Benchmarking Advanced Security Closure of Physical Layouts ISPD 2023 Contest

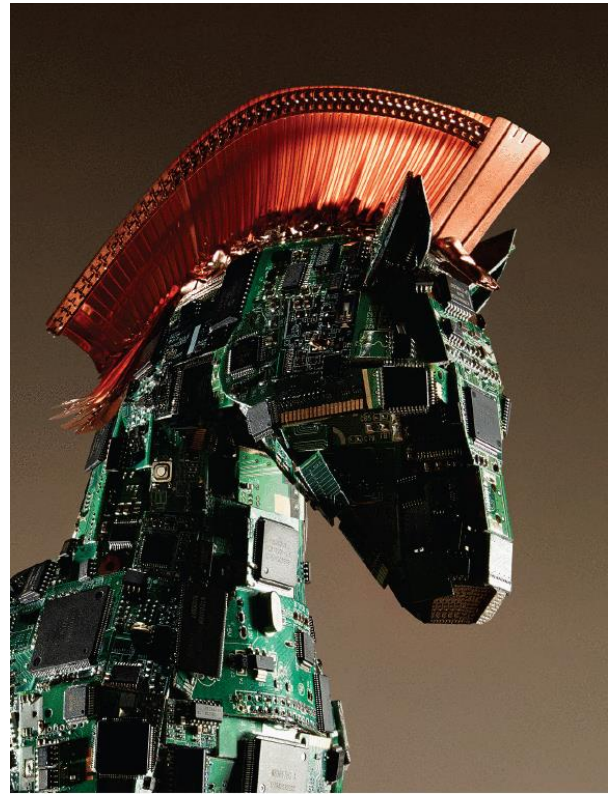
Mohammad Eslami[1], Johann Knechtel[2], Ozgur Sinanoglu[2], Ramesh Karri[3], Samuel Pagliarini[1]

Tallinn University of Technology (TalTech)[1], NYU Abu Dhabi[2], NYU New York[3]

Overview

- Motivation:
  - More and more threats are arising that affect hardware
  - Build up related knowledge and experience in CAD community

- Main theme:
  - Incorporating techniques for designing secure and trustworthy ICs in future CAD flows
  - Hardening layouts at design time against threats that are executed post-design: this year, Hardware trojan horses



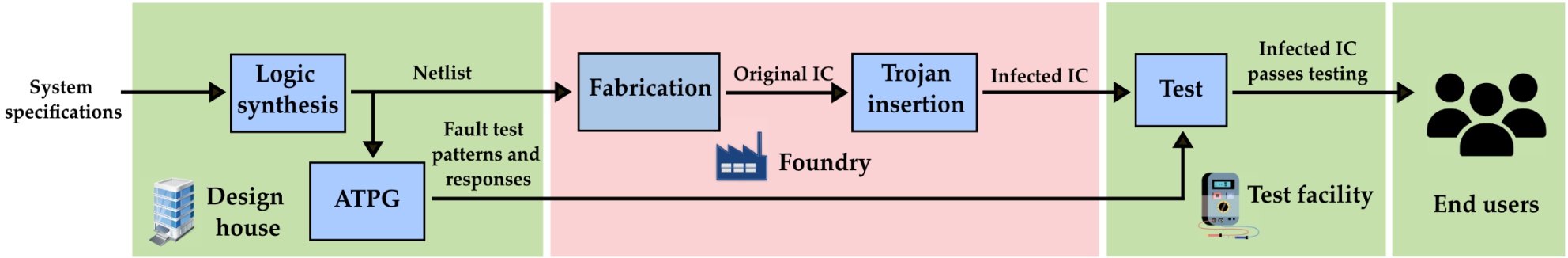
Part 1: background, some details on contest; Part 2: teams, rankings, awards

Background: Hardware Trojans

IC Supply Chain and Threats:

- Companies outsource the fabrication process to third parties
- New challenges to the security and trustworthiness of ICs since there is significantly less control and oversight during the fabrication process

Hardware Trojan: a generic term for malicious modifications to a design, either via addition, subtraction, or replacement of the existing logic



N. Limaye et al., 2022. PolyWorm: Leveraging Polymorphic Behavior to Implant Hardware Trojans. Trans. Emerg. Top. Comp. 10, 3 (2022), 1443–1455

Contest Objectives

- Implement physical-design measures to proactively harden layouts against post-design Trojan insertion during mask generation or manufacturing

- Participants would want to enhance the security while accounting for the impact on design checks and PPA by the defense approach

- There is no single, right or wrong approach toward that end; a complex multi-objective problem

Benchmarks

- 6 different crypto cores as benchmarks:

  AES128, Camellia, CAST, MISTY, SEED, and SHA256

- Different sizes and complexities, ensuring different difficulty levels across the benchmarks
- Cadence Genus for logic synthesis
- Cadence Innovus for physical implementation
- Custom timing constraints for each benchmark
- Optimization is refrained from on purpose, to keep some margin for the teams to work with
- The vanilla scripts for logical and physical synthesis have been made available early to help the participants adapt to the ASAP7 library

Benchmarks

ASAP7 PDK and Library:

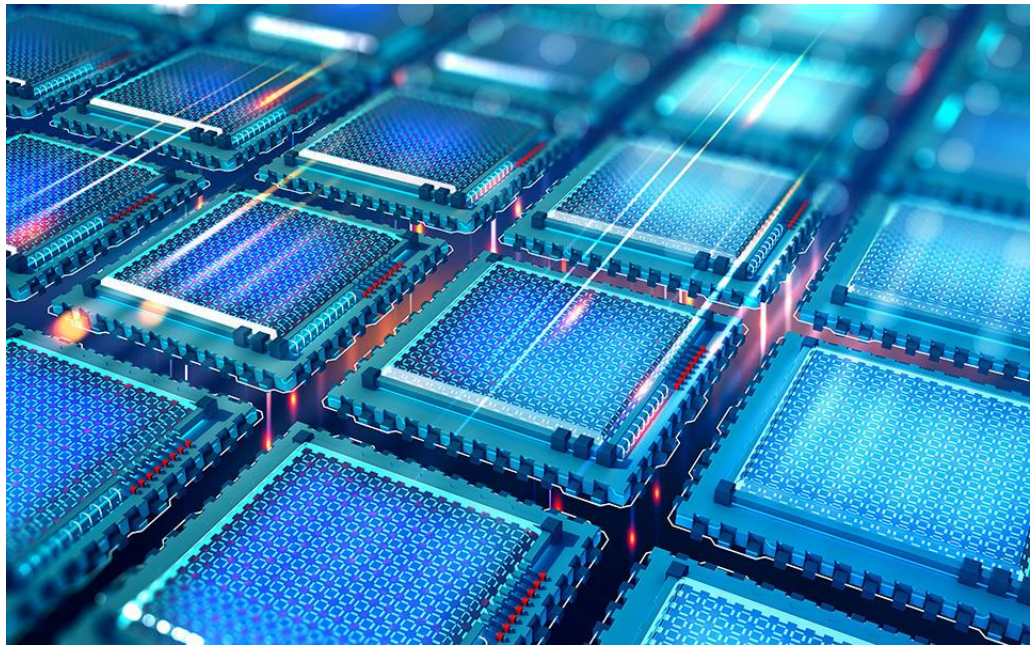
- Originally developed by teams from Arizona State and ARM
- Likely the most complete PDK developed by academia
- Many files provided do resemble a commercial PDK, including multi-Vth cells, extraction decks, DRC decks
- A few modifications were made to the library:
  - Addition of colored metals
  - Introduced max density rules for all metal layers

- Replaces the Nangate 45nm Open Cell Library used in 2022

Benchmarks

The benchmark release includes:

- The post-route Verilog netlist and DEF file
- Design database
- The SDC timing files
- List of cell assets
- The reports for the evaluation
- Scoring of the baseline layout
- Evaluation and scoring scripts

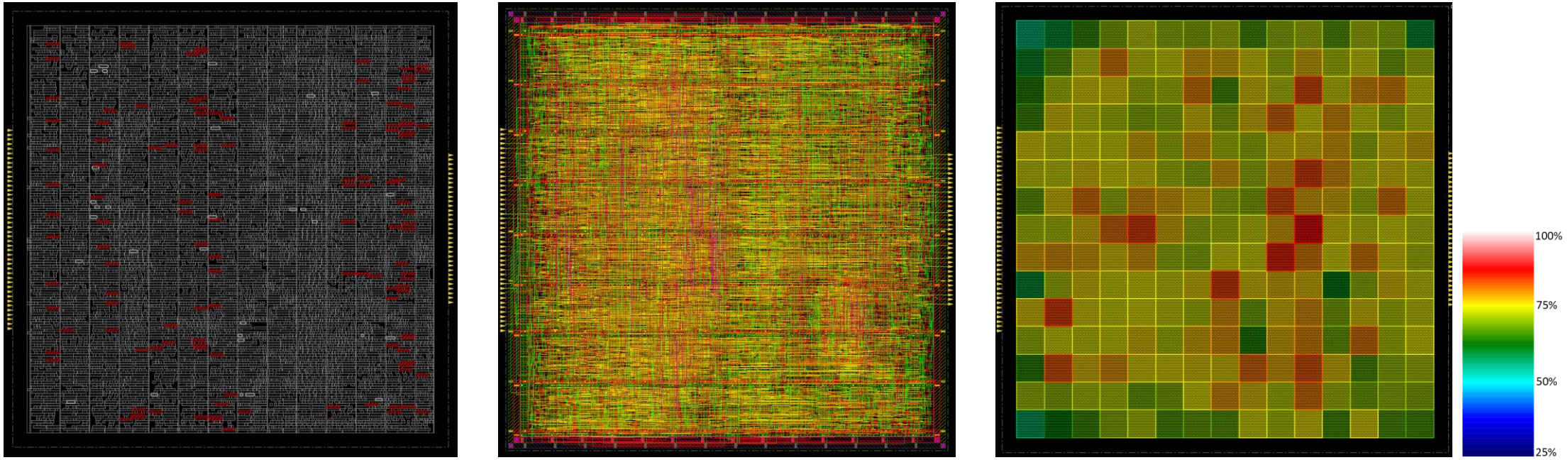


nist.gov

- https://wp.nyu.edu/ispd23_contest
- Benchmarks will stay online
- Best results will be published

Sample Benchmark: SHA256

A sample benchmark was provided early on as a warm-up design to help get familiar ASAP7 as well as to adapt to the stricter rules and constraints of this year's contest.

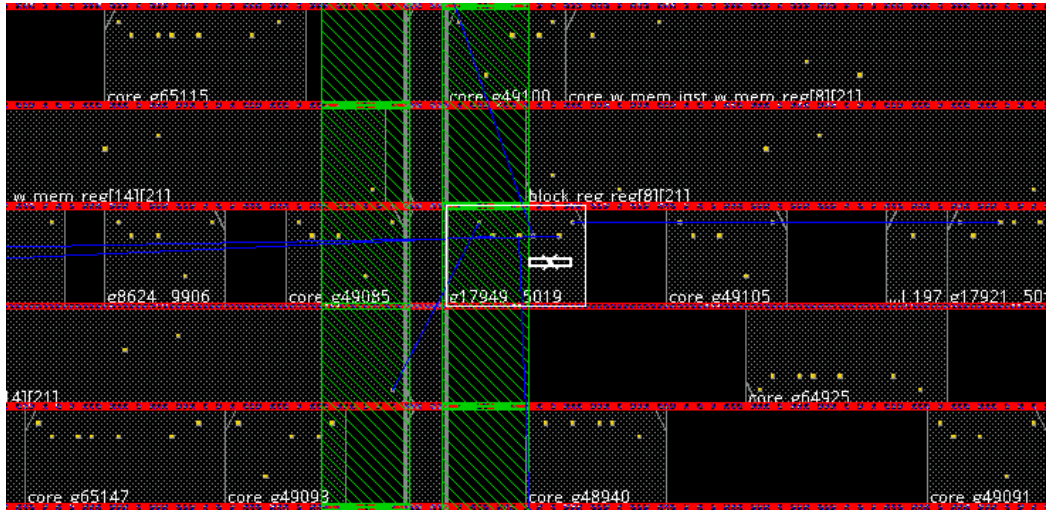


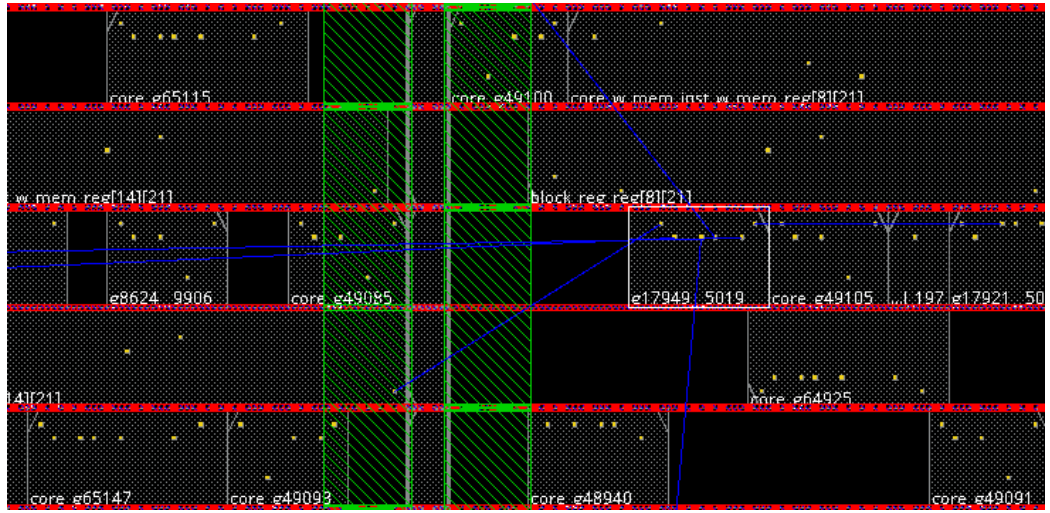
Implementation Flow

1) Defining global variables: library files, design files, timing, etc.
2) Floorplanning and PDN planning: ring spacing, offset, and size; stripe-to-stripe distance
3) Pin Assignment: all input pins on the left side and all the output pins on the right side.
4) PDN: core rings in M6 and M7, follow pins in M1 and M2 (“stapled style”), vertical and horizontal stripes in M3 and M4
5) Place, CTS, and route
6) “Tape out”: Performing all necessary checks and verification, exporting layout, and post-route reports for PPA, etc.

Challenge: DRC Violations

- DRC violations are ***expected,*** for example for pin access around the power stripes
- They can become very challenging for dense layouts, which is also part of the challenge put forward in this contest

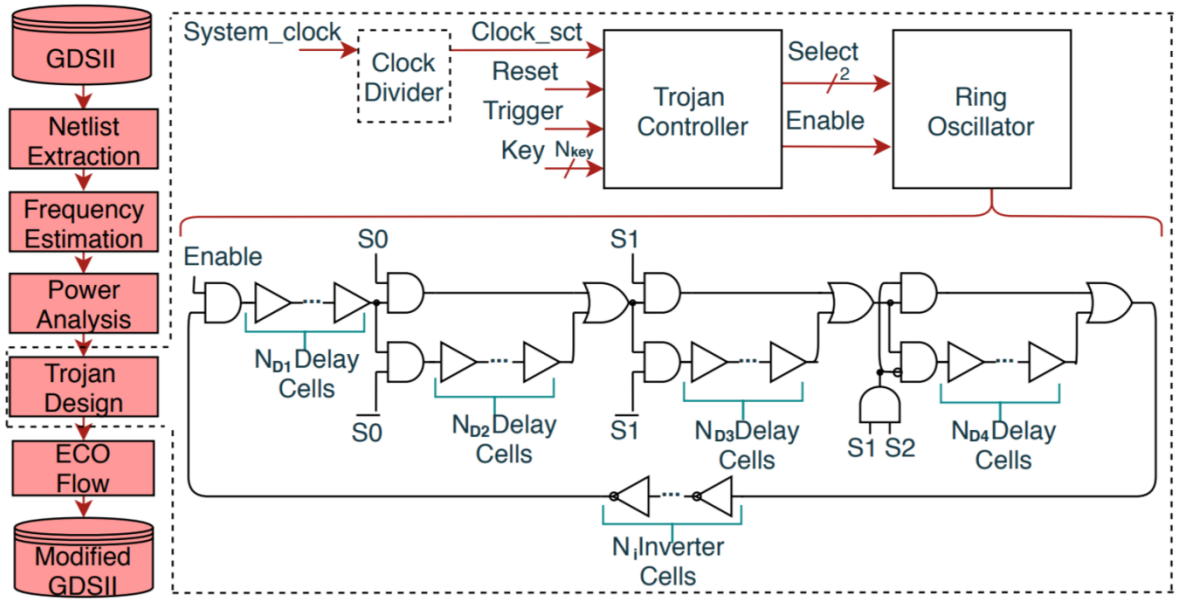




Metrics and Scoring

- PPA

1) Security for alpha/qualifying round: first-order metrics
    - Regions of 20+ continuous open placement sites
    - Free routing tracks
2) Security for final round: extended with actual Trojan insertion, based on ECO



T. Perez, M. Imran, P. Vaz and S. Pagliarini, "Side-Channel Trojan Insertion – a Practical Foundry-Side Attack via ECO," Proc. Int. Symp. Circ. Sys. (ISCAS), 2021, pp. 1-5

Actual Trojan Insertion (Final Round)

There are 6 different Trojans per benchmark

Triggering conditions - activation mechanism

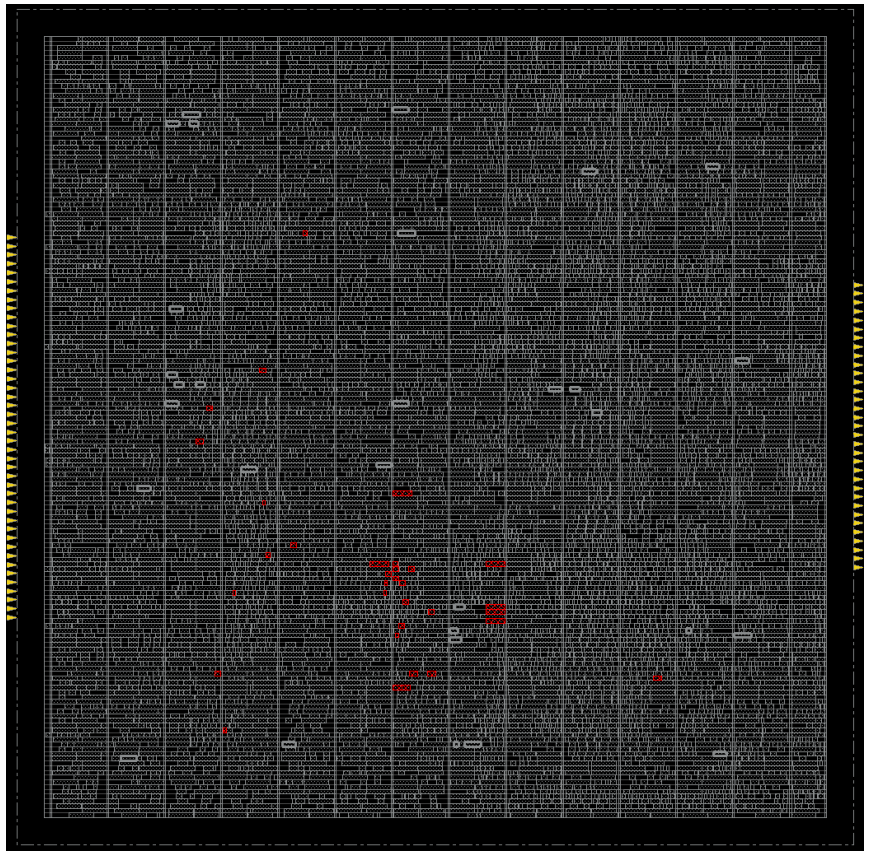
- Targeted: set of asset cells chosen from a common layout region
- Random: set of asset cells chosen randomly

