WPI

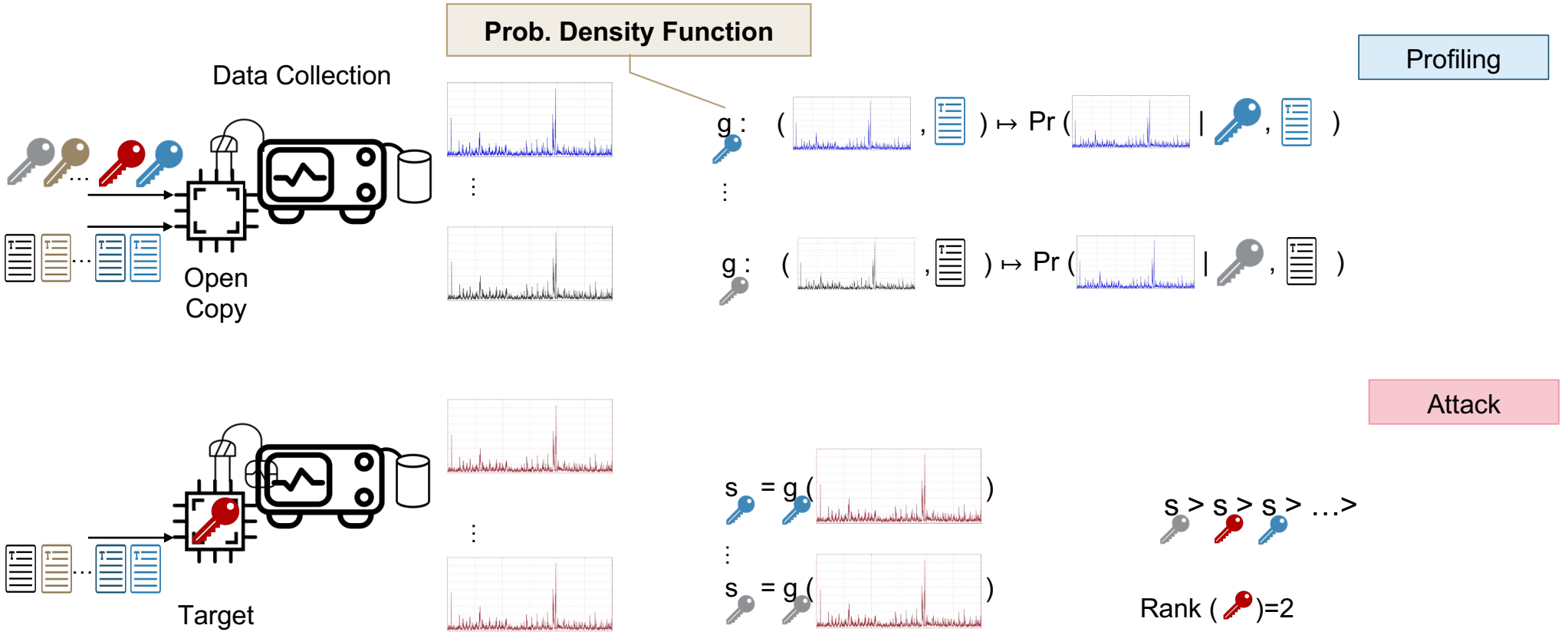
Uncertainty Estimation in Neural Network-enabled Side-channel Analysis and Links to Explainability

