UNIVERSITY OF ARKANSAS

Power Based Side-Channel Attack Analysis on PQC Algorithms

Tendayi Kamucheka, Michael Fahr, Tristen Teague, Alexander Nelson,
David Andrews, Miaoqing Huang

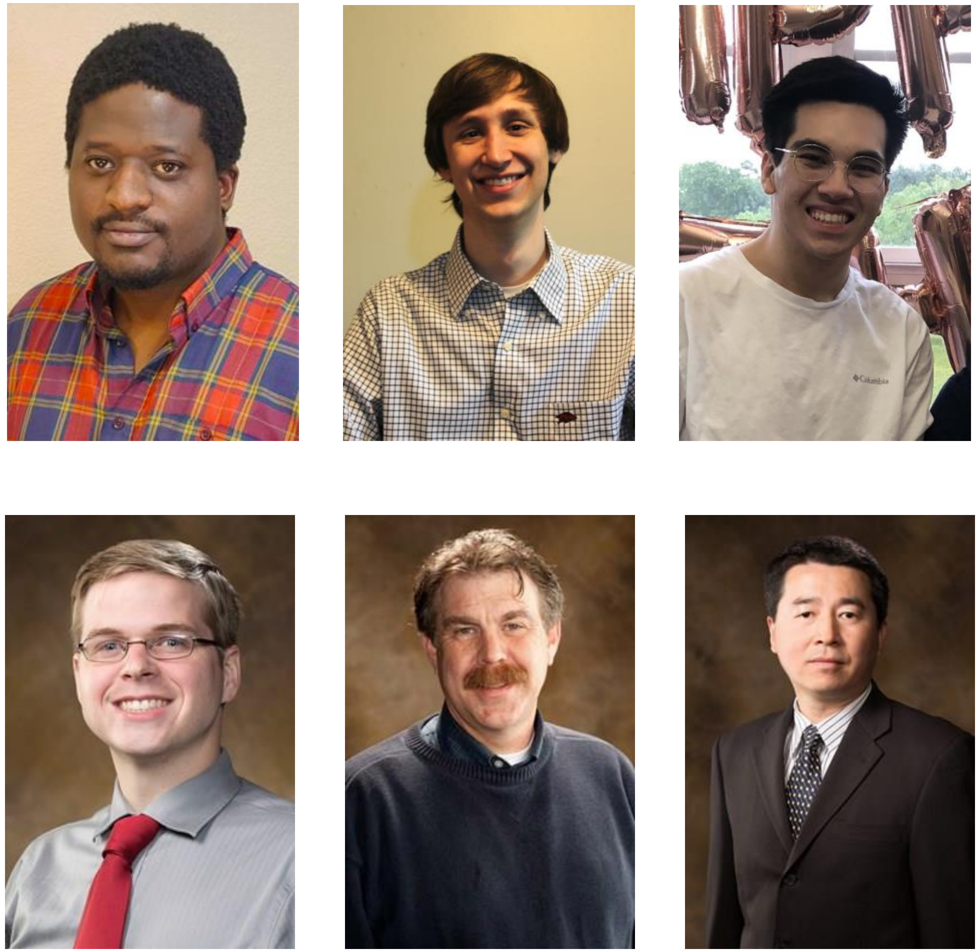
Acknowledgement: NIST – Award 60NANB20D016

NIST

About Us

- Computer Systems Design Lab & AESIR Lab at University of Arkansas – Computer Science & Computer Engineering Department

- Background – Hardware design, Embedded Systems, High Performance Computing, FPGAs, GPGPU



(Top) Tendayi Kamucheka, Michael Fahr, Tristen Teague

(Bottom) Alexander Nelson, David Andrews, Miaoqing Huang

UNIVERSITY OF ARKANSAS

Research Motivation

- Round 3 places significant interest on:
  - perfect forward secrecy,
  - side-channel and multi-key attacks,
  - and resistance to misuse.
- What can a well-equipped bad actor do with different types of equipment?