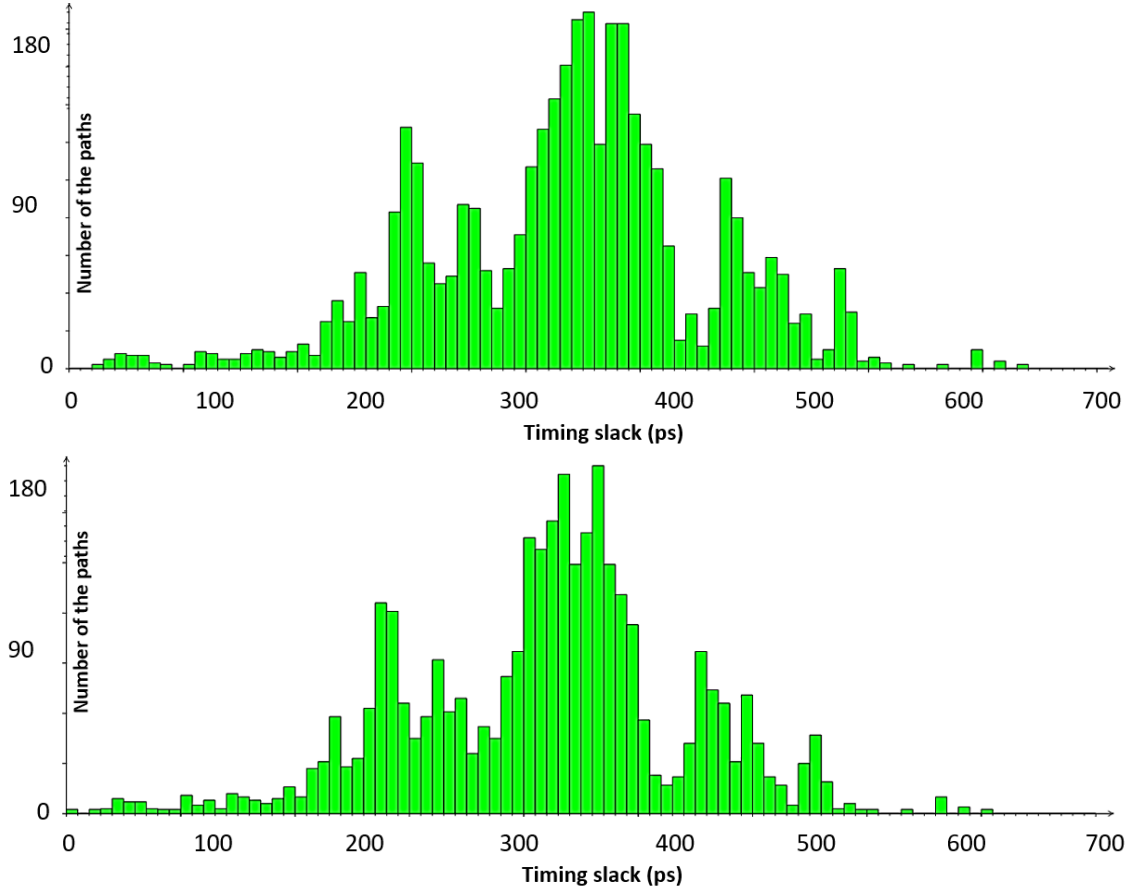
Trojan payload - effect of the Trojan

- Leak: Trojan is connected to the output of some sensitive asset FFs
- Modify: Trojan flips the output of some sensitive asset FFs
- Burn: Trojan adds a redundant FF chain / RO to consume more power

Actual Trojan Insertion (Final Round)

An exemplary Trojan inserted into the SHA256 benchmark





Scoring

$$score = [sec + des]/2 = [(1/2 \times sec\_ti\_gen + 1/2 \times sec\_ti\_ECO) + des]/2$$

(1) Trojan insertion, generic evaluation – sec_ti_gen

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

50% sum, 33.3% max, 16.6% median

(b) 50% weighted: free routing resources of whole layout ($sec\_ti\_f\ ts$)

(2) Trojan insertion, actual ECO insertion – sec_ti_ECO

- Score sheet, with lower scores for better defense / more difficulties for Trojan insertion

  0—2 design failures; 5—7 DRC violations; 10—12 setup AND hold violations;
  15—17 setup XOR hold violations; 20—22 DRV OR clock check violations;
  25—27 no violations
- Normalized over 27; averaged across different ECO modes; gap b/w categories intended

Scoring

(3) Design quality – des

(a) 33.3% weighted: power (des_pwr)

- $score$ (des_pwr_tot) = des_pwr_tot (s)/des_pwr_tot (b)

(b) 33.3% weighted: performance ($des\_pr\ f$)

- 50% weighted: ($des\_pr\ f\_W\ N\ S\_set$)
- 50% weighted: ($des\_pr\ f\_W\ N\ S\_hld$)

(c) 33.3% weighted: area (des_ara)

- $score$ (des_ara_die) = des_ara_die (s)/des_ara_die (b)

Constraints

- Submissions cannot incorporate trivial defenses --- filler, decap, and tap cells are purged
- Submissions must meet setup, hold timing checks using the provided SDC files for timing analysis
- Submissions must have 0 DRC violations
- Submissions must maintain the general IO pin placement
- Participants must maintain the overall functional equivalence of the underlying design

Constraints

- Participants must maintain the assets
- Participants cannot design custom cells
- Participants cannot revise the metal layers/metal stack
- Participants must include a clock tree in their submission
- Participants must follow the PDN recipe provided in the reference flow

Benchmarking Advanced Security Closure of Physical Layouts ISPD 2023 Contest

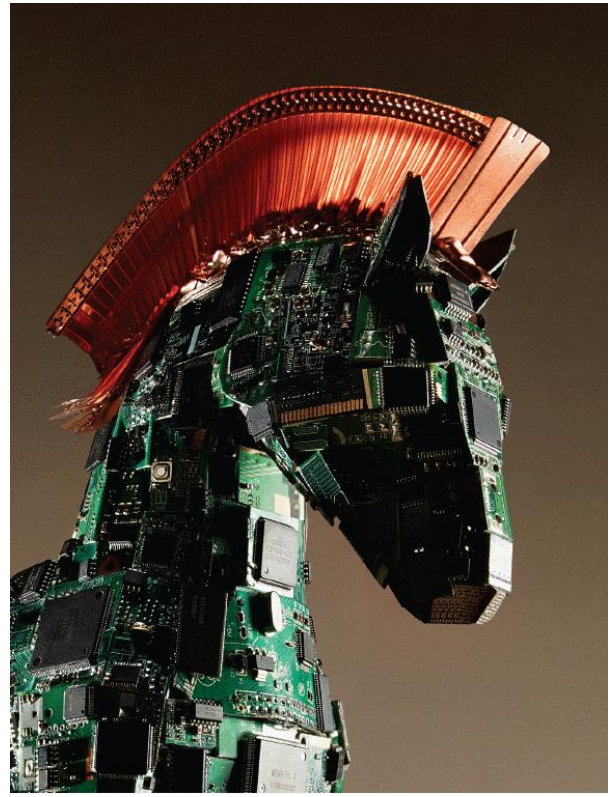
Mohammad Eslami[1], Johann Knechtel[2], Ozgur Sinanoglu[2], Ramesh Karri[3], Samuel Pagliarini[1]

Tallinn University of Technology (TalTech)[1], NYU Abu Dhabi[2], NYU New York[3]

Overview

- Motivation:
  - More and more threats are arising that affect hardware
  - Build up knowledge and experience in CAD community

- Main theme:
  - Incorporating techniques for designing secure and trustworthy ICs in future CAD flows
  - Hardening layouts at design time against threats that are executed post-Design Scores: this year, Hardware trojan horses



Part 1: background, some details on contest; **Part 2: teams, rankings, awards**

Teams

- 14 from Americas, Europe, and Asia had registered
- 4 finalist teams
- (Last year: 17 registrations, 8 finalists)

Finalist Teams

- **XDSecurity-II, XiDian University**
  Shunyang Bi, Guangxin Guo, Haonan Wu, Zhengguang Tang, Hailong You, Cong Li

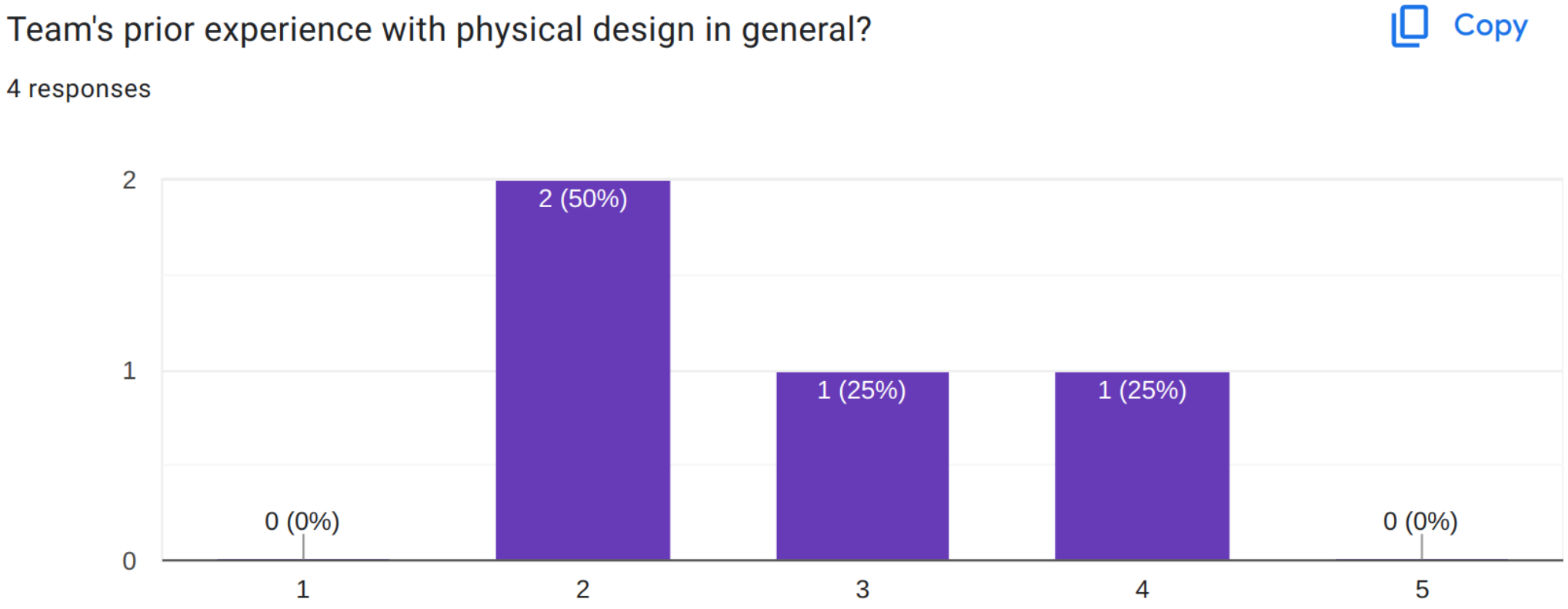
- **CUEDA, The Chinese University of Hong Kong**
  Bangqi Fu, Qijing Wang, Yang Sun, Qin Luo, Anthony W. H. Lau, Fangzhou Wang, Evangeline F. Y. Young

- **FDUEDA, Fudan University**
  Peng Zou, Min Wei, Xingyu Tong, Binggang Qiu, Zhijie Cai, Guohao Chen, Benchao Zhu, Jiawei Li, Jun Yu, Jianli Chen

- **NTHU-TCLAB, National Tsing Hua University**
  Chun-Wei Chiu, Min-Feng Hsieh, Chia-Hsiu Ou, Ting-Chi Wang

Finalist Team Videos

Survey



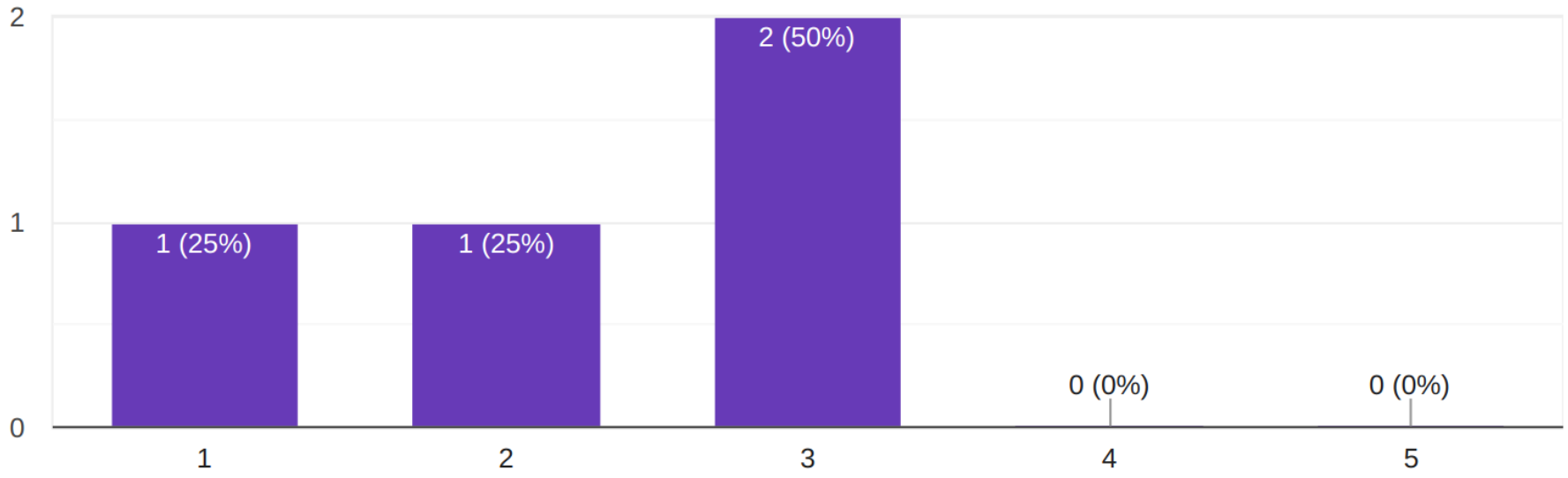
1/left: none; 5/right: excellent

Survey

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

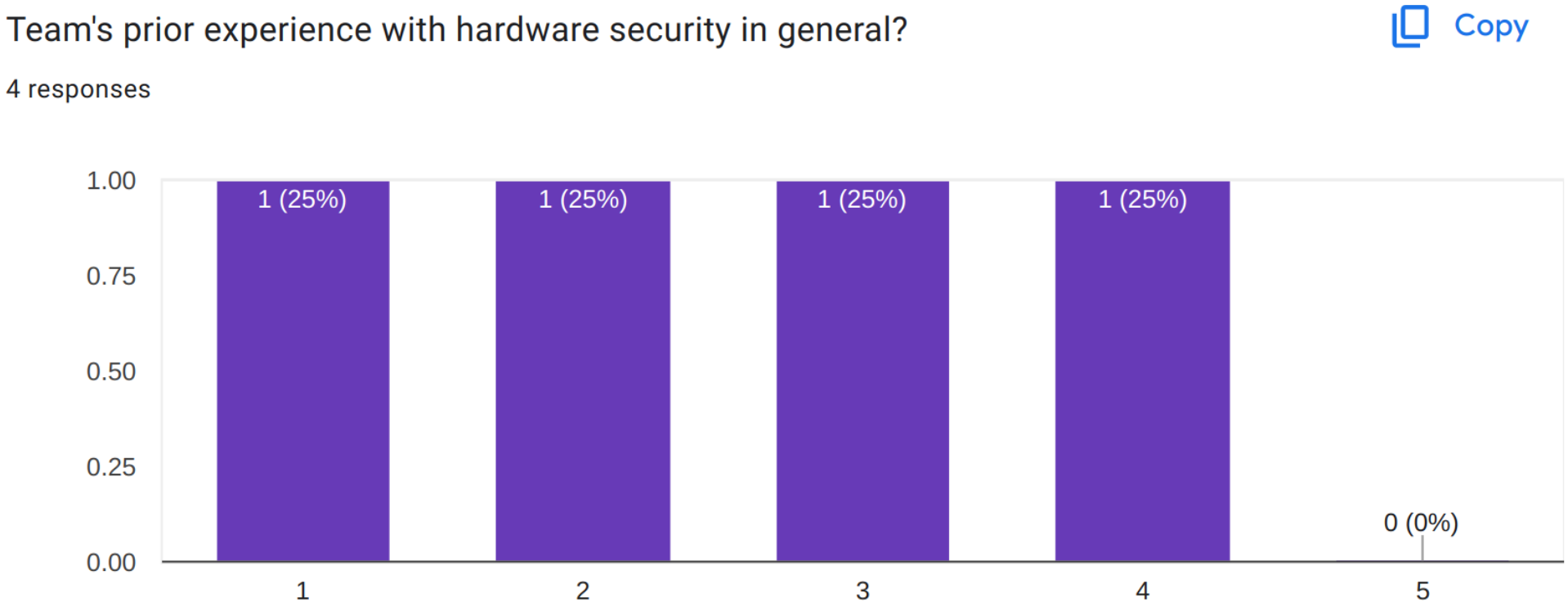
Copy

4 responses



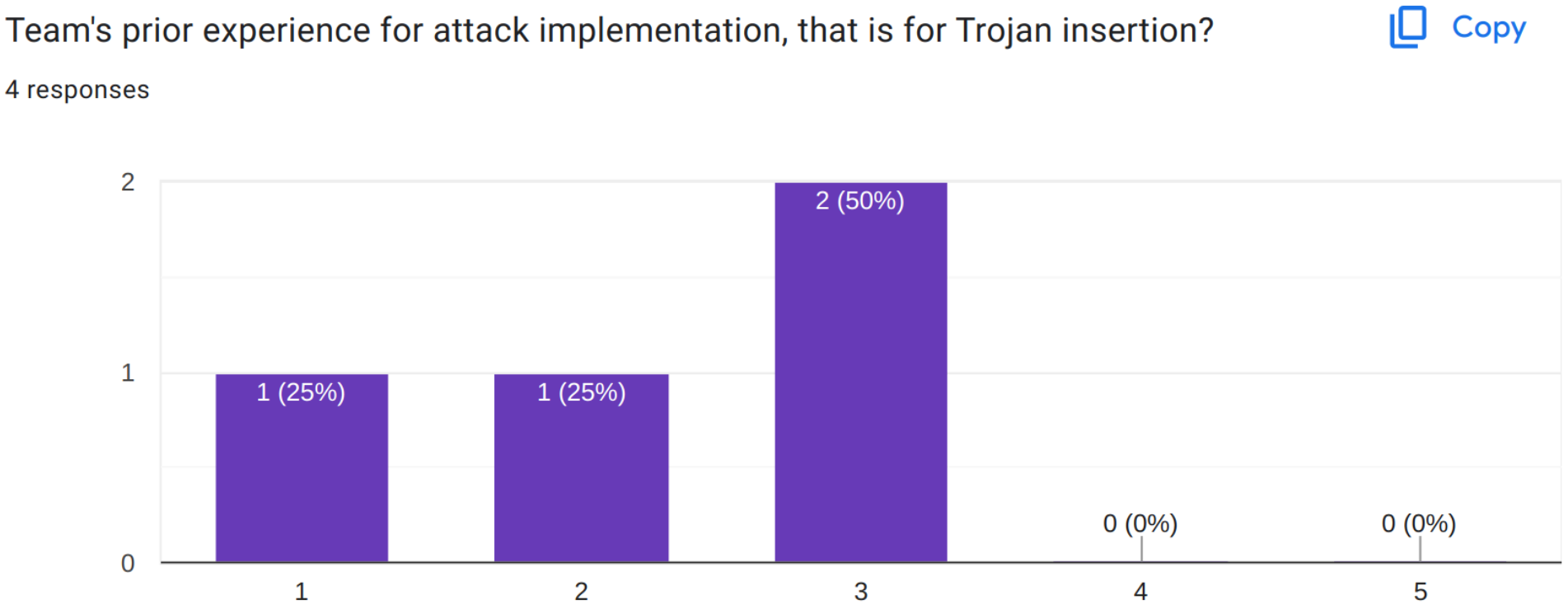
1/left: none; 5/right: excellent

Survey



1/left: none; 5/right: excellent

Survey



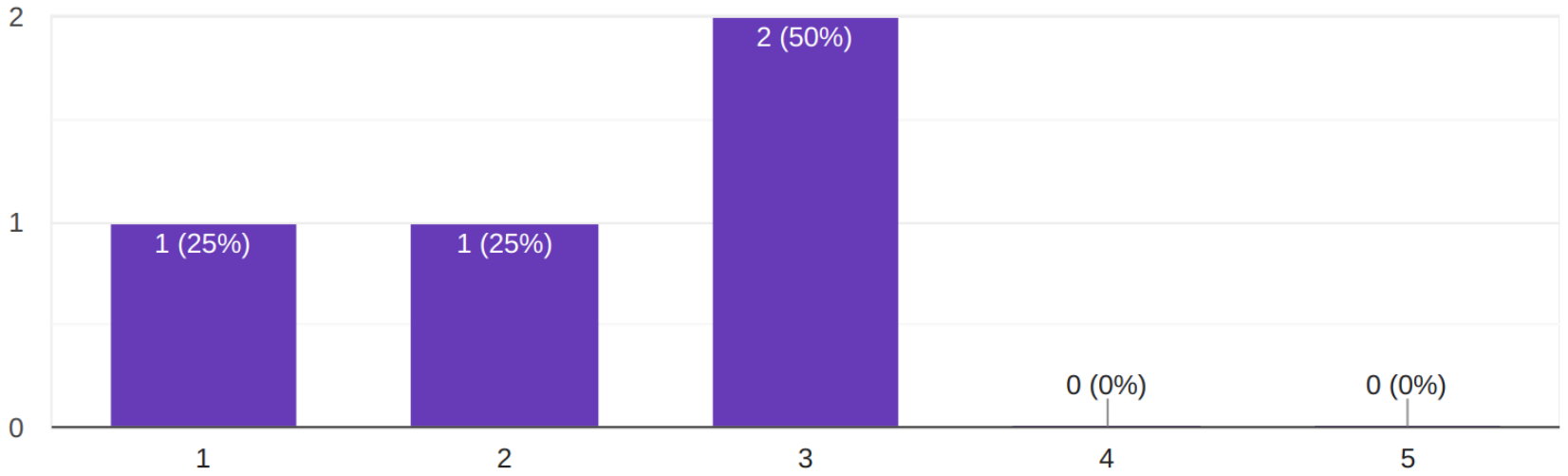
1/left: none; 5/right: excellent

Survey

Team's prior experience for defense implementation, that is for Trojan detection or Trojan mitigation?

