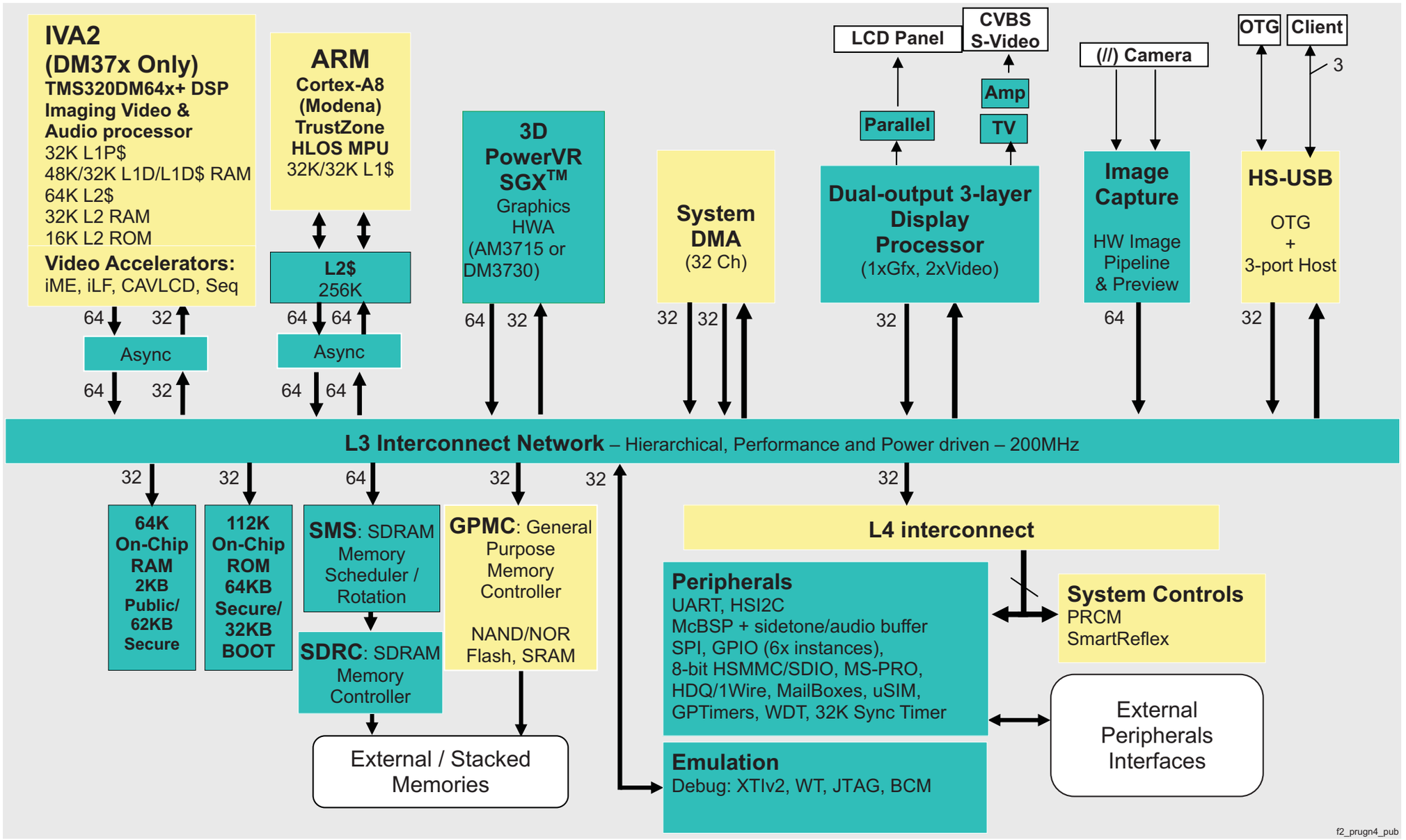
Understanding Leaks in SoC devices

Dr. Marios Omar Choudary

Facultatea de Automatică și Calculatoare

4 iulie 2018

