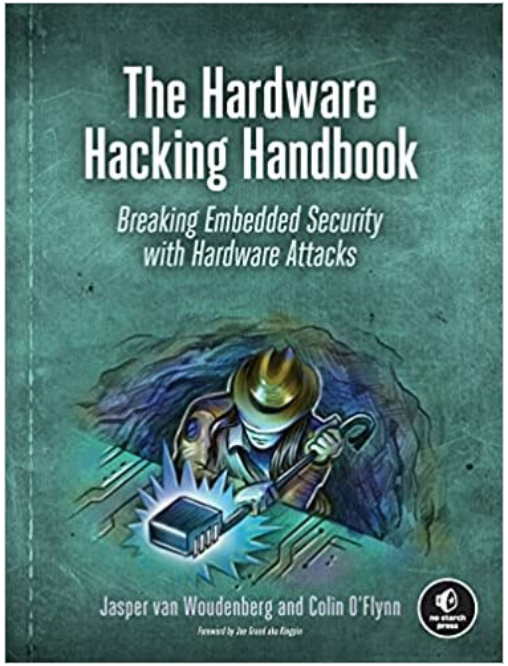
Open Problems in Hardware Security Research

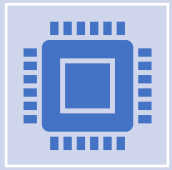
Dr. Colin O'Flynn

About Me

- Started ChipWhisperer project
  - Started as purely open-source tooling, now combination of open-source + commercially supported tooling for power analysis & fault injection.
  - Extensive use in academic + industrial research groups (> 100 published papers *using* ChipWhisperer, not just citations)
- PhD from Dalhousie University (2017)
  - Served as assistant professor after PhD, currently adjunct while pursuing industrial opportunity
- Standard academic & industrial publications + presentations (papers, patents, books).



Audience for this Talk



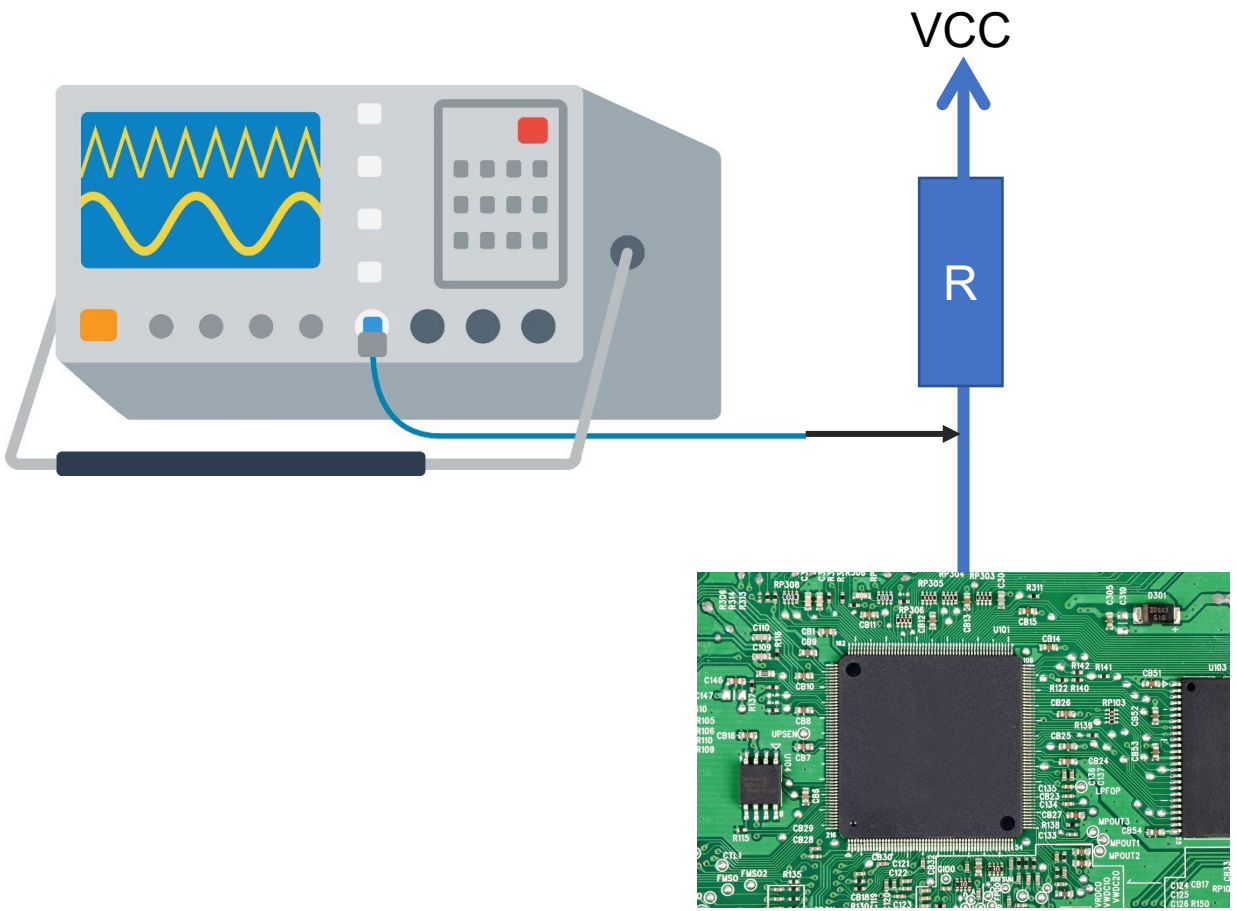
Assume you have extensive experience in related fields:

- Communications theory
- Semiconductor physics
- VLSI Design
- FPGA implementations
- Deep Learning

Assume you want to extend this into “cyber” because:

- Cybersecurity is a high-priority area for grants / industry.
- Considerable interest from students

Example of Old School → New School



Correlation Power Analysis

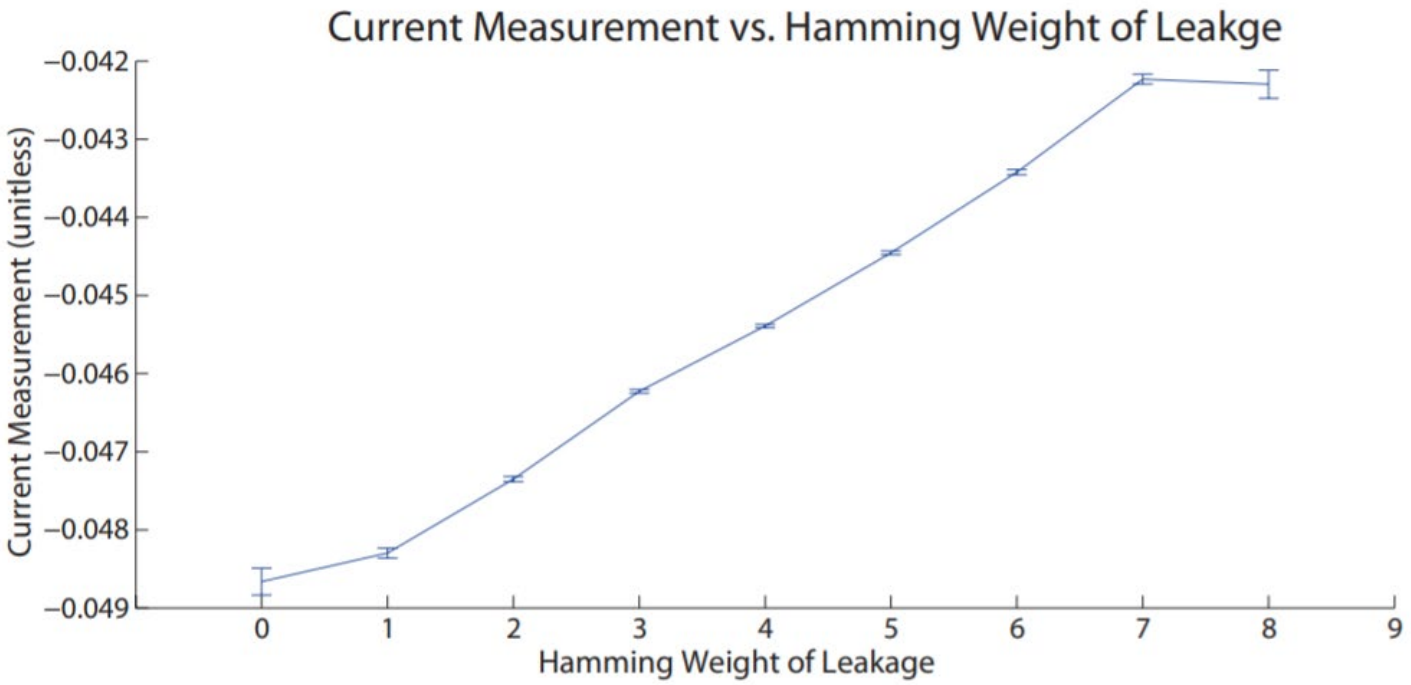


Figure 2.3: Power consumption of device under attack performing an operation on data with different Hamming Weights (HW), showing the average current consumption of the AtMega328P microcontroller for each possible hamming weight of an 8-bit number. Error bars show 95% confidence on average (based on the sample standard deviation).

Correlation for Power Analysis (2004)

