

# Benchmarking Security Closure of Physical Layouts

## ISPD 2022 Contest

Johann Knechtel<sup>1</sup>, Jayanth Gopinath<sup>2</sup>, Mohammed Ashraf<sup>1</sup>, Jitendra Bhandari<sup>2</sup>,  
Ozgur Sinanoglu<sup>1</sup>, Ramesh Karri<sup>2</sup>

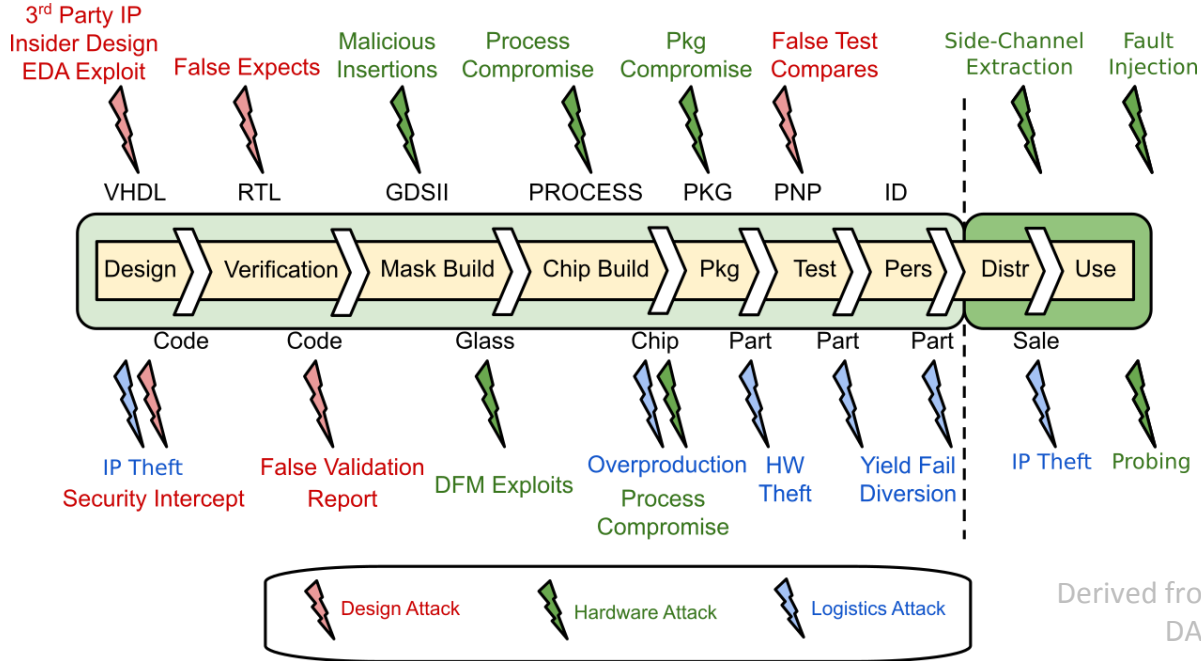
NYU Abu Dhabi<sup>1</sup>, NYU New York<sup>2</sup>

# Overview

- Motivation:
  - Number of serious hardware security threats are emerging
  - Build knowledge and experience within the community for security and its close relation to physical design
- Theme: security closure of physical layouts, i.e., hardening the physical layouts at design time
- 1<sup>st</sup> time as contest
- Selected threats: Trojan insertion and probing, fault injection
  - Limited, manageable scope for threats
  - Once taken in, can be well approached by physical design teams
- Benchmarks and submissions are based on DEF format and related files
  - Participants are free to use any physical-design tools of their choice
  - Open to the community at large
- Part 1: background, theme, some details on contest; Part 2: teams, rankings, awards

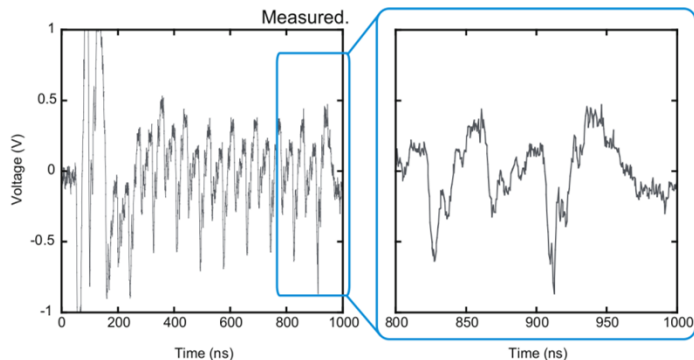


# Background: IC Supply Chain and Threats

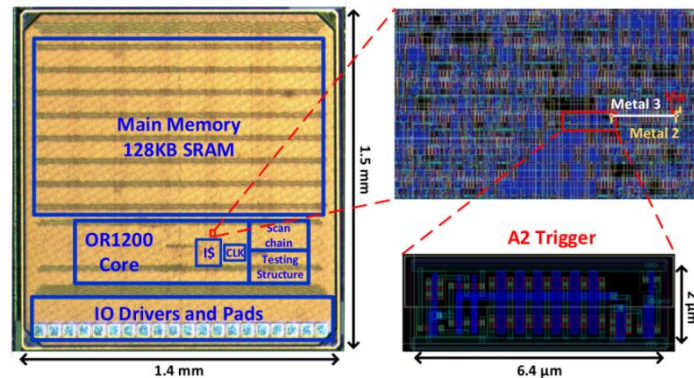


Derived from Kerry Bernstein,  
DARPA, 2016

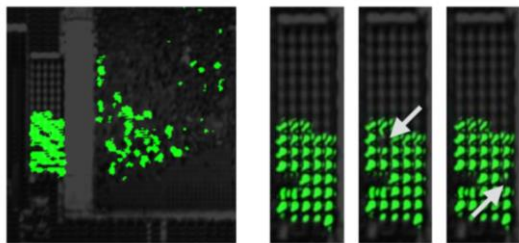
# Background: Selected Threats



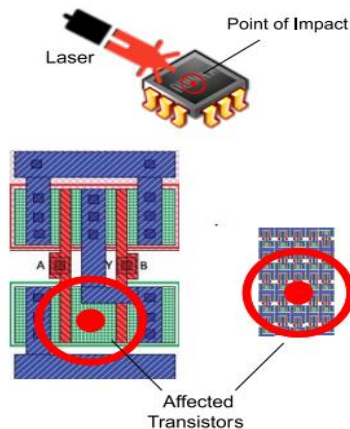
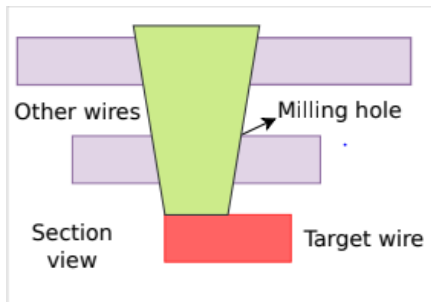
Fujimoto et al., EMC 2014



Yang et al., SP 2016

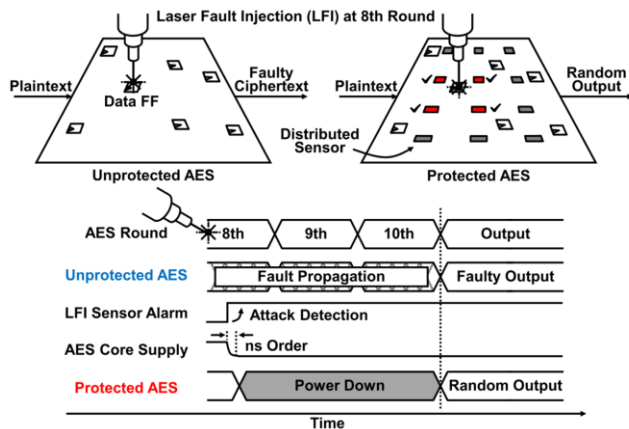


Tajik et al., CCS 2017

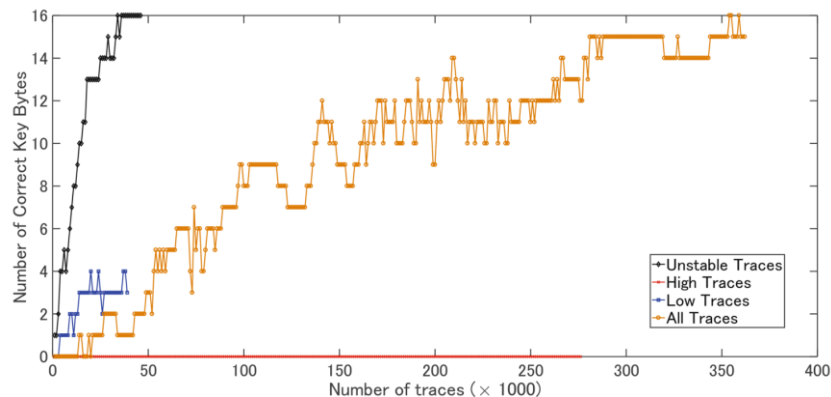


# Theme: Security Closure – What and Why?

- What: enable CAD tools to harden physical layouts against threats that are executed post-design time
- Why:
  - Most threats target on vulnerabilities of layouts
  - Vulnerabilities can be hardly fixed, if at all, after design time
  - IV&V and hardening of outsourced designs
  - Maintain security efforts taken at higher layers – may otherwise well be “optimized out” or failing altogether

