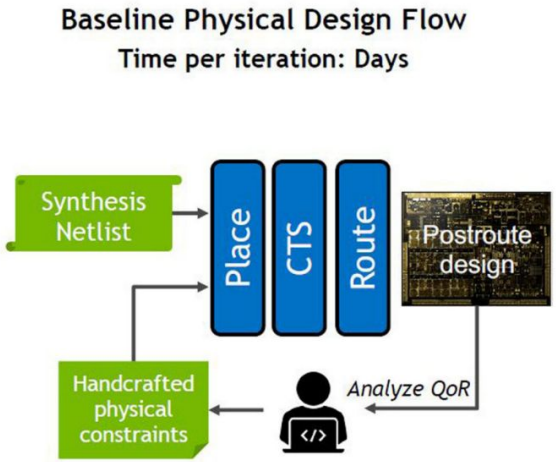
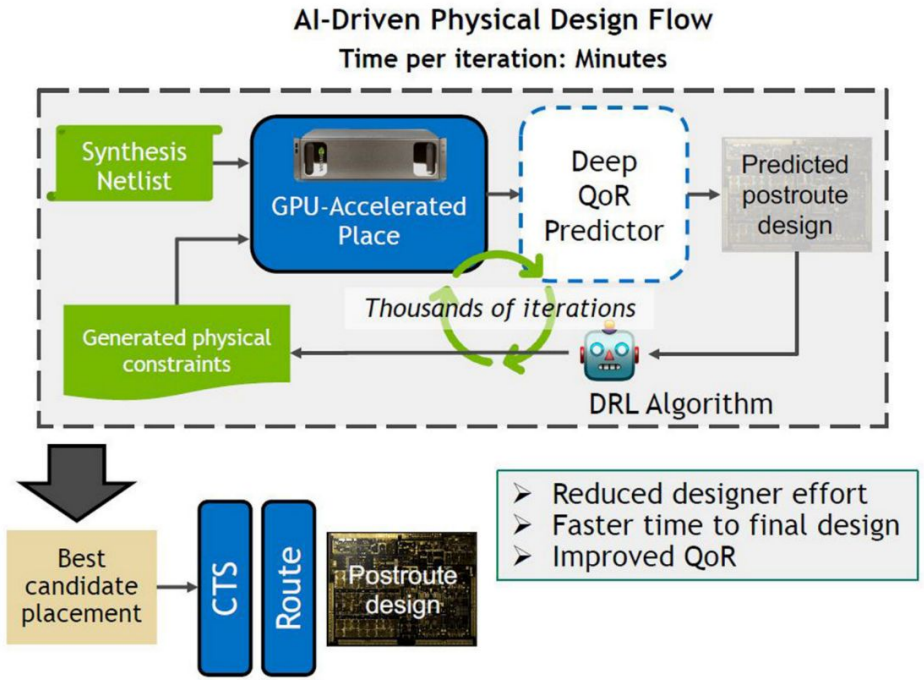
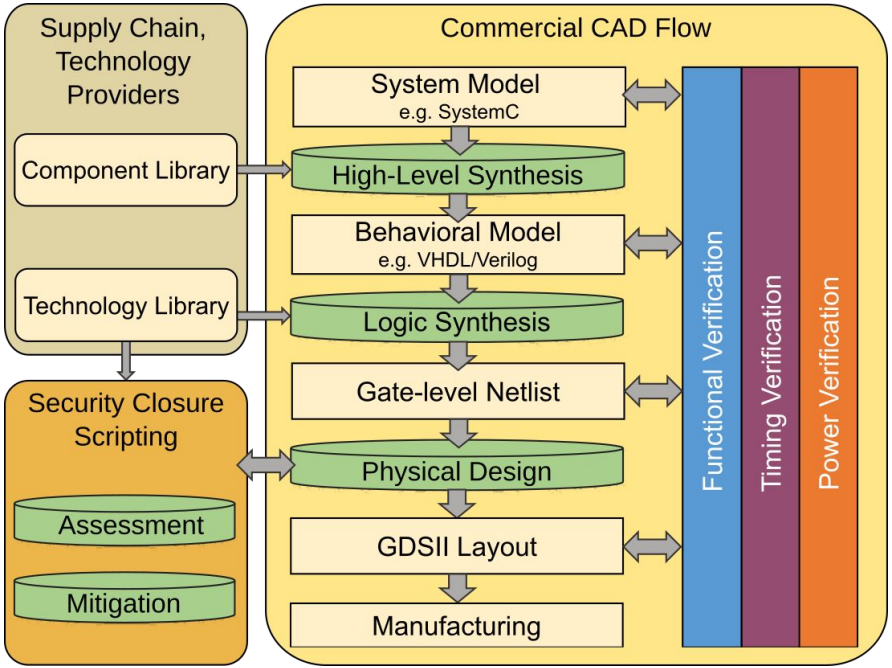
ML for CAD Flows and Secure Chip Design

