AN OPEN CAD FLOW TO OPTIMISED KEY GATE INSERTION IN LOGIC LOCKING

ROSELYNE CHOTIN AND LILIA ZAOURAR

ROSELYNE.CHOTIN@LIP6.FR, SORBONNE UNIVERSITÉ, CNRS, LIP6. LILIA.ZAOURAR@CEA.FR - UNIVERSITÉ PARIS-SACLAY, CEA, LIST, F-91120 PALAISEAU, FRANCE

Context and motivation

- Increasing complexity of Integrated Circuits (ICs)
  ⟹ increase in production costs.
- Parts of the design and manufacturing are delegated to third party companies.
- Loss of control over these steps increases.
- High risk of threats such as theft of dedicated hardware blocks (IP), overproduction of ICs, and insertion of **Hardware Trojan (HT)**.
- Safety-related methods must be integrated into the design flow to be widely used.
- To have a full control of the design phase, integrating this kind of methodology in an **open Computer Aided Design (CAD)** flow, can be helpful.

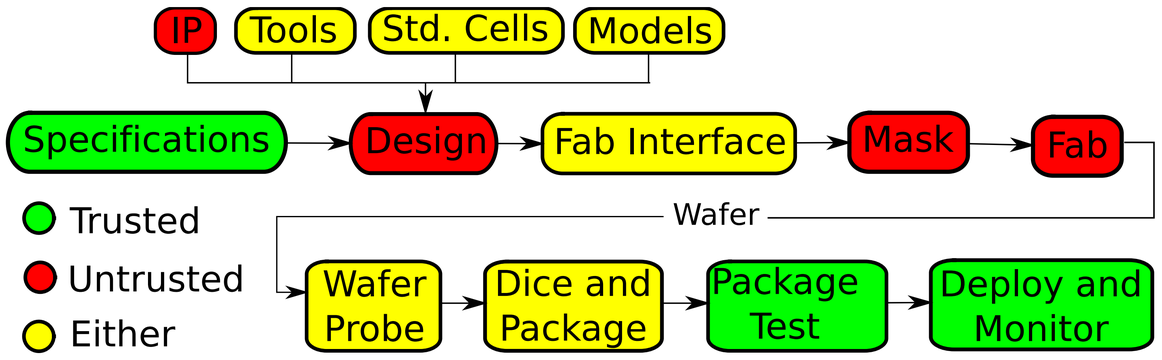


Fig. 1 : Major parts of the IC supply chain are untrusted (source: Mentor Graphics 2015).

