SaTC: STARSS: Small: Analysis of Security of Split Manufacturing Using Machine Learning

Azadeh Davoodi
Department of Electrical and Computer Engineering
University of Wisconsin - Madison

Background

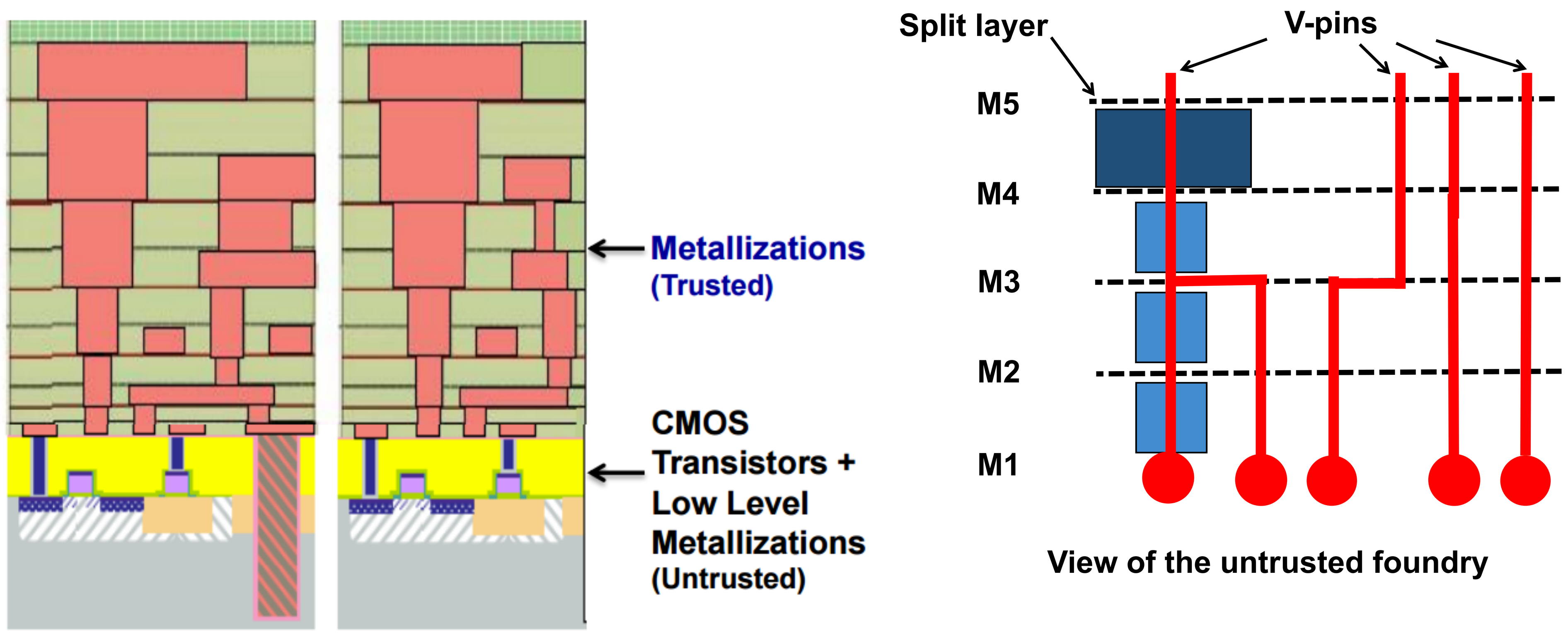


Image Source: https://www.iarpa.gov/images/files/programs/tic/08-TIC_final.pdf

Motivation:
Avoids disclosing complete wiring information of a design.

