Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Security Assessment of Neuromorphic Hardware

With the rise in popularity of Machine Learning for diverse tasks the choice of hardware accelerator becomes more important. Examples for ASICs are Google's TPU or Intel's Loihi.

However, by implementing Neural Networks (NN) on edge devices they are also prune to Side Channel Analysis (SCA). Batina et al. (1) proved the feasability of differential power analysis on NN and Dubey et al. (2,3) additionally implemented a countermeasure.

The task of this work is to gather the state-of-the-art of hardware attacks on NN implementations in a survey.

References:

(1) CSINN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel; Batina, L.; Bhasin, S.; Jap, D. & Picek, S.; 28th USENIX Security Symposium (USENIX Security 19), 2019, 515-532

(2) MaskedNet: A Pathway for Secure Inference against Power Side-Channel Attacks; Dubey, A.; Cammarota, R. & Aysu, A.; arXiv preprint arXiv:1910.13063, 2019

(3) BoMaNet: Boolean Masking of an Entire Neural Network; Dubey, A.; Cammarota, R. & Aysu, A.;arXiv preprint arXiv:2006.09532, 2020;

Contact

Request Topic

Advisors

Matthias Probst