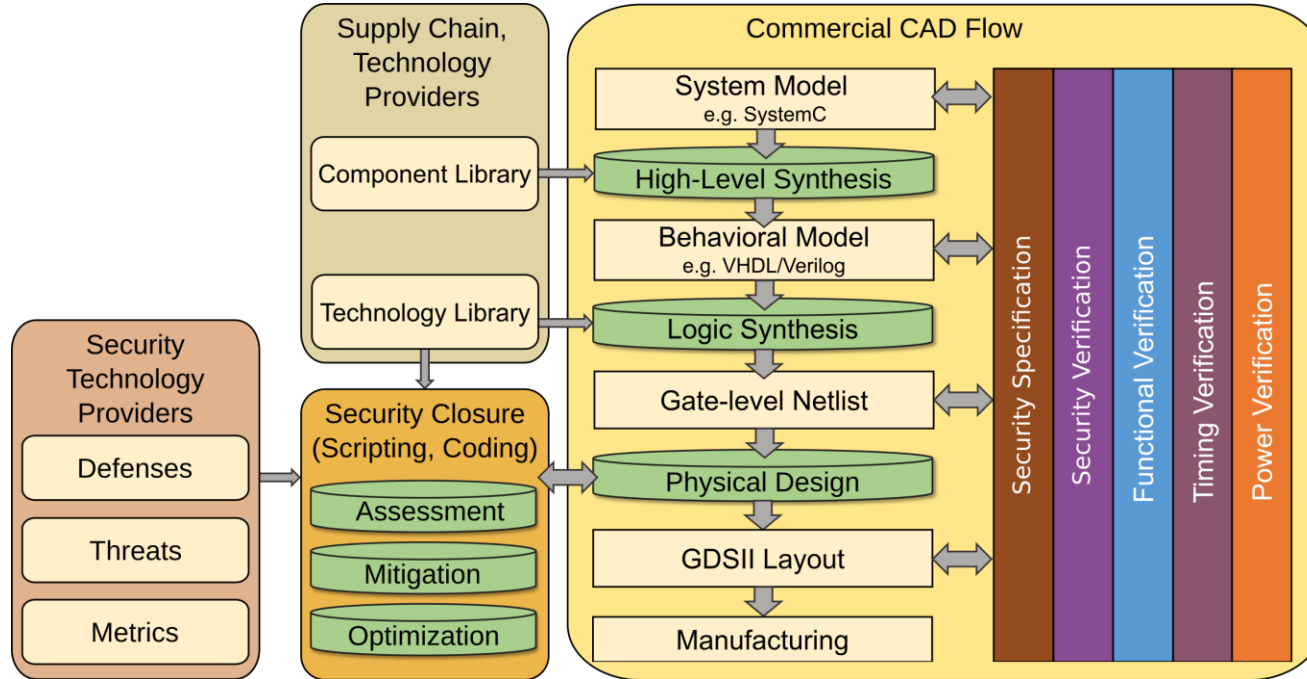


Matsuda et al., JSSC 2018



Li et al., Inscrypt 2019

# Theme: Security Closure – How?

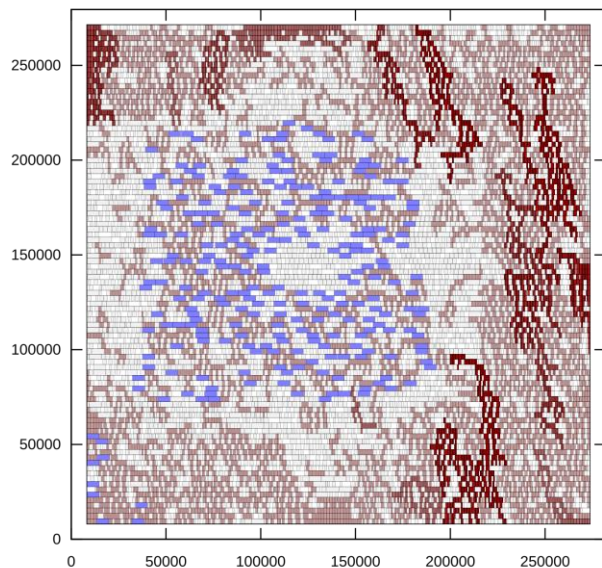


## Contest Objectives

To employ defense measures for the physical layouts against the threat of:

- Trojan insertion – fix exploitable regions
- Probing, fault injection at frontside – fix exposed areas

Some details follow for metrics; more general background and references in paper





# Contest Logistics

- Alpha/qualifying round, final round
- Intermediate scoring released to promote competition
- Website with Q&A, email discussion and sometimes polls
- Design flow participants: any of choice
- Our backend:
  - Cadence Innovus, LEC, custom tcl and bash scripts
  - Data and process management via bash scripts
- Frontend participants: Google drive, email notifications

```
3) Checking team folder "fallech" (Google team folder ID "16AePD16XKw4A9jK4g3F5rmVwZ94Yb") for new submission files ...
3) Checking team folder "XDSecurity" (Google team folder ID "1PpwZ2uckH8pHw7B_FE2dvXSj_y5T0h") for new submission files ...
3) Checking team folder "TCLAB" (Google team folder ID "1YXUUP4TV7Bc1Ac5K12jK8-AAX62e0b") for new submission files ...
3) Download new submission file "solution_03-28-20-41.zip" (Google file ID "11i01CZ79V_aRD-INCB8_2KUXg20jbgxK") into dedicated folder "/home/jk176/ISPD22/data/final/DASYS/MISTY/downloads/downloads_1648471329"
3) Unpacking zip file "solution_03-28-20-41.zip" into dedicated folder "/home/jk176/ISPD22/data/final/DASYS/MISTY/downloads/downloads_1648471329"
3) Download new submission file "design_fatherofhope" (Google file ID "1SFDKc0YPC707v5wG1-s0-hTcxSJW-yV") into dedicated folder "/home/jk176/ISPD22/data/final/DASYS/MISTY/downloads/downloads_1648471329"
3) Done

4) Start evaluation processing of newly downloaded submission files, if any ...
4) Time: Mon Mar 28 08:44:43 EDT 2022
4) Time stamp: 1648471483
4)
4) [ DASYS -- MISTY -- 1648471472 ]: Start processing within dedicated work folder "/home/jk176/ISPD22/data/final/DASYS/MISTY/work/downloads_1648471472"
4) [ DASYS -- MISTY -- 1648471472 ]: Send out email about processing start ...
4) [ DASYS -- MISTY -- 1648471472 ]: Init work folder ...
4) [ DASYS -- MISTY -- 1648471472 ]: Check submission files ...
4) [ DASYS -- MISTY -- 1648471472 ]: Check whether assets are maintained ...
4) [ DASYS -- MISTY -- 1648471472 ]: Check cell assets ...
4) [ DASYS -- MISTY -- 1648471472 ]: Check net assets ...
4) [ DASYS -- MISTY -- 1648471472 ]: Check whether assets are maintained passed.
4) [ DASYS -- MISTY -- 1648471472 ]: Pins design checks ...
4) [ DASYS -- MISTY -- 1648471472 ]: PDN checks ...
4) [ DASYS -- MISTY -- 1648471472 ]: LEC design checks ...
4) [ DASYS -- MISTY -- 1648471472 ]: Basic design checks ...
4) [ DASYS -- MISTY -- 1648471472 ]: Pins design checks passed.
4) [ DASYS -- MISTY -- 1648471472 ]: LEC design checks done.
4) [ DASYS -- MISTY -- 1648471472 ]: PDN checks passed.
4) [ DASYS -- MISTY -- 1648471472 ]: Basic design checks done.
4) [ DASYS -- MISTY -- 1648471472 ]: All checks done
4) [ DASYS -- MISTY -- 1648471472 ]: Exploitable regions: start background run for script version considering 6 metal layers...
4) [ DASYS -- MISTY -- 1648471472 ]: Probing: start background run ...
4) Done

5) Sleep/wait for 60 s ...
5) Time: Mon Mar 28 08:45:23 EDT 2022
5) Time stamp: 1648471523
5)
5) Sleeping ...
5) .....[ 100 %
5) Done

1) Check status of ongoing evaluation processing, if any ...
1) Time: Mon Mar 28 08:46:25 EDT 2022
1) Time stamp: 1648471585
1)
1) Checking work folder "/home/jk176/ISPD22/data/final/DASYS/Camellia/work/downloads_1648471329"
1) Exploitable regions: done
1) Probing: done
1) Computing scores ...
1) Copying report files to uploads folder "/home/jk176/ISPD22/data/final/DASYS/Camellia/uploads/results_1648471329" ...
1) Including backup of processed files to uploads folder "/home/jk176/ISPD22/data/final/DASYS/Camellia/uploads/results_1648471329" ...
1) Backup work folder to "/home/jk176/ISPD22/data/final/DASYS/Camellia/backup.work/downloads_1648471329.zip" ...
1)
1) Checking work folder "/home/jk176/ISPD22/data/final/DASYS/MISTY/work/downloads_1648471472"
1) Exploitable regions: still working ...
1) Probing: done
1)
1) Checking work folder "/home/jk176/ISPD22/data/final/DASYS/SEED/work/downloads_1648471138"
1) Exploitable regions: done
1) Probing: done
0 bash 1 bash 2 bash 3 bash 4 bash 5 bash 6 bash 7 bash
```



# Benchmarks

1. Public crypto cores (i.e., Camellia, CAST, MISTY, SEED, TDEA)
2. Opencore openMSP430 microcontroller
3. MIT-LL CEP SoC i.e., security-centric SoC design with crypto, DSP, GPS etc.
4. PRESENT, SPARX crypto cores from in-house projects

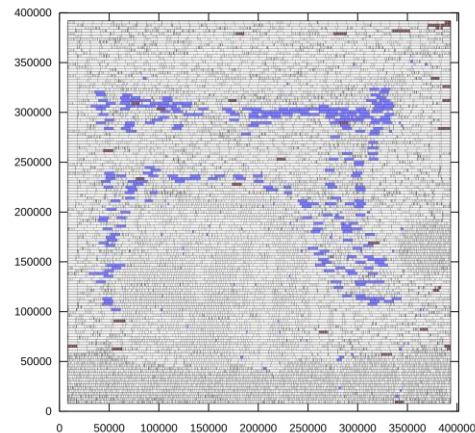
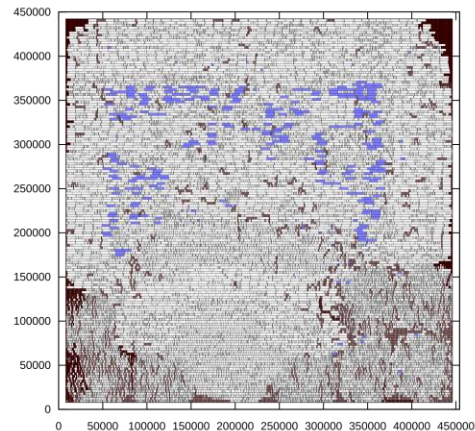
## Characteristics of benchmarks:

1. Synthesized, implemented using Synopsys DC, Cadence Innovus with Nangate 45nm Open Cell Library
2. Varied range of layouts: different timing constraints, utilization, and library configuration
3. Security assets, e.g., cells and nets related to key FFs, are identified from the post-layout netlists

Participants are provided with an archive files containing DEF, SDC, MMMC, custom list for sensitive cells and nets, LIB/LEF, various snapshots with sensitive cells and nets highlighted, and a README

