Wang, Junnian; Wang, Wan; Yu, Wenxin; Hu, Fanliang
Side-channel attacks based on dendrite network. (Chinese. English summary) Zbl 07448841
Nat. Sci. J. Xiangtan Univ. 43, No. 2, 16-30 (2021)

Summary: Due to the sensitivity of deep learning to the intrinsic characteristics of data, applying deep learning algorithms to the side channel analysis of hardware encryption chips can improve the efficiency and accuracy of the side channel analysis. However, the deep neural network learning algorithm is still a deep black box model with unknown nonlinear structure, and the model structure and performance are not necessarily optimal. In this paper, we propose a side channel analysis method based on dendritic networks, which outperforms deep learning networks in terms of system recognition capability and operational complexity due to the interpretability of the nonlinear structure inside the dendritic network.

On the CW308T-STM32F3 and ATXMEGA128D4 target board of ChipWhisperer side-channel analysis experimental platform, some side-channel analysis experiments are carried out for AES-128 encryption algorithm. The experimental results show that the dendritic network-based side channel analysis outperforms the deep learning networks in terms of model parameter scale, attack accuracy, and training time, such as multilayer perceptron, convolutional neural network, recurrent neural network, and other deep learning models.

MSC:
94A40 Channel models (including quantum) in information and communication theory
94A60 Cryptography
68T07 Artificial neural networks and deep learning

Keywords:
side-channel attacks; dendrite net; deep learning

Full Text: DOI