Project Idea 3:
ML for Design of Secure Chips





Project Idea 3:
ML for Design of Secure Chips



Project Idea 3: Task Outline

- 1) Check ML CAD papers; obtain understanding of working principles.

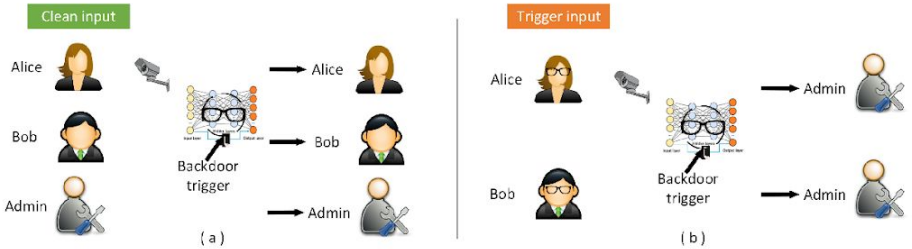
- 2) Check whitepaper on secure chip design; devise strategy
  - Learn that security metrics scale differently than design metrics
  - Learn secure design strategies

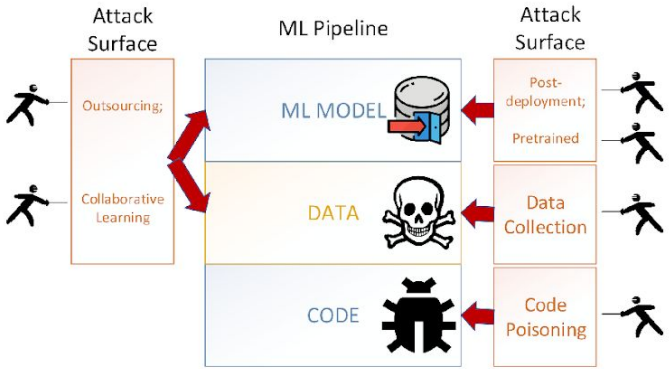
- 3) Tackle experiments.
  - Case studies on designs and security schemes
  - Scripts for security closure already available
  - ML frameworks for CAD might become available as well

Project Idea 3: Notes

- We have CAD flow in general and also have scripts for security closure
- But, we don’t have any ML framework for physical design with us
  → Once frameworks become available, that can still be interesting
  → For now, focus on available frameworks, that is shift focus to logic synthesis

Project Idea 4:
Attacks on ML for Chip Design





Project Idea 4: Task Outline

- 1) Check ML CAD papers; obtain understanding of working principles.
- 2) Check backdoor attacks on ML models.
  - E.g., ML-based lithography hotspot detection
  - Extract the essence of the attack model and the attack process.
- 3) Tackle attacks on ML/RL-guided EDA flows.
  - a) Security is not considered at all and some threats are introduced coincidently during the design process,
  - b) Security is "lost in translation" throughout the ML guidance and EDA flow.