# Closer Look Into Benchmarks

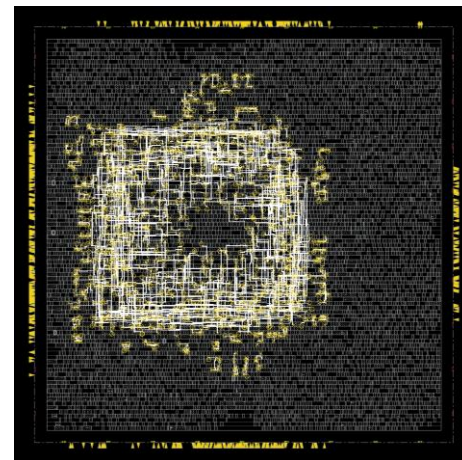
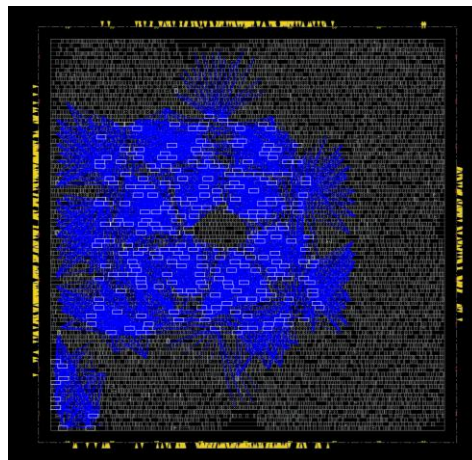
- Sample benchmarks: “warm-up” for the theme
  - AES layout with 70% utilization
  - AES layout with 90% utilization
  - AES layout with 70% util. and some shielding of cells and nets
- Insights provided to participants:
  - Increasing utilization hardens the layout against Trojan insertion and probing, fault injection but also make timing closure difficult
  - Shielding protects mainly against probing but also degrades PPA
  - Competitive schemes should achieve security closure while maintaining design quality



## Closer Look Into Benchmarks

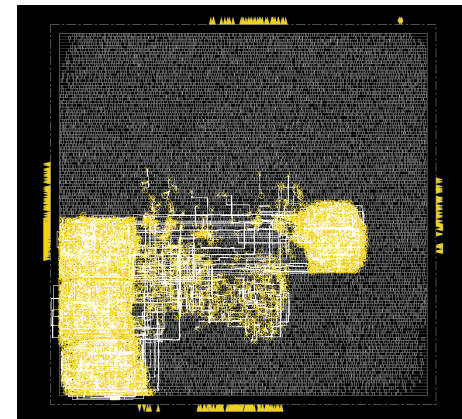
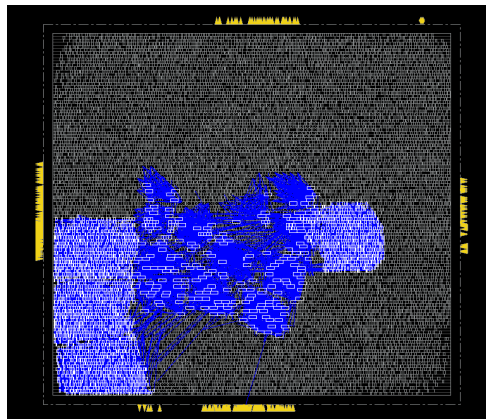
Camellia benchmark:

- 265 cell assets (out of 6710 cells in total; ratio of 3.94%)
- 384 net assets (out of 7094 nets in total; ratio of 5.41%)



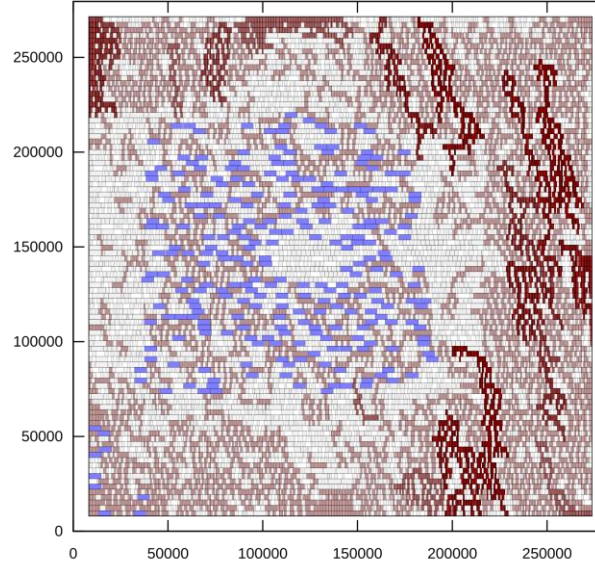
CAST benchmark:

- 1886 cell assets (out of 12682 cells in total; ratio of 14.87%)
- 1919 net assets (out of 13050 nets in total; ratio of 14.70%)



# Metrics: Trojan Insertion

- Exploitable regions: placement sites along with routing resources
  - Based on timing-constrained distances: NAND gate placed in region and routed to asset would not violate timing
  - Regions formed by 20+ sites that are connected within and across rows
  - Simplification; e.g., does not account for possibility of attacker to shift nearby cells



## Metrics: Frontside Probing, Fault Injection

- Exploitable area of cell, net assets: area not covered by other metals above
  - Simplification: sum up disconnected regions for area



# Constraints

1. Maintain security assets
2. Maintain functional equivalence
3. No additional dedicated circuitry, e.g., sensors to detect fault injection
4. No custom cells, only those provided in LIB/LEF
5. No additional metal layers
6. Cannot move the PG network to different layers, and must maintain ratio of PG metals to die area
7. Various constraints on design metrics
8. Participants should not incorporate trivial defenses such as filler cells

# Scoring

- The overall score, to be minimized, is defined as:  
$$\text{score} = \text{sec} \times \text{des} = (\text{ti} + \text{fsp\_fi})/2 \times \text{des}$$
- Various metric components defined for Trojan insertion, frontside probing, fault injection, design quality
  - Weight and sum up normalized metric components across their categories
- Metric values are normalized to baseline, i.e, provided benchmark layout
  - Ranges of 0 (max improvement) to 1 (no improvement) to inf (max deterioration)
- Multiplication instead of addition
  - Scoring penalizes deterioration; meant to keep design cost in bounds
  - For typical range of design cost (like 0.6—1.1), this also serves well to emphasize on security optimization
    - E.g., des = 0.7, sec = 0.6 is worse than des = 0.9, sec = 0.2
  - Once teams pushed sec toward zero, des becomes mute; imposed constraints on design quality



# Scoring

## 1) Trojan insertion – ti

### (a) 50% weighted: placement sites of exploitable regions

- Ratio wrt to baseline; 50%, 33.3% and 16.6% for total, max and avg # free sites, respectively

### (b) 50% weighted: routing resources of exploitable regions

- Ratio wrt to baseline; 50%, 33.3% and 16.6% for total, max and avg # free routing tracks, respectively

## 2) Frontside probing and fault injection – fsp\_fi

### (a) 50% weighted: exposed area of standard cell assets

- Ratio wrt to baseline; 50%, 33.3% and 16.6% for total, max, avg exposed area of cells assets, respectively

### (b) 50% weighted: exposed area of net assets

- Ratio wrt to baseline; 50%, 33.3% and 16.6% for total, max, avg exposed area of net assets, respectively

# Scoring

## 3) Design quality – des

### (a) 25% weighted: power

- Ratio wrt to baseline power

### (b) 25% weighted: performance

- 50%, 33.3% and 16.6% weighted for setup\_TNS, setup\_WNS and setup\_FEP, respectively

### (c) 25% weighted: area

- Ratio wrt to baseline die area

### (d) 25% weighted: design checks

- Ratio wrt to baseline checks: Non-equivalent points, Unreachable points, Undriven pins, Open output ports, Net output floating, Basic routing issues, Module pin issues, Unplaced components issues, Placement and/or routing issues, DRC issues

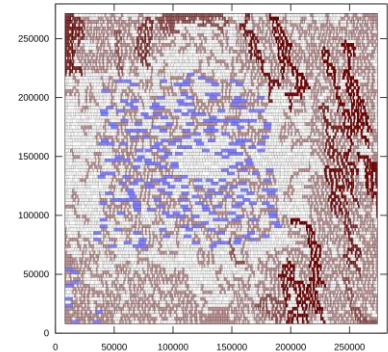
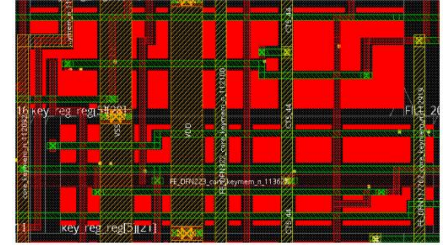
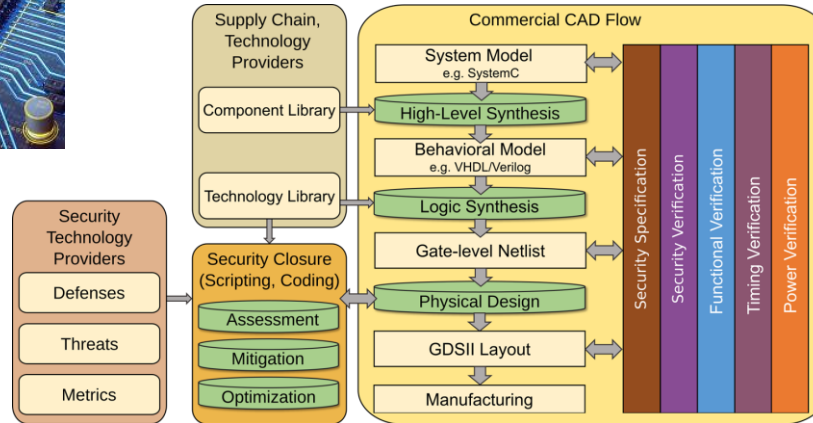
# Conclusion Part 1

- Various threats on layouts, but CAD flows are not ready for security yet
  - Need for security closure, secure-by-design CAD flows
- First-ever contest on this challenge
  - Great efforts from all!



Thank you!

Next part: teams, results



# Overview

- **Motivation:**
  - Number of serious hardware security threats are emerging
  - Build knowledge and experience within the community for security and its close relation to physical design
- **Theme:** security closure of physical layouts, i.e., hardening the physical layouts at design time
- **Selected threats:** Trojan insertion and probing, fault injection
  - Limited, manageable scope for threats
  - Once taken in, can be well approached by physical design teams
- **Teams**
  - **17 teams registered from Americas, Europe, Asia**
  - **8 teams pushed through alpha and final round**



# Teams

- DASYS
  - Peking University
  - Xinming Wei, Jiaxi Zhang, Guojie Luo
- CUEDA
  - The Chinese University of Hong Kong
  - Fangzhou Wang, Qijing Wang, Bangqi Fu, Shui Jiang, Xiaopeng Zhang, Tsung-Yi Ho, Evangeline F.Y. Young
- XDSecurity
  - Xidian University: Zhengguang Tang, Guangxin Guo, Benzhen Li, Hailong You, Jiangyi Shi
  - Giga Design Automation: Xiaojuan Zhang
- UT\_pda
  - University of Texas at Austin
  - Zhili Xiong, Alexander Nguyen, David Pan

# Teams

- TalTech
  - Tallinn University of Technology
  - Tiago Perez, Mohammad Eslami, Felipe Almeida, Samuel Pagliarini
- TCLAB
  - National Tsing Hua University
  - En-Yu Liao, I-Yu Chen, Zi-Hao Guo, Tzu-Chuan Lin, Po-Yu CHOU, Ting-Chi Wang
- NTUsplace
  - National Taiwan University
  - Jhih-Wei Hsu, Kuan-Cheng Chen, Yu-Hsiang Lo, Yan-Syuan Chen, Yao-Wen Chang
- 1 more anonymous team