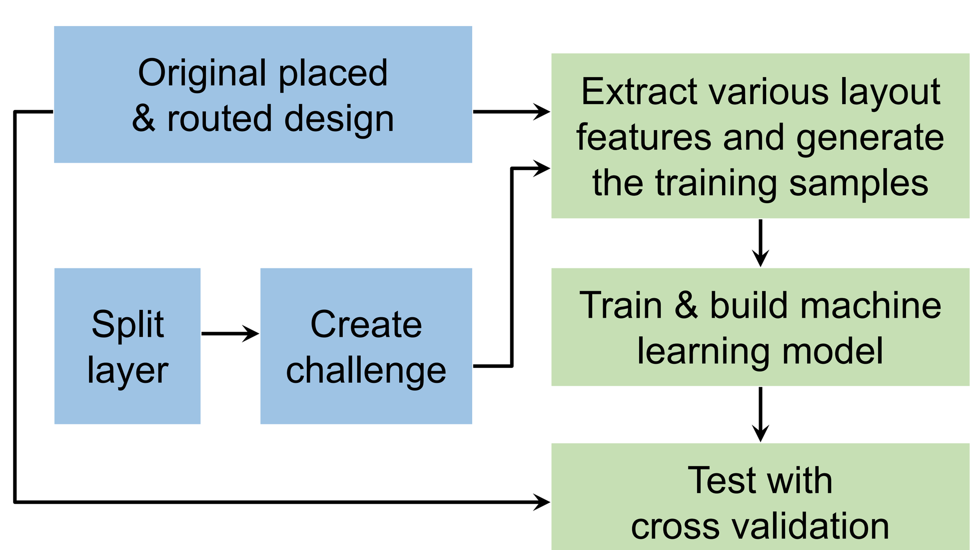
Attack Model:
Given FEOL and the split layer (top layer of FEOL), try to guess connections in BEOL.

Proximity Attack (PA):
Generate a list of candidate "v-pins" for each broken wire and pick the closest candidate on split layer as the match.

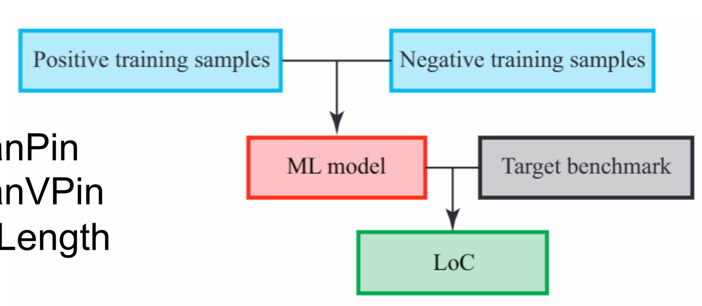
Performance Metrics

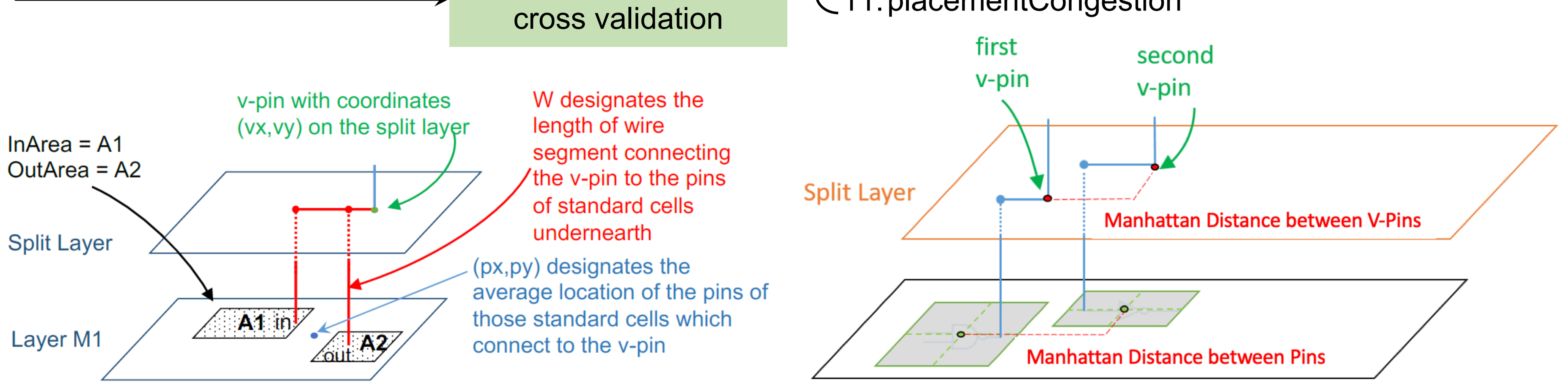
- **|LoC|**: Size of List of Candidates (LoC) for each broken wire.
- **Accuracy**: Likelihood that LoC contains the actual match.
- **%PA**: Likelihood of picking the correct match from LoC, currently done by PA.

