# Research Project Proposal:

# IP Protection through Logic Locking at Register-Transfer Level

Luca Collini
luca.collini@mail.polimi.it
CSE

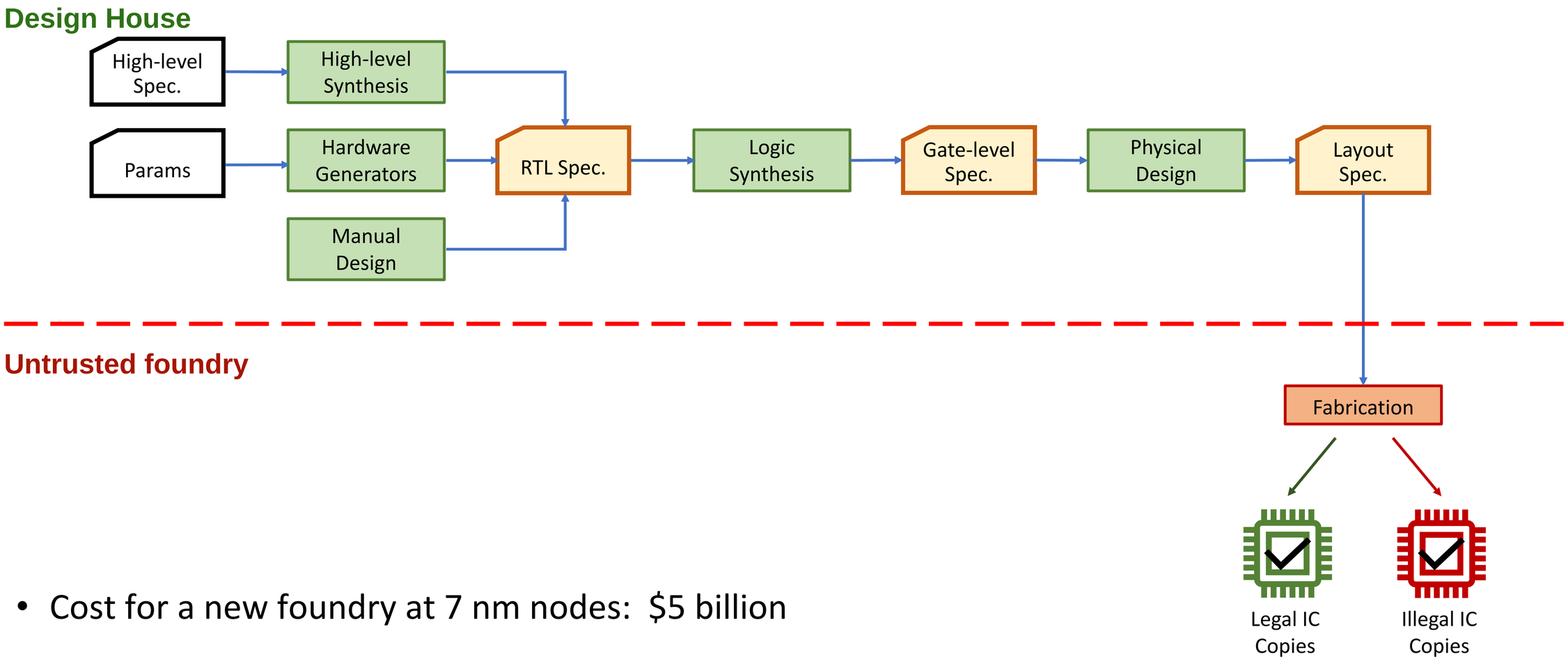
POLITECNICO
MILANO 1863

HONOURS PROGRAMME
HP-SR
in Information Technology

# Outline

- **Introduction to the problem**
  - Globalization of the IC supply chain & security threats
  - Logic locking
- Research goal
- State of the art
- Research plan

