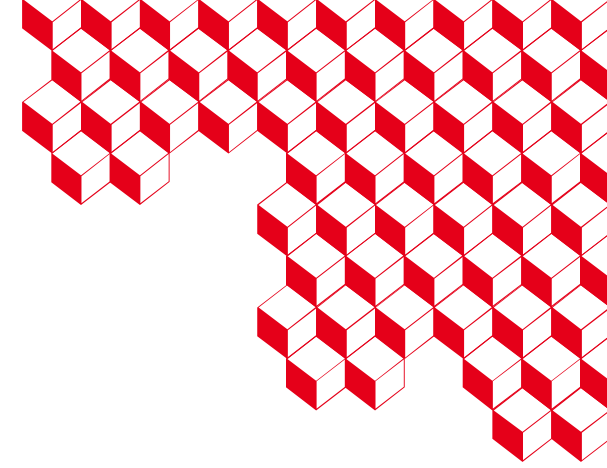




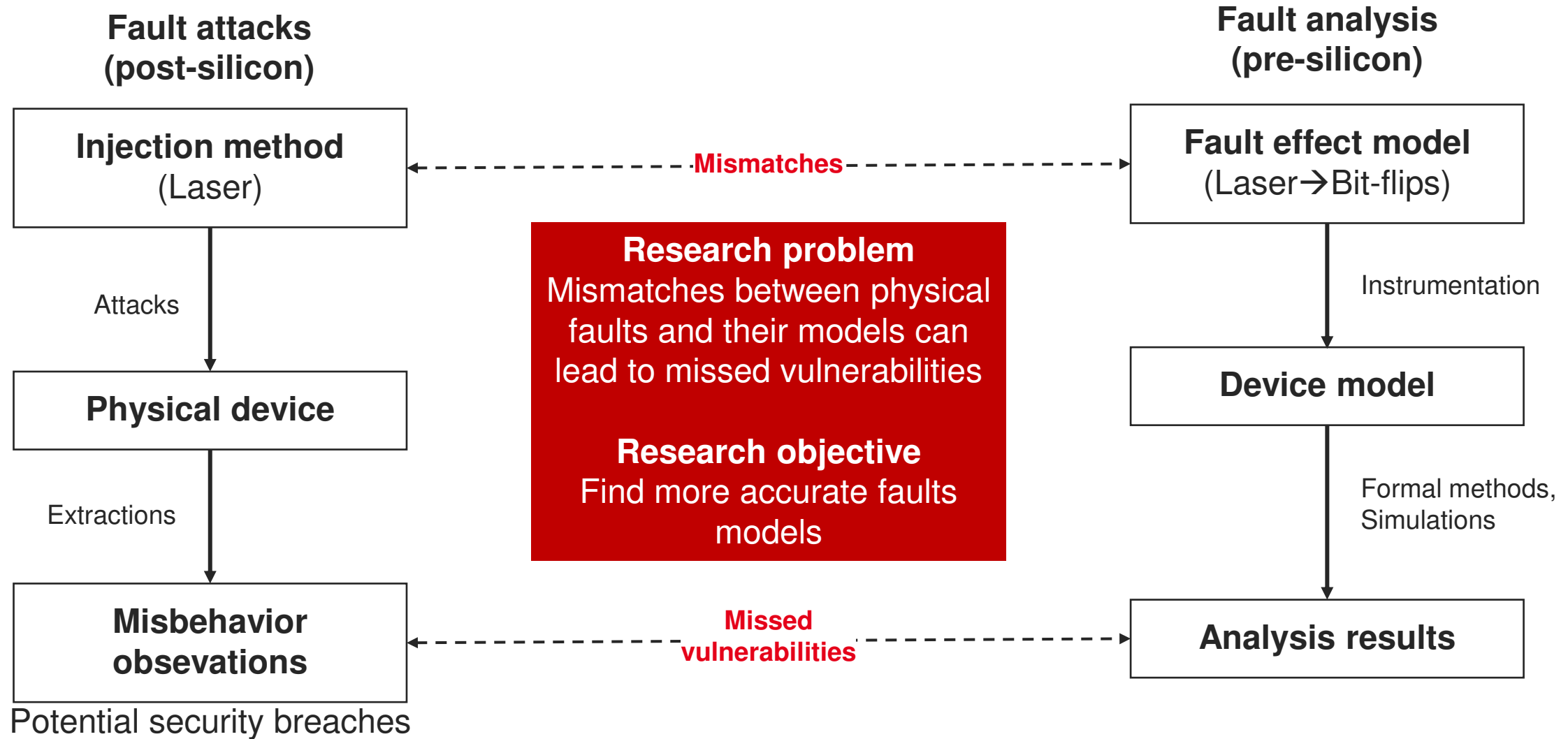
Synthèse de programmes de caractérisation à partir du RTL pour l'injection de fautes

Jonah Alle Monne (CEA), Guillaume Bouffard (ANSSI), Damien Couroussé (CEA), Mathieu Jan (CEA)

JAIF 2026 Presentation



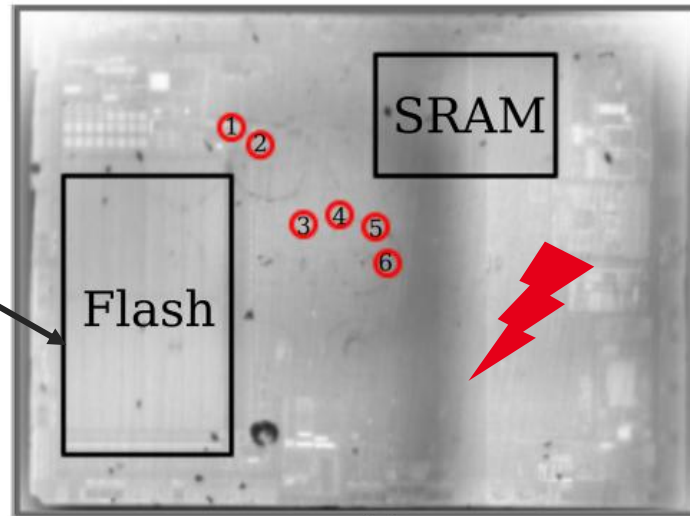
Attack vs analysis



Characterization tests

Objective: Find representative faults models (fault effect, fault location, fault time)

```
i1: add r0, r0, 0x1
i2: add r0, r0, 0x2
i3: add r0, r0, 0x3
i4: add r0, r0, 0x4
i5: add r1, r1, 0x1
i6: add r2, r2, 0x1
i7: add r3, r3, 0x1
i8: add r4, r4, 0x1
i9: add r0, r0, 0x5
i10: add r0, r0, 0x6
i11: add r0, r0, 0x7
i12: add r0, r0, 0x8
```



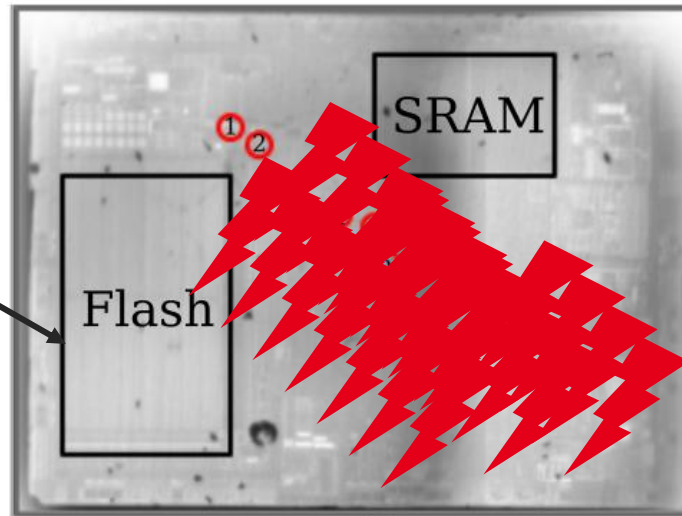
Extracted from [khuat, 2021]

- Run a **characterization program** on the target
- Randomly **inject faults**
- Observe** the register file output
CRASH
NO FAULT MANIFESTATION
FAULT MANIFESTATION
- Infer a **fault model** associated to each **fault manifestation** with educated guess

Problem: several **faults models** can lead to the same **fault manifestation**

Characterization tests

```
i1:  add r0, r0, 0x1
i2:  add r0, r0, 0x2
i3:  add r0, r0, 0x3
i4:  add r0, r0, 0x4
i5:  add r1, r1, 0x1
i6:  add r2, r2, 0x1
i7:  add r3, r3, 0x1
i8:  add r4, r4, 0x1
i9:  add r0, r0, 0x5
i10: add r0, r0, 0x6
i11: add r0, r0, 0x7
i12: add r0, r0, 0x8
```



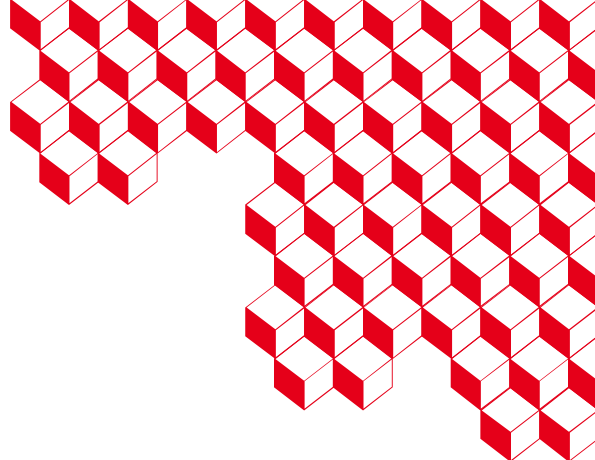
Extracted from [khuat, 2021]

If fault effect equivalent to skip of i6
(r2 not updated):

=> **24 models candidates** can explain
the fault manifestation (RISC-V
equivalent program on CV32E40P)

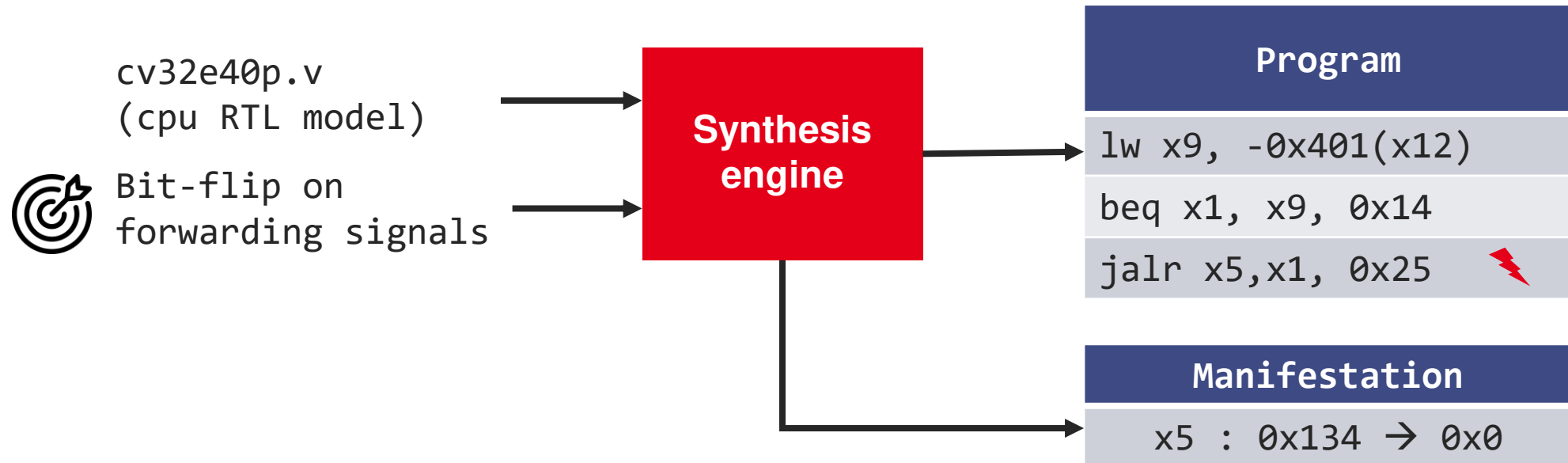
Why?

- Current approaches programs are handwritten
→ small set of programs to characterize a full CPU