---

# Teams

- Intro videos



# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - For some time, overall scores varied

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.008447 | 0.041552 | 0.271596 | 0.000001 | 0.194594 | 0.052321 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.010548 | 0.101933 | 0.324694 | 0.430016 | 0.101044 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.003901 | 0.056400 | 0.295023 | 0.000001 | 0.000001 | 0.061247 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.017719 | 0.093440 | 0.749726 | 0.000000 | -----    | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.016850 | 0.087135 | 0.751540 | 0.000001 | -----    | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.002300 | 0.055931 | 0.749526 | -----    | -----    | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.009447 | 0.105195 | 0.554981 | 0.554621 | 0.000001 | 0.170911 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.001957 | 0.079465 | 0.749990 | 0.110556 | 0.000498 | 0.043454 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000001 | 0.086032 | 0.775886 | 0.000001 | -----    | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.008851 | 0.126647 | 0.478162 | 0.107474 | 0.002950 | 0.111408 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.008447 | 0.041552 | 0.271596 | 0.000001 | 0.194594 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.010548 | 0.101933 | 0.324694 | 0.430016 | 0.101044 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.003901 | 0.056400 | 0.295023 | 0.000001 | 0.000001 | 0.061247 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.017719 | 0.093440 | 0.749726 | 0.000000 | -----    | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.016850 | 0.087135 | 0.751540 | 0.000001 | -----    | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.002300 | 0.050516 | 0.469573 | -----    | 0.749405 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.009447 | 0.105195 | 0.460420 | 0.554621 | 0.000001 | 0.170911 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.001957 | 0.079465 | 0.749990 | 0.014029 | 0.000498 | 0.043454 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000001 | 0.086032 | 0.775886 | 0.000001 | -----    | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.008851 | 0.126647 | 0.478162 | 0.014590 | 0.002950 | 0.111408 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.008447 | 0.041552 | 0.271596 | 0.000001 | 0.194594 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.000001 | 0.069438 | 0.324694 | 0.430016 | 0.101044 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.003901 | 0.056400 | 0.295023 | 0.000001 | 0.000001 | 0.061247 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.017719 | 0.093440 | 0.281597 | 0.000000 | -----    | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.016850 | 0.087135 | 0.438146 | 0.000001 | -----    | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.002300 | 0.050516 | 0.469573 | -----    | 0.749405 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.009447 | 0.099805 | 0.460420 | 0.000000 | 0.000001 | 0.170911 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.001957 | 0.079465 | 0.749990 | 0.014029 | 0.000498 | 0.043454 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000001 | 0.086032 | 0.775886 | 0.000001 | -----    | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.008851 | 0.126647 | 0.478162 | 0.014590 | 0.002950 | 0.111408 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.000000 | 0.041552 | 0.271596 | 0.000001 | 0.194594 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.000000 | 0.069438 | 0.324694 | 0.000001 | 0.101044 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.000000 | 0.056400 | 0.295023 | 0.000001 | 0.000001 | 0.061247 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.017719 | 0.093440 | 0.281597 | 0.000000 | -----    | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.016850 | 0.087135 | 0.438146 | 0.000001 | -----    | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.002300 | 0.050516 | 0.469573 | 0.000002 | 0.749405 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.009447 | 0.099805 | 0.460420 | 0.000000 | 0.000001 | 0.170911 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.001957 | 0.079465 | 0.749990 | 0.000000 | 0.000498 | 0.043454 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.086032 | 0.775886 | 0.000001 | -----    | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.008851 | 0.126647 | 0.478162 | 0.014590 | 0.002950 | 0.111408 |

# Scores

- Overall scores –  $\text{score} = \text{sec} \times \text{des}$ 
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.000000 | 0.041552 | 0.271596 | 0.000001 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.000000 | 0.069438 | 0.324694 | 0.000000 | 0.000001 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.000000 | 0.056400 | 0.295023 | 0.000000 | 0.000001 | 0.061247 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.000000 | 0.093440 | 0.281597 | 0.000000 | 0.116623 | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.000000 | 0.087135 | 0.300895 | 0.000001 | 0.000001 | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.000000 | 0.050516 | 0.298437 | 0.000002 | 0.375521 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.000000 | 0.099805 | 0.460420 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.000000 | 0.079465 | 0.507525 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.086032 | 0.775886 | 0.000000 | 0.131423 | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.000000 | 0.126647 | 0.246417 | 0.000000 | 0.002950 | 0.111408 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.000000 | 0.041552 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.000000 | 0.069438 | 0.324694 | 0.000000 | 0.000001 | 0.104176 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.000000 | 0.056400 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.000000 | 0.093440 | 0.281597 | 0.000000 | 0.116623 | 0.122173 |
| CAST           | 1.000000 | 1.687787 | 0.244816 | 0.000000 | 0.087135 | 0.300895 | 0.000001 | 0.000001 | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.255207 | 0.000000 | 0.050516 | 0.298437 | 0.000002 | 0.375521 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.000000 | 0.099805 | 0.437003 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.000000 | 0.079465 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.086032 | 0.775886 | 0.000000 | 0.131423 | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.350483 | 0.000000 | 0.126647 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.299508 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.514212 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.497878 | 0.000000 | 0.056400 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.000000 | 0.093440 | 0.281597 | 0.000000 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.687787 | 0.100418 | 0.000000 | 0.087135 | 0.300895 | 0.000001 | 0.000001 | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.050516 | 0.254930 | 0.000002 | 0.375521 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.000000 | 0.099805 | 0.344685 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.289205 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.086032 | 0.372406 | 0.000000 | 0.000001 | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.004239 | 0.000000 | 0.126647 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |



# Scores

- Overall scores –  $\text{score} = \text{sec} \times \text{des}$ 
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.046463 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.056414 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.000001 | 0.000000 | 0.000000 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.260423 | 0.000000 | 0.000000 | 0.281597 | 0.000000 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.687787 | 0.000001 | 0.000000 | 0.000000 | 0.300895 | 0.000000 | 0.000001 | 0.128377 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.050516 | 0.254930 | 0.000002 | 0.375521 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.322593 | 0.000000 | 0.000000 | 0.344685 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.036302 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.086032 | 0.372406 | 0.000000 | 0.000001 | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.004239 | 0.000000 | 0.126647 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.046463 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.056414 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.000001 | 0.000000 | 0.000000 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.000001 | 0.000000 | 0.000000 | 0.281597 | 0.000000 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.687787 | 0.000001 | 0.000000 | 0.000000 | 0.300895 | 0.000000 | 0.000001 | 0.026720 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.000000 | 0.254930 | 0.000002 | 0.375521 | 0.081914 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.000000 | 0.000000 | 0.000000 | 0.344685 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.000001 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.316475 | 0.000000 | 0.000000 | 0.372406 | 0.000000 | 0.000001 | 0.174475 |
| TDEA           | 0.750000 | 0.596819 | 0.004239 | 0.000000 | 0.126647 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.046463 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.056414 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.000001 | 0.000000 | 0.000000 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.000001 | 0.000000 | 0.000000 | 0.281597 | 0.000000 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.687787 | 0.000001 | 0.000000 | 0.000000 | 0.300895 | 0.000000 | 0.000001 | 0.000001 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.000000 | 0.254930 | 0.000002 | 0.000001 | 0.000001 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.000000 | 0.000000 | 0.000000 | 0.344685 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.000001 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.000001 | 0.000000 | 0.000000 | 0.372406 | 0.000000 | 0.000001 | 0.000001 |
| TDEA           | 0.750000 | 0.596819 | 0.004239 | 0.000000 | 0.000000 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.046450 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.056414 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.000001 | 0.000000 | 0.000000 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.000001 | 0.000000 | 0.000000 | 0.281597 | 0.000000 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.687787 | 0.000001 | 0.000000 | 0.000000 | 0.300895 | 0.000000 | 0.000001 | 0.000001 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.000000 | 0.254930 | 0.000002 | 0.000001 | 0.000001 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.000000 | 0.000000 | 0.000000 | 0.344685 | 0.000000 | 0.000001 | 0.000001 |
| PRESENT        | 0.750000 | 0.629633 | 0.000001 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.000001 | 0.000000 | 0.000000 | 0.372406 | 0.000000 | 0.000001 | 0.000001 |
| TDEA           | 0.750000 | 0.596819 | 0.003351 | 0.000000 | 0.000000 | 0.246417 | 0.000000 | 0.002950 | 0.000001 |

# Scores

- Overall scores – score = sec × des
  - Intermediate scores published online
  - In the final week, teams pushed toward zero/perfect security scores
  - Not final scores yet ...

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.764884 | 0.025684 | 0.000000 | 0.000000 | 0.271596 | 0.000000 | 0.000001 | 0.000000 |
| AES_2          | 1.000000 | 1.687749 | 0.054186 | 0.000000 | 0.000000 | 0.324694 | 0.000000 | 0.000001 | 0.000000 |
| AES_3          | 1.000000 | 1.332768 | 0.000001 | 0.000000 | 0.000000 | 0.295023 | 0.000000 | 0.000001 | 0.000000 |
| Camellia       | 0.750000 | 0.676397 | 0.000001 | 0.000000 | 0.000000 | 0.281597 | 0.000000 | 0.000001 | 0.000000 |
| CAST           | 1.000000 | 1.687787 | 0.000001 | 0.000000 | 0.000000 | 0.300895 | 0.000000 | 0.000001 | 0.000000 |
| MISTY          | 0.750000 | 3.178107 | 0.000001 | 0.000000 | 0.000000 | 0.254930 | 0.000000 | 0.000001 | 0.000000 |
| openMSP430_1   | 0.750000 | 0.841673 | 0.000000 | 0.000000 | 0.000000 | 0.344685 | 0.000000 | 0.000001 | 0.000000 |
| PRESENT        | 0.750000 | 0.629633 | 0.000001 | 0.000000 | 0.000000 | 0.319908 | 0.000000 | 0.000498 | 0.000000 |
| SEED           | 1.000000 | 2.203857 | 0.000001 | 0.000000 | 0.000000 | 0.207375 | 0.000000 | 0.000001 | 0.000000 |
| TDEA           | 0.750000 | 0.596819 | 0.003351 | 0.000000 | 0.000000 | 0.246417 | 0.000000 | 0.002950 | 0.000000 |