# Globalization of the IC supply chain




- Cost for a new foundry at 7 nm nodes: $5 billion

# Security threats

**Reverse Engineering**

## Intellectual Property theft

**estimated loss due to IP violations alone was $4 billions in 2008**

**total loss from IC counterfeiting was estimated to be about $169 billions in 2011**

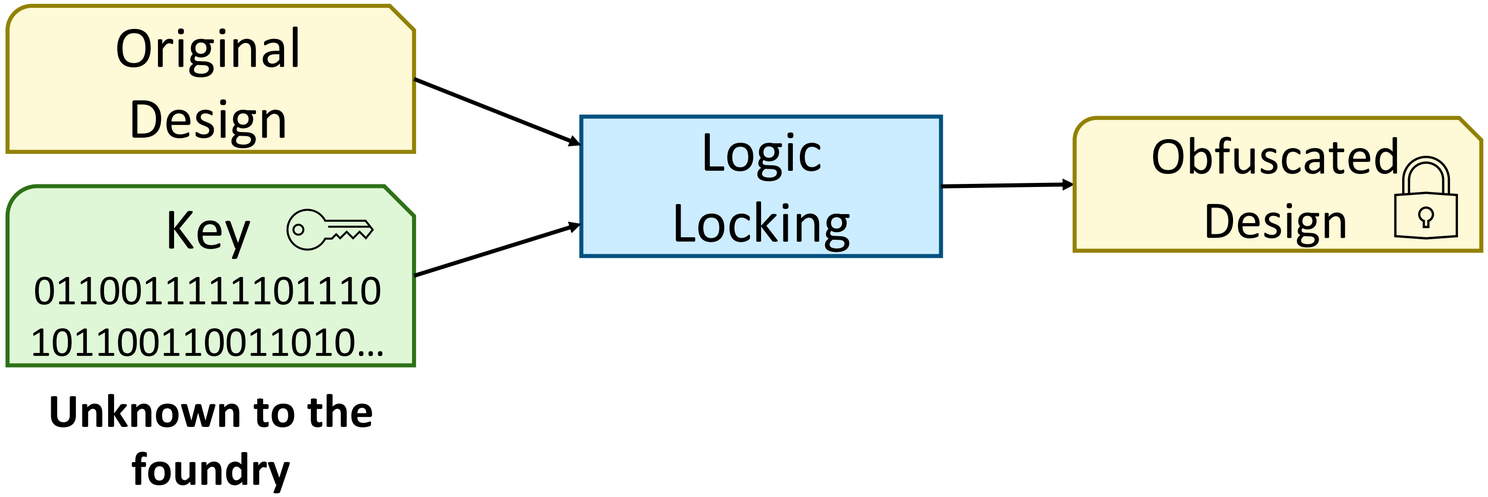
## Malicious modifications

**backdoor insertion**

**planned obsolescence trojans**

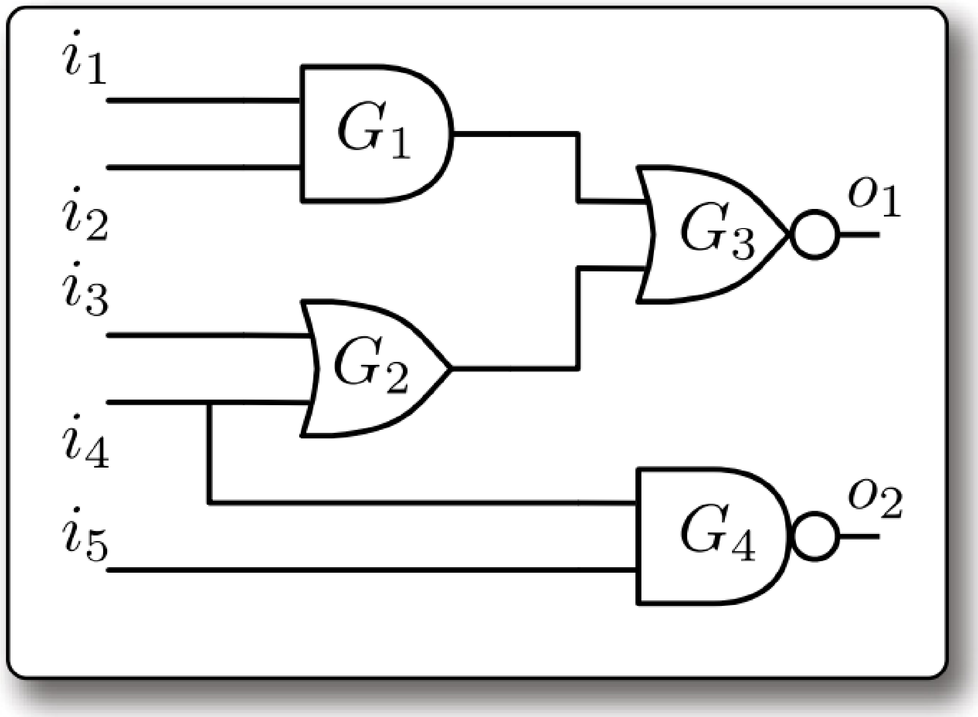
# Logic Locking

**Thwarting reverse engineering**

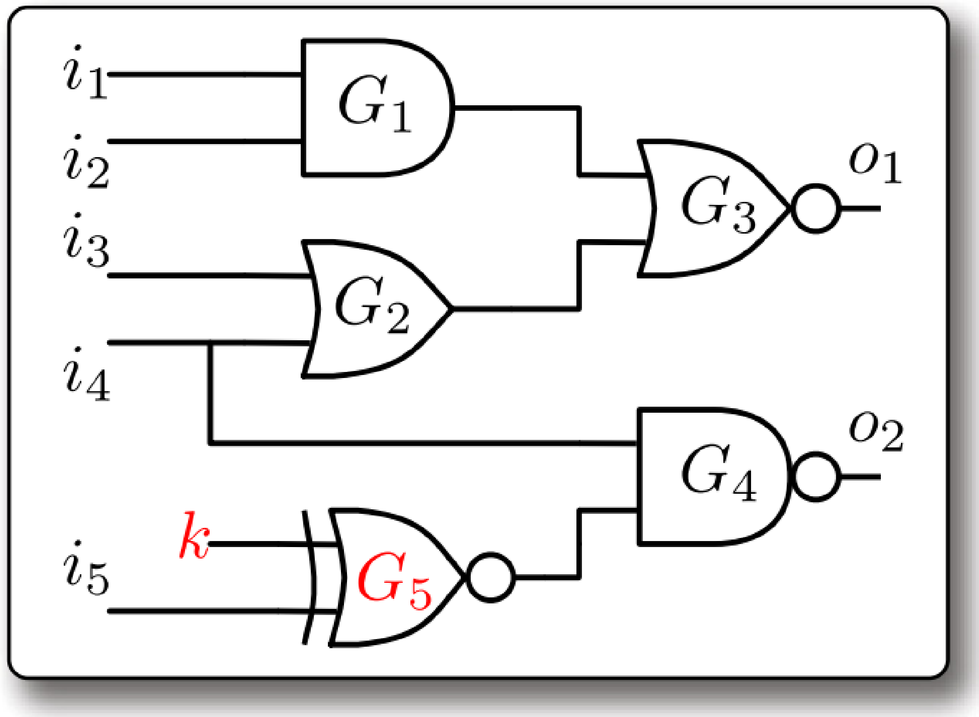


