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

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

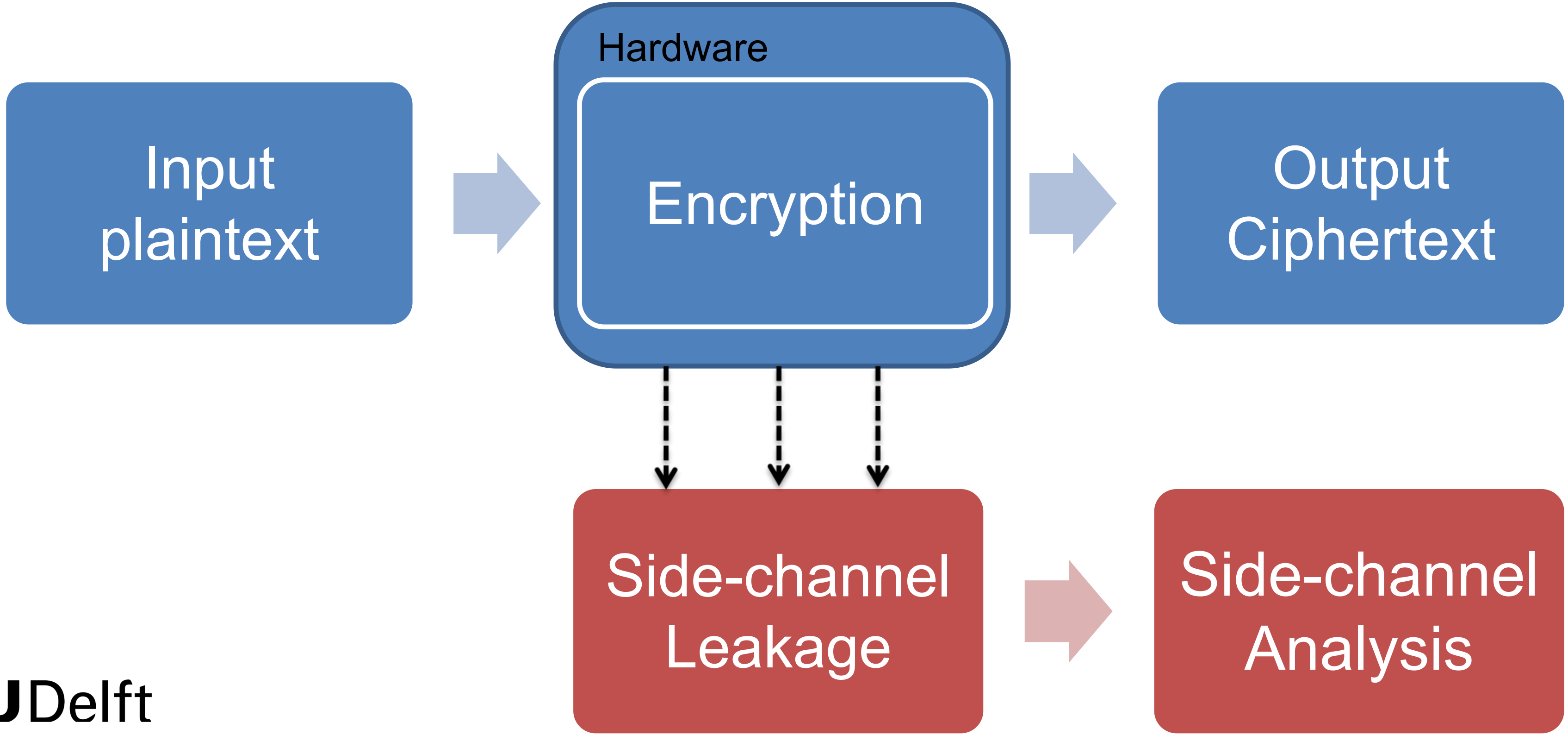
TU Delft

Outlines

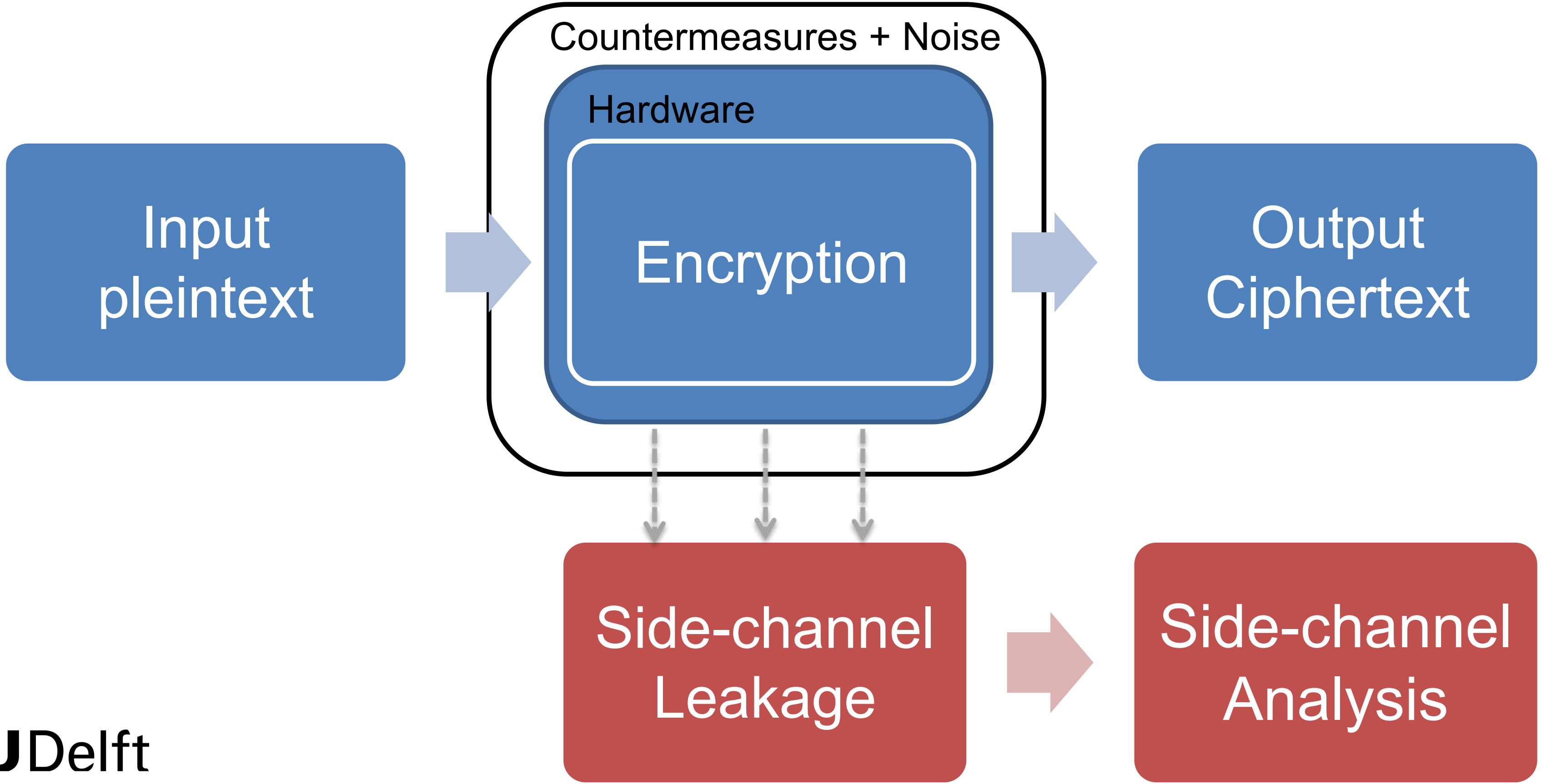
- Side-channel analysis
- Denoising autoencoder
- Denoising strategy: white-box setting
- Denoising strategy: black-box setting
- Conclusions and future works

