



University of  
New Hampshire

# A Comprehensive Study on the Hardware Trojans in 3D ICs

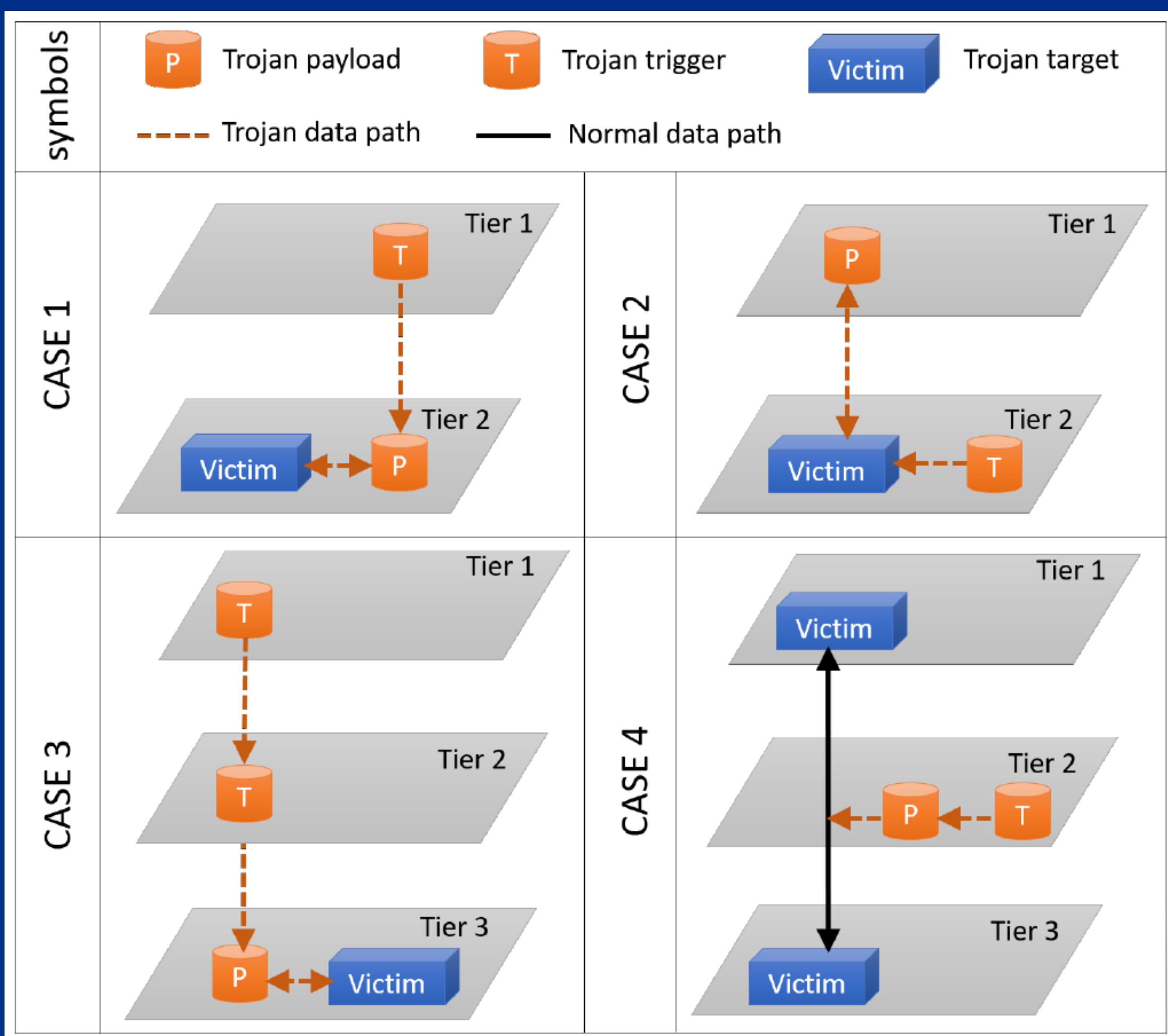
Zhiming Zhang and Qiaoyan Yu  
University of New Hampshire, Durham, NH



