Security Evaluation Against Electromagnetic Analysis at Design Time

Huiyun Li, A. Theodore Markettos, Simon Moore

University of Cambridge

Outline

- Motivation
- Simulation methodology for EMA
  - System partitioning
  - Simulation flow
  - Types of EM emissions
  - EMA measurement equipment
- Results
- Conclusion

Motivation – side channel attacks

ISO Interface

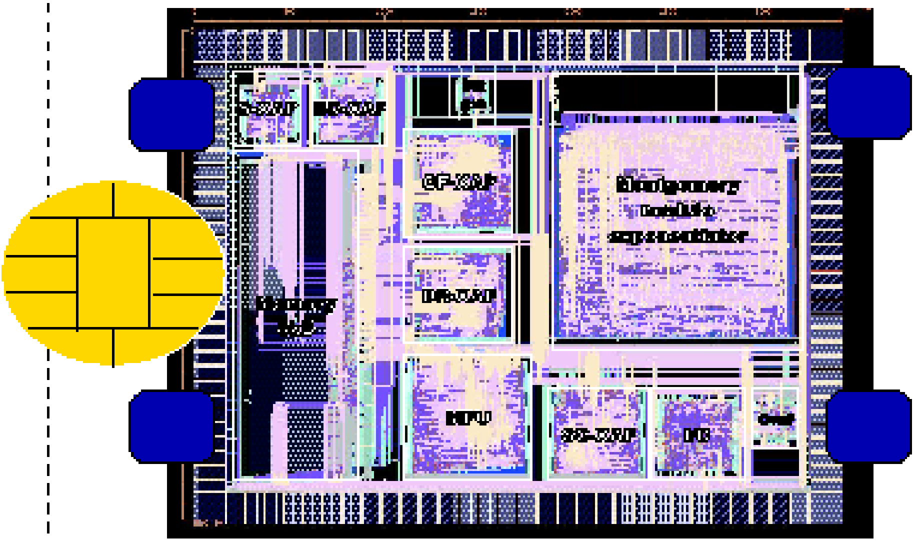
Chip Surface

1

Timing of computation

2

Power consumption



Electromagnetic radiation

3

Motivation

Post-manufacture test:

- Time consuming
- Error prone
- Expensive
- So that has driven the study of design-time security evaluation

EM Simulator

- EM Simulation -- Solve Maxwell’s Equations for simulating wave propagation
  - Pro: accurate
  - Con: computationally complex, time-consuming

EMA measurement equipment

- Near-field $(r < \lambda / 2\pi)$ electric field sensors

$$E \propto I$$

- Near-field magnetic field sensors

$$B \propto I$$

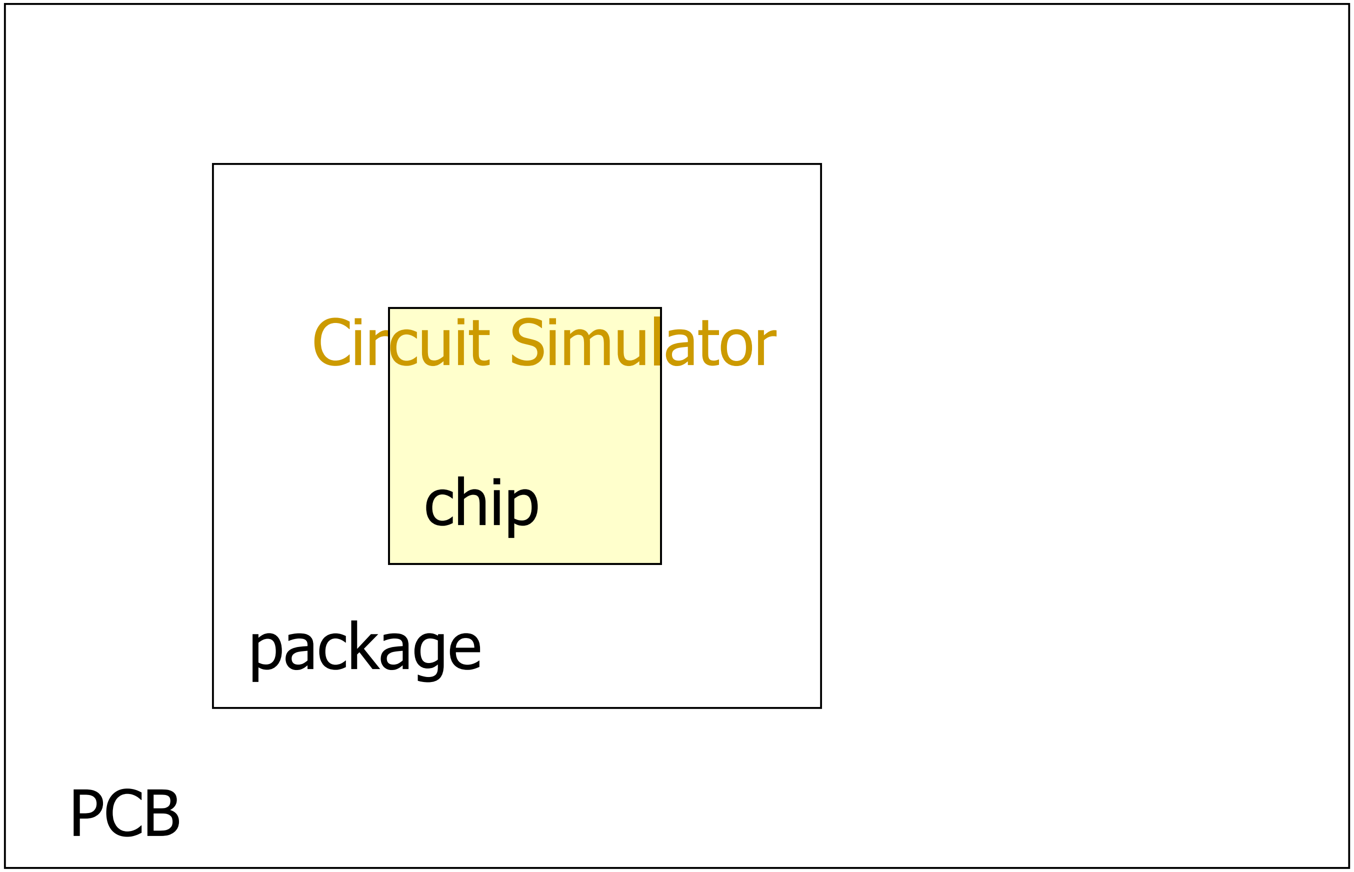
- Far-field $(r > \lambda / 2\pi)$ electromagnetic field sensors