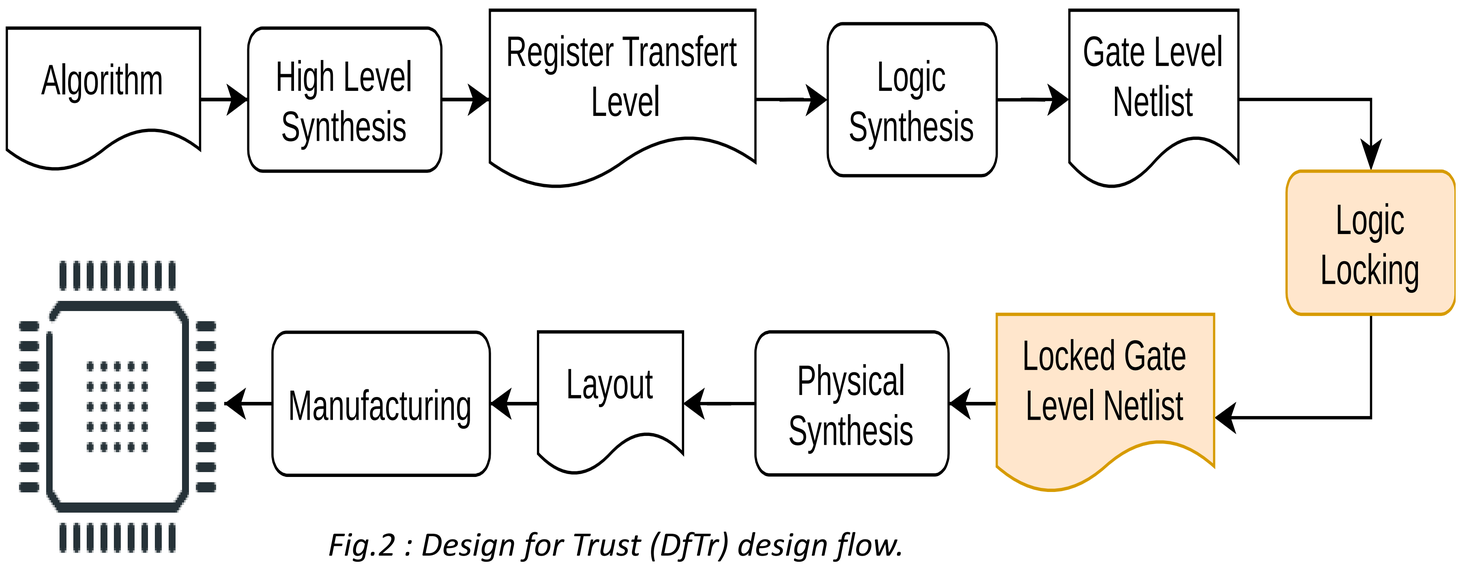


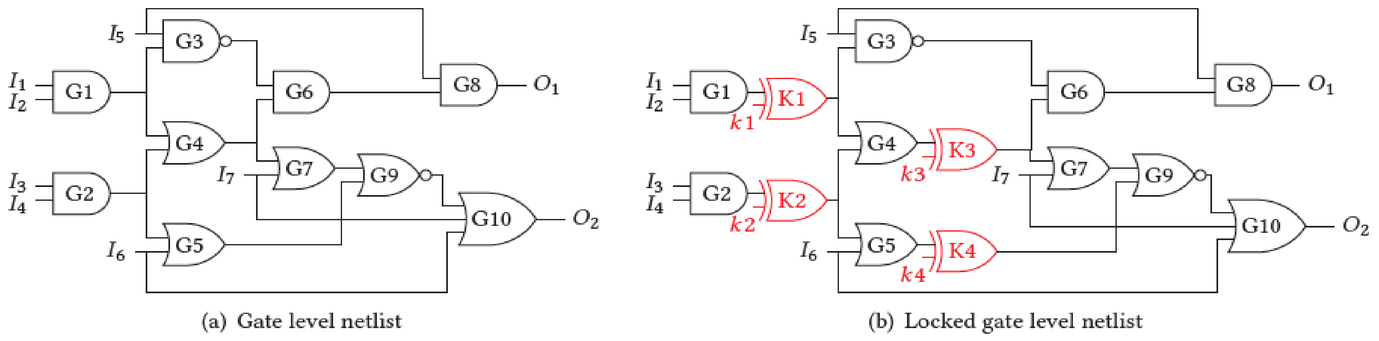
Fig.2 : Design for Trust (DfTr) design flow.

Logic Locking

- A promising DfTr solution to counteract overproduction [1, 2].
- Method adds logic gates in the circuit, connected to an unreadable memory that serves as a digital key.
- This allows to block any illicit use of the circuit and IC security is ensured.
- Lock the functionality of the circuit by modifying the gate level netlist, obtained after logic synthesis in a conventional IC design flow, through key gates insertion.
- It includes the counter-costs : delay, area, and power consumption.

Existing techniques

- Design for Hardware Trust (DfHT) have been developed.
- Goal : guarantee the proper functioning of ICs despite the use of unreliable IP blocks and manufacturing in an unreliable foundry.



(a) Gate level netlist (b) Locked gate level netlist

Fig. 3 Logic locking and key gates insertion.

Contributions

- Take into account, as early in the design phase, both countermeasures against HTs and performance.
- Ensure that the SoC behavior is guaranteed despite untrusted IPs vendors or foundry.
- Establish and evaluate security properties and integrate them during synthesis with **multi-objective optimization** techniques
- Mathematical modeling of the problem that takes into account both the performance and the HTs‘ effects.
- Security measure is calculated as in [5] : rely on the **size of the cliques** present in the **interference graph** of the circuit.
- Optimize this measure while keeping IC performance.
- First method models the key-gates insertion problem and its exact. resolution, as well as an heuristic approach using non linear program.
- Numerical results : good solution with an **Hamming distance** around **40%** in a computation time of **less than 40 min** (for the largest bench).

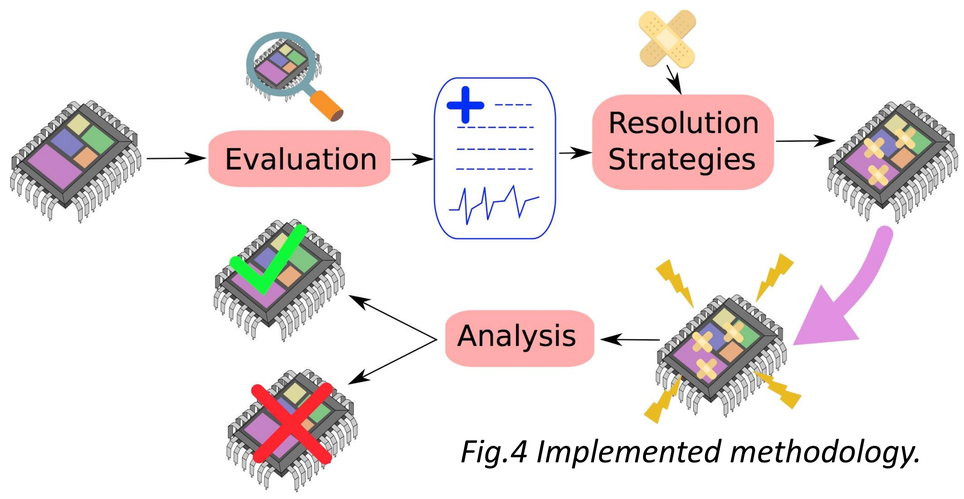


Fig.4 Implemented methodology.

CAD Flow

- Methodology successfully integrated in a standard open CAD flow : Yosys & Coriolis.
- **Yosys** synthetizes the RTL description of the circuit
- **Coriolis** can manipulate the obtained netlist to add the key gates to the points given by the resolution of the key-gates insertion problem to produce the locked netlist

Acknowledgment

This work is a part of the project MOOSIC ANR-18-CE39-0005, funded by The French National Research Agency.

[1] J. Rajendran et al. “Security Analysis of Logic Obfuscation”, DAC 2012, pp. 83–89.
[2] S. Dupuis et al. “A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans”, IOLTS 2014.
[3] C. Wolf et al. “Yosys-a free Verilog synthesis suite”. Austrochip 2013.
[4] C. Alexandre et al. “TSUNAMI: An Integrated Timing-Driven Place And Route Research Platform”. DATE 2005
[5] K Xiao et al. “Hardware Trojans: Lessons Learned after One Decade of Research”. In: DAC 2016.