$$r_{i,j} = \frac{\sum_{d=1}^{D} \left[\left(p_{d,i} - \overline{P_j} \right) \left(t_{d,j} - \overline{t_j} \right) \right]}{\sqrt{\sum_{d=1}^{D} \left(p_{d,i} - \overline{P_j} \right)^2 \sum_{d=1}^{D} \left(t_{d,j} - \overline{t_j} \right)^2}} \tag{2.1}$$

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y} = \frac{E\left[(X - \mu_X)(Y - \mu_Y) \right]}{\sqrt{E\left[(X - \mu_X)^2 \right]} \sqrt{E\left[(Y - \mu_Y)^2 \right]}} \tag{2.2}$$

Matched Filtering (1943)

$$r(t) = s(t) + n(t) \tag{2.3}$$

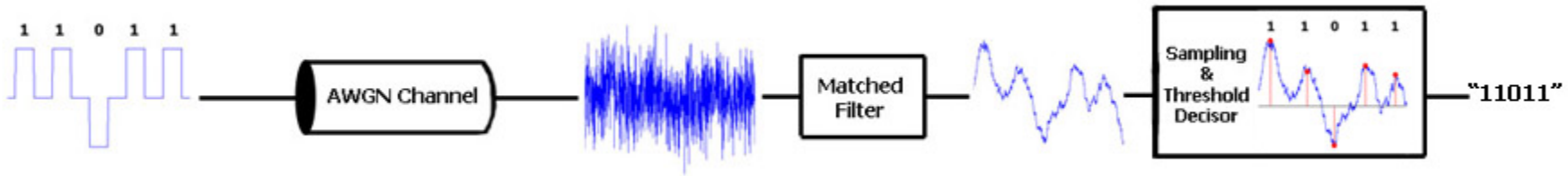


Figure by El pak (Public Domain, Wikimedia Commons)

$$y(t) = r(t) * h(t) = \int r(\tau)h(t-\tau)d\tau$$

$$y(T) = \int_0^T r(\tau)s(\tau)d\tau$$

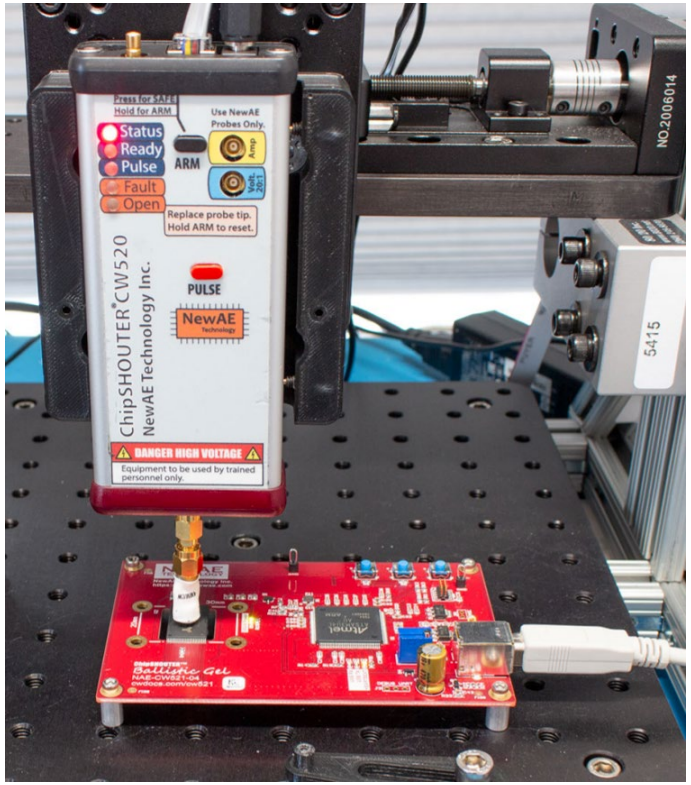
Some Open Problems I'll Discuss

- Fault Injection & Physical Effects
- Power Analysis
  - Optimum Measurement Information?
- Countermeasures
- Deep Learning Opportunities