## Introduction

- Three-dimensional (3D) integration brings in new security challenges
- New types of hardware Trojans can be launched by exploiting 3D stacking structure
- We characterize the 3D hardware Trojan with four cases for better investigating 3D IC security
- A thermal-triggered 3D Trojan is demonstrated to verify the feasibility and efficiency in 3D environment

## Proposed Trojan Characterization

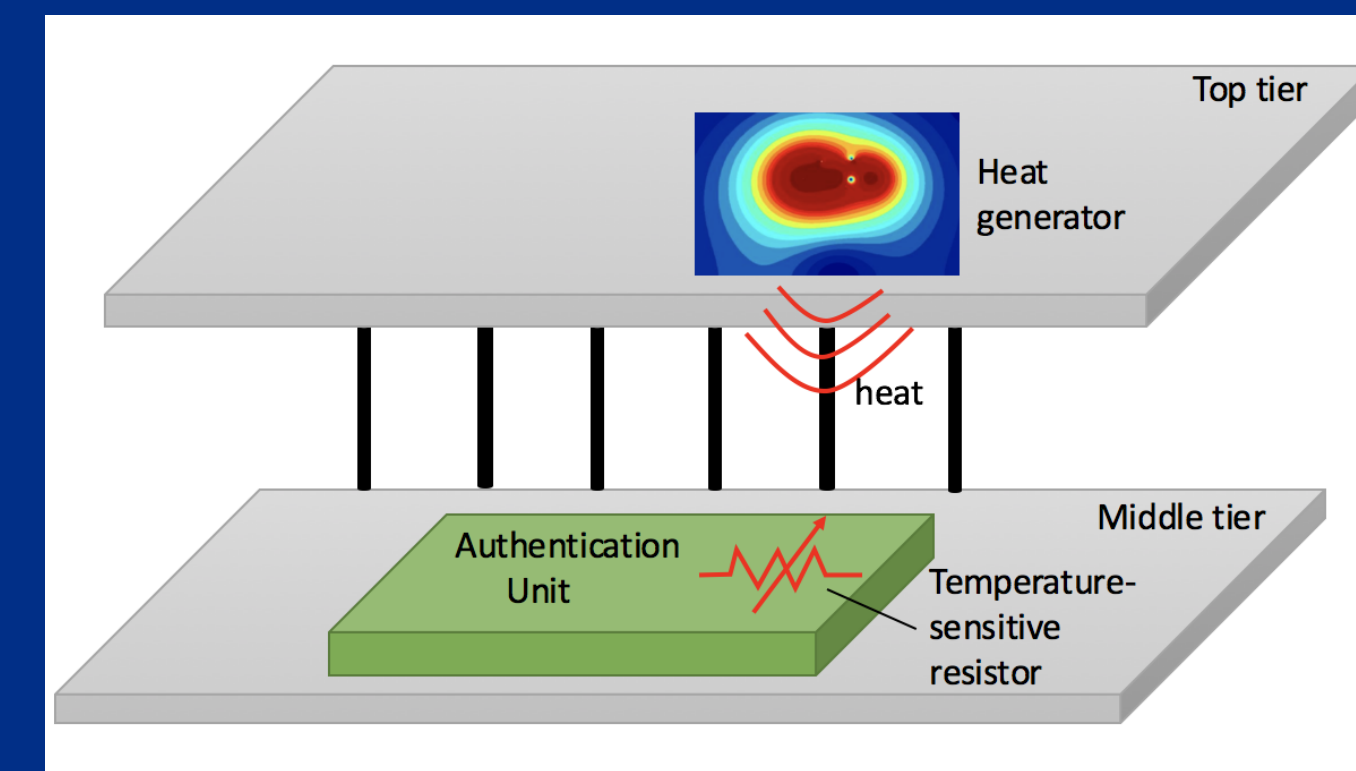


- **Case1: Cross-Tier Trojan Trigger**