$$emf \propto I$$

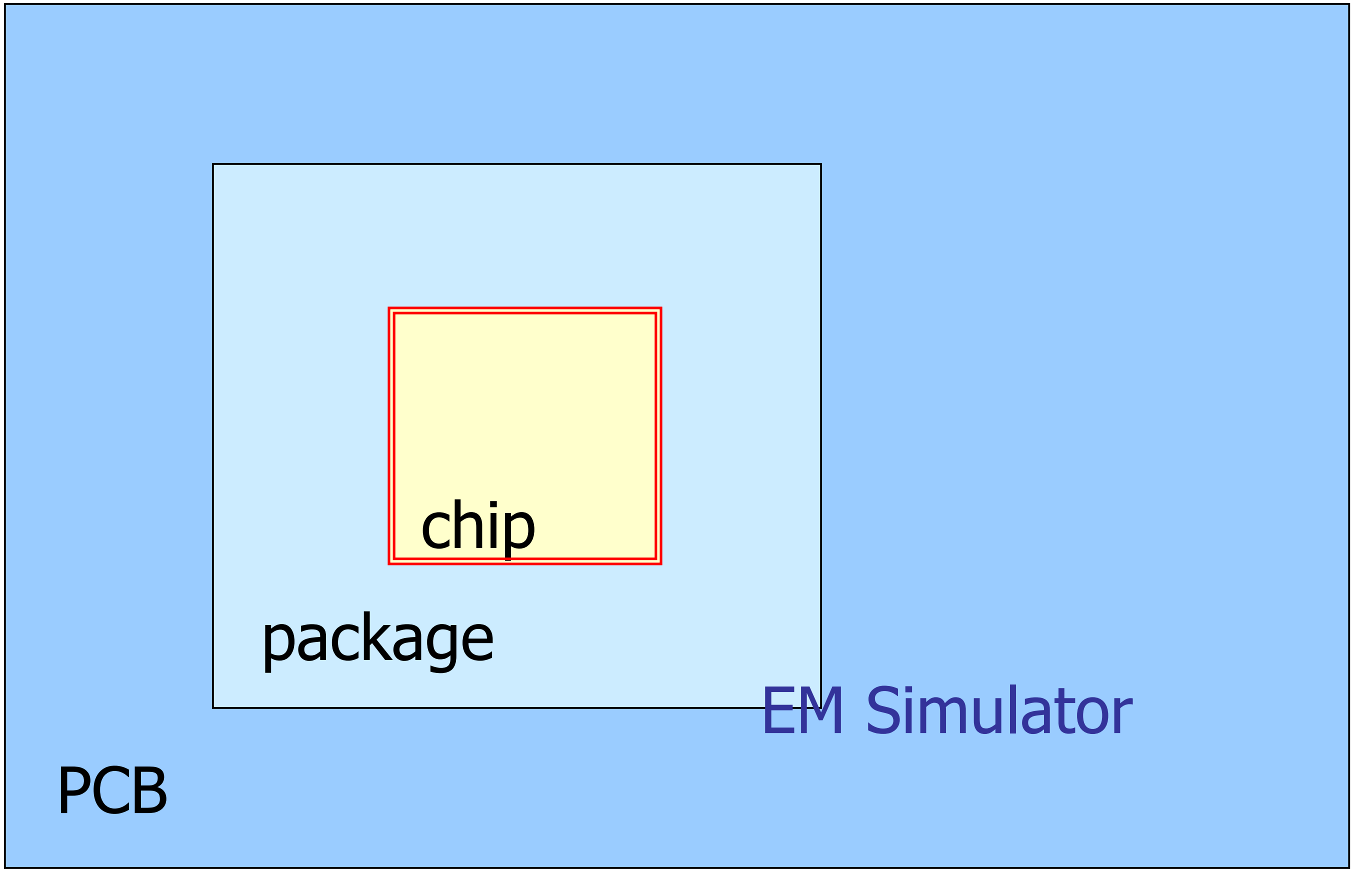
Circuit Simulator

- Circuit Simulation – solve for V & I according to Kirchhoff's voltage and current laws
  - Pro: fast
  - Con: accuracy limited by the accuracy of lumped element models; validity limited by range of frequencies, geometries etc

