

# SaTC: STARSS: Small: Collaborative: Managing Hardware Security in Three Dimensional Integrated Circuits

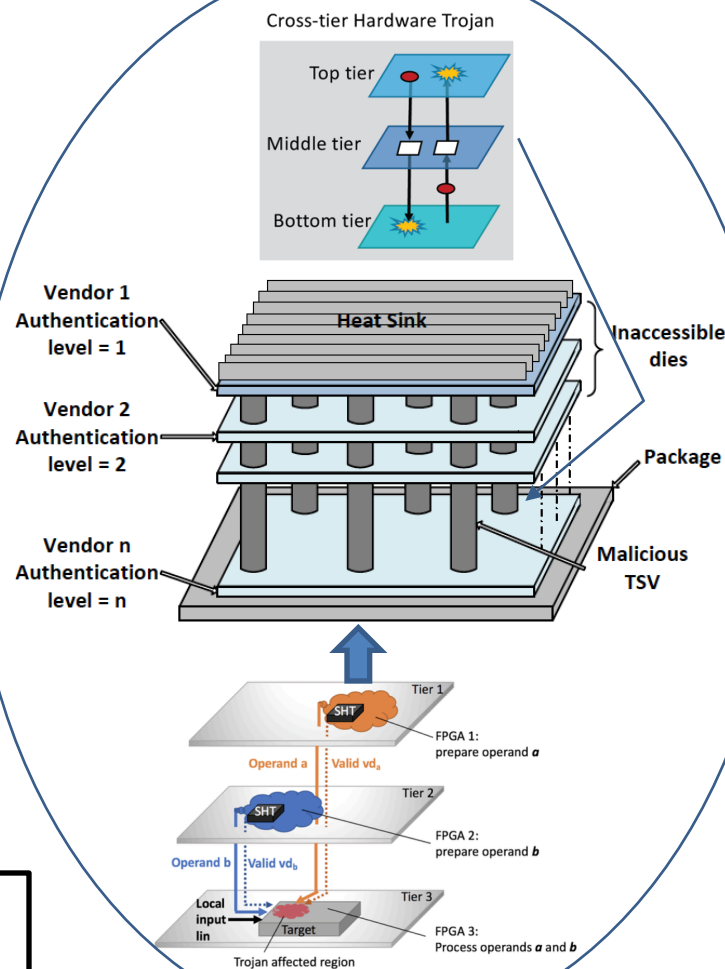


## Challenge:

- Despite the well-characterized advantages (such as reduction in delay and power), three-dimensional ICs are vulnerable to new security threats from
  - Untrusted 3D foundries
  - Reverse engineering on vertical dimension
  - Multi-tier power side channel attack

## Solution:

- 3D power grid noise is exploited to address side-channel attacks
- Camouflaged logic gate is designed to harden monolithic 3D IC



## Scientific Impact:

- This project provides comprehensive attack models for 3D hardware Trojans
- The scalable solution produced by this project will guarantee hardware security in 3D ICs while eliminating the need to access a trusted foundry

## Broader Impact:

- The primary outcome of this project will be a systematic framework to assess and enhance trustworthiness of 3D ICs for both commercial and defense-specific applications
- This outcome is critical for emerging 3D industry since plug-and-play based 3D ICs will significantly suffer from authentication and security

CNS-1717130  
 Lead PI: Qiaoyan Yu  
 University of New Hampshire  
 PI: Emre Salman  
 Stony Brook University