Security Evaluation of Asynchronous Circuits

Jacques Fournier[1], Simon Moore[2],
Huiyun Li[2], Robert Mullins[2] and George Taylor[2]

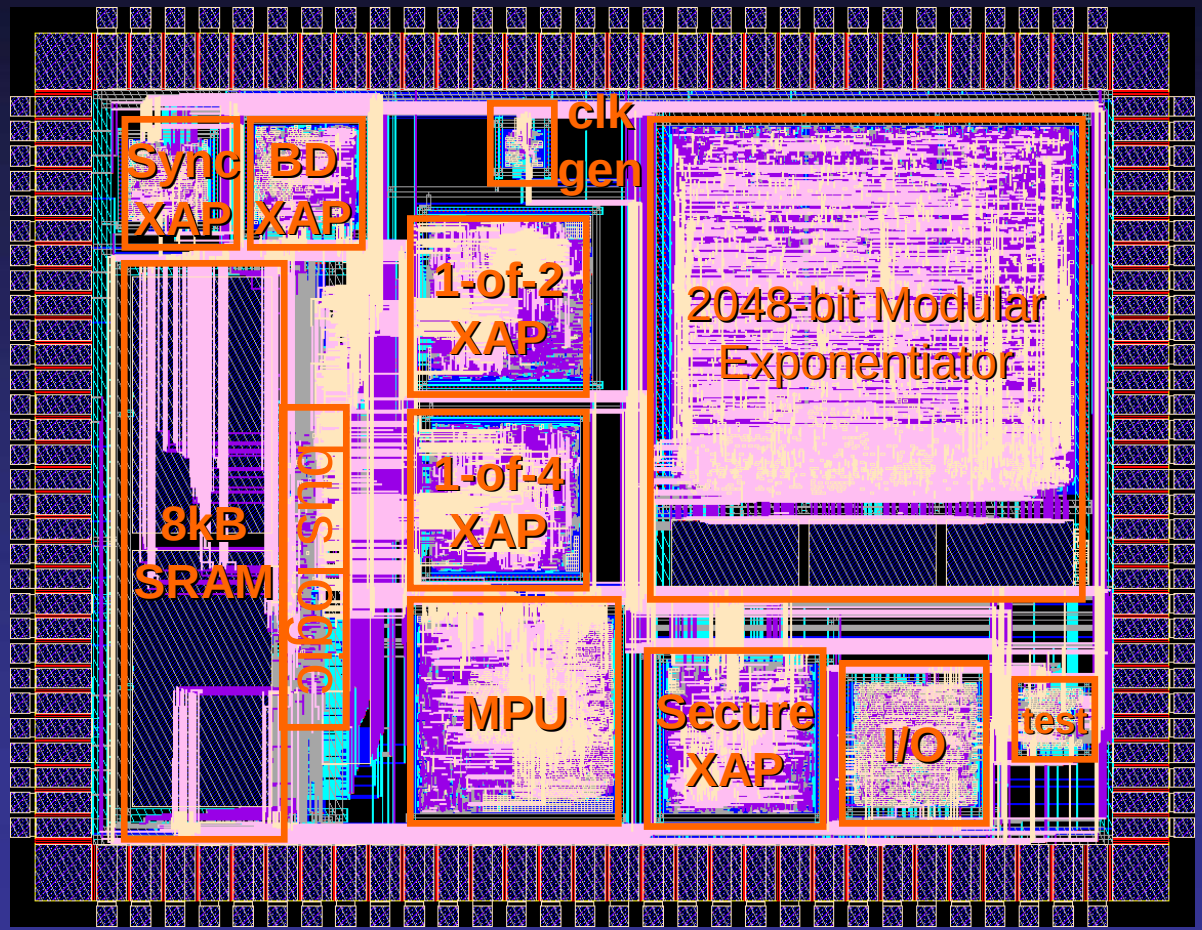
1 GEMPLUS

2 UNIVERSITY OF CAMBRIDGE Computer Laboratory

Motivation for using async. circuits

- Environment tolerance to fault injection
  - Light/laser, voltage glitches
- Redundant data encoding
  - Fault tolerance and alarm propagation
- Balanced power consumption
  - Resistance to power analysis
- Absence of a clock signal
  - Removes clock glitch attack