  - No symptom without valid cross-tier trigger signal
- **Case2: Cross-Tier Trojan Payload**
  - Trojan effect is not observable in tier-level testing
- **Case3: Multi-Tier Collaborative Trojan Trigger**
  - Much lower triggering probability than 2D counterpart
- **Case4: Information Leaking in Passive Layer**
  - No alteration to normal operation and communication
  - Weak side-channel

## Example on Each Trojan Case

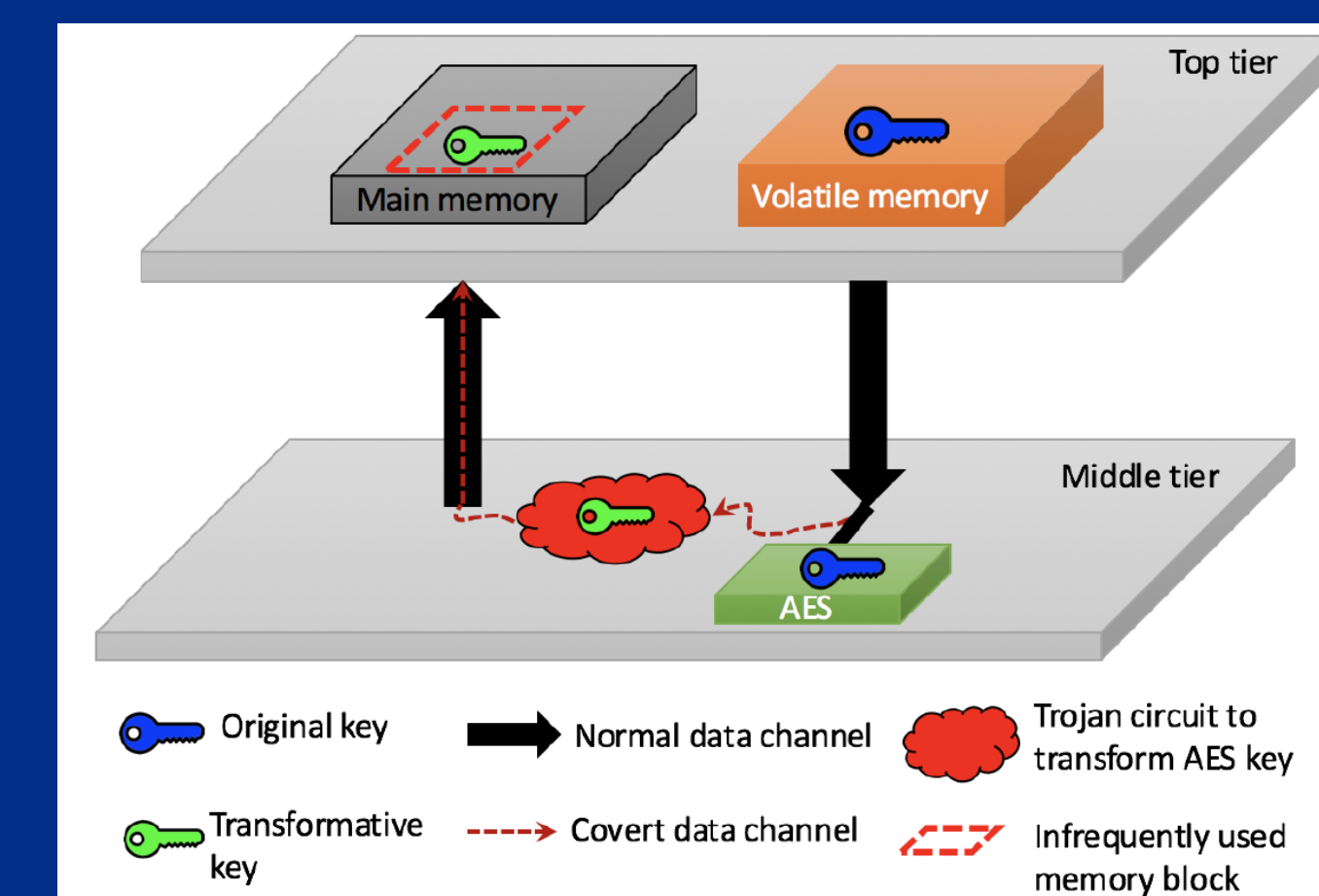
### • Case1: Thermal-triggered Trojan Example

