Name of this document: PC2\_CB2\_XMEGA\_2B\_M\_50k.docx

Dataset name: PC2\_CB2\_XMEGA\_2B\_M\_50k.npz

Dataset Link on OneDrive: [PC2\_CB2\_XMEGA\_2B\_M\_50k.npz](https://mailuc-my.sharepoint.com/personal/wang2ba_ucmail_uc_edu/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fwang2ba_ucmail_uc_edu%2FDocuments%2Fworks%2Fproposals%2F2021%2Fnsf_reu_rhest_program%2F2022_program%2Frhest_2022_program_shared_students%2Fprojects_documents%2Fproject1_2022_wang_emmert%2Fdatasets_joel%2FPC2_CB2_XMEGA_2B_M_50k.npz&parent=%2Fpersonal%2Fwang2ba_ucmail_uc_edu%2FDocuments%2Fworks%2Fproposals%2F2021%2Fnsf_reu_rhest_program%2F2022_program%2Frhest_2022_program_shared_students%2Fprojects_documents%2Fproject1_2022_wang_emmert%2Fdatasets_joel)

MD5 hash value of this dataset: 7550c054d9afa90254a9542c6f4a9f5e

Type: Power traces

Target Type: AVR XMEGA 8-bit microcontroller

Data Attributes in npz: (power\_trace, plain\_text, key)

No. of Traces: 50,000

Data Collected by: Joel Ward, REU student from Cedarville University

Email: joelbenward@gmail.com

Collection Date: 06/27/2022

Encryption Algorithm: AES-128, Masked

Encryption Implementation: SecAES-ATmega8515 written in assembly

Encryption Implementation Link: https://github.com/ANSSI-FR/secAES-ATmega8515

Key: 0x2b7e151628aed2a6abf7158809cf4f3c

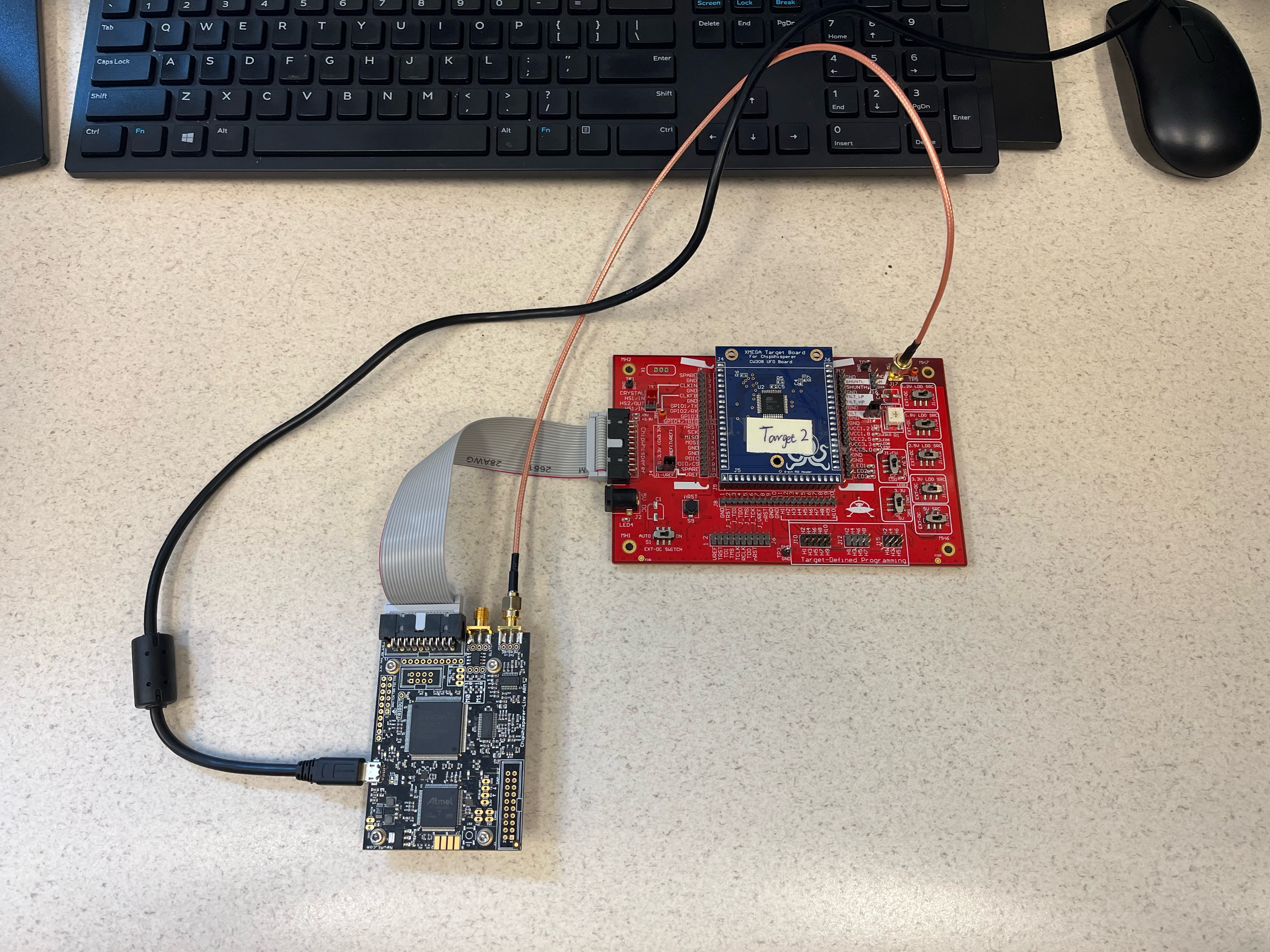
Collection Hardware

Computer: A desktop in Dr. Wang’s lab, Linux (Ubuntu 20.04.4), PC ID: PC2

Capture Board: Chipwhisperer Level-1 Kit (Jimmy’s Kit in Dr. Wang’s lab)