Springbank Testchip



Test environment

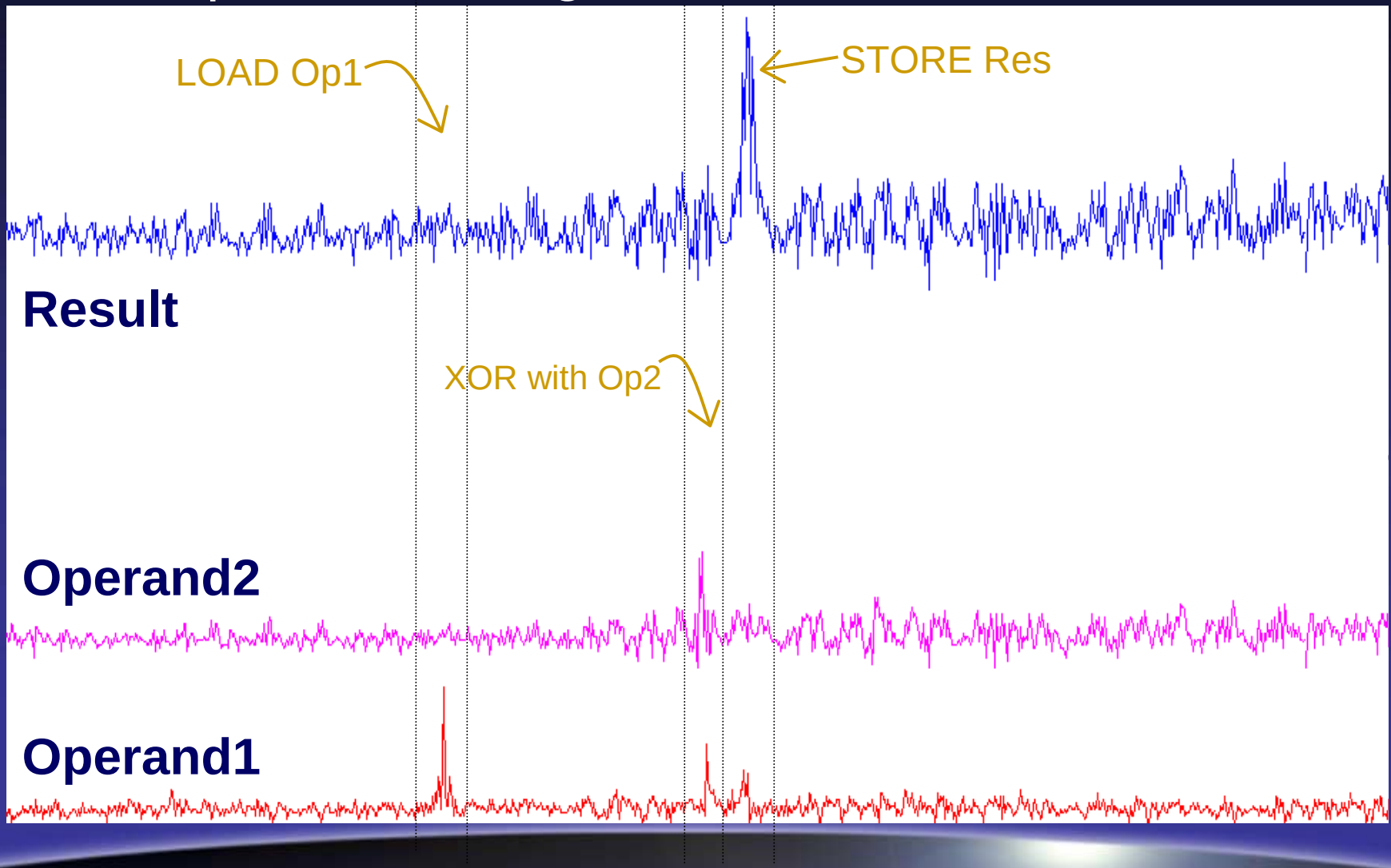
- Objectives
  - Test: CPA, DEMA & Fault injections
  - Keep the testing as simple as possible to critically evaluate robustness of test chip
- Approach
  - Short sections of code
  - Synchronisation pulse on output pin at start
  - Read out state of system after test
  - All program and data are known

Test 1: CPA on Sec XAP

- Measurements corrupted by noisy environment
- Found significant correlation values between the Hamming weight of the data processed and the current variations
- Same measurements and treatment were done on synchronous XAP
  - Found a reduction of about 10-15% in max correlation
  - Asynchronous XAP has a reduced data dependant information leakage of about 20-25dB