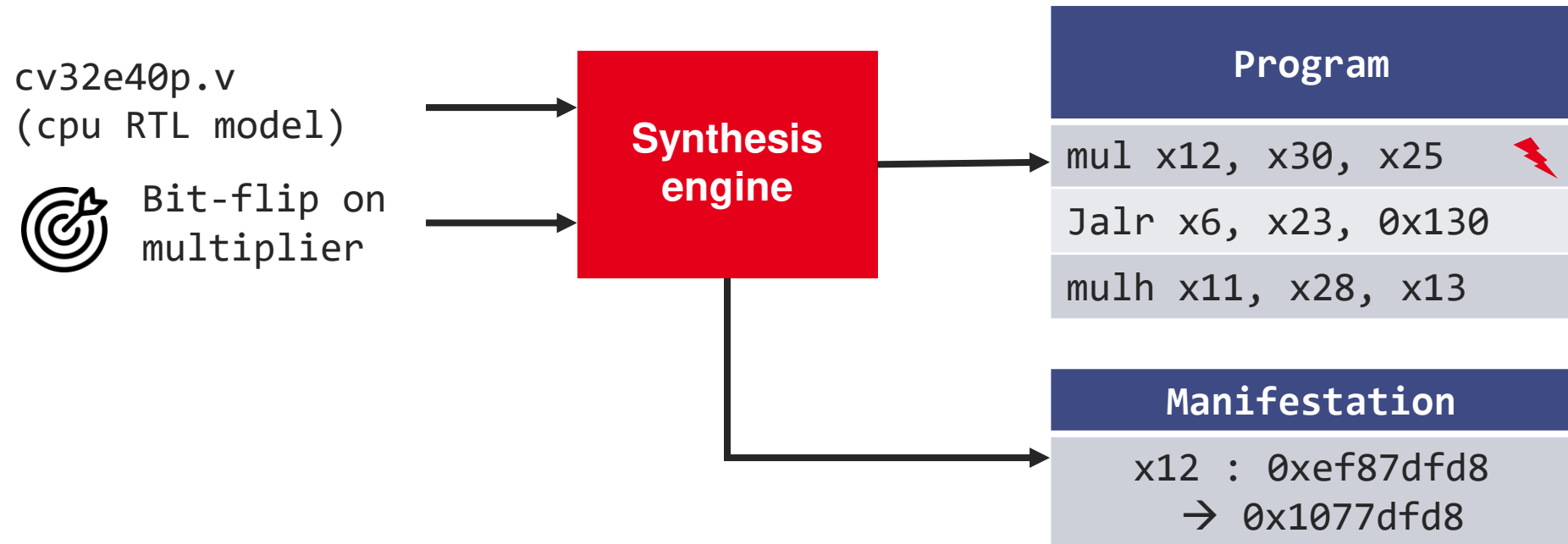


**“ How could we automate
characterization programs
creation and evaluate
their discrimination?”**

Proposal: Program synthesis using model checking



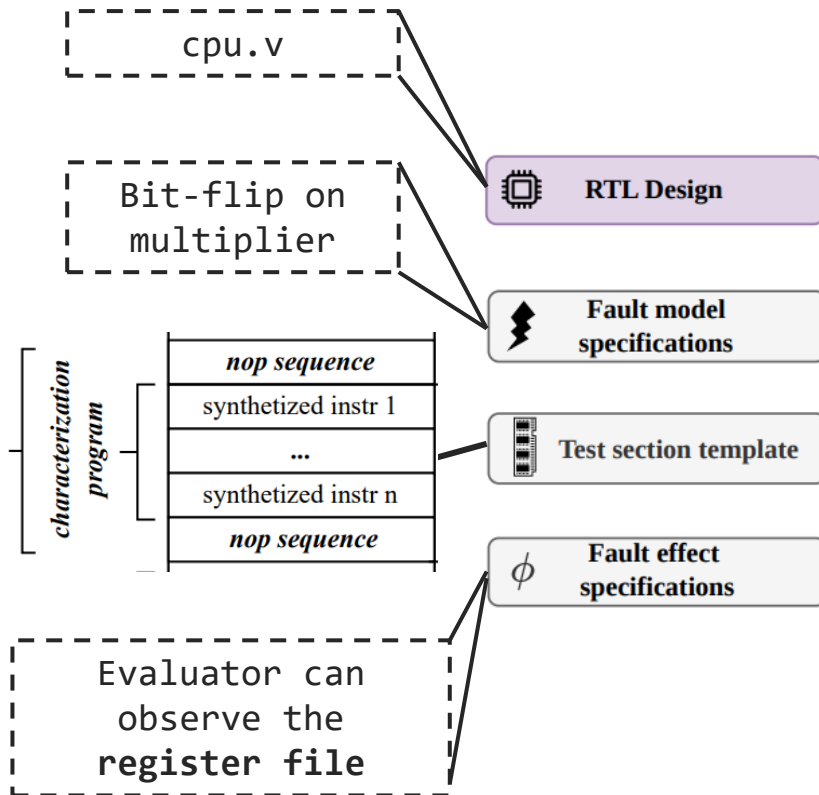
Proposal: Program synthesis using model checking



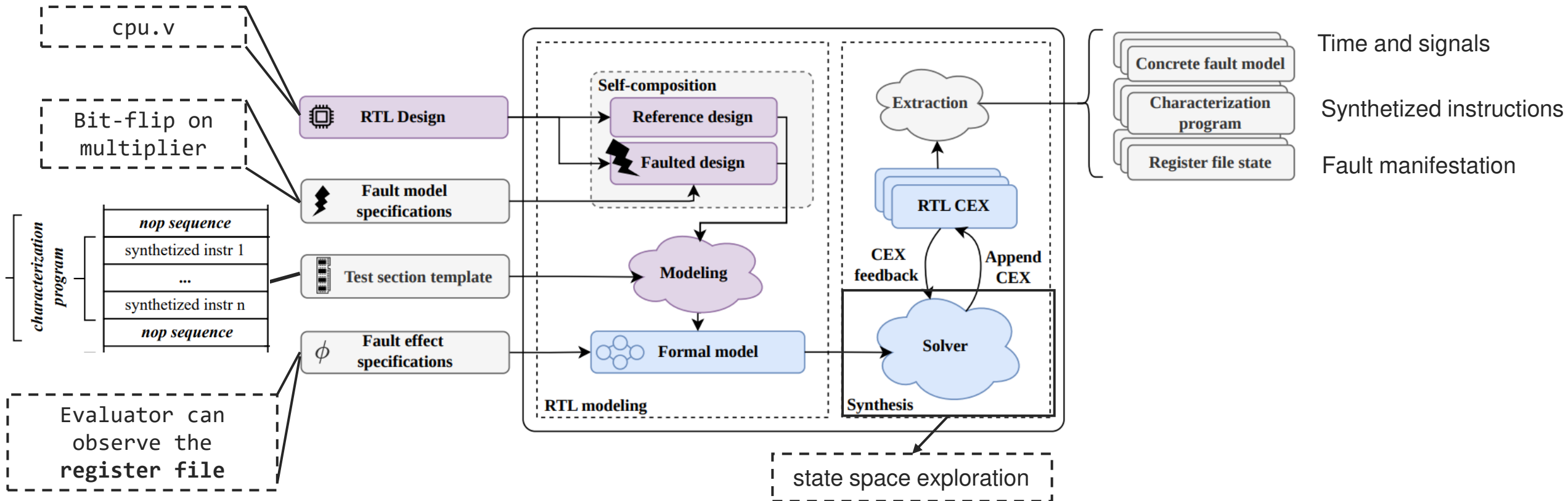


■ Methodology

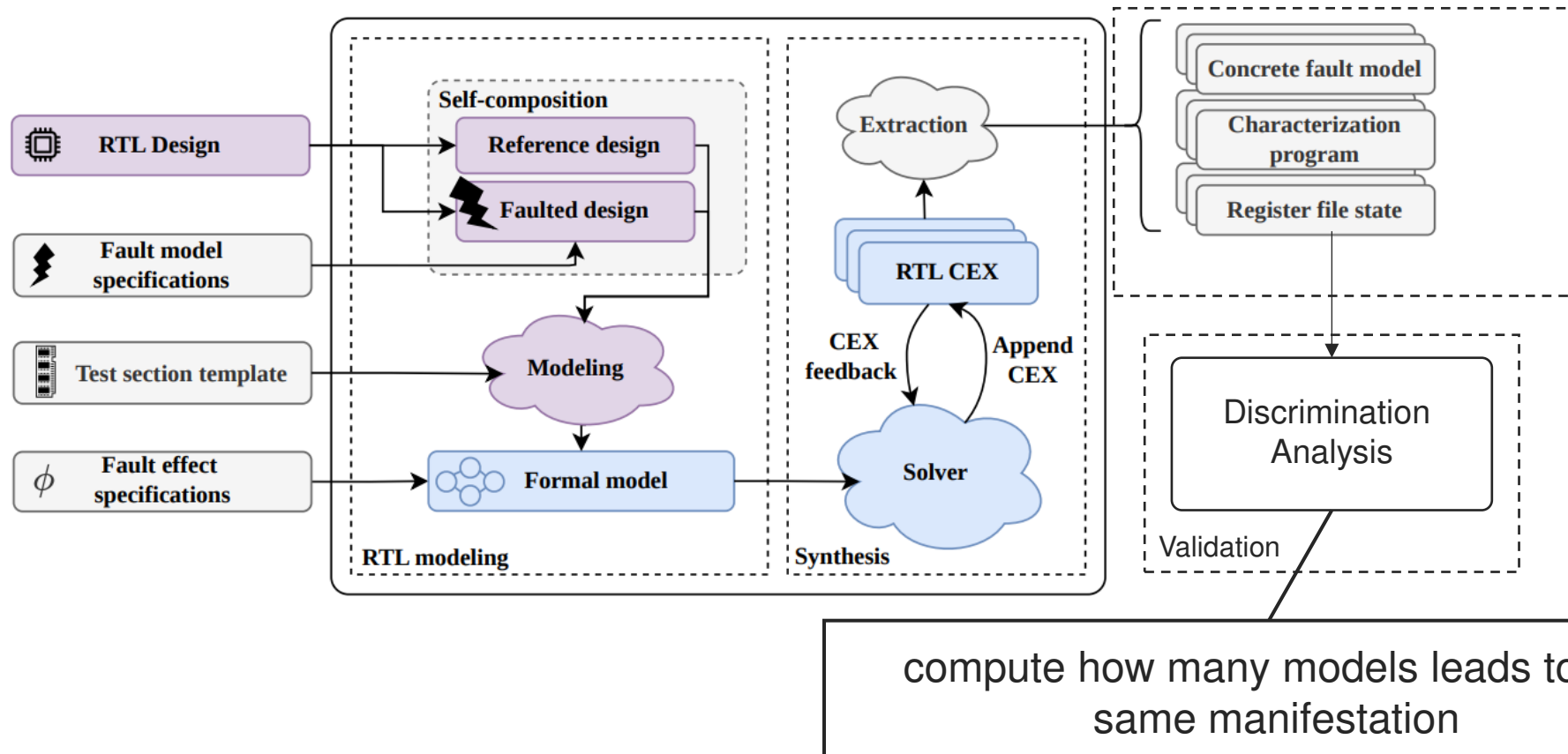
Methodology: RTL Modeling



Methodology: Synthesis



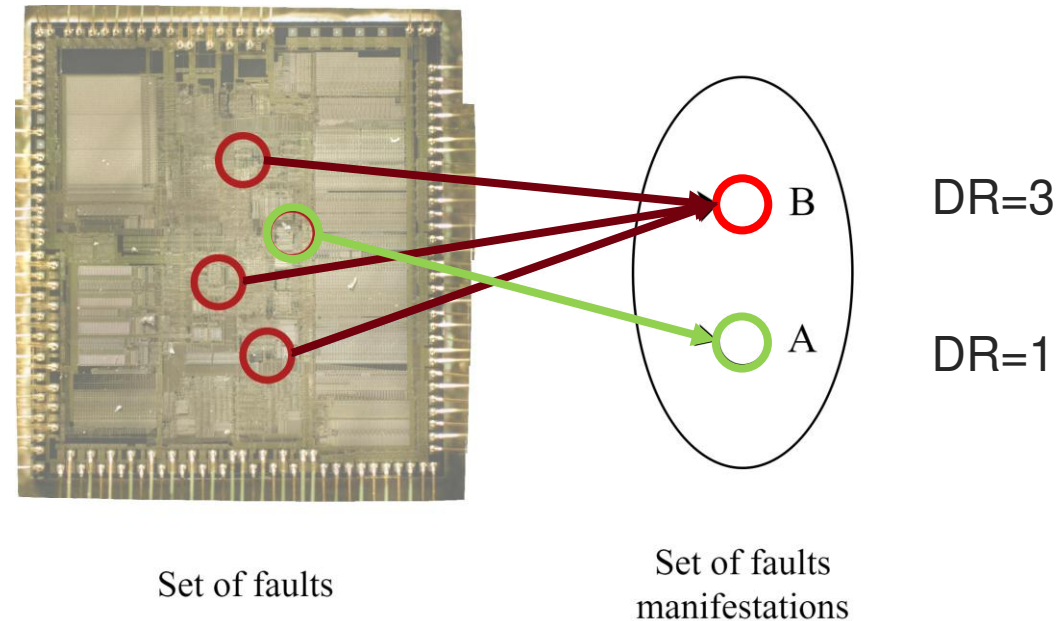
Methodology



Discrimination analysis

Discrimination: ability of a test to explain faults relying on their manifestation

Discrimination Rate (DR): number of fault models leading to a fault manifestation



➔ **Objective: Ideally $DR = 1$**



■ Validation

Validation: experimental setup

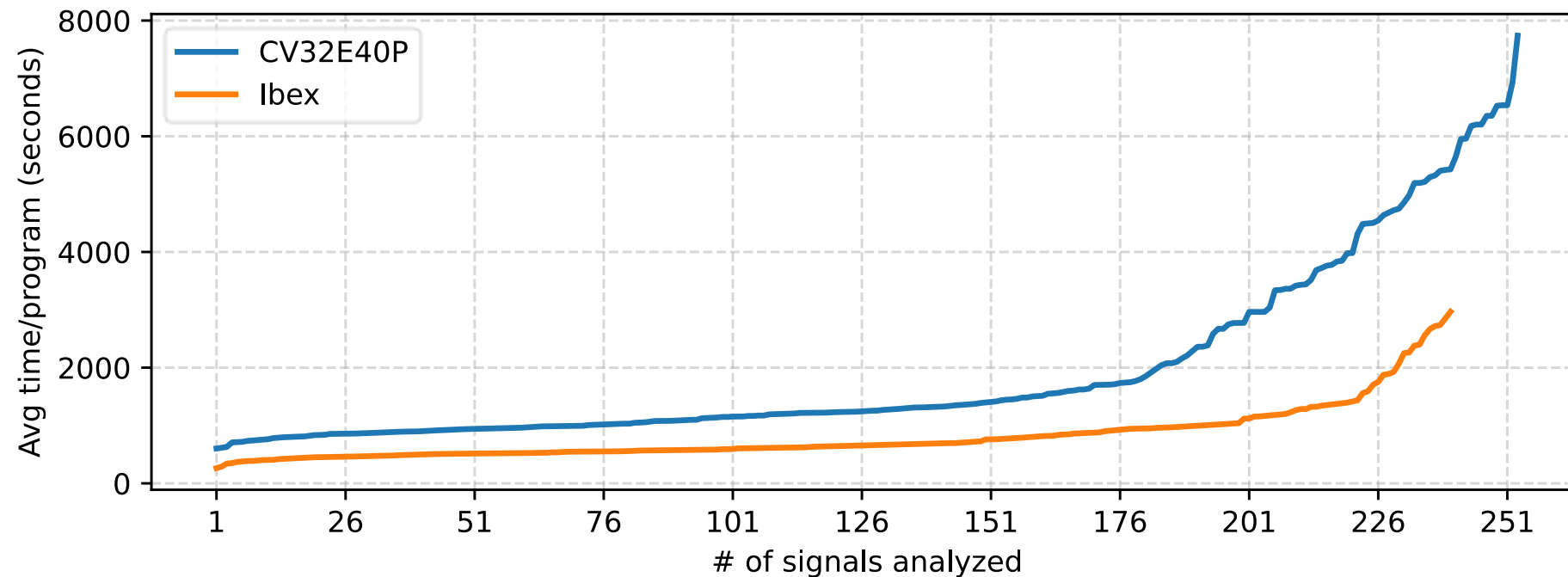


	CV32E40P	lbex
Size (Yosys internal cells)	2498	1749
Architecture	RISC-V 32bits IMC	RISC-V 32bits IMC
Stages #	4	3
Experimental parameters		
Fault effect	Bit flip	
Fault location	Each control signals (size ≤ 2)	
Program length	3 instructions	
Methodology	Iterate synthesis over all signals in the scope	