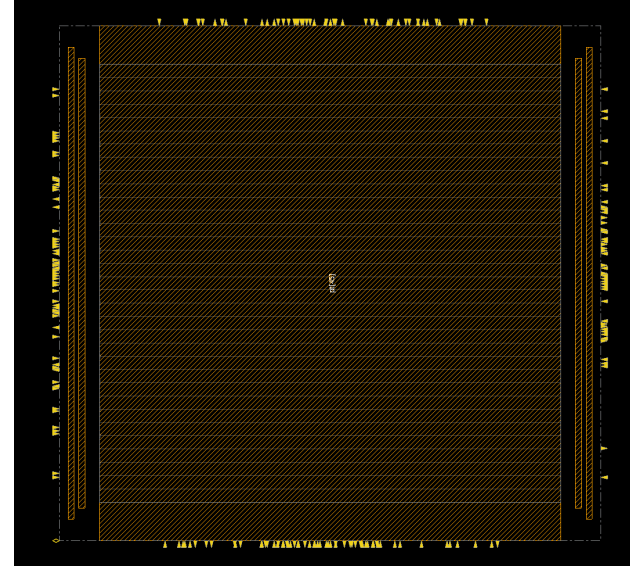
## Scores: Closer Look

- Security scores –  $\text{sec} = (\text{ti} + \text{fsp\_fi})/2$ 
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Frontside probing, fault injection – fsp\_fi: exposed areas
    - $\text{fsp\_fi} = 0.5 \times (\text{ratio of cell assets' exposed area metrics}) + 0.5 \times (\text{ratio of net assets' exposed area metrics})$
    - For this score component, 0.000001 is perfect score (rounding residue)
    - exposed areas are fully covered

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.537375 | 0.695379 | 0.000001 | 0.000001 | 0.562047 | 0.000001 | 0.000001 | 0.000001 |
| AES_2          | 1.000000 | 0.487216 | 0.000001 | 0.000001 | 0.000001 | 0.741724 | 0.000001 | 0.000001 | 0.000001 |
| AES_3          | 1.000000 | 0.374094 | 0.000001 | 0.000001 | 0.201192 | 0.476947 | 0.000001 | 0.000001 | 0.000001 |
| Camellia       | 1.000000 | 0.682213 | 0.788406 | 0.000001 | 0.431735 | 0.663271 | 0.000001 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 0.846023 | 0.119481 | 0.000001 | 0.382591 | 0.897107 | 0.000001 | 0.000001 | 0.545860 |
| MISTY          | 1.000000 | 0.592981 | 0.000001 | 0.000001 | 0.251337 | 0.832392 | 0.000001 | 0.000001 | 0.332613 |
| openMSP430_1   | 1.000000 | 0.698719 | 0.889443 | 0.000001 | 0.390164 | 0.929519 | 0.000001 | 0.000001 | 0.000001 |
| PRESENT        | 1.000000 | 0.514055 | 0.899452 | 0.000001 | 0.000001 | 0.917443 | 0.000001 | 0.000986 | 0.000001 |
| SEED           | 1.000000 | 0.820386 | 0.783684 | 0.000001 | 0.357478 | 0.886364 | 0.000001 | 0.000001 | 0.617597 |
| TDEA           | 1.000000 | 0.681616 | 0.010362 | 0.000001 | 0.432585 | 0.922771 | 0.000001 | 0.007298 | 0.000001 |

## Scores: Closer Look

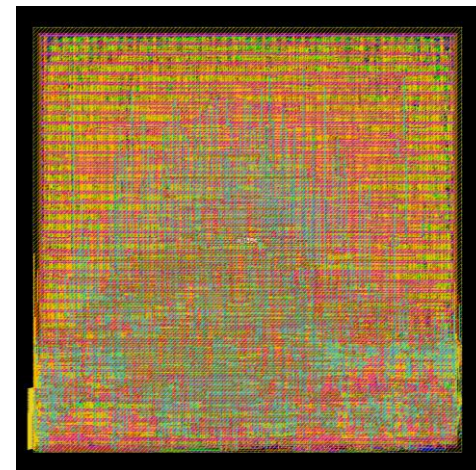
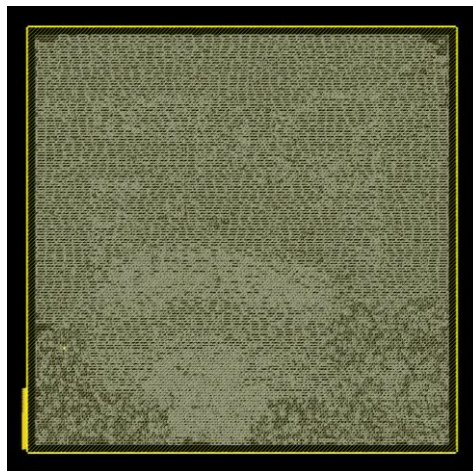
- Frontside probing, fault injection: exposed areas are fully covered
  - Pushing wires below others
  - Large-scale shielding/filling in metal layers





## Scores: Closer Look

- Large-scale shielding/filling in metal layers
  - Once such layouts came in, we thought about their acceptance
    - Valid in principle, also done in prior art
    - But, implementations here are not ideal: fully continuous in one layer; but should rather follow max width constraints and be in multiple layers
    - But, Nangate lib is missing such constraints
    - Acceptable for this 1<sup>st</sup> contest
  - PPA
    - Loss for signal routing
    - Impact on power, performance, also by coupling issues





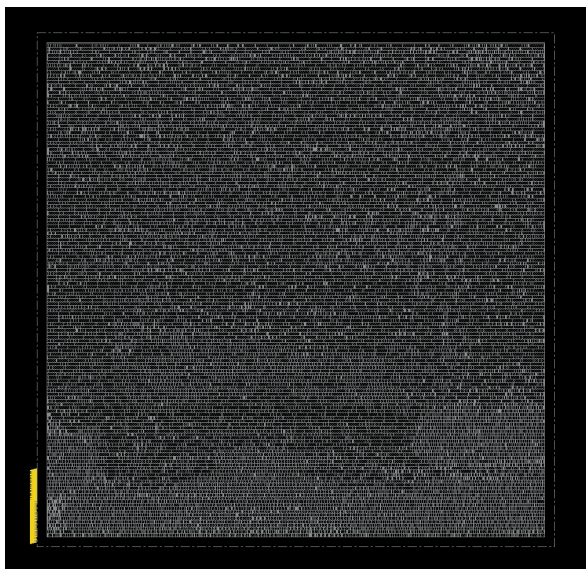
## Scores: Closer Look

- Security scores –  $\text{sec} = (\text{ti} + \text{fsp\_fi})/2$ 
    - Remarks:
      - Some intermediate results, not matching with final overall scores
      - Misalignment in table columns due to cutting off team names; order of columns same as before
    - Trojan insertion –  $\text{ti}$ : exploitable regions
      - $\text{ti} = 0.5 \times (\text{ratio of placement-sites metrics}) + 0.5 \times (\text{ratio of free-tracks metrics})$
      - For this score component, 0.000001 is perfect score (rounding residue)
- exploitable regions are fully resolved

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 1.000000 | 0.127644 | 0.000001 | 0.000001 | 0.467379 | 0.000001 | 0.000001 | 0.000001 |
| AES_2          | 1.000000 | 0.415961 | 0.160752 | 0.000001 | 0.000001 | 0.461672 | 0.000001 | 0.000001 | 0.000001 |
| AES_3          | 1.000000 | 0.616881 | 0.000001 | 0.000001 | 0.000001 | 0.564013 | 0.000001 | 0.000001 | 0.000001 |
| Camellia       | 1.000000 | 1.114042 | 0.000001 | 0.000001 | 0.000001 | 0.534155 | 0.000001 | 0.000001 | 0.000001 |
| CAST           | 1.000000 | 1.183486 | 0.000001 | 0.000001 | 0.000001 | 0.400182 | 0.000001 | 0.000001 | 0.000001 |
| MISTY          | 1.000000 | 0.675793 | 0.000001 | 0.000001 | 0.000001 | 0.281843 | 0.000001 | 0.487425 | 0.064780 |
| openMSP430_1   | 1.000000 | 1.527625 | 0.100694 | 0.000001 | 0.000001 | 0.475041 | 0.000001 | 0.000001 | 0.000001 |
| PRESENT        | 1.000000 | 1.160261 | 0.000001 | 0.000001 | 0.000001 | 0.458420 | 0.000001 | 0.000001 | 0.000001 |
| SEED           | 1.000000 | 1.478484 | 0.114483 | 0.000001 | 0.000001 | 0.773054 | 0.000001 | 0.000001 | 0.000001 |
| TDEA           | 1.000000 | 0.908223 | 0.000001 | 0.000001 | 0.000001 | 0.000001 | 0.000001 | 0.000001 | 0.000001 |

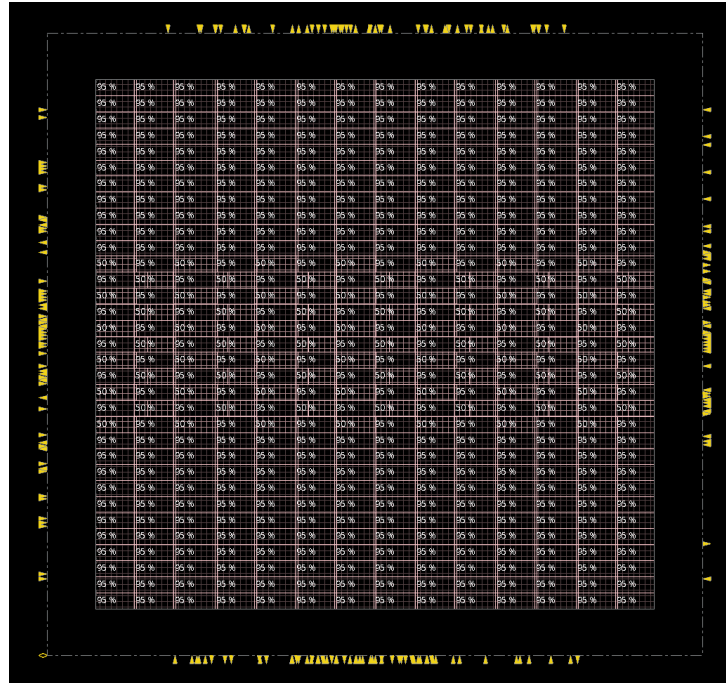
# Scores: Closer Look

- Trojan insertion: exploitable regions are fully resolved
  - Dense placement
  - Buffer insertion, shifting of cells



# Scores: Closer Look

- Trojan insertion: exploitable regions are fully resolved
  - Placement blockages



## Scores: Closer Look

- Design quality – des: 25% each P, P, A, and design checks
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Design quality overall