Machine Learning Workflow



1. diffVpinX
2. diffVpinY
3. diffPinX
4. diffPinY
5. manhattanPin
6. manhattanVPin
7. totalWireLength
8. totalArea
9. diffArea
10. routingCongestion
11. placementCongestion





Challenges

Poor scalability when moving to lower layers
e.g., the average number of v-pins for split layers 8, 6, 4, are 11K, 59K, and 160K, respectively

Challenges include:
1. Poor runtime for both testing ($O(n^2)$) and training ($O(n)$).
2. Degradation in quality of results, i.e., classification accuracy
3. Larger size of LoC (many more potential candidates are identified for each v-pin)

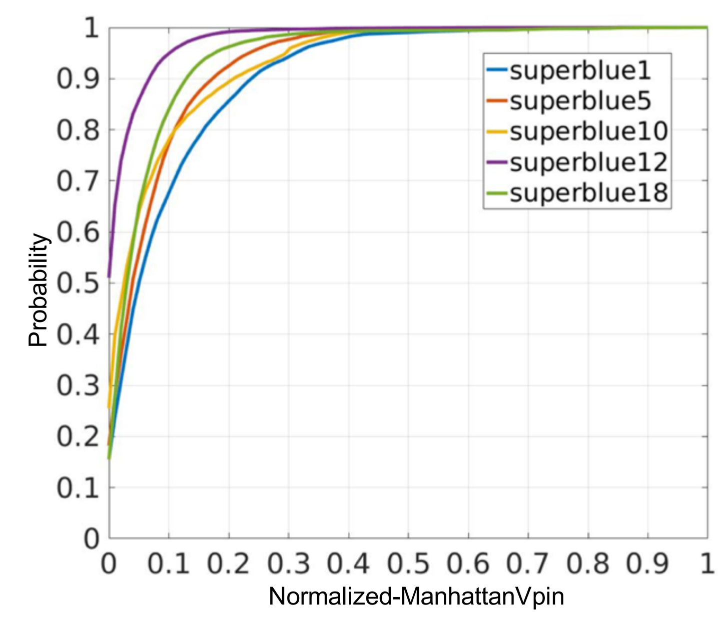
Our Contributions

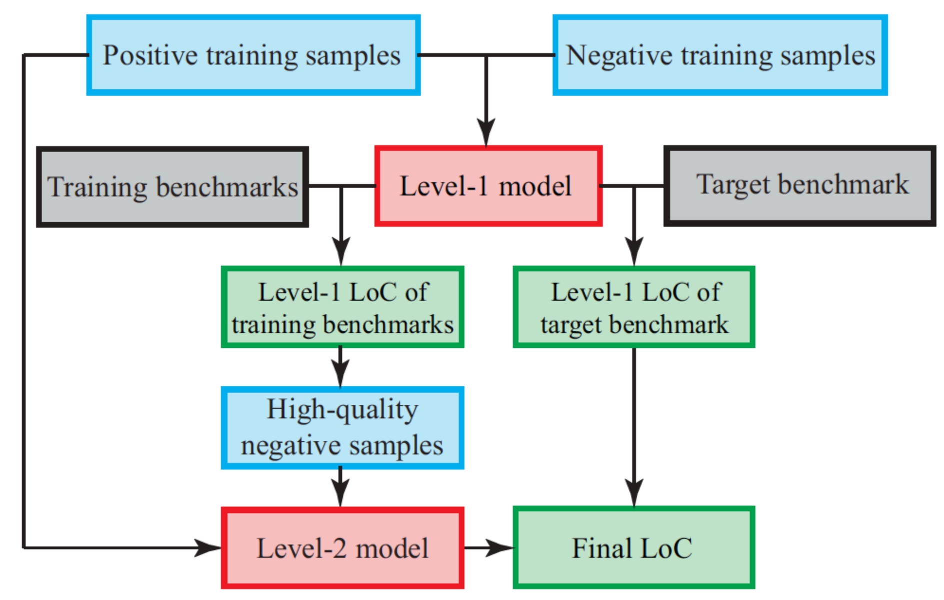
- We study the ranking of features in general. Each feature is measured in several metrics signifying its importance.
- We propose novel ways to make the training and testing scalable, including
  1) Addressing poor runtime scalability,
  2) Addressing degradation in classification accuracy,
  3) Controlling the size of LoC.
- Significant runtime improvement without sacrifice in the quality of attacks.
- Improvement on classification accuracy & PA performance compared to prior works.

Proposed Techniques

1. Addressing runtime scalability

Key idea: Most v-pin pairs can be easily classified as not connected simply because they are **far apart**.
Approach: Avoid these v-pin pairs both during training and testing, by only examining pairs near each other (thresholds determined by observing the distribution of Manhattan distances).





