

# The KYBER Binomial Sampler Dataset

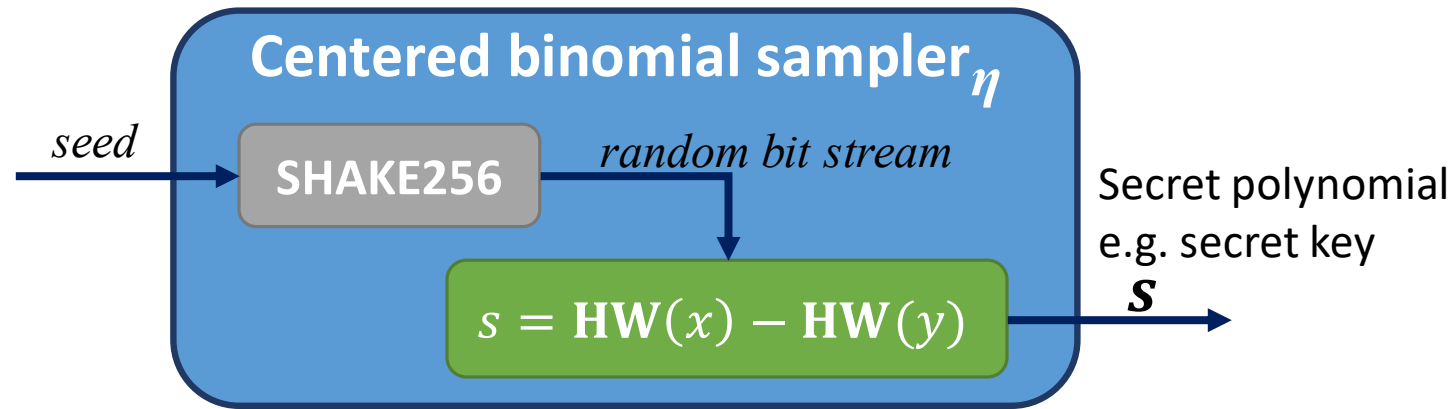
Eric Chun-Yu Peng, Markus G. Kuhn

University of Cambridge

14 September, OPTIMIST Workshop '25

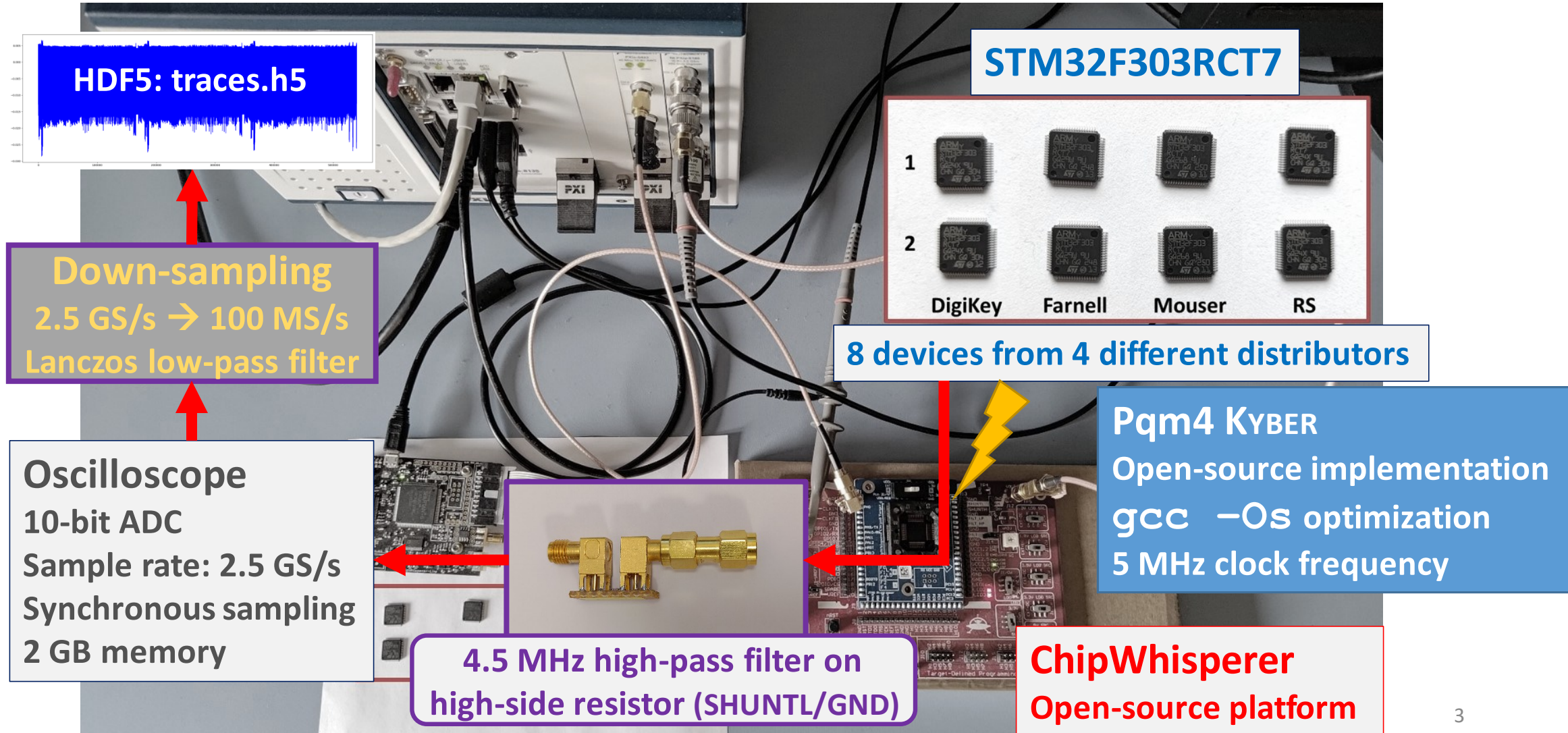
# Binomial sampler in KYBER

- Generates all the secret “noise” polynomials in KYBER



