# A Method of Thwarting EM Probe Attacks on IC Interconnect

S J Hollis, S W Moore
Computer Laboratory, University of Cambridge: {Simon.Hollis, Simon.Moore}@cl.cam.ac.uk

**Key words to describe the work:** side-channel attack, interconnect, EMA, EMC, CDMA.

**Key Results:** Sensitive electromagnetic data emissions are no longer detectable by existing probes.

**How does the work advance the state-of-the-art?:** Currently, physical shielding is the only tractable way to increase the difficulty of an EM attack. This paper outlines a method that uses CDMA in hardware to do much better.

**Motivation (problems addressed):** Security devices are always under attack. This technique increases their security.

## 1. Introduction

Hardware security devices are under constant attack by a range of individuals and organisations spanning the spectrum from academic researchers to organised crime. Attacks fall broadly into three categories: *invasive*, where chips are depackaged and probed; *semi-invasive*, where they are depackaged but are not destructive to the circuit; and *non-invasive* [3]. The last is the cheapest and easiest to carry out and exploits *side-channels* (unintended emissions of an IC, including power consumption, execution timing and EM radiation). A popular attack has been *power analysis*, where power consumption is monitored to infer information about switching activity. However, the non-invasive technique with perhaps the greatest potential is that of *electromagnetic analysis* (EMA) [1]. It allows the attacker to gain a localised emission readout rather than the global, aggregated view provided by power analysis. The attack is carried out using an EM probe attached to an oscilloscope. Radiation emitted by multiple runs of the device under attack is then captured, allowing for off-line statistical processing. This paper is restricted to defeating the first phase of such attacks.

An underlying assumption is that interconnect is much more capacitive than logic gates and so is responsible for the majority of EM emissions. High capacitance implies high current flow, which generates large EM fields. Our technique helps to secure these emissions.

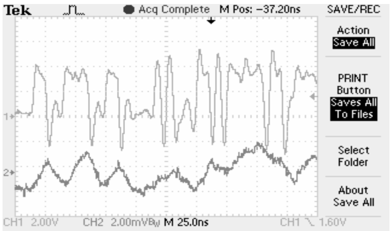

**Figure 1: Bit integration due to bandwidth limitation**

## 2. Probes

It is clear that the choice of probe is critical to the success of the attack. Markettos [4] provides a good overview of probes. The most important point to note is that all probe-scope combinations have a cutoff frequency $f_{cut,}$ above which a signal is detected much more weakly, if at all. As the frequency of an EM emission is essentially the same as the wire rate of data being transferred, any data being transferred substantially faster than $f_{cut}$ will not be resolved by the probe. Instead, several bits will have their signatures blurred by integration over time, rendering their exact values undetectable. This is illustrated in Figure 1, where the upper trace shows a pin emitting a data stream and the lower trace shows the effect on the signal from a pickup antenna that has been limited in bandwidth to 20MHz.

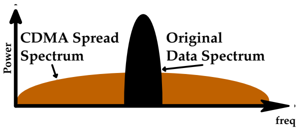

**Figure 2: Spectrum spreading effect of CDMA**

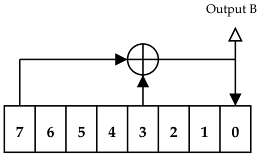

**Figure 3: 8-bit LFSR in m-sequence configuration**

## 3. CDMA

Hardware security devices normally have a low clock speed (less than 100MHz) which cannot be increased globally, either because power is limited or because they contain complex combinatorial paths. This speed is substantially lower than $f_{cut}$ for most probes. Therefore, we require a method of increasing selected sensitive interconnect line rates in order to push them above this threshold.

Code Division Multiple Access (CDMA) provides a way of transforming a signal spectrum into one that is much wider and has a lower peak power (see Figure 2). Using this, we can not only push the signal into the undetectable range, but also reduce emission at those frequencies which remain detectable. The general approach is to take a pseudo-random noise (pn) sequence running at some multiple $m$ of the logic clock rate $f$ and XOR successive bits of it with the (slower) data stream. This produces a code stream at rate $m{\cdot}f$ with, on average, an equal number of '1's and '0's. Decoding takes an identical copy of the pn stream and XORs again to recover the original data. We get $m$ identical copies of each data bit, which we sum and threshold at $m/2$ to give us the original data bit with error detection and correction. With the figures given above we are likely to require a value of $m \geq 10$. For simplicity, let us set $m$ to be 10. This gives a *chipping rate* of 10 chips/bit. The scheme is illustrated in Figure 4, where we see the slowly changing data bits XORed with ten more rapidly changing pn chipping bits, to produce the output code at ten times the data rate.