Test 2: EM Analysis on the *Secure* XAP

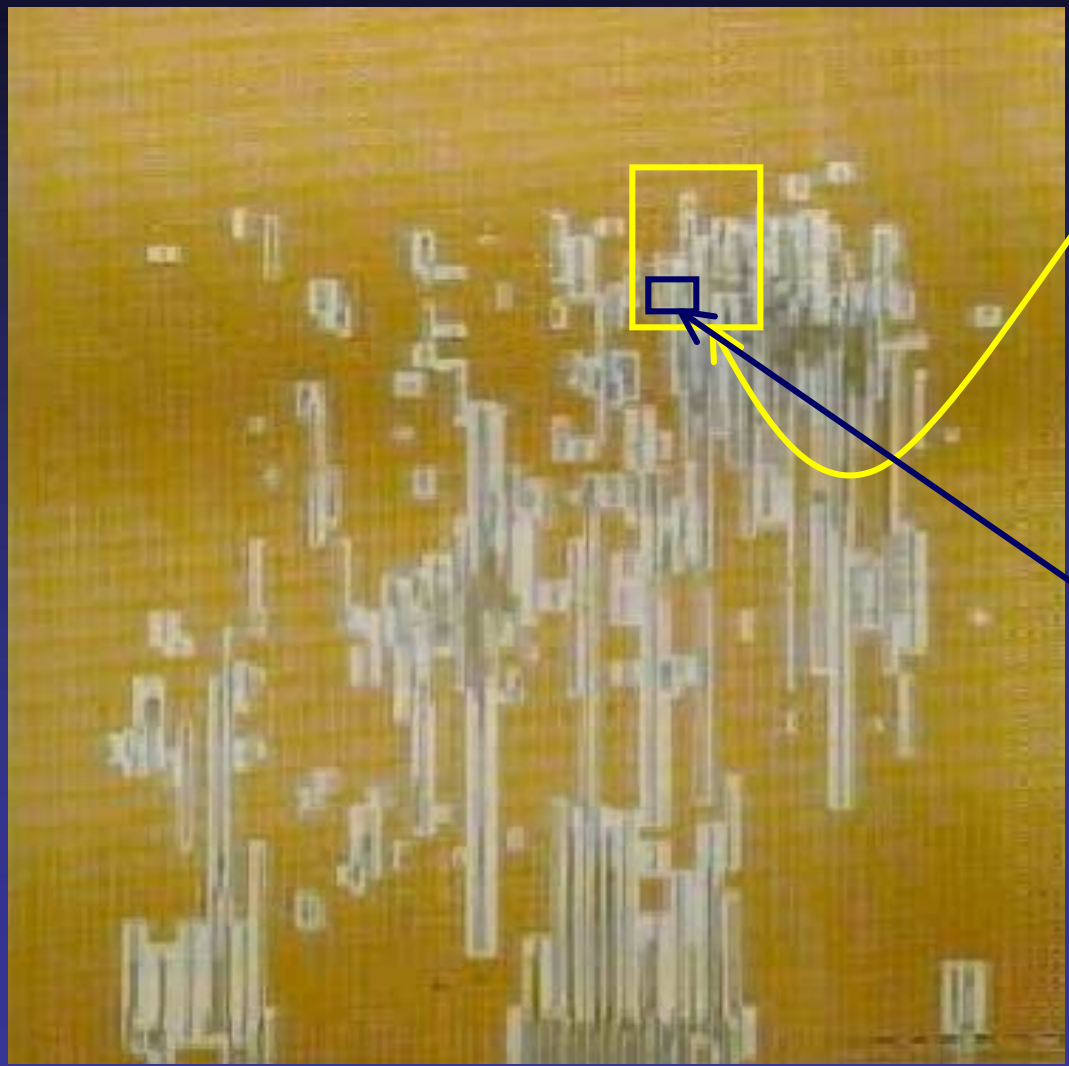
- CPA peaks with high correlation ratios



Test 3: Optical Fault Injection

- Laser fault injection
  - Systematic scan over the chip
  - Systematic timing variation of the laser pulse from start of software sequence
  - Primarily tested XOR instruction
- Results
  - Many of the asynchronous circuits correctly produced an alarm signal or the circuit halted
  - But register bits were zeroed due to bad design

