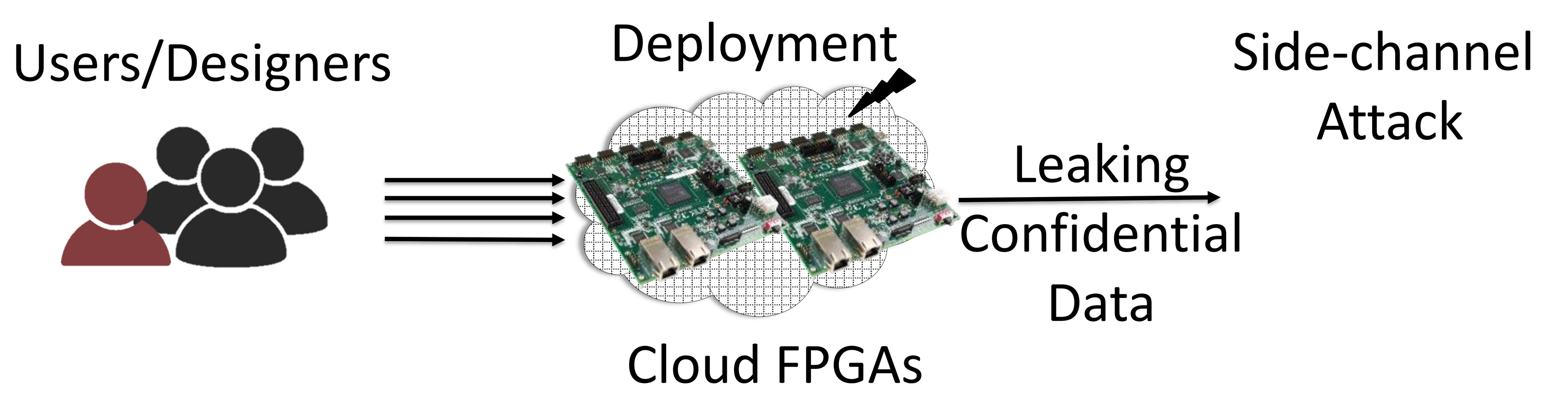
Efficient Security for Emerging Computing Platforms: Side-channel Attacks and Defenses

Mahya Morid Ahmadi
Vienna University of Technology (TU Wien)

Advisor: Muhammad Shafique
New York University Abu Dhabi (NYUAD)

