Overview of Algorithmic Methods in IC Reverse Engineering

Leonid Azriel

Technion

Hiroshi Fujiwara Cyber Security Research Center

Outline

Hiroshi Fujiwara Cyber Security Research Center

- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

Ethics of Reverse Engineering

Kasch, "The Semiconductor Chip Protection Act: Past, Present, And Future."High Technology Law Journal 7, 1992

Ethics of Reverse Engineering

- Semiconductor Chip Protection Act (US) 1984 allows reverse engineering of commercial semiconductor products for **educational purposes**

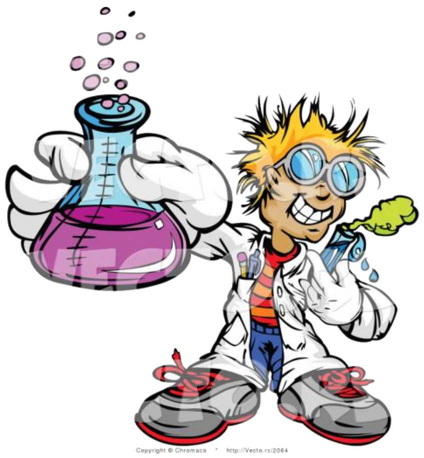
- Ethical goals
  - Detect vulnerabilities that allow reverse engineering and propose countermeasures
  - Explore legitimate usages of the reverse engineering for defense
    - Hardware Trojans detection
    - IP theft detection

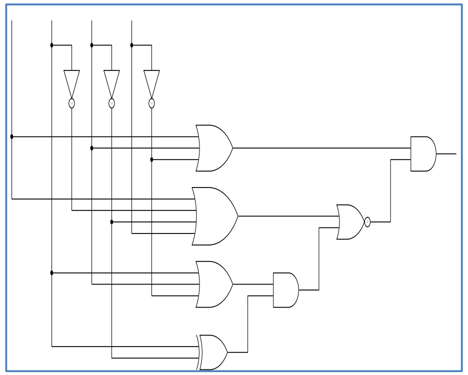
Kasch, "The Semiconductor Chip Protection Act: Past, Present, And Future."High Technology Law Journal 7, 1992

Reverse Engineering of an IC

Hiroshi Fujiwara Cyber Security Research Center

Netlist





Phase 1 IC → Circuit

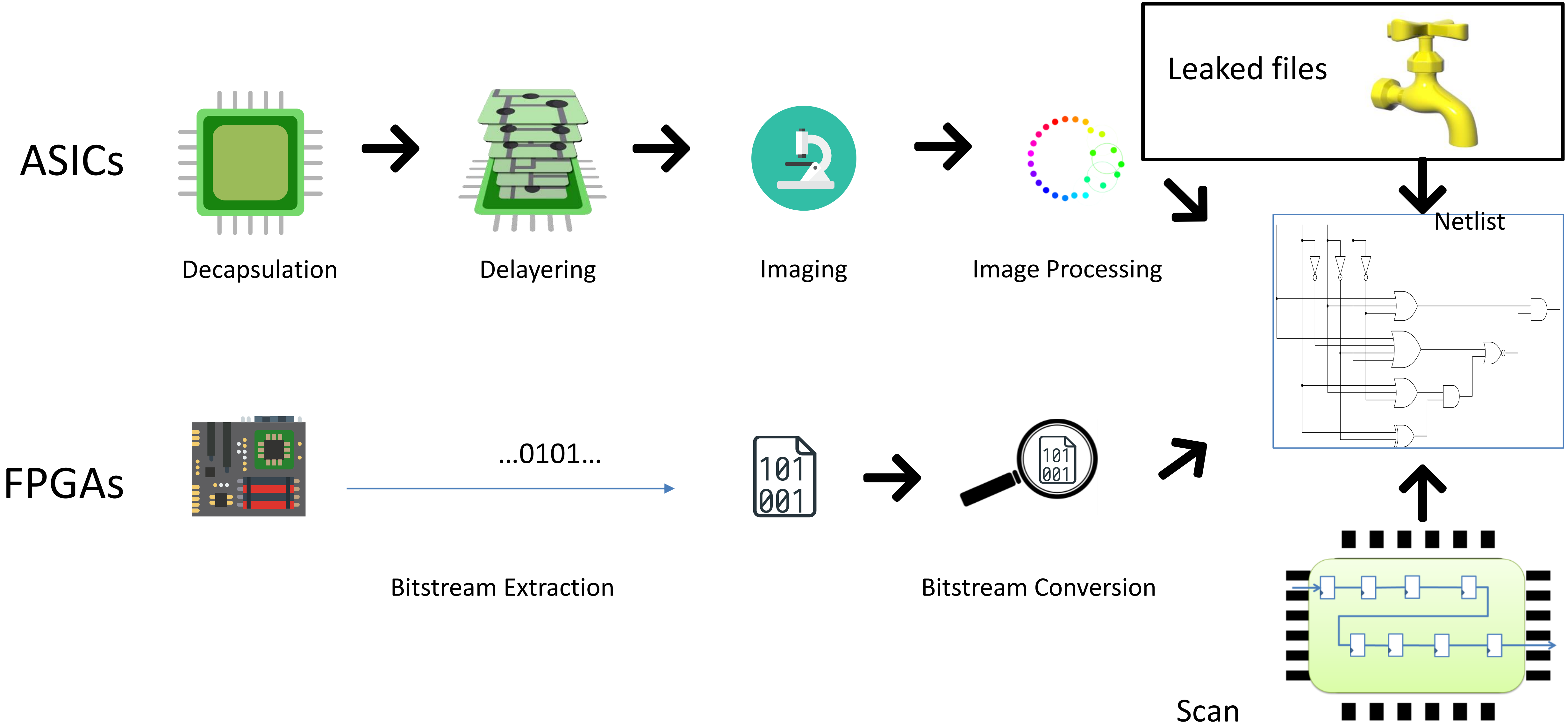
Phase 2 Circuit → Spec

Outline

Hiroshi Fujiwara Cyber Security Research Center

- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

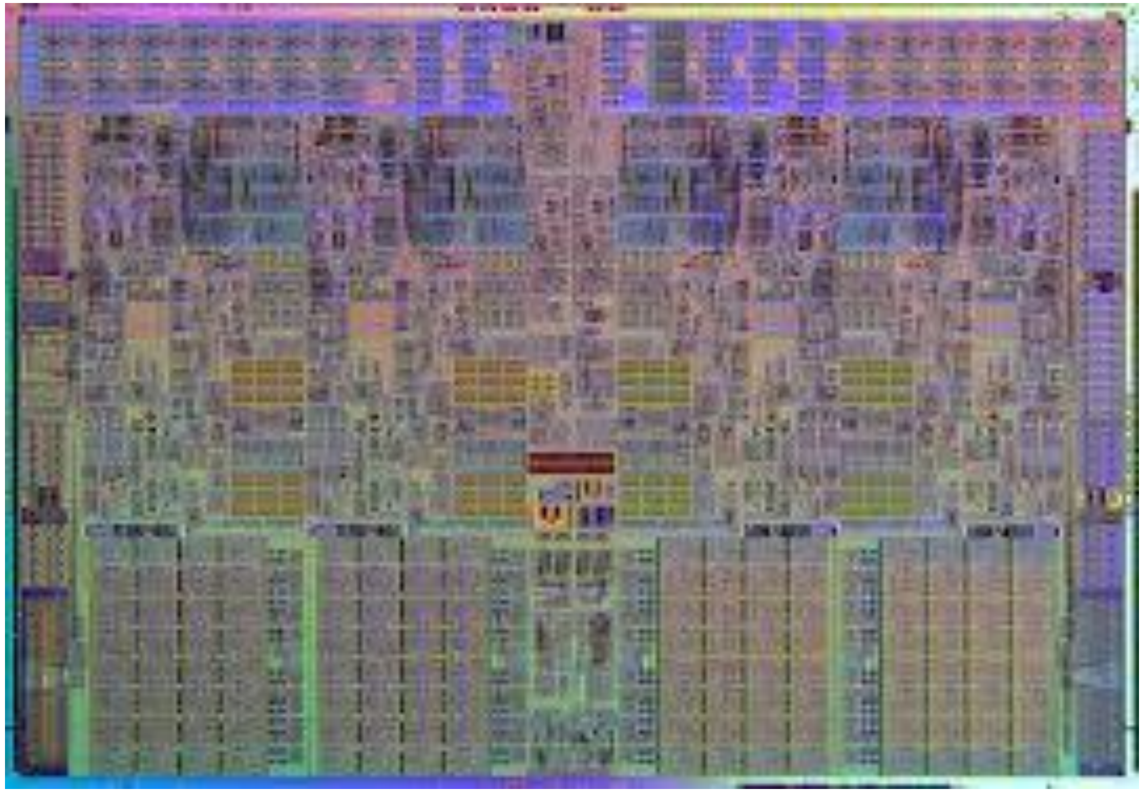
Netlist Extraction



Ender et al, Insights into the Mind of a Trojan Designer. The Challenge to Integrate a Trojan into the Bitstream," ASP-DAC 2019

The Scan Technique

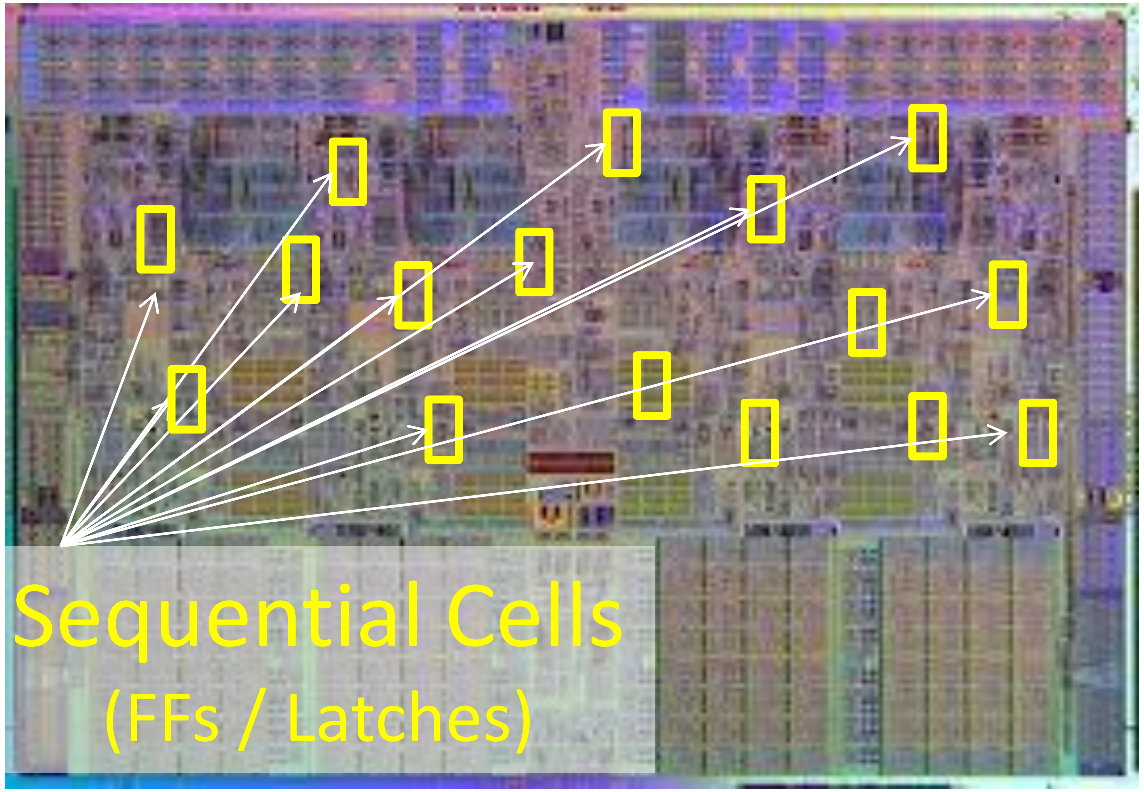
Hiroshi Fujiwara Cyber Security Research Center



Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

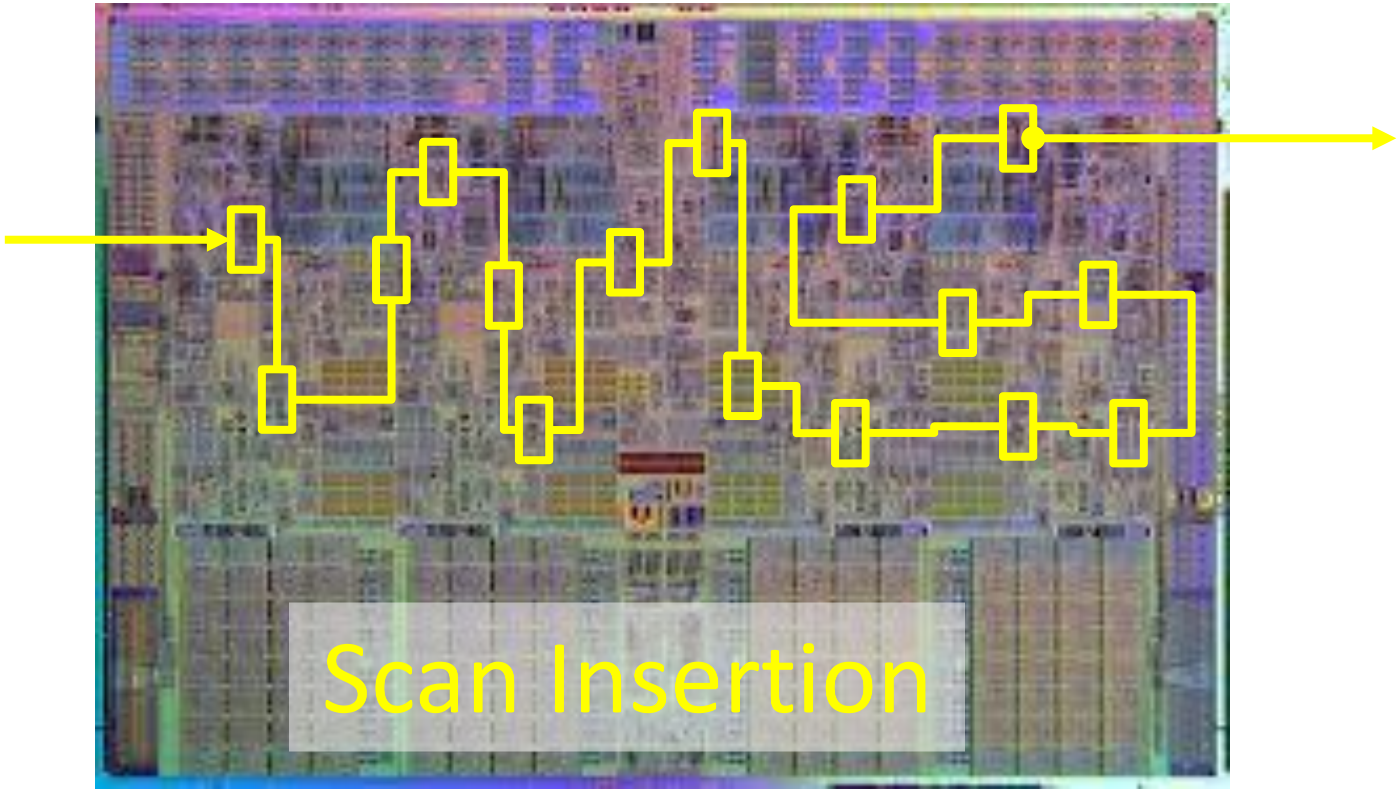
The Scan Technique

Hiroshi Fujiwara Cyber Security Research Center



Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

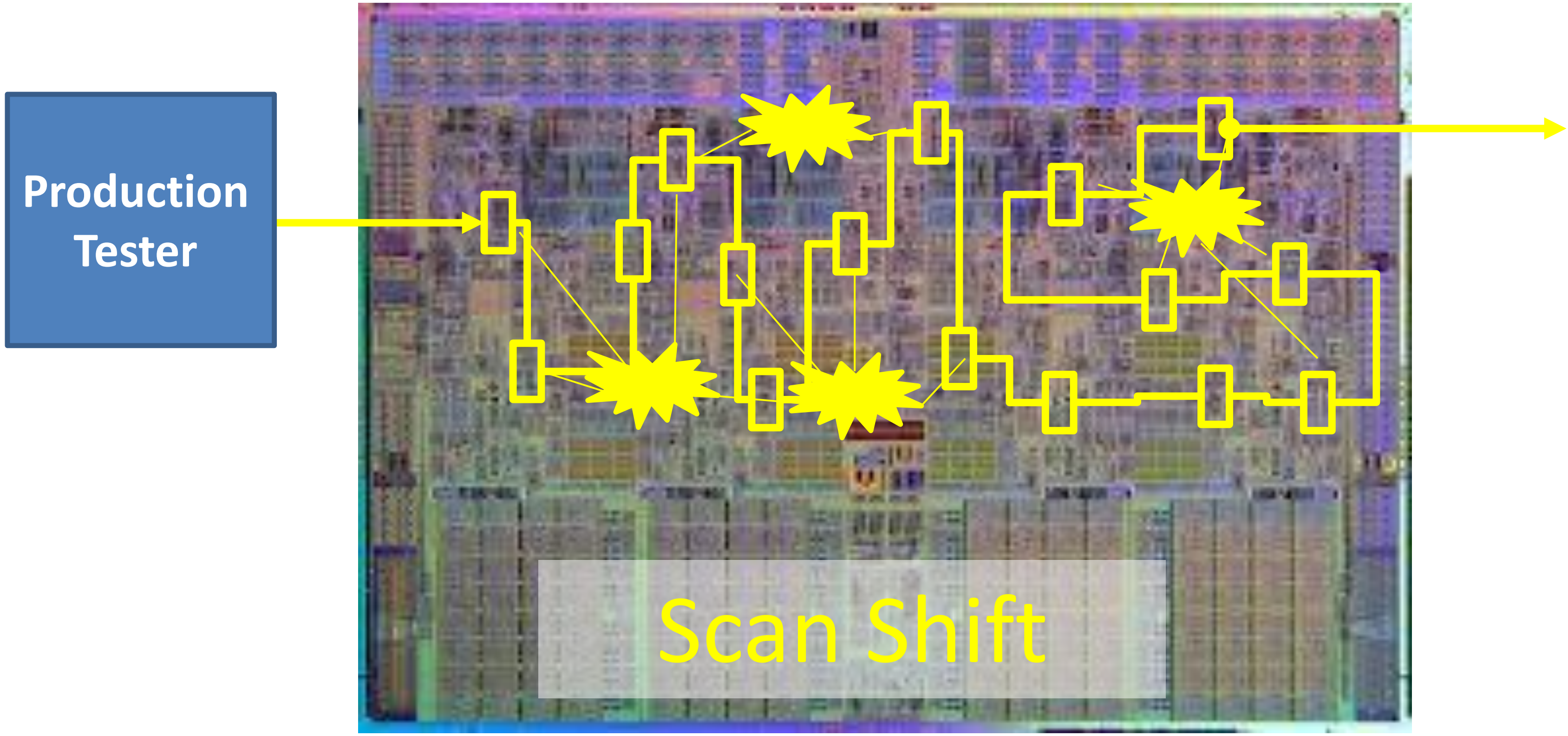
The Scan Technique



Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

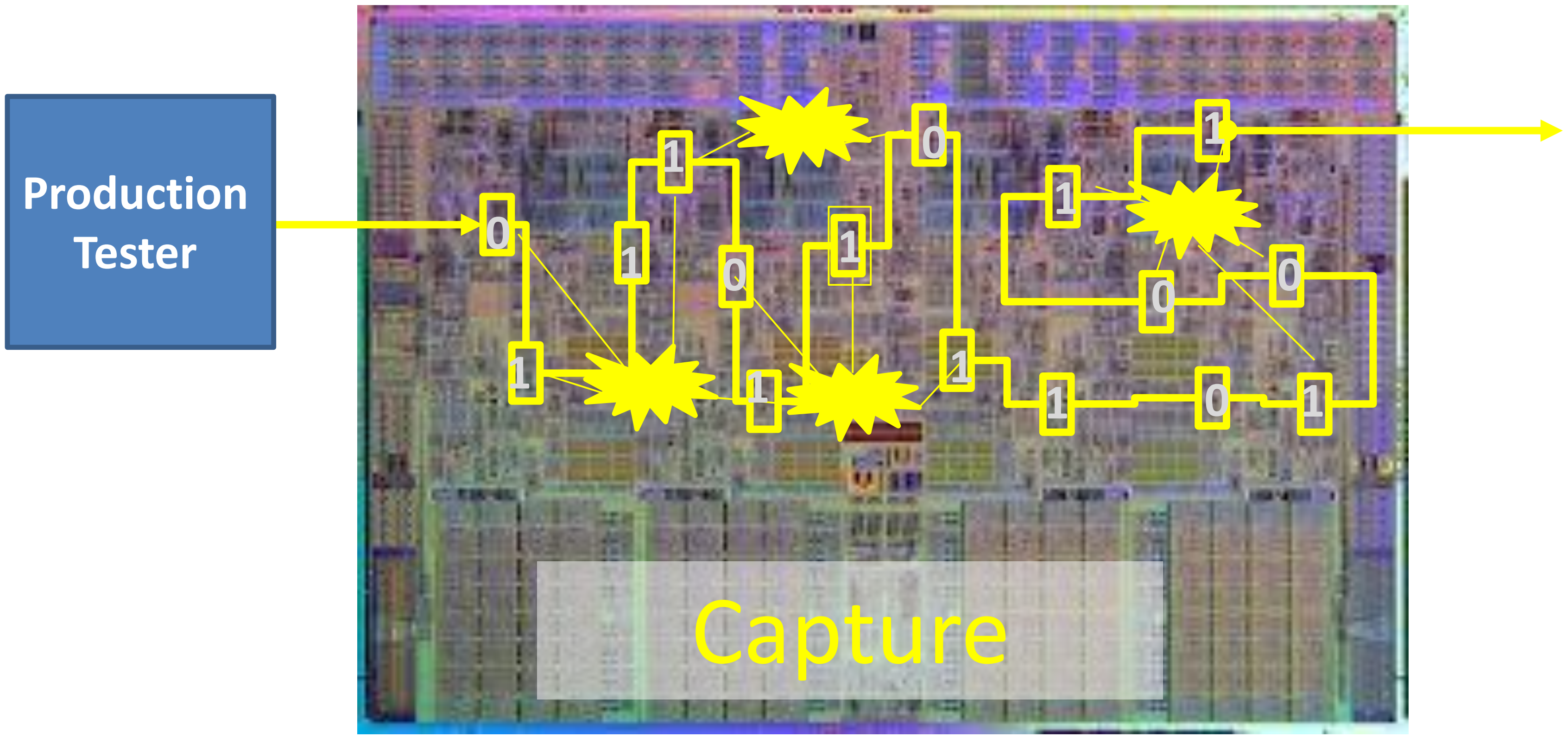
The Scan Technique

Hiroshi Fujiwara Cyber Security Research Center



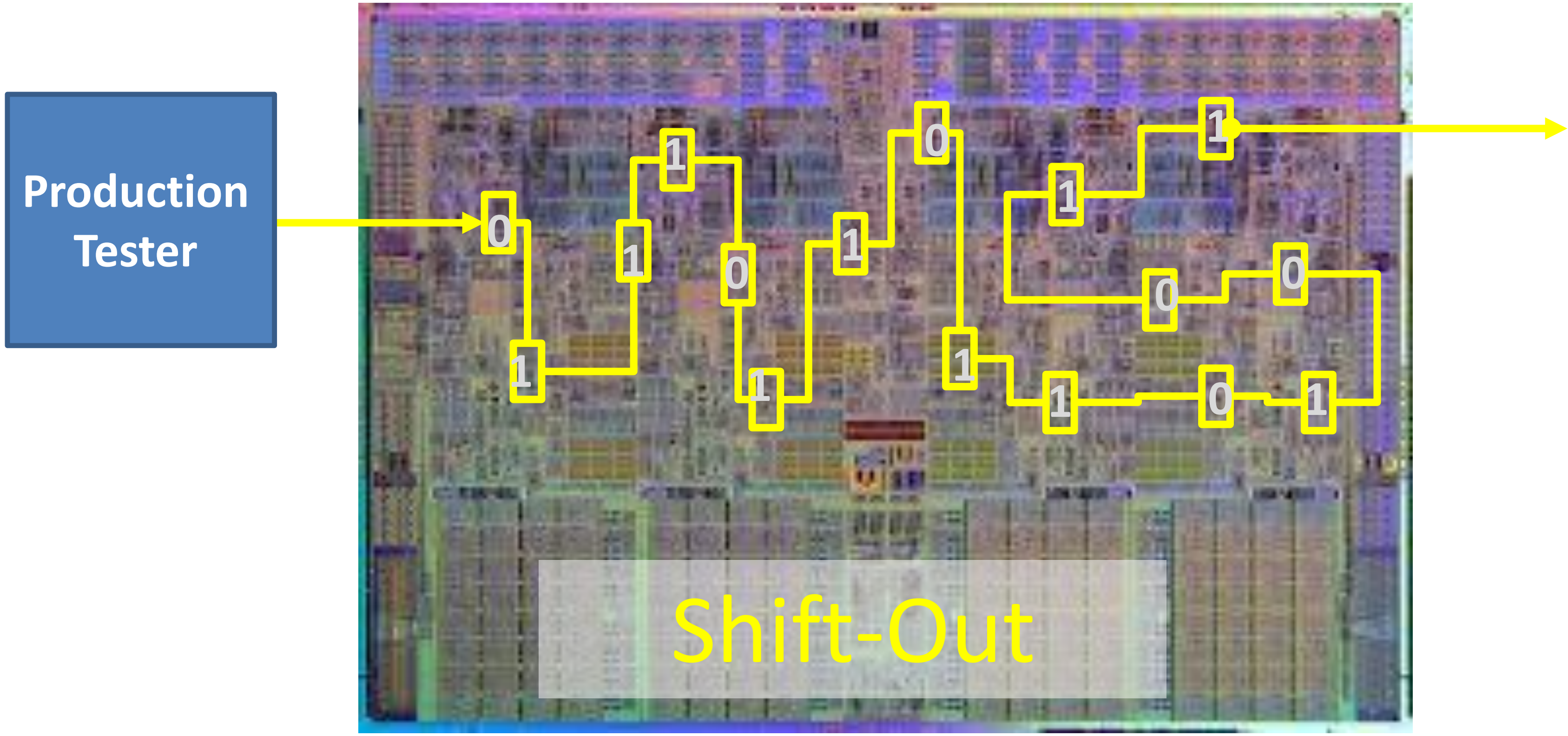
Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The Scan Technique