# Logic Locking

**Plain design**

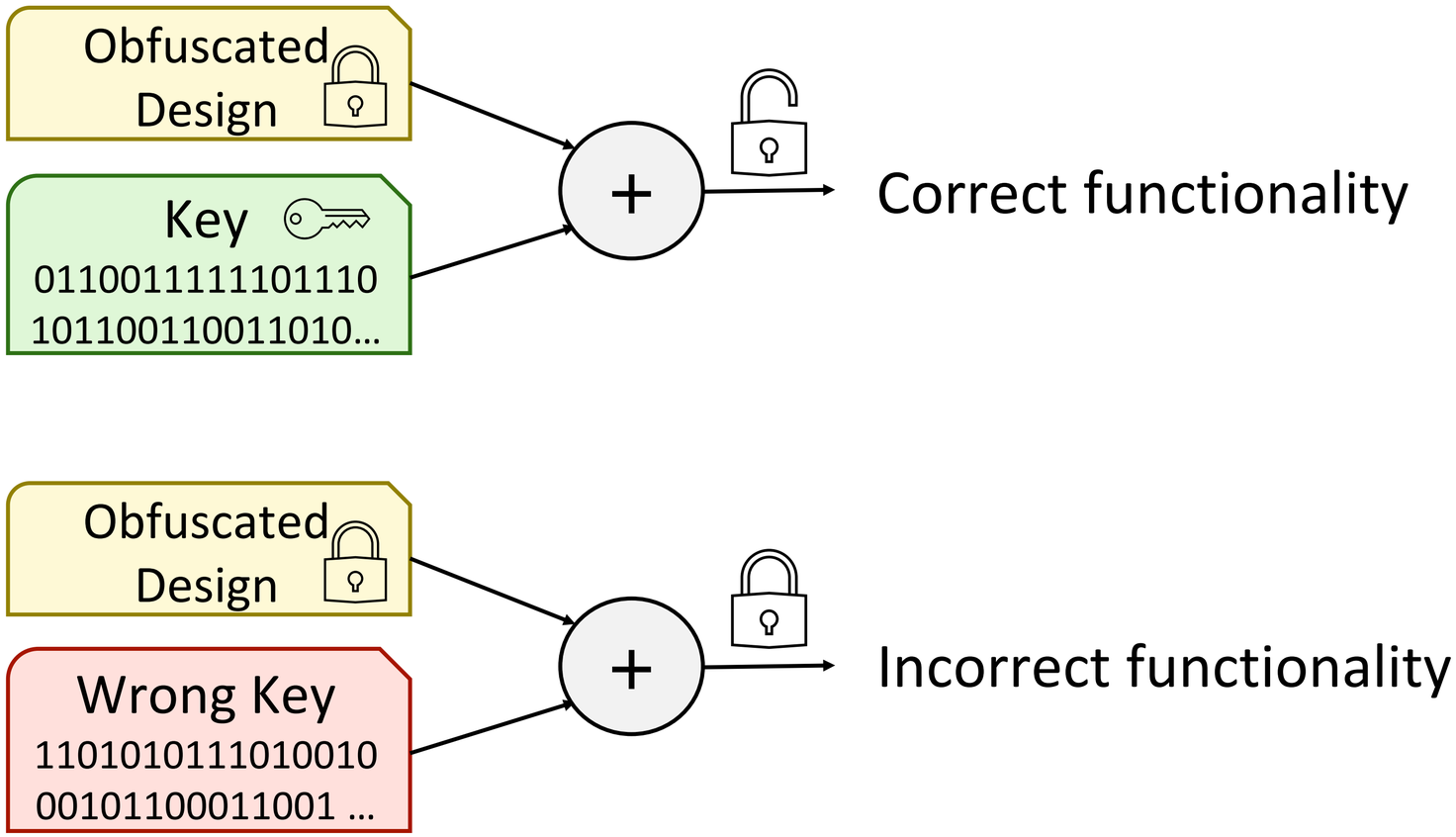



**Obfuscated design**




Shamsi, K., Li, M., Plaks, K., Fazzari, S., Pan, D. Z., and Jin, Y. Ip protection and supply chain security through logic obfuscation: A systematic overview