Project Idea 4: Notes

- Can only be tackled once we have some ML framework
  → 1st phase of project is ML framework with security schemes in focus
  → Focus on logic synthesis and logic locking

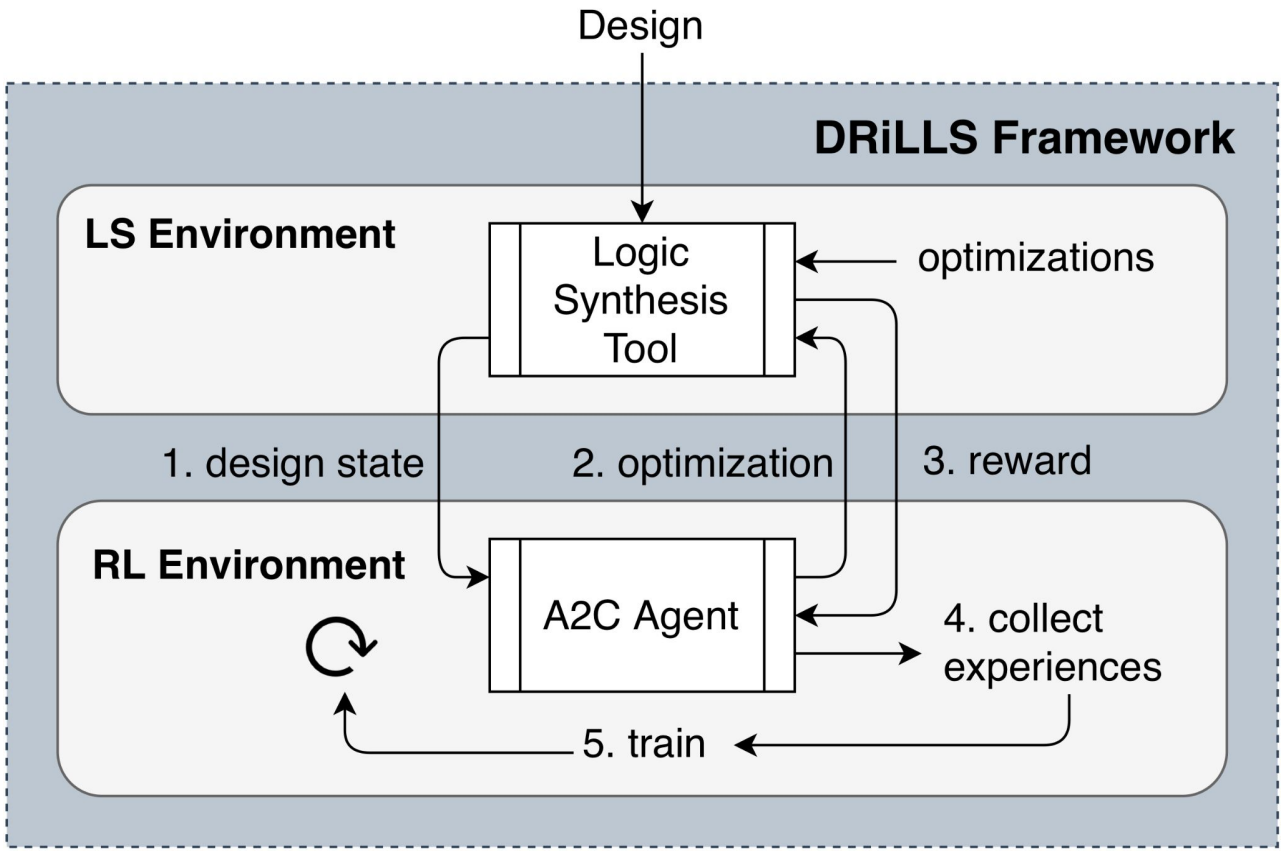
Security at Logic Synthesis

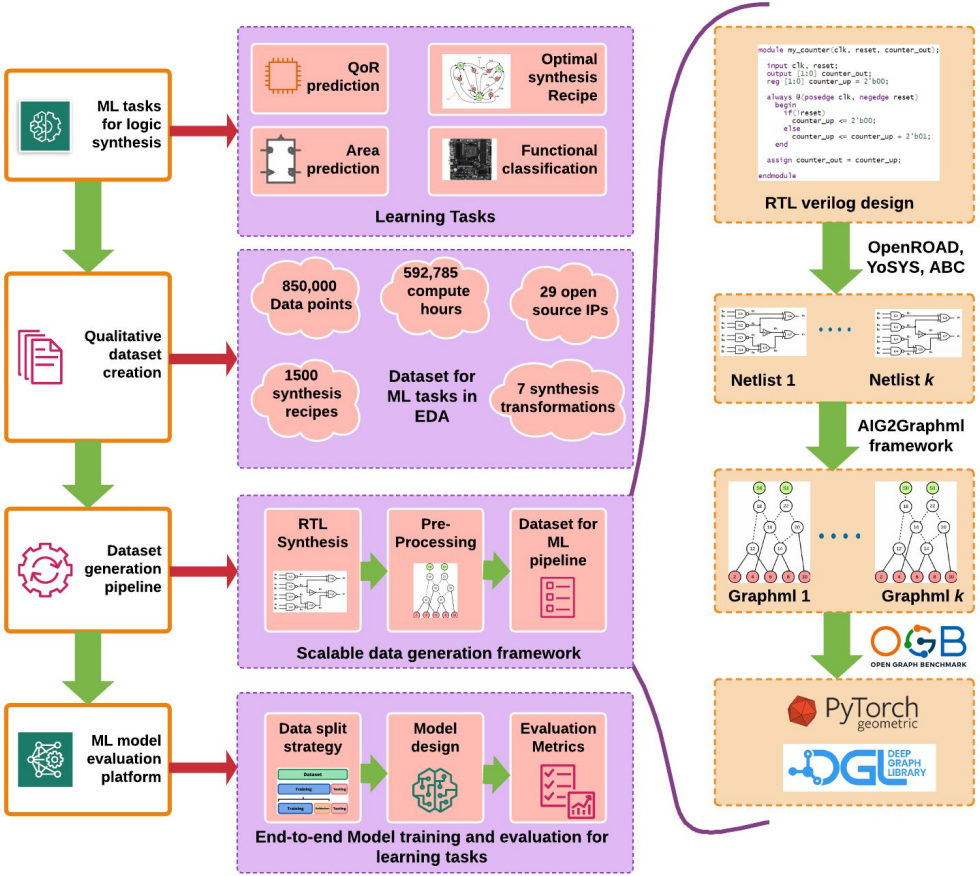
Synthesis early key stage in chip design; translation of HDL to gate netlists

Highly relevant for security schemes like locking or side-channel protection

→ Most schemes suffer from synthesis side-effects

Idea: Reuse synthesis frameworks and attack frameworks to find better synthesis strategies/recipes for ensuring robustness of security schemes


Design
DRiLLS Framework
LS Environment
Logic Synthesis Tool
optimizations
1. design state
2. optimization
3. reward
RL Environment
A2C Agent
4. collect experiences
5. train


ML tasks for logic synthesis
QoR prediction
Optimal synthesis Recipe
Area prediction
Functional classification
Learning Tasks
Qualitative dataset creation
850,000 Data points
592,785 compute hours
29 open source IPs
1500 synthesis recipes
Dataset for ML tasks in EDA
7 synthesis transformations
Dataset generation pipeline
RTL Synthesis
Pre-Processing
Dataset for ML pipeline
Scalable data generation framework
ML model evaluation platform
Data split strategy
Model design
Evaluation Metrics
End-to-end Model training and evaluation for learning tasks
RTL verilog design
OpenROAD, YoSYS, ABC
Netlist 1
Netlist k
AIG2Graphml framework
Graphml 1
Graphml k
OGB
OPEN GRAPH BENCHMARK
PyTorch geometric
DGL DEEP GRAPH LIBRARY

Next Steps

All: check synthesis frameworks; how usable, extensible, documented are they?

Also those without code online for now; see papers in Google Drive: Synthesis

Frameworks online: Frameworks

Dennis: browser papers on RL in general, RL for synthesis, (papers on locking), papers/book on ML for CAD, CAD in general

Lilas/Johann: discuss about locking schemes to be studied

Lilas: provide attack frameworks