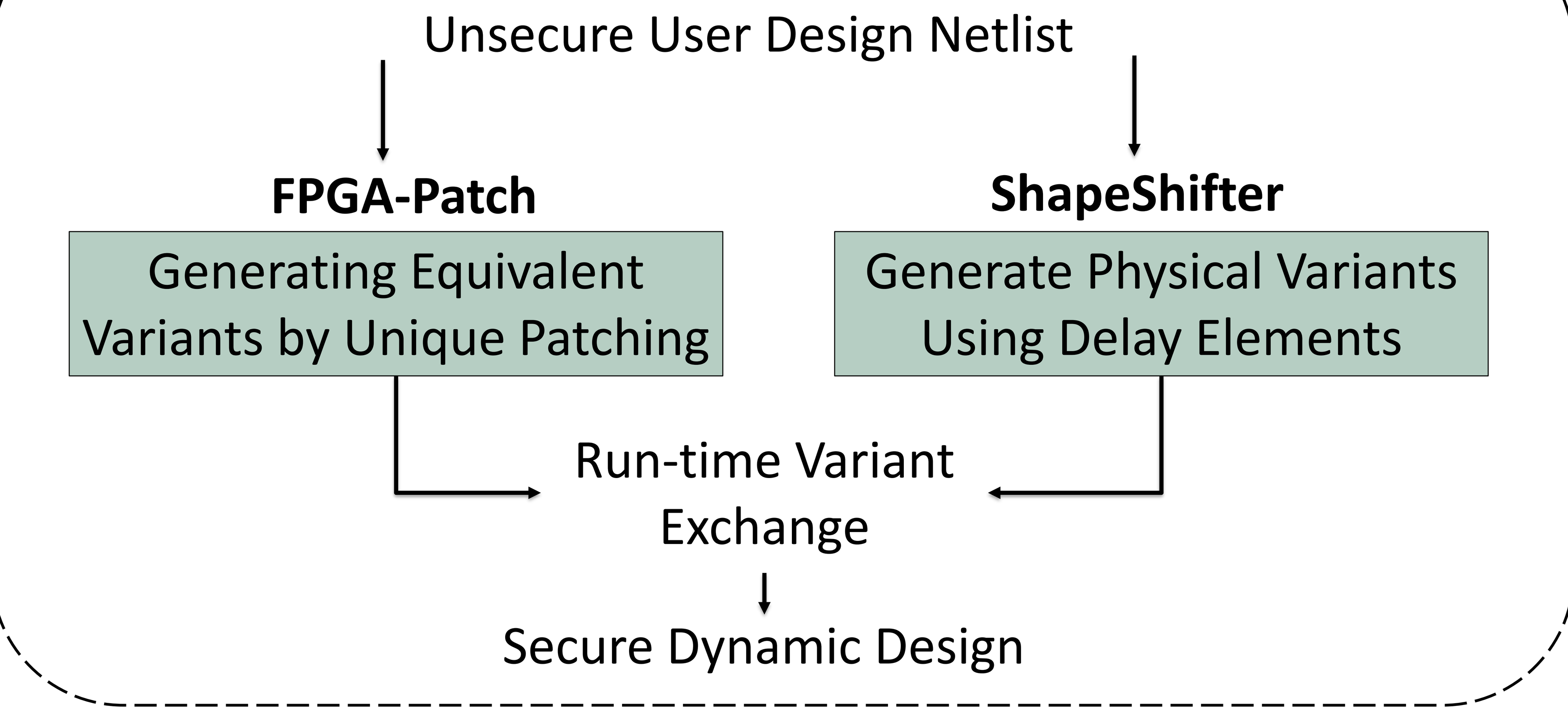
Hardware-based Side-Channel Attacks and Mitigation

Motivation



Employing confidential applications in multi-tenant FPGAs, requires protection from malicious users.