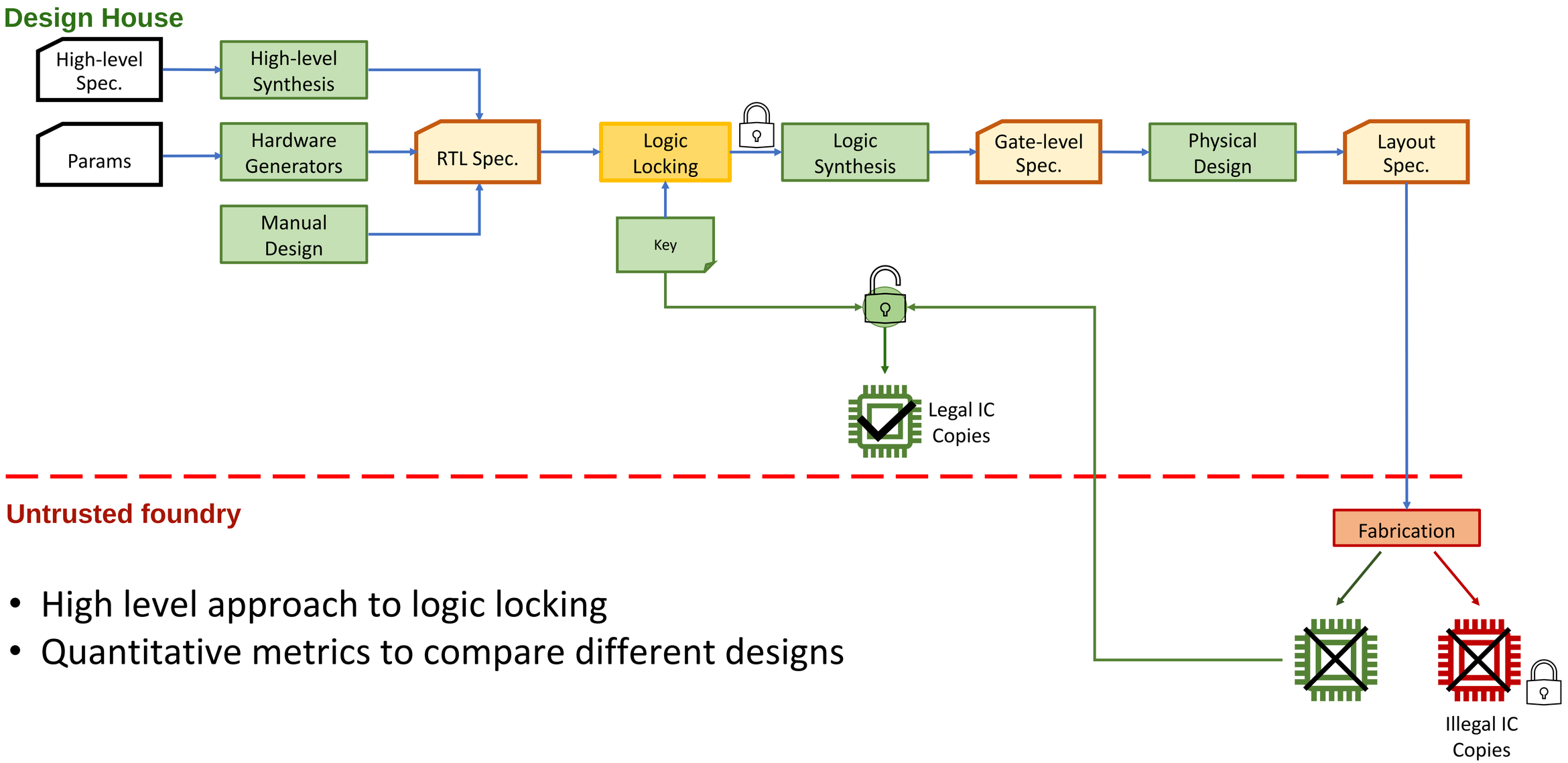
# Logic Locking



# Outline

- Introduction to the problem
  - Globalization of the IC supply chain & security threats
  - Logic locking
- **Research goal**
- State of the art
- Research plan

# Research goal




- High level approach to logic locking
- Quantitative metrics to compare different designs

# Outline

- Introduction to the problem
  - Globalization of the IC supply chain & security threats
  - Logic locking
- Research goal
- **State of the art**
- Research plan

# State of the art

**Threat model**: defines goals and abilities of the attackers

## Logic locking threat models

- *Oracle:* a chip that performs correct computations
- *Ambiguity:* ability of an attacker to distinguish between primary inputs and key inputs

## Common threat models:

- *Distinct ambiguity oracle-guided:* commercial products
- *Distinct ambiguity oracle-less:* low volume chips

# State of the art

## Evaluation metrics

| Metric | Description | Property |
|---|---|---|
| **Verification failure** | Measures how the obfuscated design introduces failing points with wrong keys | Related to functionality |
| **Entropy** | Measures the number of distinct outputs of the circuit | Related to power and resiliency towards oracle-less attacks |
| **Differential entropy** | Measures the proportion of bits that differ between the obfuscated and the plain design | Related to power overhead |
| **Reconvergence** | Measures the rate of internal signals converging in other nodes | Related to resiliency towards key sensitization attack |
| **Key structure metric** | Measures the structural interconnection between the key gates | Related to resiliency towards key sensitization attack |

# State of the art

## Pre-synthesis logic locking techniques

- TAO: HLS tool to produce obfuscated RTL descriptions
- ASSURE: pre-synthesis tool that works at RT level
- CDFG: RT level technique that obfuscates the data flow graph of a design
- BDD: pre-synthesis technique that works on Binary Decision Diagrams

## Post-synthesis logic locking techniques

- RLL: random insertion of logic gates (typically XOR or XNOR gates) controlled by a key bit
- SLL: strengthens the insertion of logic gates by inserting key-gates with complex interference among them
- Anti-SAT: technique that aims at making SAT attacks unfeasible
- Cone size: integrates the key gates with other gates that have the largest fanin or fanout cone or both

