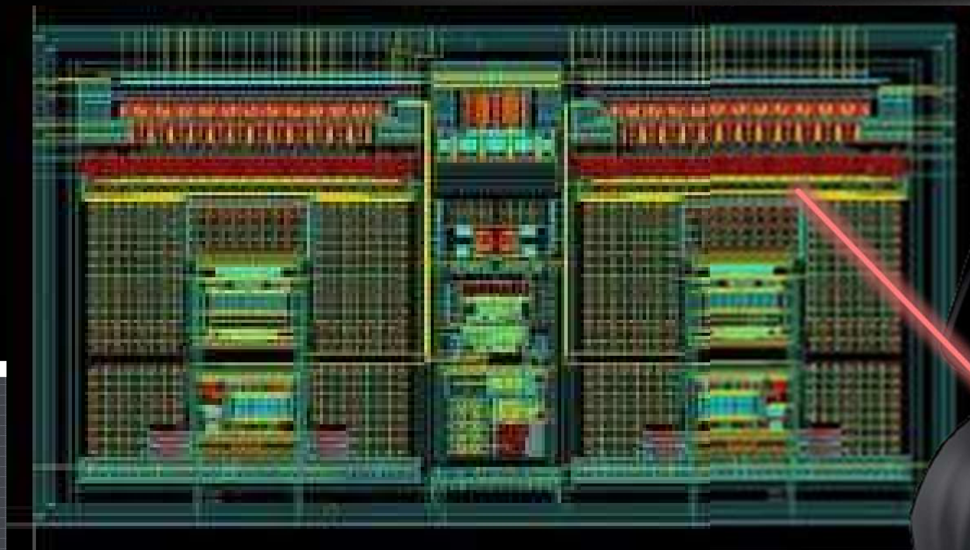
Laser-Induced Fault Simulation

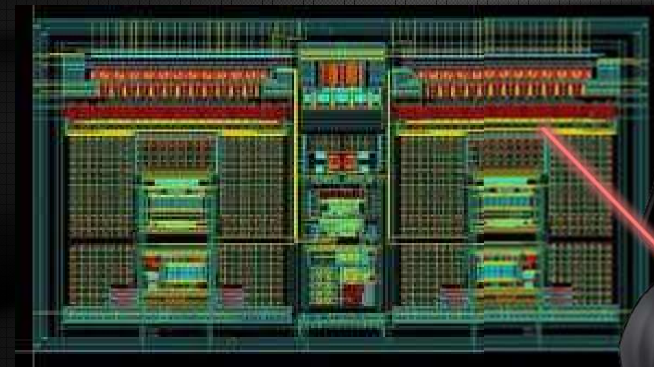


Feng LU, Giorgio Di Natale,
Marie-Lise Flottes, Bruno Rouzeyre

Introduction

Background: Secure Circuit & Fault Attacks

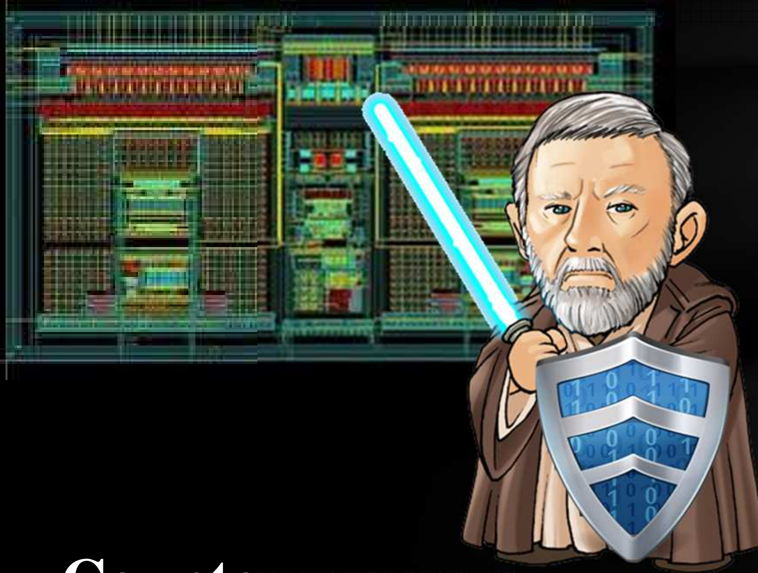
Secure Circuits



Fault Attacks to retrieve secret data (laser-induced fault attacks)