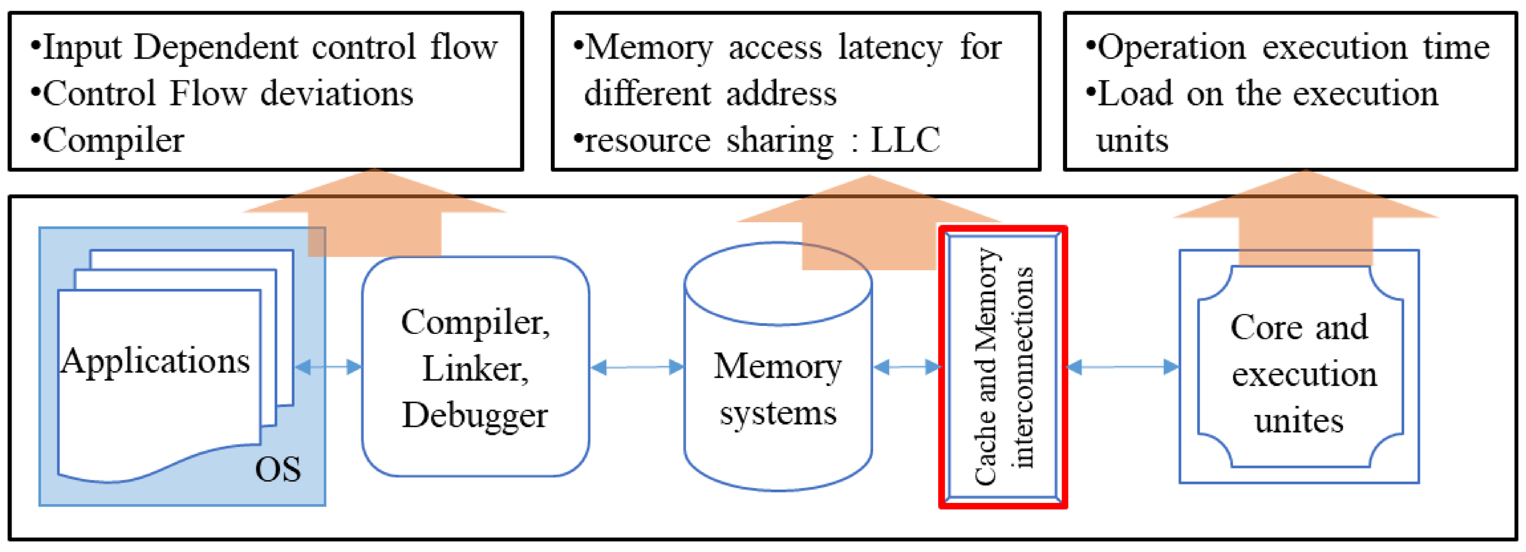
Our solutions



Recently, Cloud Service Providers have found a surge of interest in enabling multi-tenancy in cloud FPGAs, (i.e., multi-tenant usage of a single FPGA through virtualization) in order to maximize resource utilization. Although multi-tenancy comes with great benefits, it is associated with new security risks in shared FPGA platforms.