## 4. Our solution

The proposed technique utilises CDMA to push any sensitive data transmissions which may normally be below $f_{cut}$ well above it, rendering them unresolvable. Our technique has multiple benefits over other possible schemes including small silicon footprint, error detection/correction and, most importantly, no requirement for the input and output circuits to be altered in any manner. The system presents a standard parallel bus interface and transparently converts the link to a serial one employing CDMA. The line frequency is thus pushed above $f_{cut}$. As we perform serial-to-parallel conversion, the "data clock" signal presented in Figure 4 will actually be the clock of a shift register running at rate $d{\cdot}f$, where $d$ is the width of a data word. The chipping clock therefore runs at $m{\cdot}d{\cdot}f$. Since the output code obeys the average of one '1' to every one '0', every input data bit integrates to ½ over all ten chips — data values are masked by smoothing effect of a probe.

Markettos provides the value of $f_{cut}$ for the best probe he found: 760MHz. Since impedance $Z = 2\pi fL + 1/2\pi fC + R$ and the $L$ term dominates at high $f$ we can see that, for a 4kΩ scope input, a ten times increase in $f$ translates to a tenfold decrease in signal magnitude. This gives a similar increase in allowable interconnect current whilst still maintaining a comparable signal level. Equivalently, we can say that this will indicate how much more expensive an attacker's equipment will need to be to still succeed. If neither alteration can be made, we have reduced the EM emissions to negligible levels.

There are two major factors remaining in order to complete the specification of the system: the first is how to generate the pn sequence, which will be addressed by LFSRs; the second is how to synchronise the states of the encoder and decoder, which is ongoing research not addressed here.

## 5. LFSRs

There are many different algorithms that generate pn sequences ranging in complexity and perceived security, but the rule of thumb is that the more secure the algorithm then the larger its silicon footprint. Since CDMA may need to be implemented on many sensitive interconnect lines, we want the smallest possible footprint. This is provided by a Linear Feedback Shift Register (LFSR) in a so-called *m-sequence* configuration [2]. This produces a stream of $2^n$-1 pn bits at the expense of only $n$ flip-flops and a handful of XOR gates. We can also choose an arbitrary starting point in the sequence via a secret key. This makes it harder for an attacker to guess its current state. This makes it ideal for our situation. An 8-bit example is illustrated in Figure 3.
Our interconnect system then uses an m-LFSR to produce a pn sequence for use with CDMA.

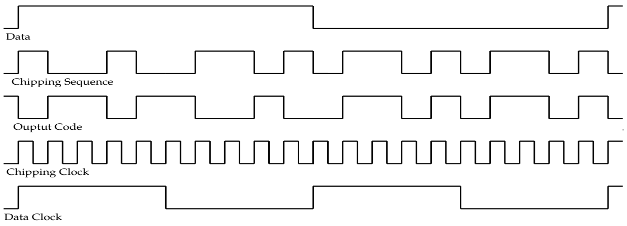

**Figure 4: Chips are XORed with the data, yielding the code**

## 6. Conclusions

We have presented a method of securing an arbitrary link from EMA using CDMA to transform the frequency spectrum into one that is undetectable by existing probe-scope combinations. As chips get faster, this will become easier to implement, whilst physical constraints on probes will remain in place. Therefore, the system should increase in utility.

[1] Peter Hofreiter and Peter Laackmann. Electromagnetic Espionage From Smart Cards – Attacks and Countermeasures. Technical report, Infineon Technologies AG.

[2] Bruce Schneier, *Applied Cryptography*. Wiley, 1996.

[3] Ross Anderson and Markus Kuhn. Tamper resistance: A cautionary note. In *2nd USENIX Workshop on Electronic Commerce Proceedings*, Nov 1996.

[4] A.T. Markettos and S. Moore. Electromagnetic Analysis of Synchronous and Asynchronous Circuits using Hard Disc Heads. In *16th UK Asynchronous Forum Proceedings*. September 2004. *http://www.cl.cam.ac.uk/~atm26/*