System partitioning



System partitioning



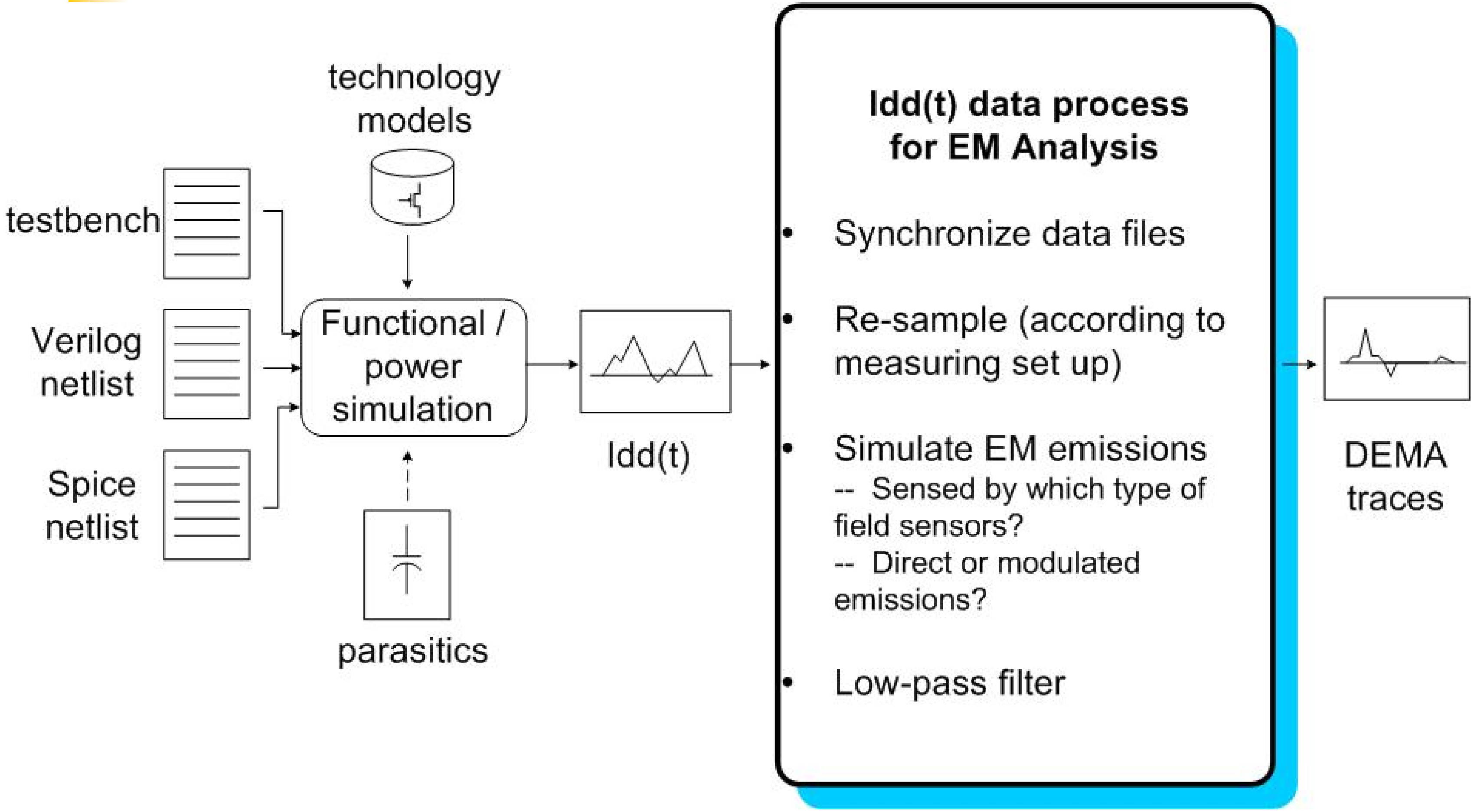
chip

package

EM Simulator

PCB

EM analysis simulation procedure



technology models

testbench

Verilog netlist

Spice netlist

Functional / power simulation

parasitics

Idd(t)

Idd(t) data process for EM Analysis

- Synchronize data files
- Re-sample (according to measuring set up)
- Simulate EM emissions
  -- Sensed by which type of field sensors?
  -- Direct or modulated emissions?
- Low-pass filter

DEMA traces

EMA measurement equipment

- Near-field $(r < \lambda / 2\pi)$ electric field sensors

$$E \propto I$$

- Near-field magnetic field sensors

$$B \propto I \qquad V \propto \frac{dB}{dt} \propto \frac{dI}{dt}$$

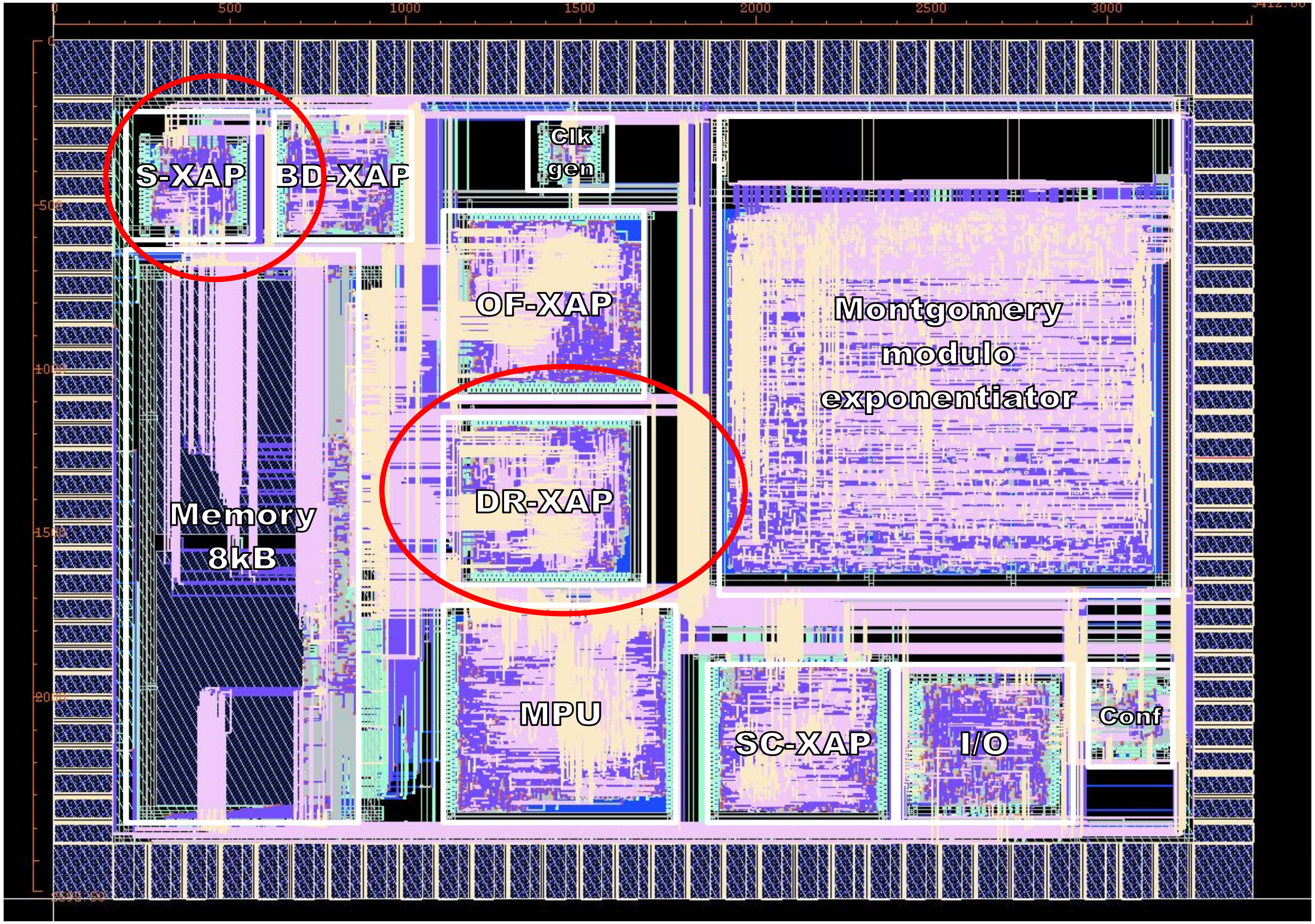
- Far-field $(r > \lambda / 2\pi)$ electromagnetic field sensors