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.995052 | 0.727824 | 0.479853 | 0.566082 | 0.527666 | 0.519014 | 1.347145 | 0.481524 |
| AES_2          | 1.000000 | 3.737360 | 0.701868 | 0.480159 | 0.565557 | 0.539630 | 0.542897 | 0.817556 | 0.576584 |
| AES_3          | 1.000000 | 2.689809 | 1.059384 | 0.506518 | 0.560662 | 0.566830 | 0.558620 | 1.171381 | 0.626798 |
| Camellia       | 0.750001 | 0.753120 | 0.660631 | 0.572059 | 0.432859 | 0.470338 | 0.663935 | 0.960094 | 0.847907 |
| CAST           | 1.000000 | 1.663247 | 0.842882 | 0.655517 | 0.455500 | 0.463882 | 0.813554 | 0.908418 | 0.470367 |
| MISTY          | 0.750001 | 5.009729 | 0.753397 | 0.626052 | 0.401977 | 0.457588 | 2.221631 | 1.540835 | 0.412254 |
| openMSP430_1   | 0.750001 | 0.756103 | 0.651614 | 0.582285 | 0.511604 | 0.490809 | 0.469361 | 1.025052 | 0.862262 |
| PRESENT        | 0.750001 | 0.752108 | 0.643068 | 0.534645 | 0.454638 | 0.465029 | 0.446817 | 1.009782 | 0.338117 |
| SEED           | 1.000000 | 1.917339 | 0.704713 | 0.658610 | 0.481326 | 0.448839 | 0.590343 | 0.924394 | 0.565012 |
| TDEA           | 0.750001 | 0.750792 | 0.818137 | 0.511633 | 0.585536 | 0.534081 | 0.524128 | 0.808416 | 1.042386 |

## Scores: Closer Look

- Design quality – des: 25% each P, P, A, and design checks
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Power: total power

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.999920 | 1.055803 | 0.919411 | 1.264325 | 1.024430 | 1.169358 | 1.146155 | 1.055397 |
| AES_2          | 1.000000 | 0.983725 | 0.964468 | 0.908431 | 1.262225 | 1.104672 | 1.130548 | 1.148666 | 1.000781 |
| AES_3          | 1.000000 | 1.017179 | 1.002526 | 1.026071 | 1.165557 | 0.958669 | 1.043793 | 1.010067 | 1.027404 |
| Camellia       | 1.000000 | 1.012478 | 1.071311 | 1.273528 | 1.167043 | 1.031619 | 1.025791 | 1.689640 | 1.400828 |
| CAST           | 1.000000 | 1.005019 | 1.053176 | 1.599079 | 1.204106 | 1.012866 | 1.096223 | 1.258500 | 1.259574 |
| MISTY          | 1.000000 | 1.011458 | 1.065396 | 1.458230 | 1.042220 | 1.026266 | 1.028274 | 1.565143 | 1.089575 |
| openMSP430_1   | 1.000000 | 1.024409 | 1.034788 | 1.323662 | 1.184008 | 1.006134 | 1.170645 | 2.064591 | 1.624873 |
| PRESENT        | 1.000000 | 1.008428 | 0.974512 | 1.109592 | 1.120440 | 1.119266 | 1.064902 | 1.850723 | 0.620249 |
| SEED           | 1.000000 | 1.003029 | 1.157018 | 1.611448 | 1.278039 | 1.031075 | 1.082790 | 1.347932 | 1.405636 |
| TDEA           | 1.000000 | 1.003167 | 1.079209 | 1.011031 | 1.282972 | 1.085703 | 1.084677 | 1.008808 | 1.422190 |

## Scores: Closer Look

- Design quality – des: 25% each P, P, A, and design checks
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Performance: 50% TNS + 33.3% WNS + 16.6% FEP

| Team/Benchmark | Baseline | J         | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|-----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 0.980286  | 0.055511 | 0.000000 | 0.000000 | 0.054797 | 0.000000 | 2.200922 | 0.000000 |
| AES_2          | 1.000000 | 11.866604 | 0.019651 | 0.000000 | 0.000000 | 0.025496 | 0.116607 | 0.076440 | 0.000000 |
| AES_3          | 1.000000 | 7.710835  | 1.234630 | 0.000000 | 0.000000 | 0.229646 | 0.053532 | 1.664033 | 0.000000 |
| Camellia       | 0.000000 | 0.000000  | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 |
| CAST           | 1.000000 | 3.647969  | 0.101282 | 0.000000 | 0.000000 | 0.107806 | 0.532876 | 0.151035 | 0.000000 |
| MISTY          | 0.000000 | 17.027459 | 0.000000 | 0.000000 | 0.000000 | 0.176666 | 7.215142 | 2.345324 | 0.000000 |
| openMSP430_1   | 0.000000 | 0.000000  | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 |
| PRESENT        | 0.000000 | 0.000000  | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 |
| SEED           | 1.000000 | 4.666328  | 0.009352 | 0.000000 | 0.000000 | 0.029426 | 0.607236 | 0.073780 | 0.182626 |
| TDEA           | 0.000000 | 0.000000  | 0.000000 | 0.000000 | 0.000000 | 0.168332 | 0.000000 | 0.000000 | 0.000000 |

## Scores: Closer Look

- Design quality – des: 25% each P, P, A, and design checks
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Area: die area

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 1.000000 | 0.799986 | 1.000000 | 1.000000 | 0.924433 | 0.906699 | 1.000000 | 0.870319 |
| AES_2          | 1.000000 | 1.000000 | 0.851834 | 1.000000 | 1.000000 | 0.924433 | 0.924433 | 1.000000 | 0.841431 |
| AES_3          | 1.000000 | 1.000000 | 1.000000 | 1.000000 | 1.077089 | 0.972002 | 1.137157 | 1.000000 | 1.064325 |
| Camellia       | 1.000000 | 1.000000 | 0.571215 | 1.000000 | 0.564392 | 0.842380 | 0.629949 | 1.000000 | 0.590064 |
| CAST           | 1.000000 | 1.000000 | 0.625118 | 1.000000 | 0.617892 | 0.734859 | 0.625118 | 1.000000 | 0.621894 |
| MISTY          | 1.000000 | 1.000000 | 0.568883 | 1.000000 | 0.565687 | 0.627421 | 0.643109 | 1.000000 | 0.559443 |
| openMSP430_1   | 1.000000 | 1.000000 | 0.571664 | 1.000000 | 0.578845 | 0.691350 | 0.630086 | 1.000000 | 0.607737 |
| PRESENT        | 1.000000 | 1.000000 | 0.597758 | 1.000000 | 0.611155 | 0.740848 | 0.722367 | 1.000000 | 0.609028 |
| SEED           | 1.000000 | 1.000000 | 0.652484 | 1.000000 | 0.647267 | 0.734859 | 0.671348 | 1.000000 | 0.671786 |
| TDEA           | 1.000000 | 1.000000 | 0.897483 | 1.000000 | 1.000000 | 0.864542 | 1.000000 | 1.000000 | 0.877532 |

## Scores: Closer Look

- Design quality – des: 25% each P, P, A, and design checks
  - Remarks:
    - Some intermediate results, not matching with final overall scores
    - Misalignment in table columns due to cutting off team names; order of columns same as before
  - Design checks: Non-equivalent points, Unreachable points, Undriven pins, Open output ports, Net output floating, Basic routing issues, Module pin issues, Unplaced components issues, Placement and/or routing issues, DRC issues
    - Equivalence checks acting as constraints; metrics only for information
    - Additional constraints not covered in metrics: maintaining of assets, ratio of PG metals to die area
    - Some effort to penalize trivial approaches, e.g., open output ports *may* indicate cells acting as fillers

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1.000000 | 1.000000 | 1.000000 | 0.000000 | 0.000000 | 0.107006 | 0.000000 | 1.041507 | 0.000380 |
| AES_2          | 1.000000 | 1.099112 | 0.971523 | 0.012204 | 0.000000 | 0.103920 | 0.000000 | 1.045118 | 0.464127 |
| AES_3          | 1.000000 | 1.031226 | 1.000380 | 0.000000 | 0.000000 | 0.107006 | 0.000000 | 1.011424 | 0.415460 |
| Camellia       | 1.000000 | 1.000000 | 1.000000 | 0.014705 | 0.000000 | 0.007352 | 1.000000 | 1.150735 | 1.400735 |
| CAST           | 1.000000 | 1.000000 | 1.591954 | 0.022988 | 0.000000 | 0.000000 | 1.000000 | 1.224137 | 0.000000 |
| MISTY          | 1.000000 | 1.000000 | 1.379310 | 0.045977 | 0.000000 | 0.000000 | 0.000000 | 1.252873 | 0.000000 |
| openMSP430_1   | 1.000000 | 1.000000 | 1.000000 | 0.005479 | 0.283561 | 0.265753 | 0.076712 | 1.035616 | 1.216438 |
| PRESENT        | 1.000000 | 1.000000 | 1.000000 | 0.028985 | 0.086956 | 0.000000 | 0.000000 | 1.188405 | 0.123188 |
| SEED           | 1.000000 | 1.000000 | 1.000000 | 0.022988 | 0.000000 | 0.000000 | 0.000000 | 1.275862 | 0.000000 |
| TDEA           | 1.000000 | 1.000000 | 1.295857 | 0.035502 | 0.059171 | 0.017751 | 0.011834 | 1.224852 | 1.869822 |



# Scores

- Final overall scores, including “blind” benchmarks
  - Remark on difference between 0 and 0.000001: for latter, at least one design metric is right at or above baseline
    - Utilized during ranking

| Team/Benchmark | Baseline | J         | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|-----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1        | 0.764884  | 0.025684 | 0        | 0        | 0.271596 | 0        | 0.000001 | 0        |
| AES_2          | 1        | 1.687.749 | 0.054186 | 0        | 0        | 0.324694 | 0        | 0.000001 | 0        |
| AES_3          | 1        | 1.332.768 | 0.000001 | 0        | 0        | 0.295023 | 0        | 0.000001 | 0        |
| Camellia       | 0.75     | 0.676397  | 0.000001 | 0        | 0        | 0.281597 | 0        | 0.000001 | 0        |
| CAST           | 1        | 1.687.787 | 0.000001 | 0        | 0        | 0.300895 | 0        | 0.000001 | 0        |
| MISTY          | 0.75     | 3.178.107 | 0.000001 | 0        | 0        | 0.25493  | 0        | 0.000001 | 0        |
| openMSP430_1   | 0.75     | 0.841673  | 0        | 0        | 0        | 0.344685 | 0        | 0.000001 | 0        |
| PRESENT        | 0.75     | 0.629633  | 0.000001 | 0        | 0        | 0.319908 | 0        | 0.000498 | 0        |
| SEED           | 1        | 2.203.857 | 0.000001 | 0        | 0        | 0.207375 | 0        | 0.000001 | 0        |
| TDEA           | 0.75     | 0.596819  | 0.003351 | 0        | 0        | 0.246417 | 0        | 0.00295  | 0        |
| openMSP430_2   | 1        | 1.031.415 | 0.000001 | 0        | 0        | 0.822795 | 0        | 0.000001 | 0        |
| SPARX          | 0.75     | 0.476022  | 0        | 0        | 0        | 0.262042 | 0        | 0.000001 | 0        |
| Average        |          | 1.258926  | 0.006936 | 0.000000 | 0.000000 | 0.327663 | 0.000000 | 0.000288 | 0.000000 |
| Ranking        |          | 8         | 6        | 2.5      | 2.5      | 7        | 2.5      | 5        | 2.5      |