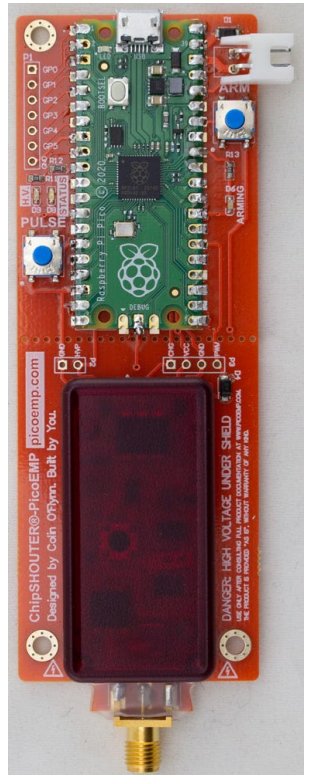
***NOTE IF YOU JUST HAVE SLIDES**: Demos associated with each slide. The demos are part of the open-source ChipWhisperer project to show you what you can accomplish with open-source/available material. Hardware is a combination of open source & proprietary depending on exact equipment.*

Fault Injection

- Physical causes of faults at silicon level.
- Counter-measures and detection?
- Fault prevention & detection in code?
- Equipment for performing fault analysis.



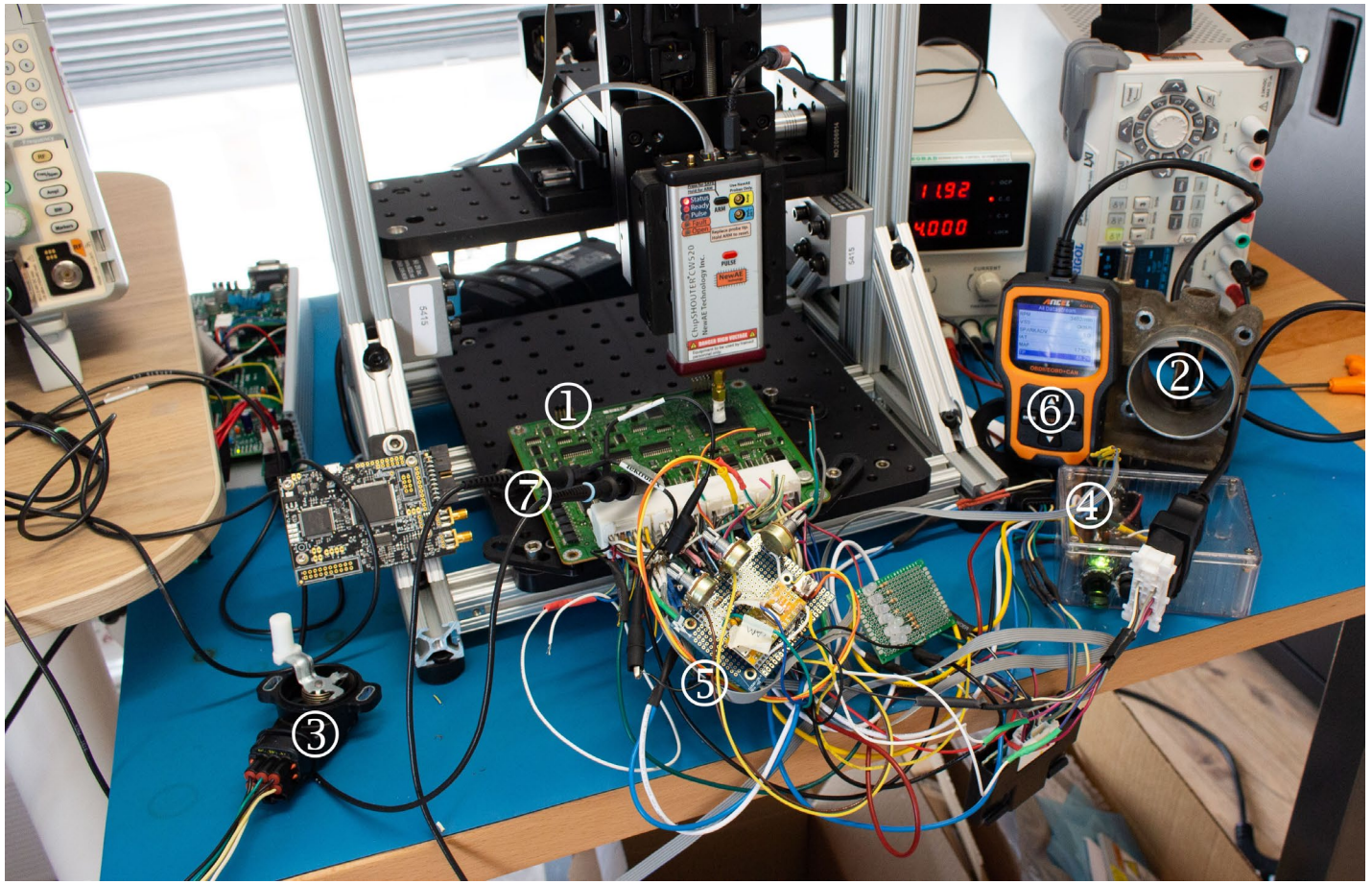
ChipSHOUTER ($3300)