$$emf \propto I$$

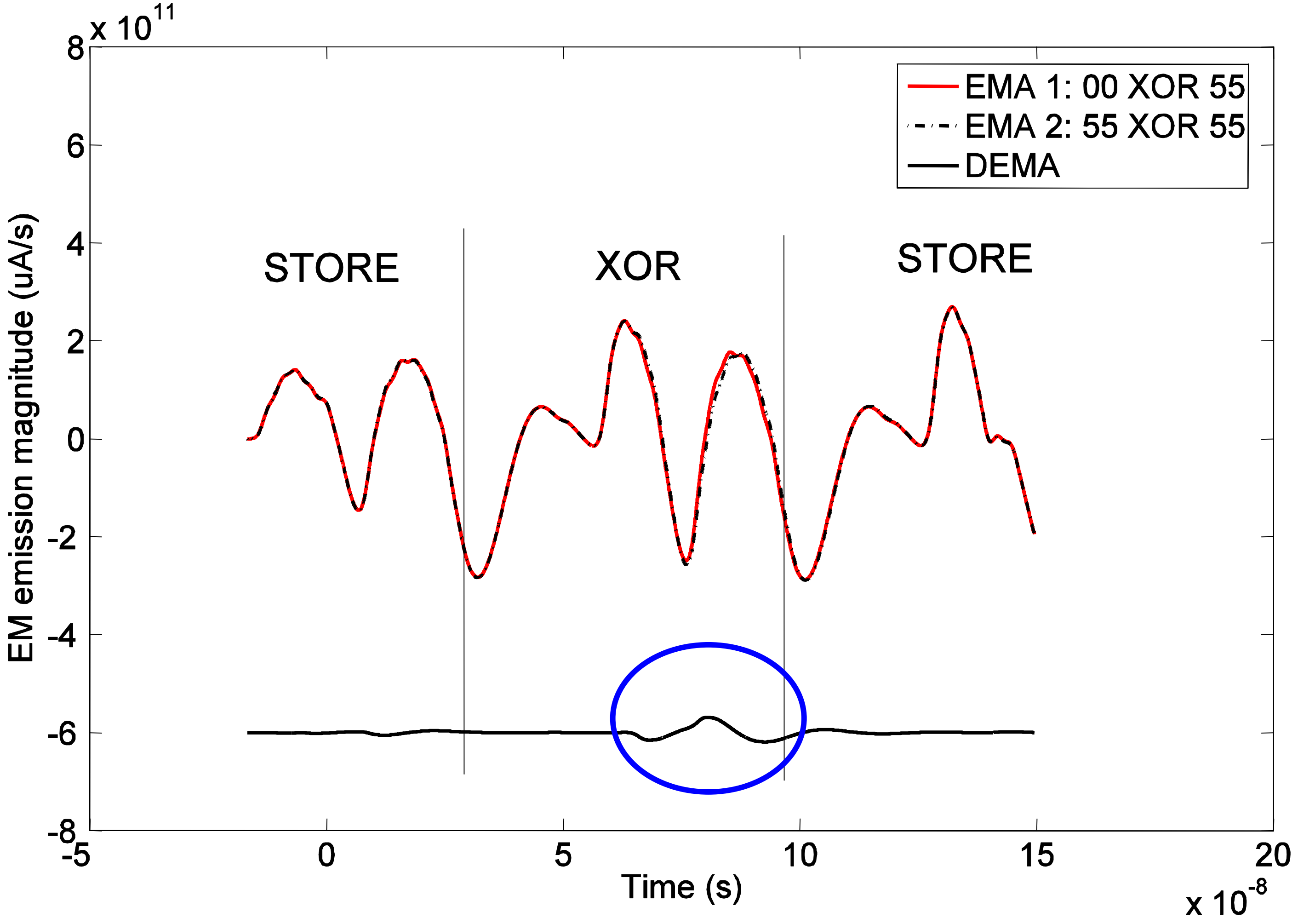
Types of EM emissions

- Direct Emissions
- Modulated Emissions
  - Amplitude Modulation
  - Angle Modulation (phase or frequency)