Hardware-agnostic Side-Channel Analysis on Emerging Systems

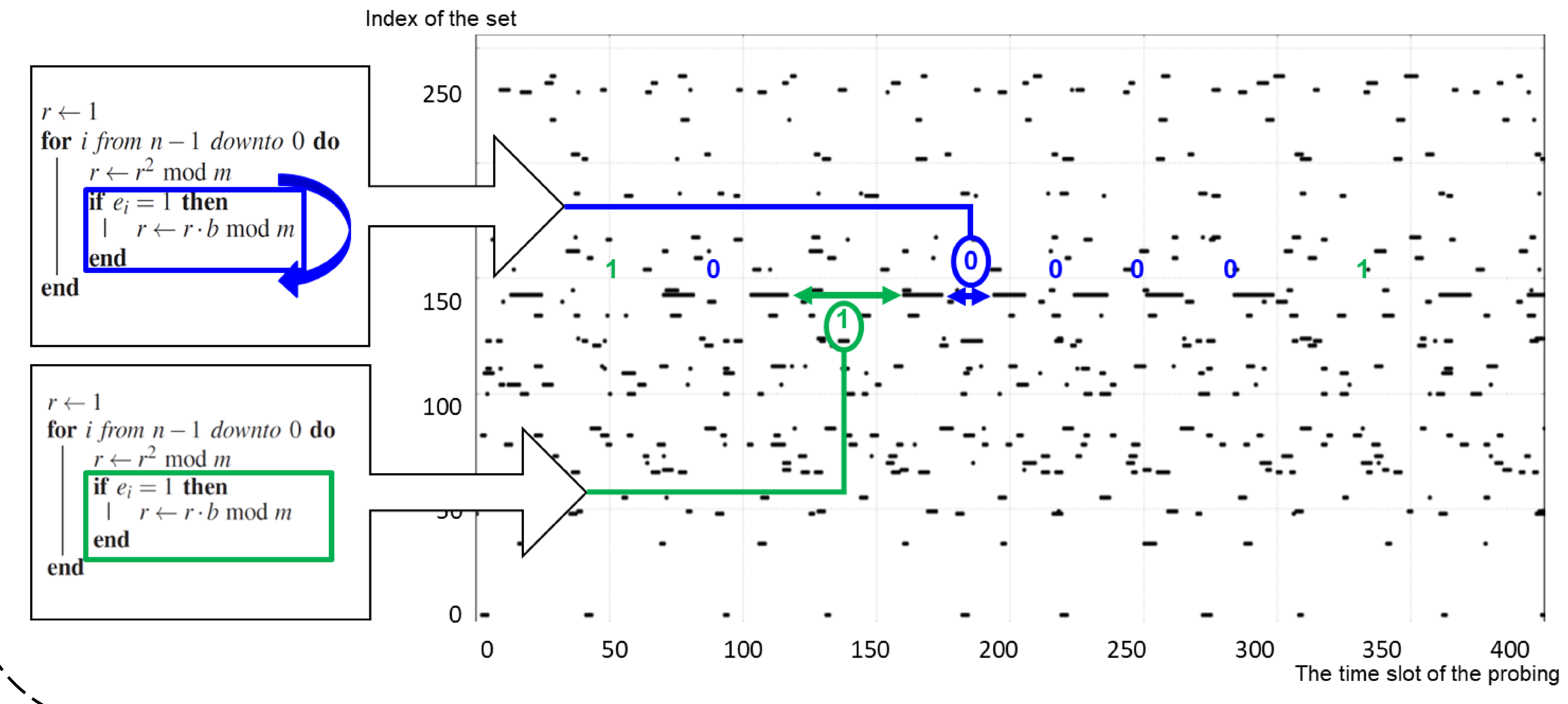
Motivation



Conventional attack vectors are required to be addressed in emerging architecture in design stages.

Our attack

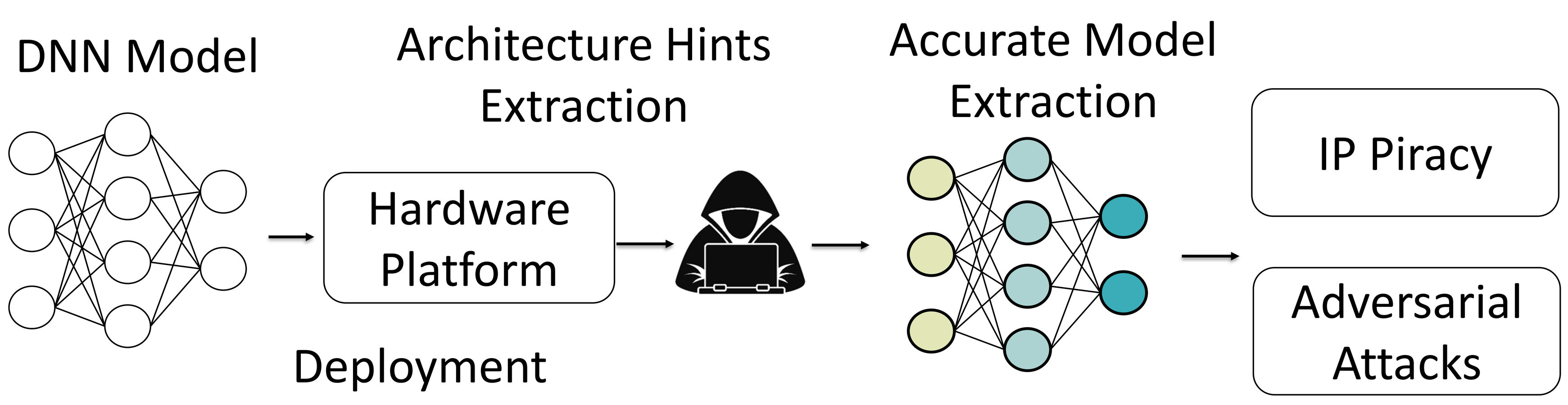
Side-Channel Attacks on RISC-V Processors



There are two main targets of SCAs: (i) the extraction of secret data, i.e., cryptographic keys or passwords for example in timing side-channel attacks, and (ii) the extraction of the structure of a system or application, i.e., side-channel architecture stealing attack (SCAS) to uncover Deep Neural Network (DNN) models.

