Improved Deep-Learning Side-Channel Attacks using Normalization layers

Damien Robissout, Gabriel Zaid,
Lilian Bossuet, Amaury Habrard
Laboratoire Hubert Curien, St-Etienne

Abstract

Recent papers used deep neural networks to improve profiled side-channel attacks. The networks were efficient even in the presence of countermeasures such as masking and de-synchronization. Nevertheless, tuning networks to perform specific tasks is difficult and there is still room for improvement. One of such improvements takes the form of normalization. Batch normalization is a well-known technique in the machine learning community to prevent the network from overfitting. In our work, using the ASCAD database, we test the addition of batch normalization layers and compare the results against the existing networks. Our experimental results cleary show that we significantly improve the attacks by reducing the number of traces needed to retrieve the key to about 1000 no matter the de-synchronization.