Advanced Security Closure of Physical Layouts

[ISPD23 Contest]

Details

Last updated: Dec 14, 2022

Security Closure

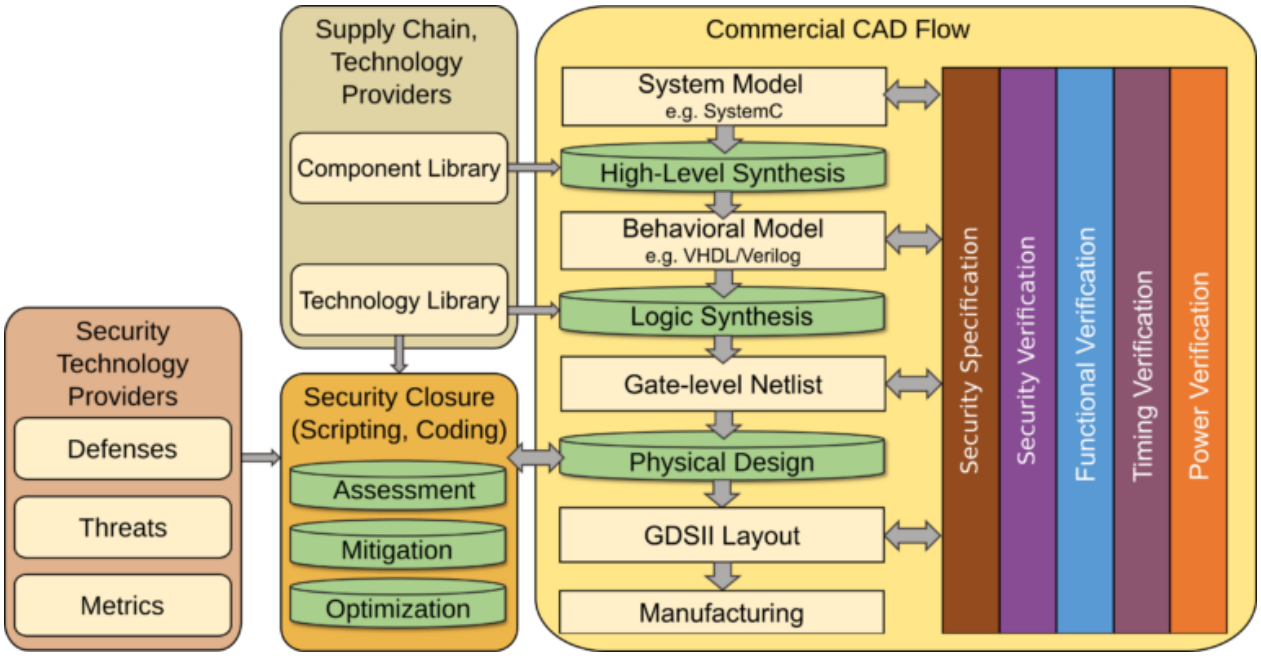
CAD tools traditionally optimize for PPA. However, considering that various and serious threats are emerging, future CAD flows should also incorporate techniques for secure IC design.

This contest is focused on *advanced security closure of physical layouts*, that is, on hardening the physical layouts at design time against various challenging threats that are executed post-design time. This topic is important for multiple reasons:

1. Many threats like Trojan insertion or side-channel attacks are directly targeting vulnerabilities of the physical layouts.
2. Threats that are not mitigated during design-time are almost impossible to fix later on; ICs are unlike patchable software.
3. Even if efforts are taken toward secure IC design at higher abstraction layers, like high-level synthesis or logic synthesis, such efforts may easily be undermined again by, e.g., security-unaware PPA optimization, thus becoming futile without dedicated support for security closure at layout level.

Secure-by-design and *security closure* are two related, emerging paradigms for CAD tools. Secure-by-design means to support (1) top-down propagation and translation of security requirements and specifications and (2) bottom-up verification and validation of defenses against attacker's technical capabilities and limitations. Security closure is

the specific paradigm for the physical design, conceptually similar to other sign-off stages like timing closure but focused on security. Means for security closure will be based on ECO placement, routing, etc., as needed. A secure-by-design CAD flow with integrated means for security closure is outlined next.



