Microelectronics System Design

Leader: Prof. Alex Yakovlev

(http://async.org.uk, http://www.ncl.ac.uk/eee/research/groups/micro)

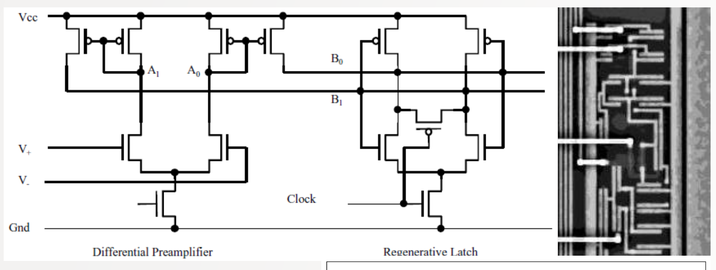
Newcastle University

School of *Electrical and Electronic Engineering*

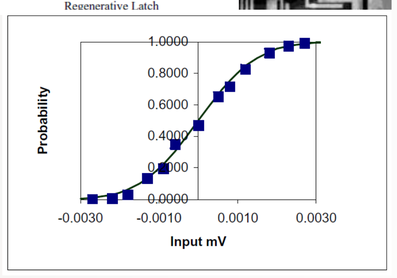
Security on-chip

- Security for chips is a vital issue for many applications
- Asynchronous techniques are relevant in many ways in chip security. For instance, dual-rail logic has a natural advantage when it comes to masking the power signatures of data, and such asynchronous artefacts as metastability may be used to make simple and low-cost true random number generators on chip.

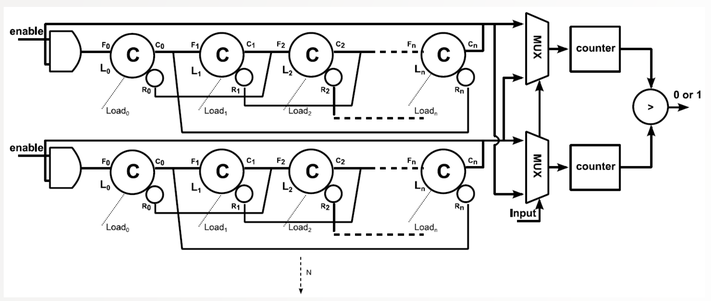
Random numbers from metastability



It is possible to use the internal noise of a bistable device in metastability to generate a stream of bits with a high level of randomness, and a frequency of over 100MHz.



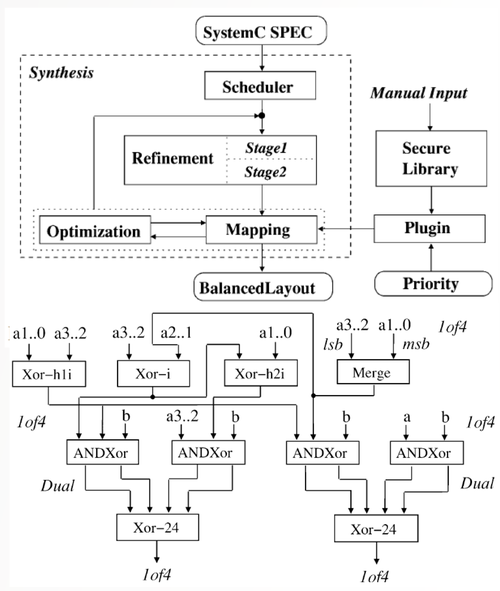
Self-timed physically unclonable functions



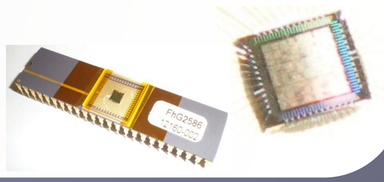
PUFs are most frequently used for device authentication. The use of self-timed logic addresses some of the inherent issues in PUFs providing a new level of robustness, entropy and size. This leads to increased resistance to modelling attacks and make real-life efficient designs feasible. This work is a recent collaboration with the **Centre for Secure Information Technologies, QUB**, as is our joint research proposal on variability-driven self-timed security.