Seyedmohammad Nouraniboosjin (Mohammad Nour) and Fatemeh Ganji

Date: 4/18/2025

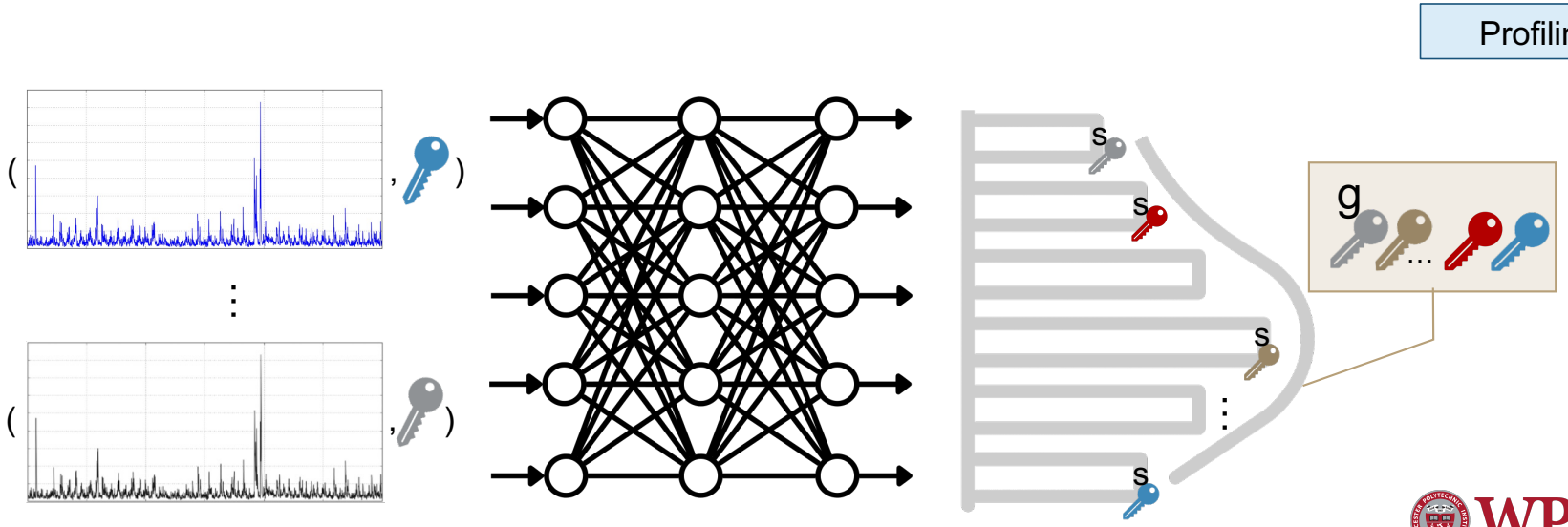
New England Hardware Security Day

Profiled SCA: in search for probability distributions!

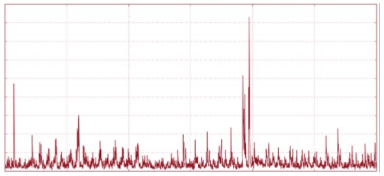


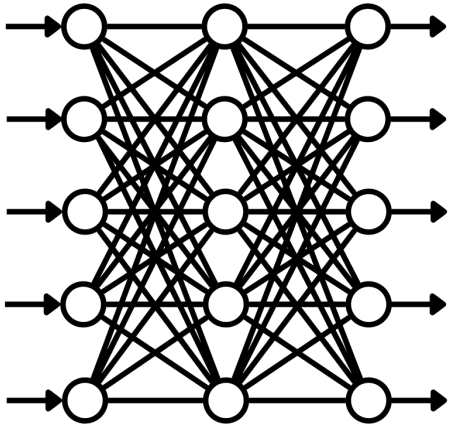
Let's bring in NNs

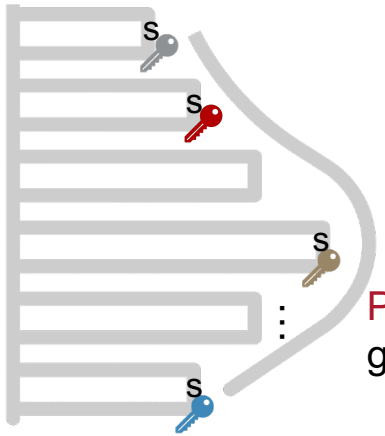
- Characterizing the leakage precisely through statistical techniques: costly in terms of the number of traces needed
- NN-assisted profiled SCA: effective against un-/protected cryptographic implementations, as well as noisy and shuffled traces