PicoEMP (~$50)

Related Area – Safety Engineering

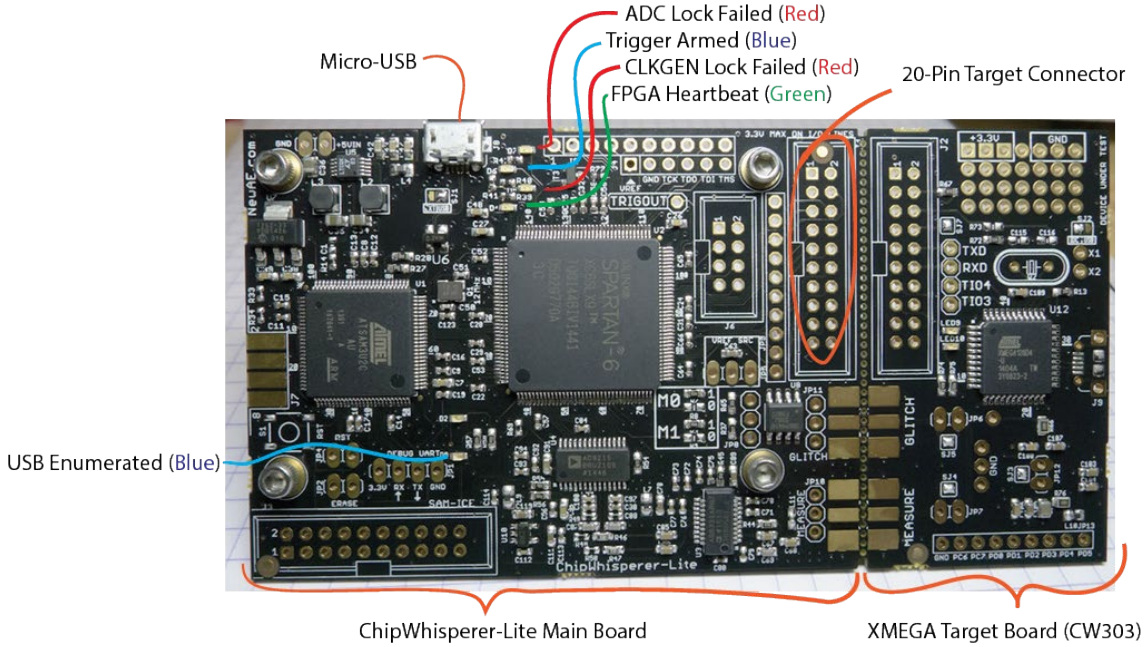
- Fault tolerant design relevant for automotive systems for many years.
- Can we use “security” fault injection for safety-testing?

