Title: Security Challenges in Automated AI Accelerator Generation

Abstract: As artificial intelligence (AI) increasingly moves from the cloud to edge devices, automated AI accelerator generation platforms have become essential infrastructure for rapidly translating trained models into efficient hardware implementations. Although these platforms greatly reduce design time and deployment cost, their security risks have not been sufficiently studied. This presentation introduces security vulnerabilities in automated AI accelerator generation and discusses countermeasures for improving the security and robustness of generated accelerators. Specifically, it focuses on platform-native threats within the accelerator generation flow, where malicious manipulations can jointly affect model parameters and hardware implementations.