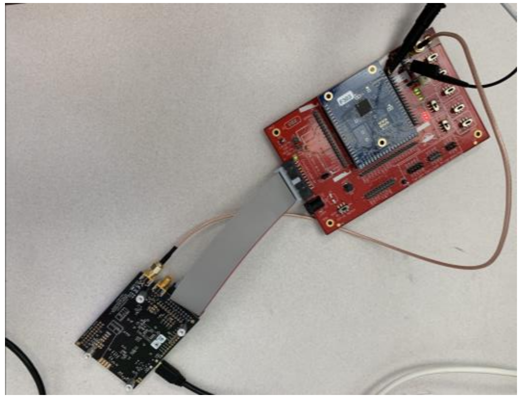
ARE WE SAFE FROM SIDE CHANNEL ATTACKS?

UNIVERSITY OF ARKANSAS

Images:
(right) Artist – Justin Middendorp, https://dribbble.com/jusmid

Our Approach: Implementation

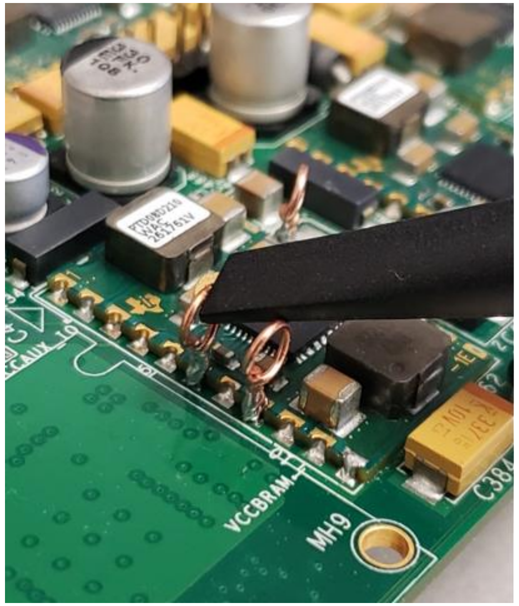
- We setup a multi-platform testing lab for power analysis on round 3 PQC algorithms
- Equipment:
  - Tektronix MDO 3 Series oscilloscope
  - ChipWhisperer-Lite
- Current target platforms:
  - Xilinx Artix-7 FPGA
  - Xilinx Virtex-7 FPGA
  - Cortex M4 microcontroller
- Current implementations:
  - Hardware version of Kyber512 (Virtex-7 FPGA)
  - Software version of masked Kyber (Cortex-M4)
  - Using PQM4 library for other testing on Cortex-M4

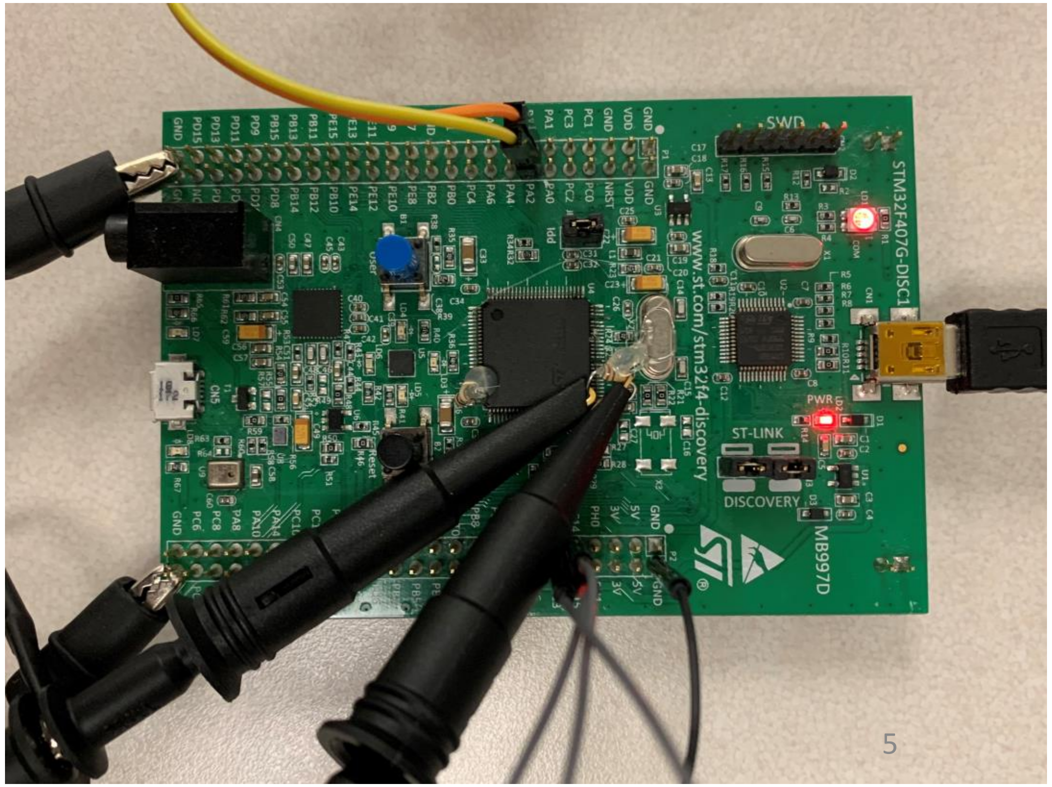


Images:
(top) Tektronix MDO 3-series oscilloscope https://www.valuetronics.com/product/mdo34-3-bw-100-tektronix-mixed-domain-oscilloscope-new
(bottom) ChipWhisperer-Lite (black) + UFO target board (red), Cortex-M4 (blue) board mounted on UFO target board.

Our Approach: Methodology

- Non-specific TVLA is used to validate our set up and identify potential leakage
- Experiment setup:
  - Control experiments – fixed vs. fixed inputs
  - Other experiments – fixed vs. random inputs
  - 2000 power traces per dataset
- FPGA board is modified to add probe points to measure current
- On microcontroller, traces are collected from current measured across a shunt resistor





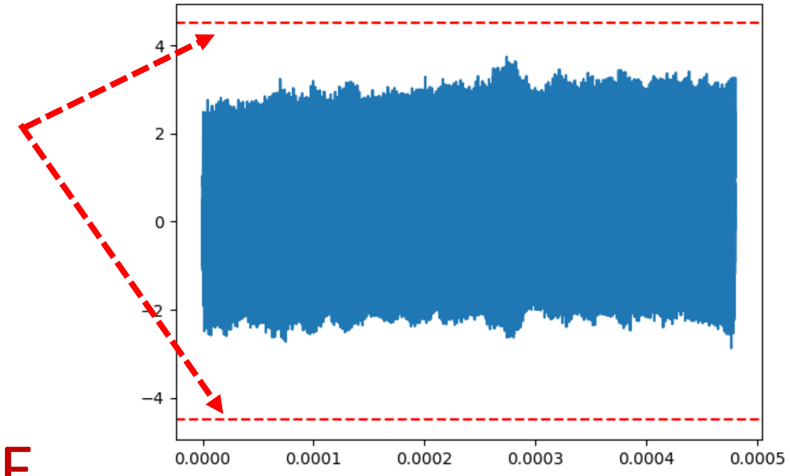
Test Vector Leakage Assessment (TVLA)

- Welch's t-test, is statistical test that highlights differences between two datasets
- Outcome is pass or fail for each trace point
- A measure of 4.5 standard deviations is set as leakage threshold
  - 99.9999% confidence that anything above the threshold is due to leakage

$$t = \frac{X_A - X_B}{\sqrt{\frac{S_A^2}{N_A} + \frac{S_B^2}{N_B}}}$$

Where:

$X_A =$ sample mean for each point across time
$S_A =$ standard deviation
$N_A =$ cardinality