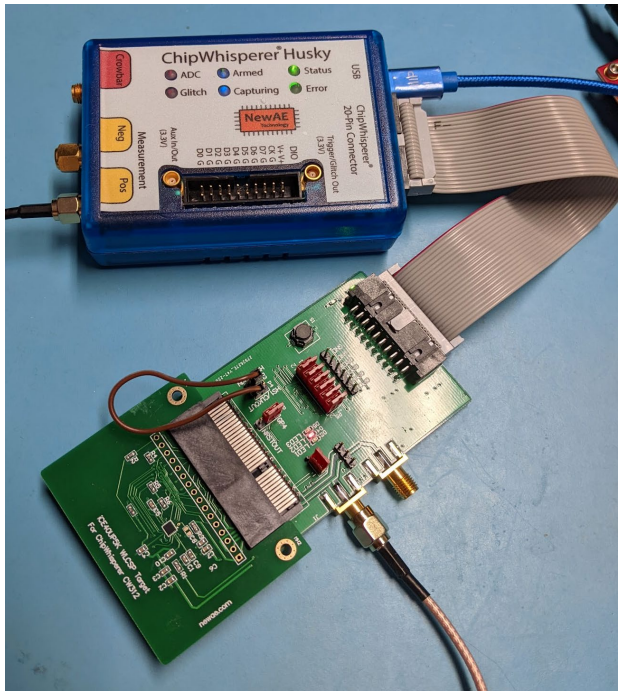


C. O’Flynn. “EMFI for Safety-Critical Testing of Automotive Systems”. 2021.

Power Analysis

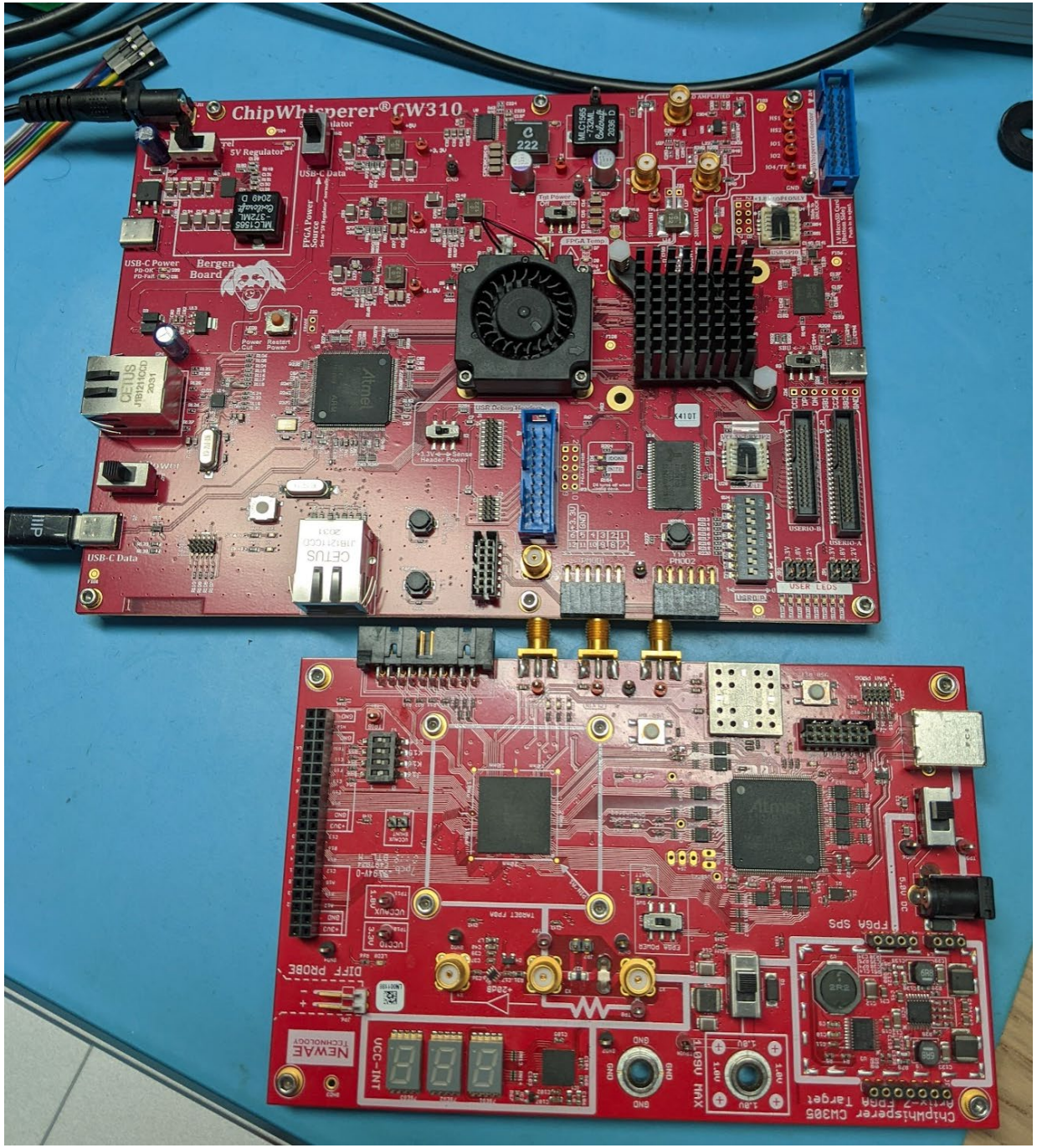
- Improving measurement methods (MIMO techniques?)
- Leakage evaluation of “pre-silicon” designs?
- Application to new algorithms (PQC) & “non-crypto” (PUF)?