NN-assisted SCA







Attack

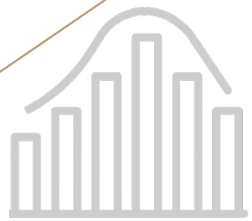
Rank ( )=3

Problem: a high prediction probability given to an incorrect key

NN model is uncertain in its predictions

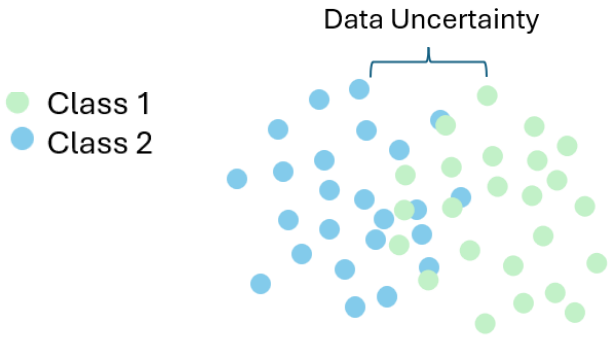
Entropy

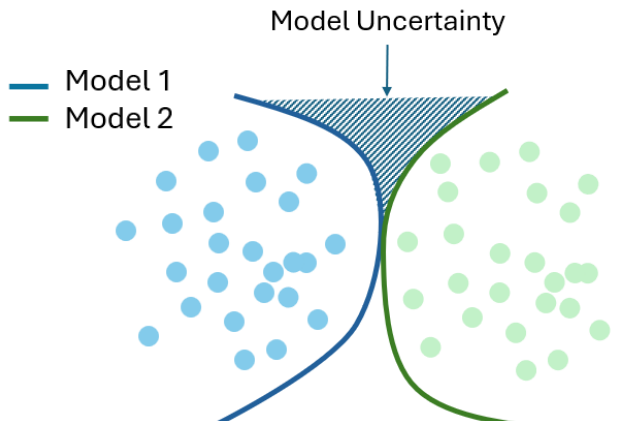
Predictive uncertainty= H ( )



WPI

High rank of the correct key: who is responsible?!

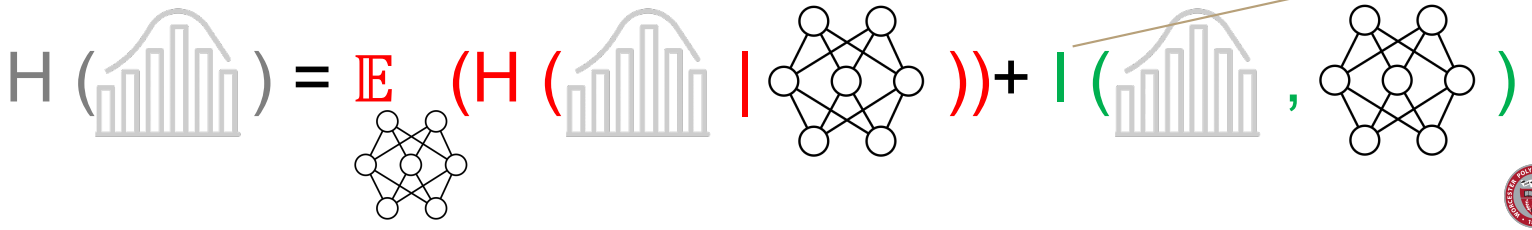




Aleatoric: not enough information

Epistemic: inappropriate model

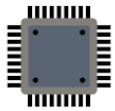
Predictive uncertainty= Aleatoric + Epistemic



WPI

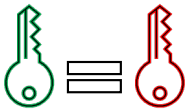
Results

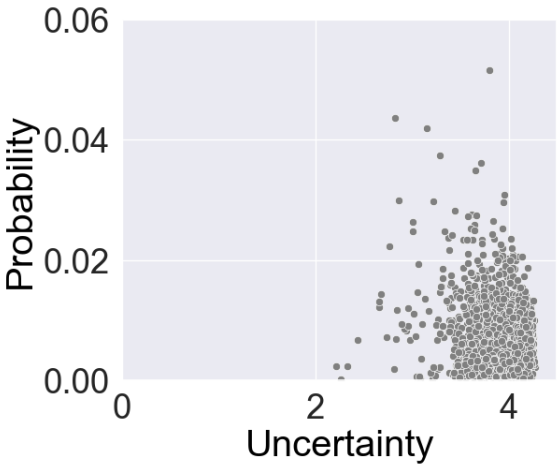
- ASCAD dataset [1]
- Model proposed in [2]

