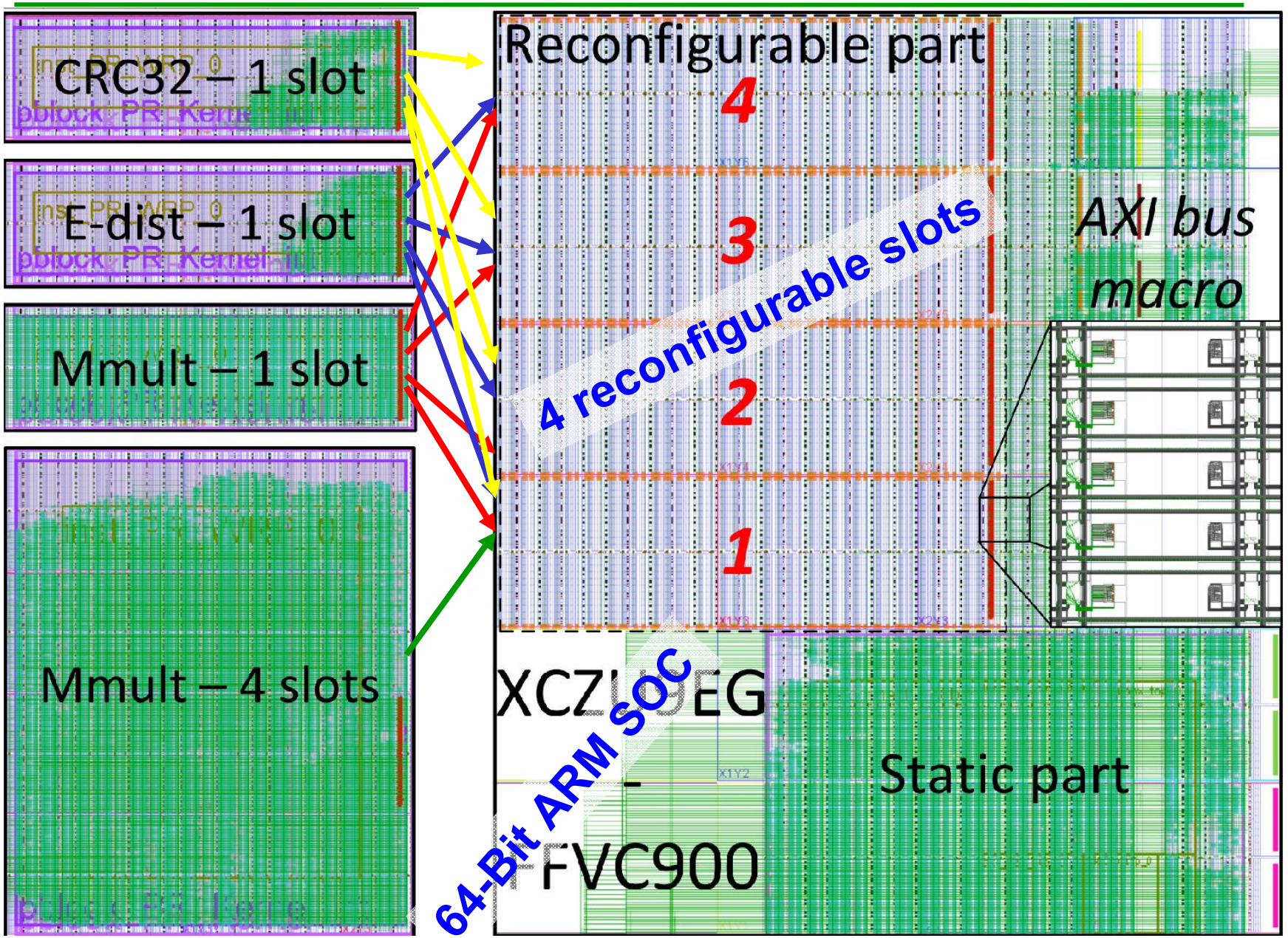
# rFAS
# –
# reconfigurable FPGA Accelerator Sandboxing


Dirk Koch, Khoa Pham (dirk.koch@manchester.ac.uk)
School of Computer Science
The University of Manchester

