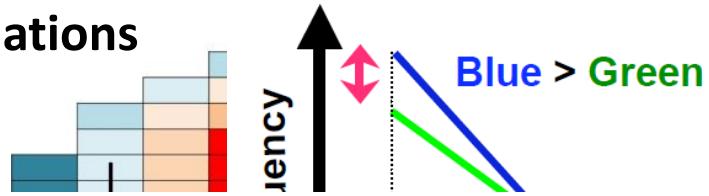
UCLA

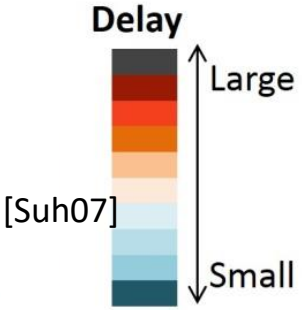
Implementation of Stable PUFs Using Gate Oxide Breakdown

Wei-Che Wang, Prof. Puneet Gupta
Dr. Yair Yona, and Prof. Suhas Diggavi
UCLA Electrical Engineering

Limitations of Silicon PUFs

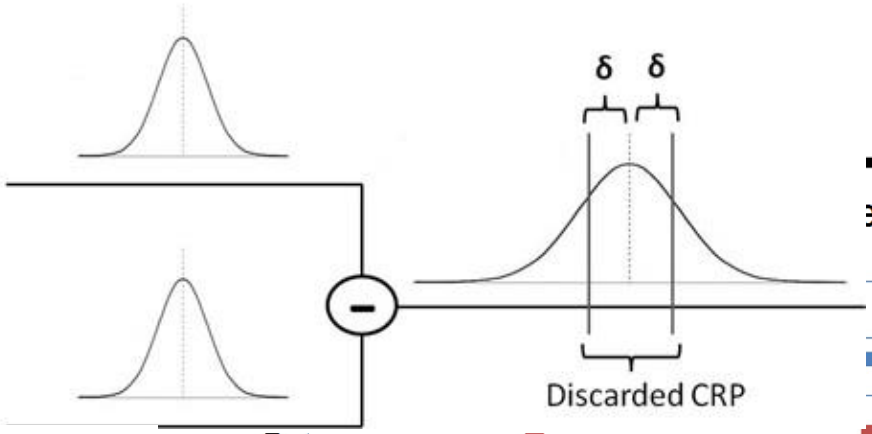
- **Stability**
  - **Environmental fluctuations**
  - **Measurement noise**

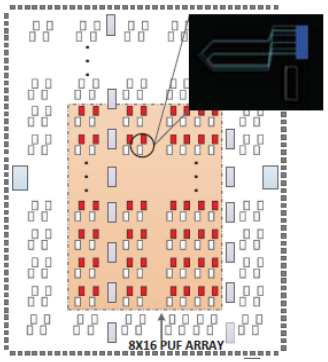




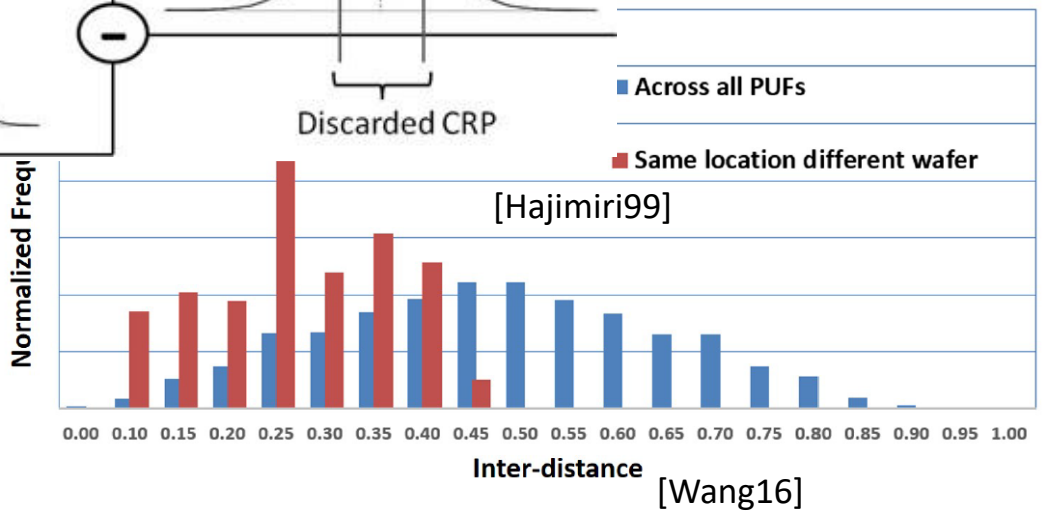
[Suh07]