- Trigger: heat generator in top tier
- Payload: temperature sensitive resistor in middle tier
- Procedure: generated heat is passed to middle tier to be sensed by payload to cause malfunction



### • Case2: Trojan Induced Crypto Key Leak

- Crypto unit AES is located in middle tier
- Crypto key is obfuscated and stored to rarely used memory in top tier

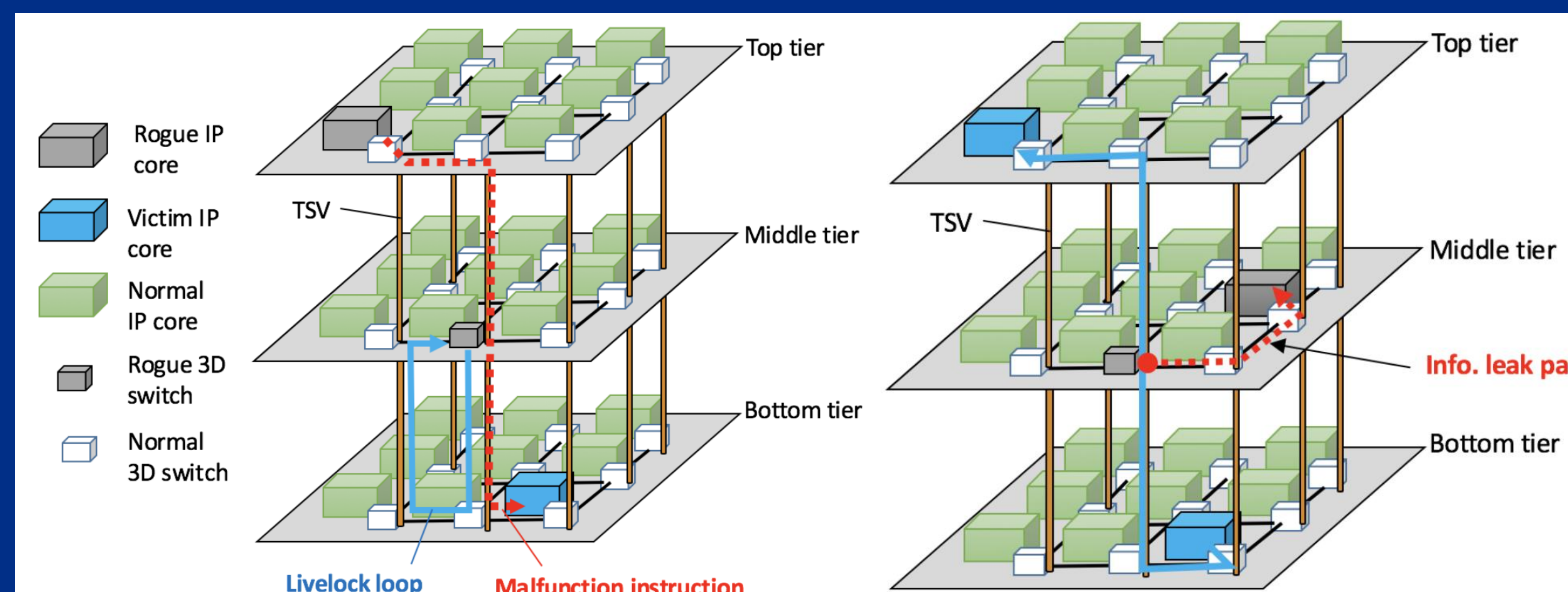


### • Case3: 3D Network-on-Chip (NoC) Trojan

- Rogue IP core in tier 1 sends malicious NoC instruction packet to rogue switch in tier 2
- Rogue switch in tier 2 passes the packet to victim IP core in bottom tier to cause malfunction or livelock