Security with balanced 1-of-n circuits

- New design flow using 1-of-n encoding provides more efficient power-balanced circuits than can be provided by dual-rail alone.
- New library of optimized power-balanced cells uses N-nary 1-of-n logic improves over dual-rail.



SURE Galois Encoded Logic AES-128 IP core



Sponsors, partners and collaborators

School of **CS** and Institute of **Neuroscience**, NU

ARM, Moortec semiconductor, ORACLE, intel, Atmel, MBDA MISSILE SYSTEMS, Imagination, CEA Leti, imec, Texas Instruments, TU/e, University of Bristol, Berkeley University of California, UPC, Politecnico di Torino, Manchester 1824 The University of Manchester, Imperial College London, MIT, EPSRC Pioneering research and skills, University of Southampton

Our Mission

MSD Newcastle is dedicated to timely innovations in design technology for computational systems and circuits in order to meet the current and future challenges facing the electronics industry. These include:

- Energy and power
- Complexity and difficulty of design
- Neural-silicon interfaces
- Variability
- Burdens of legacy
- On-chip security

MSD Newcastle is one of the **main research groups** in the School of EEE:

- 7 academic staff
- 7 research staff
- 25+ research students

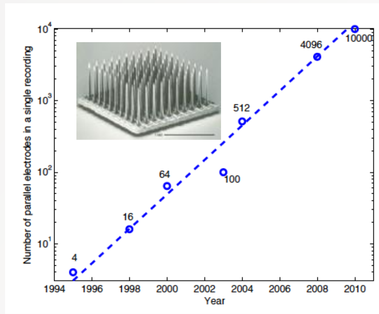
Our **expertise**:

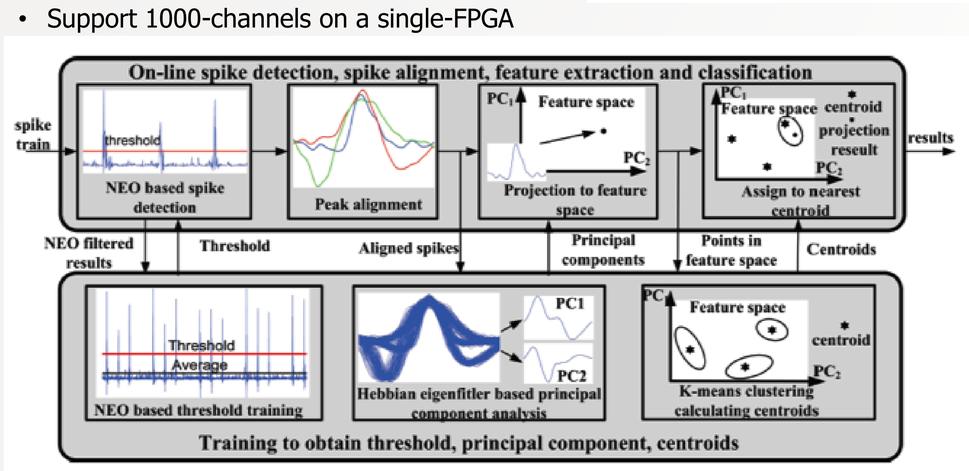
- Chip design
- FPGA prototyping
- Design automation

