Electromagnetic Analysis of Synchronous and Asynchronous Circuits using Hard Disc Heads

A. Theodore Markettos and Simon Moore
Computer Laboratory, University of Cambridge, JJ Thomson Avenue, Cambridge, CB3 0FD, UK
theo.markettos@cl.cam.ac.uk, simon.moore@cl.cam.ac.uk

Abstract

Electromagnetic analysis (EMA) involves the study of the EM fields emanating from a tamper-proof device, with a view to extracting secret information. A number of electric and magnetic field sensors for EMA, including hard disc heads, have been designed and their performance evaluated on synchronous and asynchronous secure processors.

1 Background

Electromagnetic analysis (EMA) studies the electric and/or magnetic field side channels emanated from a device to learn the operations being performed.

Use of electromagnetic emissions to compromise security systems has been mostly the domain of the government security services until recently. Notable examples include the Great Seal Bug of 1952 in the US embassy in Moscow [5] and British interception of plaintext side channels within encrypted telex traffic from the French embassy in London in the 1960s [9, pp 109–112]. Work in this area is coming to light under the US military codename 'TEMPEST'[7]. TEMPEST-proof devices including PCs, telephones and monitors have been available since at least the 1980s.

There is increasing interest in TEMPEST-style attacks on secure semiconductor devices such as smartcards. Hofreiter and Laackmann [5] provide a good background on the various attack modes. Three groups have published significant results — those at IBM [1], Gemplus [4] and Université catholique de Louvain [8]. However little information is available about the specifics of their experiments to enable them to be repeated.

We have developed and tested a number of sensors to detect electromagnetic fields. They can be divided into those that detect electric and those that detect magnetic fields.

2 Experimental method

A number of sensor test boards have been constructed, most with onboard amplifiers. All circuits were built from surface mount components on ground plane.

Further tests to perform electromagnetic analysis are detailed in Section 5.

3 Electric field sensors

The simplest EM field sensors are the antennas which generally measure the electric field component of an EM signal. Most antennas are designed for specific frequency ranges, and are poorly suited for broadband applications as required for EMA. A number of antenna topologies exist for broadband signals but many antennas of a suitable size to be placed near a chip have their frequency band in the gigahertz region or higher, making them unsuitable for EMA of megahertz-band emissions.

A traditional passive antenna is designed to resonate at the desired frequency of reception and to match the impedance of free space to that of a coaxial cable. Instead we used an active antenna, an antenna with built in amplification where matching is performed by the amplifier;

the simplest of which is the monopole. A simple monopole was constructed by baring 16mm of core of RG58A/U coaxial cable, connected directly to a Tektronix TDS2024 oscilloscope.

3.1 Results

Scanning the die area of a packaged LH77790B synchronous ARM-based microcontroller running with 25MHz clock produced no signals synchronised with the operation of the processor. By touching this probe on the chip package, it could detect signals emanating from bond wires carrying the clock and data bus, but could not discern different ALU operations.

4 Magnetic field sensing

The magnetic emanations from a chip can be detected in a number of ways. Primarily the magnetic emanations are not caused by electromagnetic radiation (photons) emitted from the device, but from currents flowing within it which create a magnetic field, the near field, which can be detected by sensors physically close to the device.

The main groups of sensors are those which use induction. For a static loop, the induced voltage is proportional to the current derivative [6]:

$$V = M\frac{dI}{dt} \tag{1}$$

where M is the mutual inductance, incorporating variables associated with the physical construction and relations of the sensing loop and current carrying wire.