# Scores

- Final design quality as tie-breaker
  - But, needs to be considered for benchmarks individually, not on average numbers
    - Ranking teams on each benchmark

| Team/Benchmark | Baseline | J        | N        | O        | E        | L        | A        | Q        | K        |
|----------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| AES_1          | 1        | 0.995052 | 0.71369  | 0.447645 | 0.475469 | 0.527666 | 0.519014 | 1.347145 | 0.481524 |
| AES_2          | 1        | 3.73736  | 0.70258  | 0.425056 | 0.458233 | 0.53963  | 0.509517 | 0.817556 | 0.46194  |
| AES_3          | 1        | 2.689809 | 1.059384 | 0.473199 | 0.498813 | 0.56683  | 0.541594 | 1.171381 | 0.523694 |
| Camellia       | 0.750001 | 0.75312  | 0.746845 | 0.398203 | 0.420739 | 0.470338 | 0.41833  | 0.960094 | 0.530811 |
| CAST           | 1        | 1.663247 | 0.851448 | 0.412035 | 0.409304 | 0.463882 | 0.439133 | 0.908418 | 0.495626 |
| MISTY          | 0.750001 | 5.009729 | 0.753397 | 0.418306 | 0.396844 | 0.457588 | 0.417127 | 1.559165 | 0.458744 |
| openMSP430_1   | 0.750001 | 0.756103 | 0.656623 | 0.406426 | 0.440711 | 0.490809 | 0.469361 | 1.025052 | 0.632471 |
| PRESENT        | 0.750001 | 0.752108 | 0.693259 | 0.359781 | 0.427651 | 0.465029 | 0.446817 | 1.009782 | 0.306888 |
| SEED           | 1        | 1.917339 | 0.892326 | 0.416061 | 0.442646 | 0.418221 | 0.44251  | 0.924394 | 0.522025 |
| TDEA           | 0.750001 | 0.750792 | 0.846279 | 0.459273 | 0.526013 | 0.534081 | 0.524128 | 0.808416 | 0.58438  |
| openMSP430_2   | 1        | 0.995805 | 0.77722  | 0.46401  | 0.543684 | 0.524049 | 0.570014 | 0.848032 | 0.608243 |
| SPARX          | 0.750001 | 0.753974 | 0.663144 | 0.397067 | 0.420406 | 0.422185 | 0.404258 | 1.047701 | 0.509065 |
| Average        |          | 1.731203 | 0.779683 | 0.423089 | 0.455043 | 0.490026 | 0.475150 | 1.035595 | 0.509618 |
| Ranking        |          | 8        | 6        | 1        | 2        | 4        | 3        | 7        | 5        |

# Rankings for Benchmarks

- Ranks for overall scores
  - Remarks on average ranks:
    - Relative consistency across benchmarks; maintains range
    - The more teams did best, the easier the benchmark was in the context of the competition, and thus the higher the related average rank (w/ lower ranks being better achievements)

| Team/Benchmark | J | N   | O   | E   | L | A   | Q   | K   |
|----------------|---|-----|-----|-----|---|-----|-----|-----|
| AES_1          | 8 | 6   | 2.5 | 2.5 | 7 | 2.5 | 5   | 2.5 |
| AES_2          | 8 | 6   | 2.5 | 2.5 | 7 | 2.5 | 5   | 2.5 |
| AES_3          | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| Camellia       | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| CAST           | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| MISTY          | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| openMSP430_1   | 8 | 3   | 3   | 3   | 7 | 3   | 6   | 3   |
| PRESENT        | 8 | 5   | 2.5 | 2.5 | 7 | 2.5 | 6   | 2.5 |
| SEED           | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| TDEA           | 8 | 6   | 2.5 | 2.5 | 7 | 2.5 | 5   | 2.5 |
| openMSP430_2   | 8 | 5.5 | 2.5 | 2.5 | 7 | 2.5 | 5.5 | 2.5 |
| SPARX          | 8 | 3   | 3   | 3   | 7 | 3   | 6   | 3   |

# Rankings for Benchmarks

- Ranks for design quality
  - Remarks on average ranks:
    - Relative consistency across benchmarks; maintains range
    - The more teams did best, the easier the benchmark was in the context of the competition, and thus the higher the related average rank (w/ lower ranks being better achievements)

| Team/Benchmark | J | N | O | E | L | A | Q | K |
|----------------|---|---|---|---|---|---|---|---|
| AES_1          | 7 | 6 | 1 | 2 | 5 | 4 | 8 | 3 |
| AES_2          | 8 | 6 | 1 | 2 | 5 | 4 | 7 | 3 |
| AES_3          | 8 | 6 | 1 | 2 | 5 | 4 | 7 | 3 |
| Camellia       | 7 | 6 | 1 | 3 | 4 | 2 | 8 | 5 |
| CAST           | 8 | 6 | 2 | 1 | 4 | 3 | 7 | 5 |
| MISTY          | 8 | 6 | 3 | 1 | 4 | 2 | 7 | 5 |
| openMSP430_1   | 7 | 6 | 1 | 2 | 4 | 3 | 8 | 5 |
| PRESENT        | 7 | 6 | 2 | 3 | 5 | 4 | 8 | 1 |
| SEED           | 8 | 6 | 1 | 4 | 2 | 3 | 7 | 5 |
| TDEA           | 6 | 8 | 1 | 3 | 4 | 2 | 7 | 5 |
| openMSP430_2   | 8 | 6 | 1 | 3 | 2 | 4 | 7 | 5 |
| SPARX          | 7 | 6 | 1 | 3 | 4 | 2 | 8 | 5 |

# Rankings for Benchmarks

- Combined, weighted ranks
  - $r(\text{OVERALL}) + 0.01 * r(\text{des})$
  - 3rd digit represents des; e.g., team N for AES\_2 had rank 6 for overall scores and ranks 6 for design quality

| Team/Benchmark | J      | N      | O      | E      | L      | A      | Q      | K      |
|----------------|--------|--------|--------|--------|--------|--------|--------|--------|
| AES_1          | 8.07   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.08   | 2.53   |
| AES_2          | 8.08   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.07   | 2.53   |
| AES_3          | 8.08   | 5.56   | 2.51   | 2.52   | 7.05   | 2.54   | 5.57   | 2.53   |
| Camellia       | 8.07   | 5.56   | 2.51   | 2.53   | 7.04   | 2.52   | 5.58   | 2.55   |
| CAST           | 8.08   | 5.56   | 2.52   | 2.51   | 7.04   | 2.53   | 5.57   | 2.55   |
| MISTY          | 8.08   | 5.56   | 2.53   | 2.51   | 7.04   | 2.52   | 5.57   | 2.55   |
| openMSP430_1   | 8.07   | 3.06   | 3.01   | 3.02   | 7.04   | 3.03   | 6.08   | 3.05   |
| PRESENT        | 8.07   | 5.06   | 2.52   | 2.53   | 7.05   | 2.54   | 6.08   | 2.51   |
| SEED           | 8.08   | 5.56   | 2.51   | 2.54   | 7.02   | 2.53   | 5.57   | 2.55   |
| TDEA           | 8.06   | 6.08   | 2.51   | 2.53   | 7.04   | 2.52   | 5.07   | 2.55   |
| openMSP430_2   | 8.08   | 5.56   | 2.51   | 2.53   | 7.02   | 2.54   | 5.57   | 2.55   |
| SPARX          | 8.07   | 3.06   | 3.01   | 3.03   | 7.04   | 3.02   | 6.08   | 3.05   |
| Average        | 8.0742 | 5.2283 | 2.5967 | 2.6075 | 7.0400 | 2.6142 | 5.5742 | 2.6250 |
|                |        |        |        |        |        |        |        |        |
|                |        |        |        |        |        |        |        |        |
|                |        |        |        |        |        |        |        |        |

# Rankings for Benchmarks

- Combined, weighted ranks
  - $r(\text{OVERALL}) + 0.01 * r(\text{des})$
  - 3rd digit represents des; e.g., team N for AES\_2 had rank 6 for overall scores and ranks 6 for design quality

| Team/Benchmark | J      | N      | O      | E      | L      | A      | Q      | K      |
|----------------|--------|--------|--------|--------|--------|--------|--------|--------|
| AES_1          | 8.07   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.08   | 2.53   |
| AES_2          | 8.08   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.07   | 2.53   |
| AES_3          | 8.08   | 5.56   | 2.51   | 2.52   | 7.05   | 2.54   | 5.57   | 2.53   |
| Camellia       | 8.07   | 5.56   | 2.51   | 2.53   | 7.04   | 2.52   | 5.58   | 2.55   |
| CAST           | 8.08   | 5.56   | 2.52   | 2.51   | 7.04   | 2.53   | 5.57   | 2.55   |
| MISTY          | 8.08   | 5.56   | 2.53   | 2.51   | 7.04   | 2.52   | 5.57   | 2.55   |
| openMSP430_1   | 8.07   | 3.06   | 3.01   | 3.02   | 7.04   | 3.03   | 6.08   | 3.05   |
| PRESENT        | 8.07   | 5.06   | 2.52   | 2.53   | 7.05   | 2.54   | 6.08   | 2.51   |
| SEED           | 8.08   | 5.56   | 2.51   | 2.54   | 7.02   | 2.53   | 5.57   | 2.55   |
| TDEA           | 8.06   | 6.08   | 2.51   | 2.53   | 7.04   | 2.52   | 5.07   | 2.55   |
| openMSP430_2   | 8.08   | 5.56   | 2.51   | 2.53   | 7.02   | 2.54   | 5.57   | 2.55   |
| SPARX          | 8.07   | 3.06   | 3.01   | 3.03   | 7.04   | 3.02   | 6.08   | 3.05   |
| Average        | 8.0742 | 5.2283 | 2.5967 | 2.6075 | 7.0400 | 2.6142 | 5.5742 | 2.6250 |
| Final ranking  | 7      | 4      | 1      | 2      | 6      | 3      | 5      | 3      |

