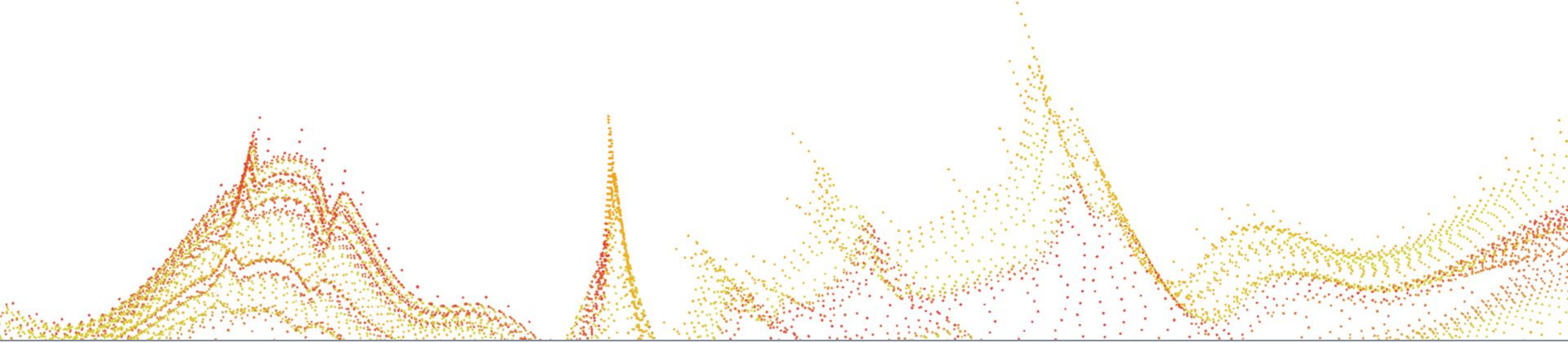
Automation for Side-Channel and Security Testing of Hardware IP

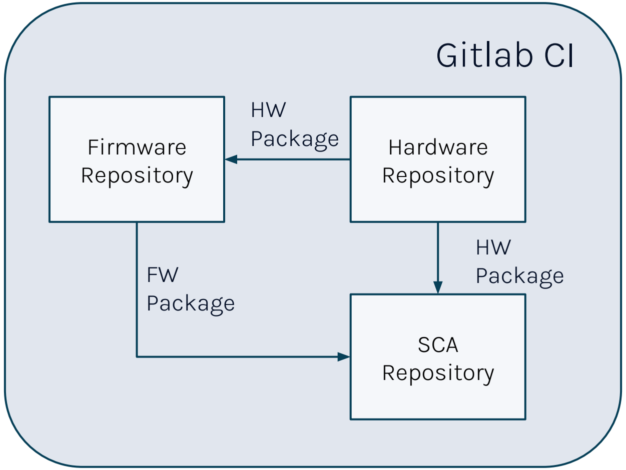
Niels Samwel (niels.samwel@pqshield.com)



Side-Channel and Security Testing Infrastructure

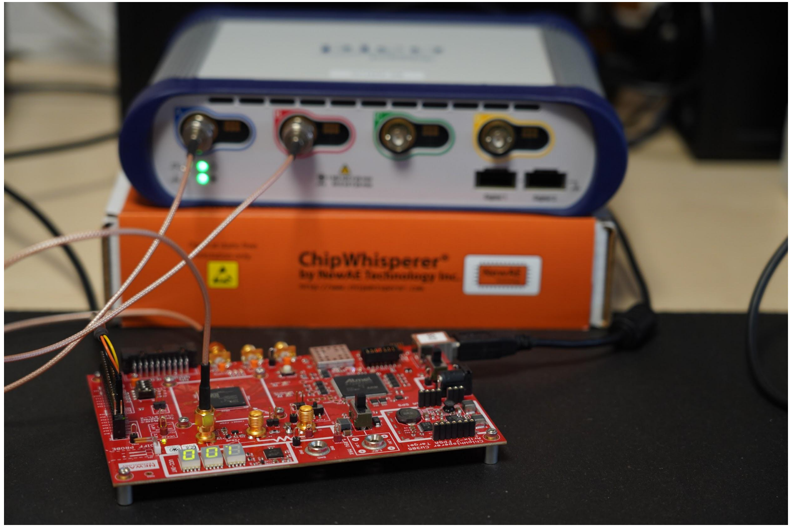
Post Quantum Cryptography Development

- Quality Testing
- Side-Channel Testing
- Fuzzing
- Future
  - Side-Channel Simulation
  - Fault Simulation