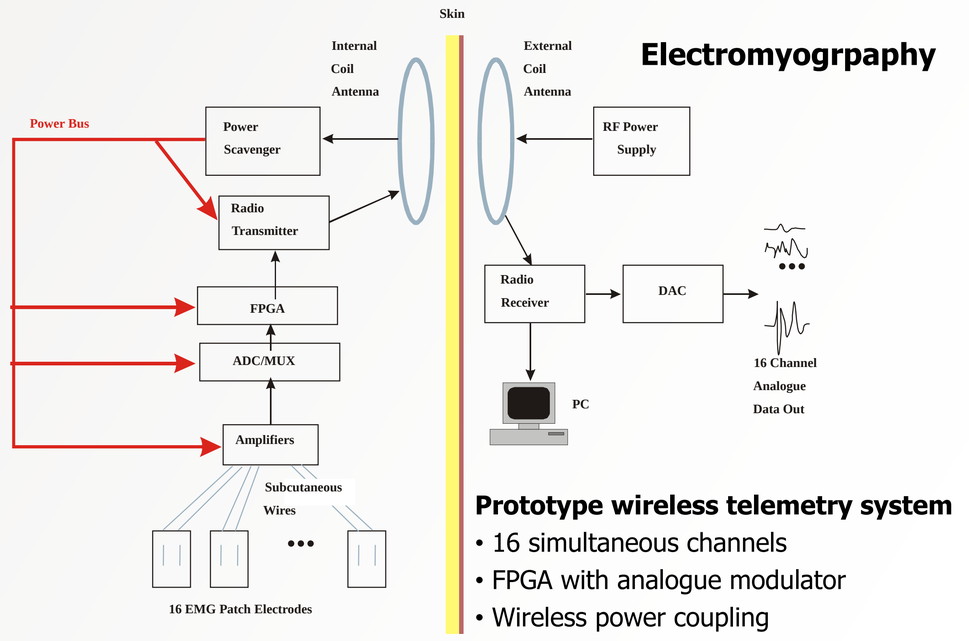
Neuro-silicon interface and wireless telemetry system for neuroscience research

BMI (Brain-Machine interface)

- Emerging technologies
  - Microelectrode array, e.g. 10K channels
- Stroke rehabilitation, bionic arm
- Real-time spike processing, spike detection, sorting and decoding
- 33x acceleration comparing to software
- 40x power improvements to classical PCAs
- Support 1000-channels on a single-FPGA







Electromyogrpaphy

Prototype wireless telemetry system

- 16 simultaneous channels
- FPGA with analogue modulator
- Wireless power coupling
- Silicone encapsulated for implantation

Energy Proportionality

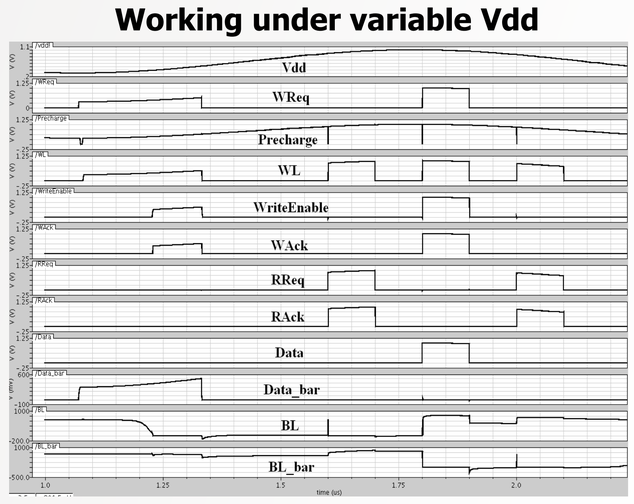
- Energy-harvesting changes the dynamic balance between supply and consumption – supply add operational constraints in real-time
- Adaptation to power changes should be at all levels of abstraction, from logic cells to systems
- Asynchronous (self-timed) techniques support more effective adaptation to Vdd changes via natural temporal robustness; they also offer better energy proportionality
- Good energy characterisation of loads (logic, memory, i/o, RF) is essential for high-quality adaptation
- More theory, models and algorithms are needed for handling the problem of power-adaptation in run-time

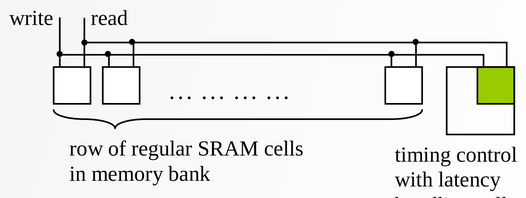
Memory subsystem working under variable Vdd

Non-deterministically variable Vdd is a characteristic of EH-powered systems. Computational electronics including memory subsystems must work under such an environmental assumption.