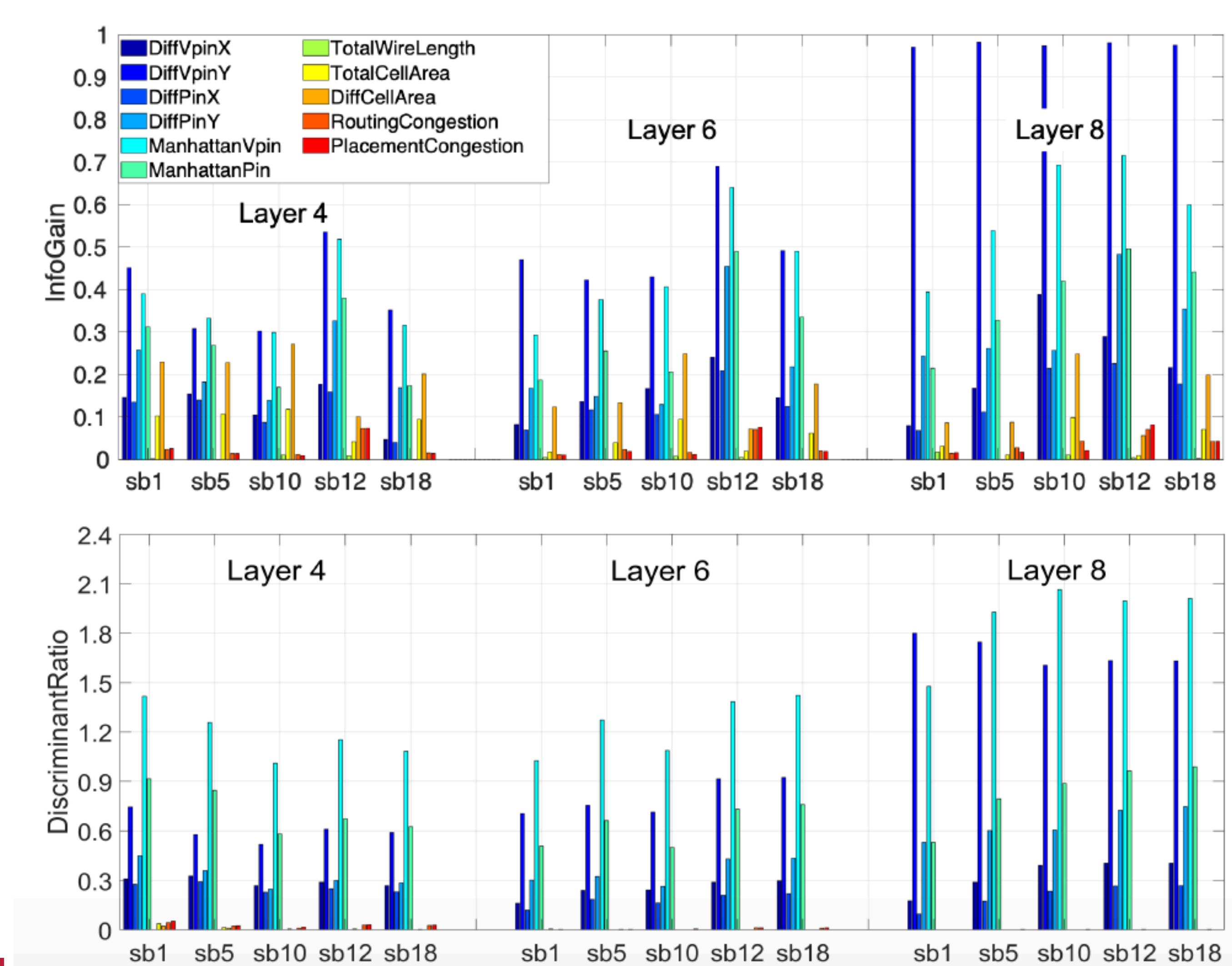
2. Addressing degradation in classification accuracy

Key idea: Quality of negative samples (unmatched v-pins) is the most important factor in accurate classification.
Approach: Treat the unmatched v-pins in LoC (false alarms) as "high quality" negative samples. Train a L2 model on top of L1 results and perform L2 classifications for v-pins in the L1 LoC.