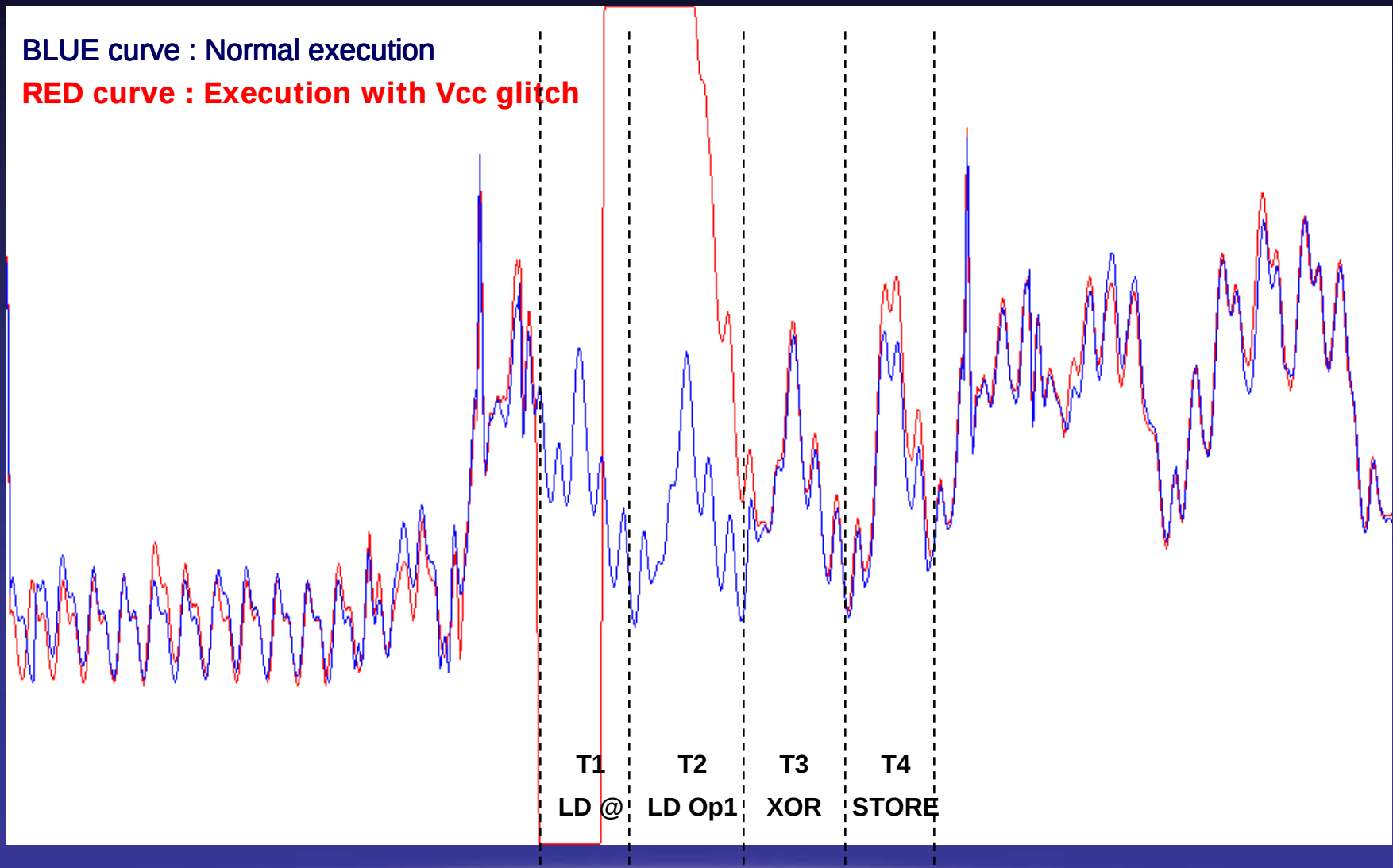
Laser on the AL-AH registers



Test 4: Vcc glitches on the Secure XAP

- Used glitches where power drops from 1.8V to 0V for definite periods
  - Kept the same program as executed for the laser experiments
- Results
  - Asynchronous circuits robust to short glitches (simply slowed down and sped up again)
  - Memory operations corrupted for longer glitches
    - Note that SRAMs are normal commercial IP

Corrupting operand load from memory



Future Directions

- Design time security analysis
  - We have simulated the effects seen through testing
  - Currently researching techniques for hierarchical design time security validation:
    - Exhaustively simulate attacks on each module
    - Construct a proof of correctness for systems built from secure modules
- New implementation technologies
  - E.g. Polysilicon transistors

Conclusions

- Well designed asynchronous circuits are demonstrably:
  1. able to resist some fault induction attacks
  2. and can leak less information
- BUT we need a design methodology which is far more rigorous
  - We believe that design time security validation is the way forward