SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

OP-TEE を用いた隔離 AI ハードウェアアクセラレーションの実装評価
Implementation and Evaluation of Isolated AI hardware acceleration with OP-TEE

中井 綱人 *† 鈴木 大輔 * 藤野 毅 †
Tsunato Nakai Daisuke Suzuki Takeshi Fujino

キーワード Trusted Execution Environment，Arm TrustZone，OP-TEE，NVDLA，Zynq MPSoC

あらまし

深層学習などの大規模な機械学習の演算には，大量の計算量やメモリ量が必要であり，多くの場合，ハードウェアアクセラレーションが行われている．特に，組み込み機器向けには，リアルタイム性や消費電力も考慮して，機械学習の演算に特化した AI ハードウェアアクセラレータが数多く開発されている．

機械学習の演算には，モデル情報やデータの機密性や実行タスクの完全性を目的とした隔離実行が求められる場合がある．例えば，生体認証等の重要な機能に機械学習を用いる場合は，通常のアプリケーションから隔離された信頼できる環境で実行される必要がある．また，知的財産になりうるモデル情報やプライバシーに関するデータを信頼できる環境でのみ処理することが考えられる．

ハードウェアアクセラレーションを用いた機械学習演算の隔離実行は，専用回路を組み込んだ独自のアーキテクチャで実現することが多い．例えば，Apple 社のデバイスでは，Face ID 等のセキュリティ・プライバシーに関わる機械学習演算を，メインプロセッサとは別のセキュリティ専用プロセッサ (Secure Enclave) が AI ハードウェアアクセラレータ (Neural Engine) にアクセスすることで隔離実行を実現している．Hua らが提案する方式 [1] においても，オープンソースの AI ハードウェアアクセラレータ (CHaiDNN) の周辺に，独自の命令セットを持つコントローラを実装して，隔離実行を実現している．

オープンソースや汎用のセキュリティ機能による AI ハードウェアアクセラレーションの隔離実行に関する先行研究として，Xie ら [2] は，設計コストを抑えた方式を提案しているが，その実装や評価は十分に示されていない．Xie らの方式は，信頼できる環境として Intel SGX を活用し，オープンソースの AI ハードウェアアクセラレータ (VTA) とのアクセスに，専用のセキュリティI/F 回路を差し込むことで，VTA の隔離実行を実現している．ただし，VTA とセキュリティI/F 回路のみが実装評価されており，Intel SGX との接続部分の実装やその評価については示されていない．

本論文では，オープンソースや汎用のセキュリティ機能を活用した AI ハードウェアアクセラレータの隔離実行に関する実装評価を報告する．実装する方式は，信頼できる環境としてオープンソースの OP-TEE を活用し，NVIDIA 社のオープンソース AI ハードウェアアクセラレータ NVDLA を隔離実行する．実装には，Xilinx 社の SoC FPGA である Zynq UltraScale+ MPSoC を採用し，提供されるセキュリティ機能も隔離実行に活用した．

本論文の寄与は，オープンソースや汎用セキュリティ機能を用いた AI ハードウェアアクセラレーションの隔離実行に関する実装評価にある．

参考文献

[1] Hua, Weizhe, et al.,“Guardnn: Secure dnn accelerator for privacy-preserving deep learning,” arXiv preprint arXiv:2008.11632 (2020)

[2] Xie, Peichen, et al.,“Customizing Trusted AI Accelerators for Efficient Privacy-Preserving Machine Learning,” arXiv preprint arXiv:2011.06376 (2020).

* 三菱電機株式会社 情報技術総合研究所, 〒 247-8501 神奈川県鎌倉市大船 5-1-1 Mitsubishi Electric Corporation, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan Nakai.Tsunato@dy.MitsubishiElectric.co.jp
† 立命館大学, 〒 525-8577 滋賀県草津市野路東 1-1-1 Ritsumeikan University, 1-1-1, Nojihigashi, Kusatsu, Shiga, 525-8577, Japan fujino@se.ritsumei.ac.jp