Introduction

Background: Laser Fault Injection



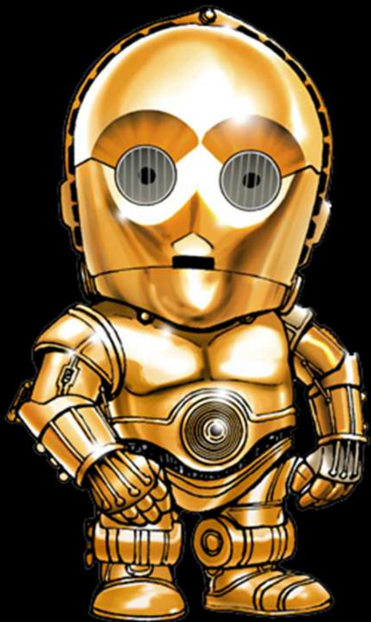
Countermeasure

Evaluation by real attacks:
- ☹ Expensive
- ☹ Long Setup time

Evaluation by Simulation:
- ☺ At Design Time
- ☺ Faster
- ☺ Inexpensive

Countermeasure Evaluation

Outline



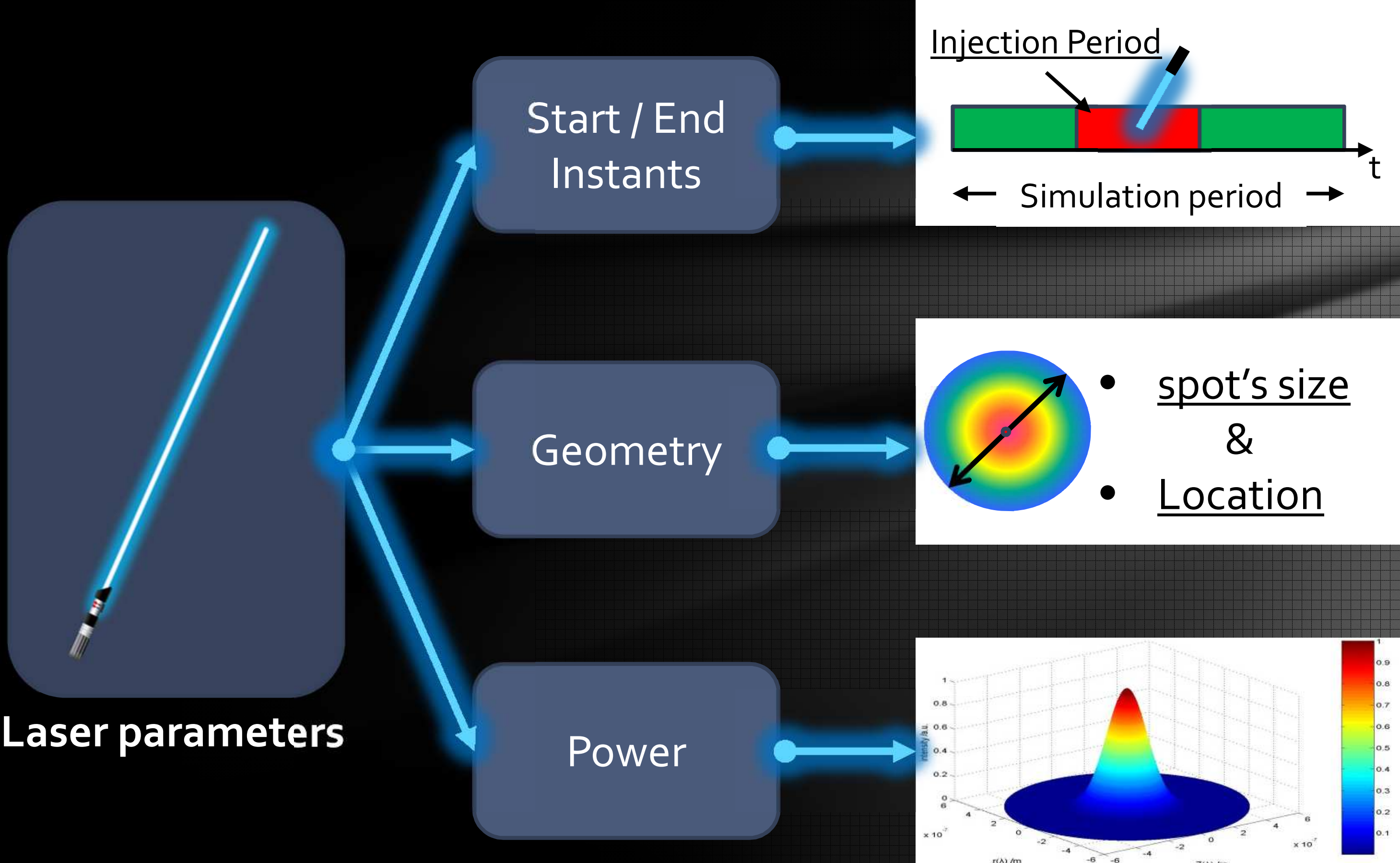
Laser Parameters

Process of Multi-level Fault Simulation

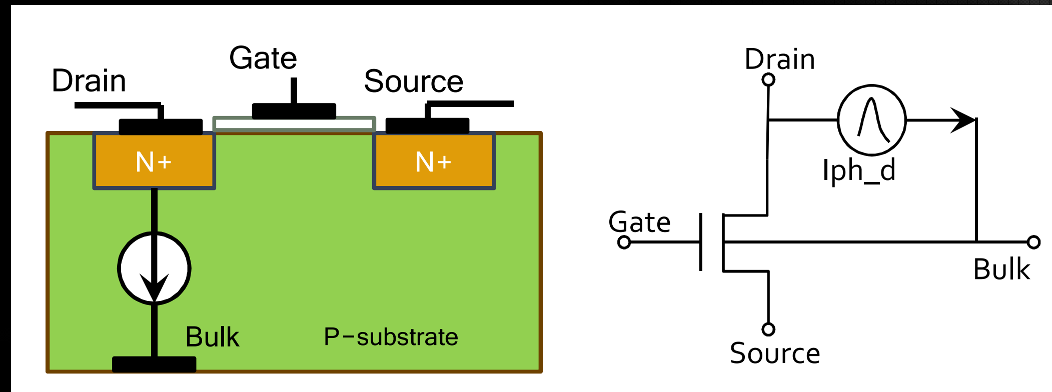
tLIFTING: Multi-level Fault Simulator

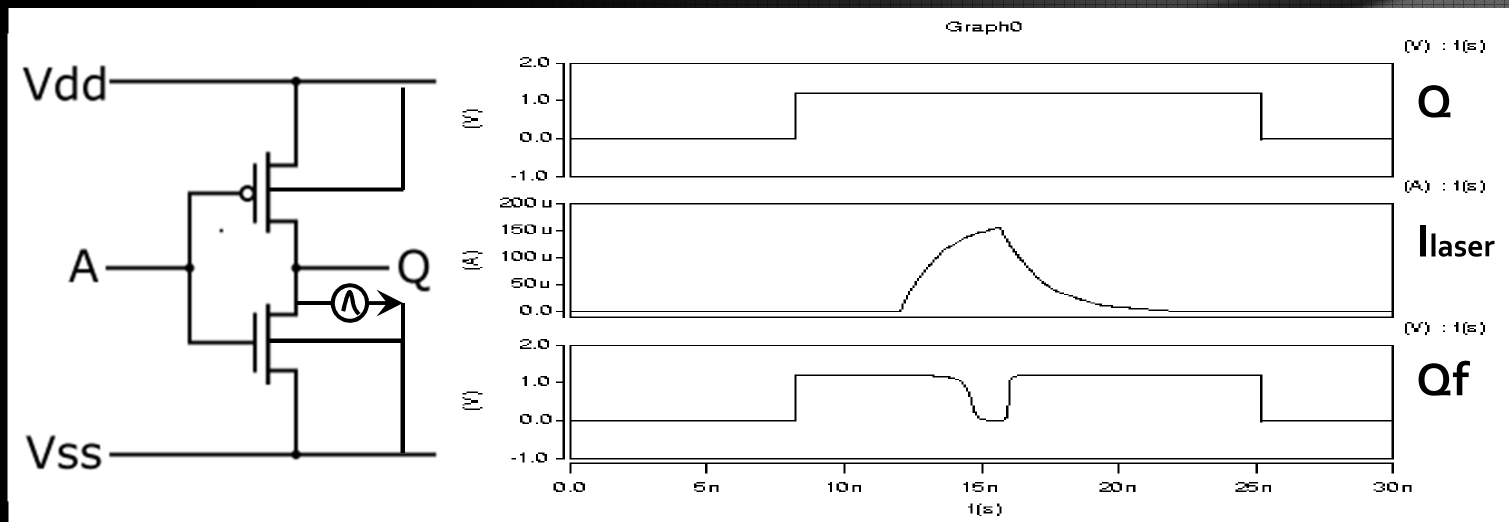
Experimental Results

Laser Parameters



Electrical Model of Laser-induced transient fault

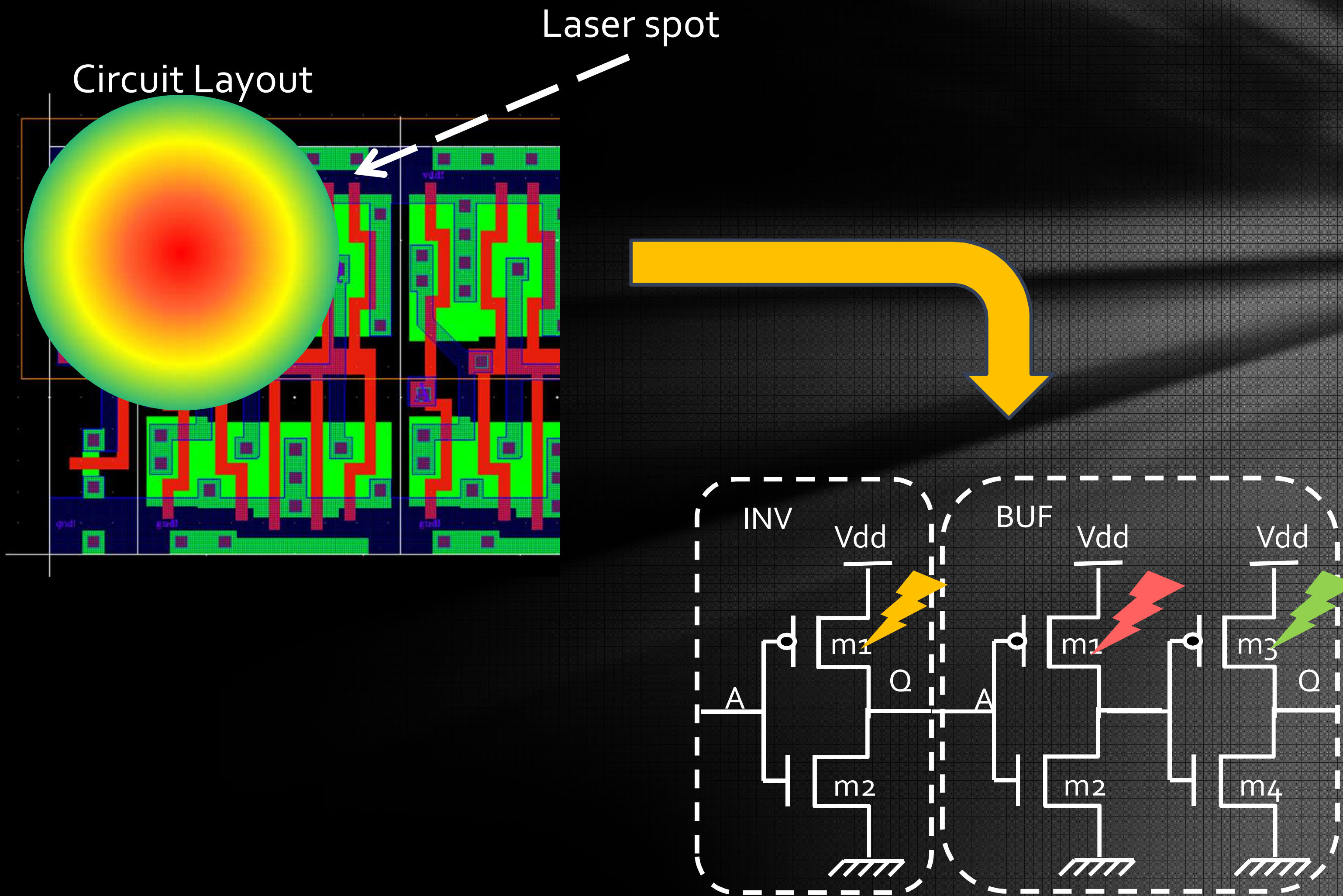




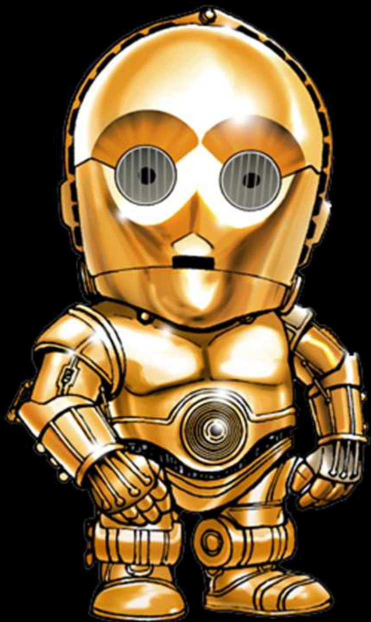
$$I_{laser} = I_o(e^{-t/ta} - e^{-t/tb})$$

[1] A. Sarafianos, R. Llido, J.M. Dutertre, O. Gagliano , V. Serradeil , M. Lisart , V.Goubier , A. Tria ,V. Pouget , D. Lewis. "Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90 nm technology ". Microelectronics Reliability 52 (2012) 2035–2038

Location of Laser Covered Sub-Circuit



Outline



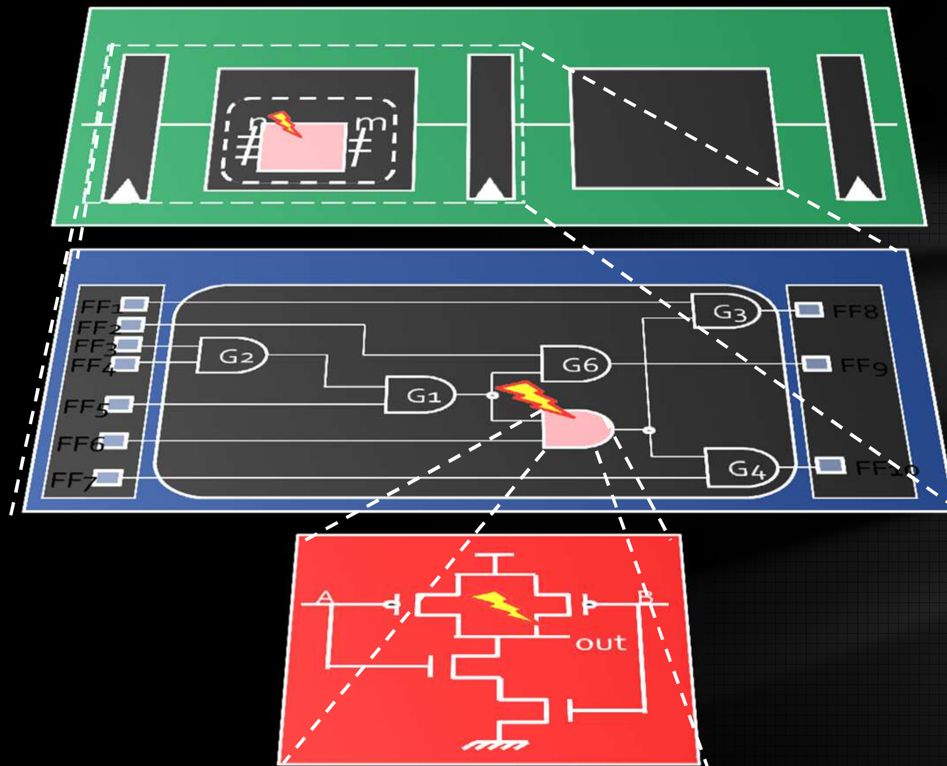
Laser Parameters

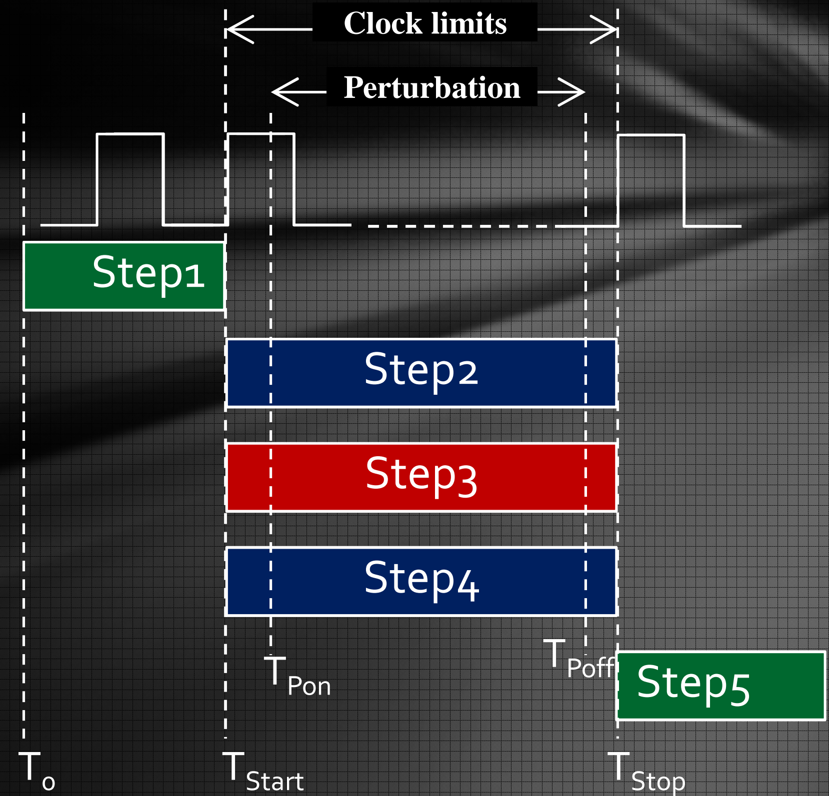
Process of Multi-level Fault Simulation

tLIFTING: Multi-level Fault Simulator

Experimental Results

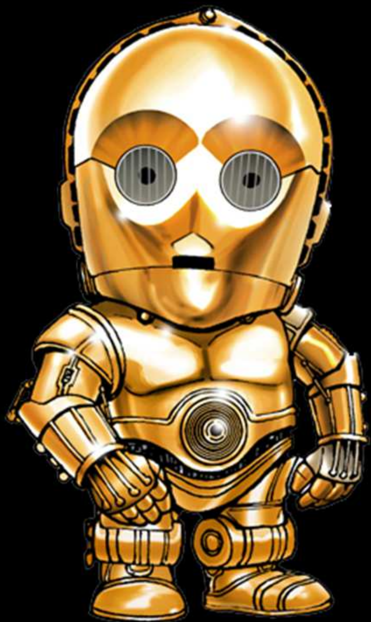
Process of Multi-level Fault Simulation





LEGEND		
0-delay Logic-level	Delay –annotated Logic-level	Analog-level

Outline



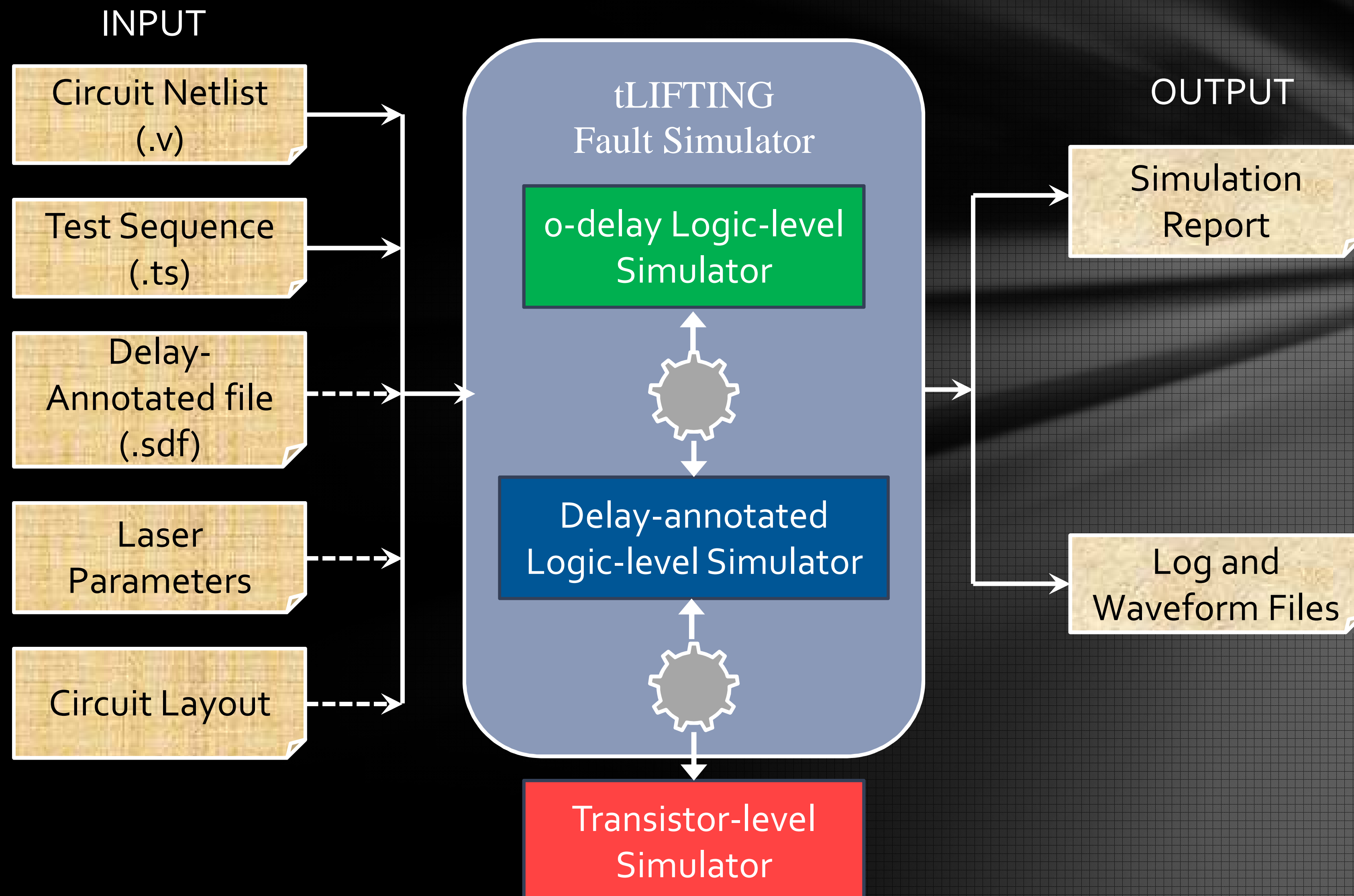
Laser Parameters

Process of Multi-level Fault Simulation

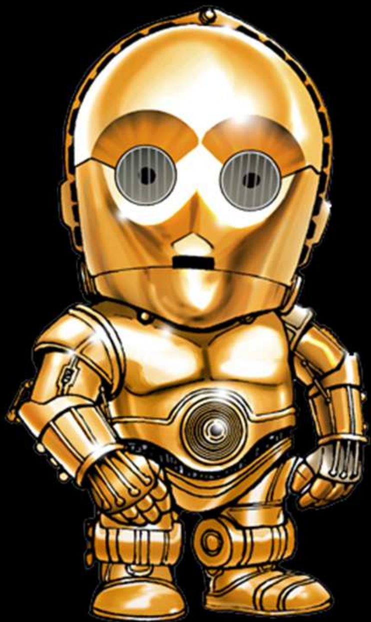
tLIFTING: Multi-level Fault Simulator

Experimental Results

tLIFTING: Mixed–Mode and Multi-Level Fault Simulator



Outline



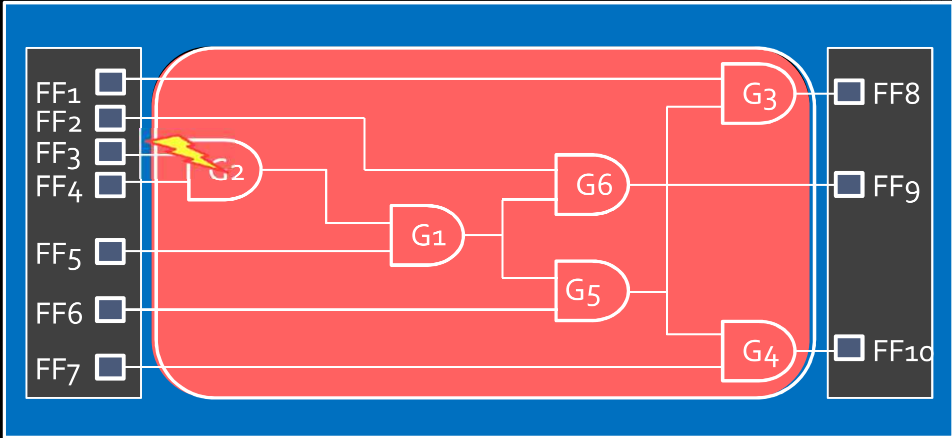
- Laser Parameters
- Process of Multi-level Fault Simulation
- tLIFTING: Multi-level Fault Simulator
- Experimental Results

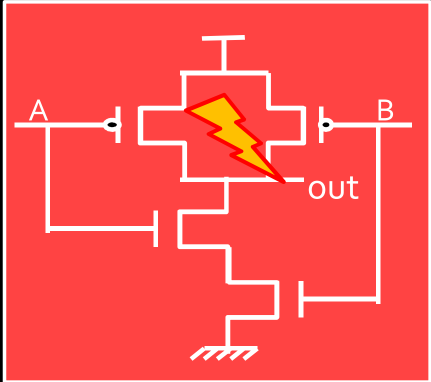
Experimental Results – *Execution Time*

tLifting vs Spice

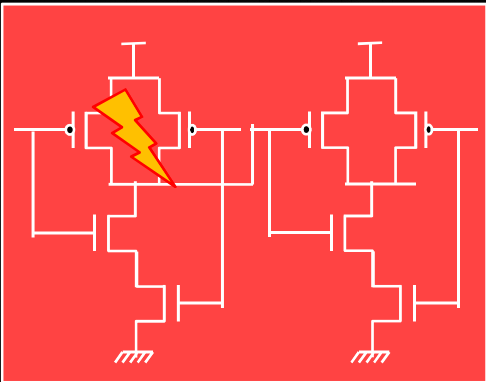
	Circuit information		Fault simulation [s]		
circuit	Size	Vectors	Multi-Level	Hspice	Factor
c432	112	77	0.116	55.78	480x
c499	133	77	0.132	89.05	674x
c1355	162	72	0.132	86.48	655x
c1908	169	80	0.228	129.12	566x
c880	204	77	0.404	119.22	295x
c2670	292	136	2.052	393.78	191x
c3540	476	171	1.916	676.7	353x
c5315	608	113	4.204	705.05	167x
c7552	705	167	9.428	1356.56	143x
c6288	1286	63	8.308	1248.75	150x
b01	31	13	0.03	6	200x
b04	41	16	0.04	5.03	125x
b10	89	128	0.09	25.97	288x

Experimental Results – *Hspice Range*



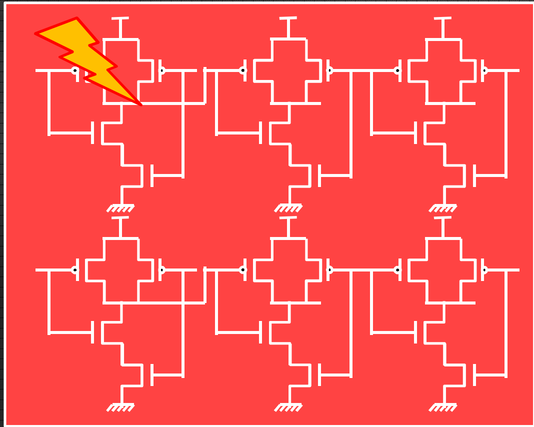


Level 1



Level 2

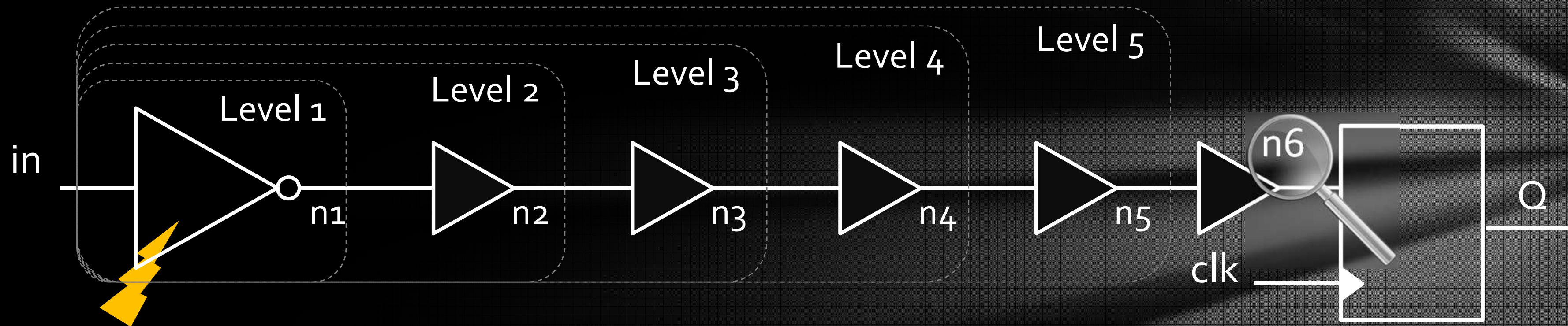
…



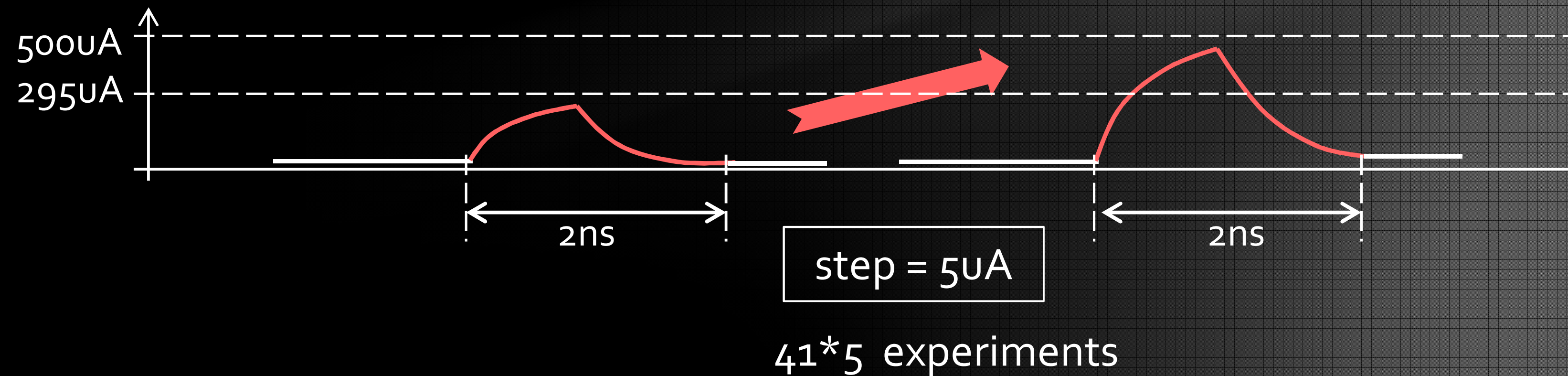
Level 4

Experimental Results – *Experimental Setup*

Test circuit

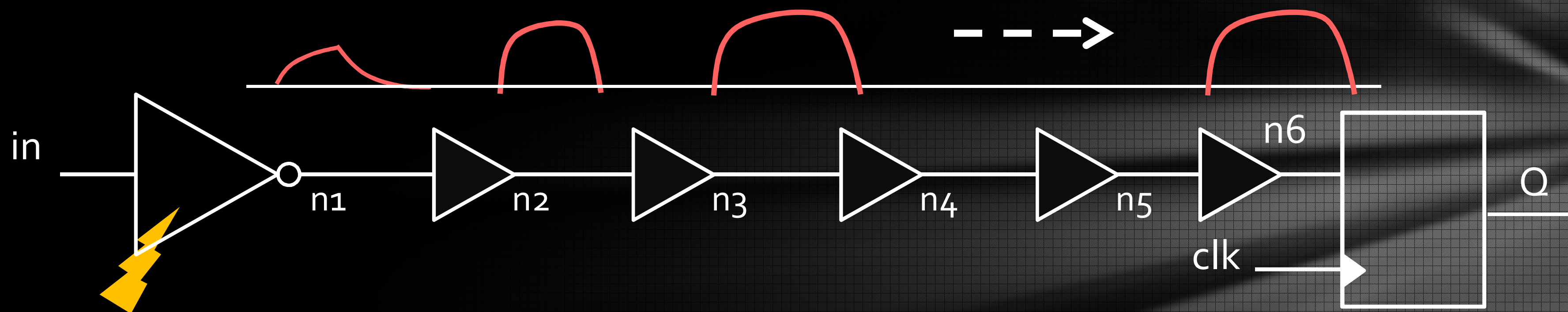


Injected Fault pulse

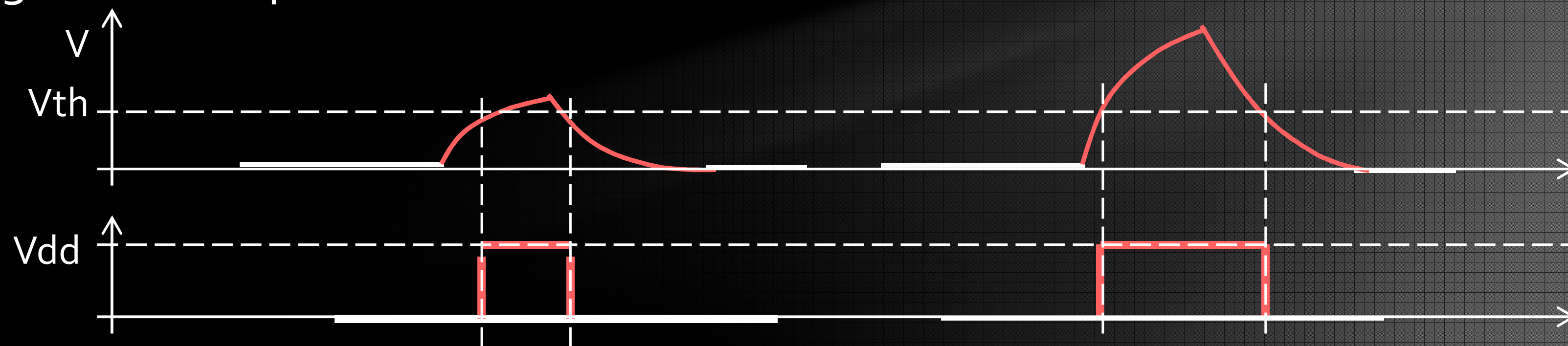


Experimental Results – *Fault pulse*

Propagation of fault pulse

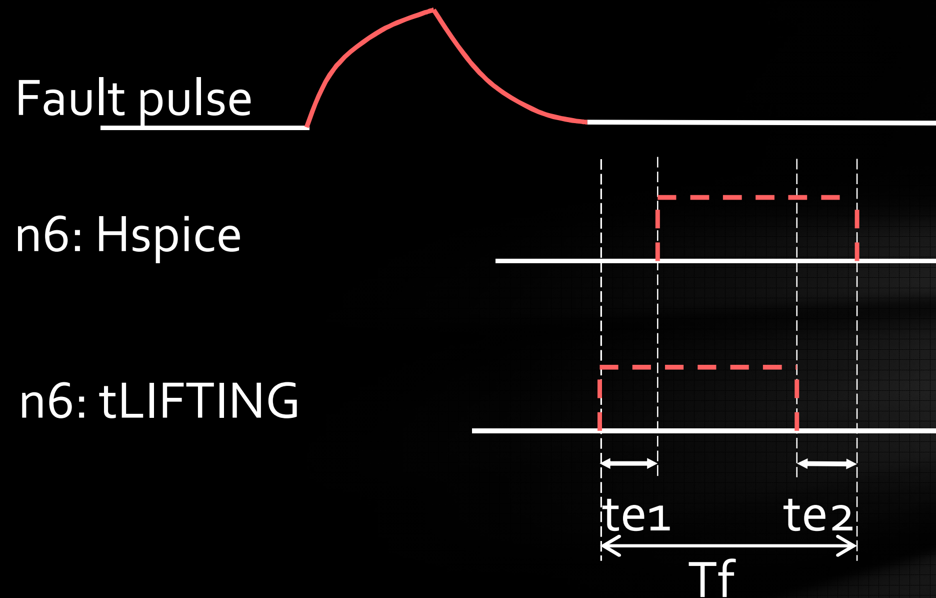


Digitized fault pulse

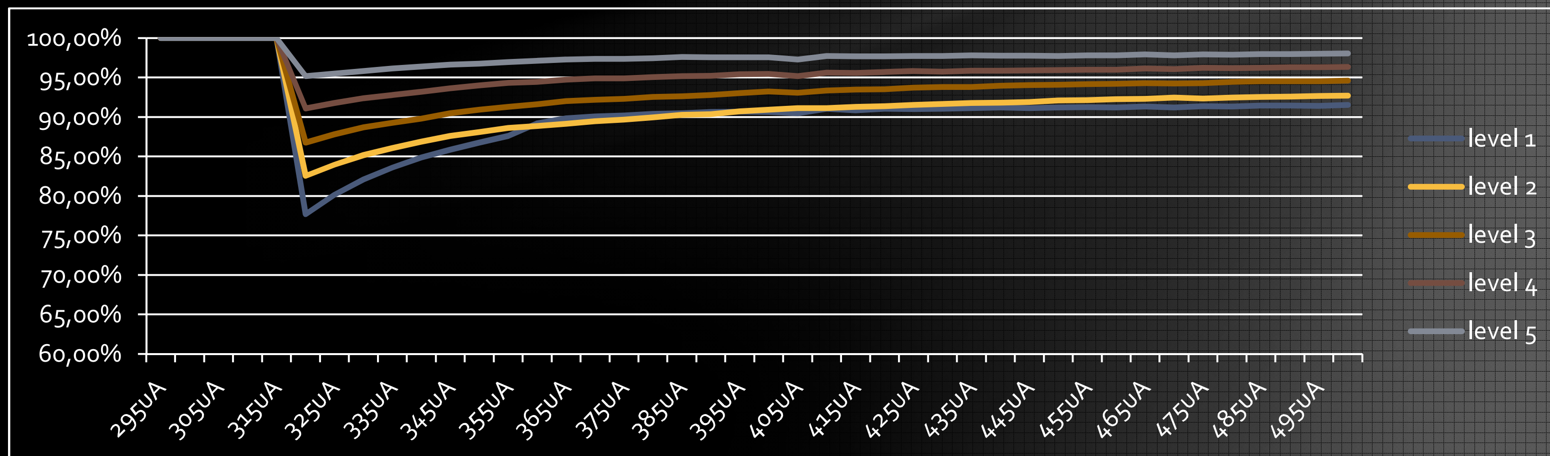


Amplitude of injected fault ∝ Width of fault pulse

Experimental Results *– Accuracy of combinational logic*



Accuracy_comb
$= 1- \sum te_i / Tf$



Experimental Results – *Accuracy Analysis*

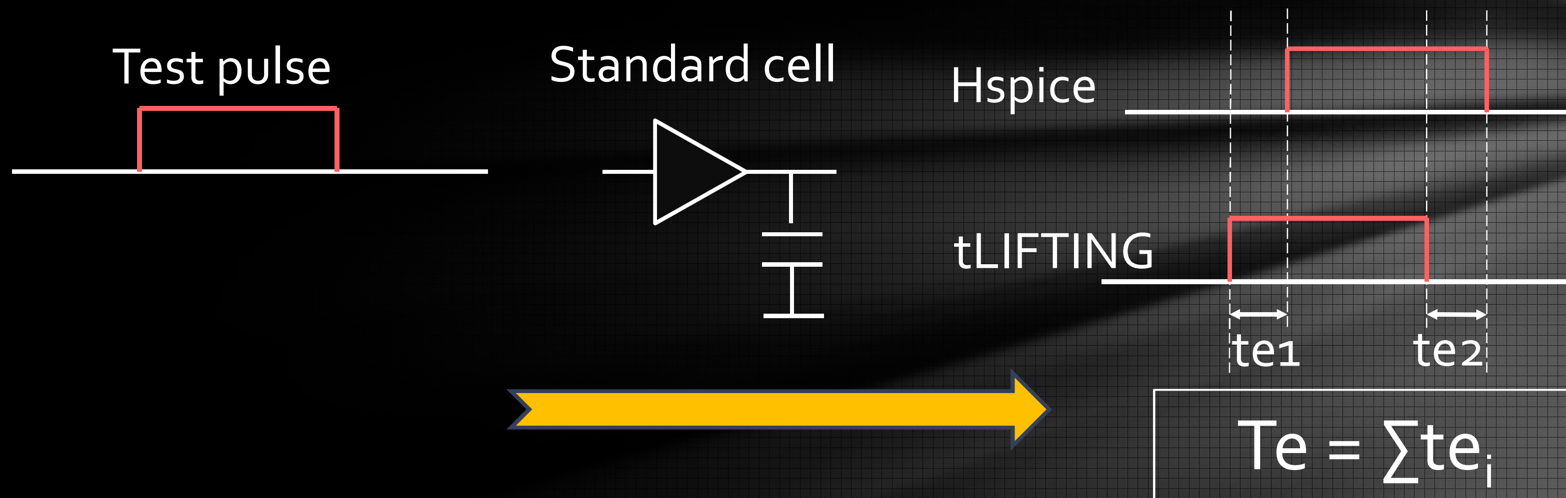
310uA to 500uA	Level1	Level2	Level3	Level4	Level5
	Te	Te	Te	Te	Te
Average [ps]	134,87	146,15	112,17	72,67	34,52
Standard deviation	49,55	2,09	1,10	1,53	1,08

$$Te = \sum te_i$$

Conclusion:

1. Level 1 is NOT proposed.
2. For Level 2 and above, Te does not change with the width of the fault pulse.
3. Te to be estimated.

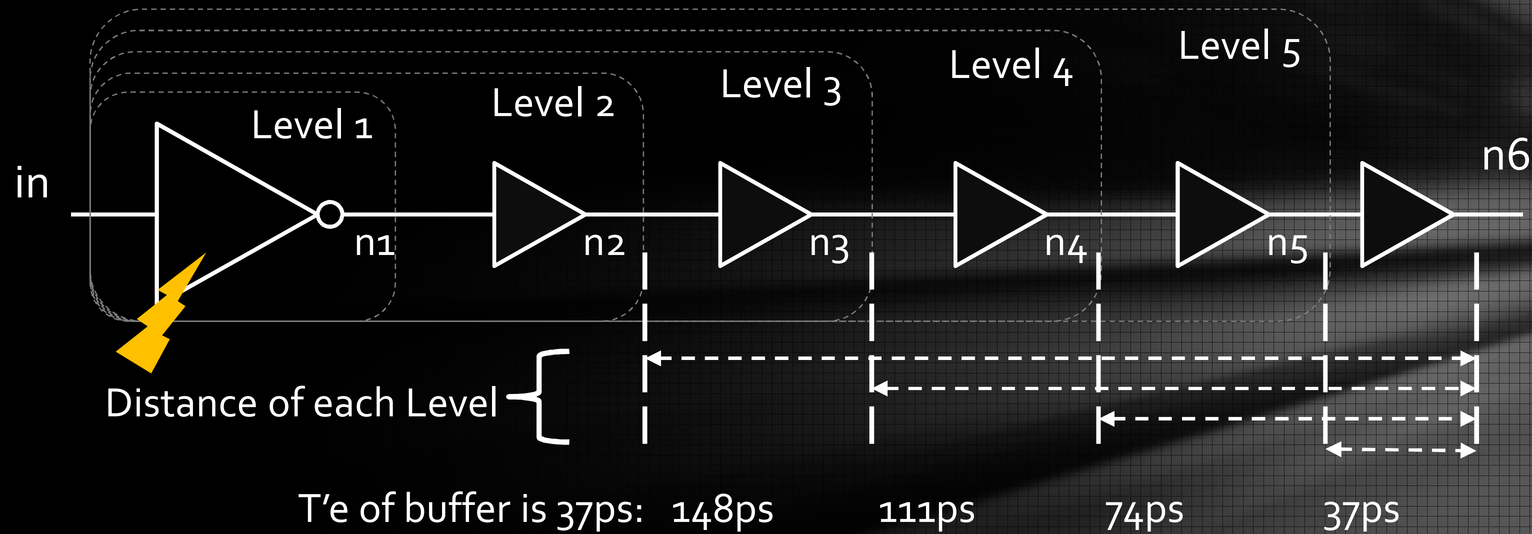
Predicting simulation level Measurements of standard cells



Different test pulses => T′e = Average of Te

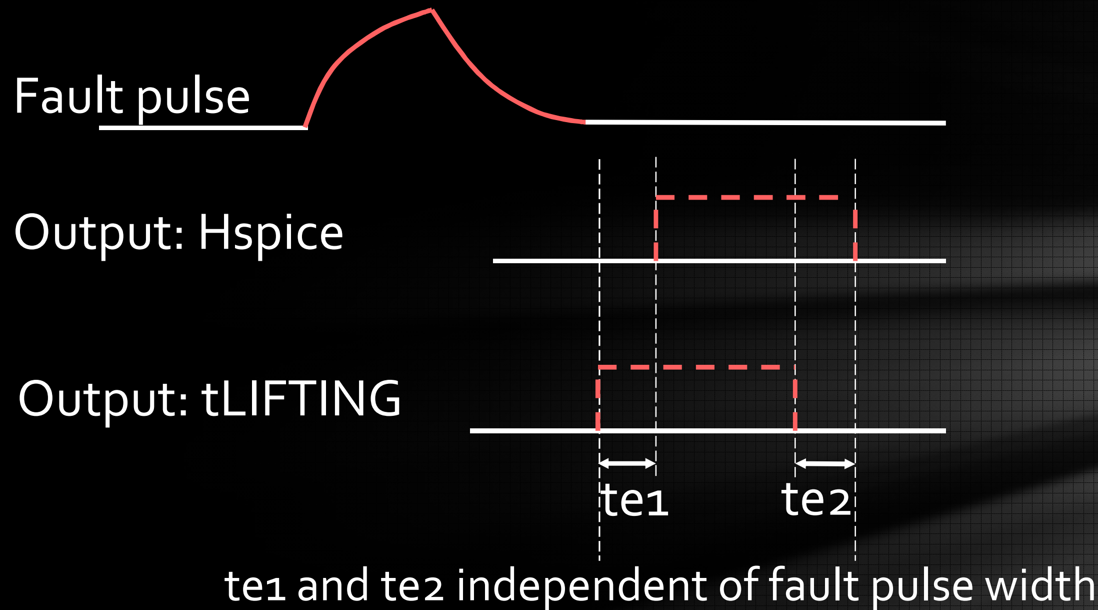
Example: T′e of this buffer is 37ps

Predicting simulation level (1) Te estimation



310uA to 500uA	Level1 Te	Level2 Te	Level3 Te	Level4 Te	Level5 Te
Average [ps]	134,87	146,15	112,17	72,67	34,52
Estimated values [ps]	/	148,00	111,00	74,00	37,00

Predicting simulation level (2) te1 & te2 estimation

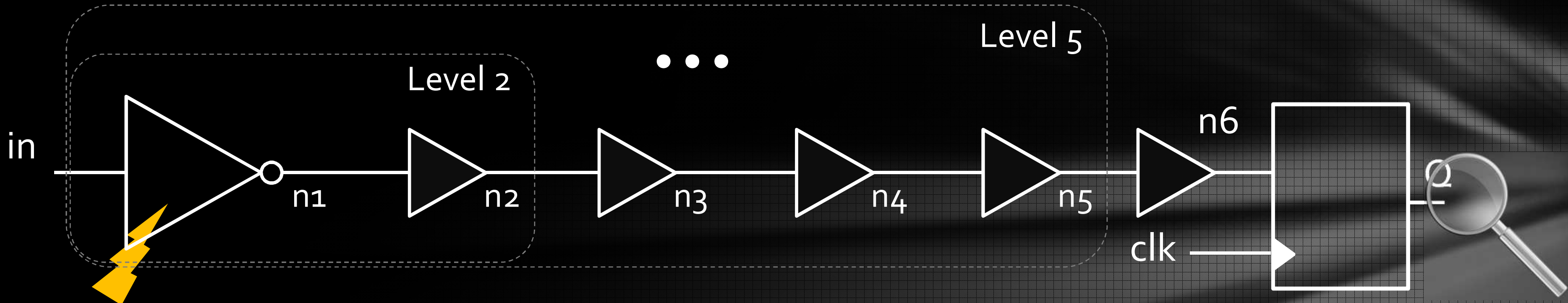


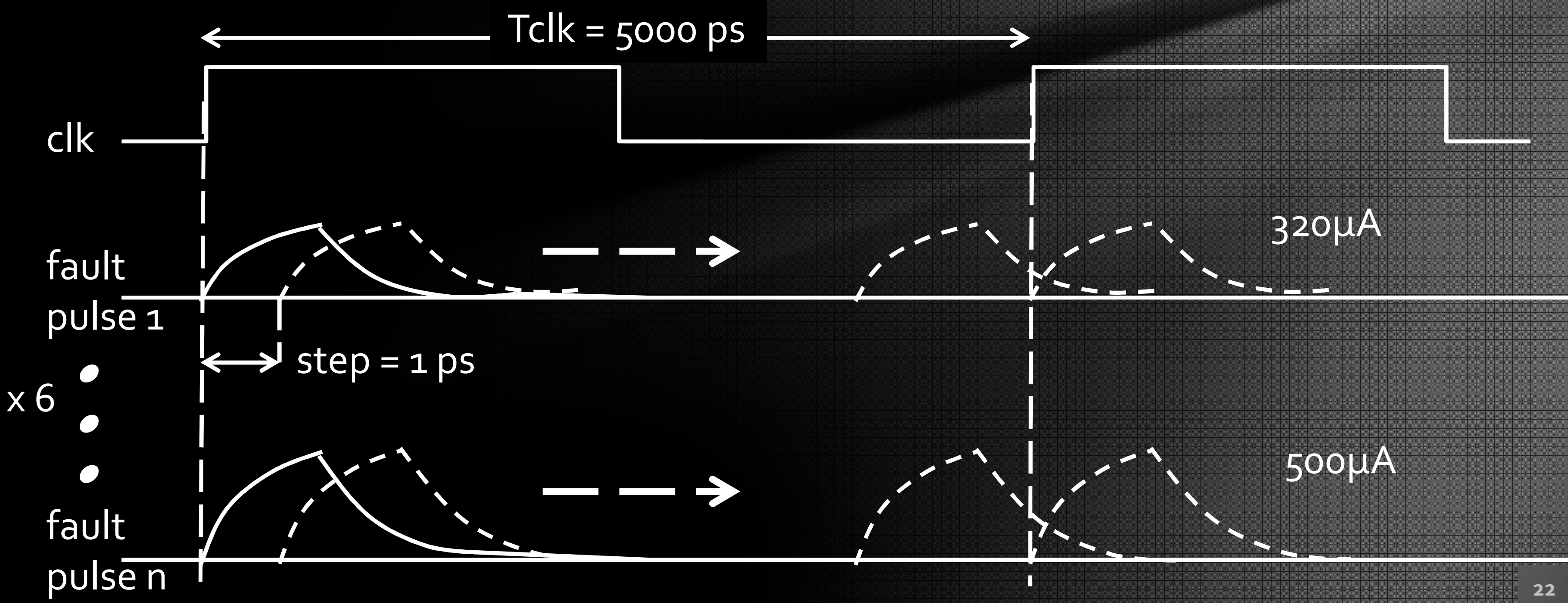
te1 and te2 independent of fault pulse width

310uA to 500uA	Level 1		Level 2		Level 3		Level 4		Level 5	
	te1	te2	te1	te2	te1	te2	te1	te2	te1	te2
Average [ps]	64,12	70,75	98,15	48,00	75,77	36,40	49,27	23,40	24,15	10,37
Estimated values [ps]	/	/	98,00	50,00	73,50	37,50	49,00	25,00	24,50	12,50

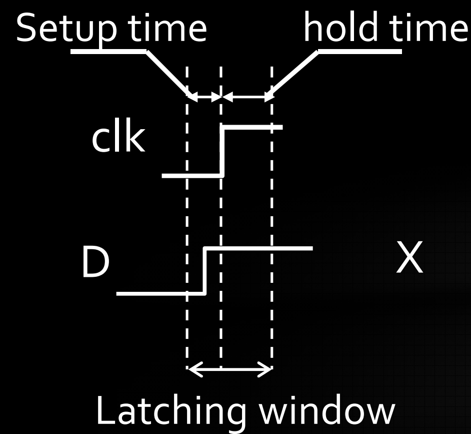
Estimation => Choice of Simulation Level

Predicting simulation level (3)





Predicting simulation level (4)



Pe(t) is Error Probability with the fault pulse which is injected at moment t.

tLIFTING	Hspice	Pe(t)
0	0	0
1	1	0
X	0	0.5
X	1	0.5
1	0	1
0	1	1

5000 experiments

Level 2

Current (mA)	Number of experiment Pe(t) = 0.5	Number of experiment Pe(t) = 1	Sum of Pe(t)
320	149	8	83,5
350	147	10	83,5
400	150	7	82
430	149	9	83,5
460	148	8	82,5
500	147	9	83,5
Average		8,5	83,08

