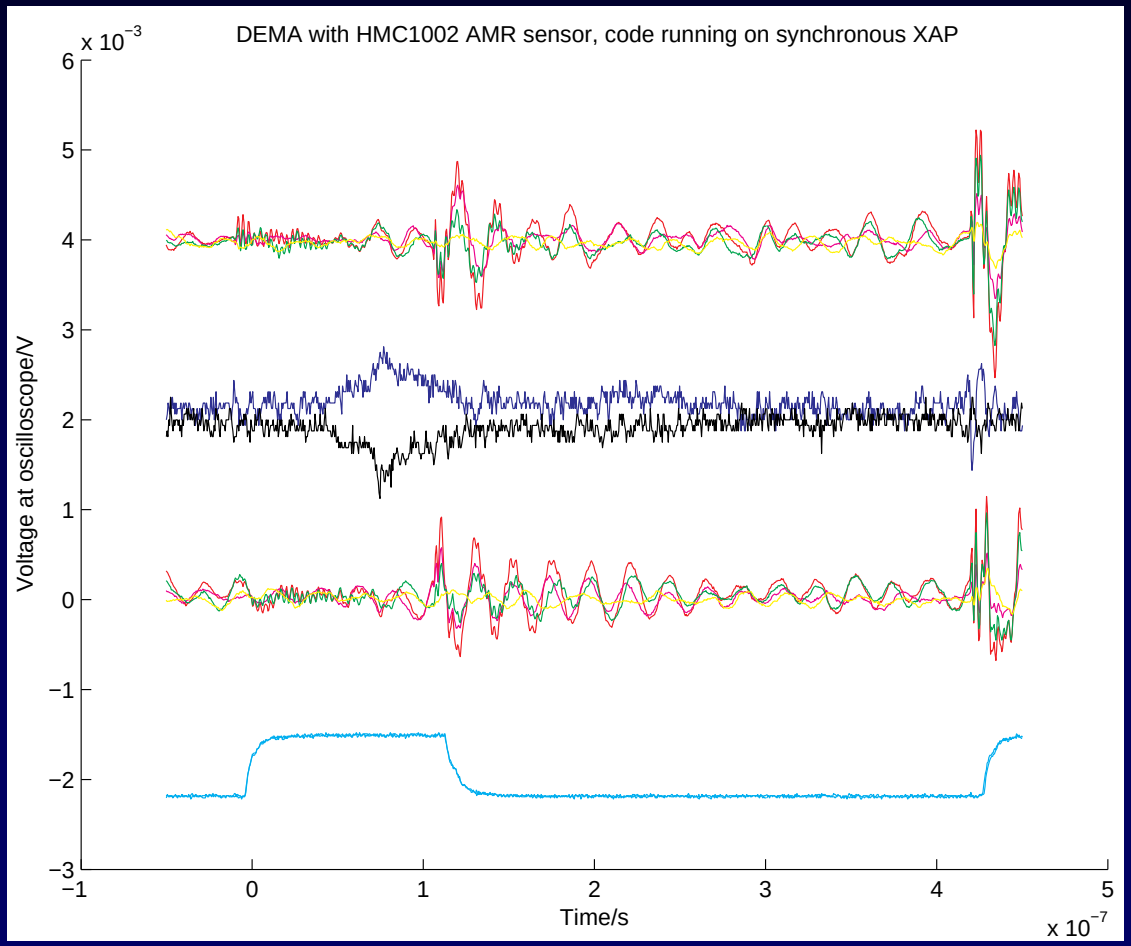
DEMA with inductive sensor: Secure async XAP



DEMA: Inductive sensor, code on async XAP, head over sync XAP



DEMA with AMR sensor



Y axis

Power

X axis

Conclusions: DEMA

- Secure XAP shows more DEMA than sync XAP
- Data dependent timing?
  - Sync XAP is resynchronised by the clock, so DEMA only evident for short period
  - Secure XAP is async; timing differences propagate
- Off-the-shelf memory block used: unbalanced, but a fixed delay inserted for memory access
  - Timing dependencies from inside XAP, not memory

Conclusions: Sensors

- E-field probe: E-field falls off with $1/r^3$ – hard to detect
- GMR: not sensitive enough?
- AMR: package makes it clumsy to position. Not very directional, two dice aren't measuring same field in quadrature
- Inductive: easy to position, good resolution, low pass (R-L) filtering effect

Further work

- Bulk data capture and die scanning
- DEMA of Springbank core
  - Test ALU operations, avoiding memory
  - Compare with Huiyun Li's simulation results
- Characterise building blocks of EMA
  - Design methodology for EMA defence

Summary

- Evaluated sensor technologies
- Demonstrated DEMA on a test chip
- Compared synchronous and asynchronous processors for DEMA