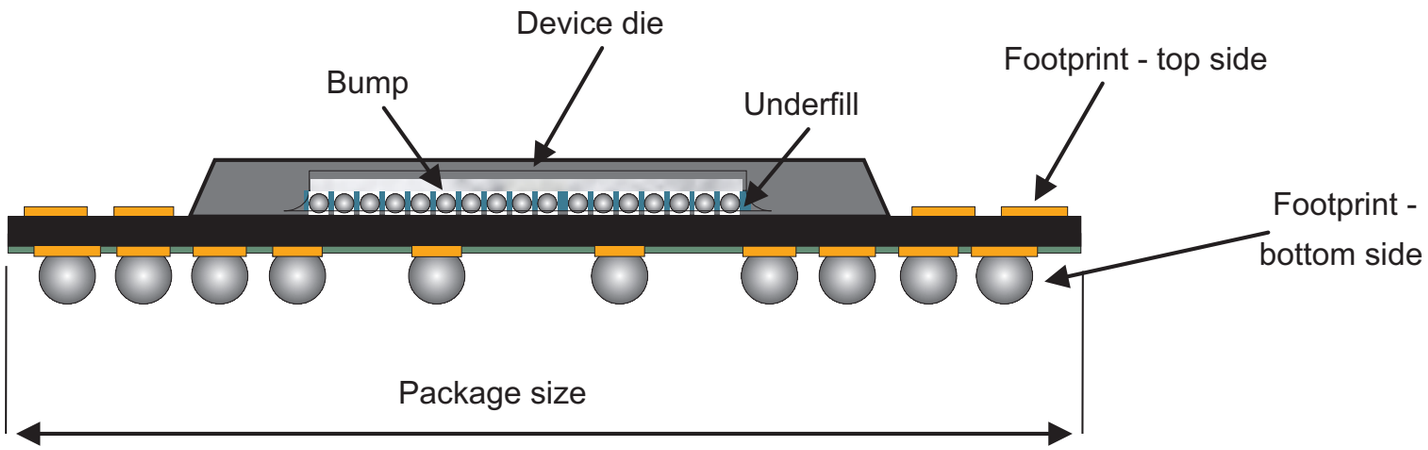
Inside a System on Chip (SoC)



Beagleboard - TI DM37x

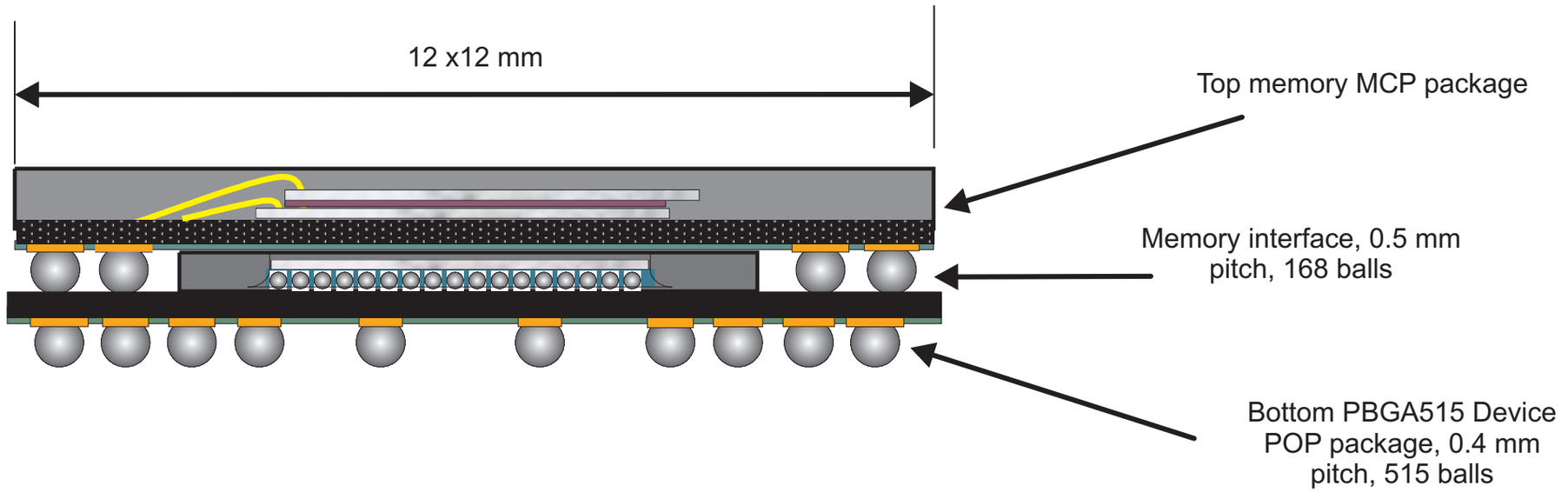
Inside a System on Chip (SoC)