# State of the art

| | | Area overhead | Power overhead | Timing overhead | SAT attack resiliency | Key sens. attack resiliency | Verification failure metric | Entropy | Differential entropy | Reconvergence | Key structure metric |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Pre-synthesis | TAO [7] | High | n.a. | Low | n.a. | n.a. | n.a. | n.a. | High [a] | n.a. | n.a. |
| | ASSURE [6] | Low | n.a. | Low | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. |
| | CDFG [2] | Low | Low | n.a | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. | n.a. |
| | BDD Random [4] | High | High | Medium | Low | High | High | Low | Medium | Medium | High |
| | BDD AntiSAT [4, 12] | High | High | Medium | Medium | High | Low | Medium | Low | High | High |
| | BDD Entropy [1] | Medium | Medium | Low | Low | High | High | High | Medium | Low | High |
| Post-synthesis | RLL [8] | Low | Low | Low | Low | Low | High | Medium | High | Medium | Low |
| | SLL [13] | Low | Low | Low | Low | Medium | medium | Medium | High | Medium | Low |
| | Cone size [1] | Low | Low | Medium | Low | Medium | Low | Medium | High | Medium | Medium |
| | AntiSAT Random [8, 12] | Medium | Medium | Low | High | Low | High | Medium | High | Low | Medium |
| | AntiSAT SLL [13, 12] | Medium | Medium | Low | High | Medium | Medium | Medium | High | Low | Medium |
| | Anti SAT Cone size [1] | Medium | Medium | Medium | High | Medium | Low | Medium | High | Low | Medium |

# State of the art - Summary

| Category | Techniques | Pros | Cons |
|---|---|---|---|
| Pre-synthesis HLS | TAO, BDD | Hide semantic information | Require modification of the design flow |
| Pre-synthesis RTL | ASSURE, CDFG | Hide semantic information<br>Do not require modifications on the design flow | ? |
| Post-synthesis | RLL, SLL, Cone Size, Anti SAT | Do not require modifications on the design flow | Cannot protect information already embedded in the design by synthesis optimizations |

# State of the art

## Conclusion

- ASSURE and CDFG showed that logic locking at register-transfer level deserves further investigations
- The proposed metrics are empiric and experimental and do not allow their use with optimization methods
- Hardware obfuscation is missing security properties clearly defined by mathematical terms

## Open questions

- How to select obfuscation points?
- How to measure the security and compare two designs?

# Outline

- Introduction to the problem
  - Globalization of the IC supply chain & security threats
  - Logic locking
- Research goal
- State of the art
- **Research plan**

# Research plan

## Research goal

develop a complete logic locking framework
at register-transfer level

and

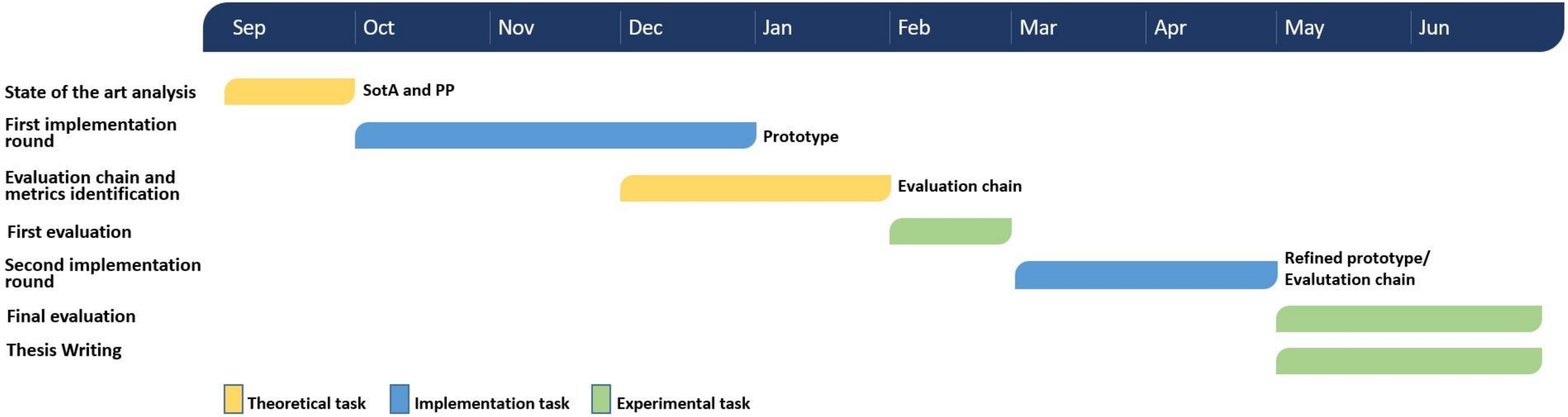
evaluate it with new security metrics

# Research plan

We plan to carry out this research with a **two-phase development plan**

- **First development round:** prototype implementing the RTL obfuscation techniques and evaluation chain to measure cost and security
- **First evaluation round:** benchmarking the prototype using the evaluation chain
- **Second development round and final evaluation:** refining the techniques and the metrics identified in the first phase thanks to the evaluation feedback

# Research plan



# Thank you for your attention!

*Luca Collini*

luca.collini@mail.polimi.it