TU Delft

Side Channel Analysis



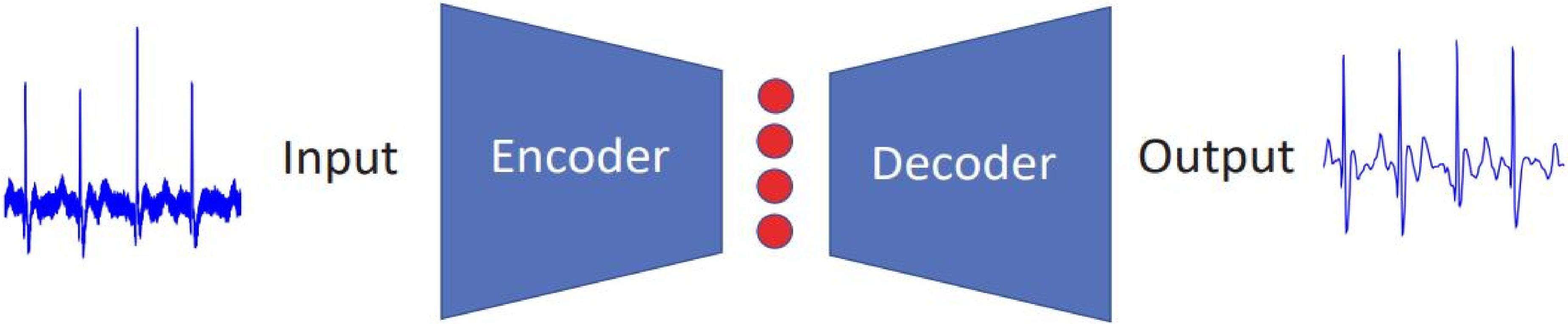
Side Channel Analysis



Remove the noise

Gaussian noise	→	Averaging
Misalignment	→	Static alignment
Gaussian noise + Misalignment	→	???

Denosing autoencoder



$$\phi, \psi = \arg\min_{\phi,\psi} \|X - (\psi \circ \phi)X\|^2$$

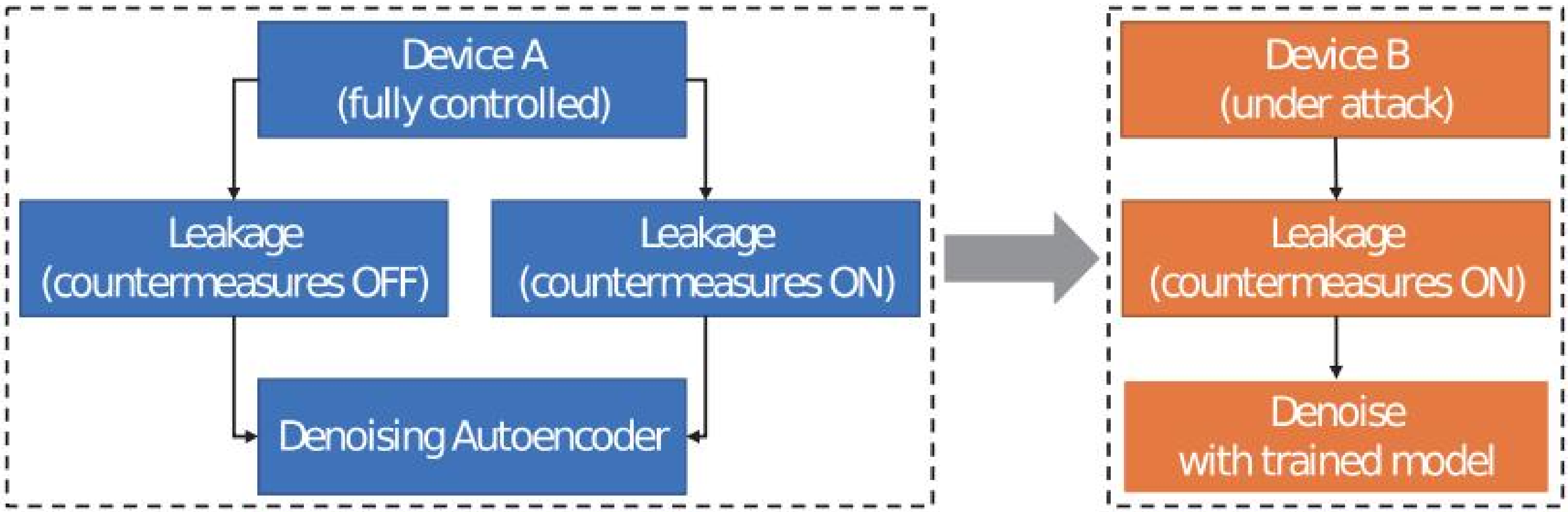
TU Delft

Denoising strategy: white-box settings

- Denoising strategy
- Validation & Benchmark
  - Gaussian noise
  - Desynchronization
  - Random delay interrupts
  - Combined noise
  - Uniformed noise
  - Clock jitters
  - Shuffling