# Rankings for Benchmarks

- Combined, weighted ranks
  - $r(\text{OVERALL}) + 0.01 * r(\text{des})$
  - 3rd digit represents des; e.g., team N for AES\_2 had rank 6 for overall scores and ranks 6 for design quality

| Team/Benchmark       | ---    | UT_pda | ???    | ???    | TCLAB  | ???    | DASYS  | ???    |
|----------------------|--------|--------|--------|--------|--------|--------|--------|--------|
| AES_1                | 8.07   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.08   | 2.53   |
| AES_2                | 8.08   | 6.06   | 2.51   | 2.52   | 7.05   | 2.54   | 5.07   | 2.53   |
| AES_3                | 8.08   | 5.56   | 2.51   | 2.52   | 7.05   | 2.54   | 5.57   | 2.53   |
| Camellia             | 8.07   | 5.56   | 2.51   | 2.53   | 7.04   | 2.52   | 5.58   | 2.55   |
| CAST                 | 8.08   | 5.56   | 2.52   | 2.51   | 7.04   | 2.53   | 5.57   | 2.55   |
| MISTY                | 8.08   | 5.56   | 2.53   | 2.51   | 7.04   | 2.52   | 5.57   | 2.55   |
| openMSP430_1         | 8.07   | 3.06   | 3.01   | 3.02   | 7.04   | 3.03   | 6.08   | 3.05   |
| PRESENT              | 8.07   | 5.06   | 2.52   | 2.53   | 7.05   | 2.54   | 6.08   | 2.51   |
| SEED                 | 8.08   | 5.56   | 2.51   | 2.54   | 7.02   | 2.53   | 5.57   | 2.55   |
| TDEA                 | 8.06   | 6.08   | 2.51   | 2.53   | 7.04   | 2.52   | 5.07   | 2.55   |
| openMSP430_2         | 8.08   | 5.56   | 2.51   | 2.53   | 7.02   | 2.54   | 5.57   | 2.55   |
| SPARX                | 8.07   | 3.06   | 3.01   | 3.03   | 7.04   | 3.02   | 6.08   | 3.05   |
| Average              | 8.0742 | 5.2283 | 2.5967 | 2.6075 | 7.0400 | 2.6142 | 5.5742 | 2.6250 |
| <u>Final ranking</u> | 7      | 4      | 1      | 2      | 6      | 3      | 5      | 3      |

# Winners



**3<sup>rd</sup> place:  
CUEDA**



**3<sup>rd</sup> place:  
TalTech**



# Winners



**2<sup>nd</sup> place:**  
**NTUsplace**



**3<sup>rd</sup> place:**  
**CUEDA**



**3<sup>rd</sup> place:**  
**TalTech**

## Winners



**2<sup>nd</sup> place:  
NTUsplace**



**1<sup>st</sup> place:  
XDSecurity**



**3<sup>rd</sup> place:  
CUEDA**



**3<sup>rd</sup> place:  
TalTech**

# Winners



**2<sup>nd</sup> place:  
NTUsplace**



**1<sup>st</sup> place:  
XDSecurity**



**3<sup>rd</sup> place:  
CUEDA**



**3<sup>rd</sup> place:  
TalTech**

## Honorable Mentions:

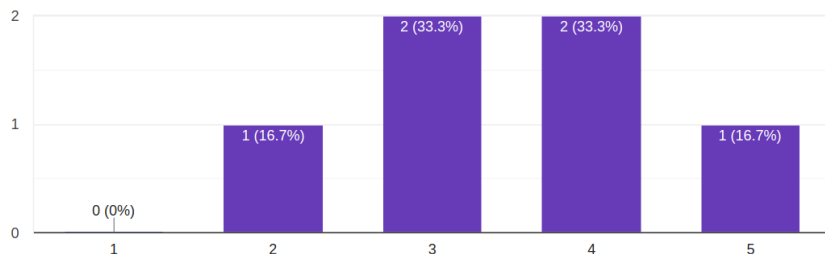
- **CUEDA** for sharing a fast evaluation tool for frontside probing, fault injection for the backend
  - **TalTech** for important feedback for the backend's design flow settings

# Survey

- Selected insights
- Scale: none (1) to excellent (5)

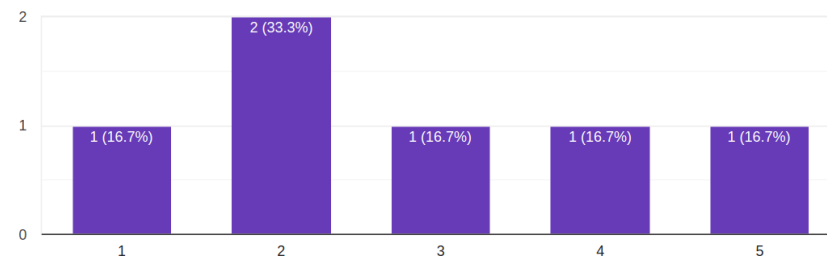
Team's prior experience with physical design in general?

6 responses



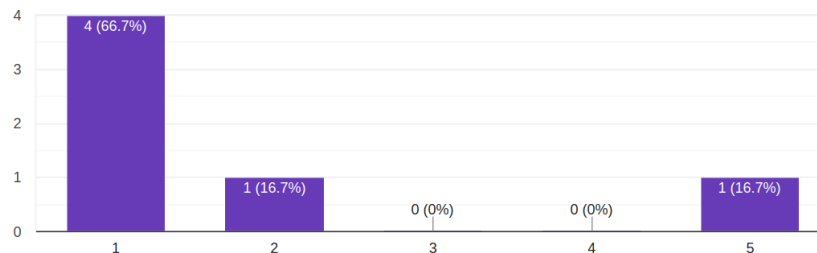
Team's prior experience with design closure, i.e., working on post-layout netlist and DEF?

6 responses



Team's prior experience with hardware security in general?

6 responses



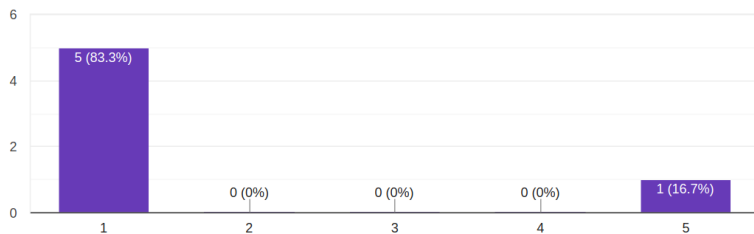
# Survey

- Selected insights
- Scale: none (1) to excellent (5)

Team's prior experience with Trojans (for attack implementation and/or defense implementation)?



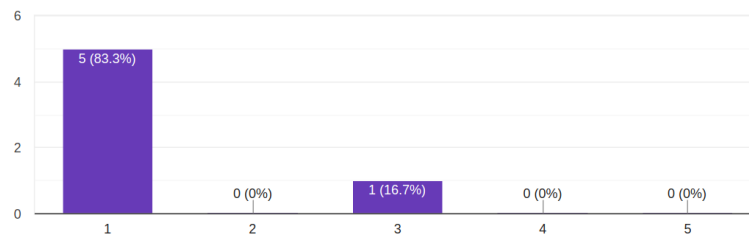
6 responses



Team's prior experience with probing (for attack implementation and/or defense implementation)?



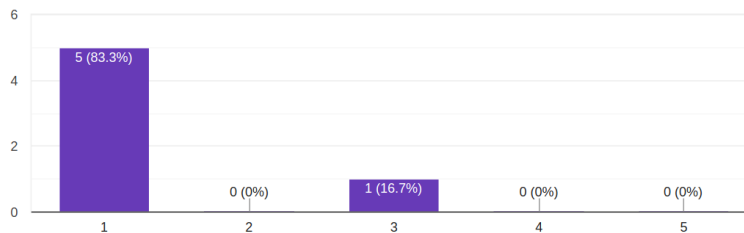
6 responses



Team's prior experience with fault injection (for attack implementation and/or defense implementation)?



6 responses



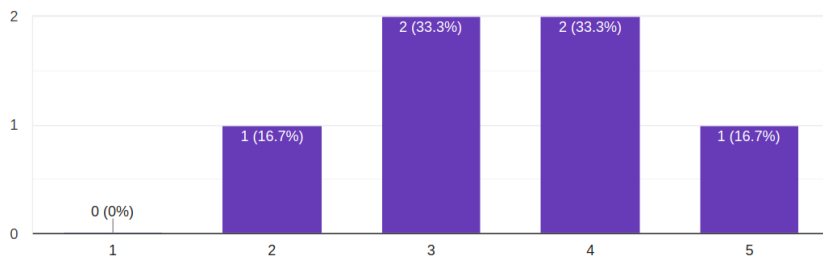
# Survey

- Selected insights
- Scale: not enough (1) to excellent (5)

Team's rating for the material, discussion, and feedback provided during the contest?

 Copy

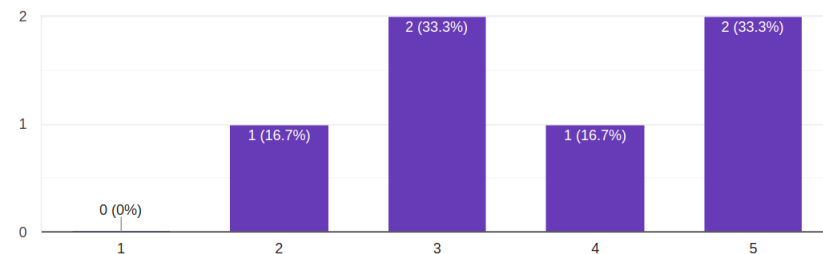
6 responses



Team's rating for the experience and learning outcome for the contest overall?

 Copy

6 responses

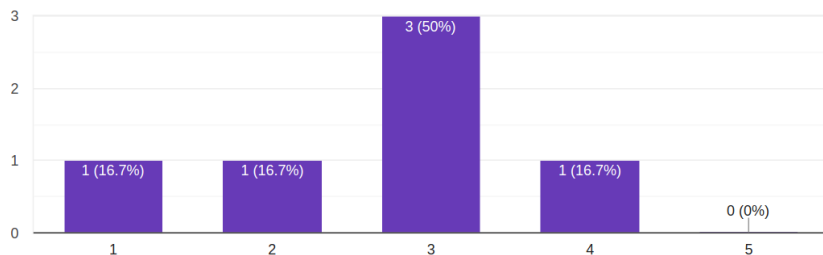


# Survey

- Selected insights
- Scale: too tight/difficult (1) to too lax/easy (5)

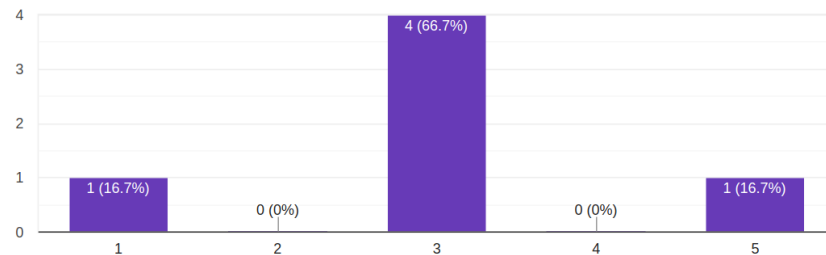
Team's rating for the timeline of the contest?

6 responses



Team's rating for the scope of the contest?

6 responses



## Conclusion Part 2

- First-ever contest on security closure of physical layouts
  - Build knowledge and experience within the community for security and its close relation to physical design
  - Great efforts from all!



Congrats and thanks again!  
See you for next year's contest!