Predicting simulation level (5) *Accuracy Calculation (1)*

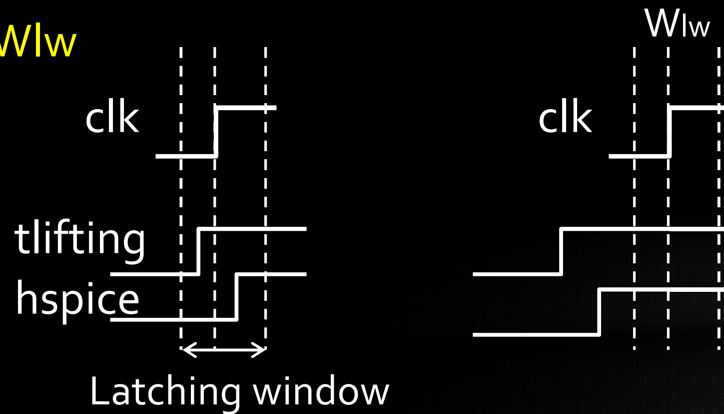
The probability for the difference of latched values of two simulators:

$$P = \frac{1}{T_{clk}} \int_0^{T_{clk}} P_e(t)\,dt$$

Predicting simulation level (6) *Accuracy*

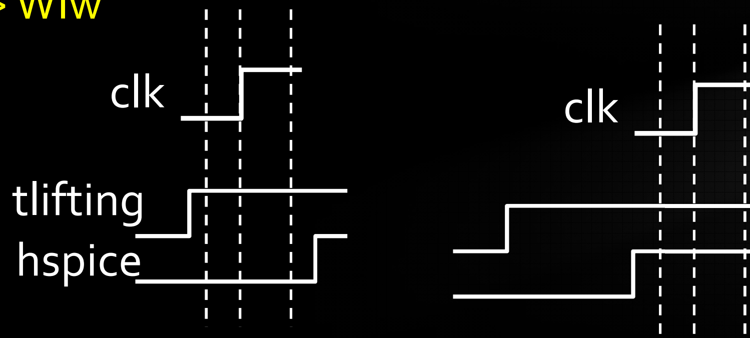
Calculation (2)

te ≤ Wlw



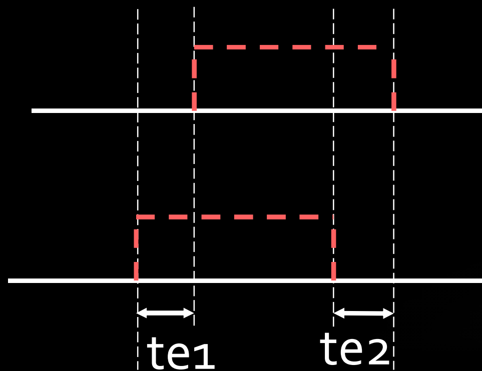
$$P = (0.5 \times W_{lw}) / T_{clk} \qquad (te \leq W_{lw})$$

te > Wlw



$$P = (te - 0.5 \times W_{lw}) / T_{clk} \qquad (te > W_{lw})$$

Predicting simulation level (7) *Calculation step*



1. The W_{lw} of the flip-flop are W_{lw1} = 110ps, W_{lw2} = 40ps. (These values are defined in SDF file).
2. For level 2 simulation, estimated t_e are t_{e1} = 98ps, t_{e2} = 50ps.
3. $t_{e1} \leq W_{lw1}$ => P_1 = 1.1%
   $t_{e2} > W_{lw2}$ => P_2 = 0.6%
4. Credibility of latched/non-latched SET fault:
   $P_c = 1 - \sum P_i = 98.3\%$

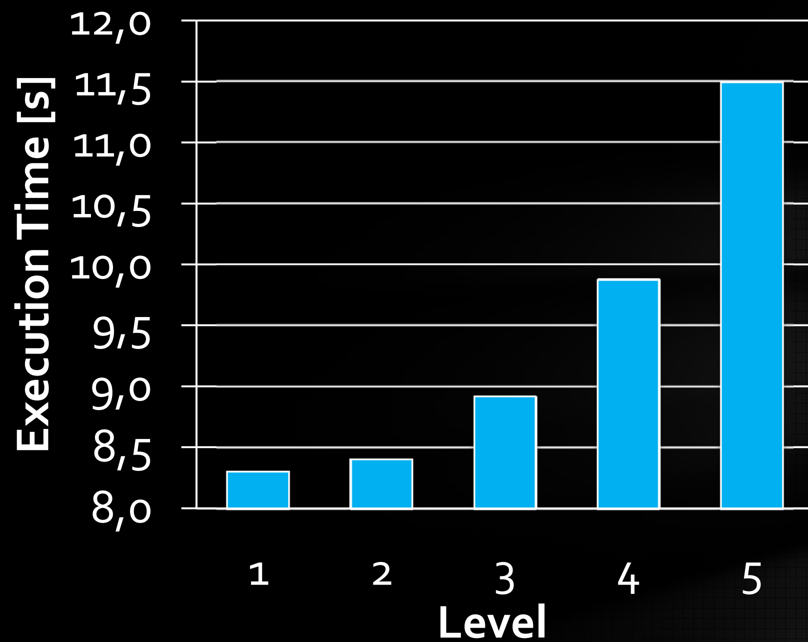
Experimental Results

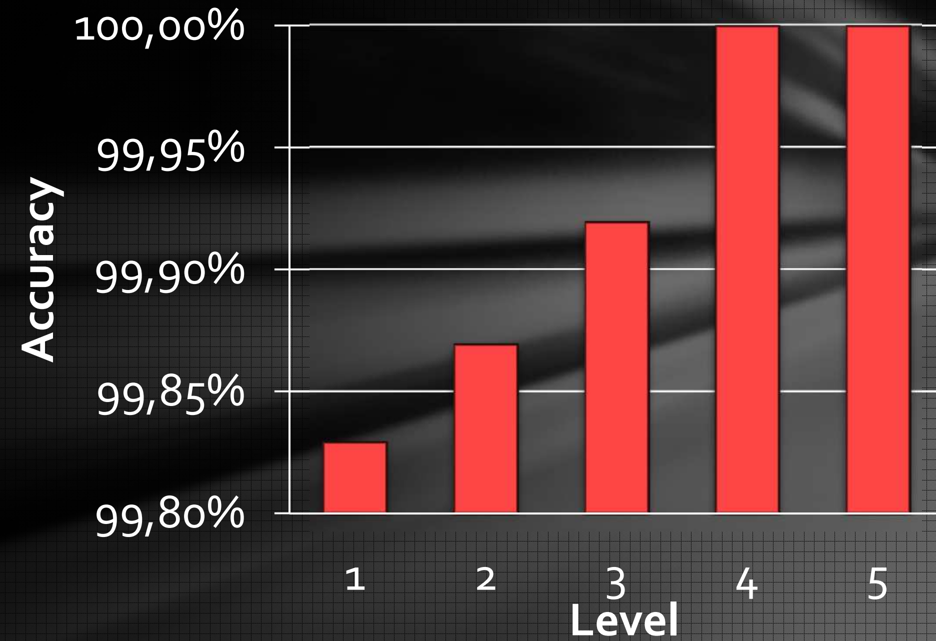
Simulation level	Number of experiments	Accuracy (experimental)	Accuracy (estimated)	Accuracy* (experimental)	Accuracy* (estimated)
2	30000	98,34%	98,3%	99,83%	99,8%
3	30000	98,5%	98,5%	100%	100%
4	30000	98,5%	98,5%	100%	100%
5	30000	98,5%	98,5%	100%	100%

* The unknown state “X” is NOT considered as an error.

=> adequate simulation level a priori determined

Execution Time Vs. Accuracy





Level

Speed

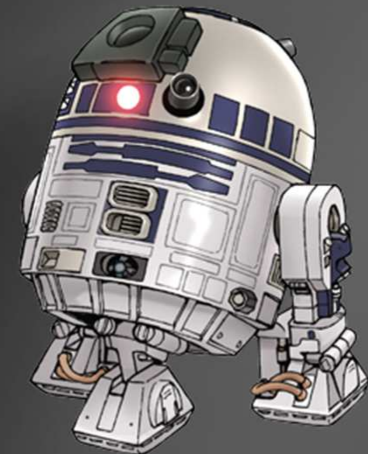
Accuracy

Conclusion

Multi-fault Simulator

User-defined precision

Flexibility



THANK YOU

On going work