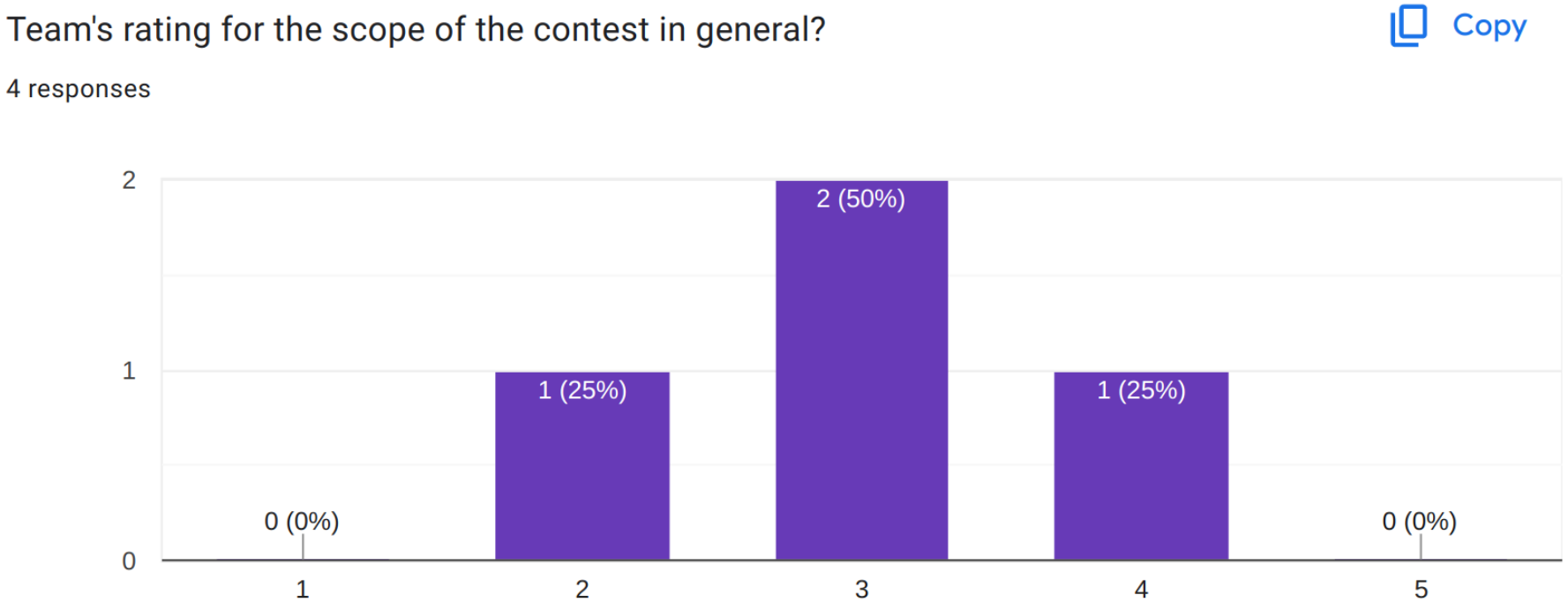
Copy

4 responses



1/left: none; 5/right: excellent

Survey



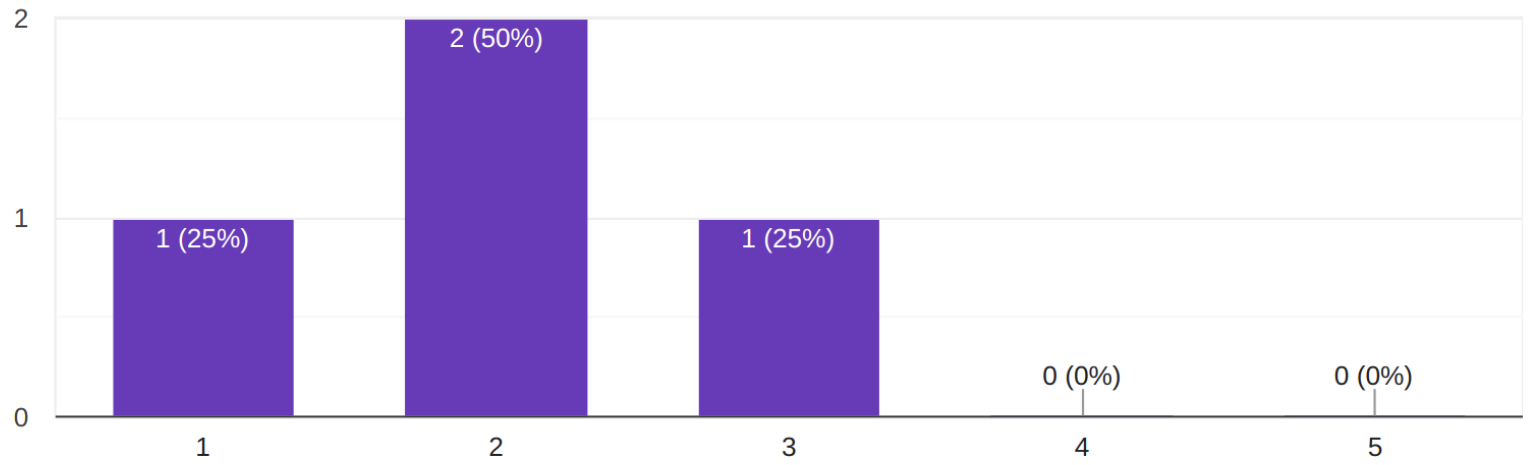
1/left: too difficult; 5/right: too easy

Survey

Team's rating for what was the bigger challenging part of the contest, physical design in general or security closure in particular?

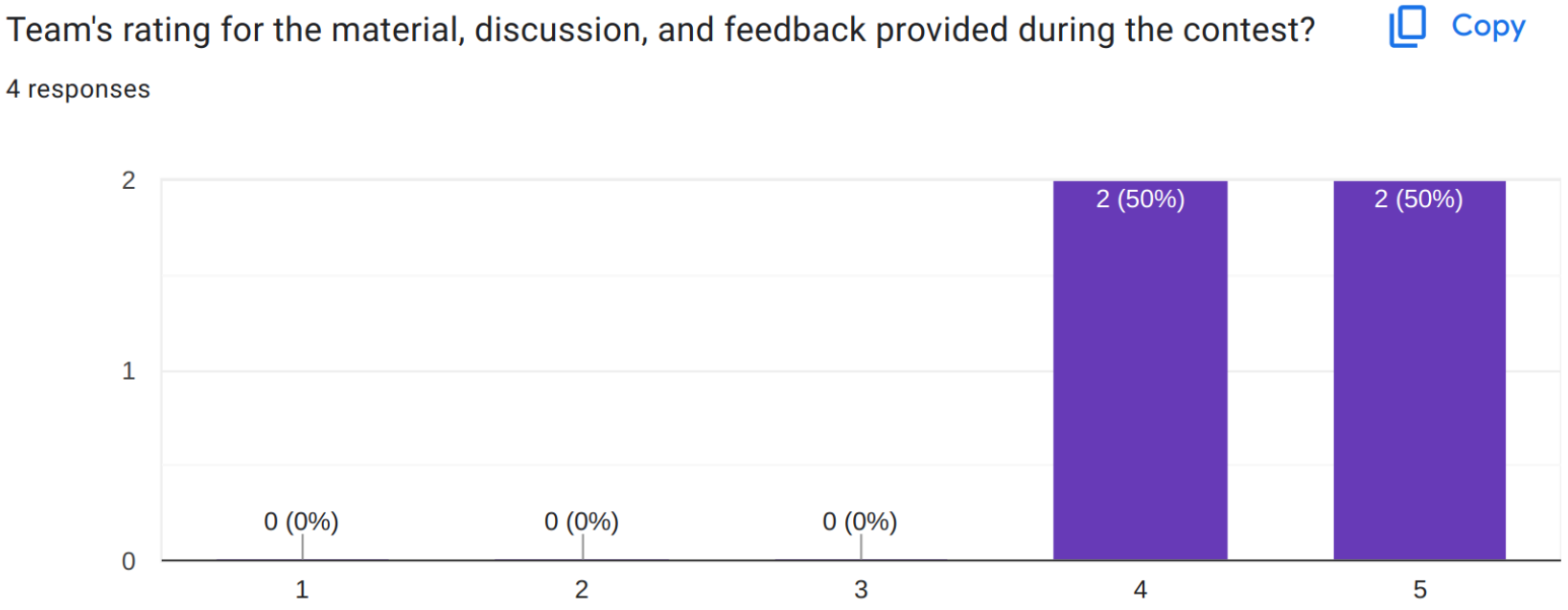
Copy

4 responses



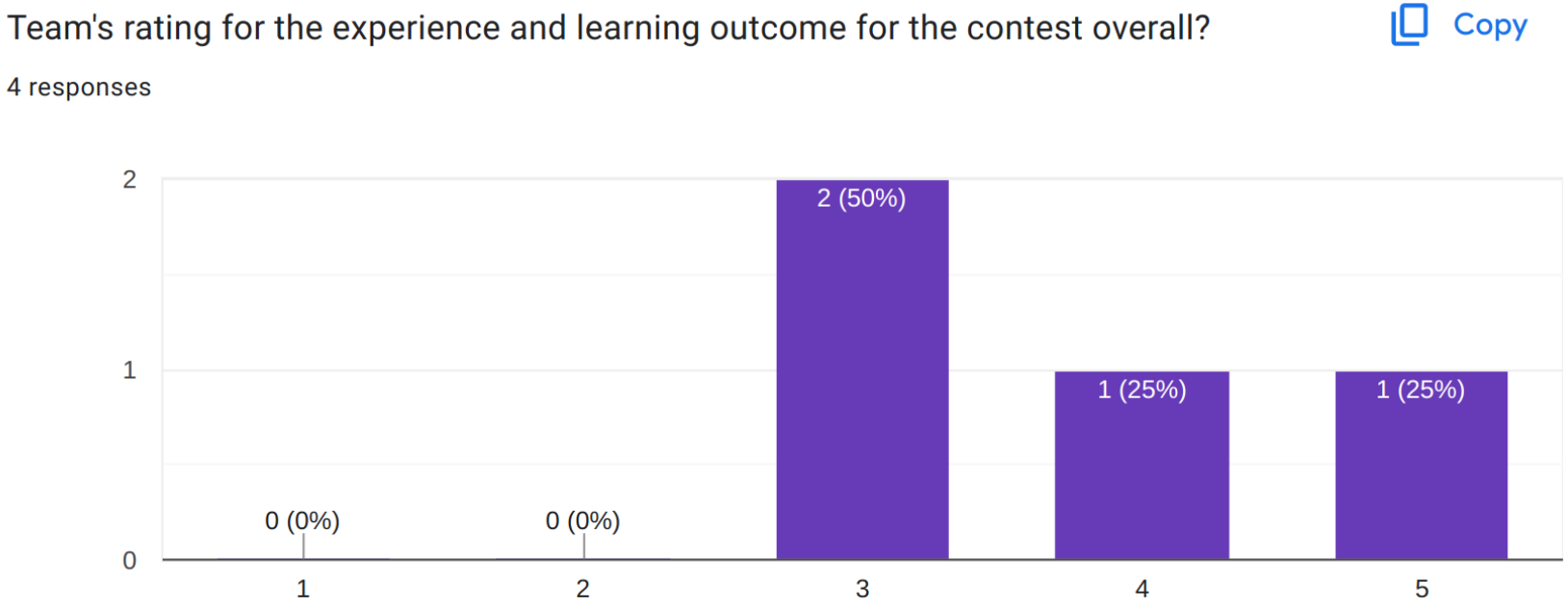
1/left: PD was bigger challenge; 5/right: security closure was bigger challenge