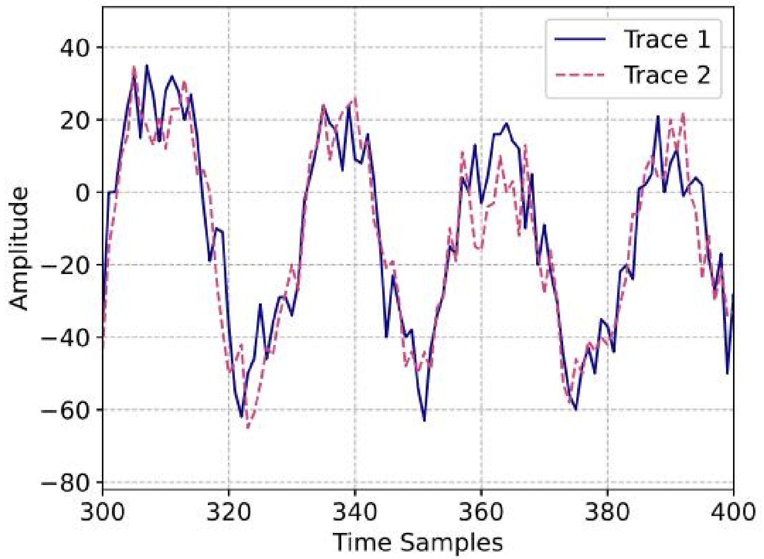
TU Delft

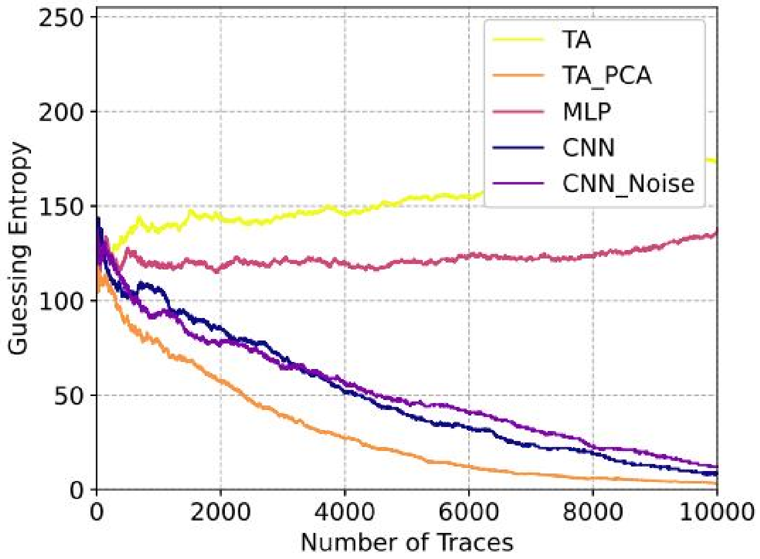
Denoising strategy: white-box setting



TU Delft

Add Guassian noise

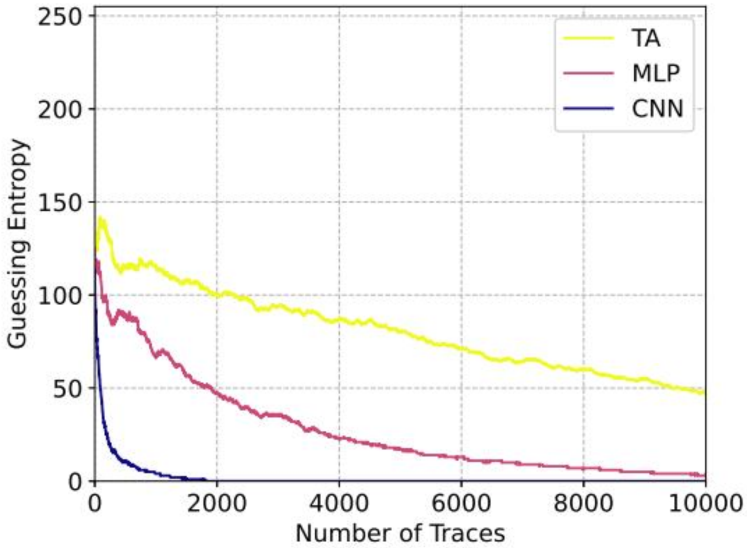




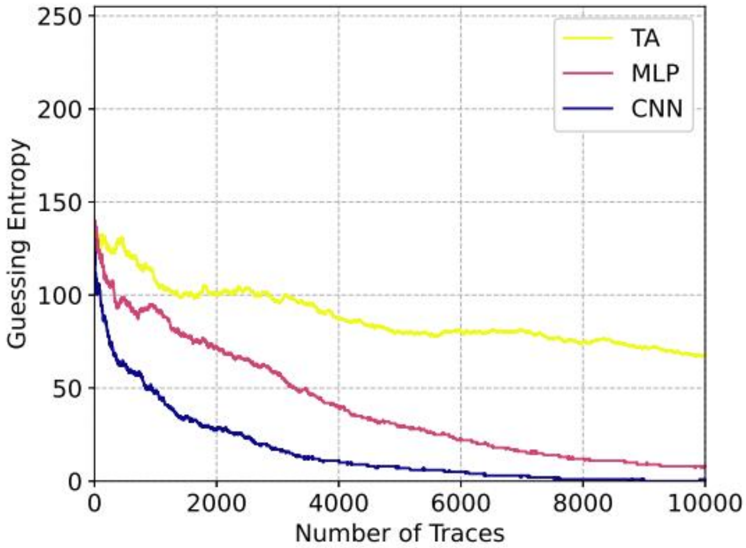
Mean=0
Std=8

TU Delft

Remove Guassian noise

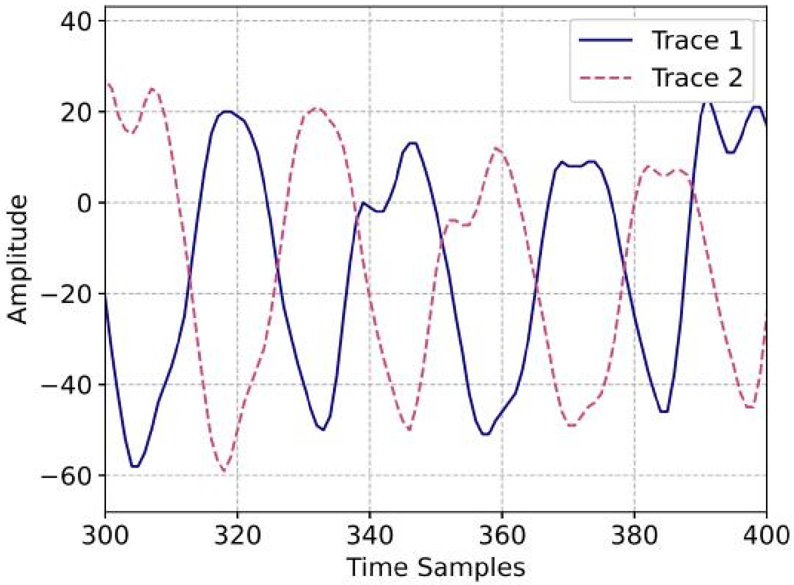


Averaging (10 traces)