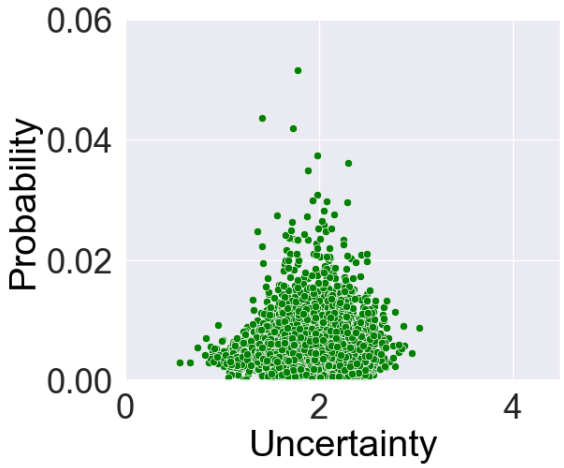

8-bit AVR

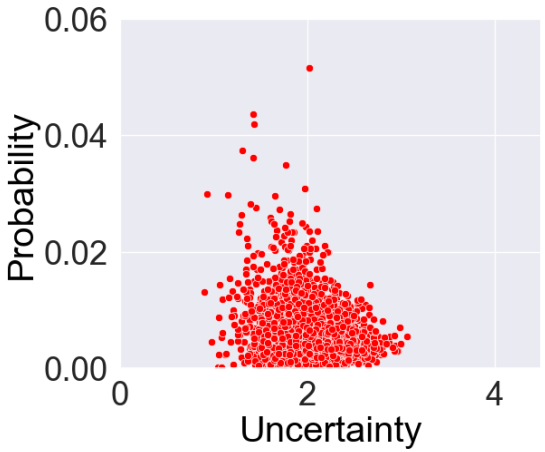

AES-128


Masked


Same key for attack phase







Each point shows the relation between the softmax output and the uncertainty for one attack trace

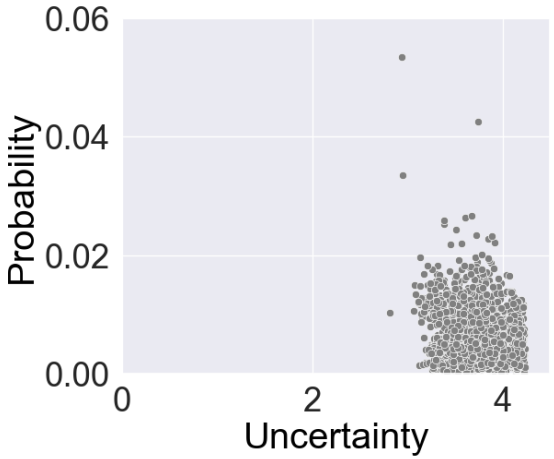
[1] Benadjila, Journal of Cryptographic Engineering, 2020. [2] Wouters, TCHES, 2020.

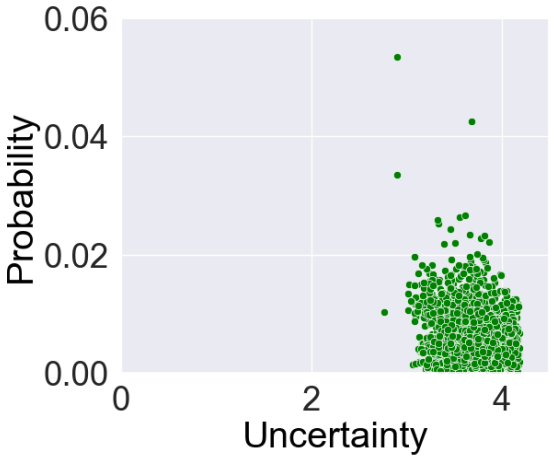
WPI

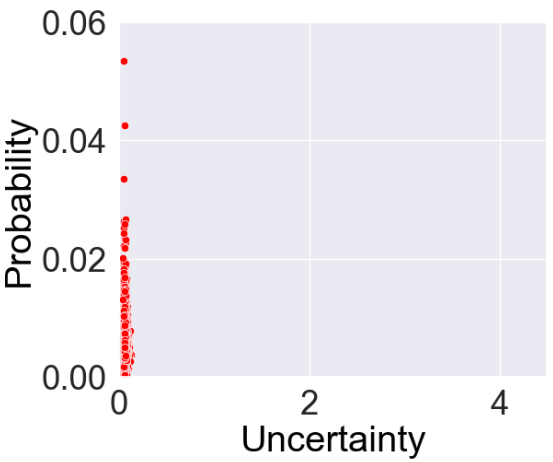
Results

- ASCAD-r dataset
- Model proposed in [1]

different key for attack phase







Better model is needed, less noisy data

[1] Wu, TETC, 2020.

WPI

Conclusion

- Introduced predictive uncertainty metric
- Demonstrated correlation between predictive uncertainty and key rank in NN-assisted SCA
  - Showing that higher uncertainty often leads to worse key guesses
- Linked explainability to uncertainty by analyzing effects of desynchronization, key randomization, and hyperparameters on model/data uncertainty
- More details in the pre-print
  - Proposed α-divergence to approximate probability distributions, addressing the limitations of Kullback-Leibler divergence in modeling side-channel leakage
  - using matrix-based Rényi α-entropy to handle high-dimensional SCA data, where traditional entropy estimation is infeasible
  - Used SHAP values to identify time samples in leakage traces contributing most to uncertainty, enabling more targeted SCA model optimization

Thank you

SNOURANIBOOSJIN@WPI.EDU