Survey



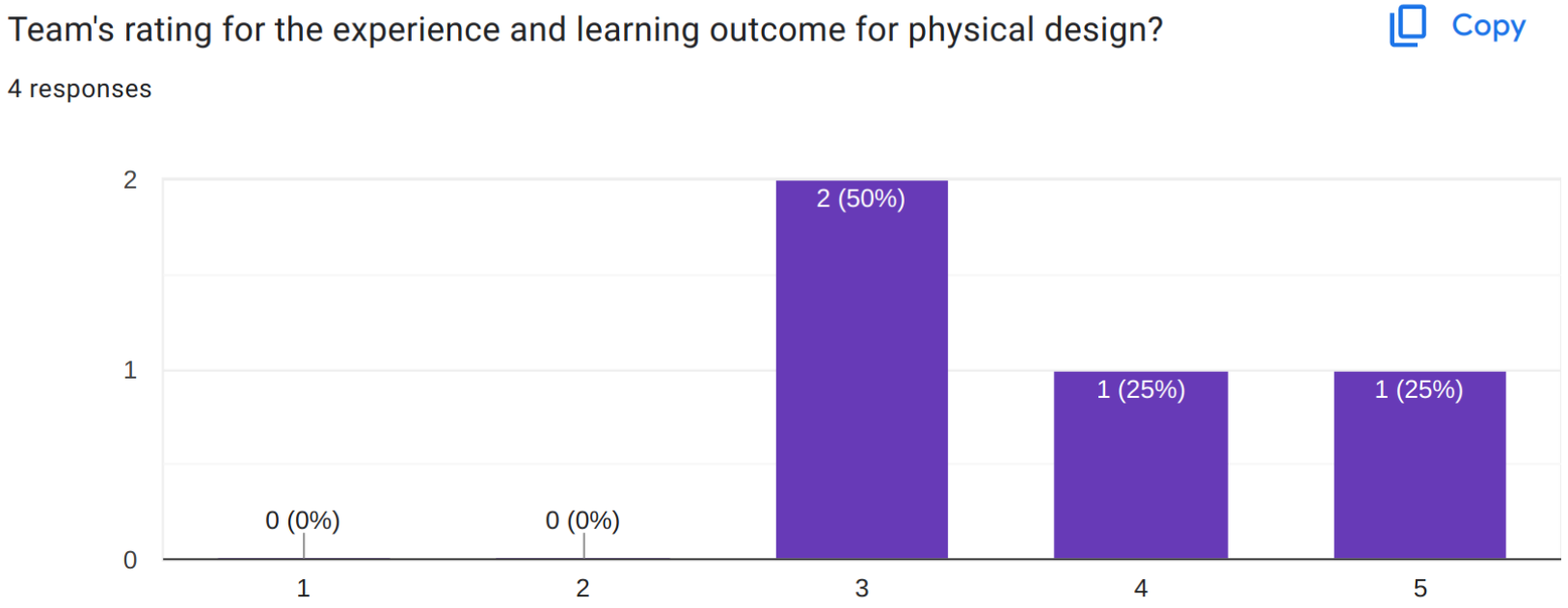
1/left: not enough; 5/right: excellent

Survey



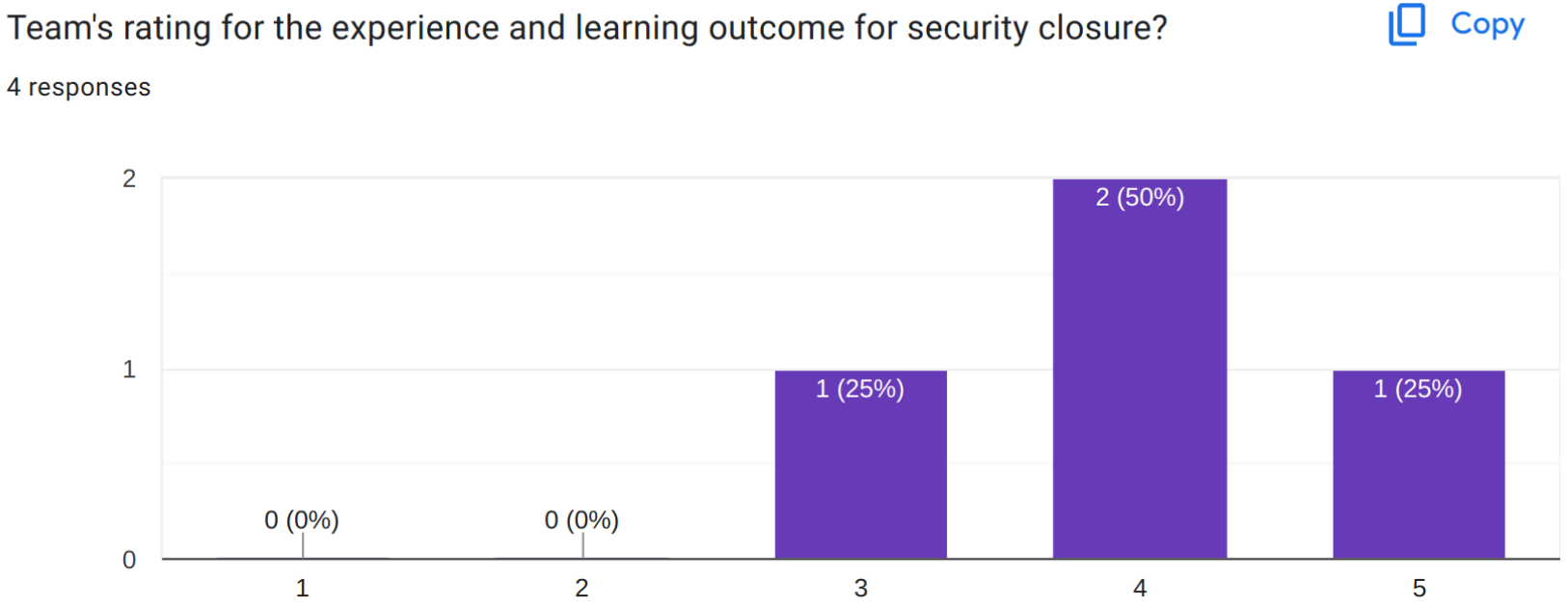
1/left: not enough; 5/right: excellent

Survey



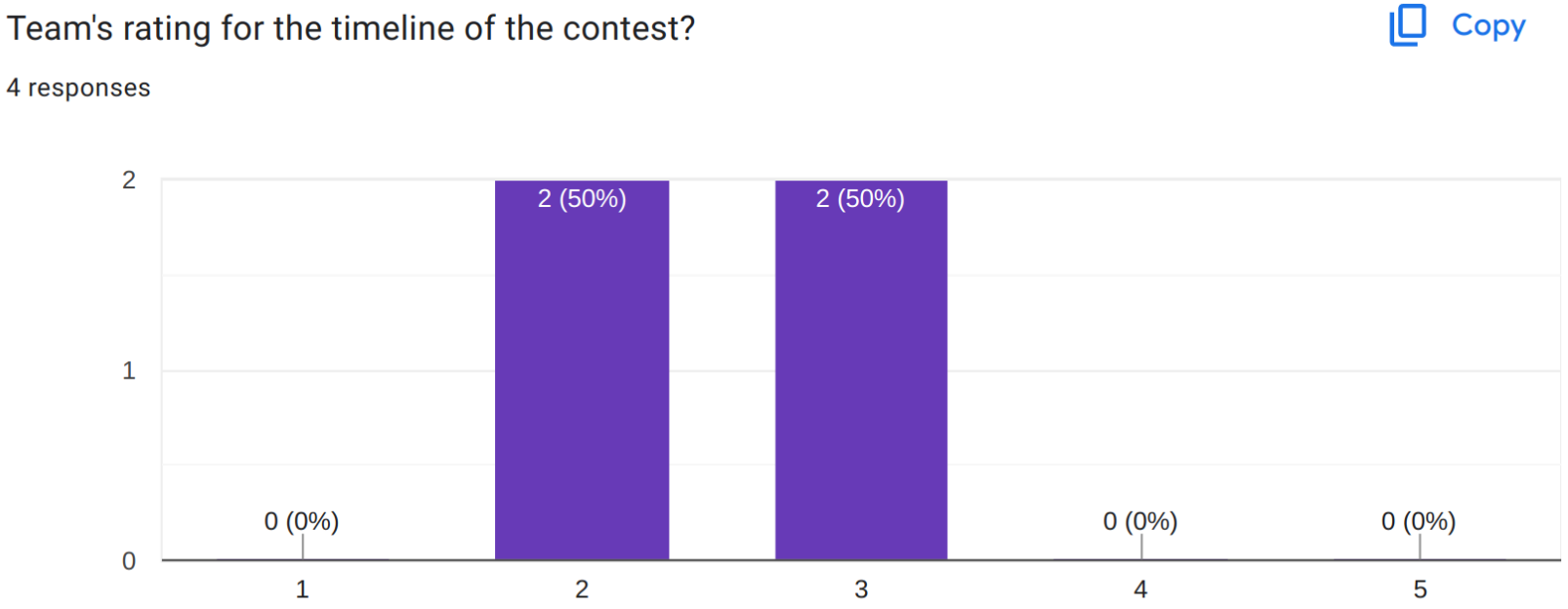
1/left: not enough; 5/right: excellent

Survey



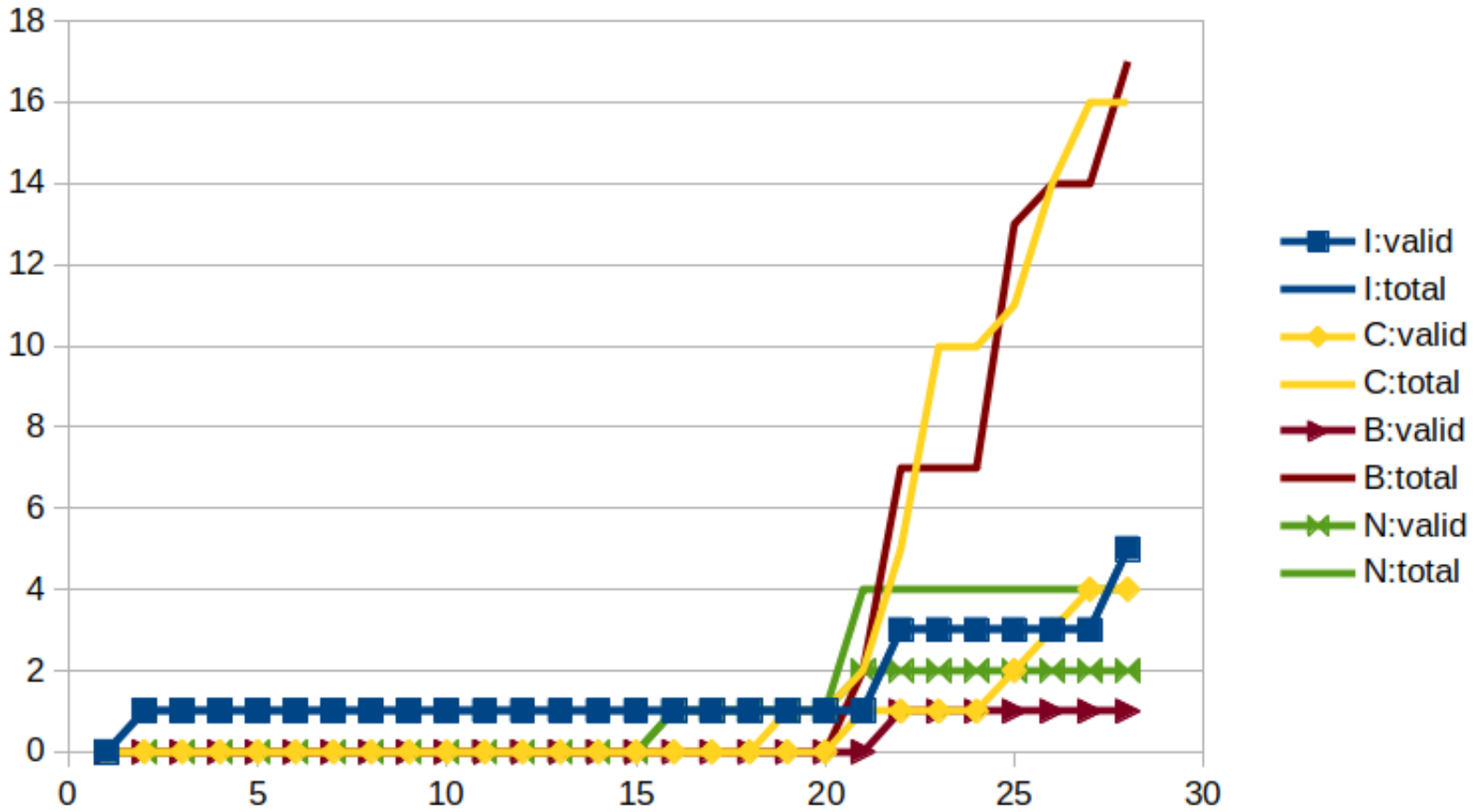
1/left: not enough; 5/right: excellent

Survey

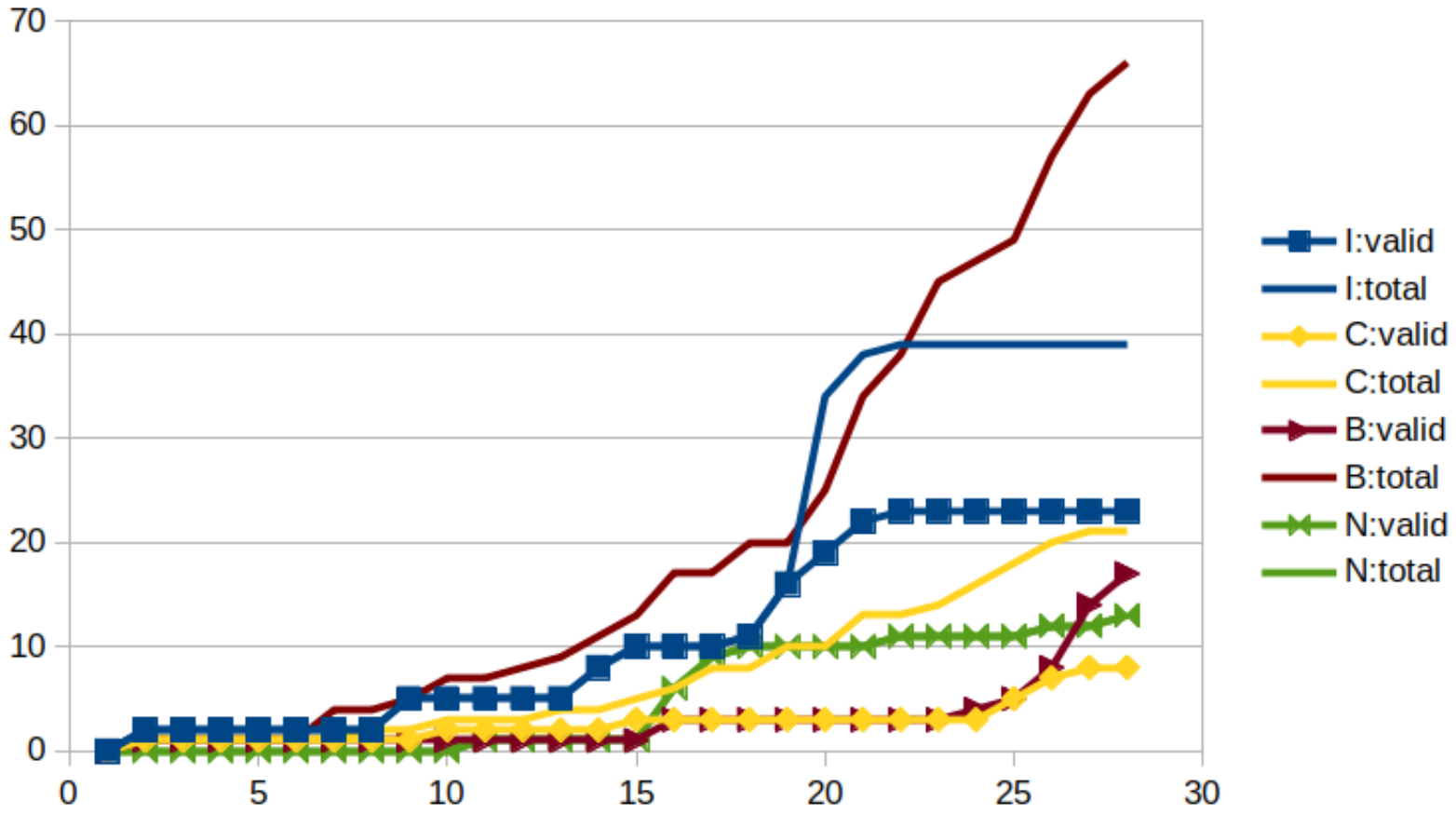


1/left: not enough time; 5/right: too much time

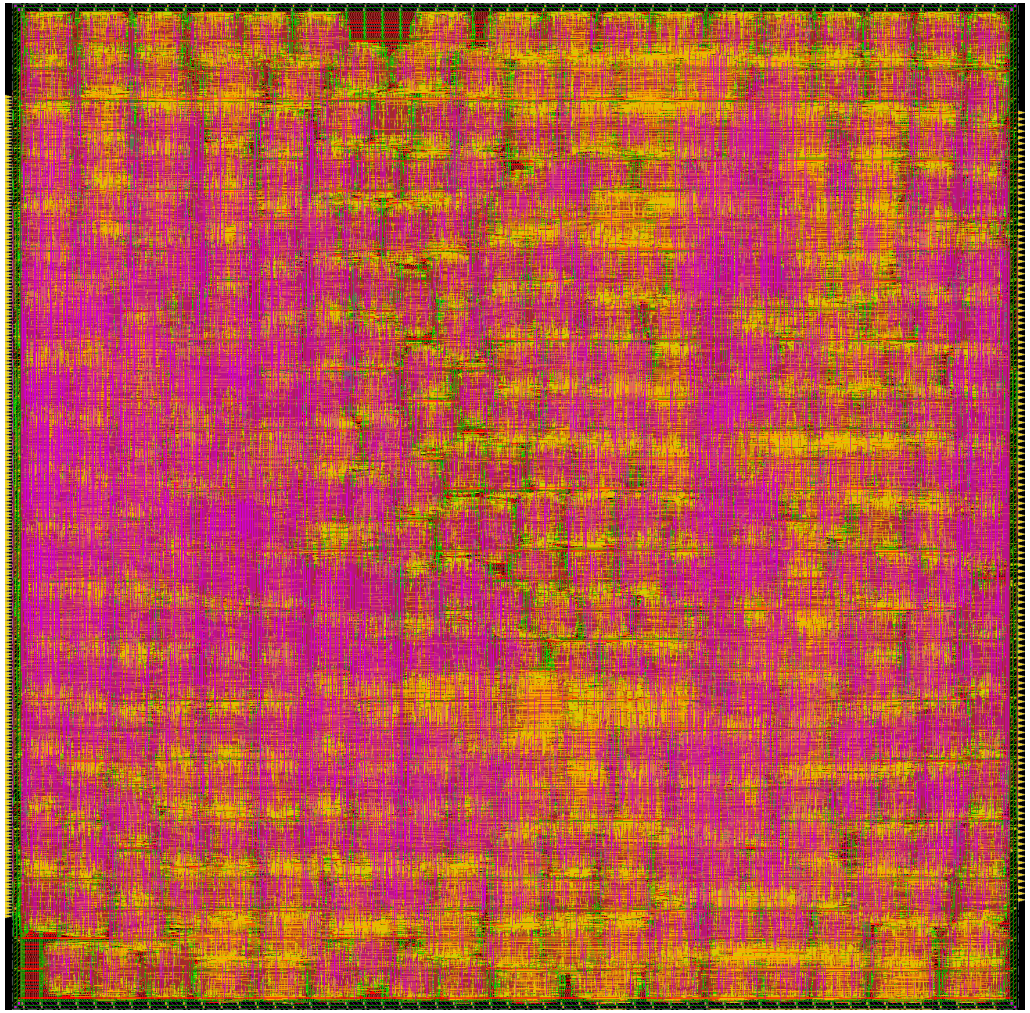
Submissions – aes



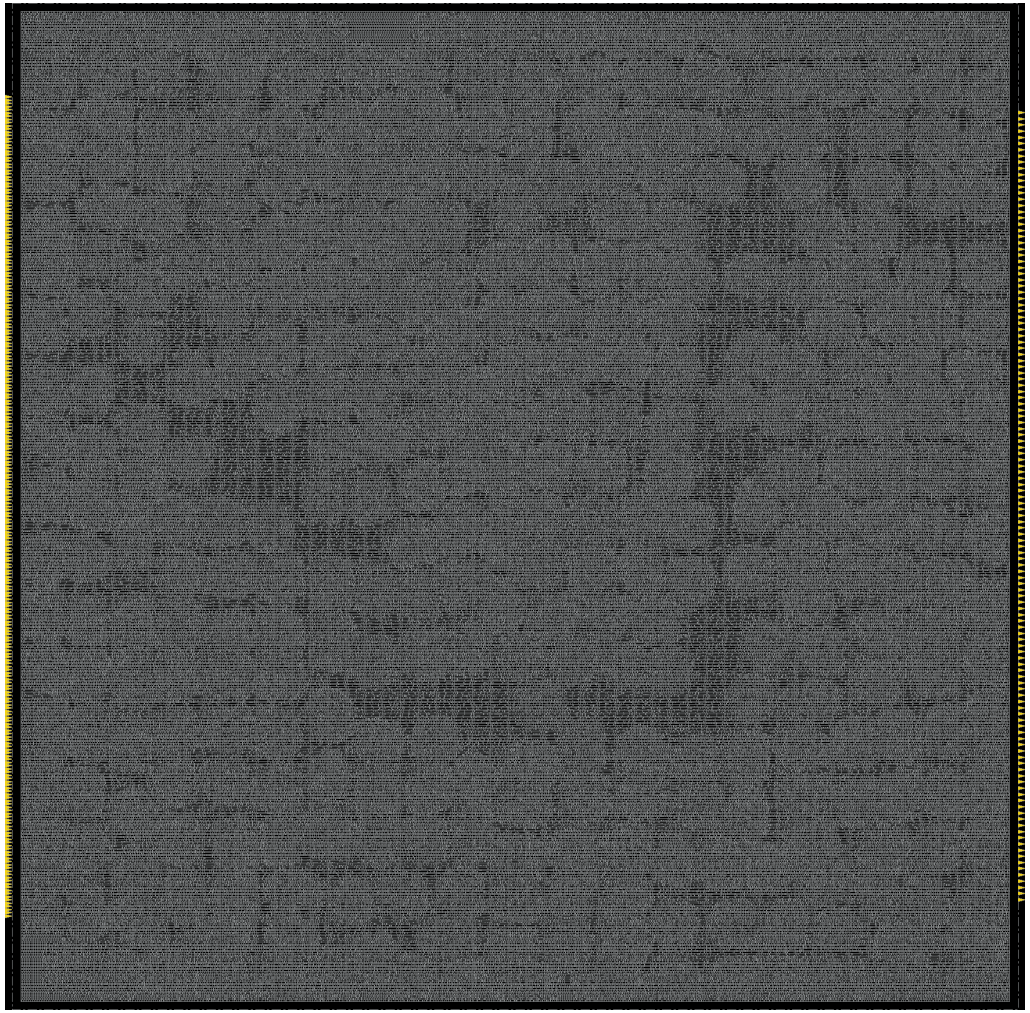
Submissions – sha256



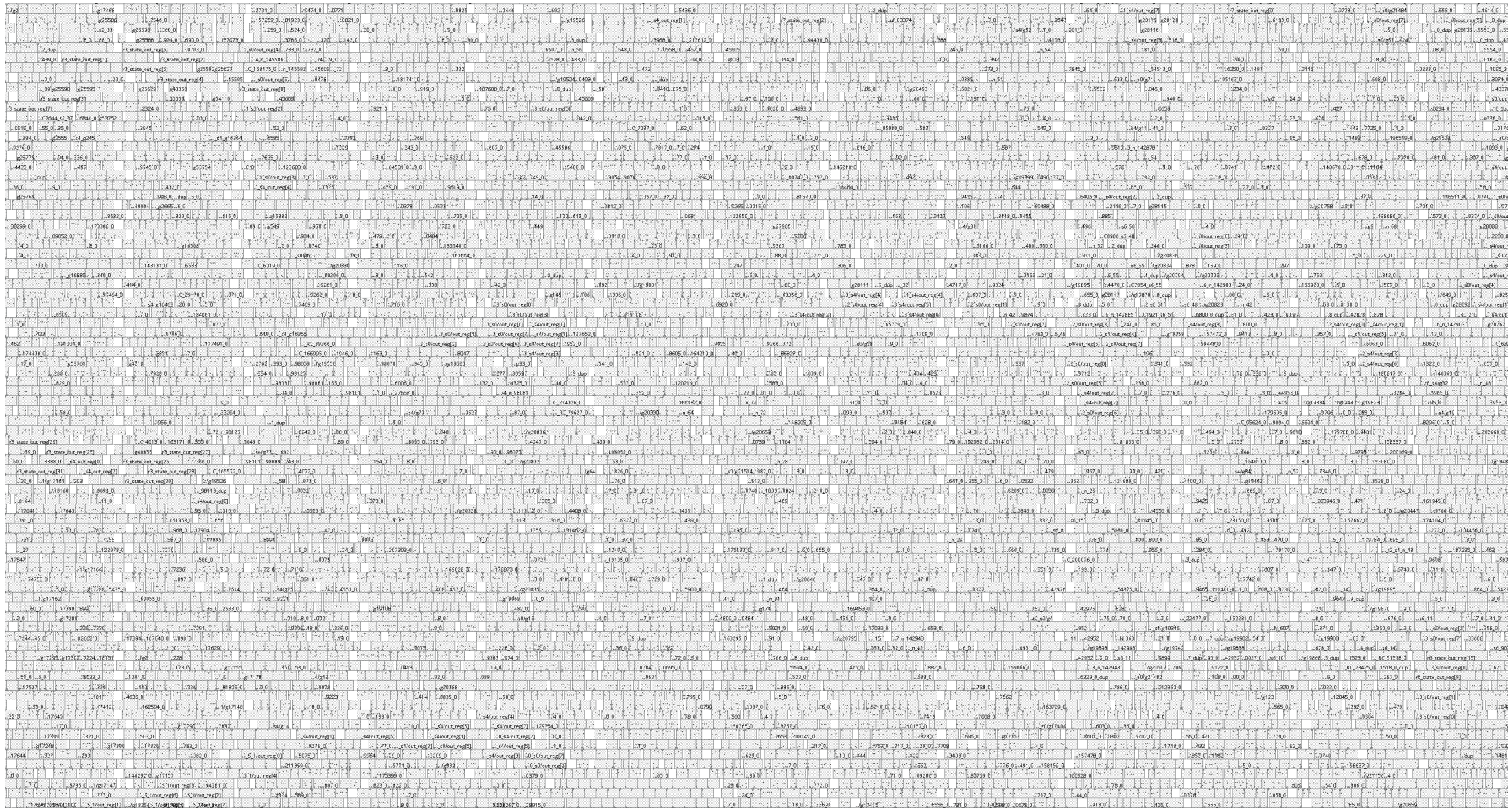
Example Submission Layout – aes



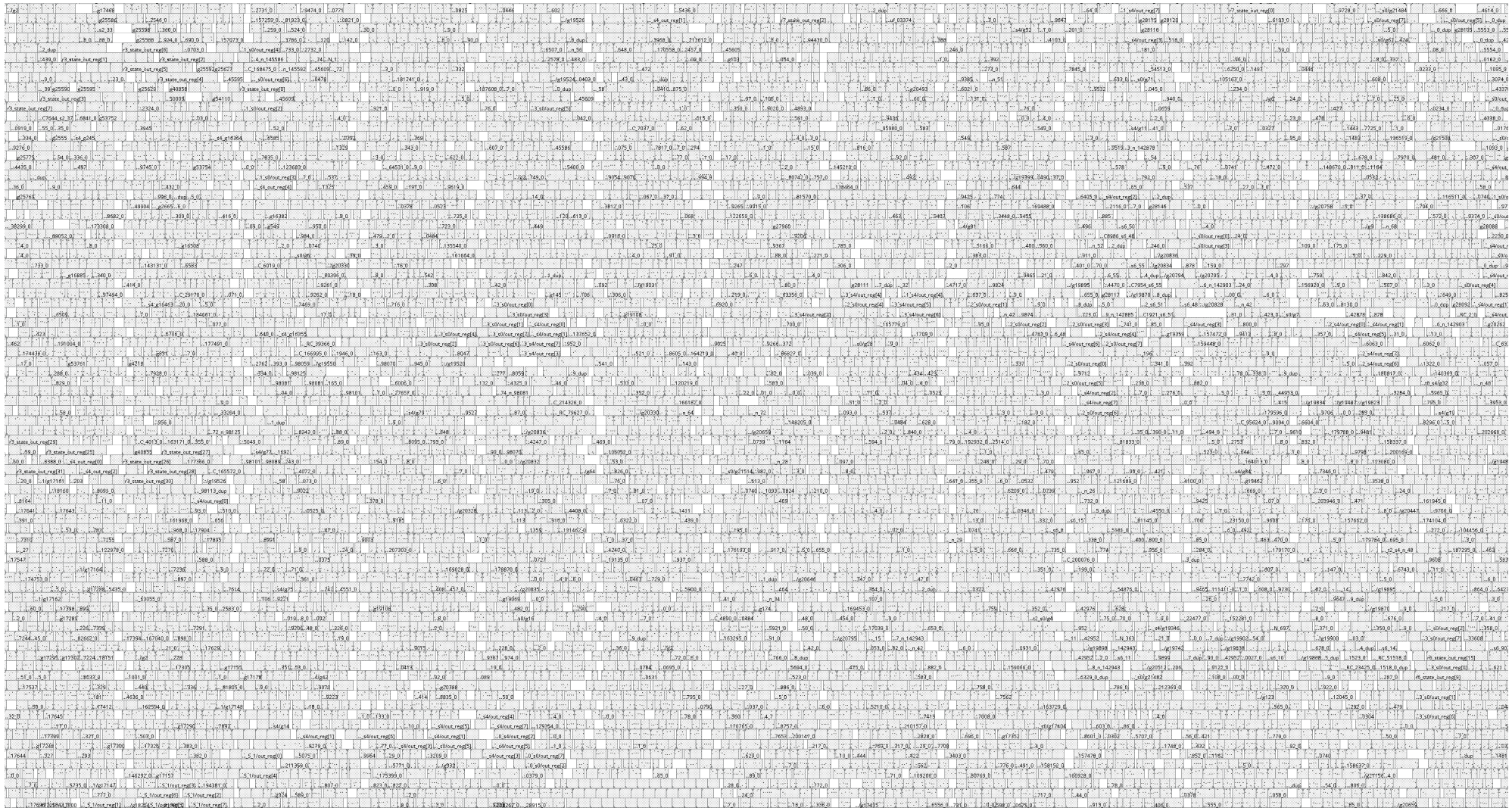
Example Submission Layout – aes



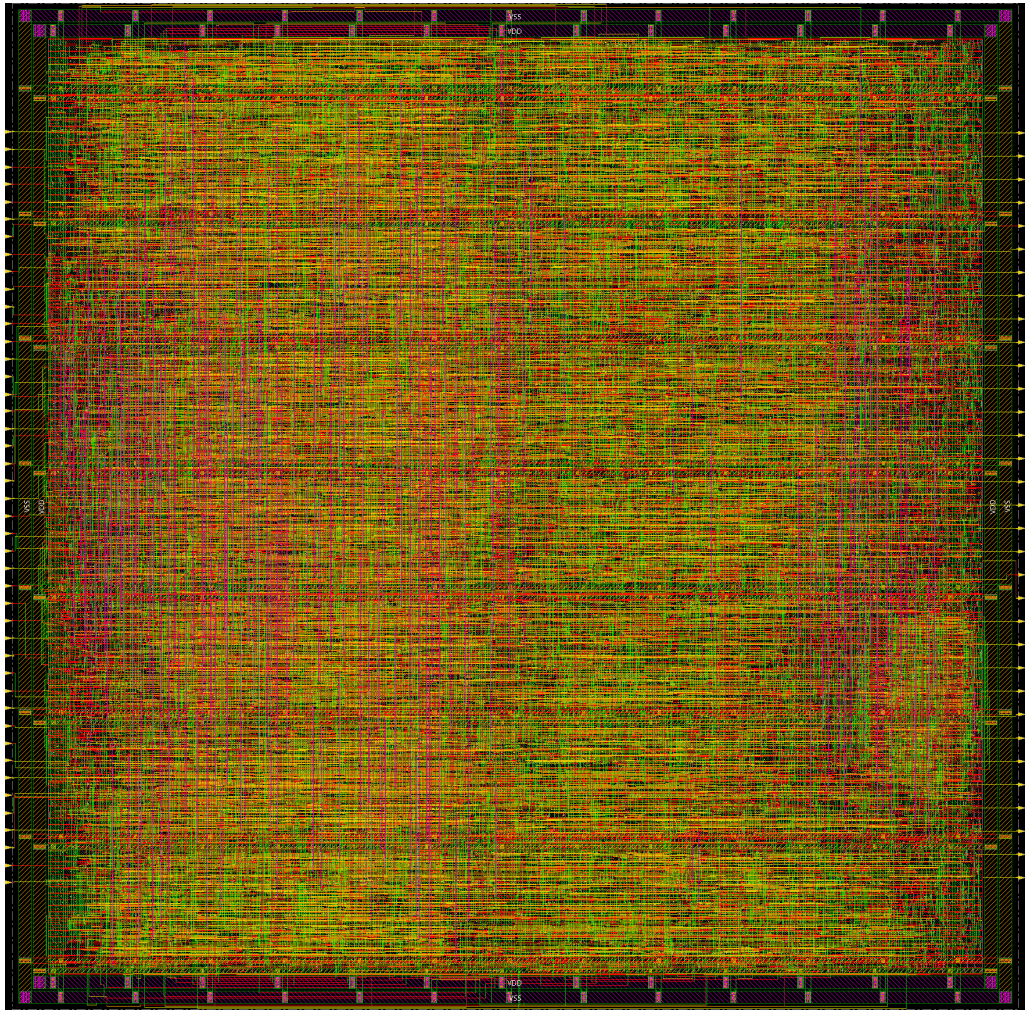
Example Submission Layout – aes



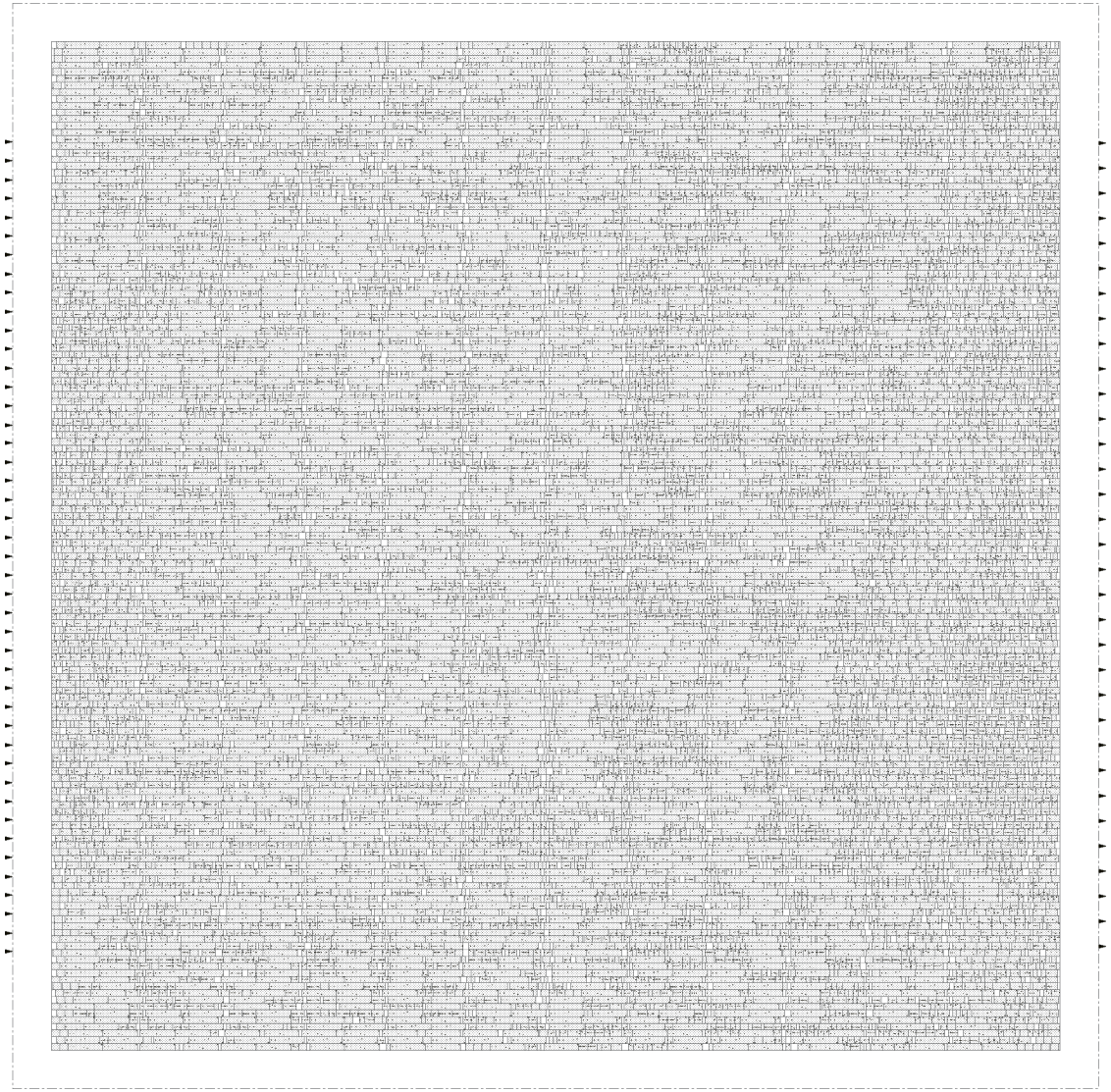
Example Submission Layout – aes – Prepared for ECO Trojan Insertion



