Advanced Security Closure of Physical Layouts

[ISPD23 Contest]

Description

Last updated: March 21, 2023 (Q&A)

Welcome! This contest is part of the International Symposium on Physical Design (ISPD) 2023.

~~Register your team here!~~ (Registration is closed by now.)

On this main page, you will find an overview on the contest. Start with this page, and then follow the links and browse through the menu. First, you want to understand the approach and logistics explained here. Second, continue reading on the Details page for more insights on the theme in general, the threats in particular, and some technical guidance for tackling this contest. Third, see the Evaluation and Benchmarks for more technical details.

FYI, the website from last year's contest still remains online for reference. The main differences for this year's contest over 2022 are also highlighted in light orange on this main page.

For those of you new to the contest for this year, don't worry, there's no disadvantage to you. Likewise, there is no real advantage to those who already participated last year — only the overall theme is the same, but the challenges and details are different.

Looking forward to your participation — good luck!

Theme

CAD tools traditionally optimize for PPA. However, considering that various and serious threats are emerging, future CAD flows should also incorporate techniques for secure IC design.

The theme of this contest is *advanced security closure of physical layouts*, that is, hardening the physical layouts at design time against challenging threats that are executed post-design time.

This year's contest is focused on the threat of Trojans, with challenging aspects for physical design in general and for hindering Trojan insertion in particular. For one, layouts are based on the ASAP7 library and rules are more strict, e.g., no DRC issues and no timing violations are allowed at all. In the alpha/qualifying round, your defense against Trojan insertion will be evaluated using first-order metrics focused on exploitable placement and routing resources, whereas in the final round, your defense will be more thoroughly evaluated through trials for actual insertion of different Trojans. The final round may also cover further threats.

Approach

The objective of this contest is to implement security closure measures, i.e., to proactively harden layouts against post-design, layout-level Trojan insertion and further threats. Also see the Details page for more details on the threats.

To achieve this objective, participants would want to, e.g., control placement and routing in such a way that insertion of Trojan components (trigger and payload) becomes difficult, all while accounting for the impact on design quality induced by the proposed defense measures. There is no single, right or wrong approach toward that end — it is up to your creativity and skills to come up with the best defense solutions.

The scoring is based on a weighted function considering security and design metrics. There are also some constraints to be considered which will be more strict for this year's contest. For example, DRC issues and timing violations are hard constraints this year. See the Evaluation page for more details.

The benchmarks as well as submission are based on DEF and related files.

Participants must realize their means for advanced security closure in the context of physical design. Participants can work on any platform and tool setup of their choice. However, the setup must be able work with the ASAP7 library. (Note that the design of

benchmark layouts as well as the evaluation backend are based on Cadence Innovus. More details are mentioned on Evaluation and Benchmarks pages.)

Logistics, Awards

This contest is open to students (undergrads, graduates, and/or post-graduates) as well as industry practitioners from around the world, with prizes limited to academic participants. Participants need to register as a team with at least one student and one advisor; there are no upper limits on the number of team members or number of registrations/teams for individual participants.

There is an alpha round, using alpha-round benchmarks with alpha results and rankings published regularly and feedback provided to the participants early on during the alpha/qualifying round. All participants that submit, for each benchmark, some valid solutions which improve upon the baseline scores, move on the final round. There, final-round benchmarks are used, covering a wider range of designs and layout complexities, that are used for final results and rankings. The final round will also feature an extended, more realistic and more challenging evaluation approach.

Note that, for both alpha and final round, you can submit as many solutions as you which. While all submissions are evaluated (and backed-up), only your currently best solutions will be considered for any ranking. Official, final rankings are subject to manual checks by the contest organizers.

The final results and rankings will be first announced at ISPD, on March 29th 2023, and only then published here as well.

Cash prizes will be awarded to the top three teams: $1500 for 1st place, $1000 for 2nd place, and $500 for 3rd place. Also, award plaques will be manufactured after the announcement and mailed out to the top three teams.

Top teams are encouraged to disseminate their results and means for advanced security closure further with the community, but that is not a requirement for participation.

Check the announcements every now and then — registered participants will also be provided with announcements via email. See also the Timeline page.