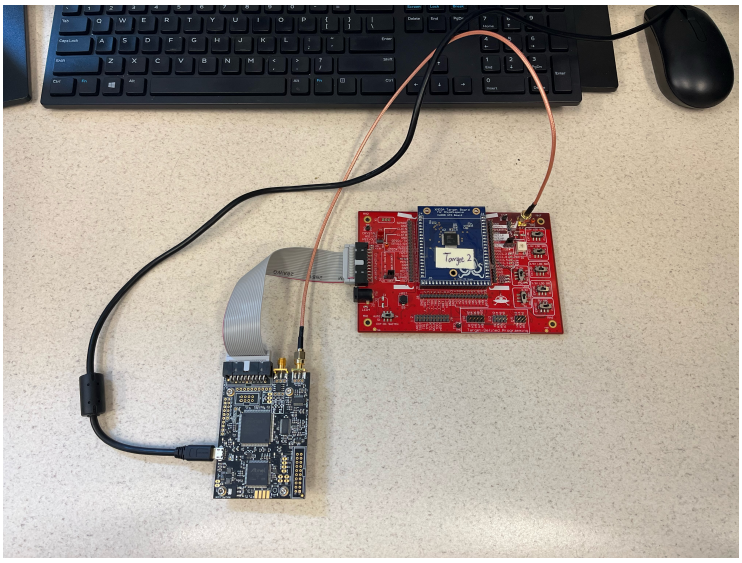
Name of this document: PC2_CB2_XMEGA_2B_M_50k_rewritten.pdf
Dataset name: PC2_CB2_XMEGA_2B_M_50k_rewritten.npz
Dataset Link on OneDrive: PC2_CB2_XMEGA_2B_M_50k_rewritten.npz

MD5 hash value of this dataset: 4c1384b3bf495dba062e4a15f967bf96
Type: Power traces
Target Type: AVR XMEGA 8-bit microcontroller

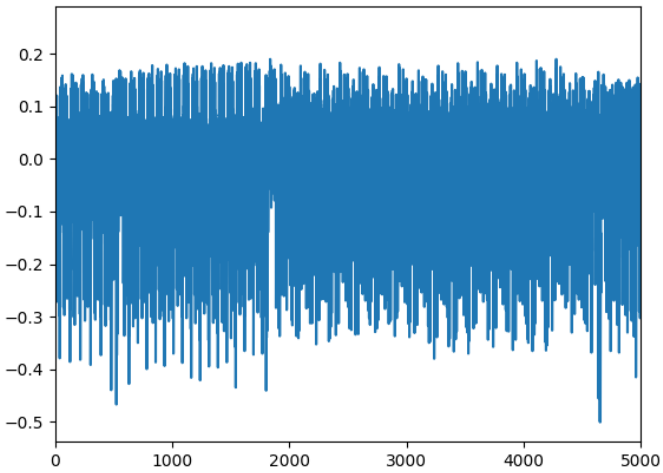
Data Attributes in npz: (key, plain_text, power_trace)
No. of Traces: 50,000
Data Collected by: Joel Ward, REU student from Cedarville University
Email: joelbenward@gmail.com
Collection Date: 06/21/2022

Encryption Algorithm: AES-128, Masked
Encryption Implementation: SecAES-ATmega8515 written in assembly with rewritten instructions
Encryption Implementation Link:
https://github.com/UCdasec/CrossSide/blob/main/code/instruction_rewriting/XMEGA/rewritten_instructions.S
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:

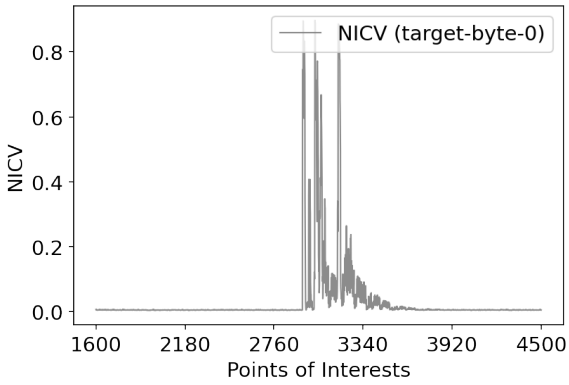


No. of samples/measurements in each trace: 20000
Points of Interests (1st Round of SubBytes): [1900, 4800]
Offset during data collection: 17,500 (default value, offset is needed for masked AES as Chipwhisperer only keeps up to 24,000 samples per trace while the 1st Round of SubBytes does not happen within the first 24,000 samples for masked AES)
A figure of a power trace with the first 5000 samples:

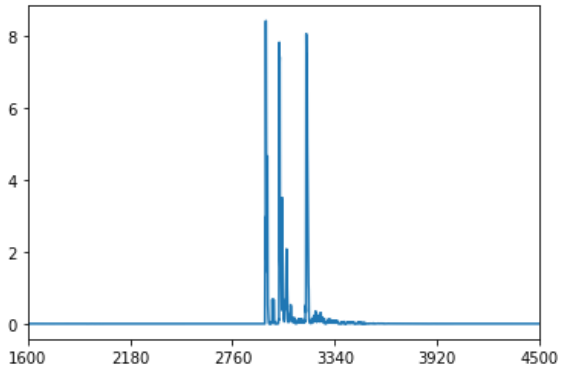


Analysis Results:

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/code/analysis/cpa/verify_the_data_CPA.ipynb
No of traces used: 100
Key Byte: 1st byte (0x2b)
Detailed results from CPA:

- Key guess: 0x2b
- Correlation: 0.951021388211042
- 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: 0.6936
Training time: ~1h 40
Key training hyperparameters:

Parameter Name	Parameter Value
Optimizer	RMSprop
Number of Epochs	100
Batch Size	100
Number of Embedding layers	2
Embedding Size	4096
Activation Function	ReLU
Pool Size	2
Pool Stride	2
Convolution Kernel Size	11
Convolution Stride Size	2
Convolution Filter Size	{64, 128, 256, 512, 512}
Number of Convolution Blocks	5

Test accuracy: 10.6%

A figure of key rank curve: