UNIVERSITY OF ARKANSAS

Towards a Cloud-Based Infrastructure for Post-Quantum Cryptography Side-Channel Analysis

Miaoqing Huang, David Andrews, and Alexander Nelson

ÆSIR Applied Embedded Systems and IoT Research

Computer Systems Design Laboratory

Introduction

- Post-Quantum Cryptography algorithms are becoming standardized
- Implementations need to be thoroughly evaluated against side-channel attacks
- There exists no SCA tool open to the public

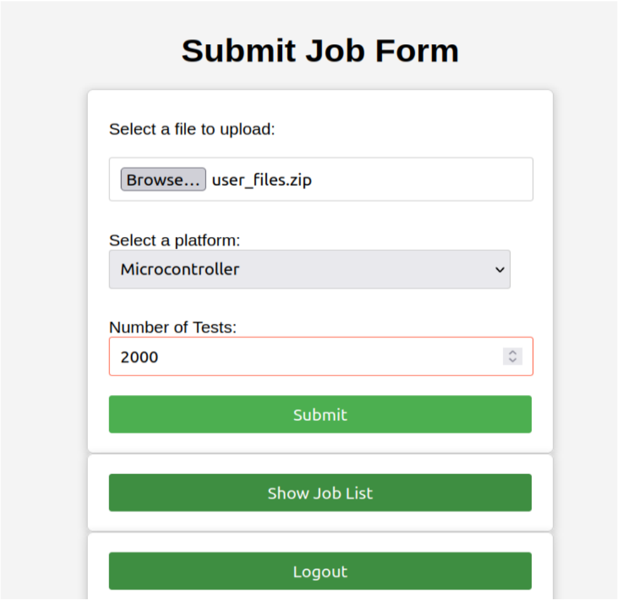
Setup

- Take user's implementation of PQC algorithm following API
- User submits job and platform for SCA evaluation
- Cloud tool processes job and does analysis on victim platform
- Cloud tool performs analysis and returns results back to the user

Goal

- Provide SCA infrastructure open to research and education
- Provide cloud-based multi-platform tool to remove effort of doing SCA
- Further increase SCA security for new standardized cryptography algorithms

Web Interface



Submit Job Form

Select a file to upload:

Browse... user_files.zip

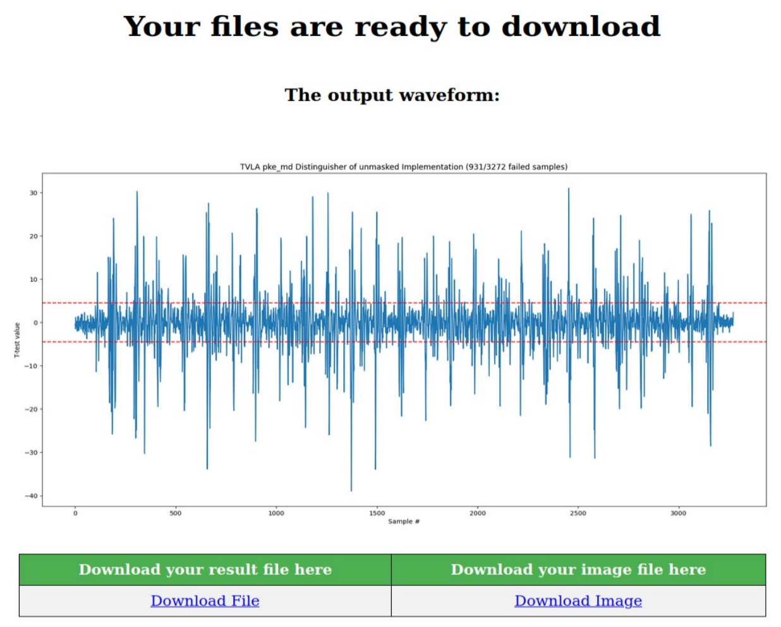
Select a platform:

Microcontroller

Number of Tests:

2000

Job Submission



Your files are ready to download

The output waveform:

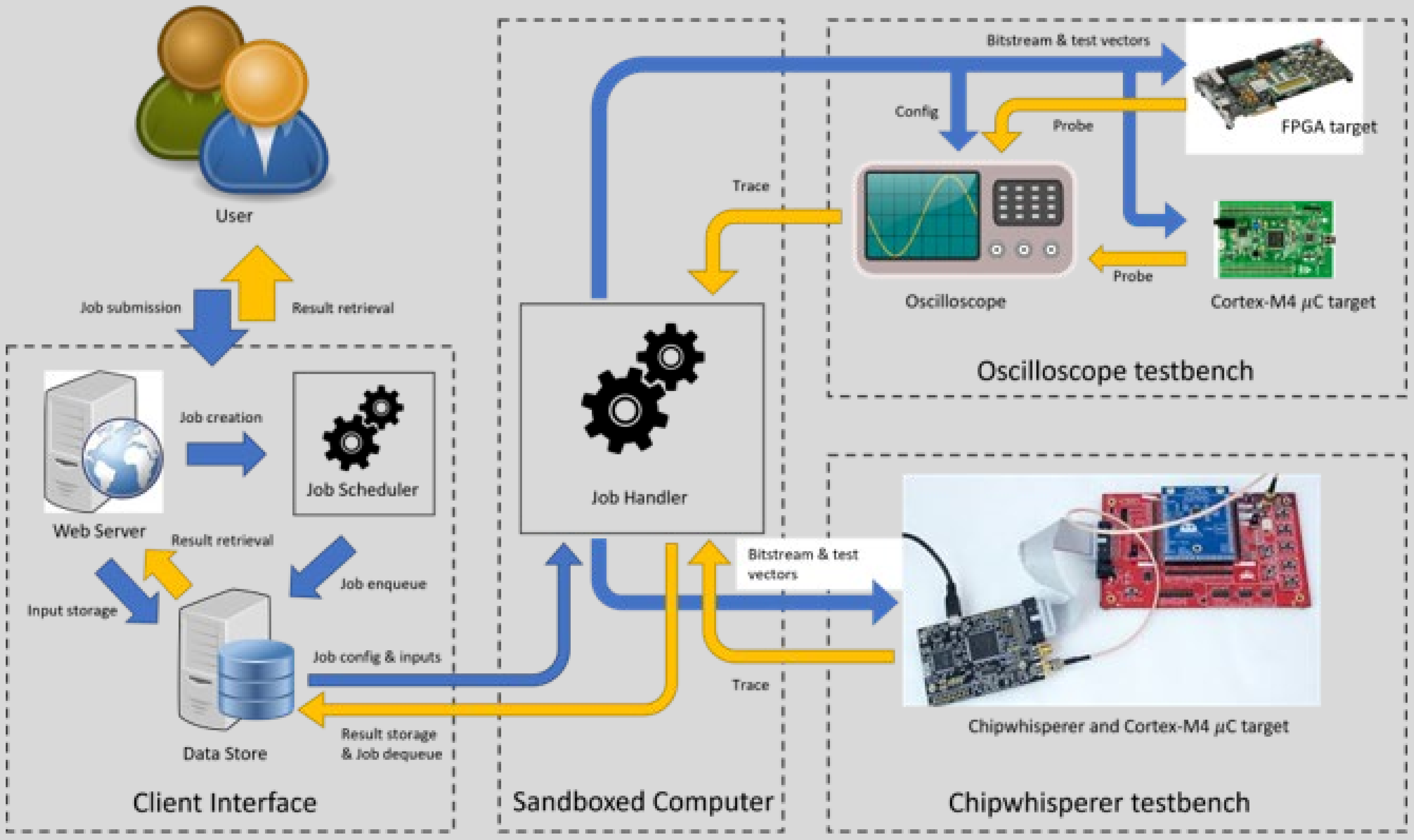
TVLA pke_md Distinguisher of unmasked Implementation (931/3272 failed samples)
T-test value
Sample #

Download your result file here	Download your image file here
Download File	Download Image