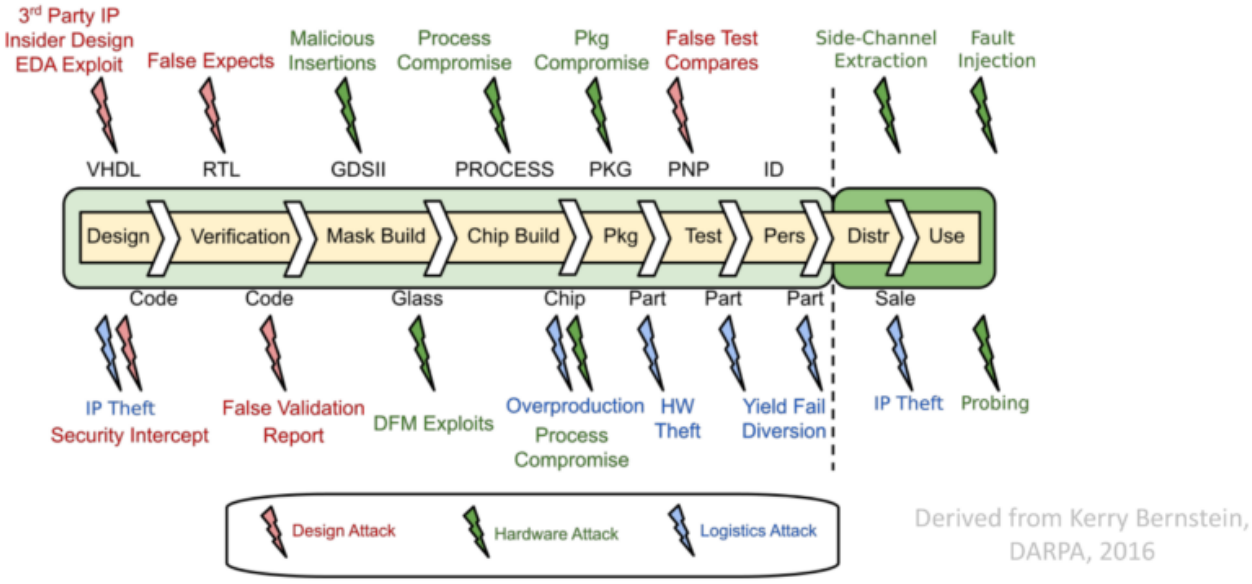
The objective of this contest is the following: implement measures for advanced security closure to proactively harden layouts against post-design, layout-level Trojan insertion. More details on this threat are discussed below, in the section on Hardware Security. *Note that the final round may cover further threats as well; this will be announced in time.*

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. At the same time, the impact of the measures on design quality must be considered as well. Given that there are different, possibly competing metrics to be considered for design quality and security closure at once, some machine learning-based guidance could be promising here. In any case, 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.

To enable a fair contest, **we have to restrict the scope of defense efforts to physical-design stages with use of standard cells.** Thus, we do not allow to, e.g., introduce any cell-level modifications. Also see the Evaluation page for more details on constraints as well as for some guidance for permissible defense efforts.

Hardware Security

There are various challenges or rather threats to consider when we talk about hardware security. An overview on threats linked to the different stages of the IC supply-chain and life-cycle is shown next.