- Sampling a noise polynomial involves two subroutines:
  - SHAKE256
  - The sampling procedure
- Our dataset is primarily for reproducing the results in our paper
  - Show how information leaks through the sampling procedure

# Measurement setup



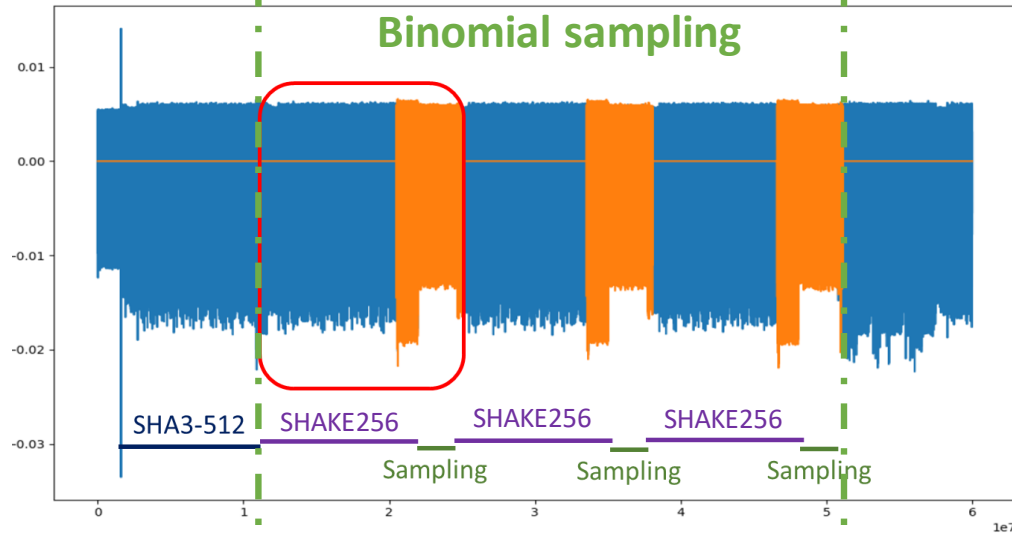
# Preprocessed trace dataset

Trace acquisition  
& meta-data (seed)