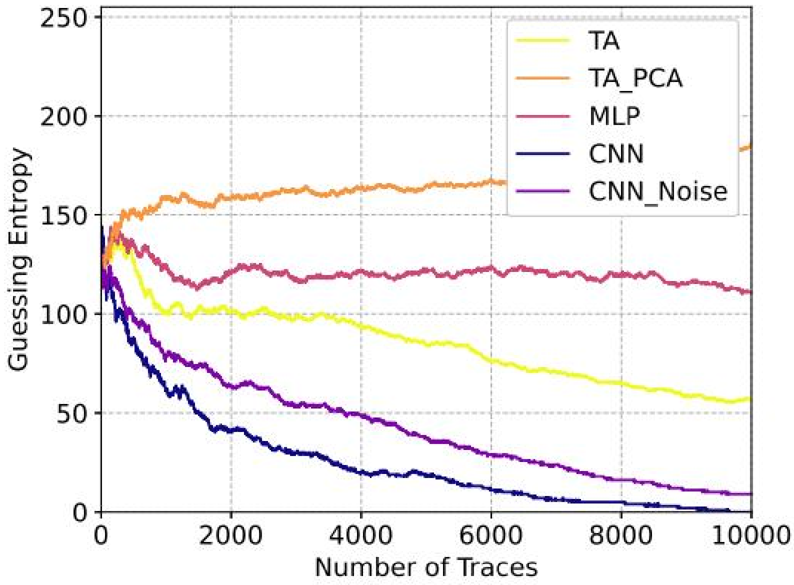


Denoising autoencoder

Add Desynchronization

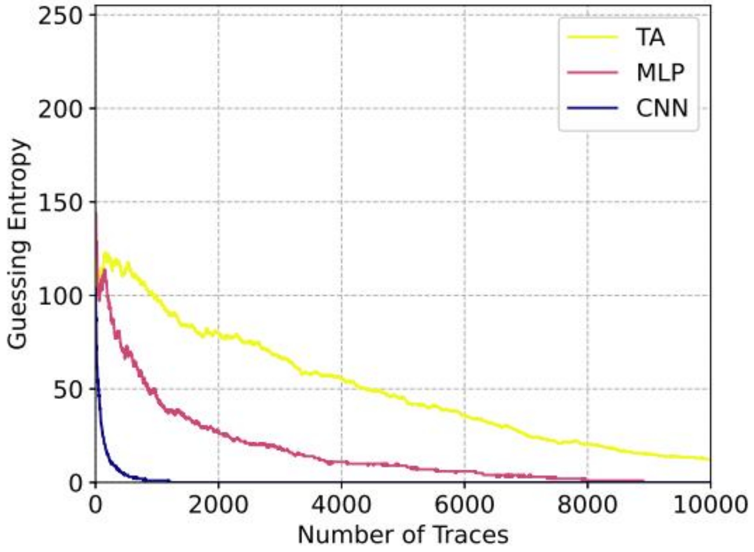


Max=50

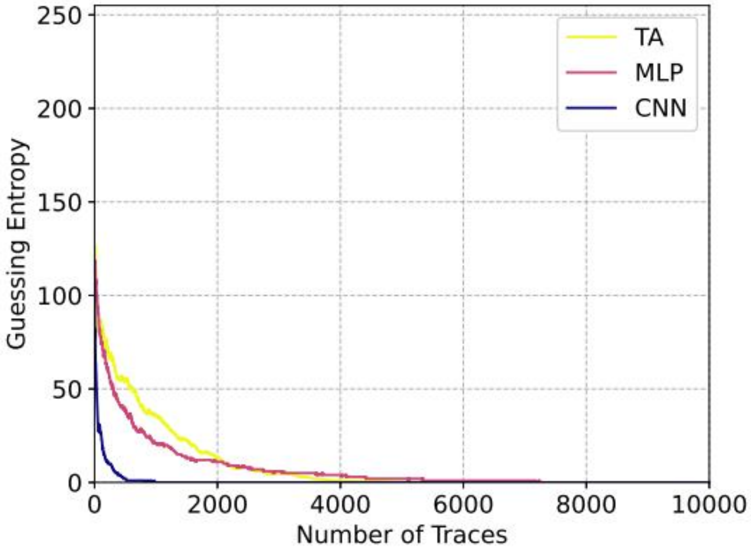


TU Delft

Remove desynchronization



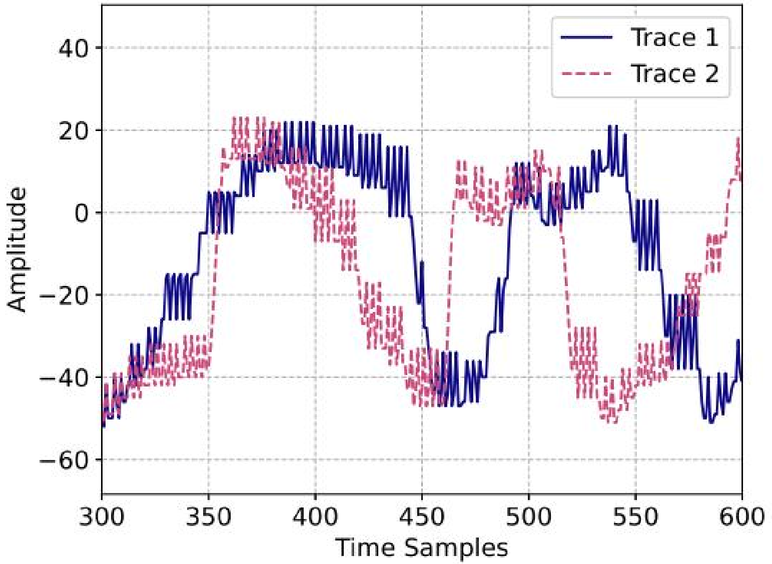
Static alignment



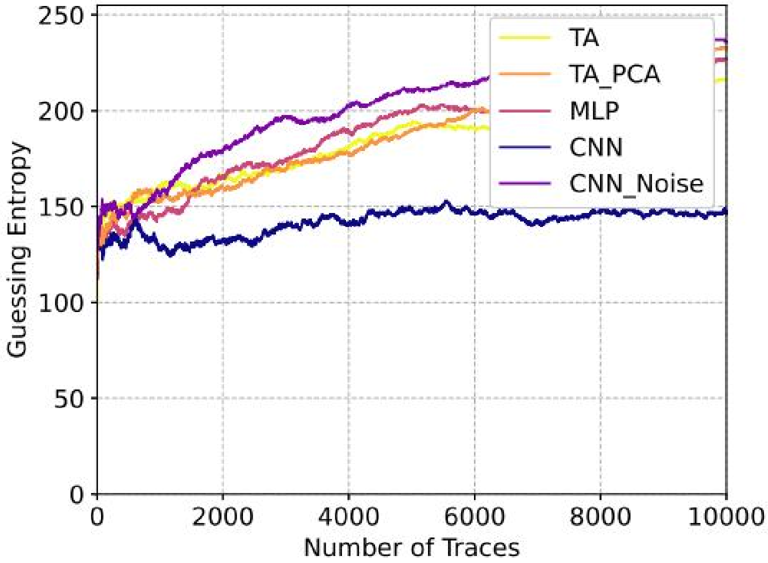
Denoising autoencoder

TU Delft

Add random delay interupts

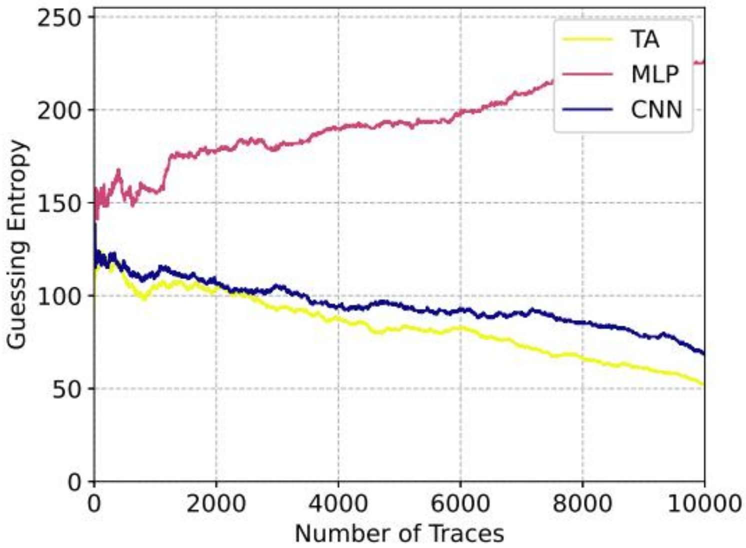


Floating Mean method

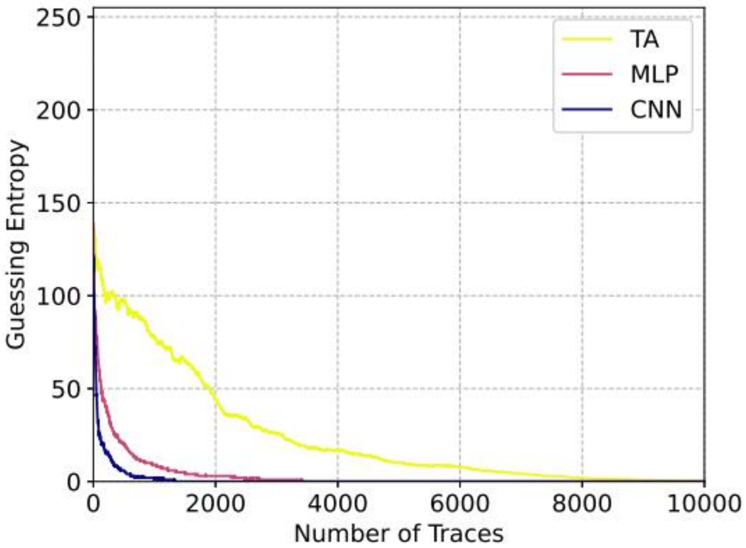


TU Delft

Remove random delay interupts



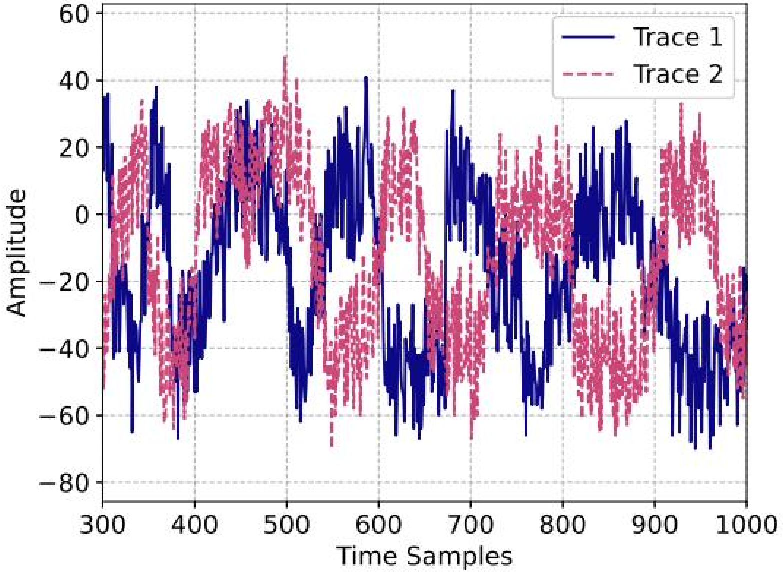