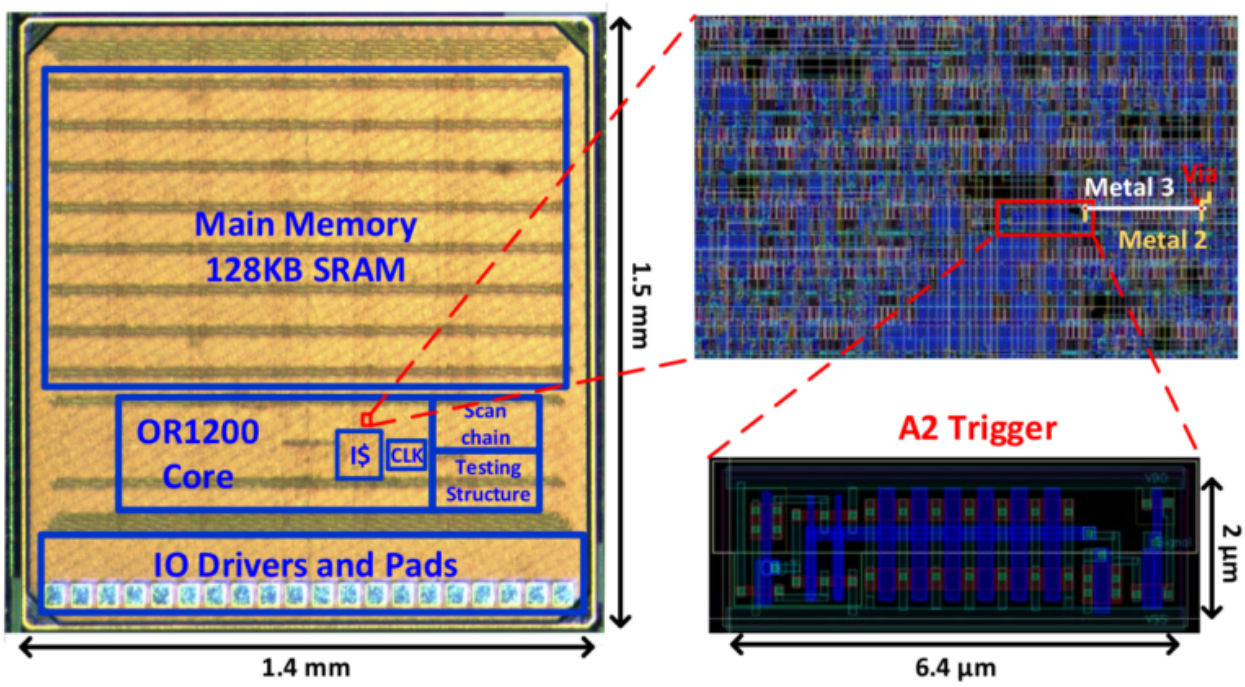
The main threats of current interest to the community are (1) Trojans, (2) side-channel attacks, (3) fault-injection attacks, (4) probing attacks, and (5) IP piracy. Typically, each kind of threat is further divided/categorized. For example, there is direct physical fault injection, e.g., using laser light, voltage glitches, etc., versus indirect fault injection, e.g., repetitive writing to physical memory locations (also known as “Rowhammer” attack). Some threats share a similar physical attack vector, like laser fault injection and laser-assisted optical probing.

The threats relevant for this contest are **Trojan insertion at the layout level and some further threat(s), yet to be disclosed, for the final round.** More details on those threats and aspects relevant for this contest are discussed next.

Trojans are malicious hardware modifications. The notion of Trojans is diverse, covering malicious hardware modifications that are: (i) targeting at the system level, RTL, gate/transistor level, and/or the physical level; (ii) seeking to leak information from an IC, reduce the IC’s performance, or disrupt an IC’s working altogether; (iii) are always on, triggered internally, or triggered externally; etc. Most Trojans comprise a trigger and a payload; the trigger activates the payload on attack conditions, and the payload serves to perform the actual attack.

Since IC supply-chains are largely outsourced nowadays, adversaries at various entities could introduce such Trojans, e.g., through untrustworthy third-party IP, by adversarial designers, during mask generation or manufacturing, or even during distribution or deployment of ICs.

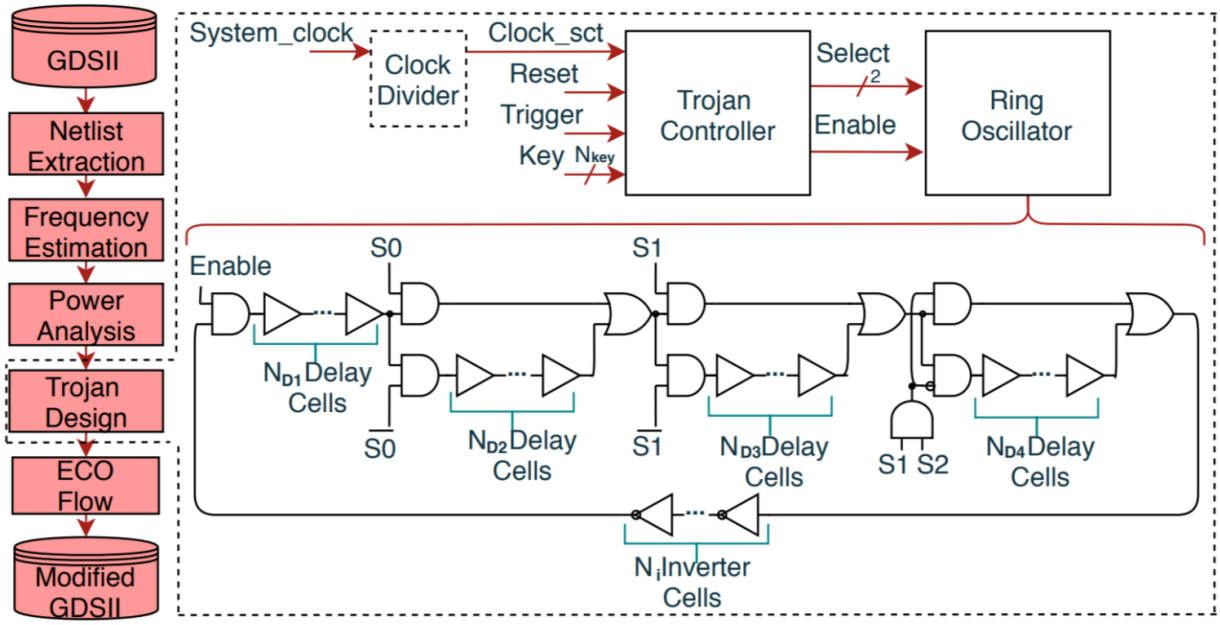
For this contest, we focus on Trojans that are inserted at the layout level post-design, i.e., during outsourced mask generation or manufacturing. An example of such a Trojan is shown next. More specifically, illustrated is the die snapshot of an OR1200 processor with the so-called A2 Trojan embedded, with the zoom-in highlighting the additional logic inserted for the Trojan trigger. The payload of the A2 Trojan, maliciously setting the privilege mode of the OR1200 processor, is not highlighted separately; only the additional routing toward the privilege-mode register is indicated by white/yellow wiring (labelled Metal3/2).