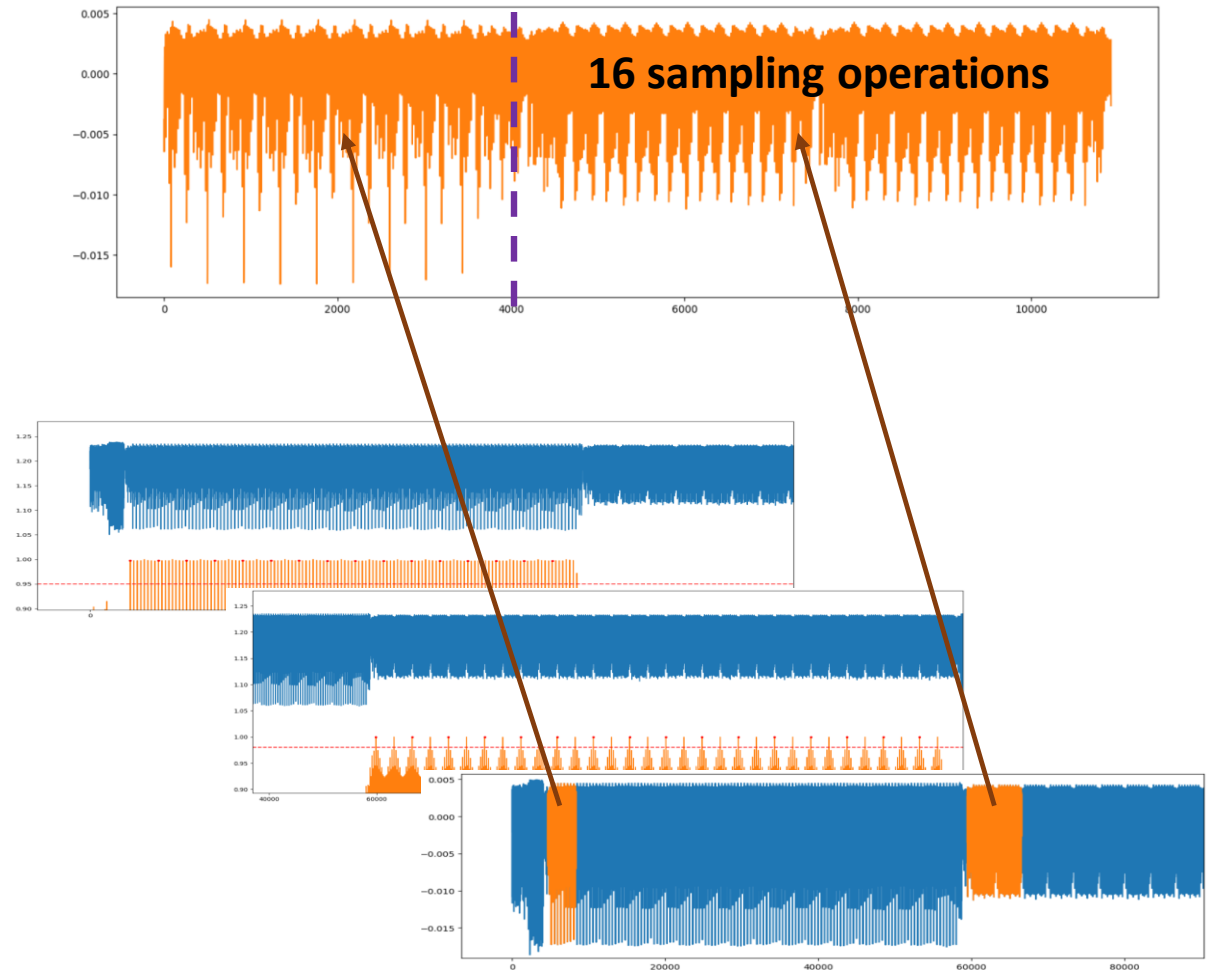


Preprocessing &  
intermediate values

KYBER768-KEM KeyGen operation



Preprocessed trace dataset



# Dataset webpage

<https://www.cl.cam.ac.uk/research/security/datasets/kyber/>



Search



[Contact us](#) | [A-Z](#) | [Advanced search](#)

## Department of Computer Science and Technology

 [Computer Laboratory](#) > [Research](#) > [Security](#) > [Data sets](#) > [Kyber-CBD dataset: adaptive template attacks on the Kyber binomial sampler](#)

### Kyber-CBD dataset

## Kyber-CBD dataset: adaptive template attacks on the Kyber binomial sampler

The dataset available here allows reproduction of some of the experiments described in the paper

Eric Chun-Yu Peng, Markus G. Kuhn: Adaptive Template Attacks on the Kyber Binomial Sampler. IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2025, No. 3, pp 470–492. DOI: 10.46586/tches.v2025.i3.470-492

The [Julia](#) code for running the experiments and reproducing some of the tables and figures in that paper is available in the GitHub repository [eric-cyp24/Kyber768cbd.jl](#). See the [README](#) file there for detailed instructions.

The required data set is available in the [data/](#) folder as a file tree of [HDF5](#) files. Best use the Julia script `scripts/downloaddata.jl` found in the code repository to download the required parts.

# Adaptive Template Attacks on the Kyber Binomial Sampler

[Eric Chun-Yu Peng](#), [Markus G. Kuhn](#)

This repository contains the [Julia](#) code needed for reproducing the experiments described in our paper

Eric Chun-Yu Peng, Markus G. Kuhn: [Adaptive Template Attacks on the Kyber Binomial Sampler](#). [IACR Transactions on Cryptographic Hardware and Embedded Systems](#), Vol. 2025, No. 3.