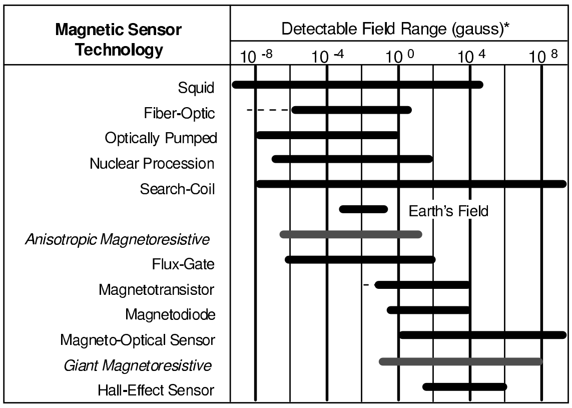
Another type of sensors are those that use the Lorentz force [6]:

$$F = q(\mathbf{v} \times \mathbf{B}) \tag{2}$$

Since, by the Biot-Savart law, the current I that flows is related to the field $\mathbf{B}$ by:

$$d\mathbf{B} = \frac{\mu}{4\pi}\frac{I\mathbf{R} \times \nabla\mathbf{L}}{|\mathbf{R}|^3} \tag{3}$$

Thus $F \propto B$ and $B \propto I$. If the transducer linearly converts the Lorentz force into a physical quantity (eg voltage or resistance) then that will be proportional to the current.



* Note: 1gauss = 10^{-4}Tesla = 10^{5}gamma

Figure 1: Sensitivity of magnetic sensors (from [2])

Figure 1 shows the relative sensitivities of various magnetic field sensors.

4.1 Hard drive head technology

Storage devices have been a primary driver of magnetic sensors in recent years with the need for ever growing storage densities. Despite shrinkage, the write head has typically remained inductive throughout, whilst the read head has progressed through several technologies since 1990. Very roughly:

Pre-1990	Inductive ferrite cored
1990-1995	Thin film inductive
1995-1999	Anisotropic magnetoresistive (AMR)
1999-2001	Giant magnetoresistive (GMR)
2001-2003	GMR or GMR variants (spin valve, spin dependent tunnelling)
2004+	Collossal magnetoresistive (CMR)

4.2 Inductive sensors

The simplest magnetic field sensor is a loop of wire. This is to a magnetic field what a dipole is to an electric field. An EMF is induced in the loop due to a change in magnetic flux through the loop caused by a changing magnetic field produced by an AC current-carrying conductor. This is the transformer effect as outlined above.

A sensor uses an inductive hard drive head from an 80MB Western Digital WDC280 drive dated 1990 followed by an NE592D8 amplifier. When

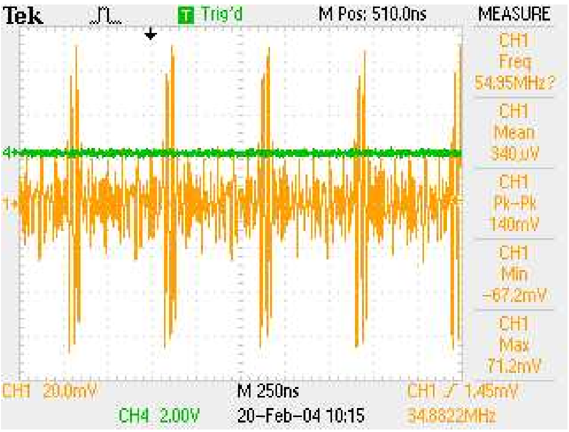


Figure 2: Inductive sensor: processor running one instruction loop

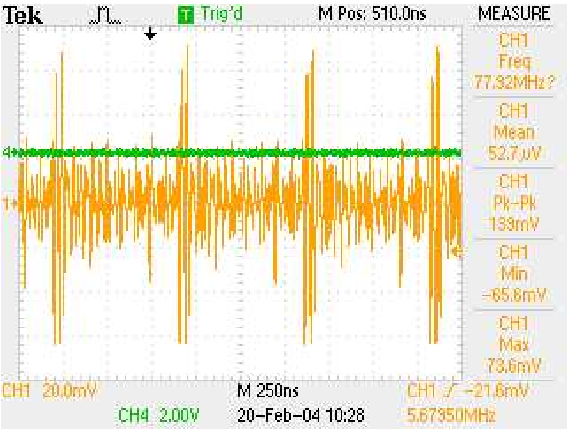


Figure 3: Inductive sensor: processor running two instruction loop

applied to the LH77790B processor, it was able to detect control flow by distinguishing one and two instruction loops (Figures 2 and 3 respectively).