Figure 1-3. POP Concept (CBP Package)



108-003

Figure 1-4. Stacked Memory Package on the POP Device (CBP Package)

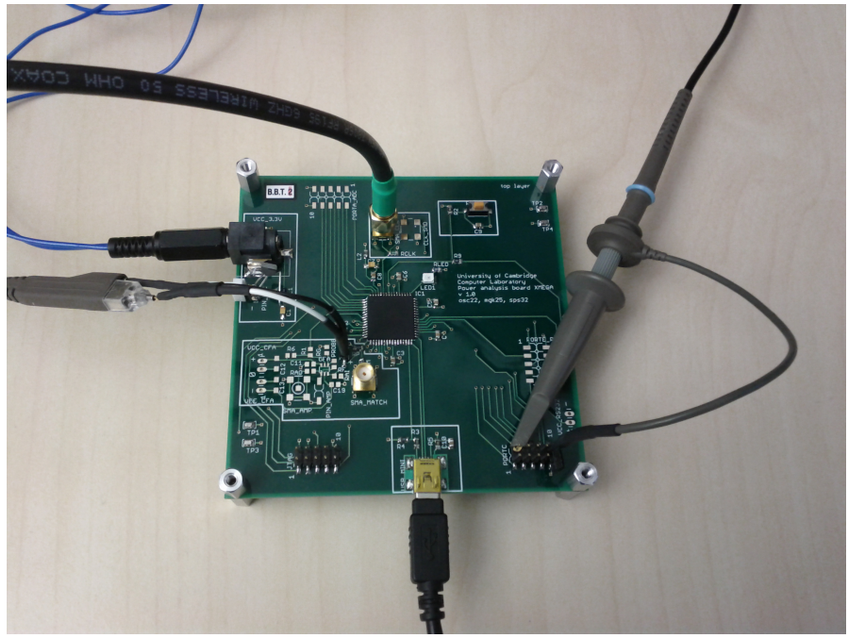


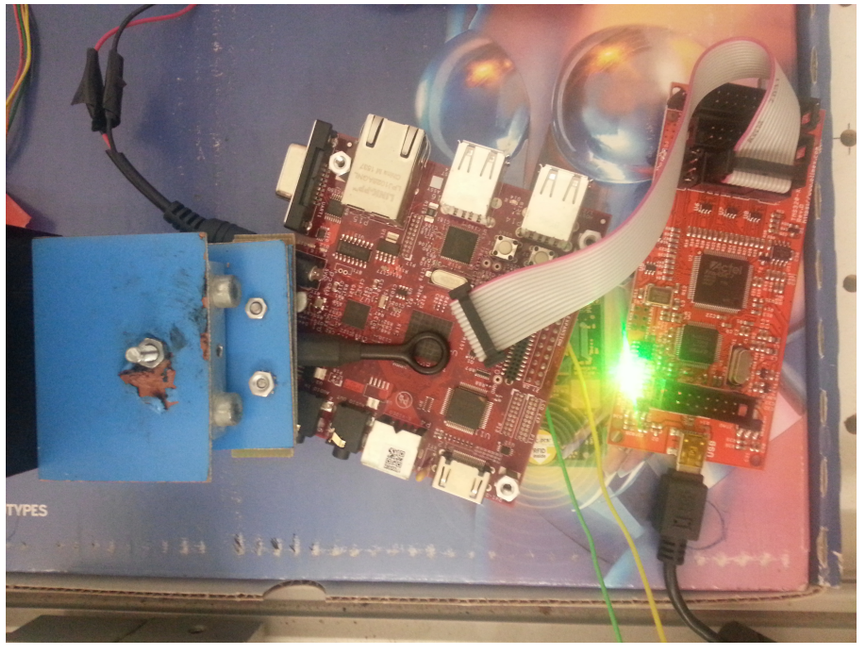
Beagleboard - TI DM37x

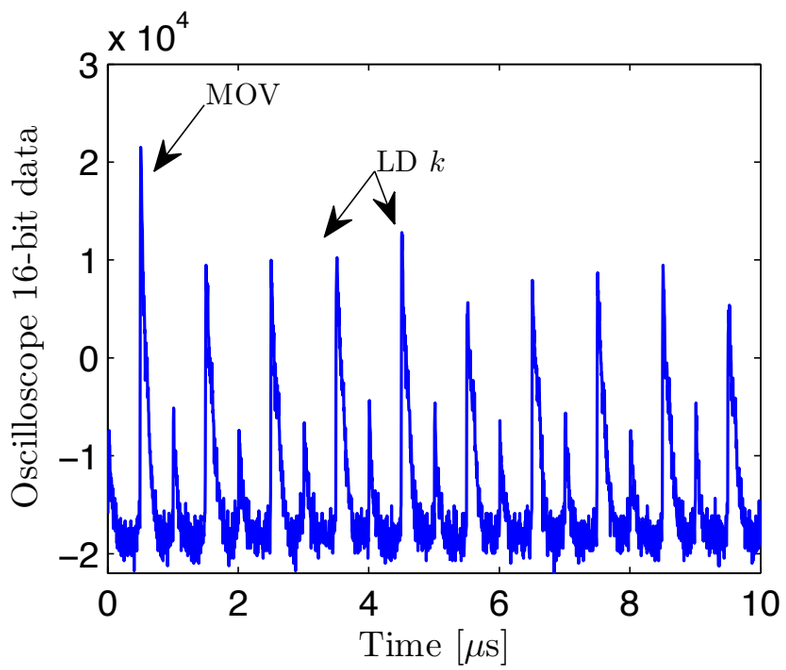
De ce este analiza side-channel pe SoC interesantă:

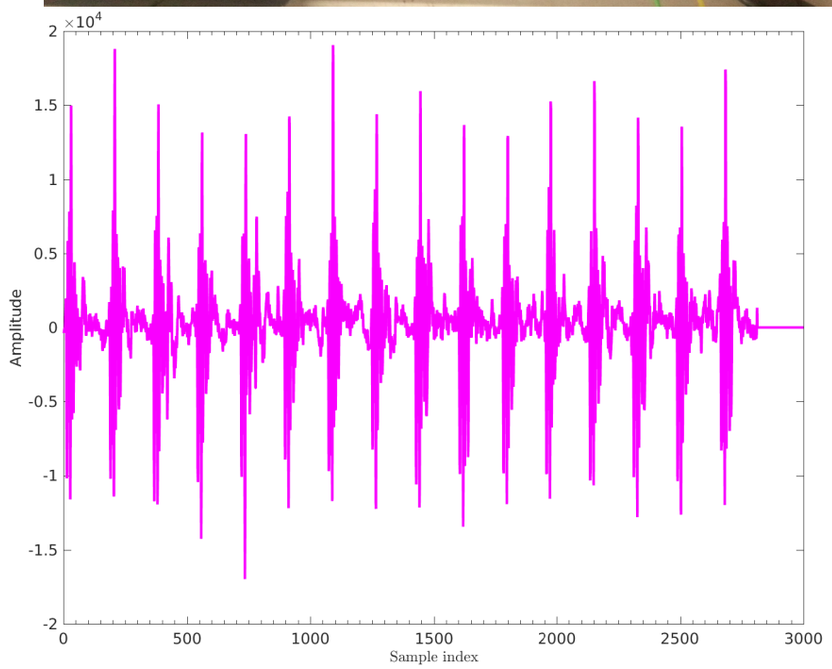
- Nu prea s-a făcut până acum
  - Primul studiu serios la CHES 2015 (Longo et al.)
- Multe probleme de rezolvat pentru un atac (analiza) eficient
  - Zgomot mare (multe componente care interacționează simultan)
  - Deep pipeline (ARM are de obicei 11-stage pipeline)
  - Greu de obținut informația side-channel: PBGA mount,Package-on-Package
  - Data bus foarte mare (32 - 128 bit width)