Frequency analysis

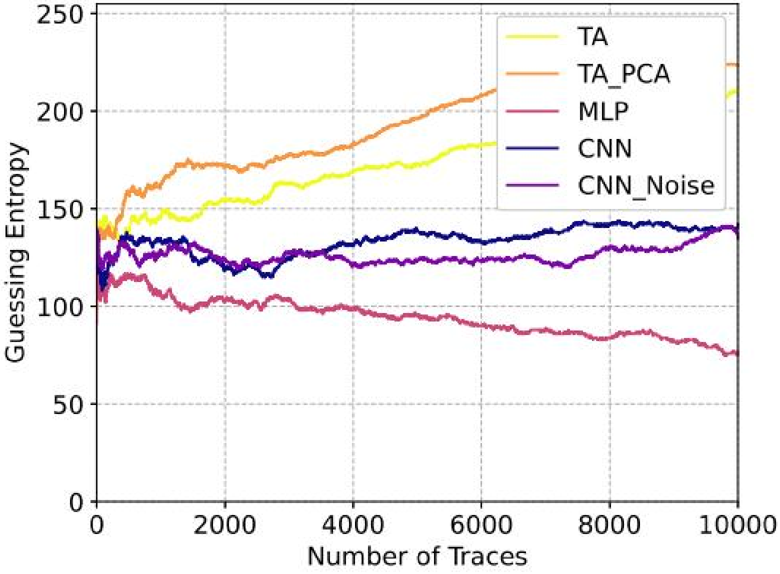


Denoising autoencoder

TUDelft

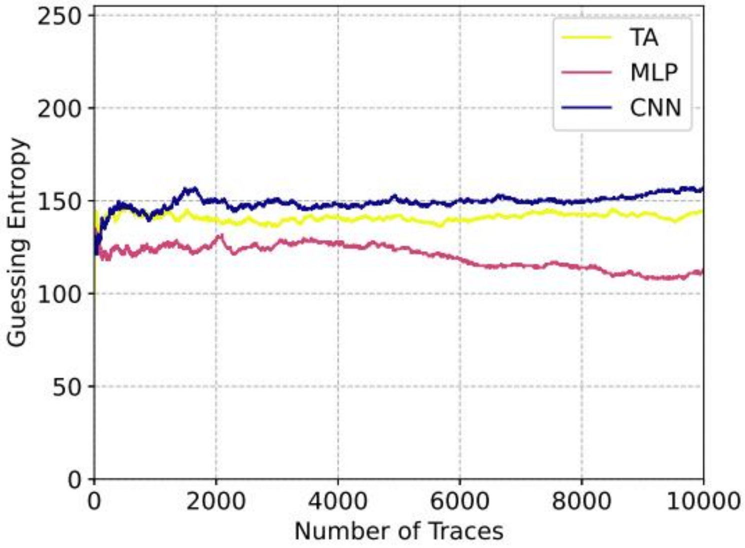
Add combined noise



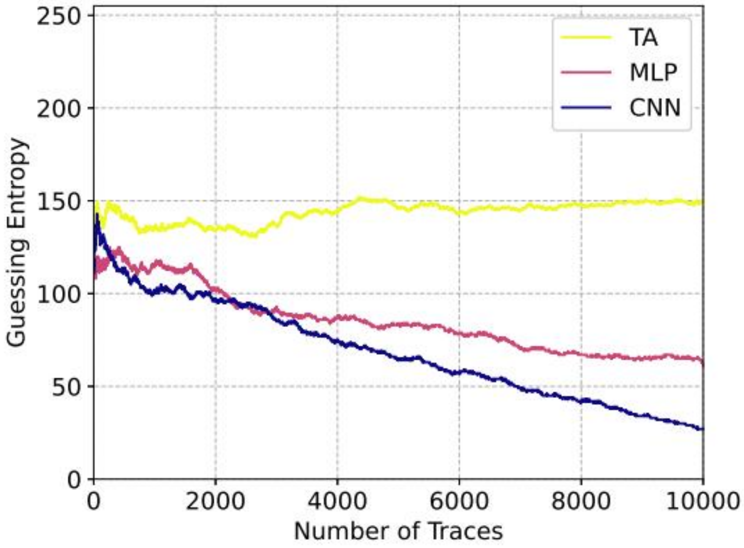


TUDelft

Remove combined noise



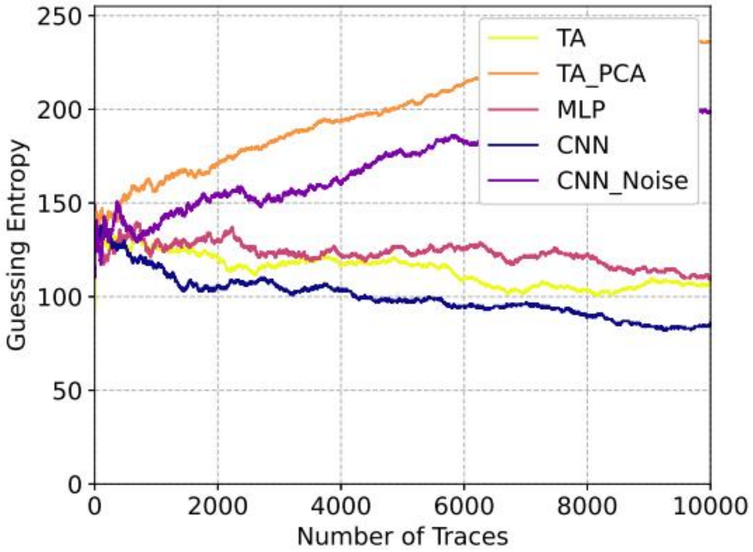
Frequency analysis



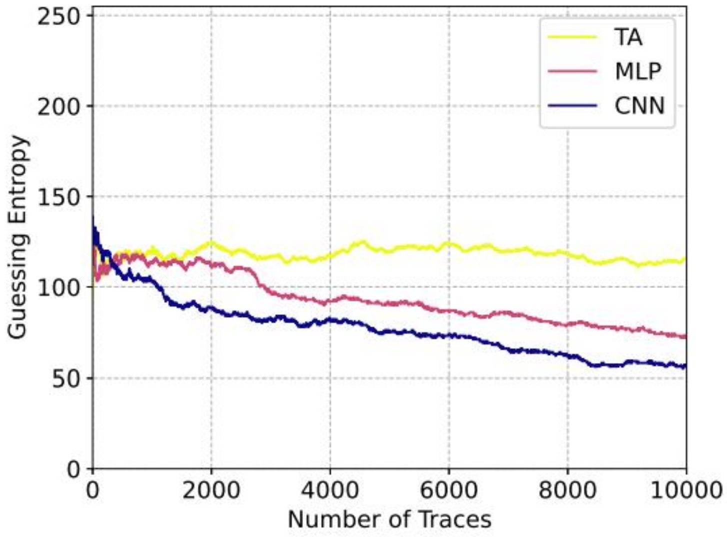
Denoising autoencoder

TUDelft

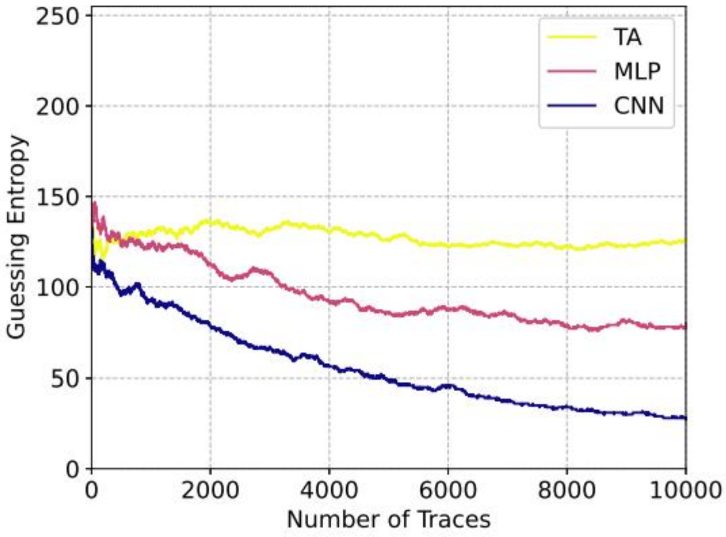
Add combined noise - random keys



Remove combined noise - random keys



Frequency analysis



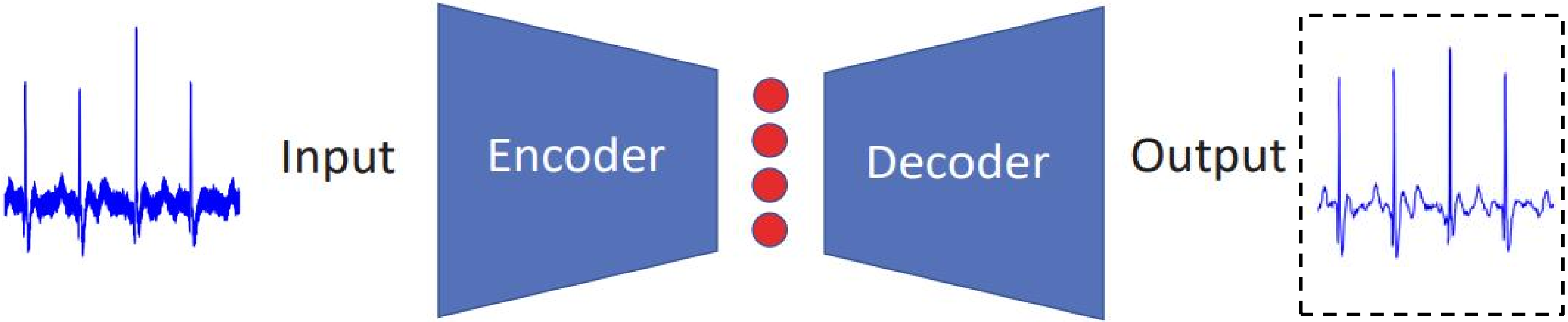