A multiple turn loop such as this will be more sensitive in the open loop case, but has an increased mutual inductance with lower cutoff frequency when terminated with a 50Ω load. However in this case we are terminating the loop with an active amplifier (the NE592D8 in this configuration has a DC input resistance of typically 4KΩ). The 300mm of 50Ω coaxial cable to the amplifier is too short to be significant at these frequencies.

Both sides of the head in series measured R = 5.42Ω, L = 9.16μH. With a 4KΩ load the 3dB cutoff by the low pass filtering effect occurs at 70MHz.

4.3 Giant magnetoresistive sensors

Another sensor uses a head from a 45GB IBM Deskstar DTLA-307045 drive (Figure 9). This is a four terminal head with two separate wire pairs; across one pair is measured 35.8Ω and the other 17.5Ω. 35.8Ω is low for a magnetoresistive head but IBM's press release states this drive uses GMR head (no other data was available). We assume this is the GMR part, the other pair being the inductive write head.

As with commercial head amplifiers, the head is biased with a 10mA current. It is followed by a high impedance CLC417 buffer and gain 400 NE592D8 amplifier.

There was only noise emanating from the output when placed near the LH77790B test chip. There was no correlation between the output and the position of the head, nor anything resembling a signal related to the processing being performed.

Figure 1 suggests that GMR is only sensitive down to 10^{-1} Gauss, or 7.9Am^{-1}. The magnetic field of a printed circuit board track of width w with the sensor placed directly above the track can be approximated by[6, p. 240]:

$$H = \frac{I_x}{2w} \tag{4}$$

Considering a power wire of perhaps 100μm, we find that a GMR sensor can resolve a current of 1.6mA. With this resolution we are unlikely to discern currents of this order through noise. A thinner track will have a stronger magnetic field for the same current, it is likely that thin tracks do not carry large currents. Despite having no data for the head under test it seems likely that it would be suffering from these problems. Therefore this avenue does not seem worth pursuing much further.

4.4 Anisotropic magnetoresistive sensors

Honeywell sell a variety of commercial magnetometer devices. The most sensitive HMC1001 and HMC1002 claim a resolution of 27μGauss (or 2.1mA/m) at 10Hz, with a typical magnetic bandwidth of 5MHz. The HMC1002 contains two dice at 90° to each other; its outputs were each buffered by a CLC417 then amplified differentially by an

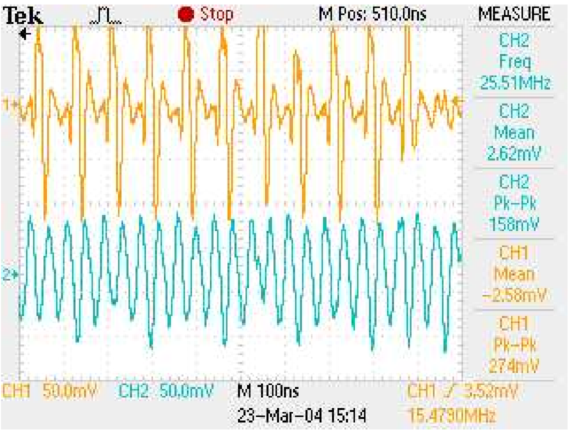


Figure 4: AMR sensor over LH77790B running single instruction test, two traces showing X and Y components of magnetic field. Note that dice that measure components are some millimetres apart.

NE592D8. The offset and set/reset straps were left unconnected.

When positioned over the LH77790B, the dice detect the clock signal very well (bottom trace of Figure 4) but it is difficult to resolve other detail.

5 Electromagnetic analysis

Differential electromagnetic analysis (DEMA) was carried out using the Springbank test chip, fabricated as part of the G3Card project [3]. This contains five processors based on the 16-bit Cambridge Consultants' XAP each in a different design style. The synchronous and secure dual-rail asynchronous XAP processors were used in these tests.