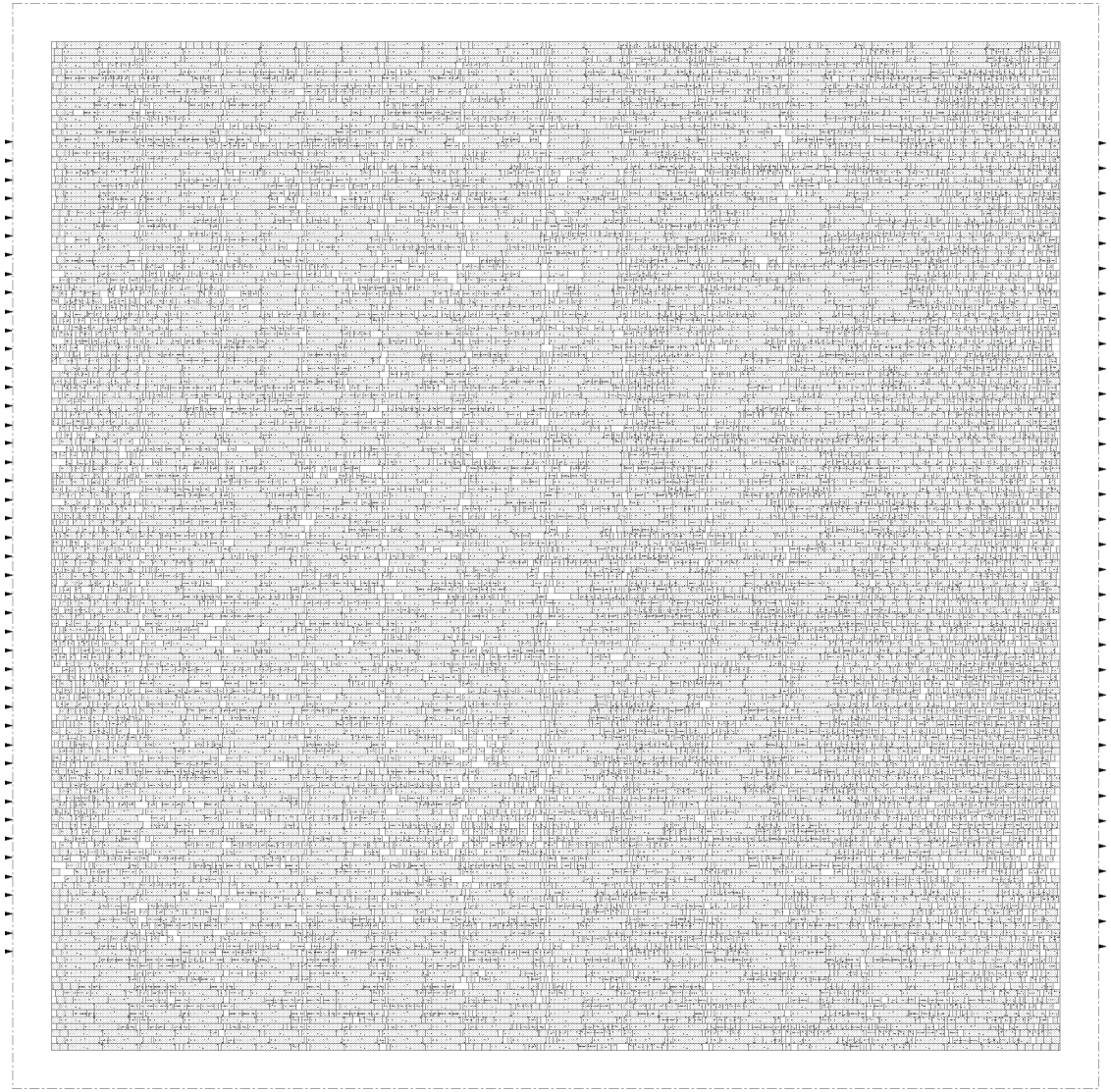
Example Submission Layout – sha256



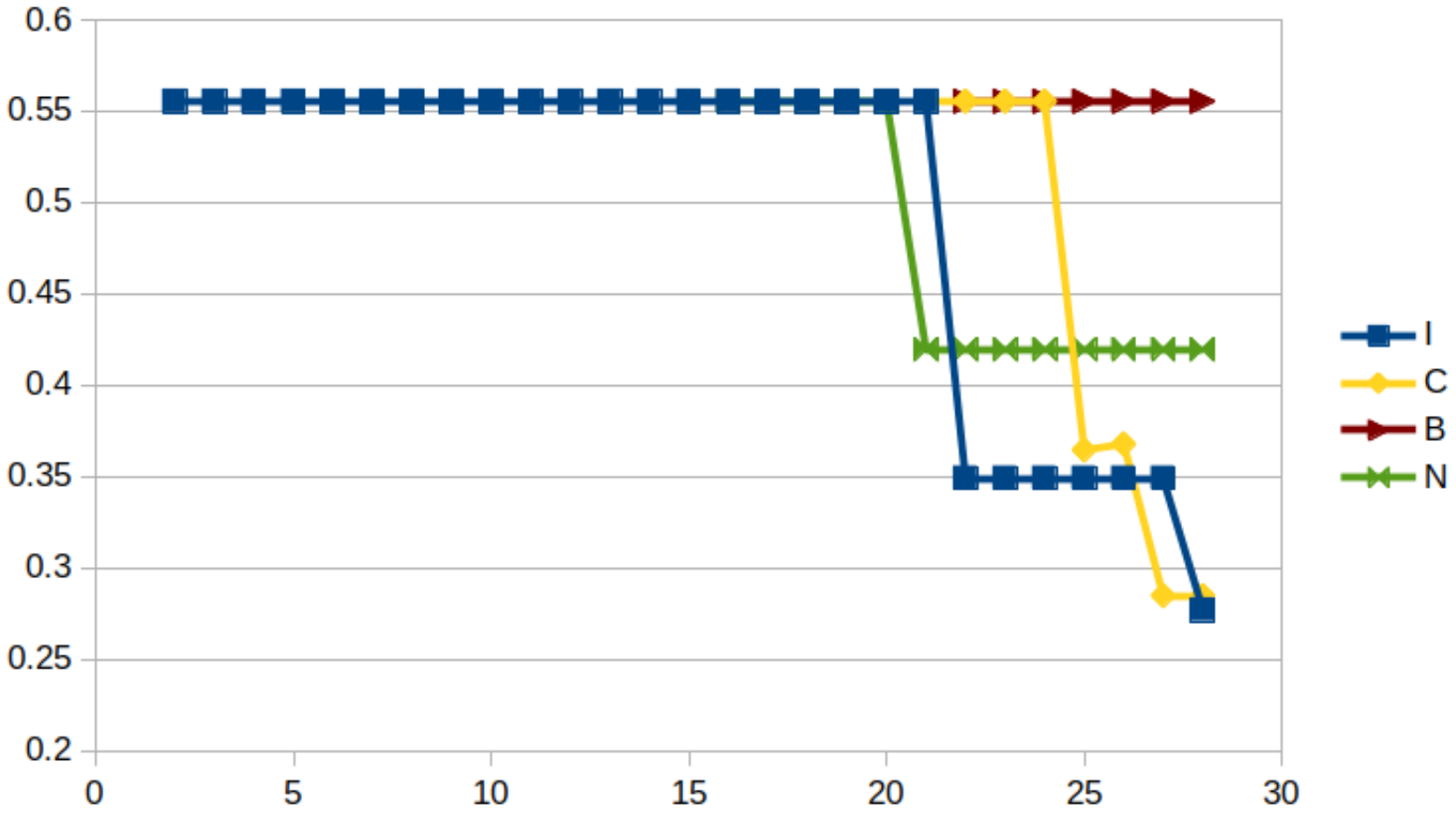
Example Submission Layout – sha256



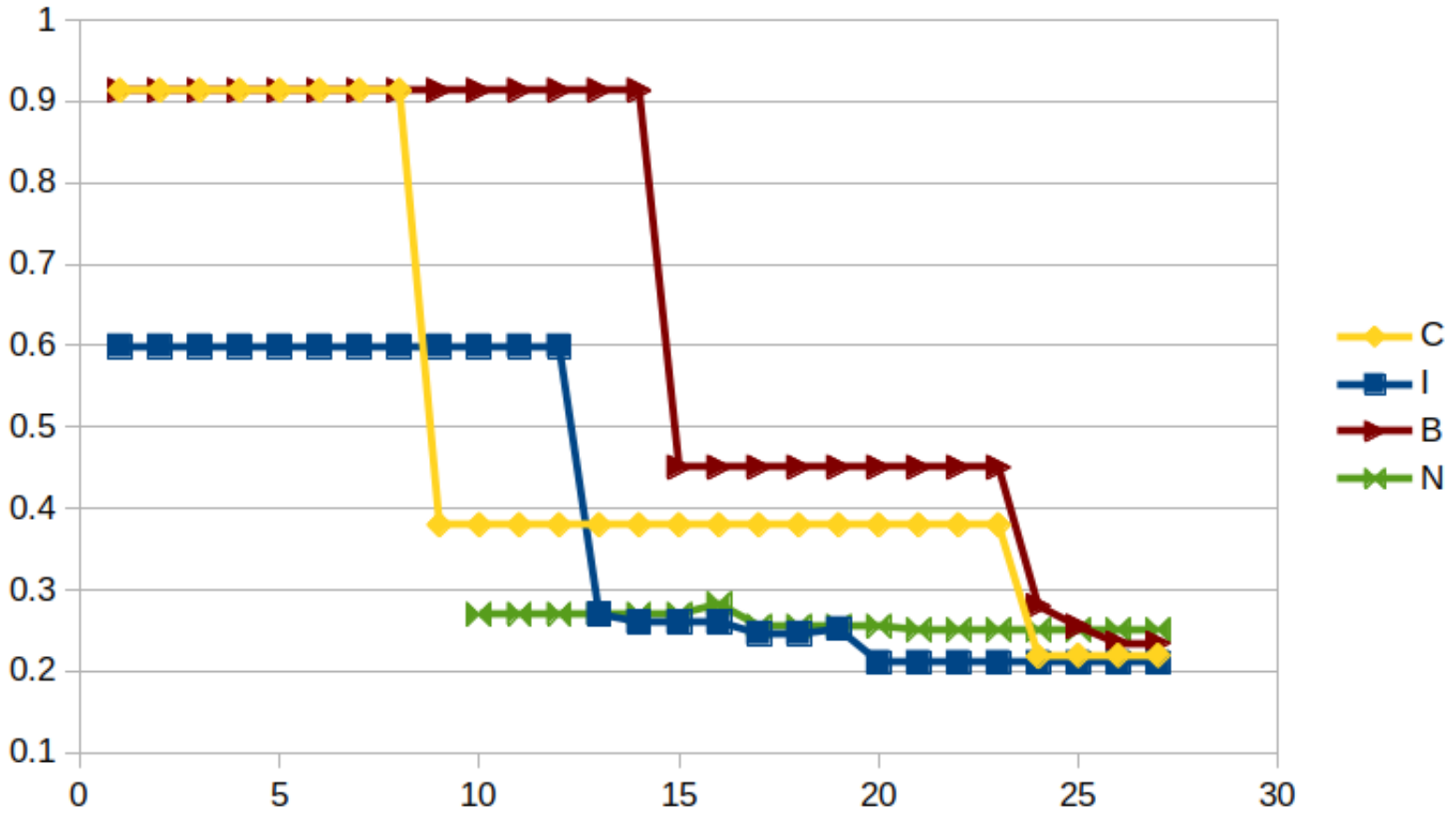
Example Submission Layout – sha256 – Prepared for ECO Trojan Insertion



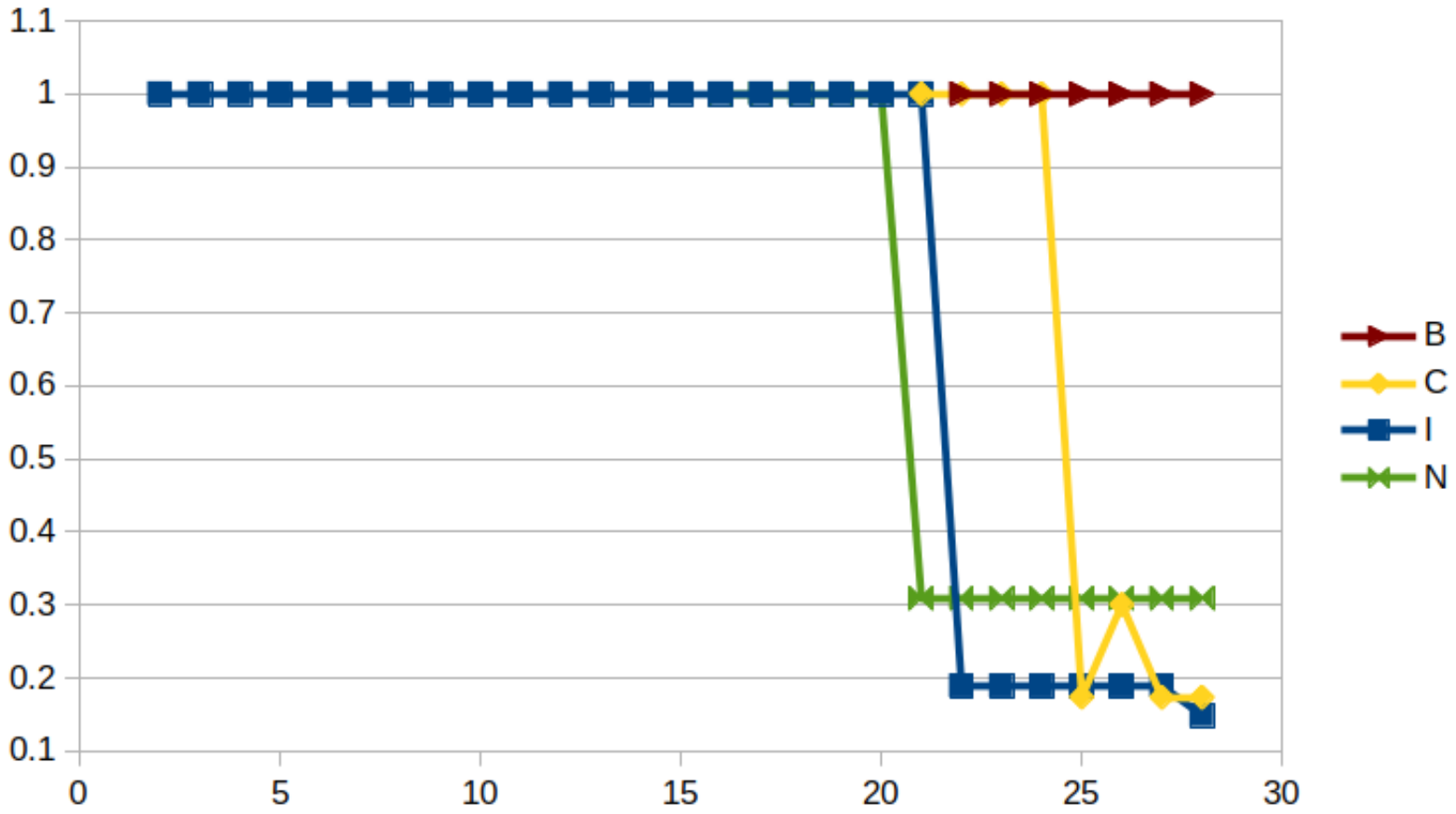
Security Scores – aes



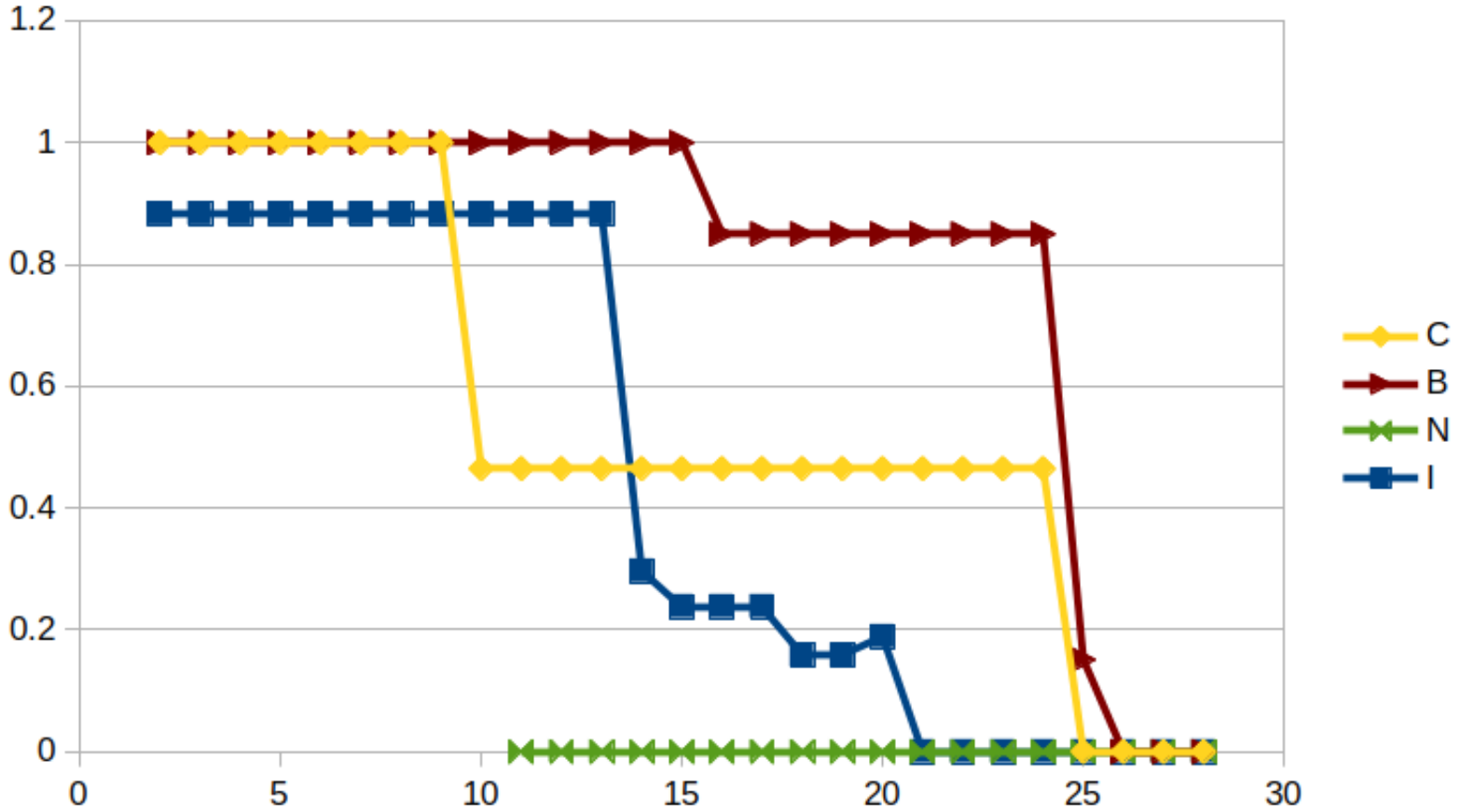
Security Scores – sha256



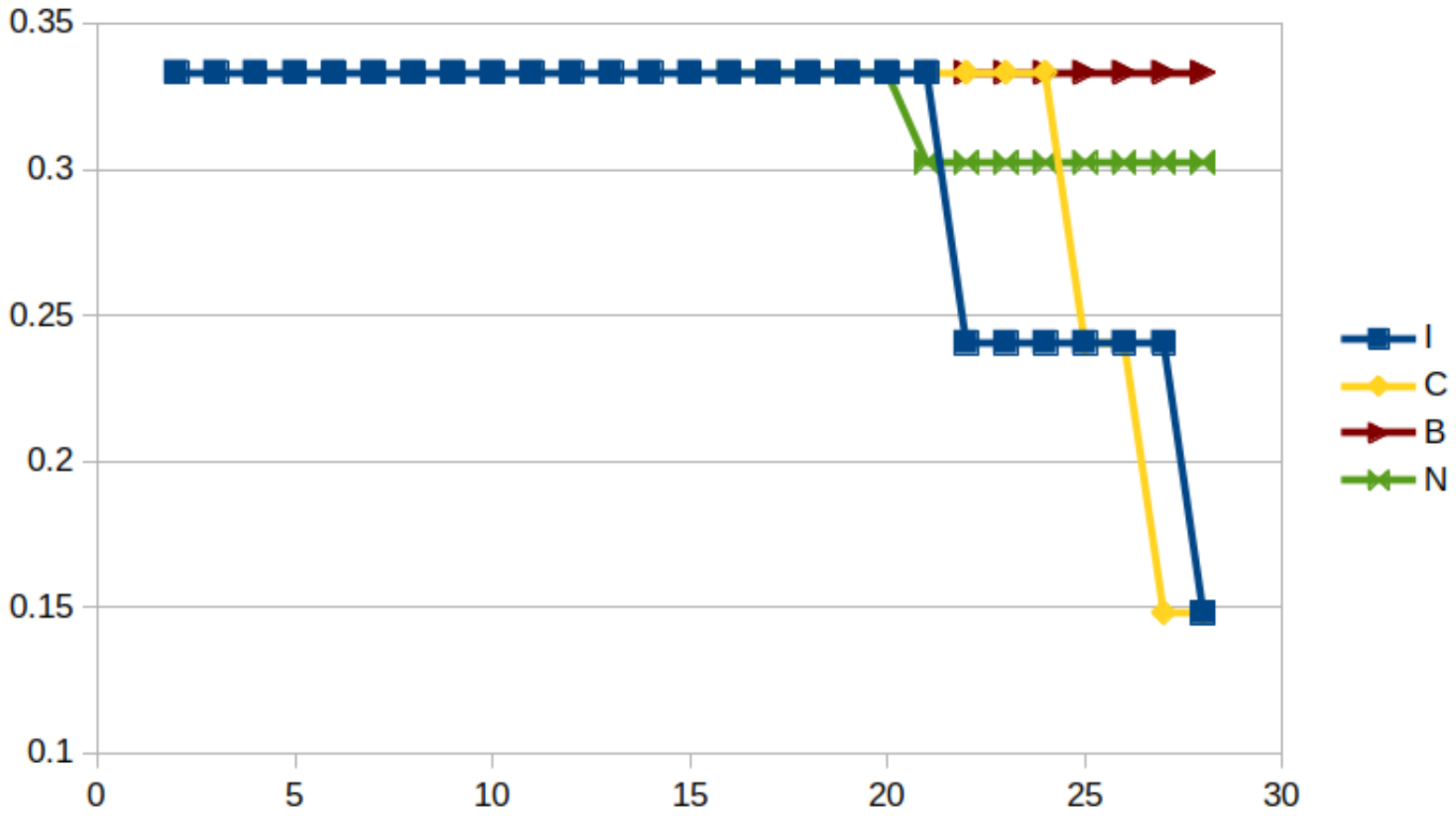
Security Scores: Exploitable Regions – aes



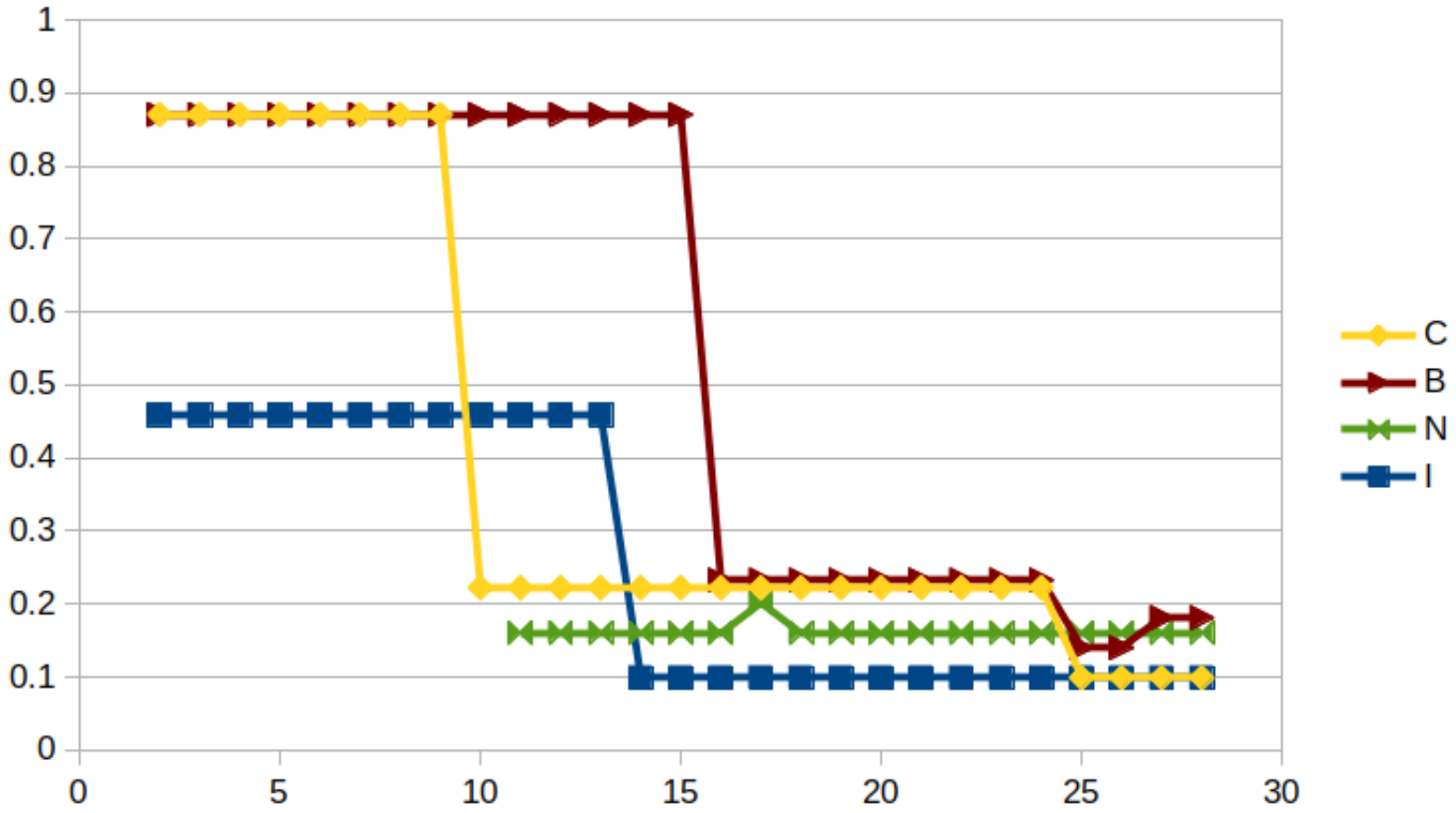
Security Scores: Exploitable Regions – sha256



