2025 IEEE 33rd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM) | 979-8-3315-0281-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/FCCM62733.2025.00028

Defending Side-Channel Attacks in Convolutional Neural Networks with Channel-Level Parallelization

Yankun Zhu, Ranxi Lin and Pingqiang Zhou
ShanghaiTech University, Shanghai, China
zhuyk, linrx2024, zhoupq@shanghaitech.edu.cn

***Abstract*—Side-channel attacks (SCAs) pose significant threats to the security of neural networks (NNs) deployed on hardware platforms, especially in cloud Field-Programmable Gate Array (FPGA) environments. This paper presents a novel approach to enhance the security of convolutional layers in NNs against SCAs by introducing a channel-level parallel structure. Compared with the original structure and the state-of-the-art masking technique, the channel-level parallel structure significantly reduces the success rate of SCAs (from 97.13% to 5.46% on average) and is able to be optimized for either low resource overhead (83.64% reduction) or good timing performance (83.01% improvement).**

I. Introduction

In recent years, stealing machine learning models from embedded systems has emerged as a significant topic in the field of hardware security. Both NN structure [1] and weights [2] face challenges from side channel leakage. Though existing methods like masking has been proven effective against such threat, it demands high randomness throughout the computation, adding resource consumption and control cost for NN. This paper proposes a new defense structure and focuses on the weight-stealing issues while avoiding the mentioned disadvantages.

II. Architecture and Experiments

Our work aims to develop a new defense method for quantized NNs that is easy to implement yet still secure against SCA attacks. We observe that the original parallel structure has its convolutional layer consisted of multiple kernels, each corresponding to a different channel. These kernels contain independent weights but share the same input while they compute the sum of products of the input and weights first and then pass through activation function. On that basis, we transform the structure so that the major step of performing MAC operations across n channels (in total N channels) is computed in parallel. Fig. 1 shows an example of the proposed channel-level parallel structure for convolutional layers where $n = N$. As it reorganizes the computation order to link a single input with weights from multiple channels, this structure is effective in preventing SCA.

We conduct experiments on PYNQ-Z2 platform to simulate a multi-tenant FPGA scenario just like [1]. We implement the first convolutional layer of three typical CNN models: VGG-16, Lenet5 and Mobilenet. The metrics for evaluation

This work was supported by the NSFC under award 62074100.

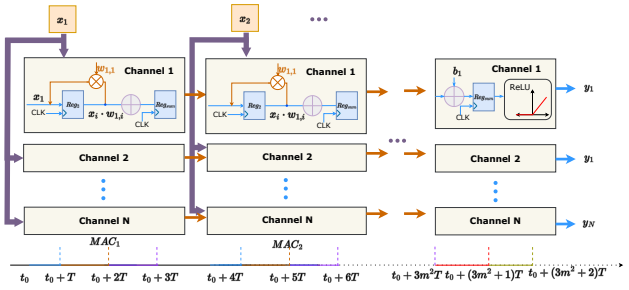

Fig. 1. The proposed channel-level parallel structure takes one element in the input matrix ($m \times m$ size) at a time and computes n channels' MACs in parallel ($n \leq N$, but here we assume $n = N$).

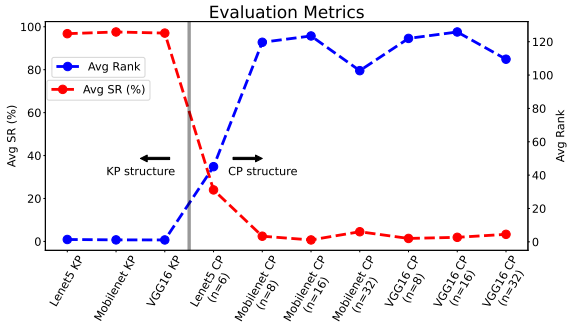

Fig. 2. Experimental results of metric evaluation.

are Average Success Rate ($Avg\ SR$) and Average Ranking ($Avg\ Rank$, the average ranking of correct weight among 256 guessed values like [2]). The results are shown in Fig. 2, implemented using either original kernel-level parallelism (KP) or channel-level parallelism (CP) with n representing the number of channels allocated for parallelism. When implemented by original KP structure, the $Avg\ SR$ exceeds 96% and the $Avg\ Rank$ is below 1.5. In contrast, the proposed CP structure exhibits a significantly lower $Avg\ SR$: approximately 24% for Lenet-5 and less than 4.5% for both VGG-16 and MobileNet. Furthermore, the $Avg\ Rank$ exceeds 45 for Lenet-5 and ranges from 100 to 130 for VGG-16 and MobileNet. The results show that our proposed structure can significantly influence the metrics and thus defend against SCA.

References

[1] Y. Zhang, et.al, "Stealing Neural Network Structure Through Remote FPGA Side-Channel Analysis," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4377-4388, 2021.
[2] Y. Gao, et.al, "NNLeak: An AI-Oriented DNN Model Extraction Attack through Multi-Stage Side Channel Analysis," *Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pp. 1-6, 2023.

2576-2621/25/$31.00 ©2025 IEEE
DOI 10.1109/FCCM62733.2025.00028