Results Page

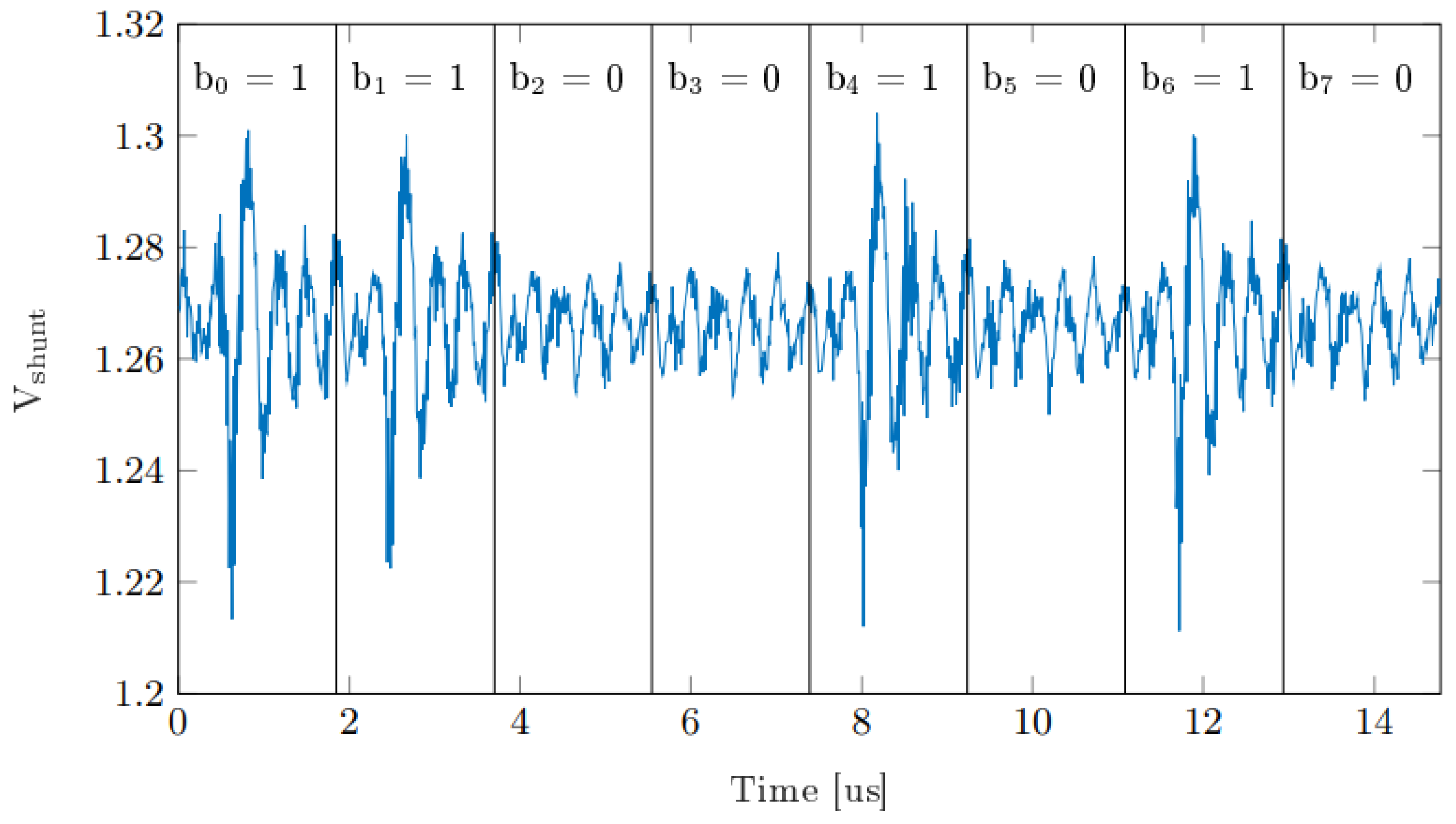
SCA-in-Cloud

A community driven cloud-based side-channel analysis tool for **Post-Quantum Cryptography** algorithms