Side-Channel Setup

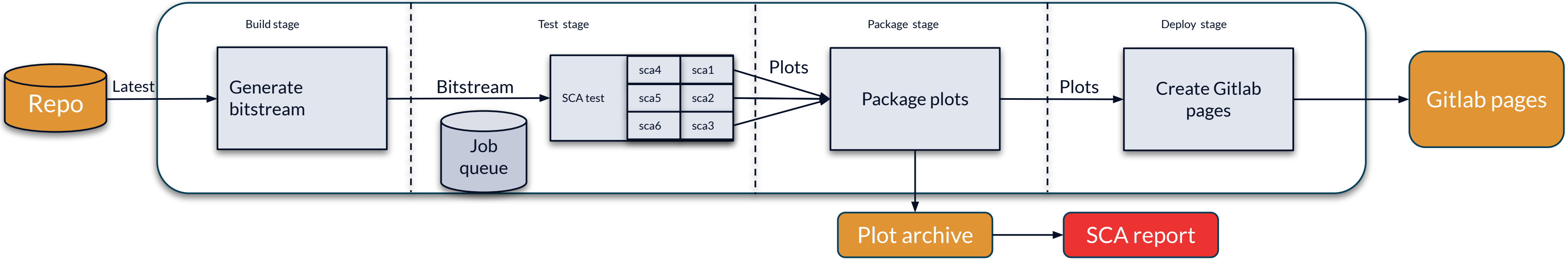
- Target
  - Chipwhisperer CW305
    - Artix 7 FPGA
- Oscilloscope
  - Picoscope 6424E
    - 8 bit resolution (can be increased to 12-bit)
    - 500 MHz bandwidth
    - 4 GS memory



Side-Channel Testing (FIPS 140-3)

- 9 Side-Channel Setups
- Challenges
  - Fully remote company
  - Number of tests

CI Pipeline



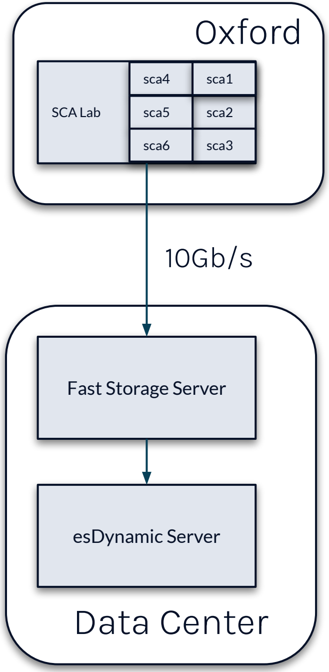
Side-Channel Testing (Common Criteria)

TVLA Limitations

- Univariate tests
- No estimation of actual security

Ad Hoc Testing

- Goal: estimate number of traces for key recovery
- Target specific vulnerabilities
- Attack types
  - Template attacks
  - Key recovery attacks
  - CPA/DPA



Product Quality Testing

Hardware

- Design Phase
  - Linting (VC Spyglass)
  - Physical design implementation
  - Automated FPGA functional testing
  - Peer review each commit
- Verification Phase
  - Constraint random verification (UVM)
  - Condition/Toggle coverage
  - Bounded model checking (VC Formal)
- Dashboards with metrics

Software

- Implementation Phase
  - Static analysis
  - Automated FPGA functional testing
  - Peer review each commit
- Verification Phase
  - System level tests
  - Integration tests
  - Functional tests
  - Unit tests
  - Coverage testing
  - Fuzzing

PQShield’s Security Levels

Level	Target	FIPS 140-3 level	Common-Criteria
0	Safe against fuzzing Safe against remote attacks*	Level 1	EAL1 AVA_VAN.1
1	Safe against “push button” physical attacks (basic attack potential)	SW: Level 2 HW: Level 3	EAL2 to 3 AVA_VAN.2
2	Safe against expert lab (high attack potential)	SW: Level 2 HW: Level 4	EAL4+ to 7 AVA_VAN.5

*For software libraries, micro-architecturale attacks such as RowHammer, Spectre, Meltdown… may be applicable if the hardware platform is vulnerable to them.