SaTC: STARSS: Small: Analysis of Security and Countermeasures for Split Manufacturing of Integrated Circuits
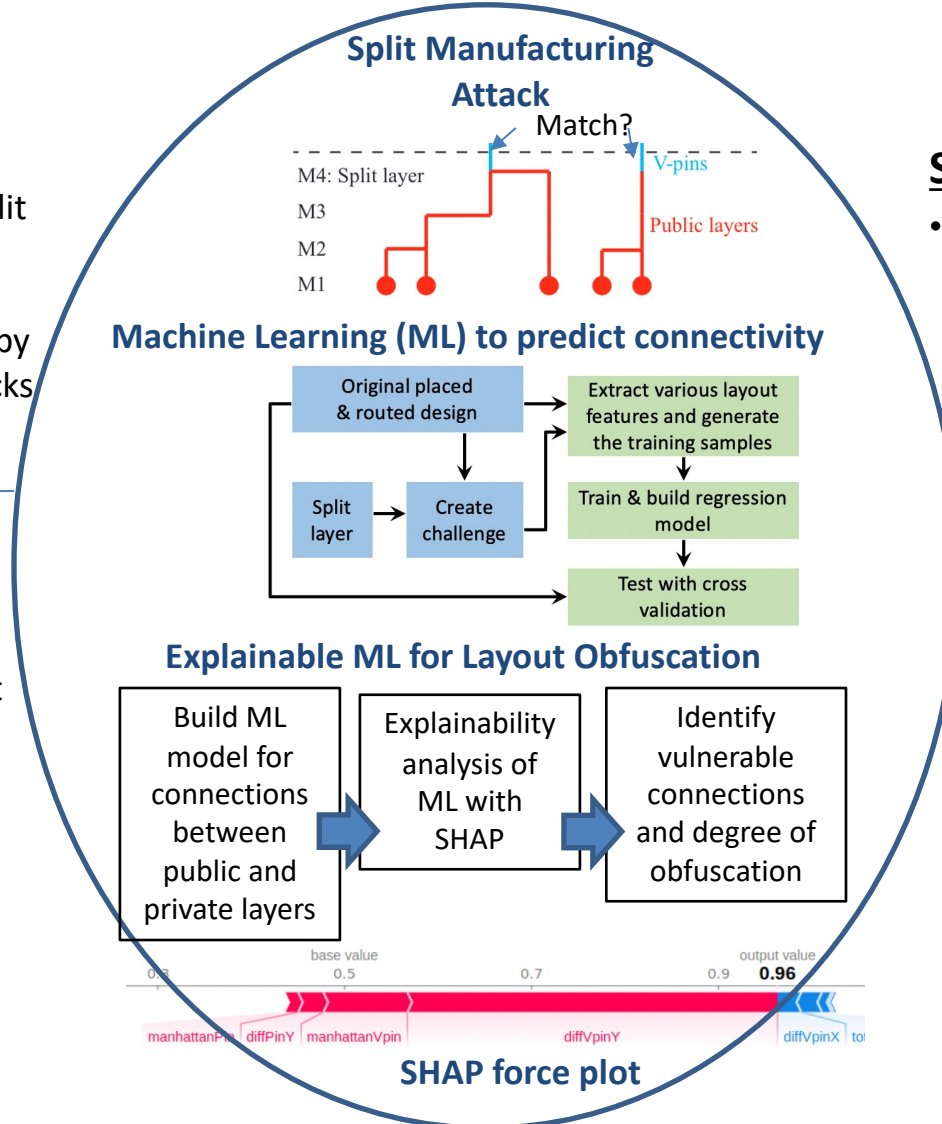
Challenge:

- Enhance security of split manufacturing of Integrated Circuits for industry-scale layouts by building effective attacks and obfuscators

Solution:

- Utilize ML to analyze split manufacturing attack and build layout obfuscators
- Extend the attack model to oracle reconstruction with minimal I/O patterns

Split Manufacturing Attack

Match?

M4: Split layer
M3
M2
M1

V-pins

Public layers

Machine Learning (ML) to predict connectivity

Original placed & routed design

Split layer → Create challenge

Extract various layout features and generate the training samples

Train & build regression model

Test with cross validation

Explainable ML for Layout Obfuscation

Build ML model for connections between public and private layers → Explainability analysis of ML with SHAP → Identify vulnerable connections and degree of obfuscation

base value
0.5
0.7
0.9
output value **0.96**

manhattanPin diffPinY manhattanVpin diffVpinY diffVpinX tot

SHAP force plot

Scientific Impact:

- Demonstrated effective utilization of machine learning and its explainability for hardware security

Broader Impact and Broader Participation:

- Collaborated with industry mentor from IBM
- Publicly released program for challenge/response creation for split manufacturing research adapted from large ISPD'11 benchmarks
- Funds partially supported one female PhD student