- **Uniquenes**
  - **Randomne**
  - **Routing co**





[Gu15]



[Hajimiri99]

[Wang16]

Novel Source of Stable Randomness

- **Hard defectivity**
  - Permanent defectivity
  - Stable across different corners

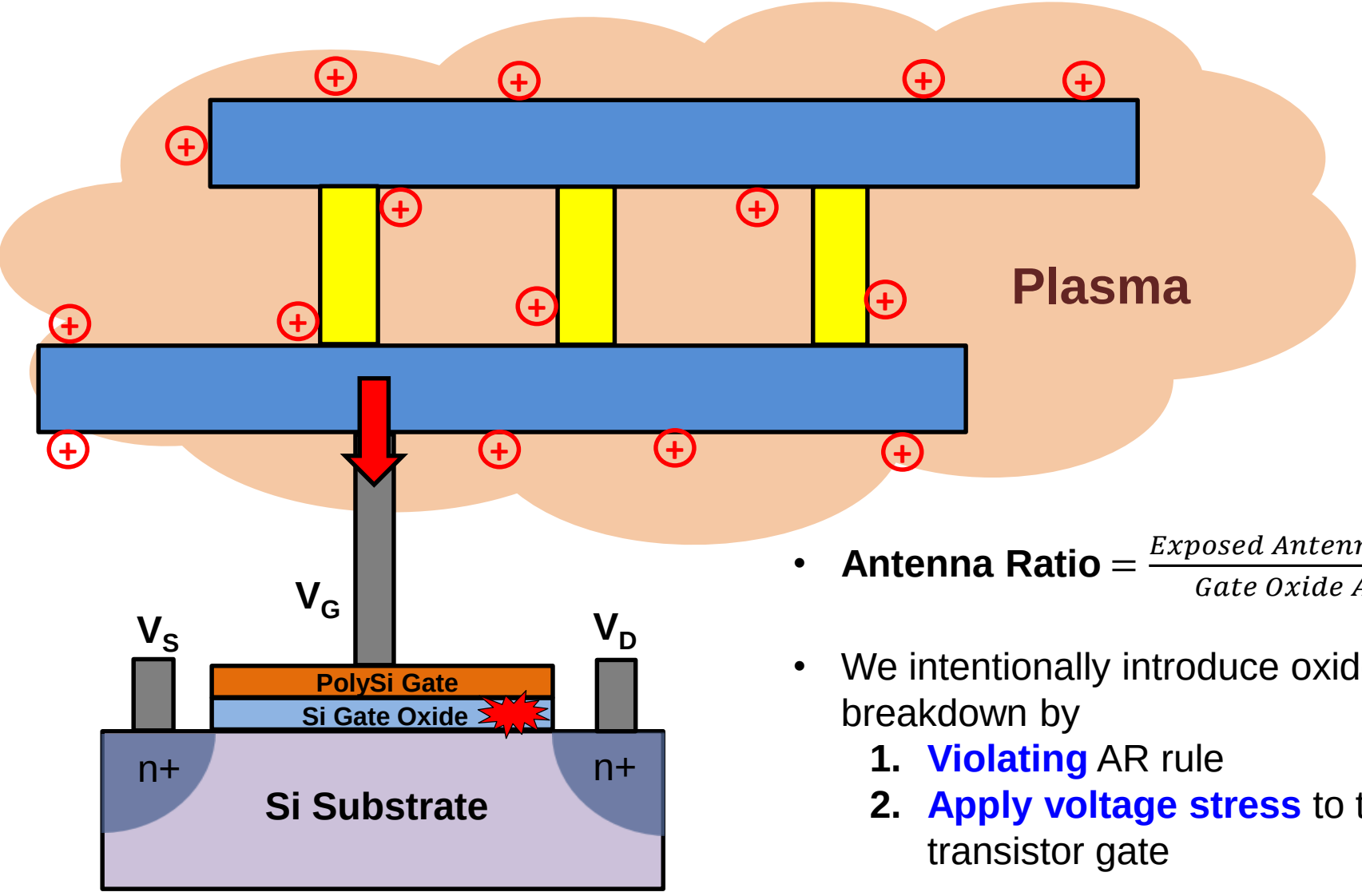
Stable!