# Why FPGAs?

- **FPGAs are ideal for number crunching problems that fit dataflow processing model**
- **FPGA advantages**
  - **Customized processing**
  - **Optimized data movement**
  - **High integration (memory, mass storage, networking, acceleration and CPU)**
  - **Generic secure substrate (if once validated)**
  - **High performance at low power (from embedded to datacenters)**

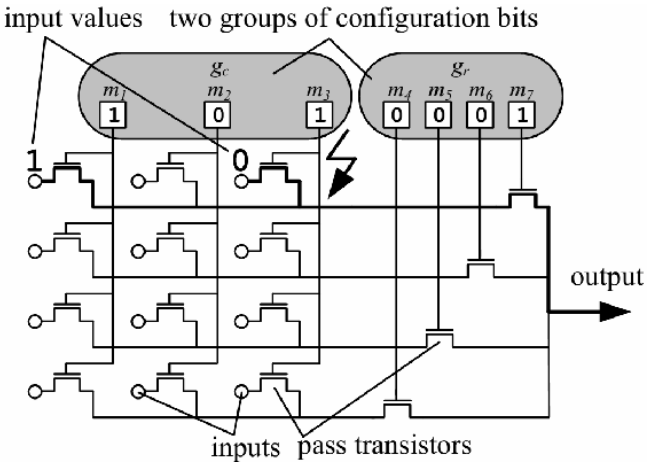
# Our initial hardware platform

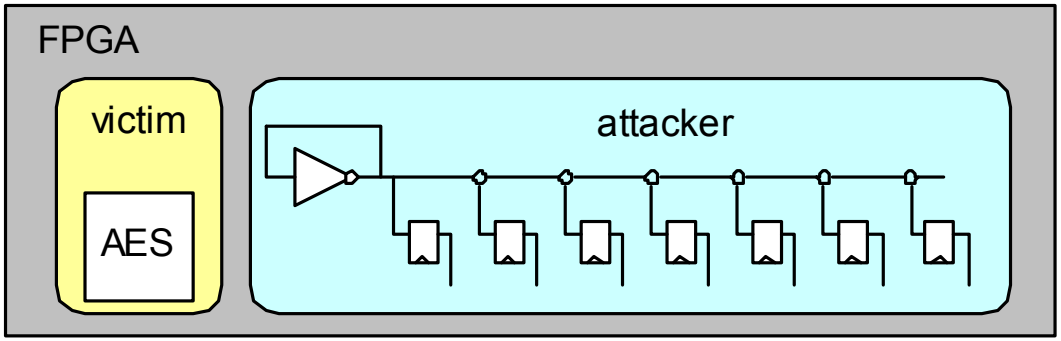


# rFAS - FPGA Accelerator Sandboxing

## FPGAs have a huge surface of attack!

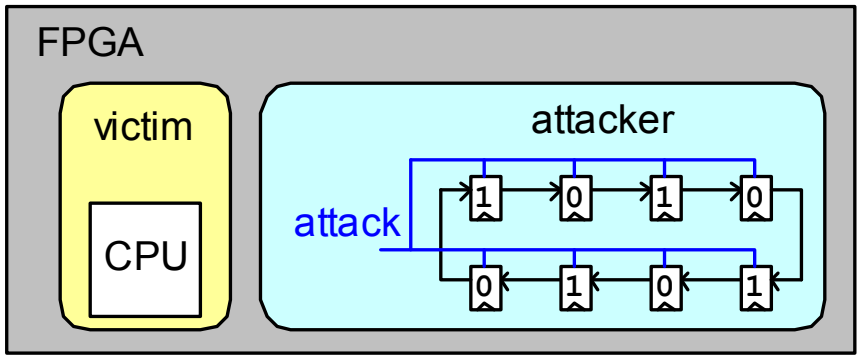
- **Remote DPA attacks**




- **Destroy or age FPGA hardware through corrupted bitstream (we have shown that!)**

- **Power hammering attacks**



# rFAS - FPGA Accelerator Sandboxing

## Goals

- Systematic review on possible FPGA attack scenarios
- Developing mitigation strategies
  - Virus scanner (detect short circuits, ring oszillators, etc.)
  - System monitors (voltage drops)
  - Configuration protection unit (protect FPGA regions)
  - Memory protection and custom interconnects
- Assessment of mitigation strategies and countermeasures

- Secure multi-tenancy scenario
  - Protect from information leakage
  - Ensure integrity of an FPGA-based system