Denoising autoencoder

TUDelft

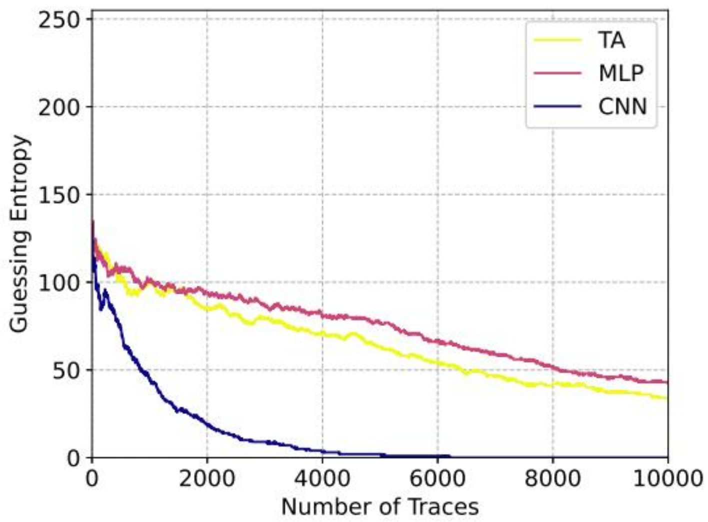
Denoising strategy: black-box settings

- Denoising strategy
- Remove Guassian noise & Desynchronization
- Remove Gaussian noise & Desynchronization (combined training)

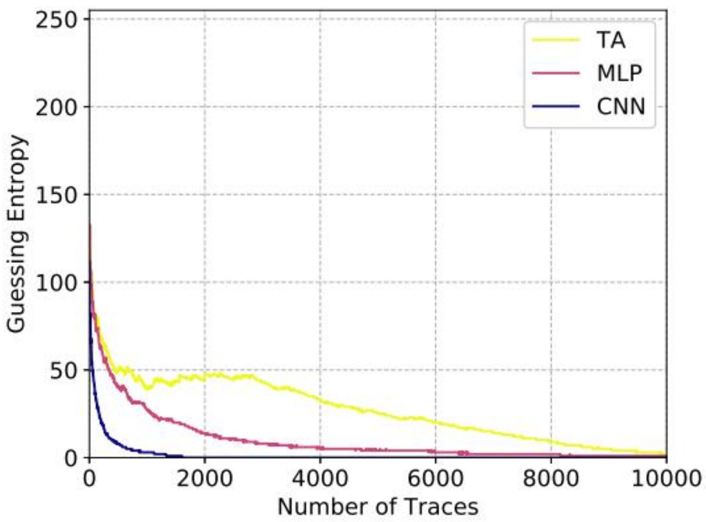
Denoising strategy: black-box setting



Remove Guassian noise & Desynchronization



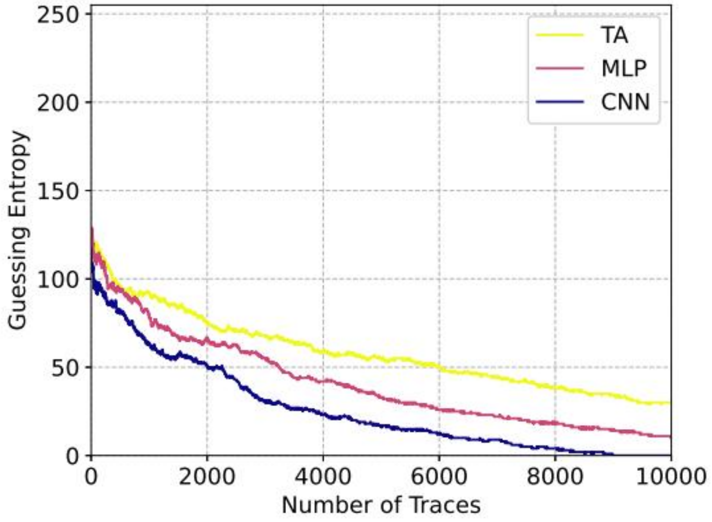
Guassian noise



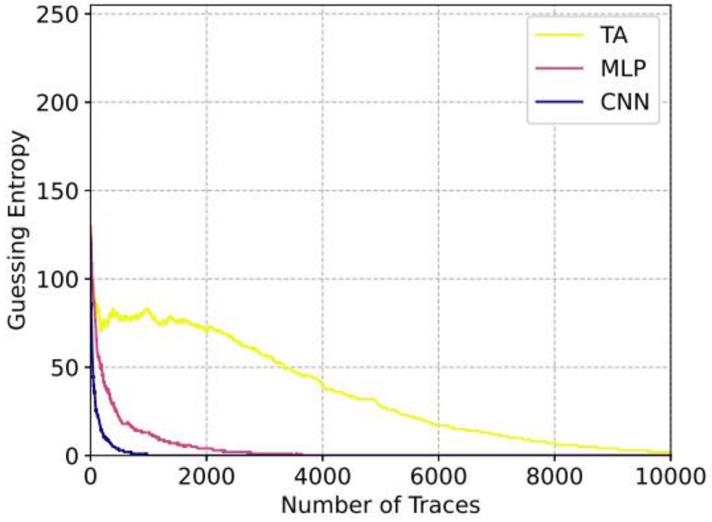
Desynchronization

TU Delft

Remove Gaussian noise & Desynchronization (combined training)