3. Controlling the LoC size

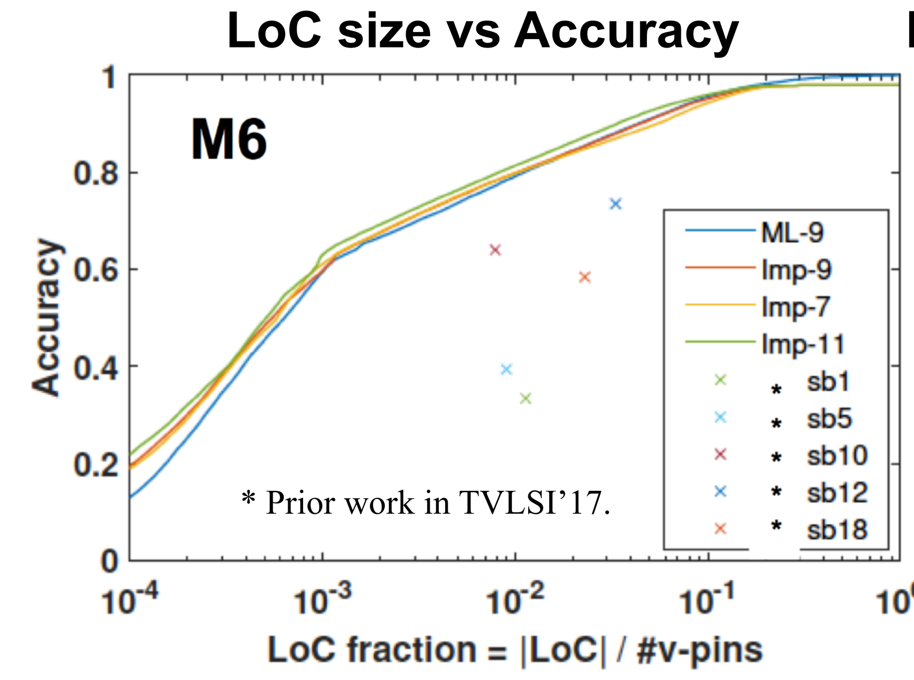
Key idea: **1)** Explore the tradeoff between LoC size vs. classification accuracy without retraining the model. **2)** Better comparison among different models.
Approach: Vary the threshold of classification during the testing phase to generate a tradeoff curve between LoC size and accuracy. Use cross validation to determine the proper LoC size for PA.

Experiments Results



Feature Ranking:
1. **V-pin locations** (e.g. DiffVpin, ManhattanVpin)
2. **Pin locations** (e.g. DiffPin, ManhattanPin)
3. **Other features**

LoC size vs Accuracy



Improvement on Runtime Scalability

Split layer	Design	DAC'18 (ML-9) |LoC|	DAC'18 (ML-9) Acc.	Imp-7 |LoC|	Imp-7 Acc.
Layer 8	superblue1	16.2	100.00%	15.2	99.85%
	superblue5	27.3	100.00%	27.2	99.60%
	superblue10	21.2	100.00%	19.4	100.00%
	superblue12	44.9	100.00%	48.0	99.75%
	superblue18	23.4	99.92%	23.3	99.87%
	Avg	26.6	99.97%	26.6	99.81%
	Runtime		8.48 min		0.48 min
Layer 6	superblue1	1712.0	83.12%	555.1	74.64%
	superblue5	1775.2	88.71%	645.6	77.79%
	superblue10	2300.8	92.65%	759.4	82.30%
	superblue12	8383.4	97.25%	2955.2	89.72%
	superblue18	2678.7	92.78%	716.8	84.08%
	Avg	3370.0	90.90%	1126.4	81.71%
	Runtime		21.65 hrs		0.42 hrs

Improvement by Two-level Pruning

Split layer	Design	Two-level pruning |LoC|	Two-level pruning Acc.	No pruning |LoC|	No pruning Acc.
Layer 8	superblue1	**3.15**	**40.95%**	5.31	22.68%
	superblue5	**4.33**	**57.51%**	6.92	39.82%
	superblue10	**4.54**	**79.87%**	7.91	66.54%
	superblue12	8.73	38.49%	**5.40**	**60.01%**
	superblue18	**5.46**	**67.86%**	7.20	53.40%
	Avg	**5.24**	**56.94%**	6.55	48.49%
	Runtime		111.7 sec		27.8 sec

Default thresholds for LoC, with Imp-11 model.

Improvement on PA Performance

Design	%PA from Cross Validation ML-9	Imp-9	Imp-7	Imp-11
Split layer 8				
sb1	15.21%	14.84%	13.03%	11.05%
sb5	20.04%	21.22%	21.35%	21.69%
sb10	42.97%	59.54%	57.78%	42.30%
sb12	10.96%	15.03%	13.84%	11.53%
sb18	13.41%	17.56%	18.43%	17.85%
Avg	20.52%	25.64%	24.89%	20.88%
Time	91.4 sec	101.8 sec	59.0 sec	60.0 sec

Prior work in TVLSI'17: 1.95% (sb1).