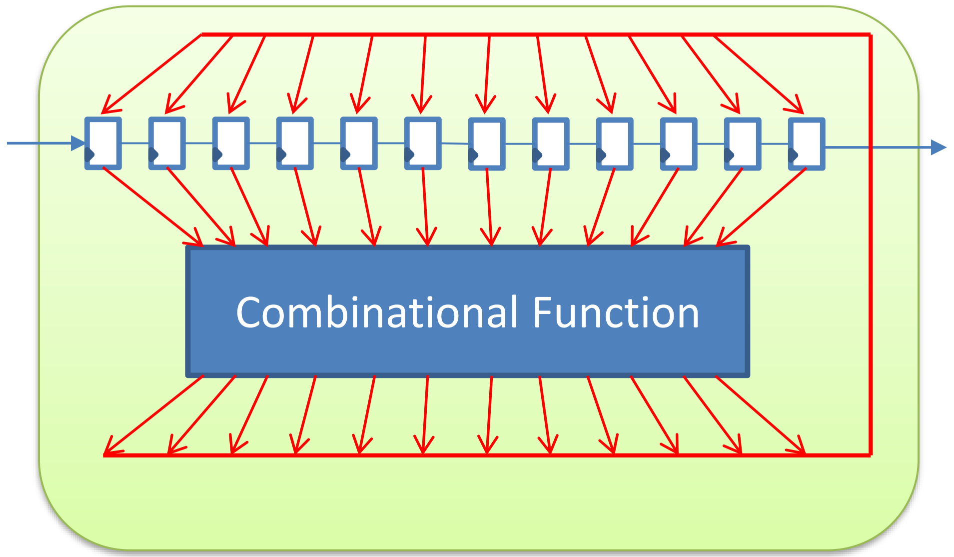
Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The Scan Technique



Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

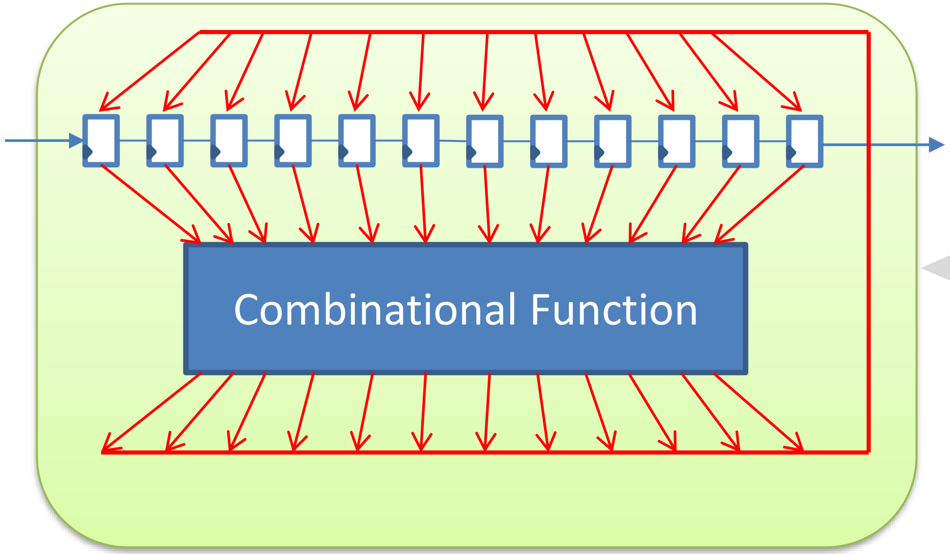
Unfolding Sequential Circuits with Scan



- Scan turns the IC to a stateless circuit
- Mapped to the Boolean Function Learning problem: $\{0,1\}^n \rightarrow \{0,1\}^n$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Unfolding Sequential Circuits with Scan



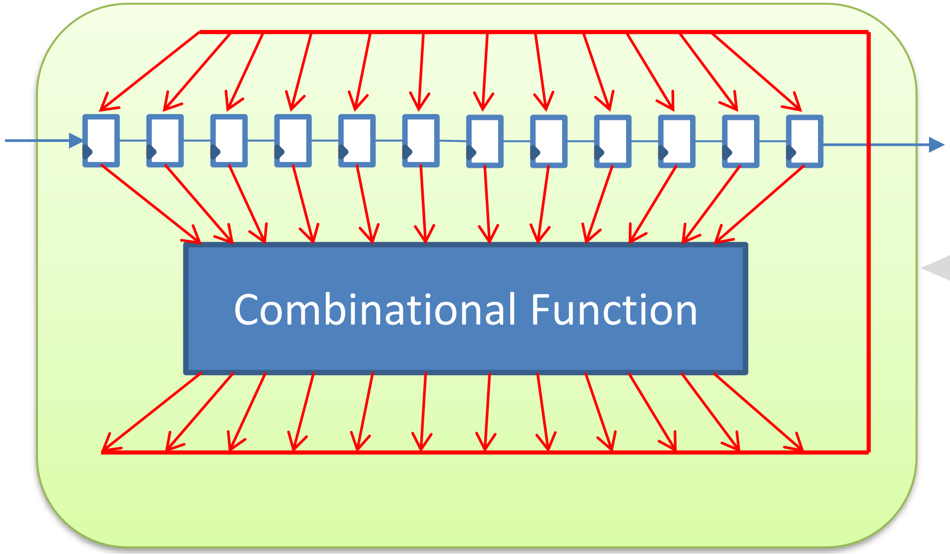
F =

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

- Scan turns the IC 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

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Unfolding Sequential Circuits with Scan



F =

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

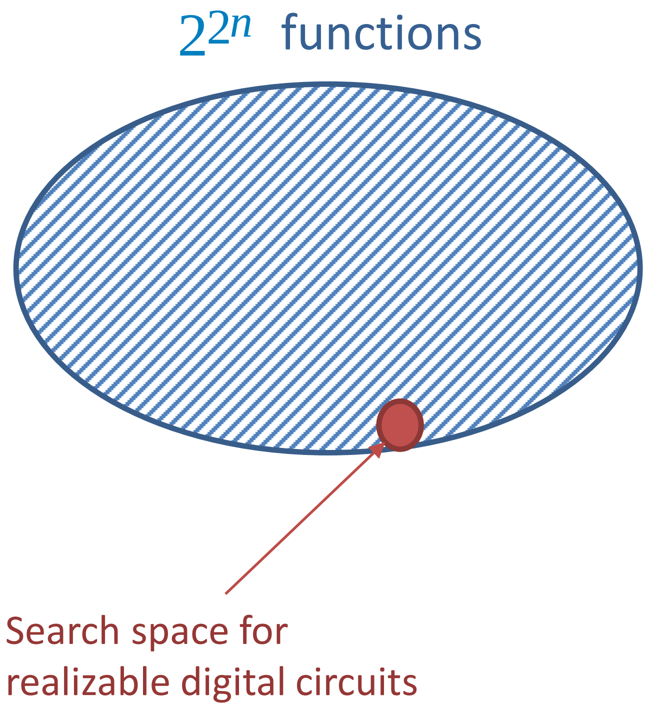
- Scan turns the IC to a stateless circuit
- Mapped to the Boolean Function Learning problem: $\{0,1\}^n \rightarrow \{0,1\}^n$
- Exhaustive Search: Extract the Truth Table by running queries for all inputs
- Exponential Size: 2^n

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Shannon Effect

- Shannon Effect: "almost all" Boolean functions have a complexity close to the maximal possible *(~O(2^n))* for the uniform probability distribution

- Corollary: For large n, "almost all" Boolean functions are not realizable in VLSI technology

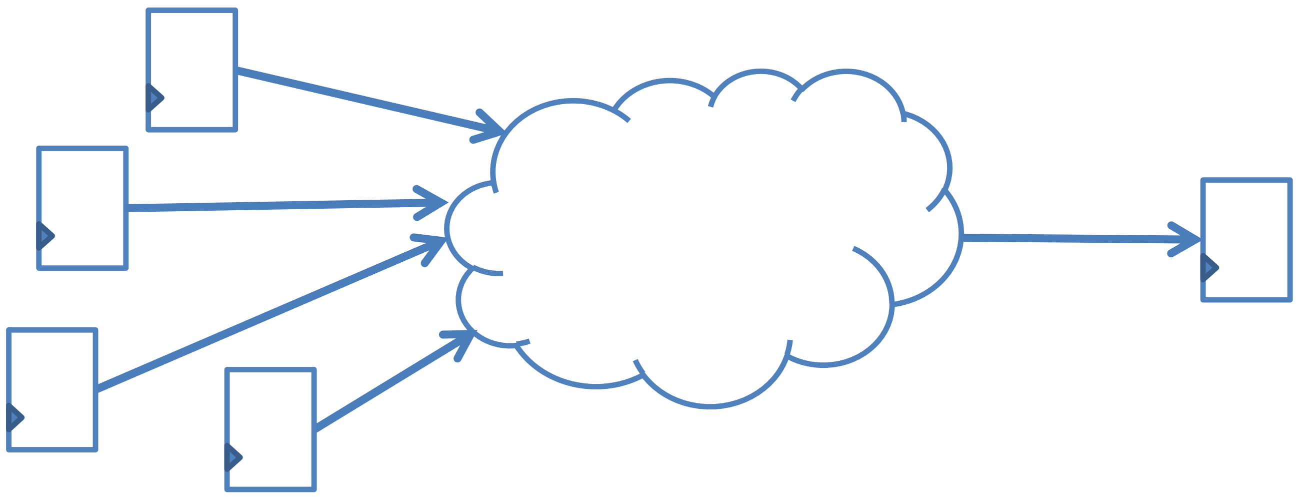


Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Limited Transitive Fan-in

Hiroshi Fujiwara
Cyber Security
Research Center

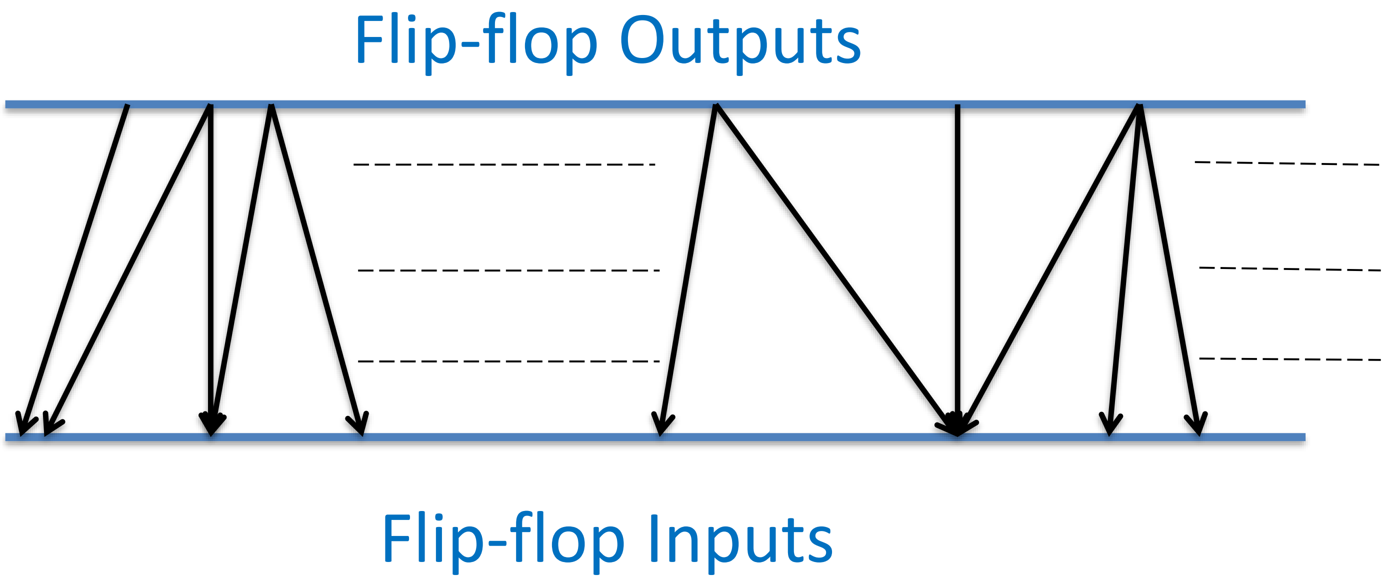
- In practice, logic cones have limited number of inputs:
  Transitive Fan In = K



Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Dependency Graph

Hiroshi Fujiwara Cyber Security Research Center



- Bipartite graph represents flip-flop dependencies
- The goal: Find dependencies
- Complexity: $2^n \rightarrow 2^k$: Scalable with the chip size

The K-Junta Algorithm

Hiroshi Fujiwara Cyber Security Research Center

$$y = f(\vec{x}), \vec{\mathrm{x}} = \{x_1, x_2, \ldots, x_i, \mathrm{x}_{i+1} \ldots, x_j, \ldots, x_n\}$$

Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

The K-Junta Algorithm

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

Generate random queries $y = f(\vec{x})$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The K-Junta Algorithm

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

Generate random queries $y = f(\vec{x})$

$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The K-Junta Algorithm

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The K-Junta Algorithm

Hiroshi Fujiwara Cyber Security Research Center

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The K-Junta Algorithm

Hiroshi Fujiwara Cyber Security Research Center

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 1$$

$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

The K-Junta Algorithm

Hiroshi Fujiwara Cyber Security Research Center

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 1$$

Relevant Variable

$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

Azriel, “Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering,” *GLSVLSI 2017*

The K-Junta Algorithm

Hiroshi Fujiwara Cyber Security Research Center

$$y = f(\vec{x}), \vec{x} = \{x_1, x_2, \ldots, x_i, x_{i+1} \ldots, x_j, \ldots, x_n\}$$

$$\vec{a} = \{0, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 0, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 0, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 0$$

$$\vec{a} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 0\}, f(\vec{a}) = 1$$

Relevant Variable

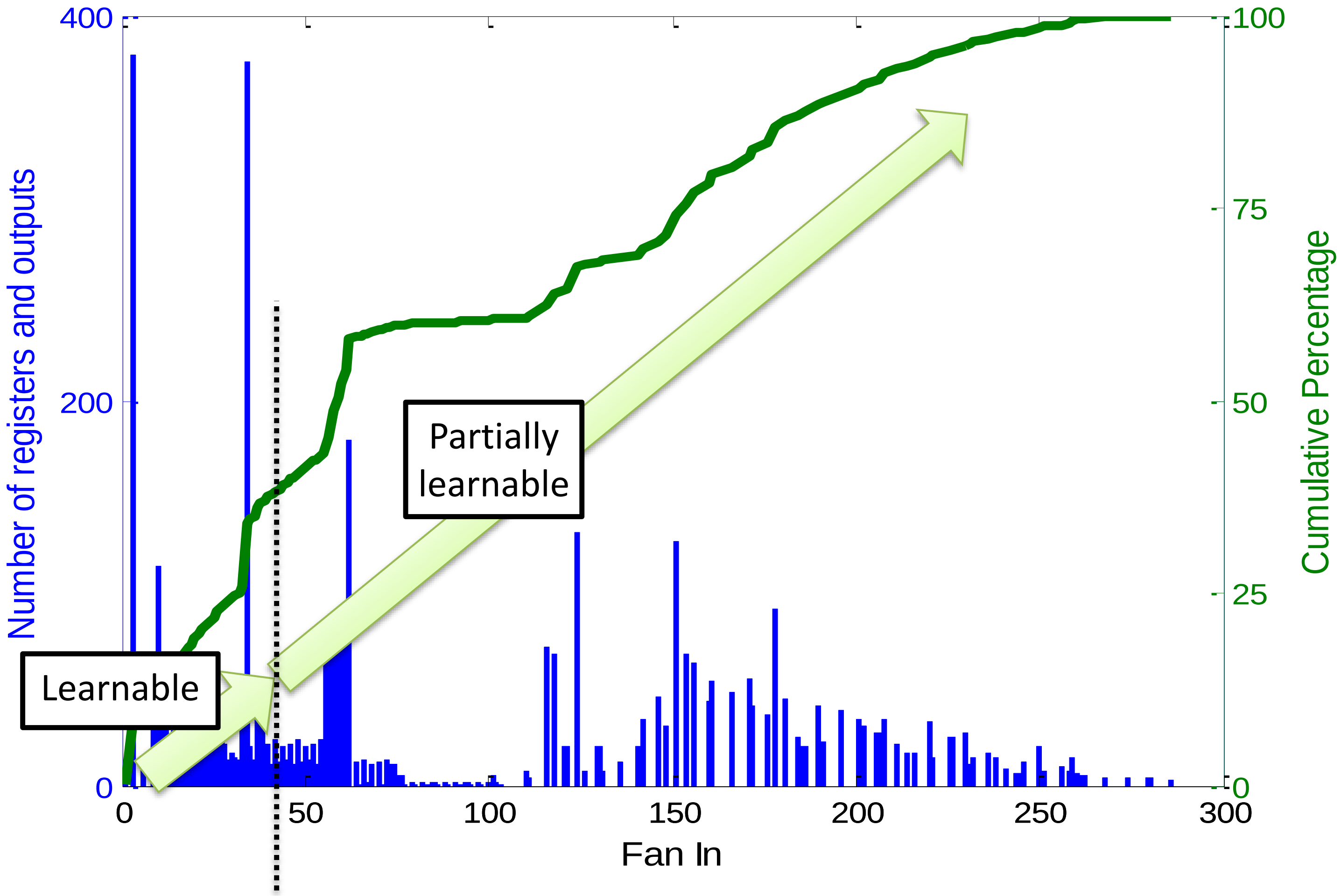
$$\vec{b} = \{1, 0, \ldots 1, 0, 1, 0, 0, \ldots, 0, 1\}, f(\vec{b}) = 1$$

$$O\left(n \cdot \log n \cdot k \cdot 2^k\right)$$

Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Transitive Fan-in for ITC'99 benchmark

Hiroshi Fujiwara
Cyber Security
Research Center



Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Assumptions

- Physical access to the device
- Scan operation protocol is known
  - Vendors use proprietary protocols
  - There are standard solutions by EDA vendors
- Scan control is not protected or protection is defeated

