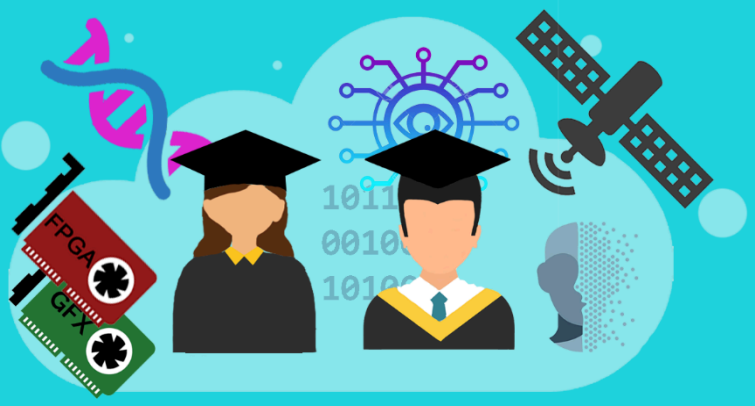
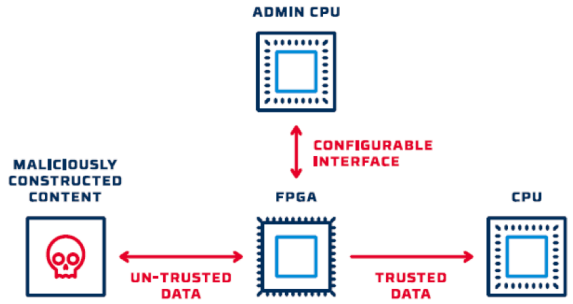
Diploma Thesis

Microproccessors and Digital Systems Laboratory



Exploring Security Threats and Countermeasures in FPGAs

In the context of emerging 6G networks, hardware accelerators are being integrated at the Edge to meet the stringent low-latency and power-efficiency requirements demanded by various services, such as the inference of AI models, Digital Signal Processing Functions (DSP) etc. Field Programmable Gate Arrays (FPGAs) are seen as a promising solution, offering both acceleration and flexibility due to their reconfigurable architecture. Furthermore, with advancements in device capabilities, the trend of supporting multiple users simultaneously on a single FPGA device is gaining traction.



However, as FPGAs become increasingly adopted in multi-tenant environments, ensuring the security of these platforms has become a critical concern, particularly in the face of evolving attack vectors and exploitation techniques. Specifically, researchers have demonstrated that multi-tenant FPGA configurations can be exploited to steal sensitive information. Malicious actors can implement custom sensors in the programmable logic to execute power side-channel attacks without requiring physical access to the device. In response, other studies are focused on strengthening the security of such platforms by utilizing Trusted Execution Environments (TEEs) within both FPGAs and host systems (CPUs), where proprietary solutions, such as ARM TrustZone and Intel's Security Guard Extensions (SGX), are commonly used to achieve this. Furthermore, one key challenge in FPGAs is the secure storage of cryptographic keys, where in order to address the security risks associated with Non-volatile Memories (NVMs), researchers have developed Physical Unclonable Functions (PUFs), which exploit unique physical variations in the semiconductor manufacturing process to securely generate and store keys. Addressing these security challenges and enhancing the already available countermeasures is crucial to ensuring the safe deployment of FPGA-based systems, highlighting the need for continued research in this field.

The objective of this thesis is to investigate various new techniques for enhancing the security of existing solutions designed for FPGA devices, as well as to examine the various attacks targeting these platforms.

AVAILABLE THESIS: **3**

PREREQUISITES:

FPGAs, C/C++, Python, VHDL, Bash

RELATED MATERIAL:

[1] Zhao, Mark, and G. Edward Suh. "FPGA-based remote power side-channel attacks." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[2] https://www.pufsecurity.com/technology/puf/

CONTACT INFORMATION:

Ilias Papalamprou, Ph.D. student [ipapalambrou@microlab.ntua.gr]

Dimosthenis Masouros, Ph.D. [dmasouros@microlab.ntua.gr]

Prof. Dimitrios Soudris [dsoudris@microlab.ntua.gr]