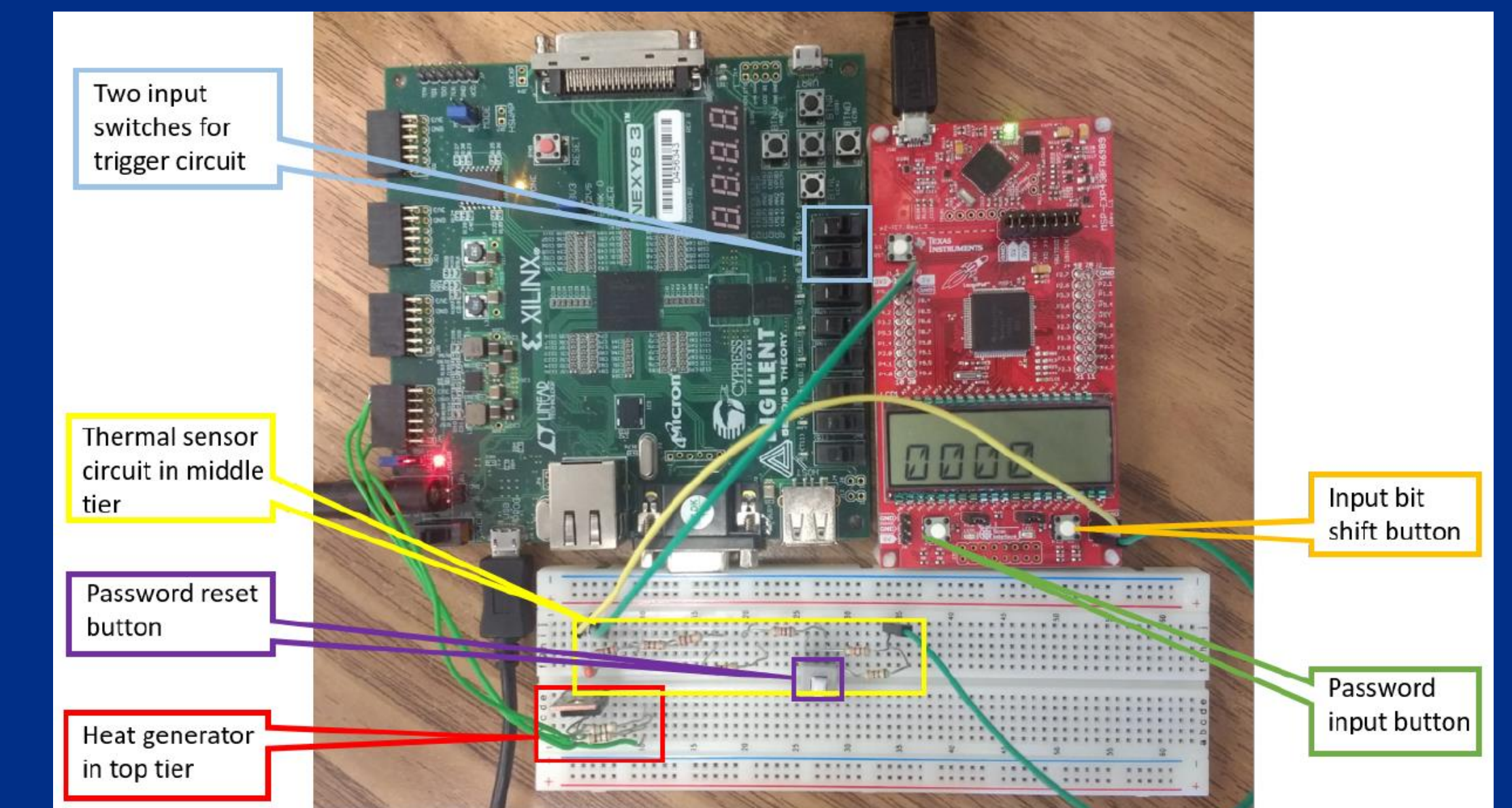
### • Case4: Information leak due to a 3D NoC Trojan