Two different programs were run on the XAP with a core loop of:

```
; positive trigger on IOM[0] output pin
                st      ah,@(0,x)
; load value from memory
                ld      al,@val
; negative trigger on IOM[0] output pin
                st      y,@(0,x)
```

By modifying the data section of the program, the value loaded was set to be 0xFFFF in one program, `LoadFFFF`, and 0x0000 in the other, `Load0`.

Electromagnetic signals were averaged over 5000 sweeps with a LeCroy LC564A oscilloscope to average out the noise power received. To minimise experimental error each of the two programs were run twice, in the order `Load0`, `LoadFFFF`, `LoadFFFF`, `Load0`. Any non-operation-dependent factors will show if the two `Load0` traces are different. We also plot one sweep of differential core power for the whole chip with no averaging. Each experiment of 4 program runs was taken over a few minutes with longer times between experiments. 15 minutes warm up time was allowed starting from cold.

5.1 WDC280 inductive head

The positioning of the head made a large difference in the received signal. When running the programs on the synchronous XAP, Figure 5 shows DEM with the head over this core. The `Load0-Load0` trace is very small, suggesting that there have been few external variations (movement, supply voltage changes etc) over the run of the experiment.

This shows a noticeable DP blip in the middle of the trigger pulse, when data is being loaded from memory. In addition, with the head over the synchronous XAP we can see a DEM pulse coincident with it which subsequently dies away. When over the secure XAP this pulse may also be present, but the picture is much harder to discern.

The converse is seen when running the program on the secure XAP. Figure 6 shows the traces with the head over this processor. In this case we see a huge DEMA trace starting from the point of data dependency when over the secure XAP, whilst a similar yet much smaller trace is seen with head over the synchronous XAP. This suggests that physical proximity is a key factor in determining the EM received.

Why is the DEMA trace for the secure XAP so much larger than that of the synchronous XAP? Both traces were taken with exactly the same gain settings. It is difficult to ensure that the probes were the same physical distances from the chip since they were moved manually between experiments — thus the magnitudes of the DEMA traces for each position should not be directly compared. However we can still see that the DEMA for the secure XAP continues much longer in time than the synchronous XAP, even including differences in execution speed shown by the length of the trigger pulse. We hypothesise this is due to data de-

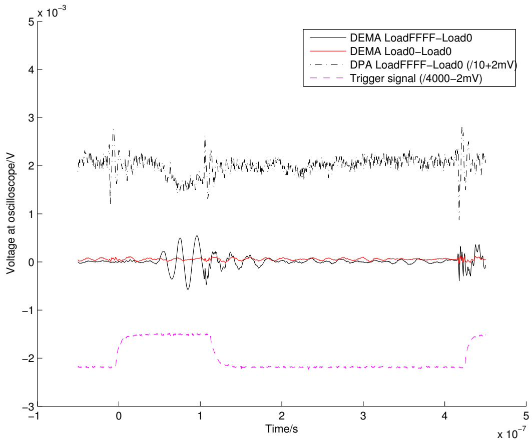


Figure 5: Inductive sensor over synchronous XAP, code running on synchronous XAP

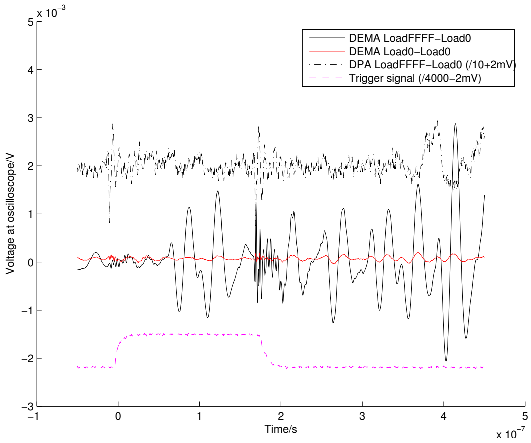


Figure 6: Inductive sensor over secure XAP, code running on secure XAP

pendent timing within the asynchronous secure XAP — loading a value with a differing Hamming weight takes a different amount of time which is reflected in the DEMA trace. This then offsets in time all subsequent operations, being visible as DEM.