Guassian noise



Desynchronization

Conclusions & Future Work

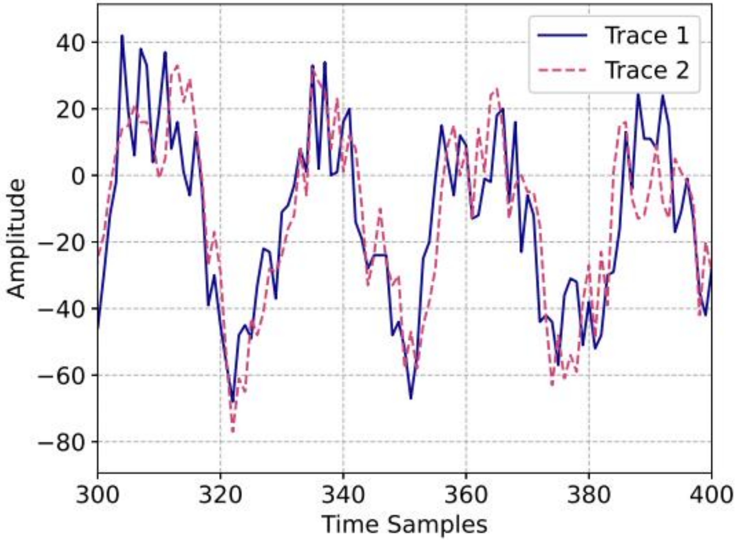
- CAE can remove/reduce various types of noise, countermeasures, and their conbinations
- Our approaches is powerful for white box setting
- We also demostrate the potential in black-box settings

- Will be interesting to use CAE to deal with portability problem
- Using encoder of CAE to launch attacks (transfer learning)

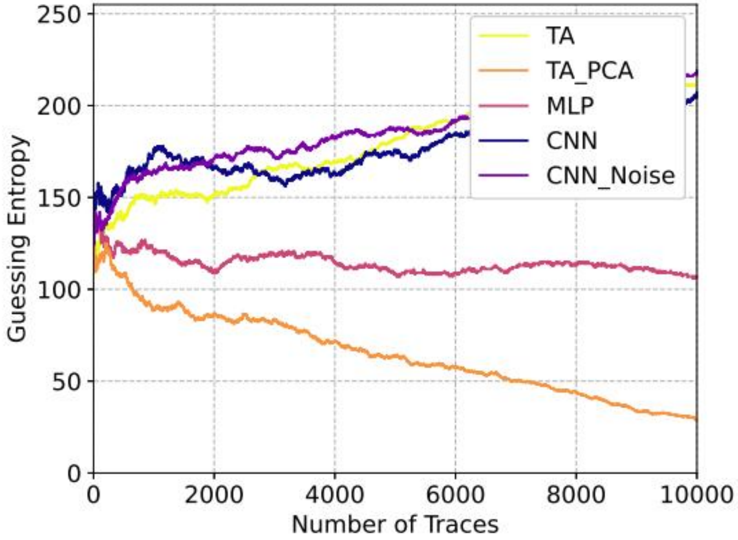
TU Delft

Thanks for your attention!

Add uniform noise

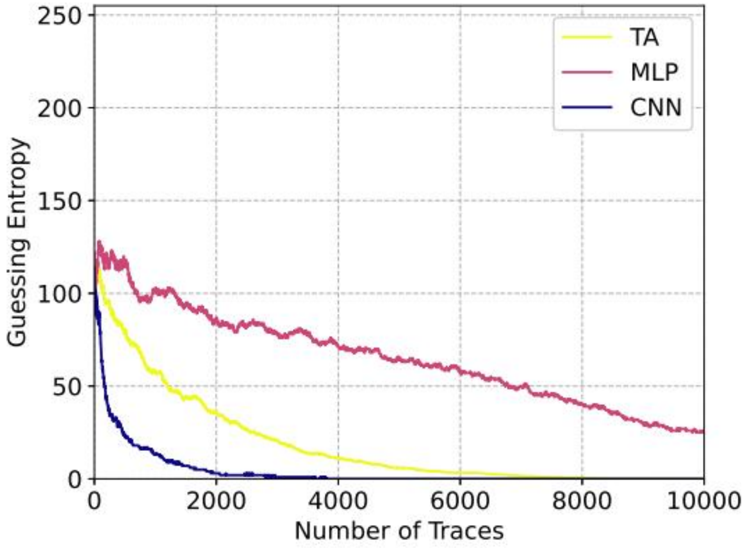


Max=20
Min=-20

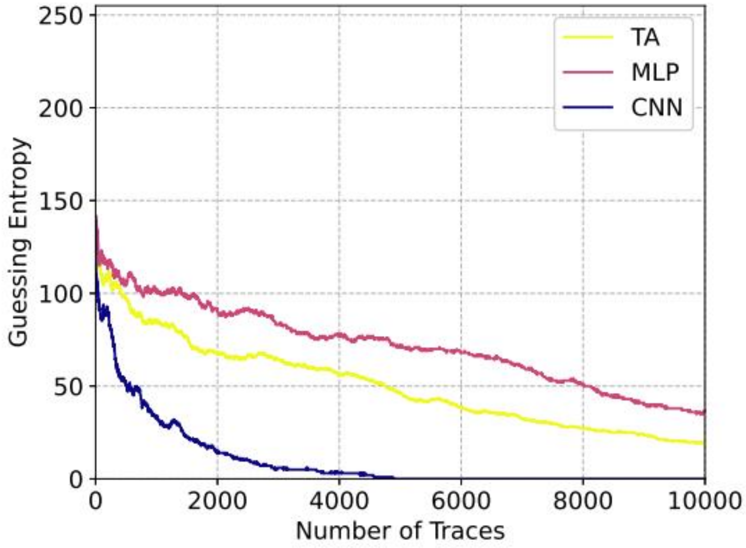


TU Delft

Remove uniform noise

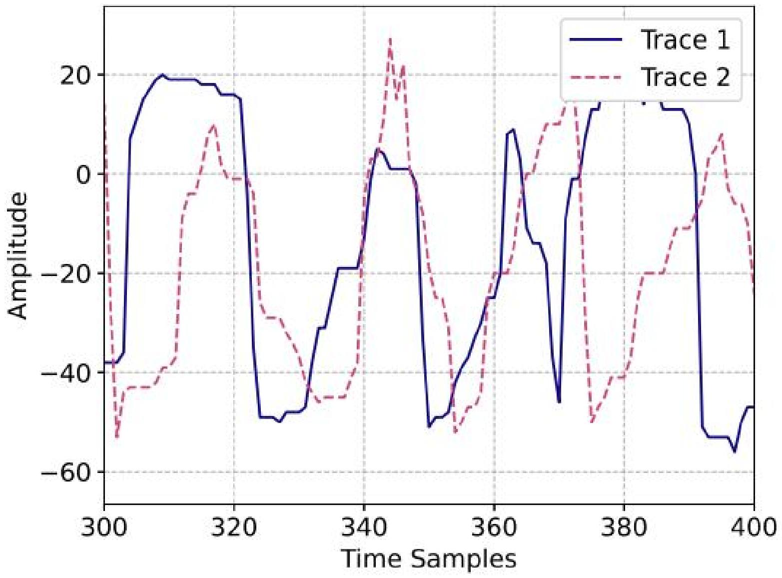


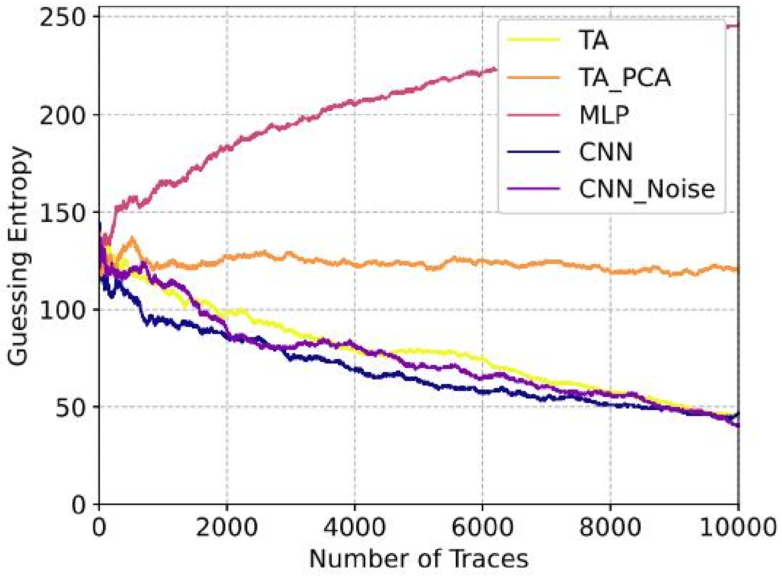
Averaging (10 traces)