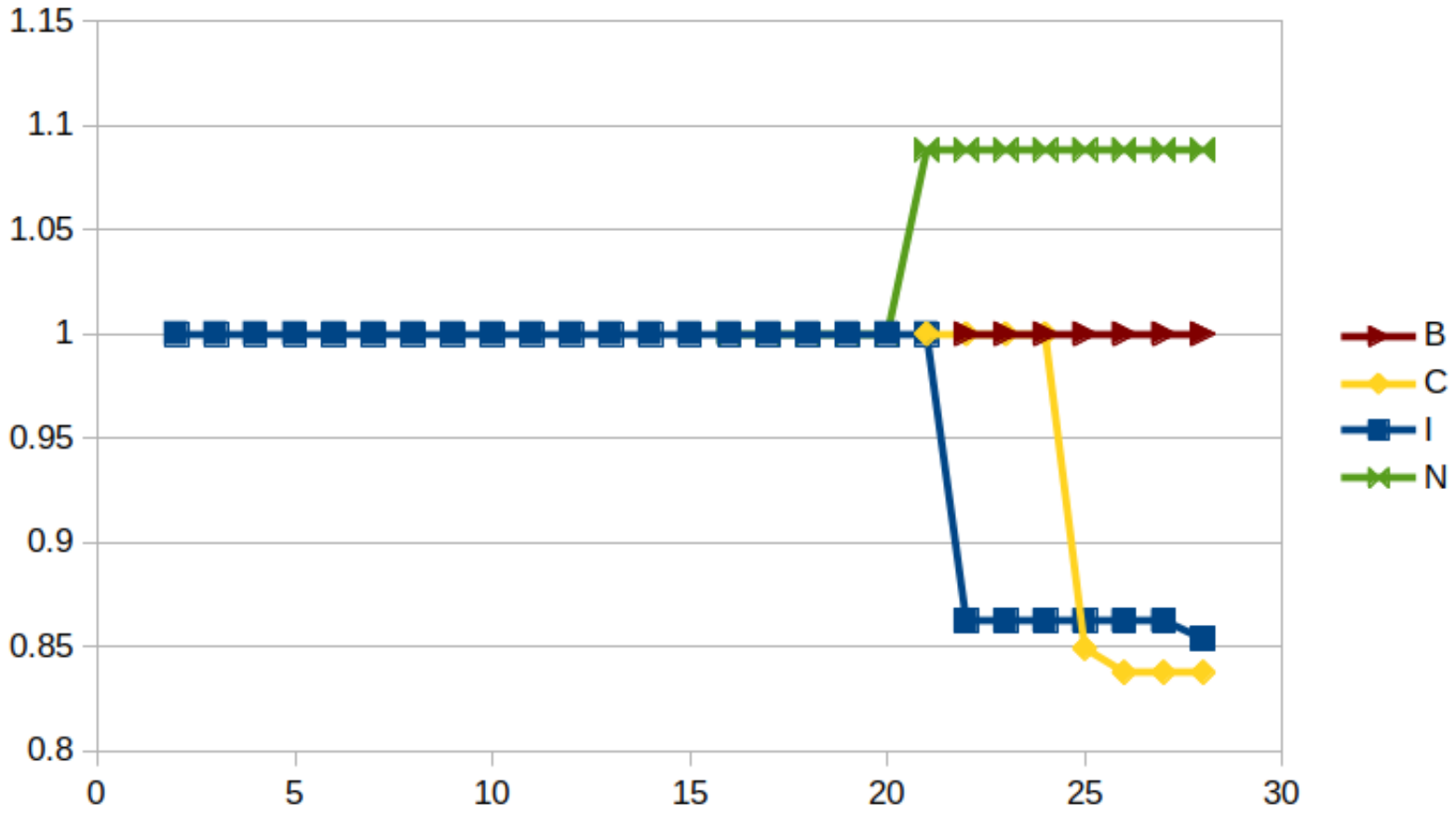
Security Scores: ECO Trojan Insertion – aes



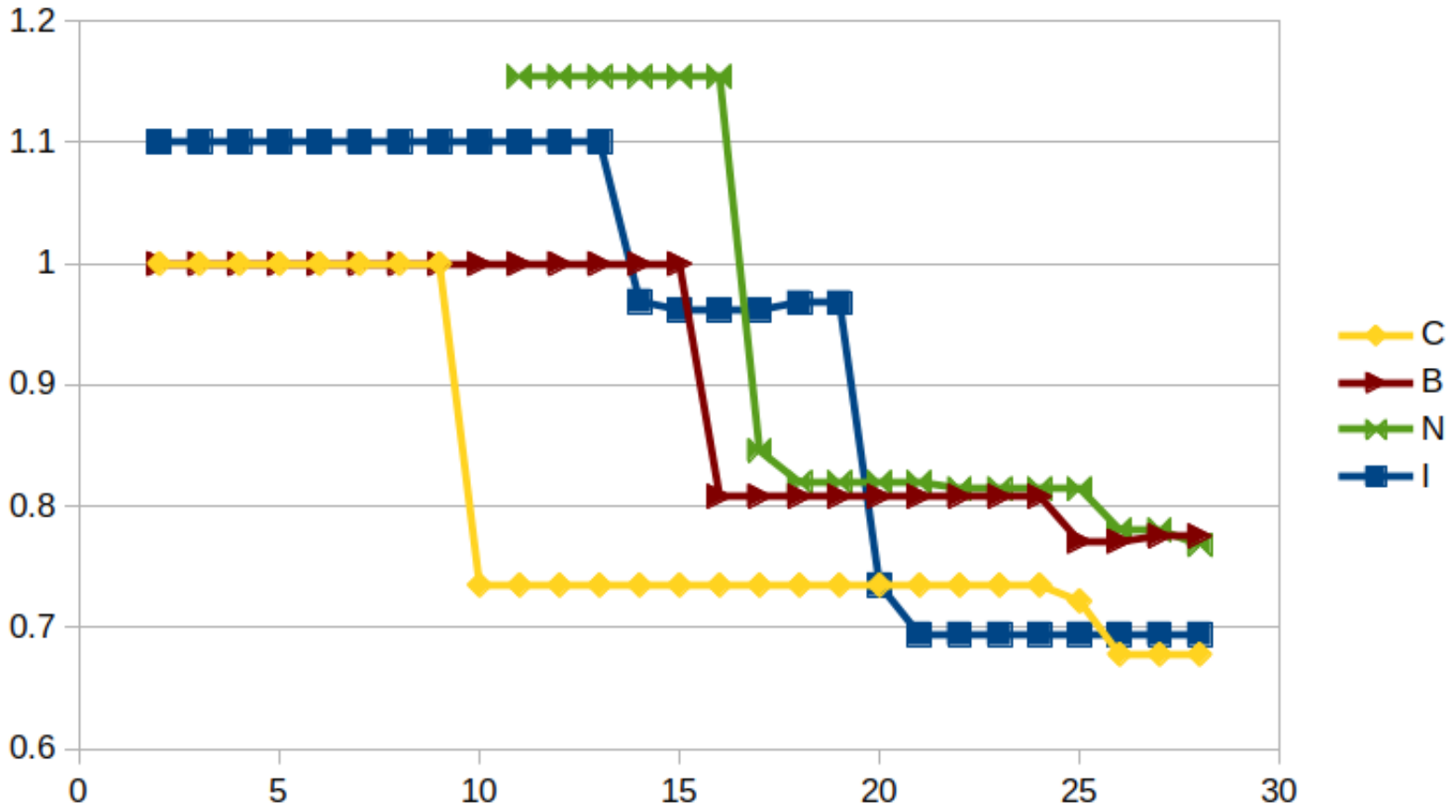
Security Scores: ECO Trojan Insertion – sha256



