Remove Some Noise: On Pre-processing of Side-channel Measurements with Autoencoders

Lichao Wu & Stjepan Picek
Delft University of Technology, The Netherlands
Outlines

• Side-channel analysis
• Denoising autoencoder
• Denoising strategy: white-box setting
• Denoising strategy: black-box setting
• Conclusions and future works
Side Channel Analysis

Input plaintext \rightarrow Encryption \rightarrow Output Ciphertext

Side-channel Leakage \rightarrow Side-channel Analysis
Side Channel Analysis
Remove the noise

- Gaussian noise
- Misalignment
- Gaussian noise + Misalignment

→

- Averaging
- Static alignment

→

???
Denosing autoencoder

\[ \phi, \psi = \arg\min_{\phi, \psi} \| X - (\psi \circ \phi)X \|^2 \]
Denoising strategy: white-box settings

- Denoising strategy
- Validation & Benchmark
  - Gaussian noise
  - Desynchronization
  - Random delay interrupts
  - Combined noise
  - Uniformed noise
  - Clock jitters
  - Shuffling
Denoising strategy: white-box setting
Add Gaussian noise

Mean=0
Std=8
Remove Gaussian noise

Averaging (10 traces)

Denoising autoencoder
Add Desynchronization

Max=50
Remove desynchronization

Static alignment

Denoising autoencoder
Add random delay interrupts

Floating Mean method
Remove random delay interrupts

**Frequency analysis**

**Denoising autoencoder**
Add combined noise
Remove combined noise

Frequency analysis

Denoising autoencoder
Add combined noise - random keys
Remove combined noise - random keys

Frequency analysis

Denoising autoencoder
Denoising strategy: black-box settings

- Denoising strategy
- Remove Gaussian noise & Desynchronization
- Remove Gaussian noise & Desynchronization (combined training)
Denoising strategy: black-box setting
Remove Gaussian noise & Desynchronization

Guassian noise

Desynchronization
Remove Gaussian noise & Desynchronization (combined training)
Conclusions & Future Work

- CAE can remove/reduce various types of noise, countermeasures, and their combinations
- Our approaches is powerful for white box setting
- We also demostrate the potential in black-box settings

- Will be interesting to use CAE to deal with portability problem
- Using encoder of CAE to launch attacks (transfer learning)
Thanks for your attention!
Add uniform noise

Max=20
Min=-20
Remove uniform noise

Averaging (10 traces)

CAE
Add clock jitters

Max=4
Min=-4
Remove clock jitters

Frequency analysis

CAE
Add shuffling
Remove shuffling

+10,000 profiling traces

Denoising autoencoder