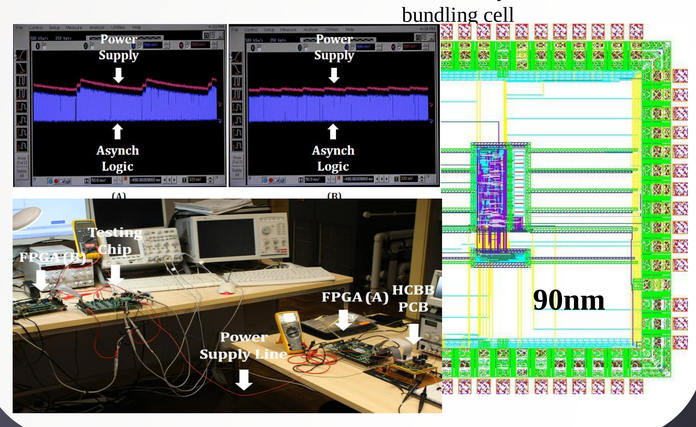
SRAM which can work under variable Vdd efficiently poses a number of challenges, best met with asynchronous technology. Full completion detection and acknowledgement for writing in SRAM was previously regarded as either impossible or impractical. In this project, we developed fully speed independent SRAM with completion detection for both reading and writing actions for the first time and demonstrated the efficiency of this method.

Working under variable Vdd





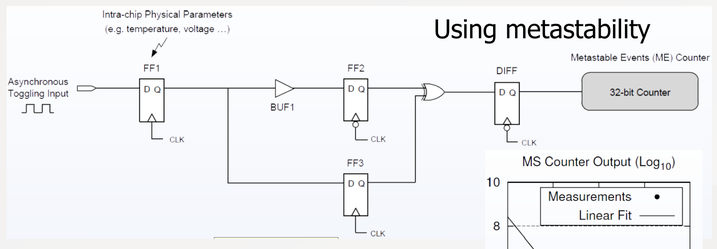
Time-bundled SRAM with fully SI cell as bundling unit

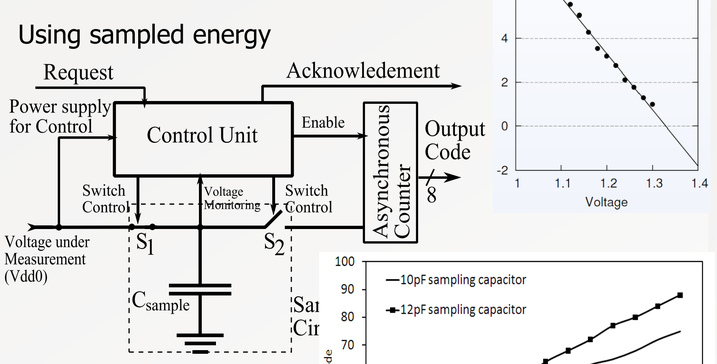


On-chip condition monitoring and sensing; On-chip communications (NoC, 2D and 3D)

On-chip reference-free voltage sensing

Voltage sensors which work under variable Vdd do not have access to reliable references.



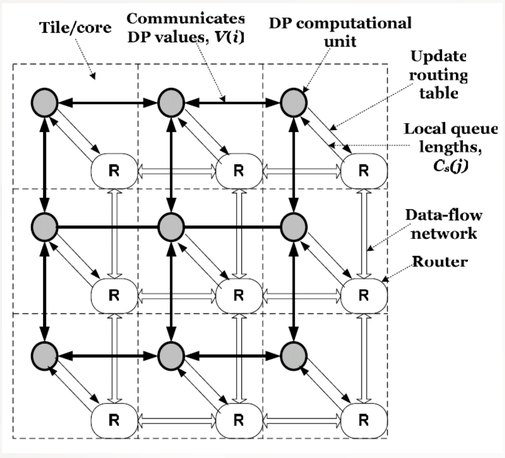


Other sensors and monitors

- Thresholds
- Temperature
- Time
- Deadlocks

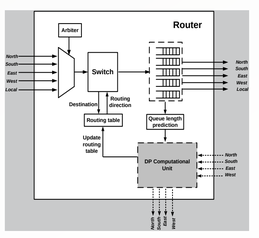
On-chip communications

Networks on chip, sending and receiving monitoring and control data, 3D, 2D.



Dynamic programming network for NoC

- A dual network approach
- Local queue length defines the cost in SP
- DP-net provides optimal decisions
- For online verification
- For traffic/power control



3D chip

- 150 nm 3D TSV process fabrication through **MIT-Lincoln Lab**
- Die: 1.5mm x 1.5mm x 3 layers