SCA-Tool Architecture

Power Analysis



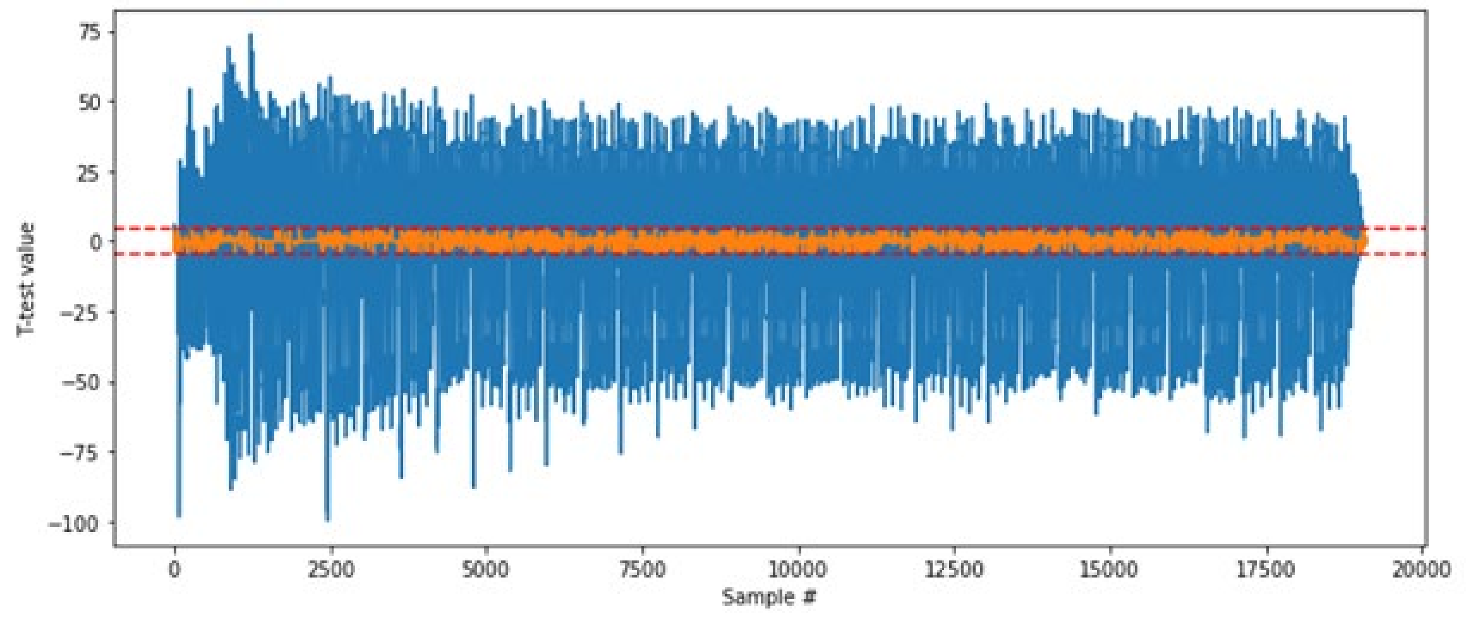
SPA on Message Encoding of NewHope

Test Vector Leakage Assessment

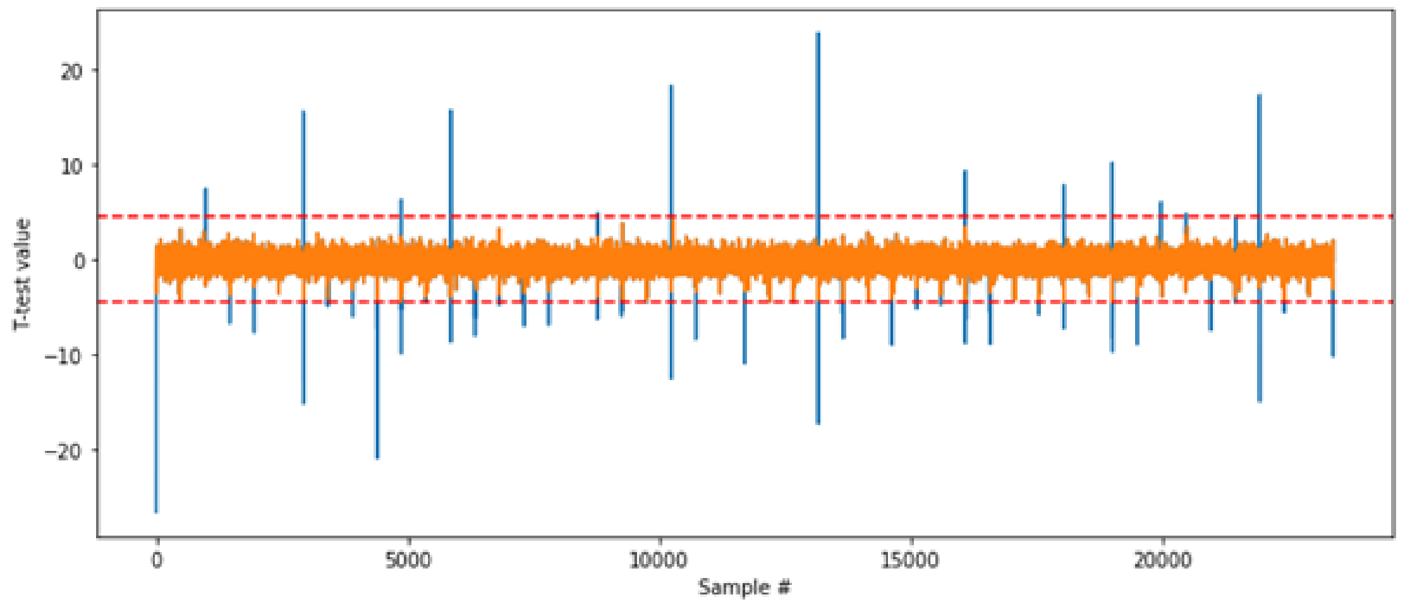
Welch's t-value

μ = mean, S = Std. Dev.

$$t = \frac{\mu_A - \mu_B}{\sqrt{\frac{S_A{}^2}{N_A} - \frac{S_B{}^2}{N_B}}}$$



Unmasked Message Encoding TVLA CRYSTALS-KYBER



Masked Message Encoding TVLA CRYSTALS-KYBER

NSF

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Department of Education United States of America