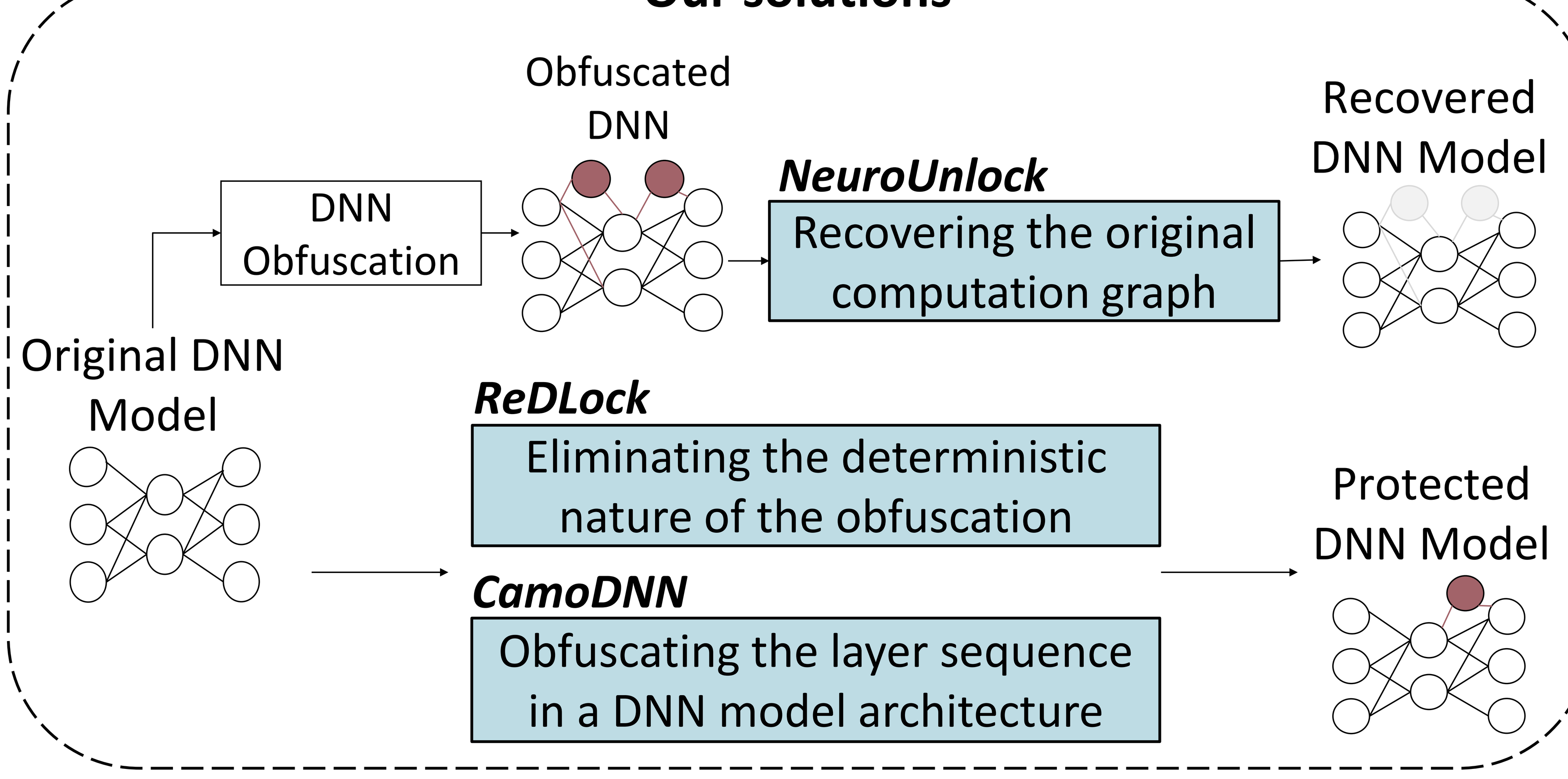
Platform-agnostic Side-Channel Attacks and Mitigation

Motivation



The characteristics of DNN models require protection from malicious users attempting to steal the IPs.

Our solutions



REFERENCES

CONTACT

mahya.ahmadi@tuwien.ac.at
muhammad.shafique@nyu.edu

ACKNOWLEDGEMENT

This work is supported by the Doctoral College Resilient Embedded Systems, which is run jointly by the TU Wien's Faculty of Informatics and the UAS Technikum Wien and is part of the Moore4Medical project funded by the ECSEL Joint Undertaking under grant number H2020-ECSEL-2019-IA-876190.