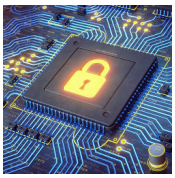

Security Closure of Physical Layouts

ISPD 2022 Contest

Description

Last updated: Sep 21st 2022

This contest was part of the International Symposium on Physical Design (ISPD) 2022.

The slides and final results can be found here. The benchmarks and scripts (would require some edits to rerun on your machine) can be found here. The layouts for final results can be made available upon request, but you need to check with the teams yourself for permission. Feel free to keep us (ispd22contest@nyu.edu) in the loop; we have the data on backup in case the teams don't have it.

See you for the 2023 contest!

~~Register here.~~ (Registration is closed.)
Looking forward to your participation — good luck!

On this main page, you will find an overview on the contest. So start with this page, and then follow the links and browse through the menu. Specifically, you first 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.

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 *security closure of physical layouts*, that is, hardening the physical layouts at design time against threats that are executed post-design time. This contest is focused on two types of threats, namely 1) Trojan insertion and 2) probing, fault injection. The objective of this contest is to implement measures for security closure, i.e., to proactively harden layouts against these threats.

Approach

More specifically, the objective of this contest is the following: implement measures for security closure to proactively harden layouts against 1) post-design Trojan insertion at gate level and 2) in-field electro-optical or contact-based probing, fault injection attacks targeting at the frontside (metal layers). Note that the latter, probing and fault injection, do share the same working principle, namely to "sneak through" metal layers down to devices or wires of interest. Again, also see the Details page for more insights 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) as well as probing and fault injection on particular devices or wires becomes difficult, all while also 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. See also the sample benchmarks for some initial ideas.

Participants must realize their means for security closure in the context of physical design. Participants can work on any platform and tool setup of their choice. The benchmarks as well as submission are based on DEF and related files.

The scoring is based on a weighted function considering security metrics for both threats as well as design-quality metrics. Participants may also work on only one of the two threats (Trojans or probing, fault injection), but that would likely undermine the scoring — likely but not necessarily, as some creative efforts to defend against one threat might also serve defending against the other threat. There are also some constraints to be considered. See the Evaluation page for more details.

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 made publicly available, with alpha results and rankings published regularly and feedback provided to the participants before and after the alpha-round deadline. All participants that submit some valid solution for each benchmark move on the final round. There, final-round benchmarks are used, a mix of public as well as blind benchmarks, covering a variety of designs and layout complexities, that are used for final results and rankings.

The final results and rankings will be first announced at ISPD, on March 30th 2022, 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 (March 30th) and mailed out to the top three teams.

Top teams are encouraged to disseminate their results and means for 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.