Defining the Level of Hardware Obfuscation using Machine Learning Techniques

Nikitha Rao B S, Xiang Lin, R. D. (Shawn) Blanton

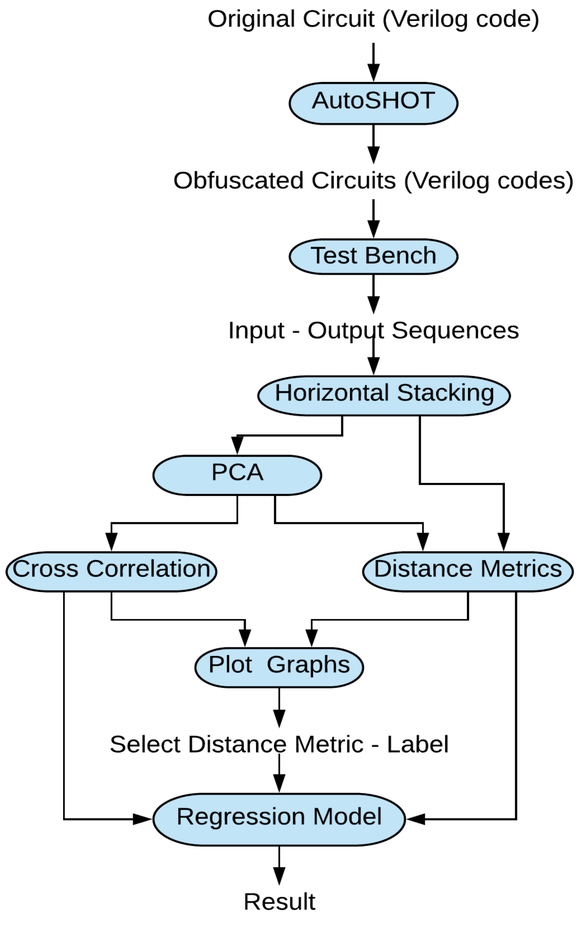
ACTL CARNEGIE MELLON ADVANCED CHIP TEST LABORATORY

Carnegie Mellon University
Electrical & Computer ENGINEERING

Motivation

- **The Problem:** Reverse Engineering of IC.
  Why?
  - IP infringement
  - Intellectual Property Theft
  - Counterfeit Products
- **A Solution:** Hardware Obfuscation
  - Data Flow
  - Control Flow
- **This Work:** Quantify the level of control flow obfuscation
  - Given the original circuit and the obfuscated circuit.
  - Return a distance metric representing the level of obfuscation.

Approach

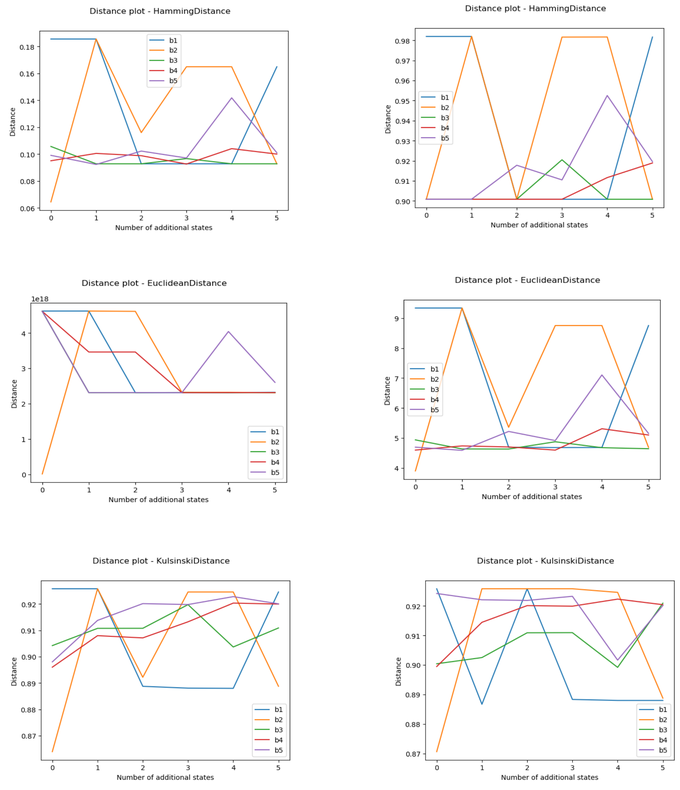


Distance Metrics

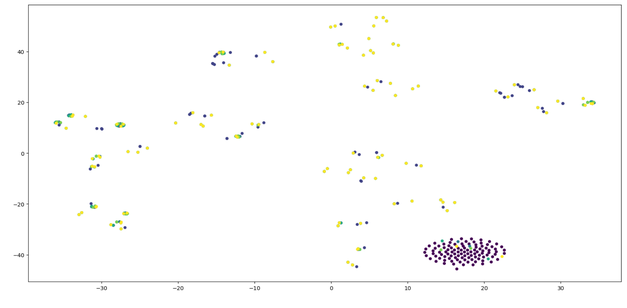
Bit wise values		Place values	
Jaccard	Rogerstanimoto	Euclidean	Chebyshev
Matching	Russellrao	Manhattan	Canberra
Dice	Sokalmichener	Hamming	Braycurtis
Kulsinski	Sokalsneath	Minkowski	

Distances for raw data (input output sequences).

Distances for PCA transformed data.



Where b is the number of obfuscated bits.



Distribution of t-SNE transformed features for original (black) and obfuscated (colored) designs.

Regression Models Comparison

Decision Tree	• MSE: 0.008434881 • Normalised MSE: 0.402434771
Random Forest	• MSE: 0.008082928 • Normalised MSE: 0.385642849
Extra Trees	• MSE: 0.008434864 • Normalised MSE: 0.402433964
Gradient Boosting	• MSE: 0.009454689 • Normalised MSE: 0.451090645
SGD	• MSE: 55557.246338 • Normalised MSE: 2650679.68
Bayesian Ridge	• MSE: 0.011162687 • Normalised MSE: 0.532580563

Conclusion

- Some distance metrics (e.g., Hamming, Euclidean, Manhattan, Chebyshev, Minkowski) show decreasing distances from the raw data as the obfuscation effort is increased, which contradicts our expectations. However, they behave as expected (increased distance as obfuscation effort increases) in the PCA transformed data.
- Other distance metrics like Kulsinski, on the other hand, exhibit trends that match our expectations on both raw and PCA transformed data.
- In some cases, the same distance (and implicitly level of obfuscation) was obtained in circuits at lower obfuscation effort and cost.

Future work

- Incorporate multiple circuit designs to get relative distances from each other.
- Implement the distance metric prediction model real time.