Simulation setup – Springbank test chip

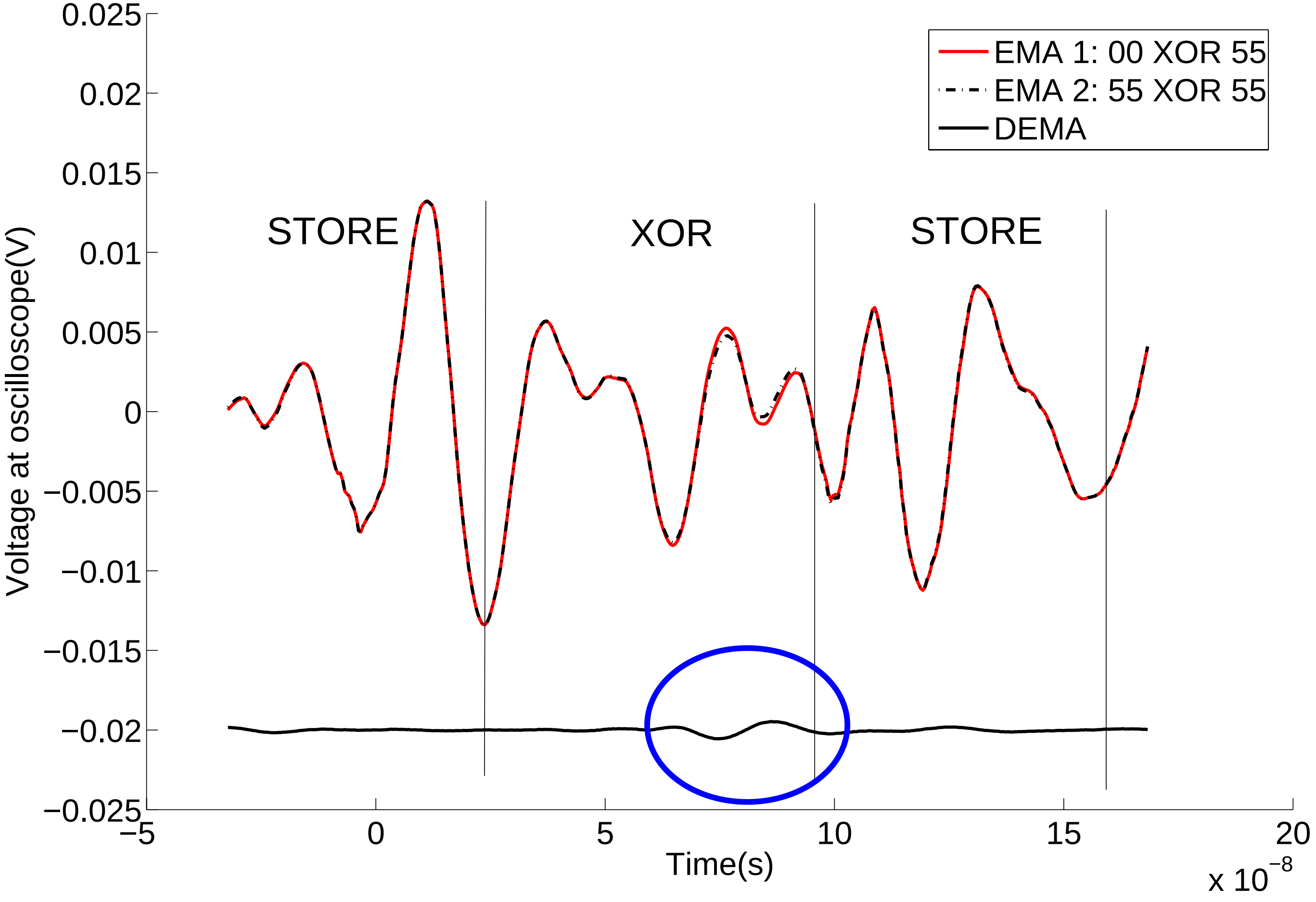


Simulation results
-- synchronous XAP processor
-- inductive sensor

