

TTM4205: ChipWhisperer Lab Common Problems

Tjerand Silde and Caroline Sandsbråten

{tjerand.silde, caroline.sandsbraten}@ntnu.no

October 2025

1 Lascar

Lascar is a framework for side-channel analysis and is used in the first ChipWhisperer lab. If you have installed ChipWhisperer manually (MacOS) or using the ChipWhisperer installer (Windows) from Newae's websites, Lascar might not be in your installation. You can install it using pip with the command

```
pip install lascar
```

inside your Python environment.

2 Dynamic Time Warp

For a few students the Dynamic Time Warp (DTW) implementation in Lascar is slower than expected. Keep in mind that Dynamic Time Warp will be slow regardless, at least compared to the SAD technique used earlier in lab 1. Aligning x traces to a reference trace using DTW where the length of each trace is L DTW will have a time complexity of $O(L^x)$. However, the DTW implementation used in the lab is an approximation algorithm, so it should have a time complexity of (roughly) $O(L \cdot r)$, with r being the radius parameter set in the lab and defines how big shifts between the traces are allowed. Note that this is not a 1-1 mapping between size of radius and size of shift allowed. If you experience that DTW is very slow, try the following:

- Reducing the number of traces you are aligning.
- Reducing the radius parameter.

- Reduce the amount of points in each trace by changing `scope.adc.samples` to a lower value.

If the above doesn't fix your issue, please contact Caroline (caroline.sandsbraten@ntnu.no) and we will evaluate if you can skip this particular task and still get full score on the lab.

3 File/Folder not found errors

If you experience file or folder not found errors, make sure that the path to the folder is correct. There has been some issues with the paths missing an additional `../`. These issues should be fixed, but be aware of this because if you are not using the latest commit on the main branch of the lab git.ntnu.no/ie-iik/chipwhisperer-lab-ttm4205/ your jupyter notebooks might not be updated with these fixes.

4 Updating Lab Notebooks from Git

Fixes to issues with the lab will continually be uploaded to git.ntnu.no/ie-iik/chipwhisperer-lab-ttm4205/. To get these updates the easiest way is to navigate to the lab folder in your terminal then use the command

```
git pull --autostash
```

to stash your changes, pull from the repository and pop your changes back into the newly updated folder. You can also make a commit first and then pull by using the command

```
git add . && git commit -m "<commit message>" && git pull
```

5 C Code

Parts of the labs will ask you to make a few changes and/or evaluate some C code. The relevant code for these tasks will always be in the same folder as the latest compiled code you flashed to your ChipWhisperer. The python command that flashes to your ChipWhisperer is

```
cw.program_target(scope, prog, <PATH/compiled.hex>)
```

and is always found in the `firmware/mcu/` folder (relative to the root of git.ntnu.no/ie-iik/chipwhisperer-lab-ttm4205/).