- **Locally enhanced randomness**
  - No impact (from hard defectivity) to other parts of the chip
  - Through physical design
  - Compatible with circuit design flow

Unique!

Real test chip fabricated!

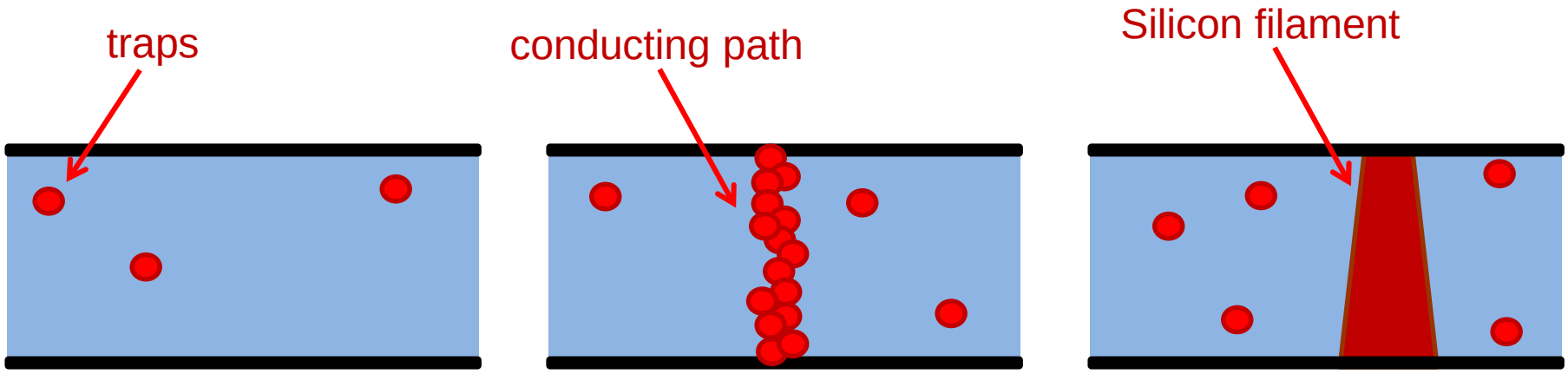
Gate Oxide Breakdown



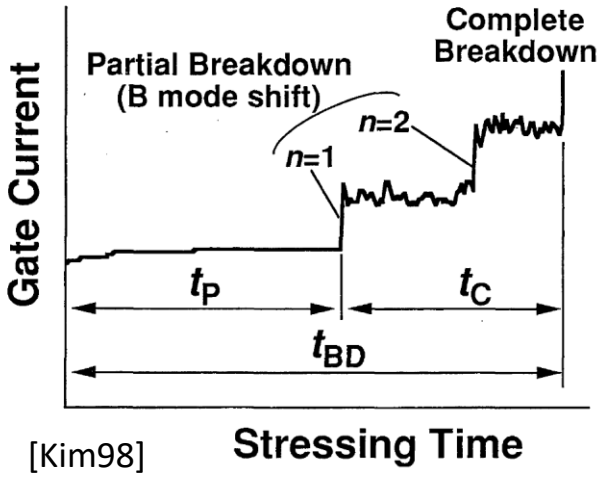
- **Antenna Ratio** $= \frac{Exposed\ Antenna\ Area}{Gate\ Oxide\ Area}$

- We intentionally introduce oxide breakdown by
  1. **Violating** AR rule
  2. **Apply voltage stress** to the transistor gate

Types of Breakdown

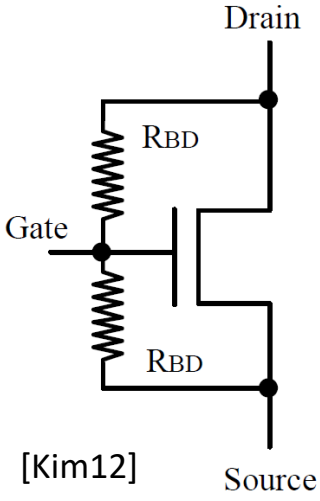


Both SBD and HBD have > 100X leakage than NBD



[Kim98]

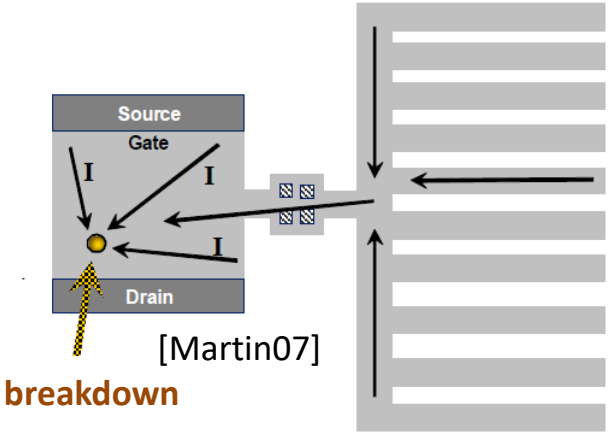
Model of a transistor with BD



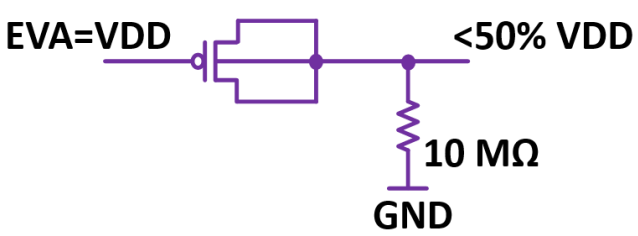
[Kim12]

Stable Signal Unit

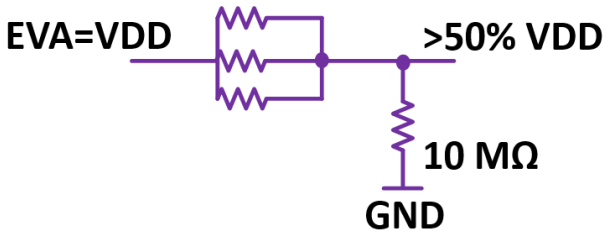
- A Stable Signal Unit (SSU) is a p-MOS transistor
  - **Violates AR rules** or **stressed with high voltage**
  - Three terminals (S,D,B) are connected to capture the effect of oxide breakdown
- When EVA is high
  - No breakdown → Output logic zero
  - Breakdown occurs → Output is logic one



breakdown



No breakdown



Breakdown occurs

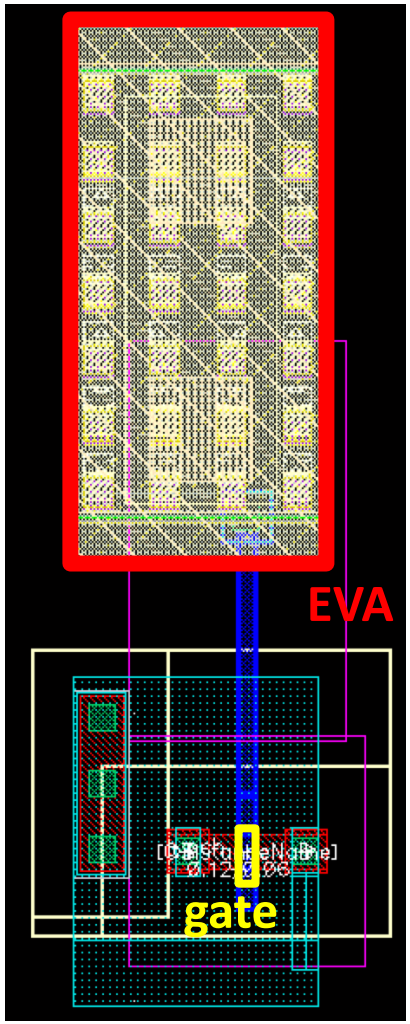
SSU Implementation

Geometries (um^2) of 29 SSUs implemented on each 65nm test chip

	Cell	VIA	Metal	Poly	Poly Perim. (um)
AR Rule		**0.144**	**36**	**1.8**	**3.6**
M_T1	36	0.87	1144.57	0.00	0.00
M_T2	360	1.17	1468.57	0.00	0.00
M_T3	1200	0.00	4398.88	0.00	0.00
M_T4	4800	0.16	36781.89	0.00	0.00
V_T1	2.4	0.87	1108.57	0.00	0.00
V_T2	8	2.31	1108.57	0.00	0.00
V_T3	90	15.27	1185.66	0.00	0.00
V_T4	804	144.91	1895.05	0.00	0.00
P_T1	4.8	1.26	1917.53	0.00	0.00
P_T2	27	1.26	1917.53	18.17	55.59
P_T3	203	1.26	1917.53	180.07	128.43
P_T4	1800	1.26	1917.53	1800.07	222.46
Test1	804	1071.86	5631.11	0.00	0.00
Test2	4.7	1.86	0.00	0.00	0.00
Test3	80	0.26	299.20	0.00	0.00
Test4	60	20.84	318.78	28.07	83.81
Test5	118	54.40	617.25	56.39	164.72

12 x 2 SSUs

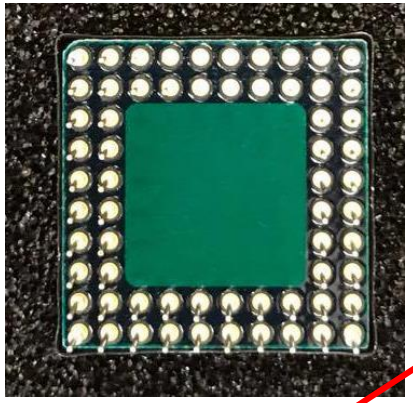
5 SSUs



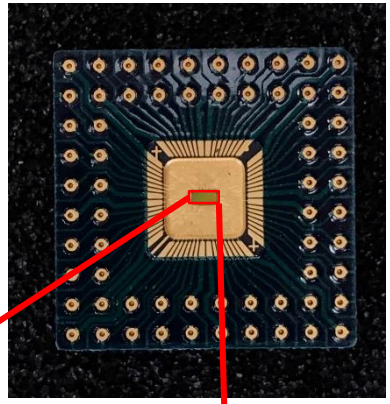
V_T1

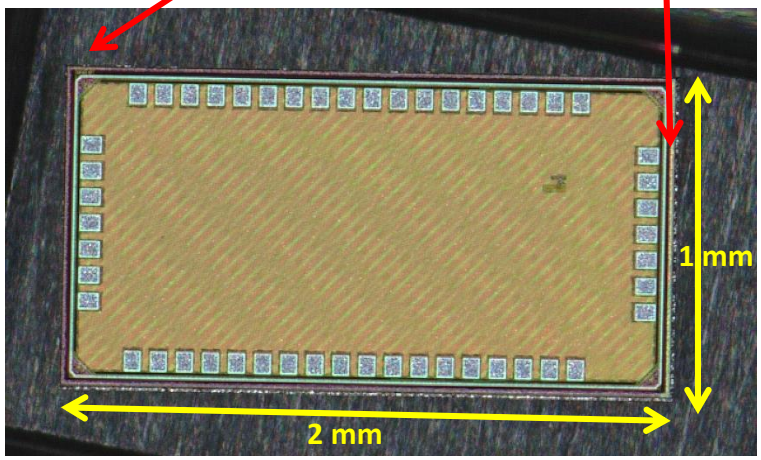
Test chip

Die package

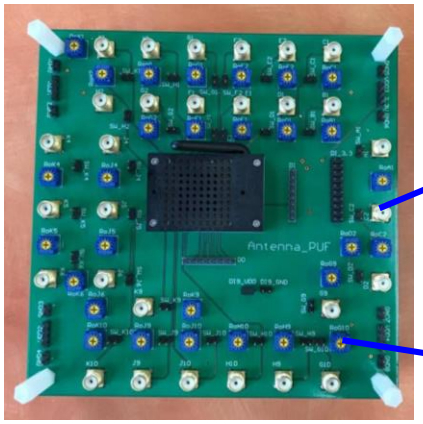


Die top view

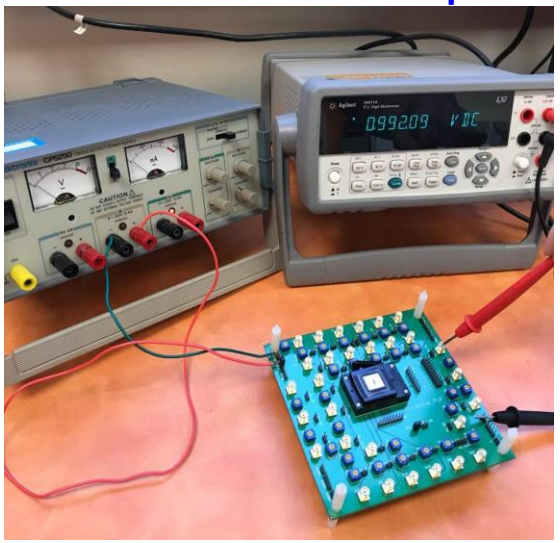




PCB

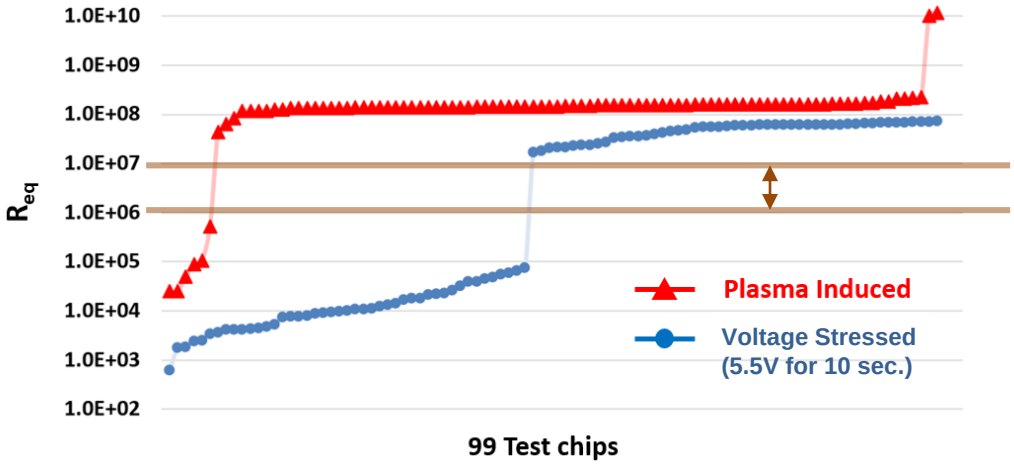


Measurement setup



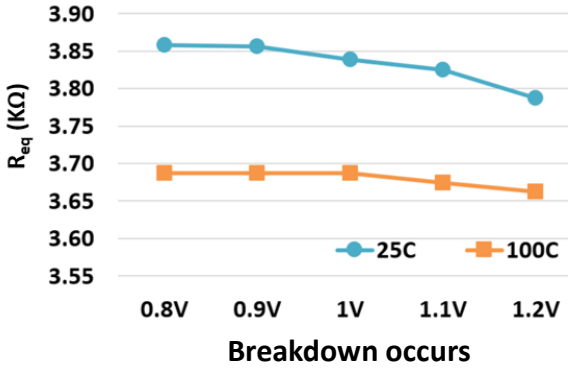
SSU R_{eq} Measurement

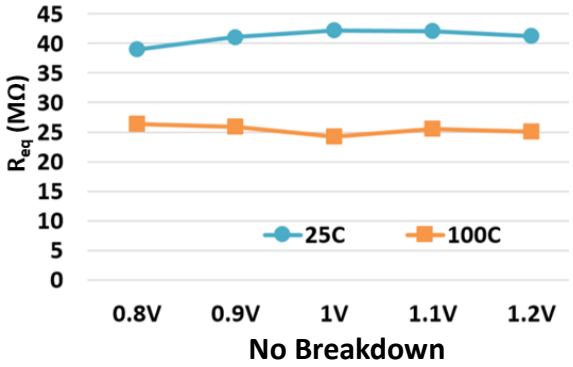
- R_{eq} of V_T1 measured at 25C, 1V



A gap in the R_{eq} distribution is observed

- R_{eq} of V_T1 measured at different corners

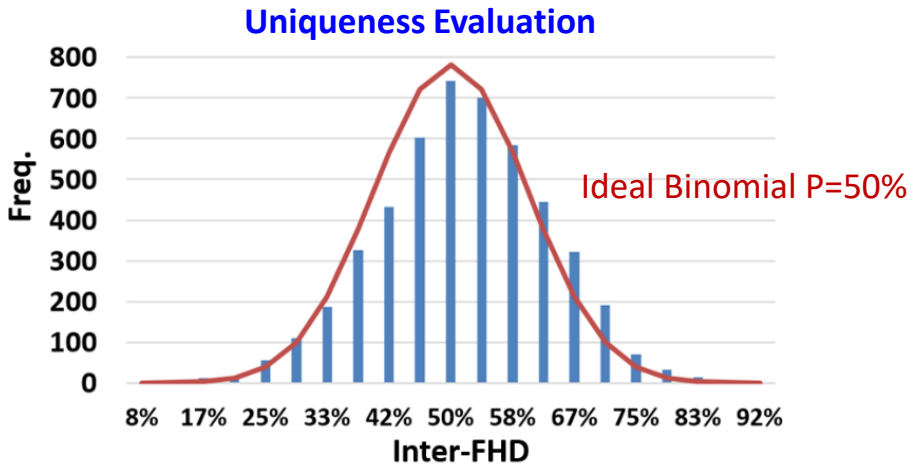




Consistent R_{eq} across corners

Breakdown Probability and Uniqueness Results

- Plasma induced breakdown probability is **much lower than 50%**
- Voltage stressed breakdown probability has **little correlation to antenna ratio**



1. **24-bit response from each of 99 test chips**
2. **Mean = 0.517, Variance = 0.013**
3. **Voltage stressed breakdown only**

Breakdown Probability

	Plasma Induced	Voltage Stressed
M_T1	0.5%	57.6%
M_T2	0.5%	51.5%
M_T3	2.5%	57.1%
M_T4	2.0%	51.0%
V_T1	0.5%	50.0%
V_T2	6.1%	54.0%
V_T3	0.0%	64.7%
V_T4	0.0%	58.6%
P_T1	1.0%	50.5%
P_T2	2.5%	51.5%
P_T3	1.0%	58.6%
P_T4	1.0%	60.0%
Test1	16.2%	N/A
Test2	2.0%	N/A
Test3	5.1%	N/A
Test4	1.0%	N/A
Test5	3.0%	N/A

Stability and Independence Results

- Each SSU is measured 10 times at different corners
- Plasma induced breakdown is **completely stable**
- Voltage stressed breakdown is not 100% stable
  - Taking majority vote eliminates the unstability

Corners	0.8V	1.0V	1.2V
25C	**0.04%**	**0.00%**	**0.12%**
100C	**0.08%**	**0.08%**	**0.08%**

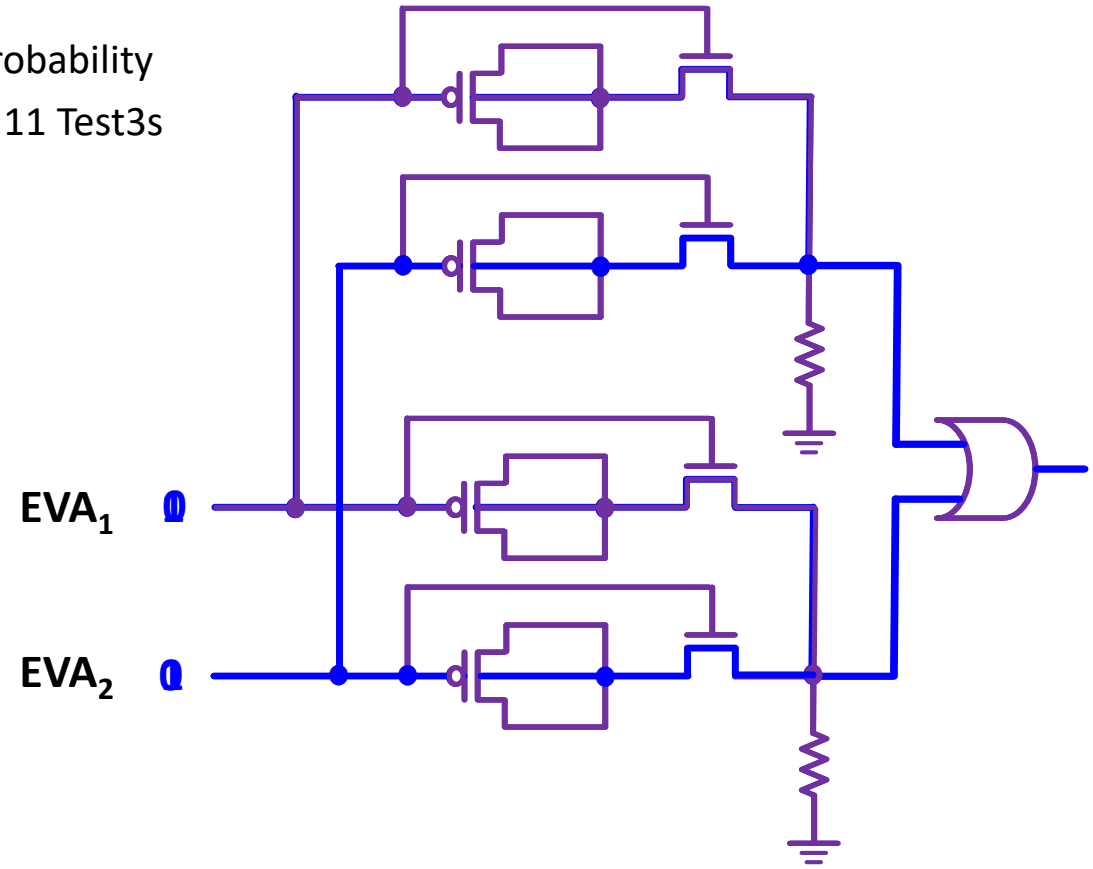
- Statistical distances measured for pairs that are
  - Next to each other
  - Having same antenna ratio