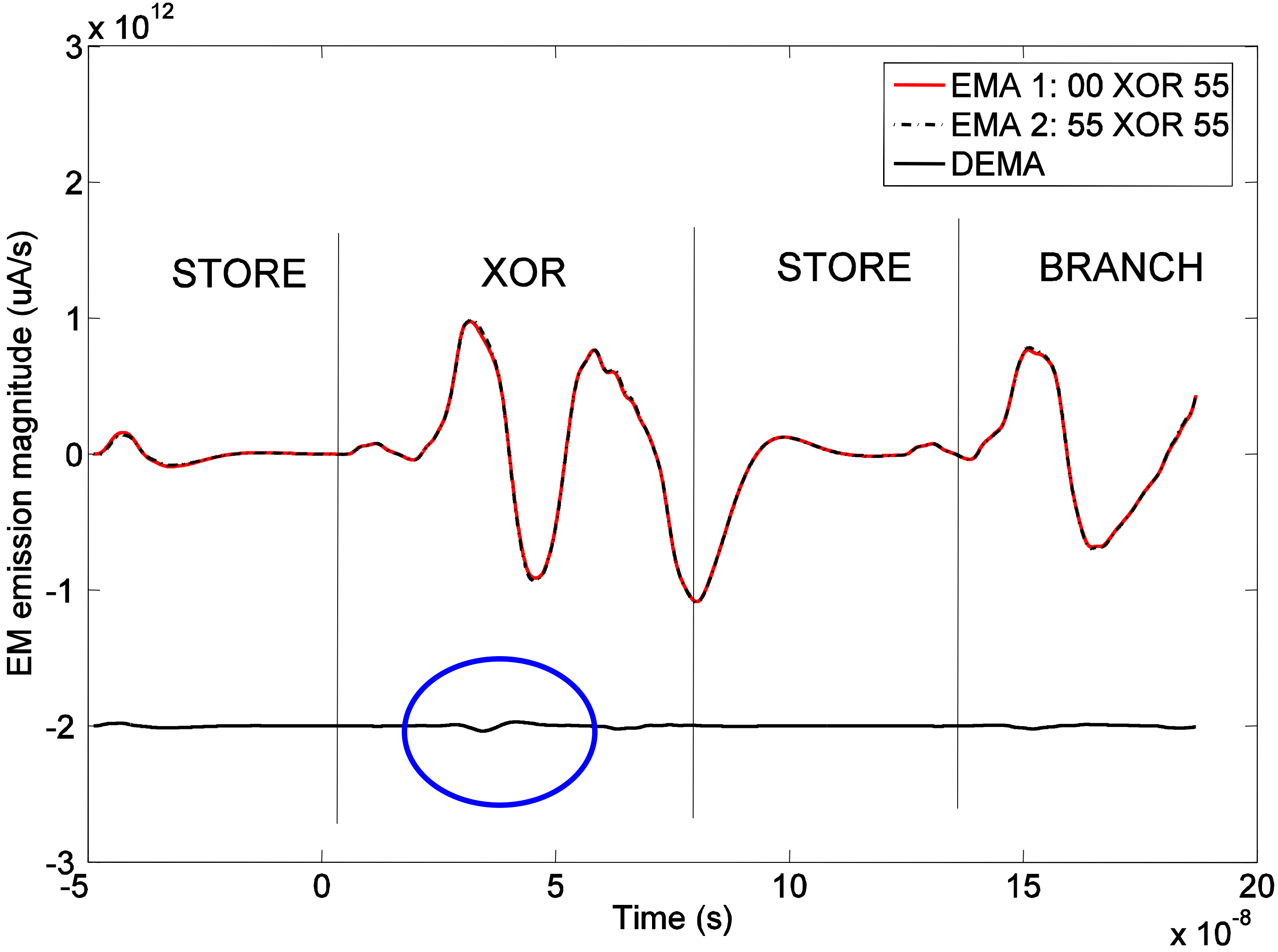


EM measurement results

-- synchronous XAP processor
-- inductive sensor

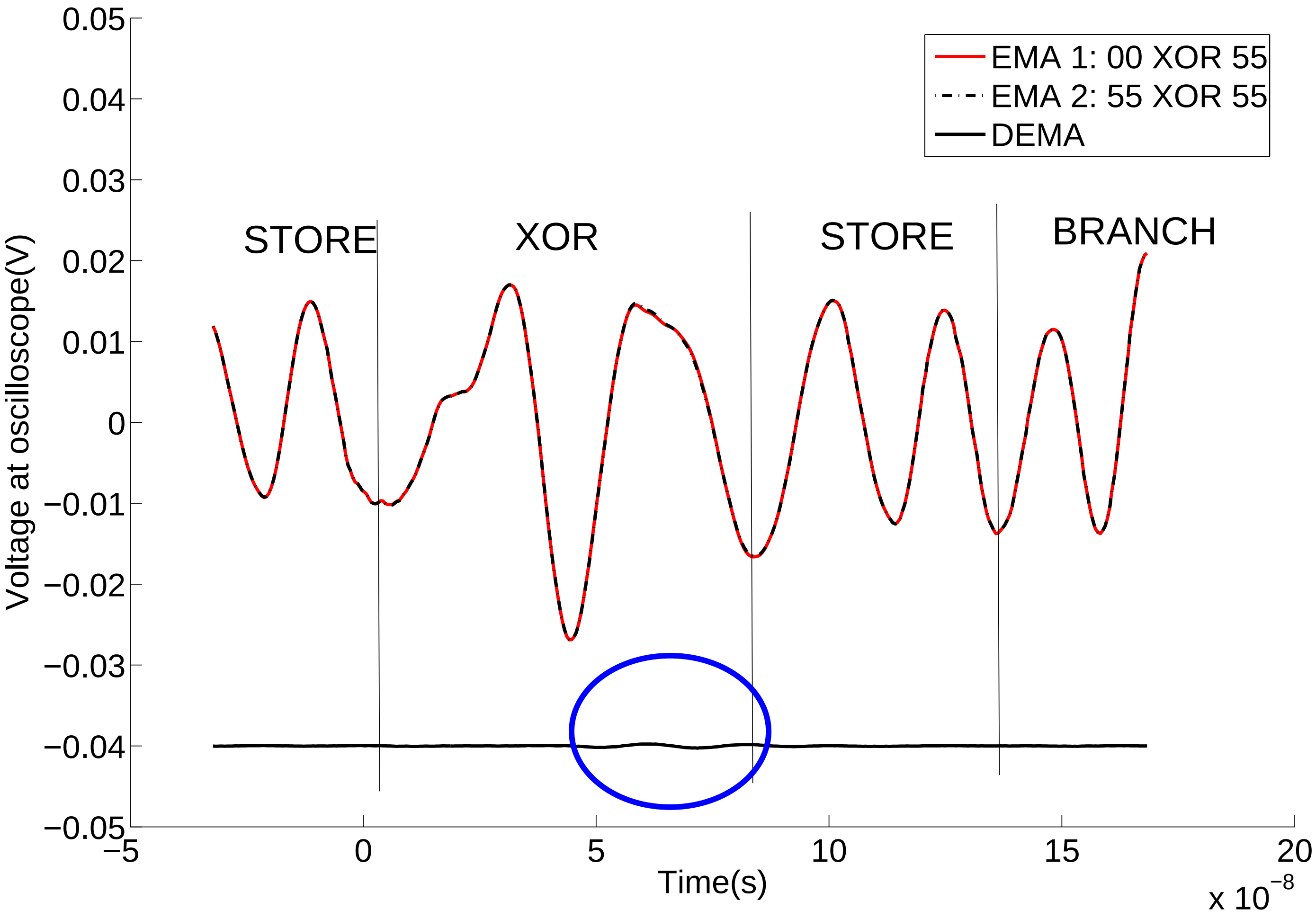


Simulation results