→ Each signal has its characterization test

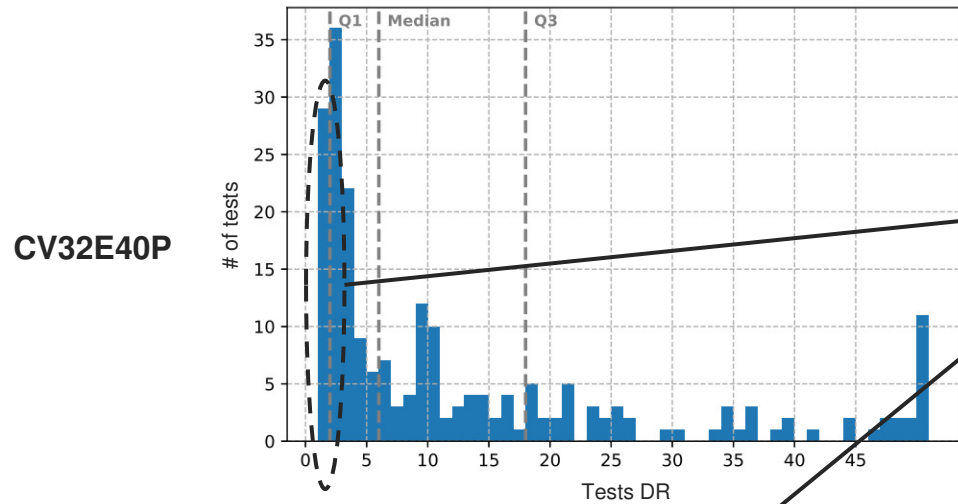
Validation: global figures

Results		
	CV32E40P	Ibex
Coverage	76%	64%
Median synthesis time	20mins50s	10mins42s
# of synthesized programs	1213	1135
Full analysis time	4.8 days	1.6 days



Validation: Program Discrimination

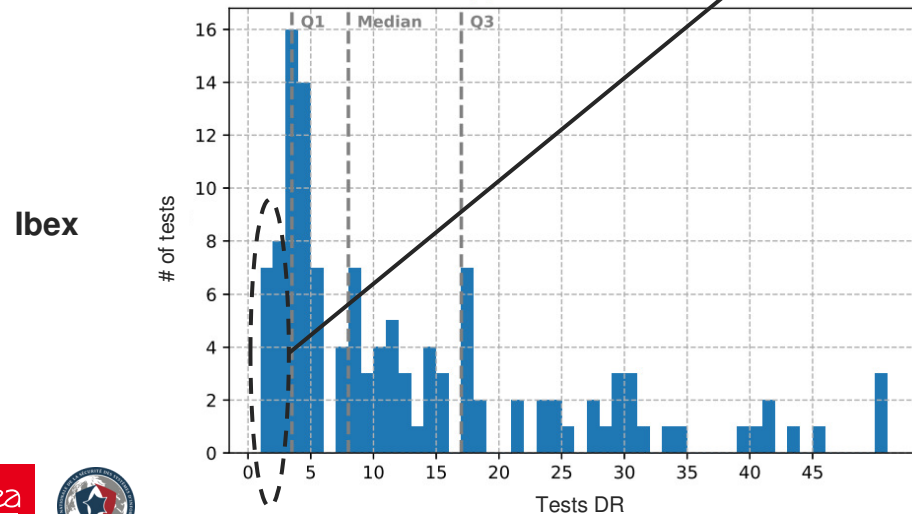
Number of signals revealed by its characterization test (smaller is better)



Perfectly discriminant tests (DR=1)

CV32E40P: 29 tests

Ibex: 7 tests



Other tests

✓ Enumeration of signals → **Great asset for evaluators**

Median discrimination:

- **CV32E40P**: 6 signals

- **Ibex**: 7 signals

For more than 75% → $DR < 24$

Validation: Discussion

Try to synthesize programs with different instruction numbers :
minimal impact over coverage and discrimination but big impact on synthesis time

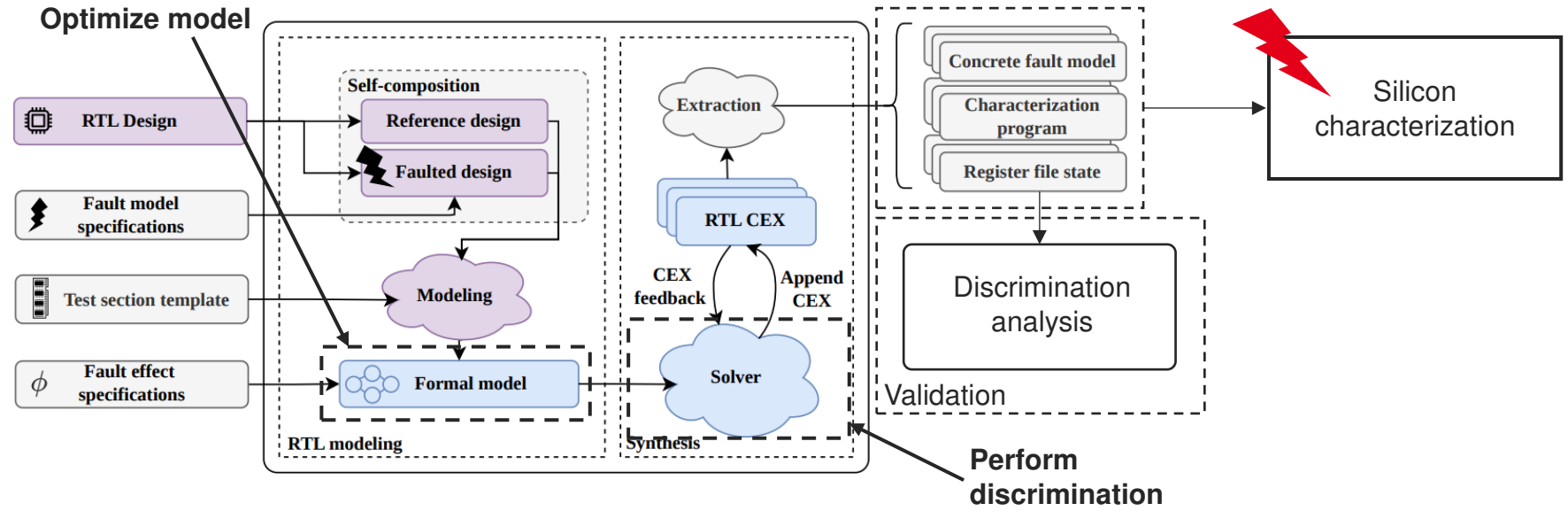
l		1	2	3	4	5	6	7	8
Coverage#		8	10	10	10	10	10	10	10
Syn. time		658	888	818	873	1239	1986	1961	2646
DR	Q1	2	2	4	3	4	3	2	3
	med	7	4	9	4	8	7	11	3
	Q3	30	37	26	13	13	22	23	25