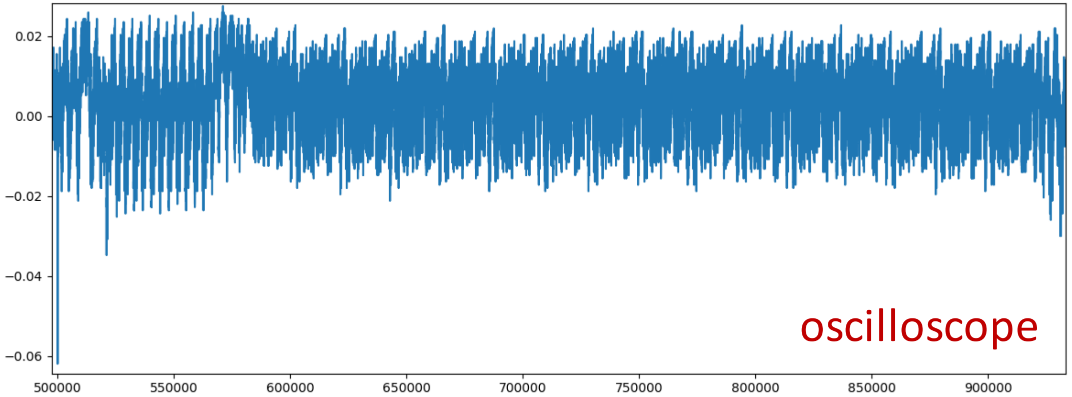


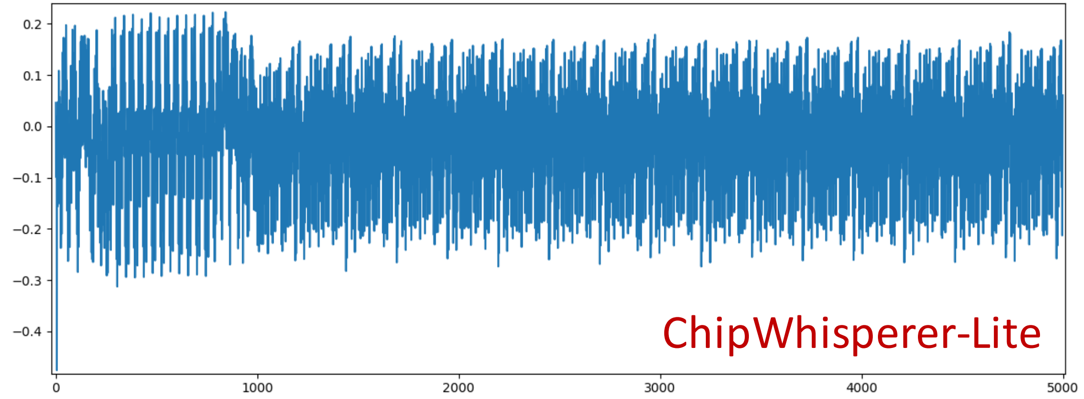
Leakage threshold

A TEST FOR SENSITIVE DATA-RELATED LEAKAGE

Results:

- Result of measuring voltage drop across shunt resistor
- Oscilloscope captures 1 million data points
- ChipWhisperer-Lite captures 5 thousand data points for same test