-- dual-rail asynchronous XAP processor
-- inductive sensor



EM measurement results

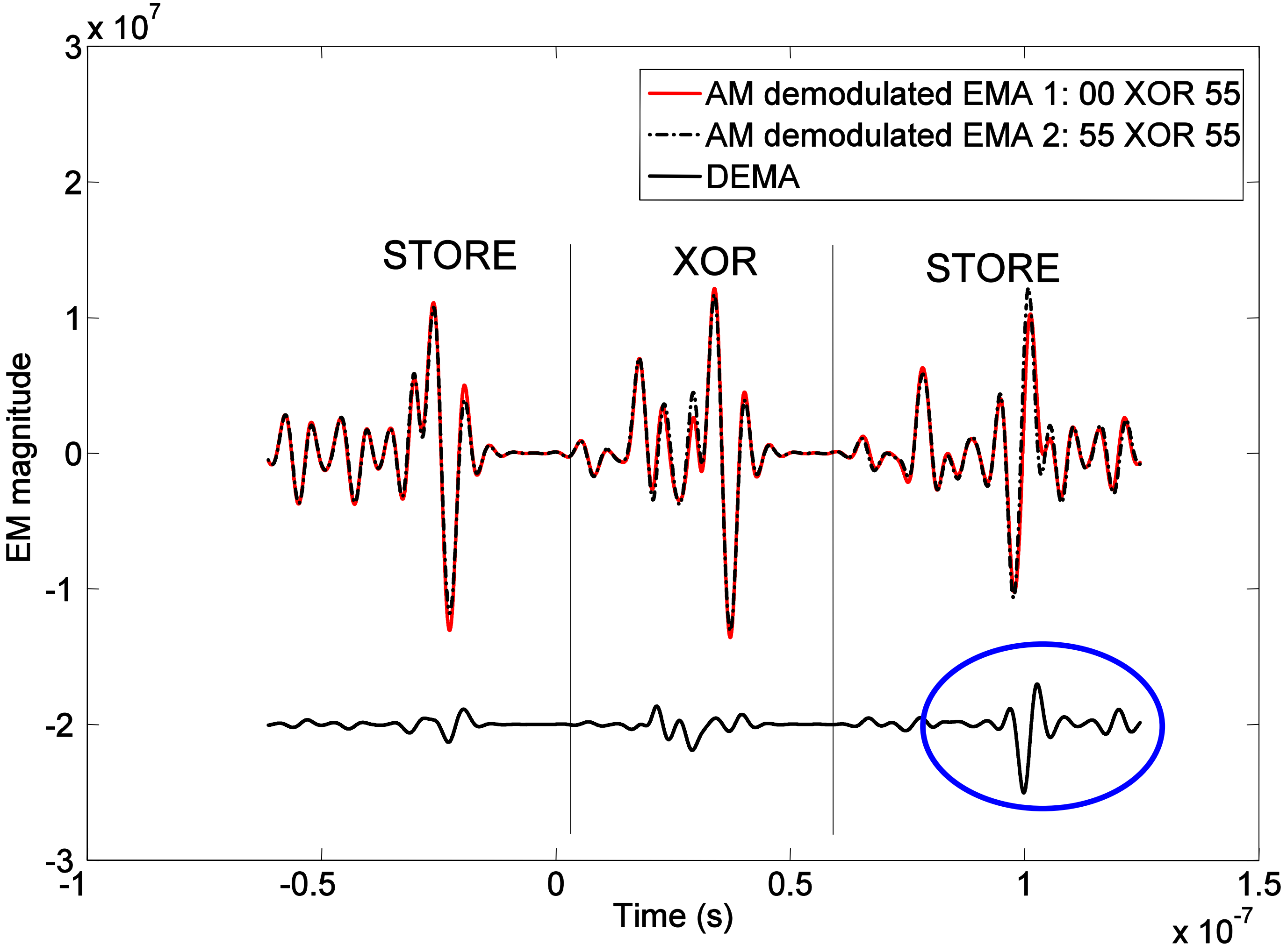
-- dual-rail asynchronous XAP processor
-- inductive sensor