- Both trigger and payload are located in middle tier
- Victims are in top and bottom tiers
- Packets transmitting through middle tier is monitored
- Target packet is stored for future use and analysis



## Hardware Demo on Thermal Trojan

### • Demo setup



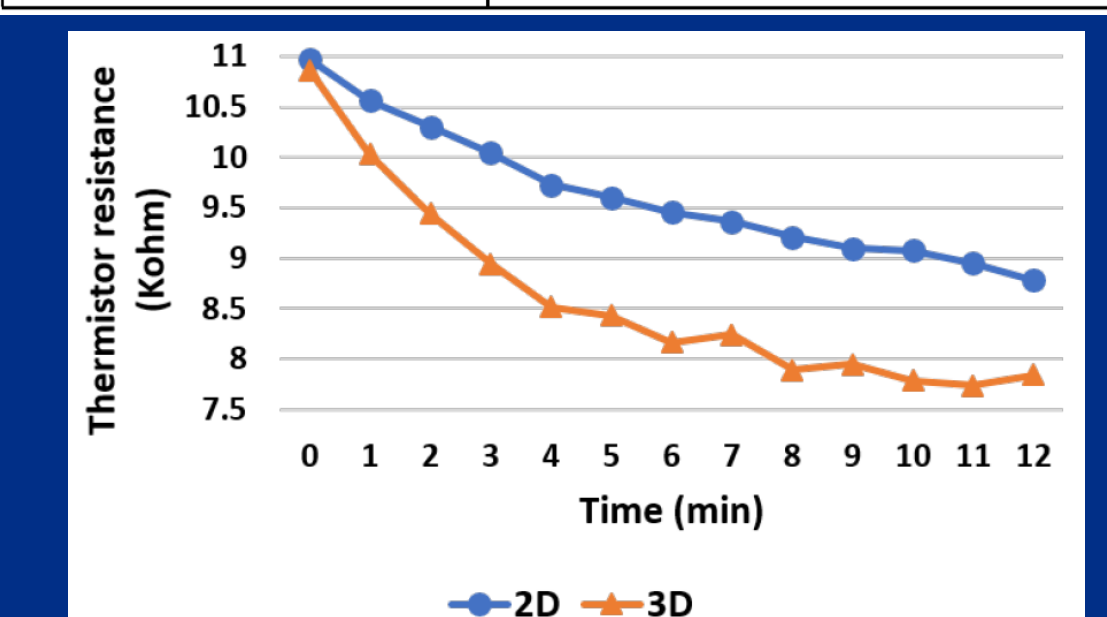
### • Experimental results

- Demo outputs: Authentication passed with incorrect password



- Efficiency comparison: Triggered faster than 2D scenario

Emulation scenarios	Time to trigger Trojan (min)
2D	11:12
3D	6:52



## Conclusions

- Characterized four representable high-level 3D hardware Trojan cases and analyzed each one with an example
- Demonstrated thermal-triggered 3D Trojan in FPGA and microcontroller platform
- Compared Trojan efficiency of 2D and 3D scenarios

## Technology Transfer

- This work is published and presented in ISVLSI'19.

## Acknowledgement

- This work was supported in part by NSF/Semiconductor Research Corporation (SRC) STARSS grant (No. CNS-1717130).