Statistical Distance	Max	Min	Mean
Kullback-Leibler	**0.11 / 0.057**	**0.0002 / 0.0001**	**0.022 / 0.015**
Total Variation Distance	**0.19 / 0.13**	**0.009 / 0.007**	**0.07 / 0.05**
Guesswork	**0.06 / 0.029**	**0.0001 / 0.00009**	**0.011 / 0.008**

(Zero means completely independent)

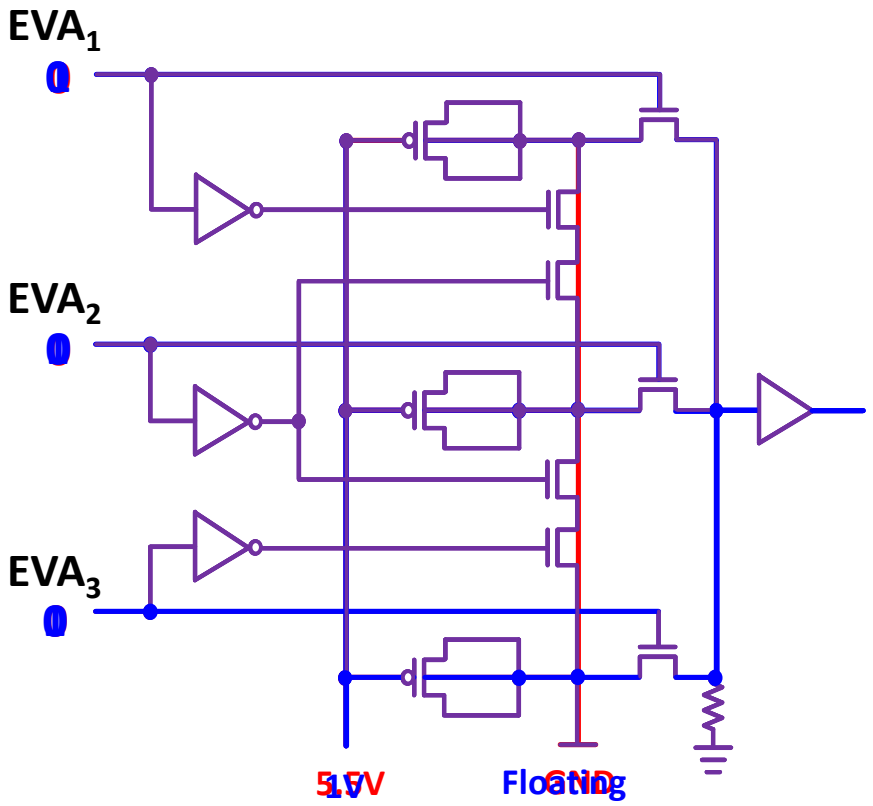
Plasma Induced Breakdown PUF

- **Precision resistor is shared amount multiple SSUs**
  - Only one EVA of the SSUs is asserted at a time
- **To generate more balanced responses, outputs of SSUs are ORed together**
  - Test3 has 5.1% breakdown probability
  - $(1\text{-}5.1\%)^{11}$ = 56% after ORing 11 Test3s
  - 3X smaller than SRAM PUF with 15% error rate
  - Completely stable



Voltage Stressed Breakdown PUF

- **Stress Phase**
  - Disable all EVAs
  - Connect SSU outputs to GND
  - Apply high voltage to the SSU gates
- **Evaluation Phase**
  - Left the SSU outputs floating
  - Apply normal voltage to SSU
  - Only on EVA is asserted at a time



Conclusion and Future Work

- **Proposed and fabricated SSUs using gate oxide breakdown**
  - Plasma induced breakdown
  - Voltage stressed breakdown
- **Test chip measurements are stable, unique, and independent**

- **Our future work includes**
  - Finding other sources of stable randomness
  - Developing applications of stability-guaranteed PUFs

Thank you!

Questions?