Synthesis for larger signals (size $\in [1:32]$)

Bit width		0:2	0:16	0:32	all
CV32E40P	# of signals	399	502	665	702
	% of design	56	71	94	100
Ibex	# of signals	475	551	721	786
	% of design	60	70	91	100

On CV32E40P : Coverage 64% / Analysis time 2.2 days

Conclusion



Contributions summary:

- An automated fault characterization program synthesis methodology
- A discrimination analysis for characterization program
- An evaluation over two open source test cases

Next steps:

- Silicon characterization test
- Time optimization: strategies to reduce synthesis time
- Perform discrimination at synthesis time



Thank you

Signal proportion per size

TABLE II: Number of signals in $\mathcal{C}$ by width.

Bit width		0:2	0:16	0:32	all
CV32E40P	# of signals	399	502	665	702
	% of design	56	71	94	100
Ibex	# of signals	475	551	721	786
	% of design	60	70	91	100

Coverage over larger signals

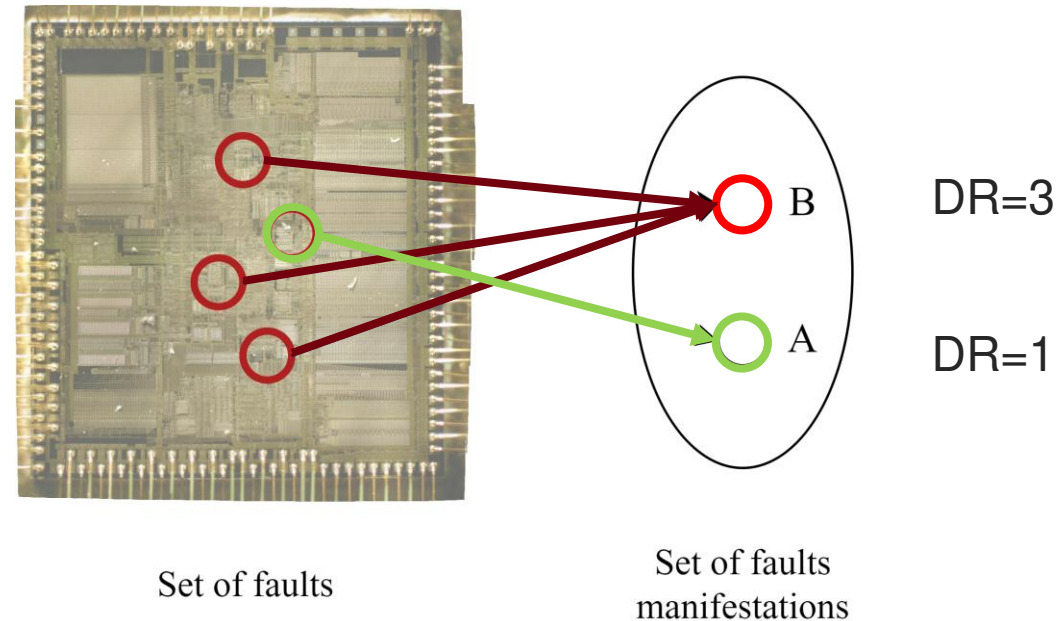
TABLE VII: Coverage for CV32E40P ($\phi_{\text{dump}}^{7,10}$), for signals with sizes ranging from 1 to 2, and 3 to 32 bits.

Module	Synthesis time	Coverage#	$ \mathcal{C}_{\text{analyzed}} $
$\mathcal{C}[0 : 2]$	117h10m14	255	332
$\mathcal{C}[3 : 32]$	54h10m07	164	256

The discrimination problem

Discrimination: ability of a test to locate faults relying on their manifestation

Discrimination Rate (DR): number of faults leading to a fault manifestation



➔ **Objective: Ideally $DR = 1$**

Impact of instruction length

l		1	2	3	4	5	6	7	8
Coverage#		8	10	10	10	10	10	10	10
Syn. time		658	888	818	873	1239	1986	1961	2646
DR	Q1	2	2	4	3	4	3	2	3
	med	7	4	9	4	8	7	11	3
	Q3	30	37	26	13	13	22	23	25