CAE

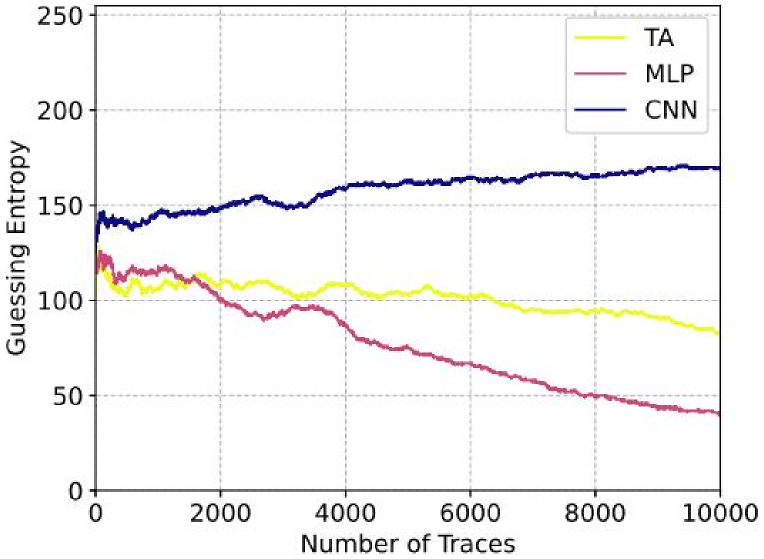
Add clock jitters



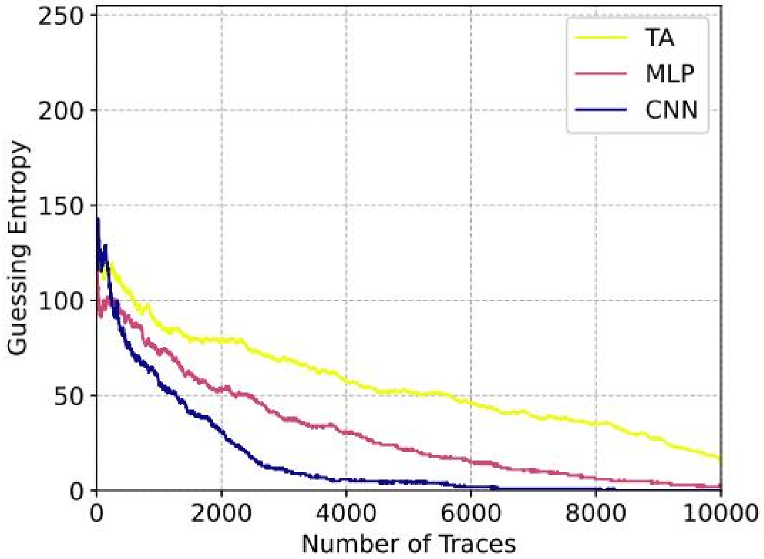


Max=4
Min=-4

Remove clock jitters



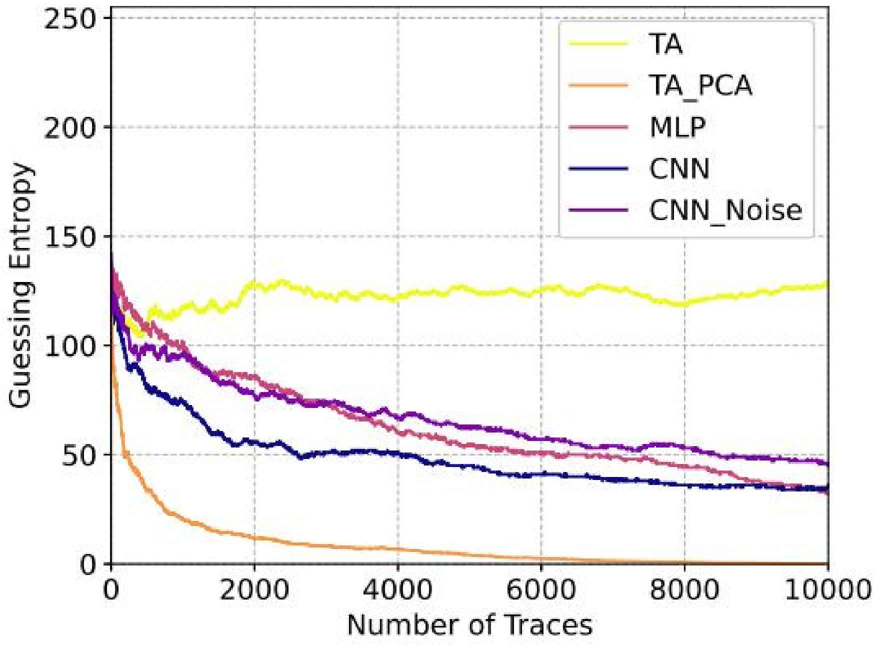
Frequency analysis



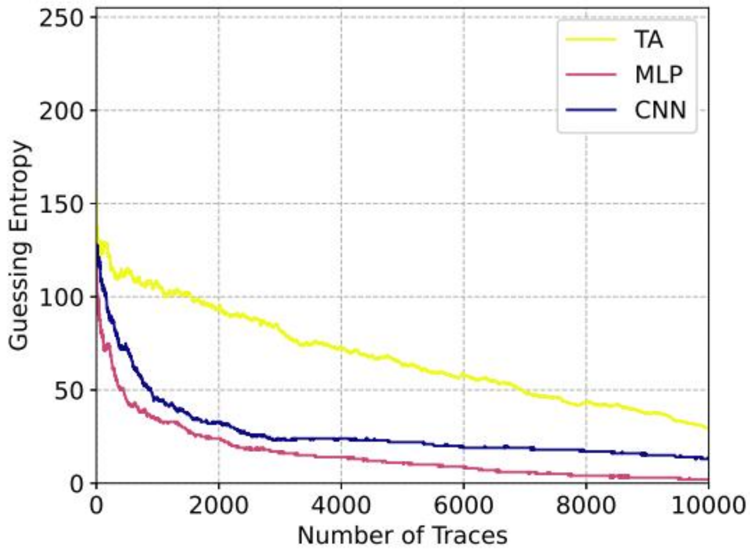
CA
E

TU Delft

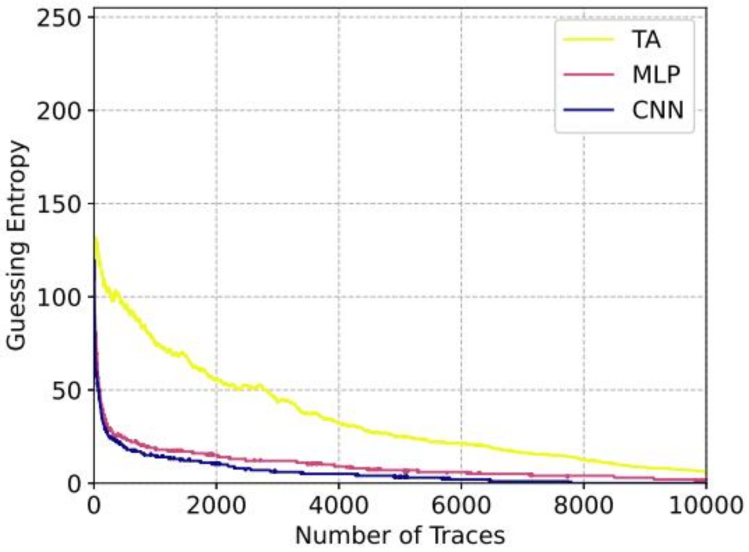
Add shuffling



Remove shuffling



+10,000 profiling traces



Denoising autoencoder

TU Delft