## Requirements

This code was mainly developed and tested on x86-64 (64-bit) computers running Ubuntu Linux 20.04 or 24.04 with 48 GB RAM. We hope it will run on any platform that is [supported by Julia](#) and has at least 16 GB RAM. **About 25 GB** disk space would be ideal, but there are also ways to run the demo with only about 12 GB disk space.

## Install Julia

To run this code, you will need [Julia](#) (version 1.11 or newer).

For Linux or macOS, best [install Julia](#) via the [juliaup](#) installation manager using the following shell command line:

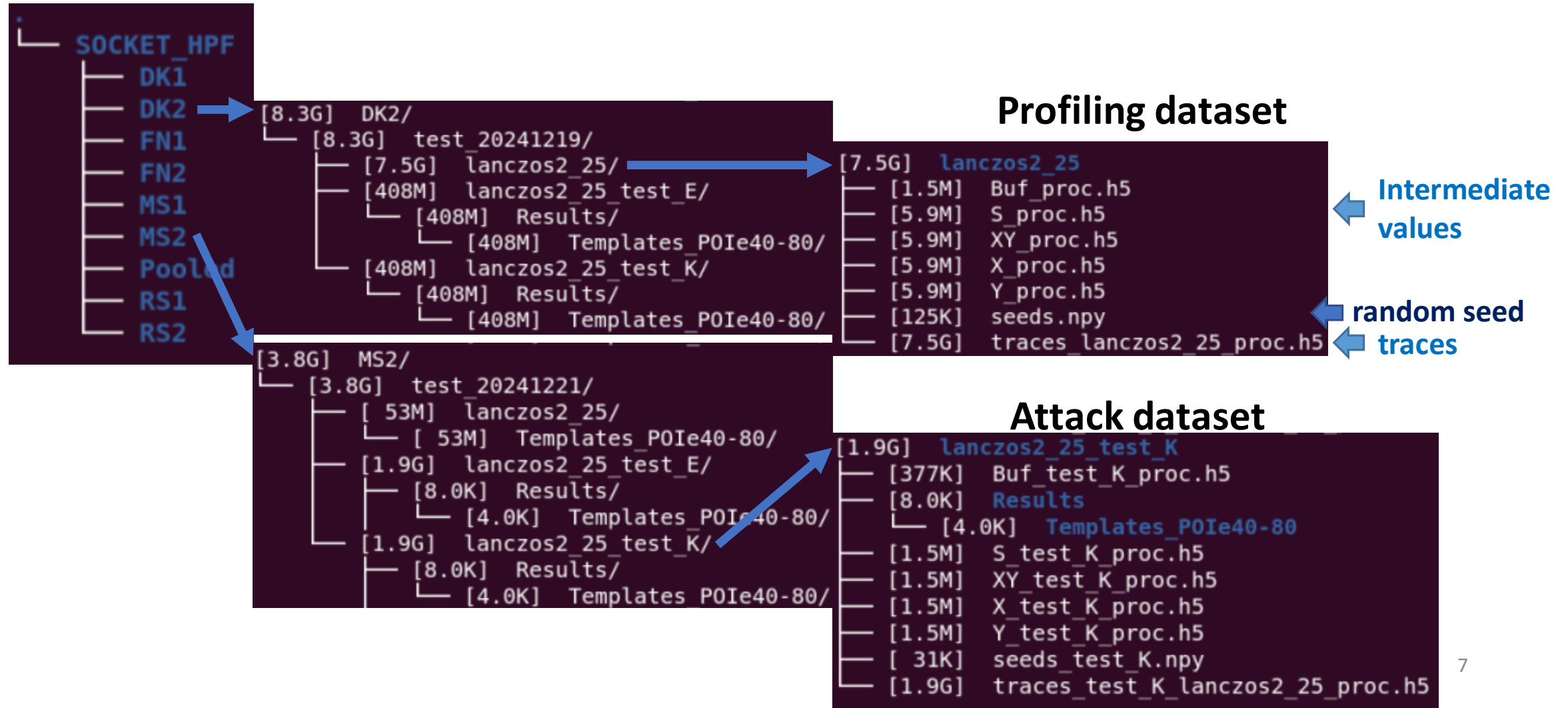
```
$ curl -fsSL https://install.julialang.org | sh
```



## Download this repository

Clone this repository and its submodules to your local machine, then install (“instantiate”) the required Julia package dependencies for this project into your Julia depot path (default: `~/.julia/`):

# Dataset file structure



# **Thank you!**

## **Q & A**

Paper: <https://doi.org/10.46586/tches.v2025.i3.470-492>

Artifact: <https://artifacts.iacr.org/tches/2025/a19/>

Dataset: <https://www.cl.cam.ac.uk/research/security/datasets/kyber/>

Code: <https://github.com/eric-cyp24/Kyber768cbd.jl/tree/tches-artifact>