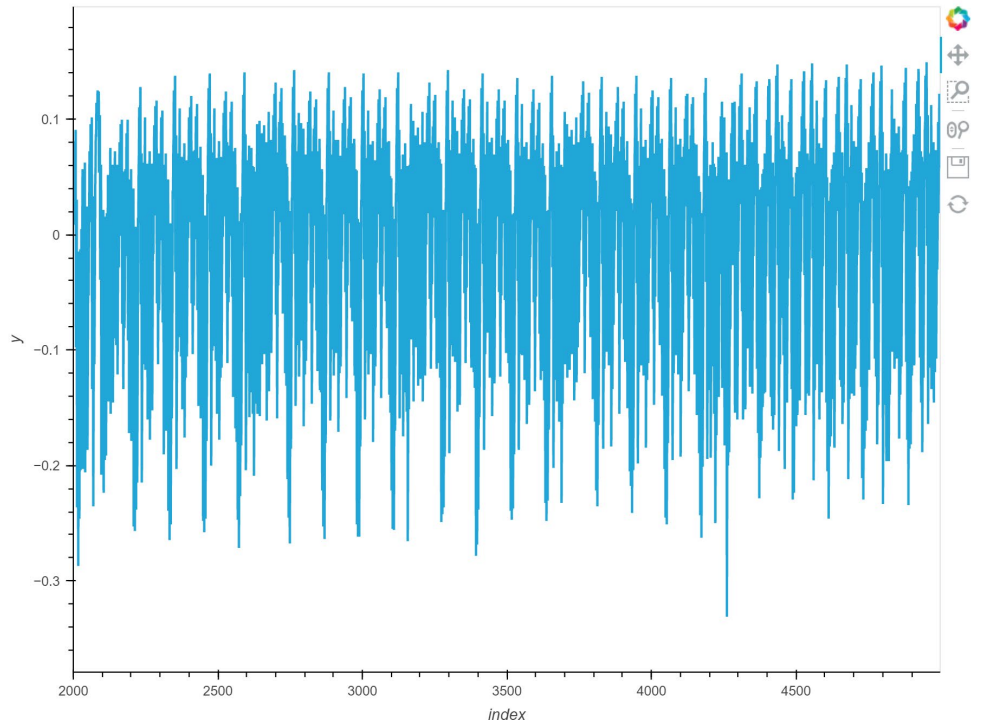
Countermeasures

- Firmware-level countermeasures?
- FPGA vs ASIC countermeasure results?
- Countermeasures with standard cells?
- Countermeasures with unique cells?



Deep Learning

- Reducing complexity of setups with deep learning?
- Deep learning for combination attacks (fault analysis + power?)
- Generation & sharing of relevant datasets.



Canadian Expertise in Hardware Security

Many exciting opportunities in “cybersecurity”. We can augment the existing expertise shown today by building bridges from existing research groups into cybersecurity topics, even if just an interested graduate student!

Questions, Thoughts, or Collaboration Proposals:

coflynn@newae.com