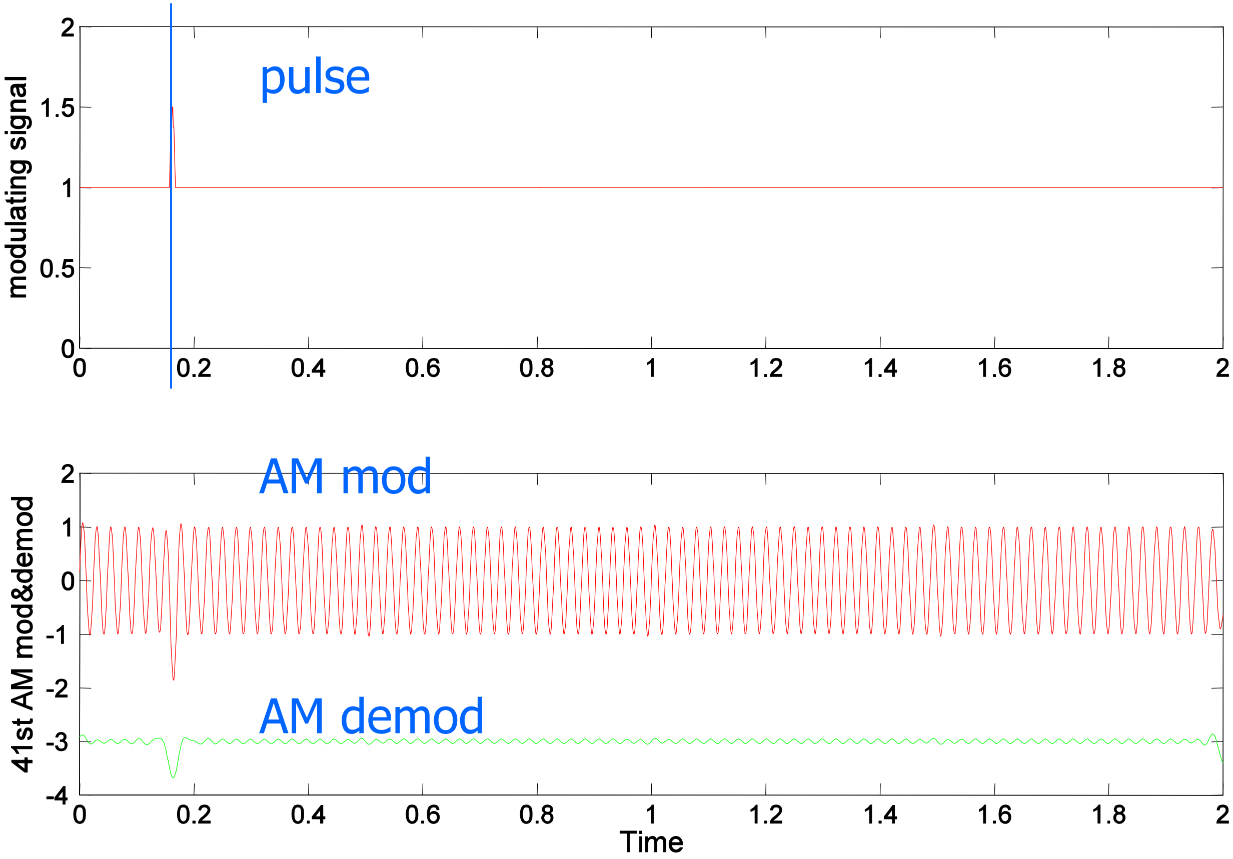
Simulation results

-- dual-rail asynchronous XAP processor

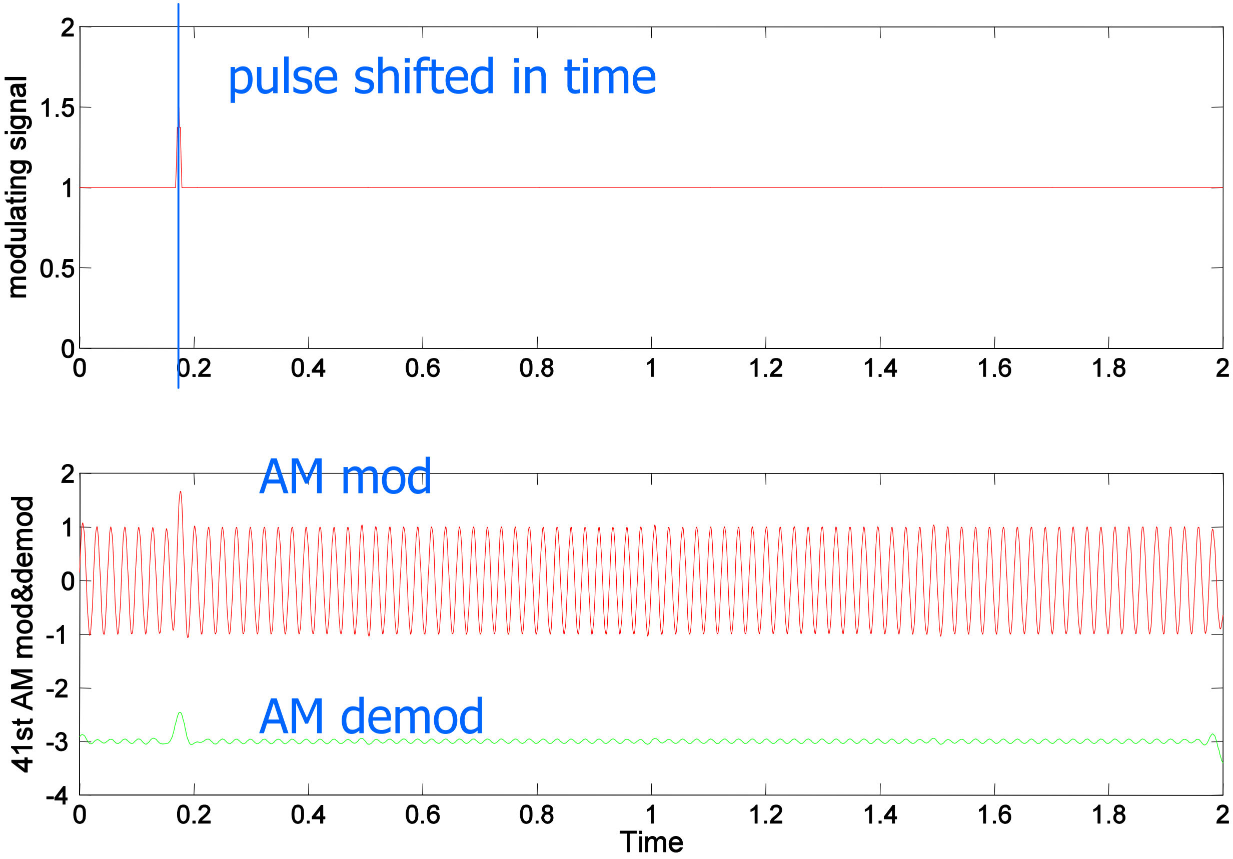
-- inductive sensor – modulated emission



How time shift affects AM modulation and demodulation



How time shift affects AM modulation and demodulation



Conclusion

- A simulation methodology for EMA has been proposed
  - EM simulator for modelling Package and PCB
  - Circuit simulator for simulating EMA of chip+ package +PCB
  - Data processing for EM analysis according to
    - sensor types (ouput $\propto$ di/dt or $\propto$ i)
    - EM emission types (direct or modulated)

Conclusion cont.

- The results also indicates that
  - The synchronous processor under test has data dependent EM emissions
  - The asynchronous processor under test has less data dependent EM emissions in direct EMA test, but demonstrated more data dependent EM emissions in modulated EMA test

Thank You!