Microcontroller vs SoC side-channel analysis

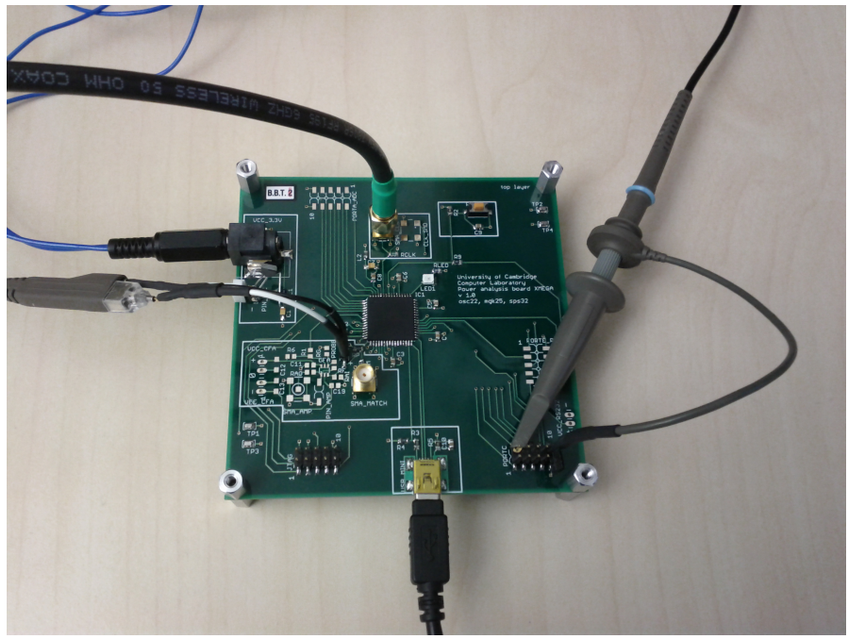


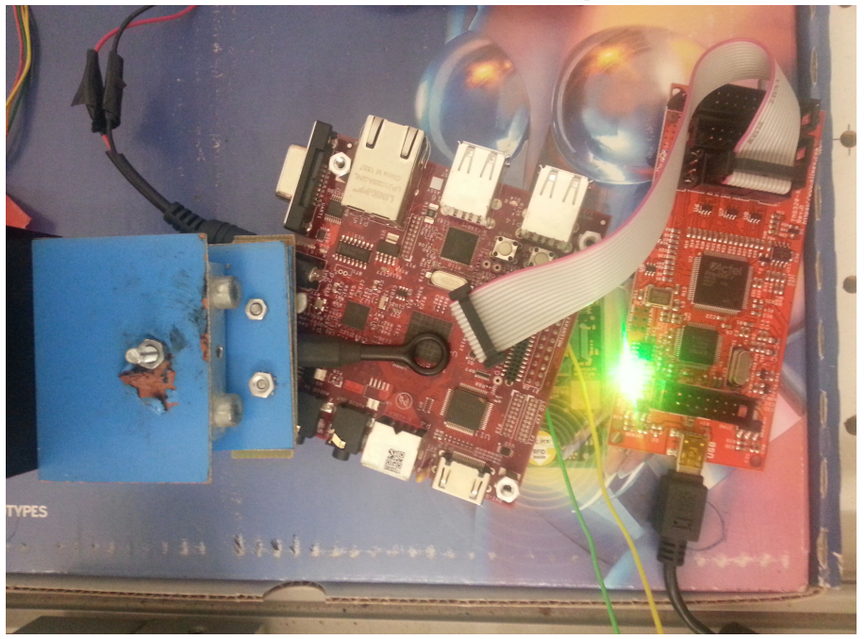


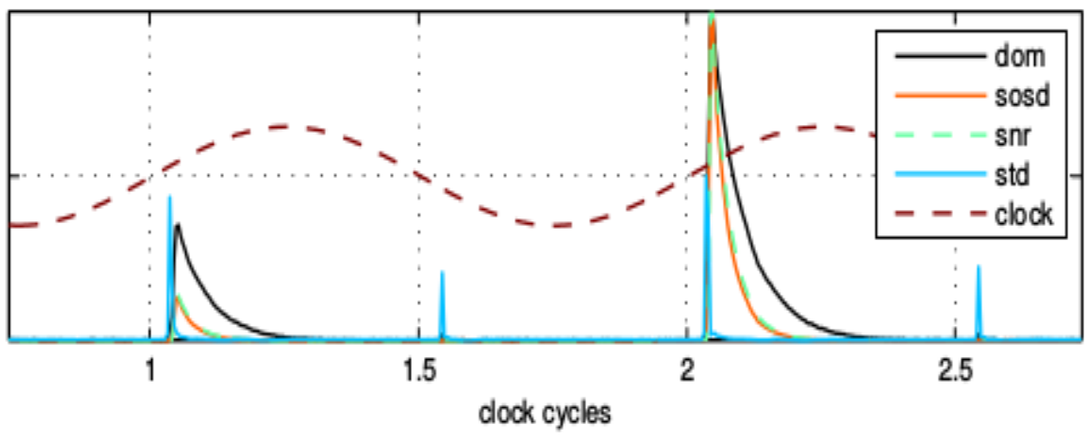


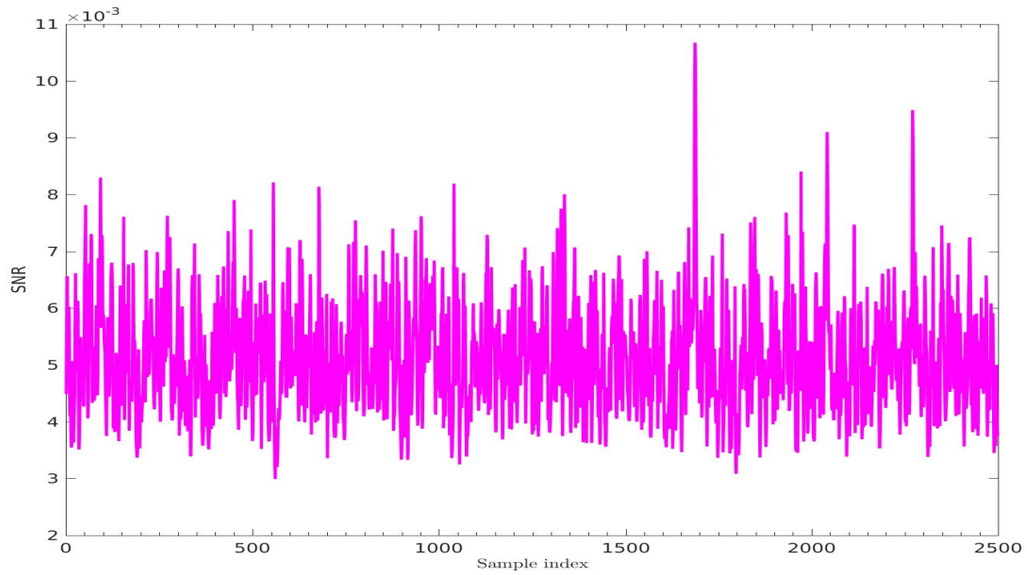


Microcontroller vs SoC side-channel analysis









Scopul proiectului

- Uînțelegerea leakage-ului din SoC
  - Modelarea a leakage-ului prin Template Attacks, Stochastic Models pentru diverse componente: ARM/Neon CPU, crypto co-processor, memorii (RAM, Cache), data bus, pipeline
- Metode de evaluare de securitate eficiente pentru SoC
  - Probleme mare cu bus-ul pe 32, 64 sau 128 biți
- Implementări criptografice resiztente la side-channel attacks
  - Folosindu-ne de analiza din pașii precedenți și folosind componentele cu leakage minim

Contact

Marios Omar Choudary

Marios.choudary@cs.pub.ro

http://www.cl.cam.ac.uk/~osc22

Notă: suntem deschiși la primirea de finanțări ☺