5.2 HMC1002 AMR sensor

Similar experiments were performed with the HMC1002 sensor. Accurate positioning is difficult to achieve visually when the target is obscured by its large SOIC package and PCB.

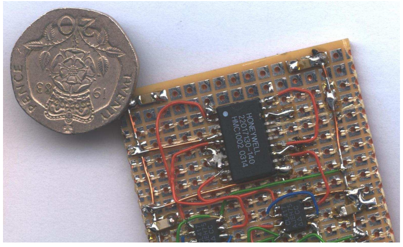


Figure 7: Honeywell HMC1002 anisotropic magnetoresistive sensor and amplifier board (20 pence coin for scale)

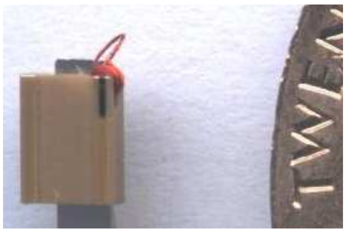


Figure 8: Inductive head from Western Digital WDC280 hard drive, circa 1990 (20 pence coin for scale)

Figure 9: Giant magnetoresistive head from IBM Deskstar DTLA-307045 drive, circa 2000 (20 pence coin for scale)

The HMC1002 data sheet does not give the distance between the two dice which separately give X and Y magnetic fields, so relative positioning between each axis cannot be accurately judged without depackaging the device. Despite this, the two axis sensors seem to give roughly similar results suggesting that the sensors are not very localised. Whilst the trace for the secure XAP is larger than that of the synchronous XAP this may be related to positioning. As it is difficult to accurately target a particular area the magnitudes may not be directly comparable. There appears to be a difference in the secure XAP case, but this requires further work to test.

6 Summary

So far we have investigated examples of inductive, anistropic magnetoresistive (AMR) and giant magnetoresistive (GMR) magnetic sensors and an electric field probe. We concluded that GMR sensors were not sensitive enough and the AMR sensor under test was bulky and not ideally suited to a test environment. The electric field probe appeared to reveal little information about a chip core but more about its I/O activity. Inductive sensors had the best performance, and were used successfully to distinguish memory loads of different Hamming weights. This distinction was more pronounced on the asynchronous test processor than the synchronous processor, suggested to be due to data dependent timing.

7 Further work

There are a number of directions arising from this work that might be pursued.

Inevitably the number of sensors tested was small. This range could be expanded to include different types of inductive sensor and also other electric field sensors.

To date there was little success with GMR heads. This is hypothesised to be because the GMR element is not sensitive enough to the magnetic fields that concern us. However GMR heads also contain an inductive write head of very small dimensions. It may be worth investigating whether any useful signal can be extracted from this, or why this is not possible.

Huiyun Li has done some simulation work on information leakage by amplitude modulation of clock harmonics. This work can be tested experimentally using EMA — either by postprocessing standard time domain traces or using AM demodulation in hardware. IBM [1] have done some other work in this field.

References

[1] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM side-channel(s). In *Proceedings of CHES2002*, pages 29–45, August 2002.

[2] Michael J. Caruso, Tamara Bratland, Carl H. Smith, and Robert Schneider. A new perspective on magnetic field sensing. *Sensors*, December 1998.

[3] G3Card Consortium. 3rd generation smart card project. `http://www.g3card.org/`.

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In *Proceedings of CHES 2001*, pages 251–261, 2001.

[5] Peter Hofreiter and Peter Laackmann. Electromagnetic espionage from smart cards - attacks and countermeasures. *SECURE*, 6:40–43, Autumn 2002.

[6] John D. Kraus. *Electromagnetics*. McGraw-Hill, fourth edition, 1991.

[7] Joel McNamara. The complete, unofficial TEMPEST information page. `http://www.eskimo.com/~joelm/tempest.html`.

[8] Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In *Proceedings of E-smart 2001*, pages 200–210, January 2001.

[9] Peter Wright. *Spycatcher — The Candid Autobiography of a Senior Intelligence Officer*. William Heinemann, Australia, 1987.