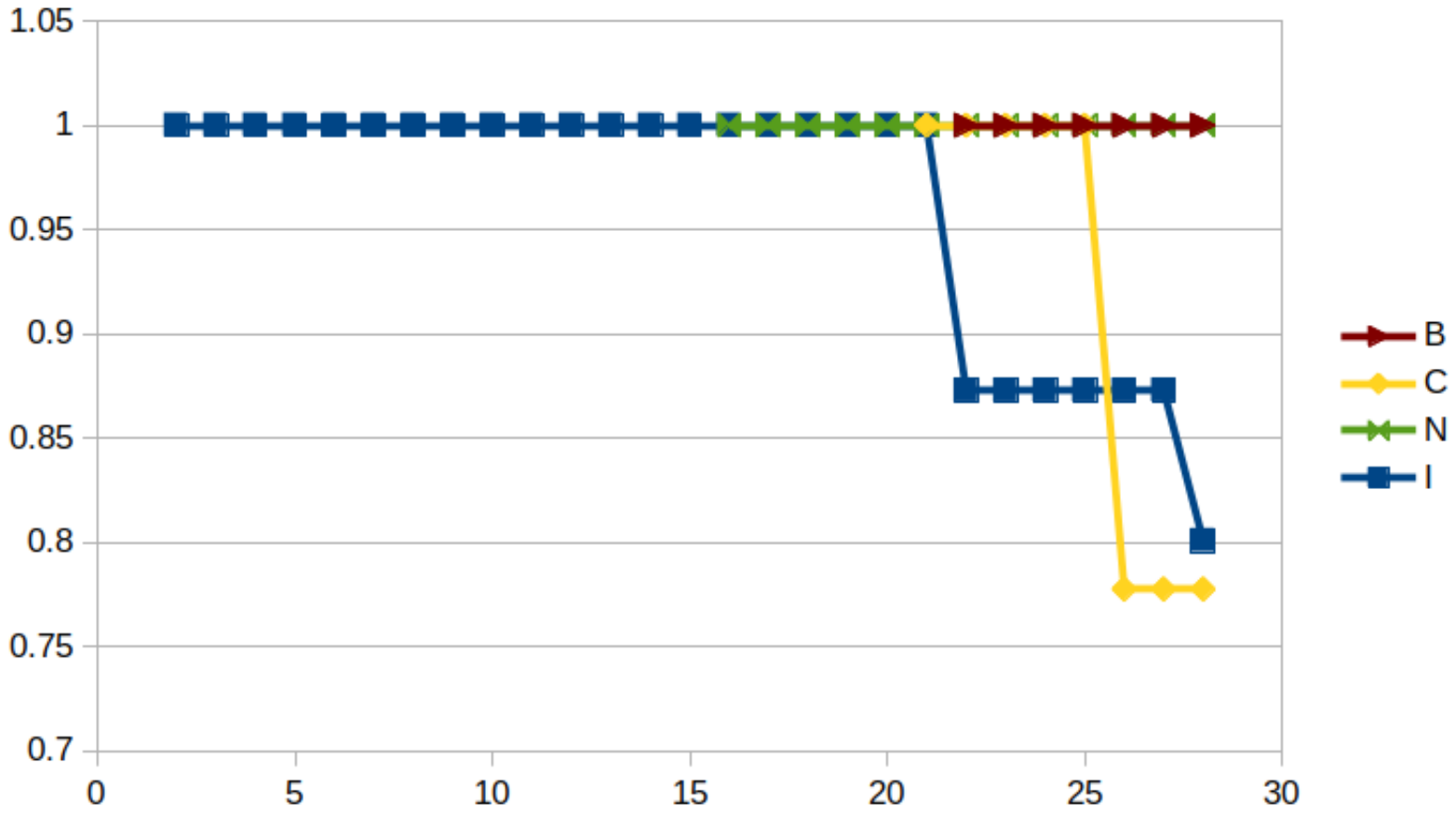
Design Scores – aes



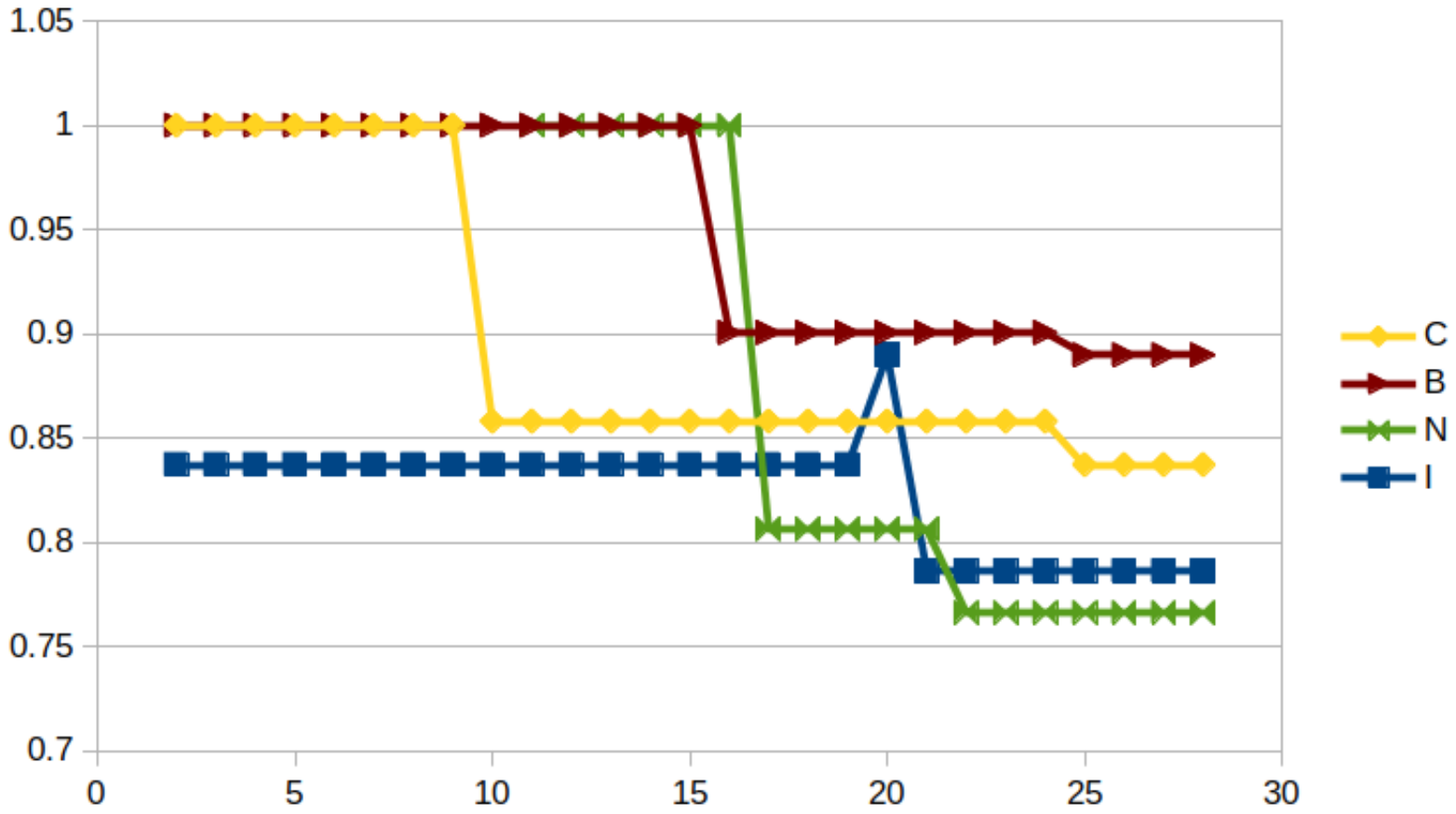
Design Scores – sha256



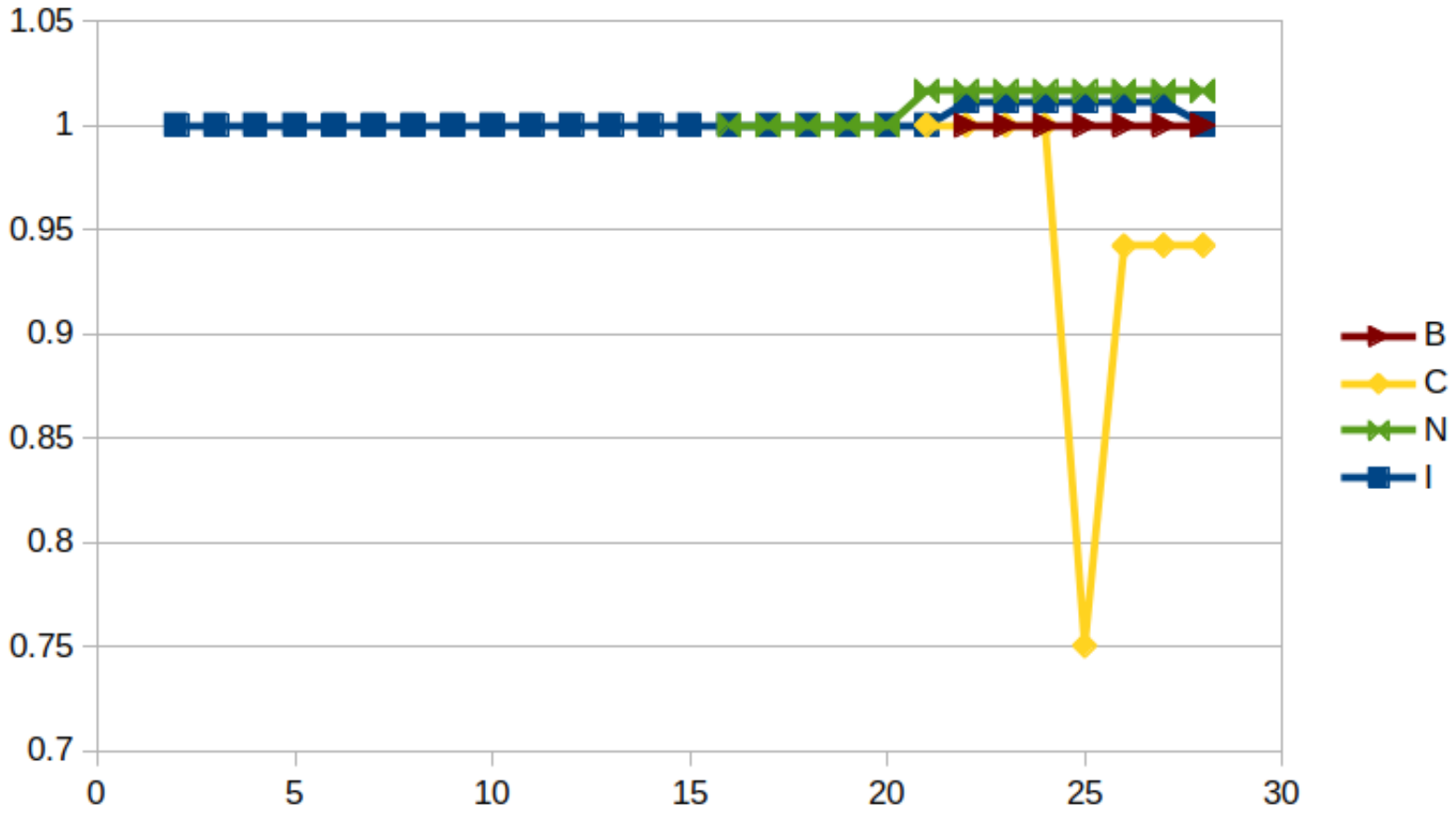
Design Scores: Area – aes



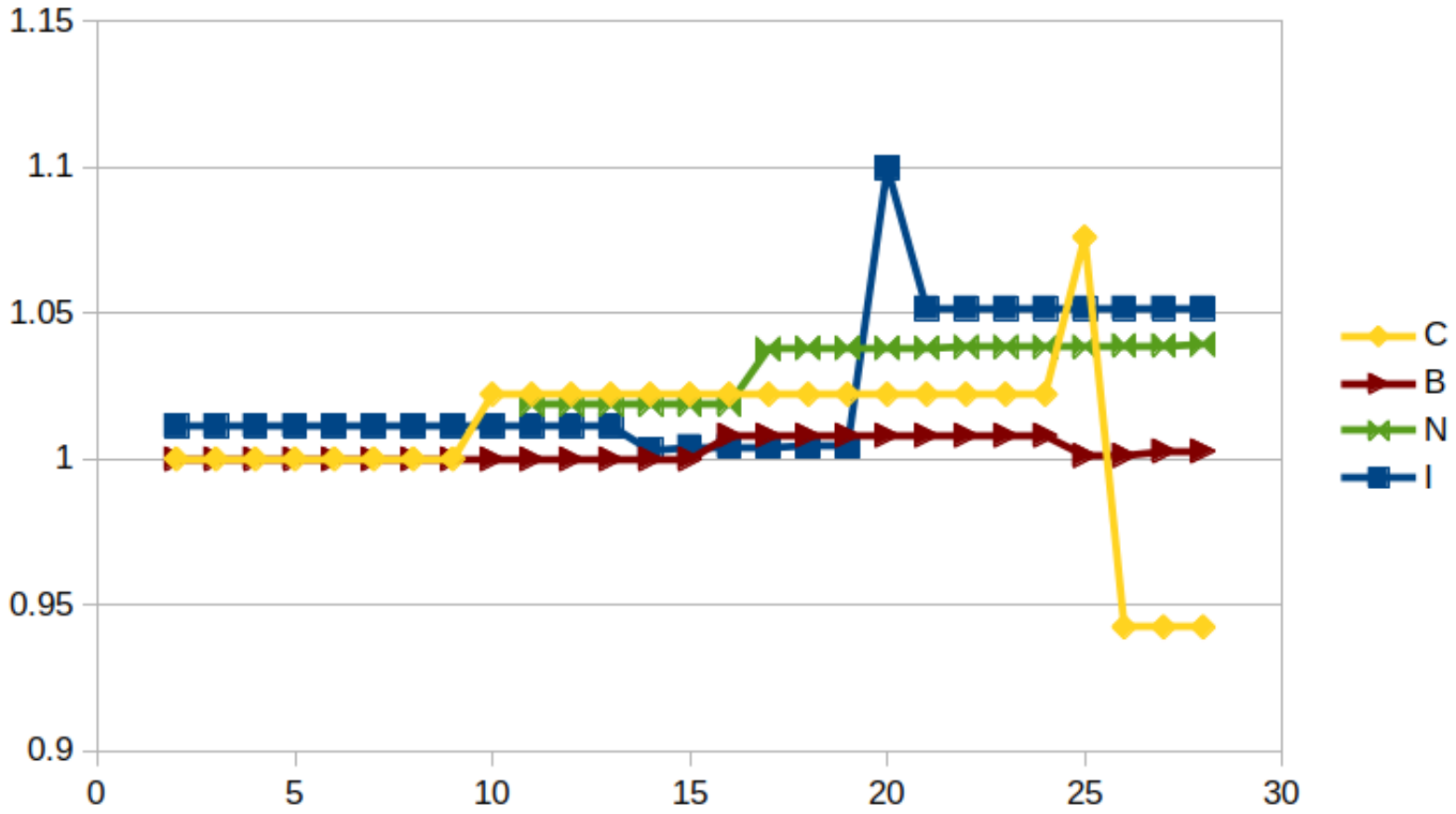
Design Scores: Area – sha256



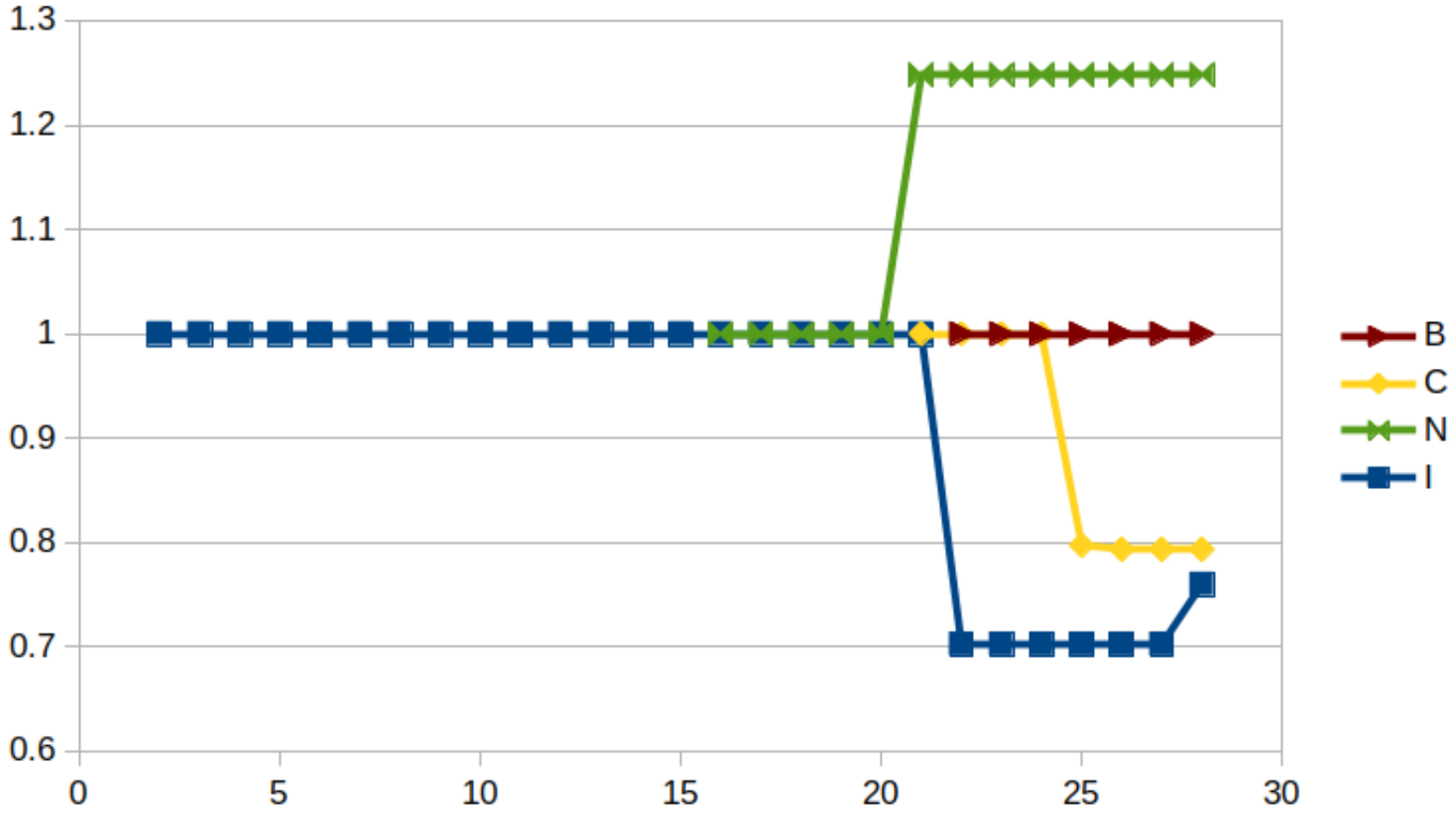
Design Scores: Power – aes



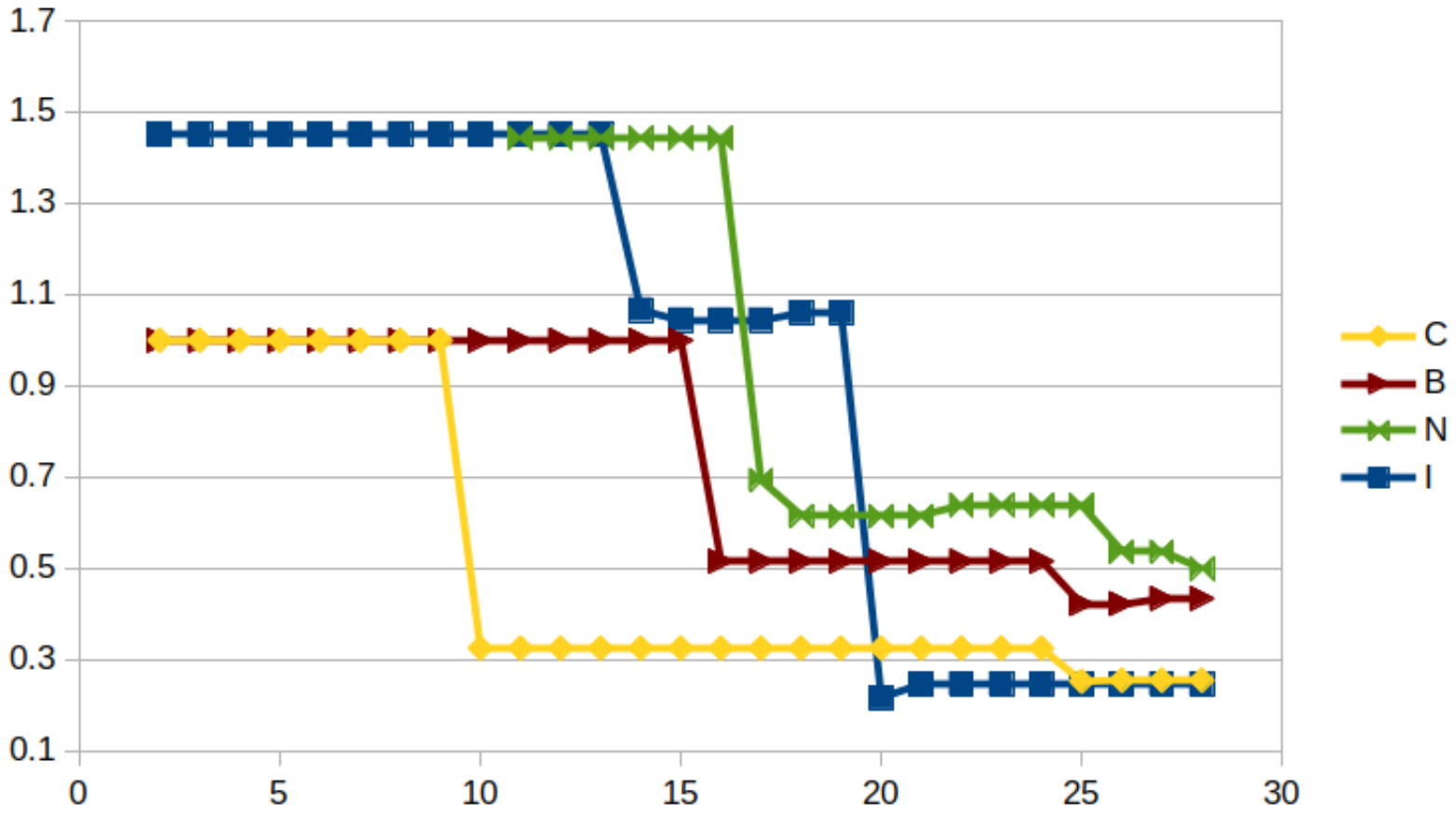
Design Scores: Power – sha256



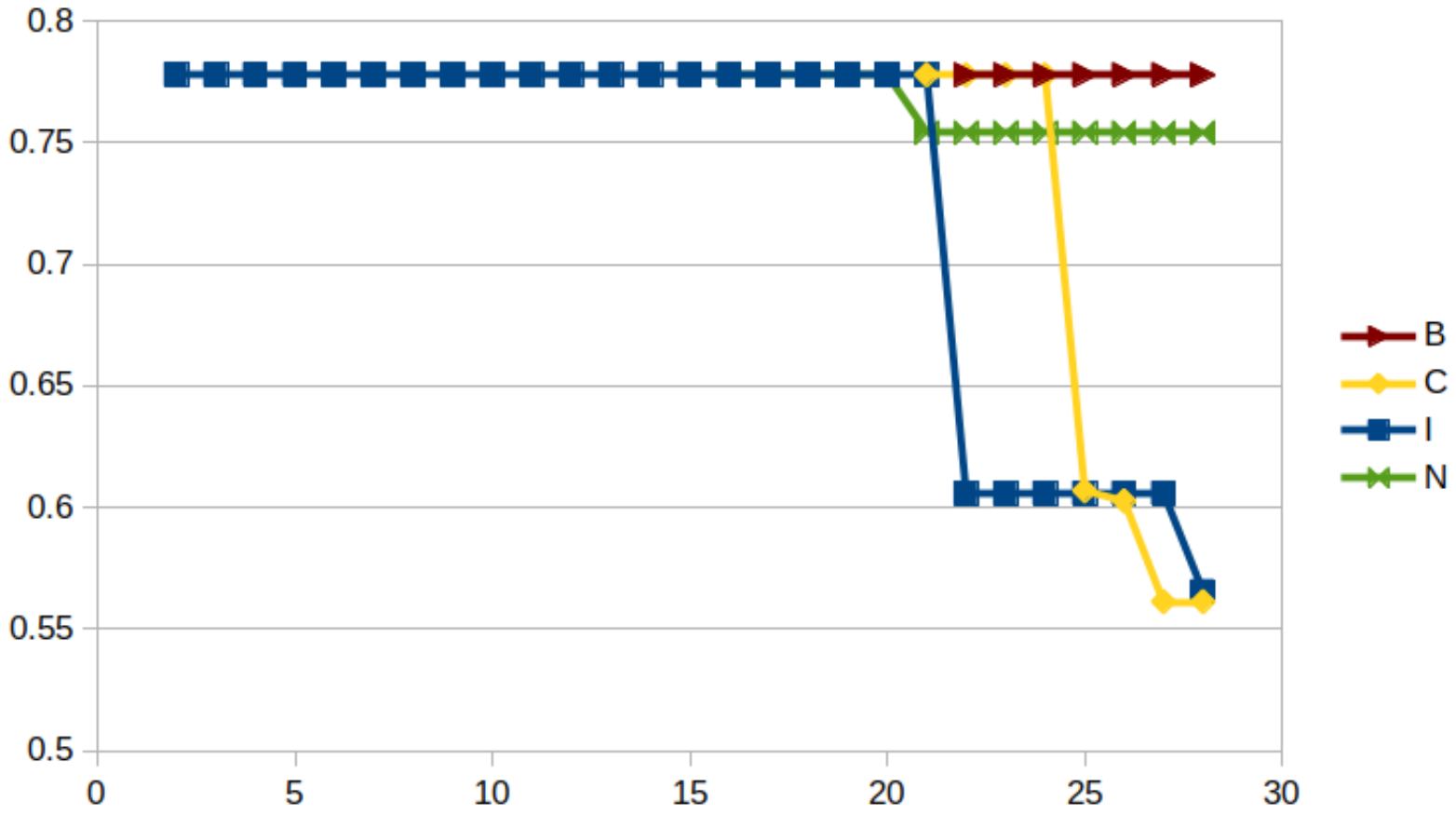
Design Scores: Performance – aes



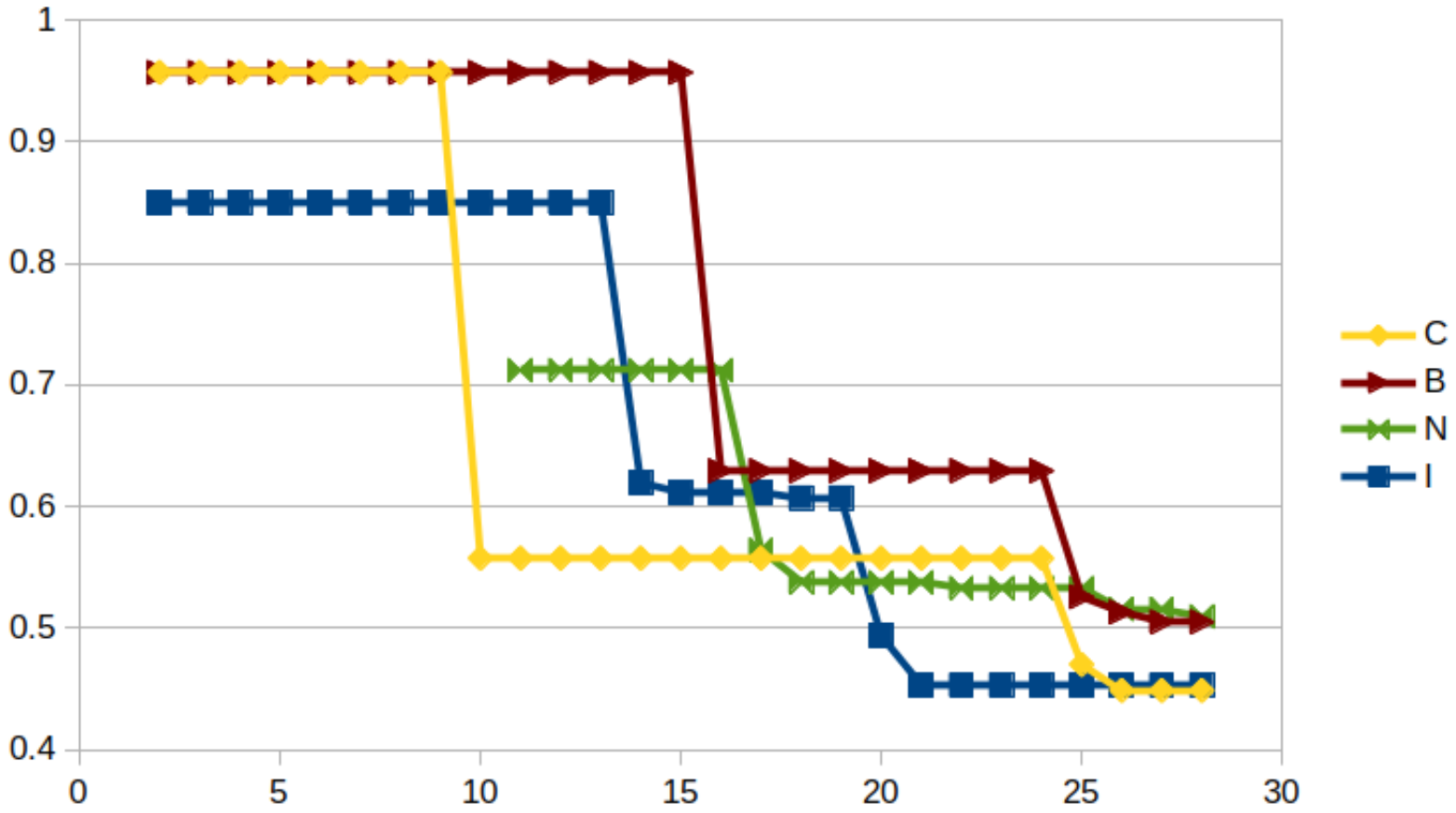
Design Scores: Performance – sha256



Overall Scores – aes



Overall Scores – sha256



Final Overall Scores

	I	C	B	N
aes	0.565435	0.561343	0.777777	0.754006
camellia	0.522997	0.494490	0.534280	0.614267
cast	0.583642	0.469255	0.598283	0.886812
misty	0.455685	0.451070	0.436367	0.668584
seed	0.623402	0.475763	0.595133	0.679480
sha256	0.452803	0.448919	0.505181	0.509680

Final Overall Scores and Ranking

	I	C	B	N
aes	2	1	4	3
camellia	2	1	3	4
cast	2	1	3	4
misty	3	2	1	4
seed	3	1	2	4
sha256	2	1	3	4
Avg. Ranks	2.333	1.167	2.667	3.833

	I	C	B	N
aes	0.565435	0.561343	0.777777	0.754006
camellia	0.522997	0.494490	0.534280	0.614267
cast	0.583642	0.469255	0.598283	0.886812
misty	0.455685	0.451070	0.436367	0.668584
seed	0.623402	0.475763	0.595133	0.679480
sha256	0.452803	0.448919	0.505181	0.509680

Announcement of Places and Winners

Announcement of Places and Winners

4th Place:
XDSecurity-II

Announcement of Places and Winners

3rd Place: CUEDA

4th Place: XDSecurity-II

Announcement of Places and Winners

2nd Place:
NTHU-TCLAB

3rd Place:
CUEDA

4th Place:
XDSecurity-II

Announcement of Places and Winners

2nd Place: NTHU-TCLAB

1st Place: FDUEDA

3rd Place: CUEDA

4th Place: XDSecurity-II

Conclusion

- Motivation:
  - More and more threats are arising that affect hardware
  - **Build up knowledge and experience in CAD community**
- Congrats to all finalists! Really great efforts!
- Thanks to everyone at ISPD committee for having us!
- Please keep in touch: https://wp.nyu.edu/ispd23_contest