Target Board: Chipwhisperer Level-1 Kit (Jimmy’s Kit in Dr. Wang’s lab)

Picture of the data collection setup:

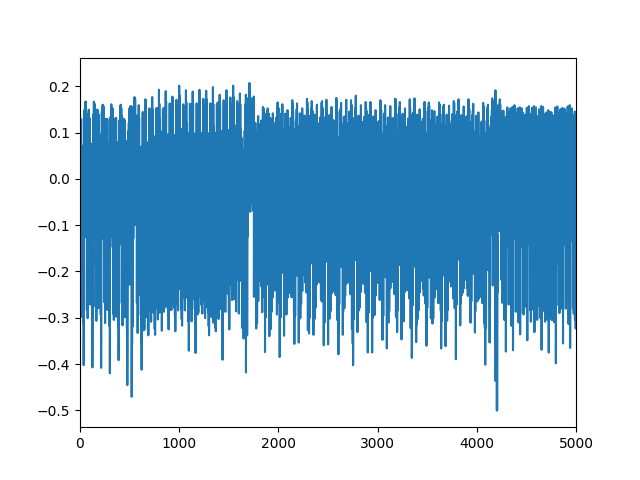


No. of samples/measurements in each trace: 20000

Points of Interests (1st Round of SubBytes): [1600, 4500]

Offset during data collection: 17,500 (default value, offset is needed for masked AES as Chipwhisperer only keeps up to 24,000 samples per trace while the 1st Round of SubBytes does not happen within the first 24,000 samples for masked AES)

A figure of a power trace with the first 5000 samples:



Analysis Results:

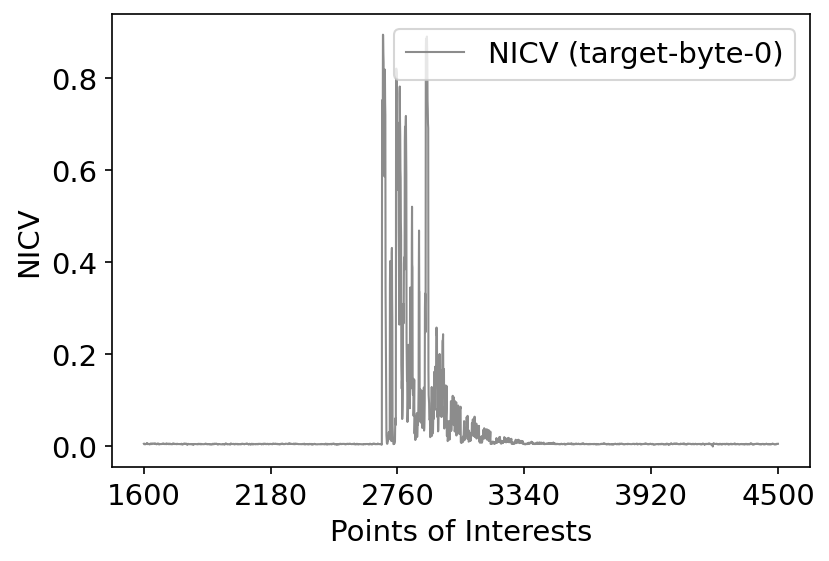
Results from Normalized Inner-Class Vector

Implementation link of NICV: https://github.com/UCdasec/TripletPower/tree/master/triplet/notebooks

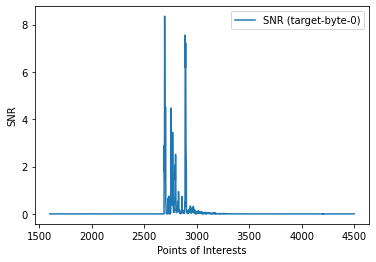
No. of traces used: 10000

Key Byte: 1st key byte (0x2b)

A figure of the NICV result:



SNR (attack window [1600, 4500]):



Results from Correlation Power Analysis

Implementation link of CPA: https://github.com/UCdasec/CrossSide/blob/main/cpa/verify\_the\_data\_CPA.ipynb

No of traces used: 100

Key Byte: 1st byte (0x2b)

Detailed results from CPA:

- Key guess: 0x2b

- Correlation: 0.9446525225032248

- Correct Key: 0x2b

Results from Deep-Learning Side-Channel Attacks using CNN

Implementation link of CNN: https://github.com/UCdasec/TripletPower/tree/master/cnn

No. of traces used for training: 40k

No. of traces used for testing: 10k

Key Byte: 1st byte (0x2b)

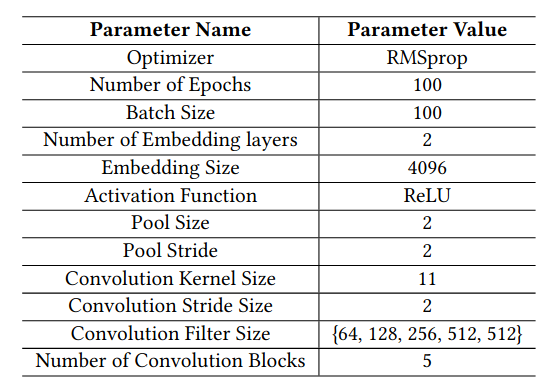
Leakage Model: Identity model (i.e., 256 classes)

Details of training and testing (please provide information here)

Training accuracy: 0.8534

Training time: ~1h 40

Key training hyperparameters:

 Test accuracy: 6.63%

A figure of key rank curve:

