Cyberday 2015

יום עיון בסייבר ואבטחת מידע

Scan Side Channel Analysis: a New Way for Non-Invasive Reverse Engineering of a VLSI Device

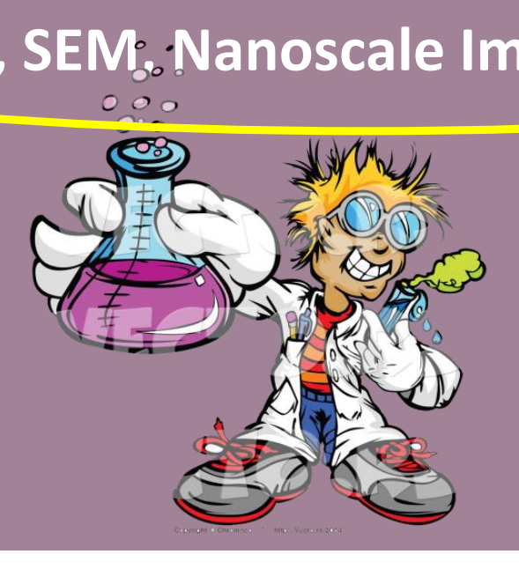
Leonid Azriel, Avi Mendelson, Ran Ginosar

Electrical Engineering, Technion - Israel Institute of Technology

Reverse Engineering of an ASIC – State of the Art

Phase 1 Invasive - ASIC to Circuit

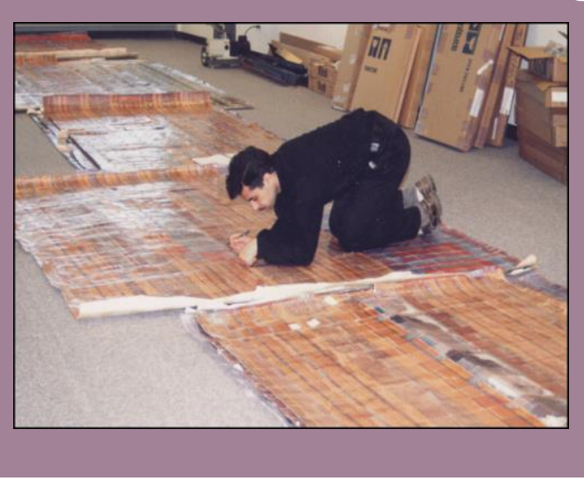
Delayering, SEM, Nanoscale Imaging, Cross-section



Our Target

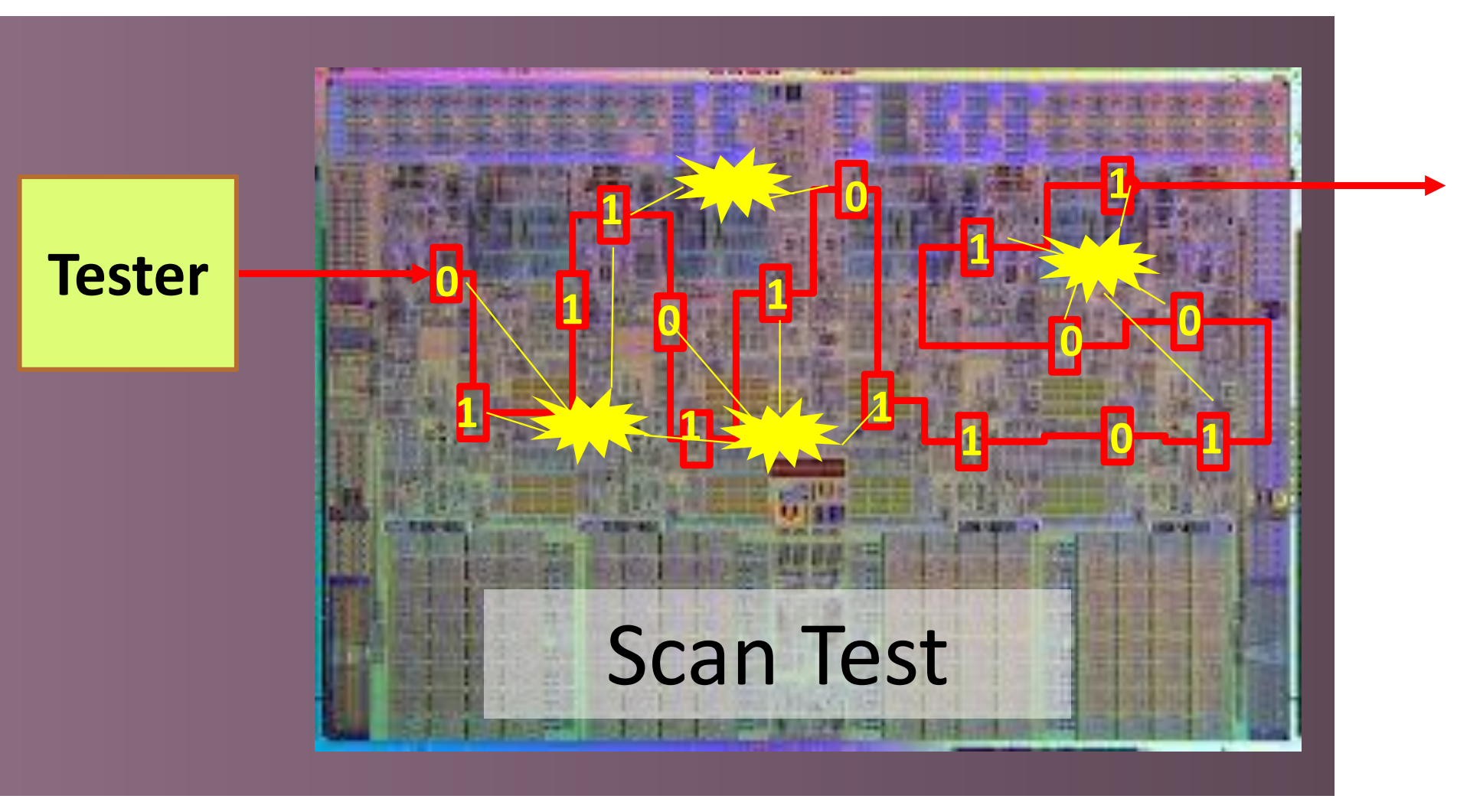
Phase 2 Algorithmic – Circuit to Spec

FSM Extraction, Model checking, SAT

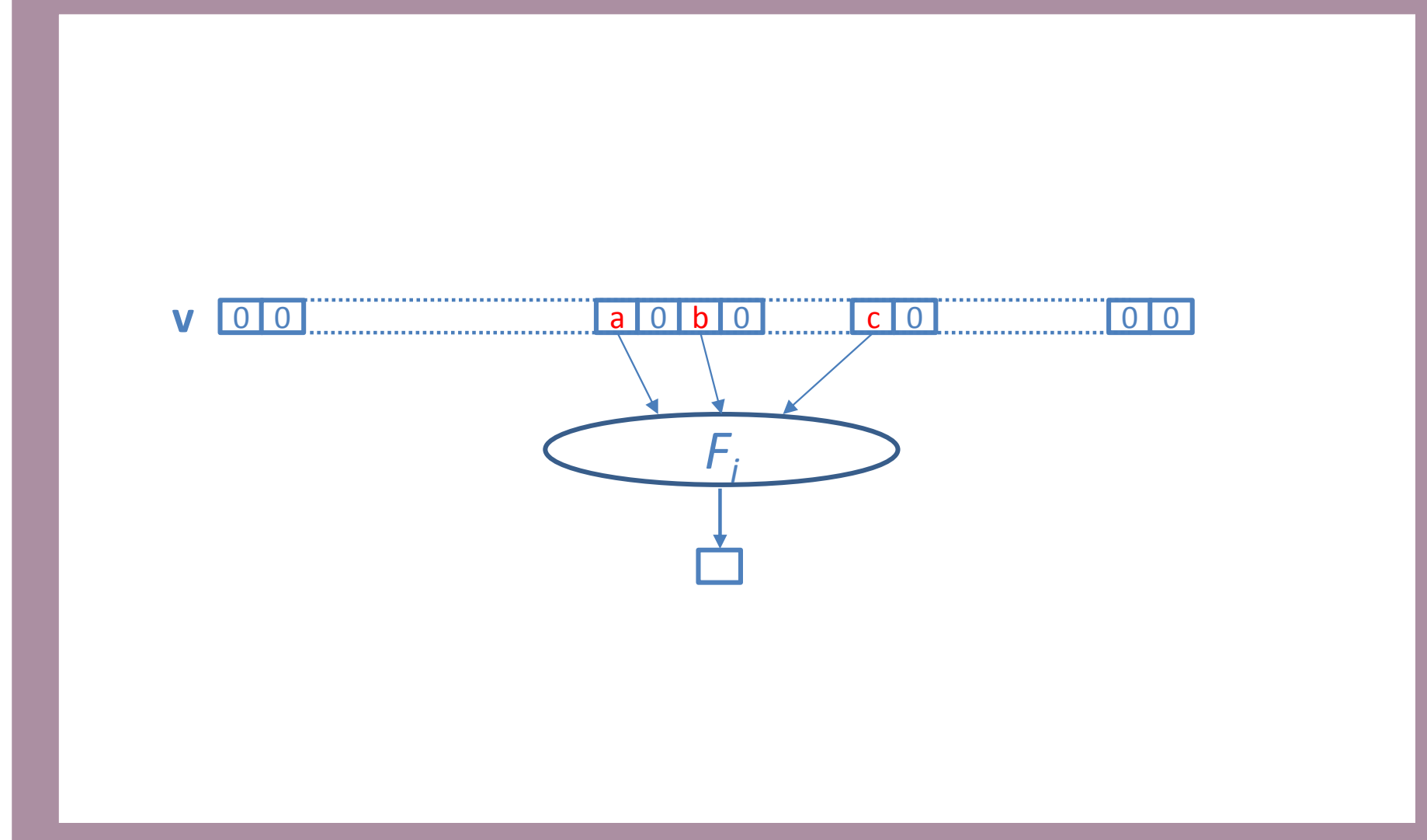


The Scan Technique

- Designed to automate production test
- Chains all memory elements in a shift register
- The tester verifies correctness by
  1. Setting the device state (Shift-In)
  2. Running one cycle (Capture)
  3. Reading the next state (Shift-Out)



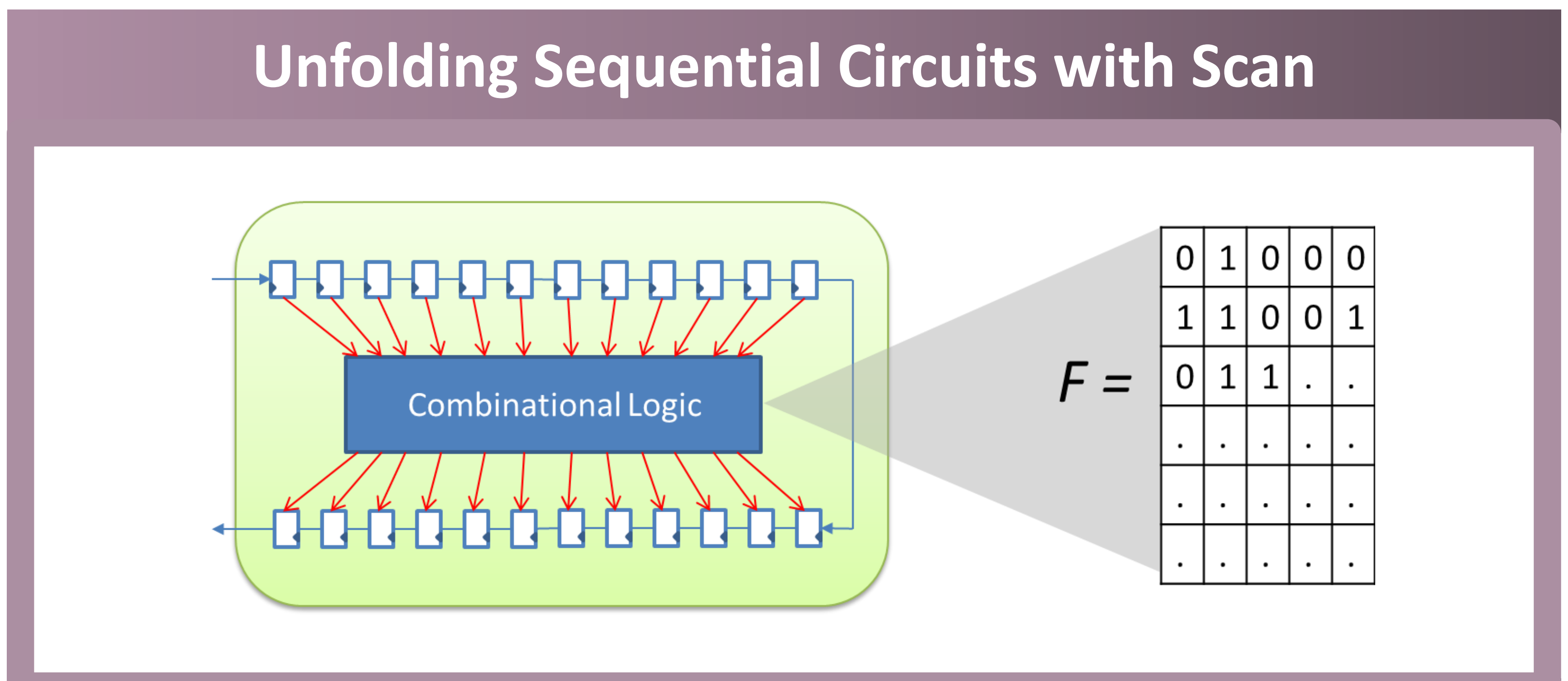
Algorithm for Limited Transitive Fan-in (K)



- Suppose *F*(0) = 0 (simple extension to any *F*)
- Example for K = 3
- Testing all values of input v with Hamming Weight 3 or less covers all combinations of {a,b,c}
- Runtime ~ n^K

- Computational complexity theory has more efficient algorithms for learning limited fan-in functions or Junta functions
- Runtime complexity: $O(n*2^k)$
- Scalable – can be applied to large scale devices
- Still exponential growth with K.

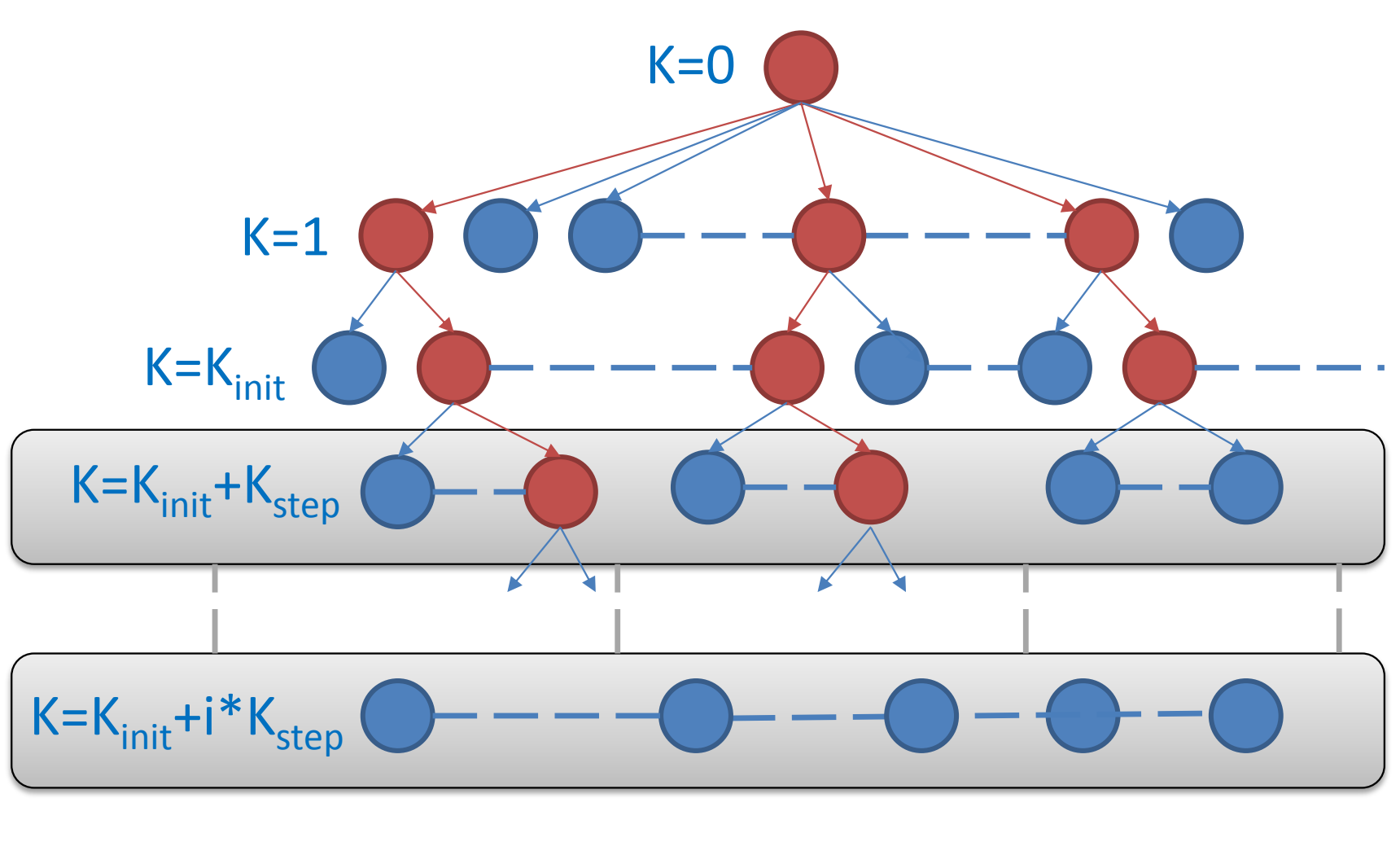
Unfolding Sequential Circuits with Scan



0	1	0	0	0
1	1	0	0	1
0	1	1	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

- Scan turns the ASIC to a stateless circuit
- Mapped to the Boolean Function Learning problem: $\{0,1\}^n \rightarrow \{0,1\}^n$
- Exhaustive Search: Extract the Truth Table by running queries for all inputs
- Exponential Size: 2^n

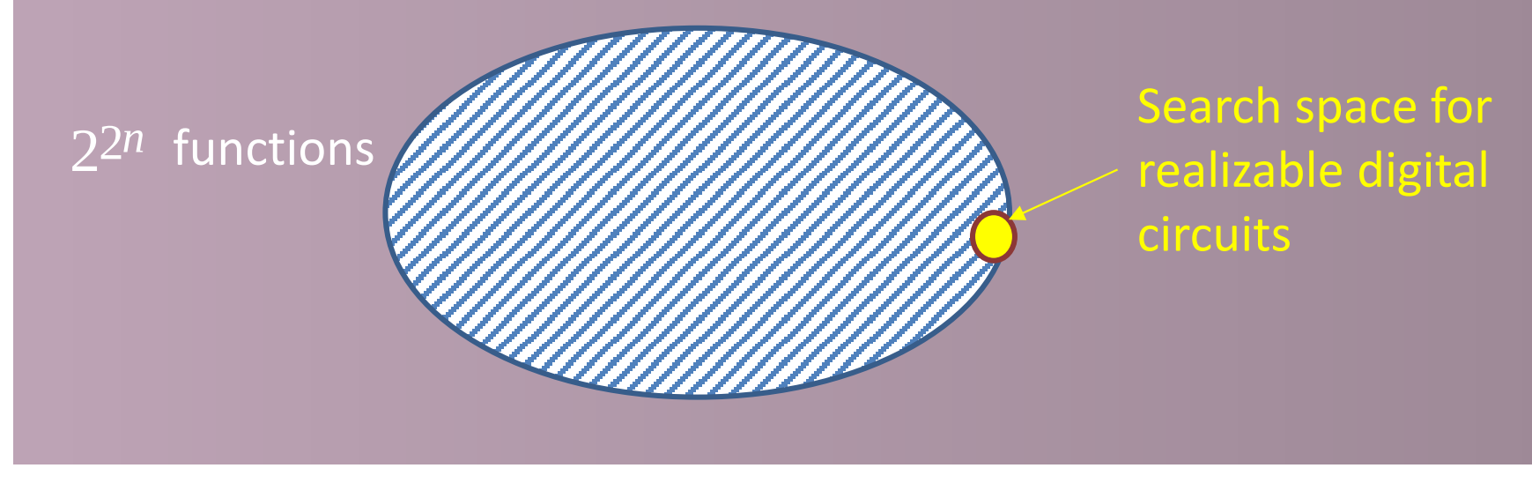
Heuristic Based Incremental Search



- Best First Approach
- When reached computational limit (large K) continue only the winning paths of the tree
- Expand already discovered implicants to new vectors
- Very efficient for arithmetic circuits (carry propagation)

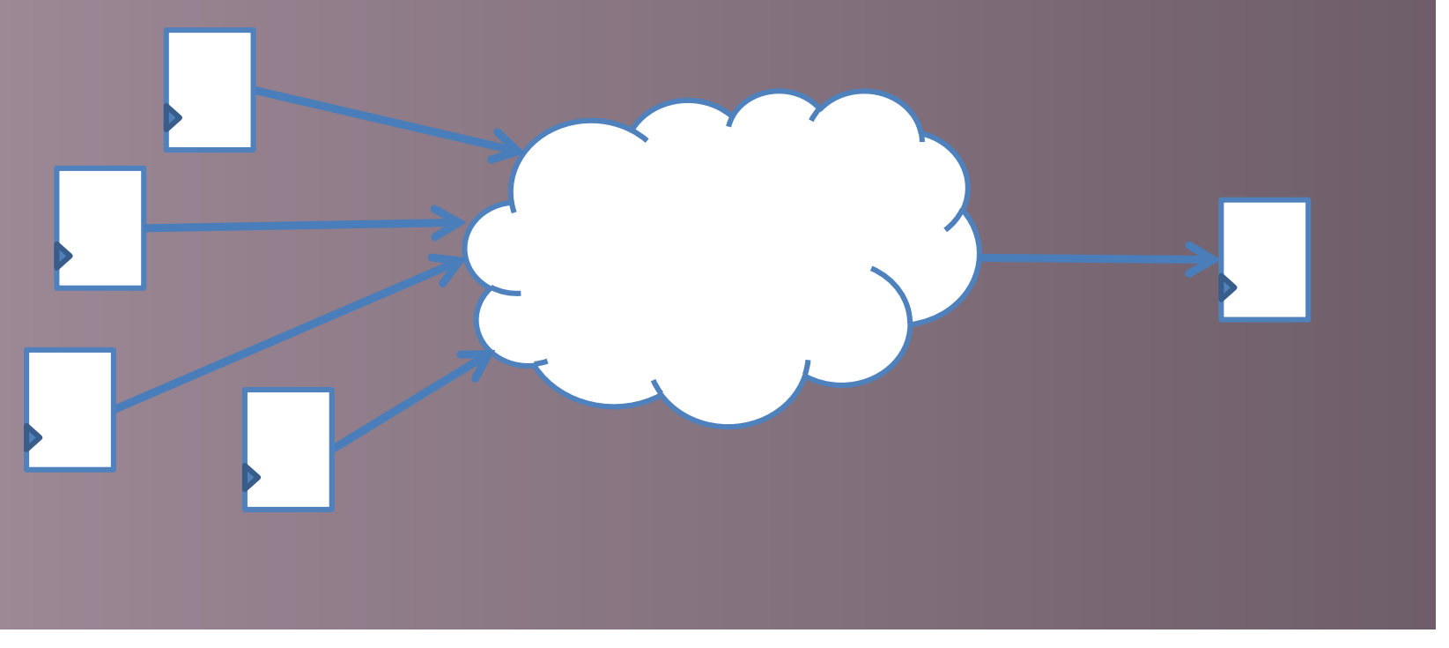
Shannon Effect

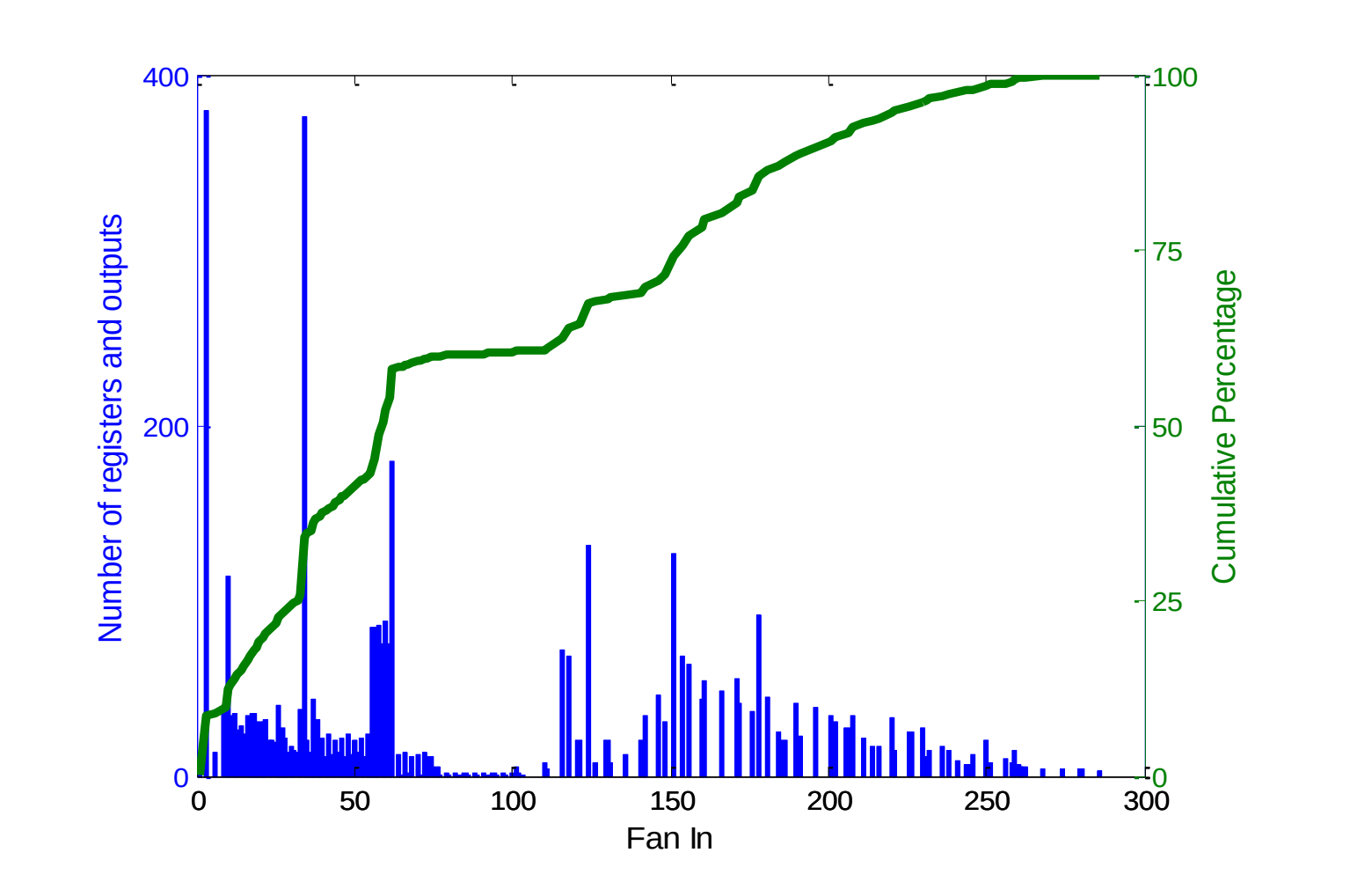
- Shannon Effect: "almost all" Boolean functions have a complexity close to the maximal possible (*~O(2ⁿ)*) for the uniform probability distribution
- Corollary: For large n, "almost all" Boolean functions are not realizable in VLSI technology



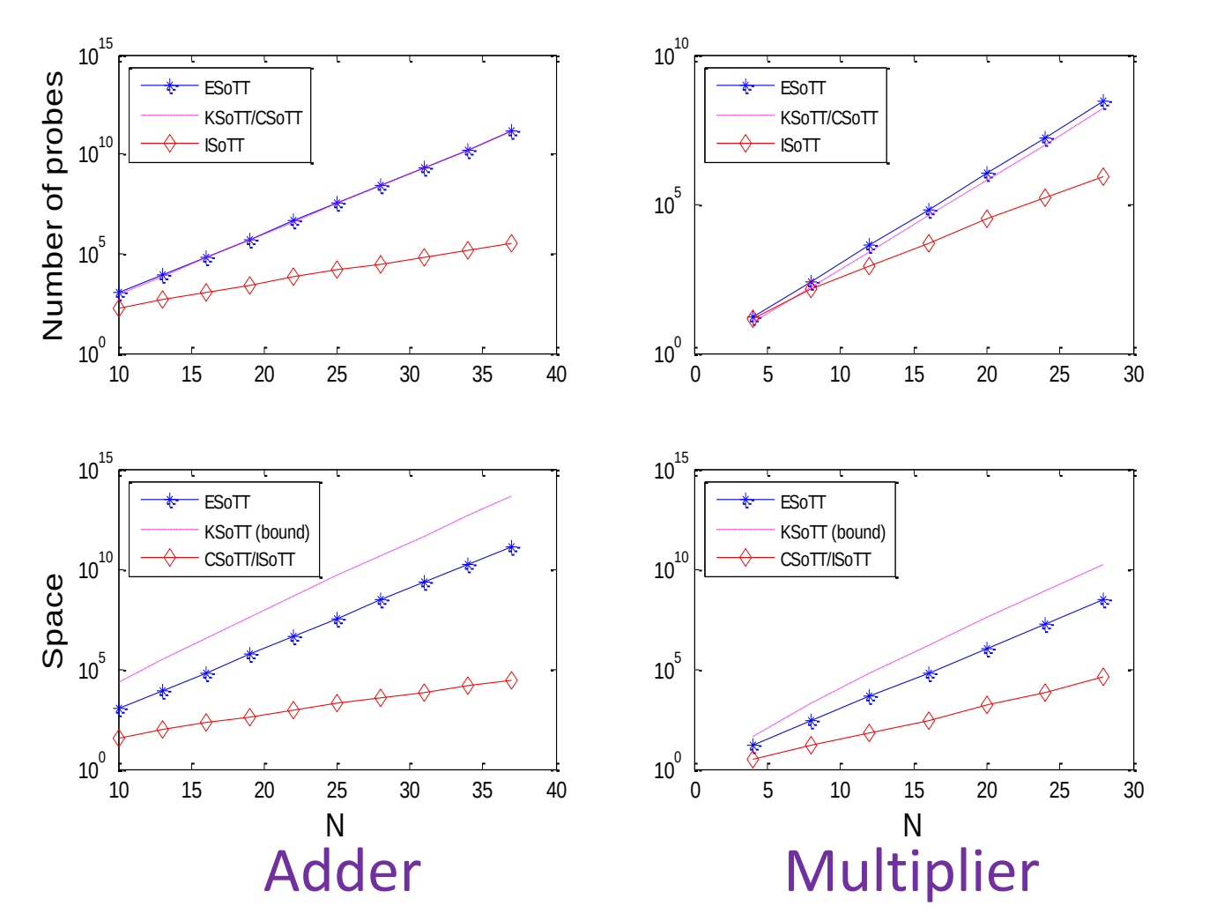
Limited Transitive Fan-in

- In practice, logic cones have limited number of inputs: Transitive Fan In = K





Transitive Fan-in Statistics for ITC'99 benchmark



Example: Arithmetic Circuits

Successfully reconstructed a full AES engine with 6K registers

What Next

- Find ways to learn high fan-in functions
  - Machine Learning
  - Special function classes (e.g. linear)
- Overcoming practical limitations
  - Compression
  - Masking
  - NPN transformations
  - Non-scan logic
- Protection methods
  - Hide the function without sacrificing testability
- Finding Hardware Trojans
  - Detecting mismatches with scan

TCE

technion computer engineering center