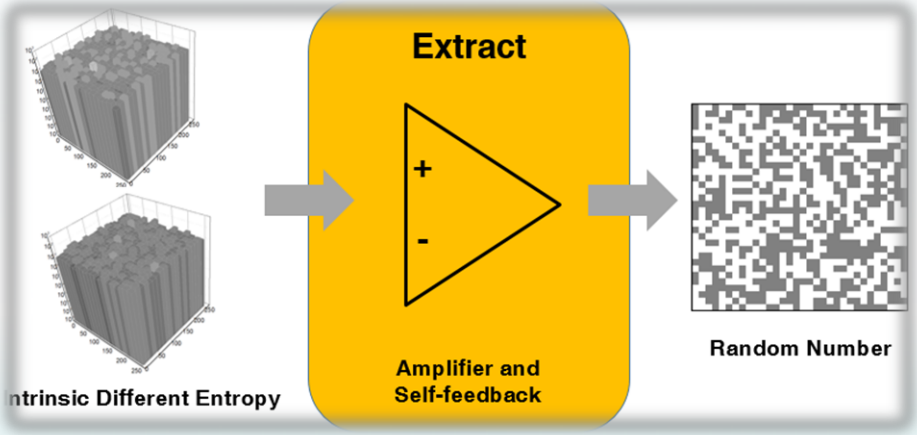
What is Physical Unclonable Functions?

Human Finger Print

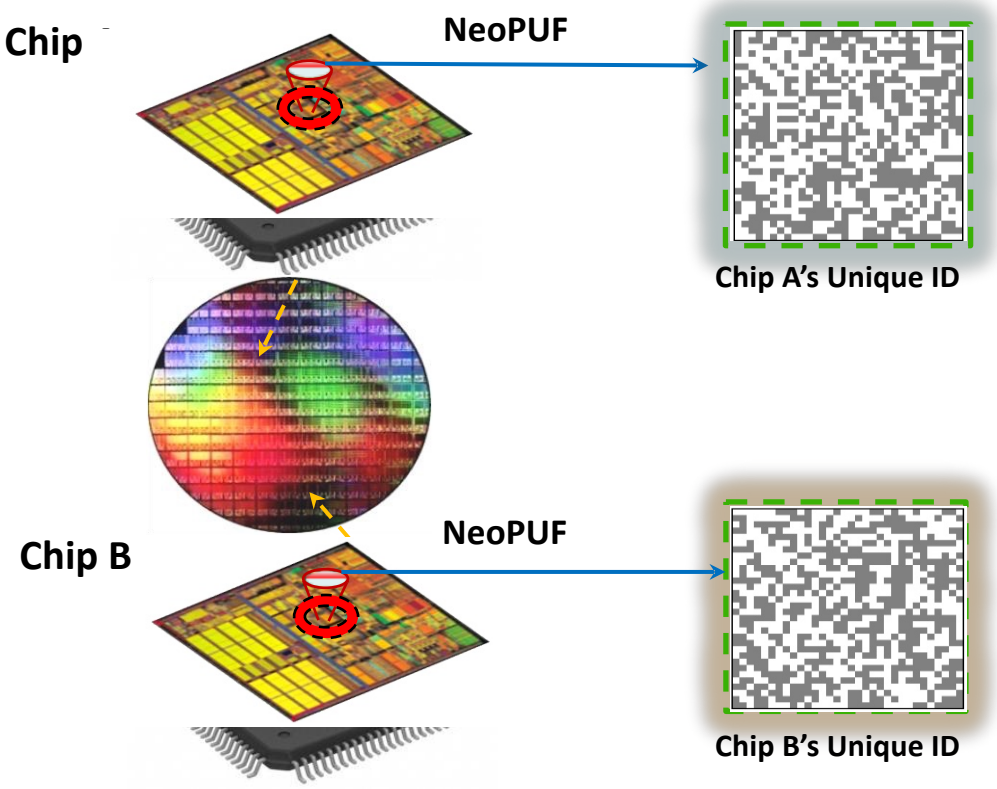
Collision Probability ≒ 1/15B ≒ $1/2^{34}$

IC Finger Print



Collision Probability = $1/2^{\text{Bits Stream Length}}$

Micor PUF - Ideal Entropy Source



Ideal Entropy Source

Physically Unclonable Function

- **Deep-rooted Root of Trust**
  Based on uncontrollable silicon manufacturing variations
- **Unclonable & Unpredictable**
  Manufacturing variations cannot be controlled or replicated
- **Chip-Unique**
  Every Chip bears its unique
  - Chip ID
  - Entropy source
- **Anti-counterfeit & Royalty countion**

NIST 800-22 Randomness Test

- **Pass the statistics randomness test based on accumulated corner samples (TT/FF/SS/SF/FS/OX+/OX-) including >3M cells.**

#	Statistical Test	Recommended n	Input Size		Sub-Test #	Decision Rule					Randonness Judgement
						Min. P-Value	Proportion		Uniformity		
		Length of bit string	n	bit stream(s)		P-Value > 0.01	mini	P/F	P-value of P-value > 0.0001	P/F	PASS/FAIL
1	Frequency	n>100	40000	75	1	-	73/75	PASS	0.238562	PASS	PASS
2	Block Frequence (m=128)	n>100	40000	75	1	-	75/75	PASS	0.72554	PASS	PASS
3	Cumulative sums - Forward	n>100	40000	75	1	-	74/75	PASS	0.519816	PASS	PASS
4	Cumulative sums - Reversed	n>100	40000	75	1	-	74/75	PASS	0.72554	PASS	PASS
5	Runs	n>100	40000	75	1	-	75/75	PASS	0.362174	PASS	PASS
6	Longest runs of ones	n>128	40000	75	1	-	75/75	PASS	0.295803	PASS	PASS
7	Binary Matrix Rank	n>38912	40000	75	1	-	73/75	PASS	0.808725	PASS	PASS
8	Spectral DFT	n>1000	40000	75	1	-	73/75	PASS	0.937294	PASS	PASS
9	Non-overlapping Templates (m=9)	n>8m-8	40000	75	148	-	71/75	PASS	0.00058	PASS	PASS
10	Overlapping Templates (m=9)	n>1E6	40000	75	1	-	75/75	PASS	0.036868	PASS	PASS
11	Serial (m=16, $\nabla\Psi m2$))	m< ($\log 2$ n)-2	40000	75	2	-	75/75	PASS	0.127498	PASS	PASS
12	Approximate Entropy (m=10)	m< ($\log_2$ n)-5	40000	75	1	-	75/75	PASS	0.339044	PASS	PASS
13	Universal	n>387840	1000000	3	1	0.341243	3/3	PASS	-	-	PASS
14	Linear complexity (M=500)	n>1E6	1000000	3	1	0.652199	3/3	PASS	-	-	PASS
15	Random Excursions	n>1E6	1000000	3	8	0.145246	3/3	PASS	-	-	PASS
16	Random Excursions Variant	n>1E6	1000000	3	18	0.036142	3/3	PASS	-	-	PASS

AIS-31 Randomness Test

- **Pass the statistics randomness test based on accumulated corner samples (TT/FF/SS/SF/FS/OX+/OX-).**

AIS-31 Statistical Tests		Minimum Length of bit string	Sub-Test #	Test Result		PASS/FAIL
P1	T0: Disjointness test	$2^{16} * 48$	1	Test T0 bestanden	Durchlauf erfolgreich beendet	PASS
	T1: Monobit test	257 * 20000	257	Test T1 bestanden	PASS (Complete and Successful)	PASS
	T2: Poker test	257 * 20000	257	Test T2 bestanden	Durchlauf erfolgreich beendet	PASS
	T3: Runs test	257 * 20000	257	Test T3 bestanden		PASS
	T4: Long run test	257 * 20000	257	Test T4 bestanden		PASS
	T5: Auto-correlation test	257 * 20000	257	Test T5 bestanden	PASS (Complete and Successful)	PASS
P2	T6a: Uniform distribution test	100000	1	Testprozedur T6a bestanden	Durchlauf erfolgreich beendet PASS (Complete and Successful)	PASS
	T6b: Uniform distribution test	100000	1	Testprozedur T6b bestanden		PASS
	T7a: Homogeneity test	100000	2	Testprozedur T7a bestanden		PASS
	T7b: Homogeneity test	100000	4	Testprozedur T7b bestanden		PASS
	T8: Entropy estimation test	7200000	1	Test T8 bestanden		PASS

What We Achieve

Metrics	Check by	Micor PUF	Ideal
Randomness	Hamming Weight (HW)	50%	50%
Uniqueness	Hamming Distance (HD)	50%	50%
Stability	Bit-Error-Rate (BER)	0	0
Repeatability/ Identifiability	Intra-ID HD	0	0
Productivity	Processes compatibility Yield & reliability	All Verified Corners Qualification Pass	Producible

Comparison

Tech.	SRAM PUF		PUF	Benchmark
	RAW SRAM	with NVM Helper		
Key Pool (bit)	>16k	256	64Kb	64Kb or higher
Bit Error Rate	15%~30%	0	0	Stable; No Aging
Help Algorithm	Voting, Pre-Burn, ECC		No	No Helper
Inter/Intra HD	6	∞	∞	∞
NIST800-22	Partial		PASS	PASS
Op. Temp.	<85^{0}C		-40~175^{0}C	Auto Grade