For those interested in more details for this particular Trojan, see the paper by Yang et al. listed in the references; however, knowledge of this particular Trojan and its specifics are not needed to tackle the contest.

The related task for this contest is to proactively harden the layouts against post-design Trojan insertion. This means to, e.g., control placement and routing in such a way that insertion of Trojan components (trigger and payload) becomes difficult, but also considering impact on design quality of such measures at the same time. As indicated, 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 actual insertion of Trojans can be realized in many different ways, also depending on the type, size, etc. of the Trojan. Note that **the final round will feature actual insertion of different types of Trojans** into the hardened layouts submitted by the participants. This is meant to provide a more meaningful and realistic evaluation of the layouts' security (and design quality) achieved by the participants. For an example of such Trojan insertion, see the figure below and the paper by T. Perez et al. listed in the references.



References

- J. Knechtel, J. Gopinath, M. Ashraf, J. Bhandari, O. Sinanoglu, and R. Karri, "Benchmarking security closure of physical layouts," in Proc. Int. Symp. Phys. Des. (ISPD), 2022
  PDF
- J. Knechtel, J. Gopinath, J. Bhandari, M. Ashraf, H. Amrouch, S. Borkar, S.-K. Lim, O. Sinanoglu, and R. Karri, "Security closure of physical layouts," in Proc. IEEE/ACM Int. Conf. Comput.-Aided Des. (ICCAD), 2021
  PDF
- J. Knechtel, E. B. Kavun, F. Regazzoni, A. Heuser, A. Chattopadhyay, D. Mukhopadhyay, S. Dey, Y. Fei, Y. Belenky, I. Levi, T. Güneysu, P. Schaumont, and I. Polian, "Towards secure composition of integrated circuits and electronic systems: On the role of EDA," in Proc. EDAA/ACM/IEEE Des. Autom. Test Eur. (DATE), pp. 508-513, 2020 (DOI: 10.23919/DATE48585.2020.9116483)
  PDF

- 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
  DOI: 10.1109/ISCAS51556.2021.9401481
- S. Mitra, H. S. P. Wong, and S. Wong, “The Trojan-proof chip,” IEEE Spectrum, 2015, 52, 46-51
  DOI: 10.1109/MSPEC.2015.7024511
  [The logo image is from this reference.]
- J. Knechtel, “Hardware security for and beyond CMOS technology,” in Proc. ACM Int. Symp. Phys. Des. (ISPD), pp. 115-126, 2021 (DOI: 10.1145/3439706.3446902)
  PDF
- Rangarajan N., Patnaik S., Knechtel J., Rakheja S., Sinanoglu O. (2021) Introduction. In: The Next Era in Hardware Security. Springer.
  DOI: 10.1007/978-3-030-85792-9_1
- W. Hu, C. -H. Chang, A. Sengupta, S. Bhunia, R. Kastner and H. Li, “An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools,” in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, pp. 1010-1038, June 2021
  DOI: 10.1109/TCAD.2020.3047976
- K. Xiao et al., “Hardware trojans: Lessons learned after one decade of research,” Trans. Des. Autom. Elec. Sys., vol. 22, no. 1, 2016
  DOI: 10.1145/2906147
- K. Yang, M. Hicks, Q. Dong, T. Austin and D. Sylvester, “A2: Analog Malicious Hardware,” 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 18-37
  DOI: 10.1109/SP.2016.10