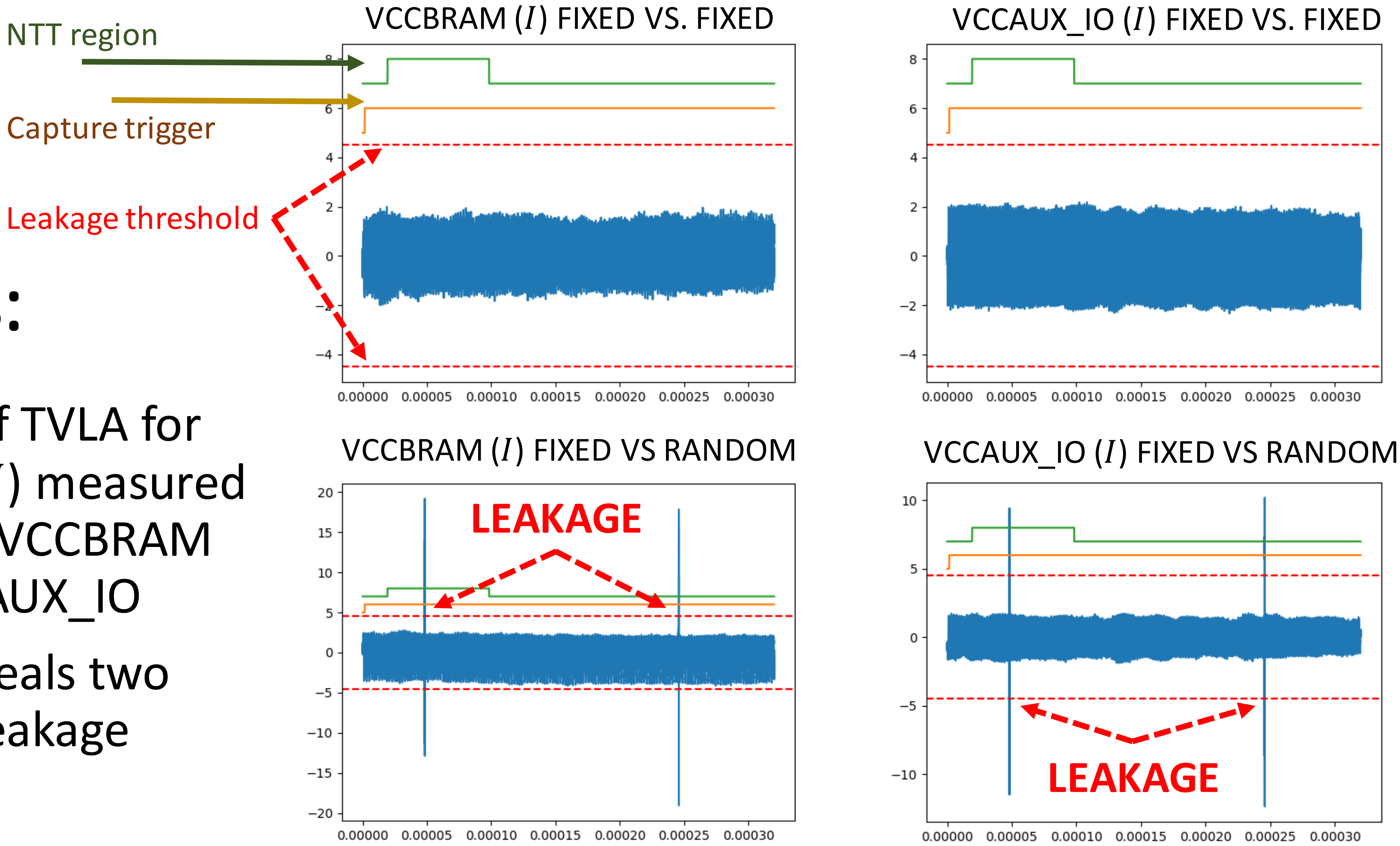


Oscilloscope captures at higher resolution

UNIVERSITY OF ARKANSAS

Results:

- Results of TVLA for current (I) measured on FPGA VCCBRAM and VCCAUX_IO
- Trace reveals two distinct leakage points



LEAKAGE TEST **FAILS** AT SAME POINTS IN BOTH TESTS

Conclusions

- We set up a multi-platform testing lab for power analysis side channel analysis
- We evaluate our setup with non-specific Test Vector Leakage Assessment
- Experiments show some leakage – Further analysis is required.
- Future work:
  - Further analysis of observed leakage
  - Exploiting leakage to develop side-channel assisted attacks

Questions?

- Contact info:
  - Tendayi Kamucheka – tfkamuch@uark.edu
  - Michael Fahr – mjfahr@uark.edu
  - Tristen Teague – tdteague@uark.edu

  - Computer Systems Design Lab (Lab P.I.s)
    - Miaoqing Huang – mqhuang@uark.edu
    - David Andrews – dandrews@uark.edu
  - AESIR Lab (Lab P.I.)
    - Alexander Nelson – ahnelson@uark.edu

Thank You