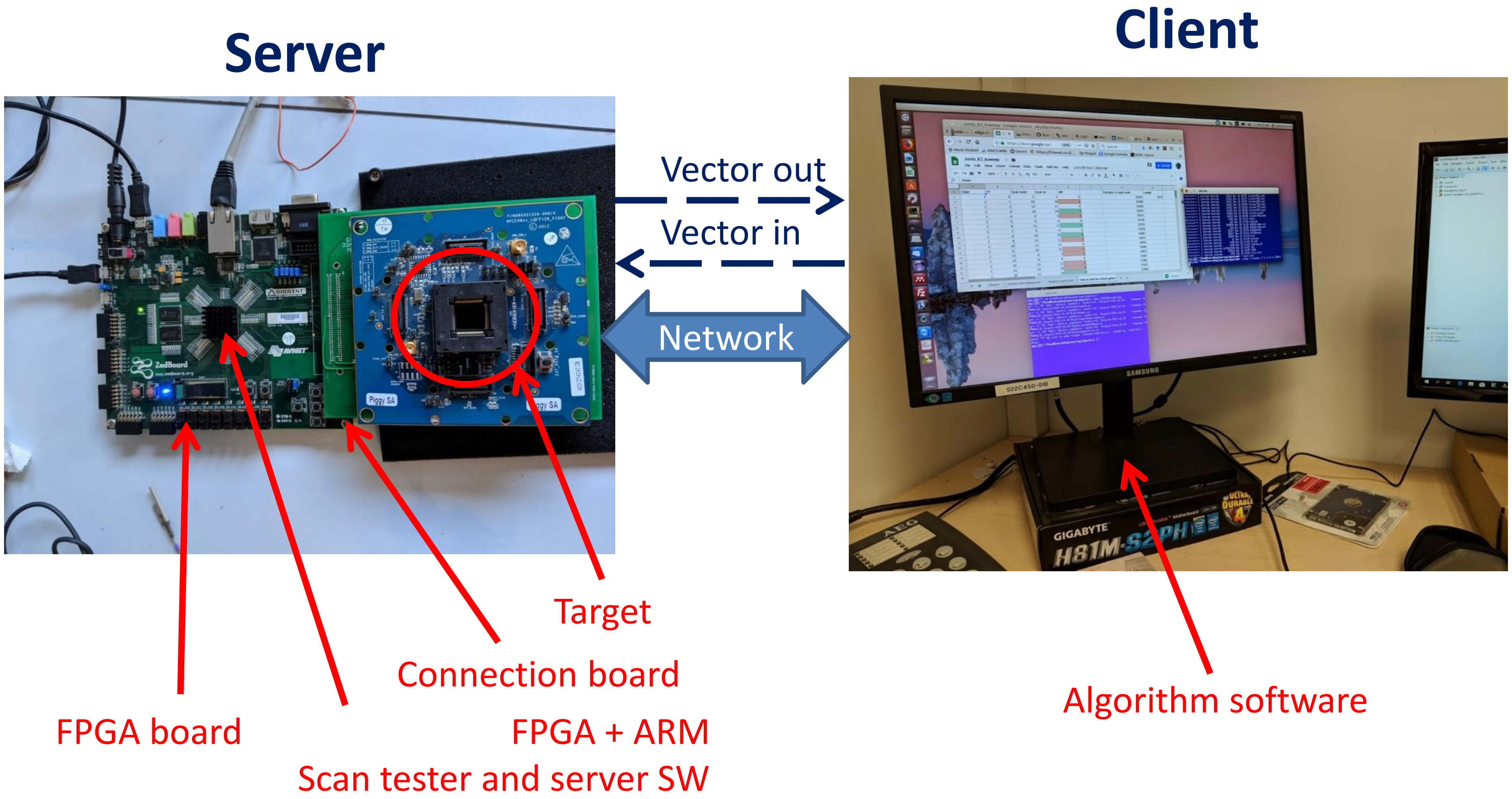
Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Assumptions

- Physical access to the device
- Scan operation protocol is known
  - Vendors use proprietary protocols
  - There are standard solutions by EDA vendors
- Scan control is not protected or protection is defeated
- Or self-owned device

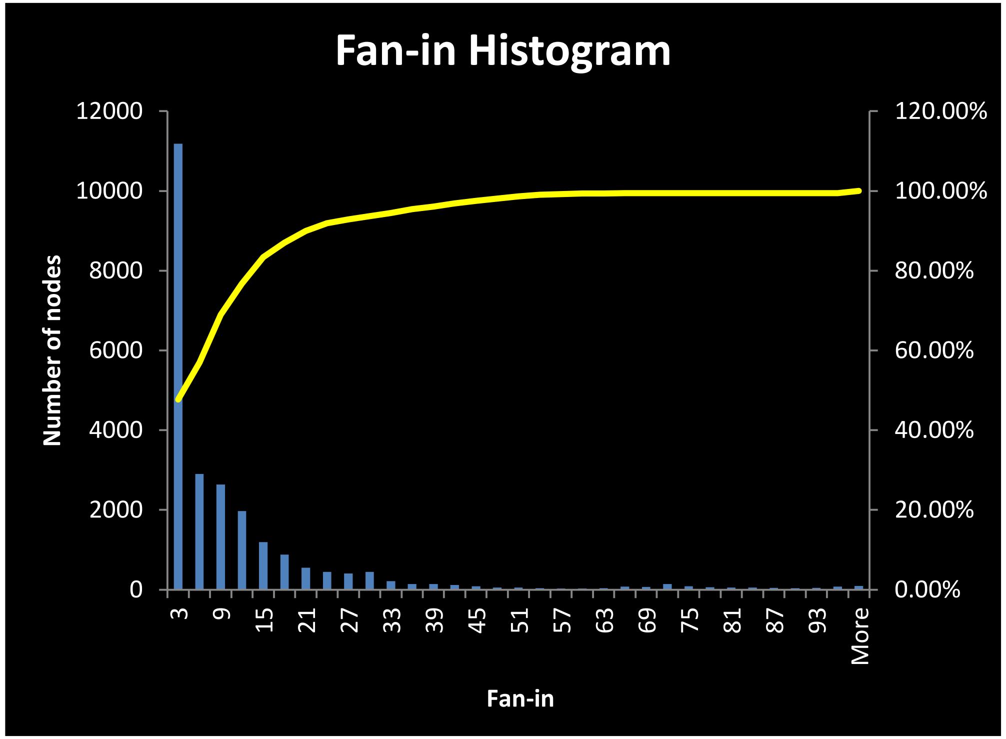
Azriel, "Revealing On-chip Proprietary Security Functions with Scan Side Channel Based Reverse Engineering," *GLSVLSI 2017*

Scan-based netlist extraction setup



Fan-in analysis

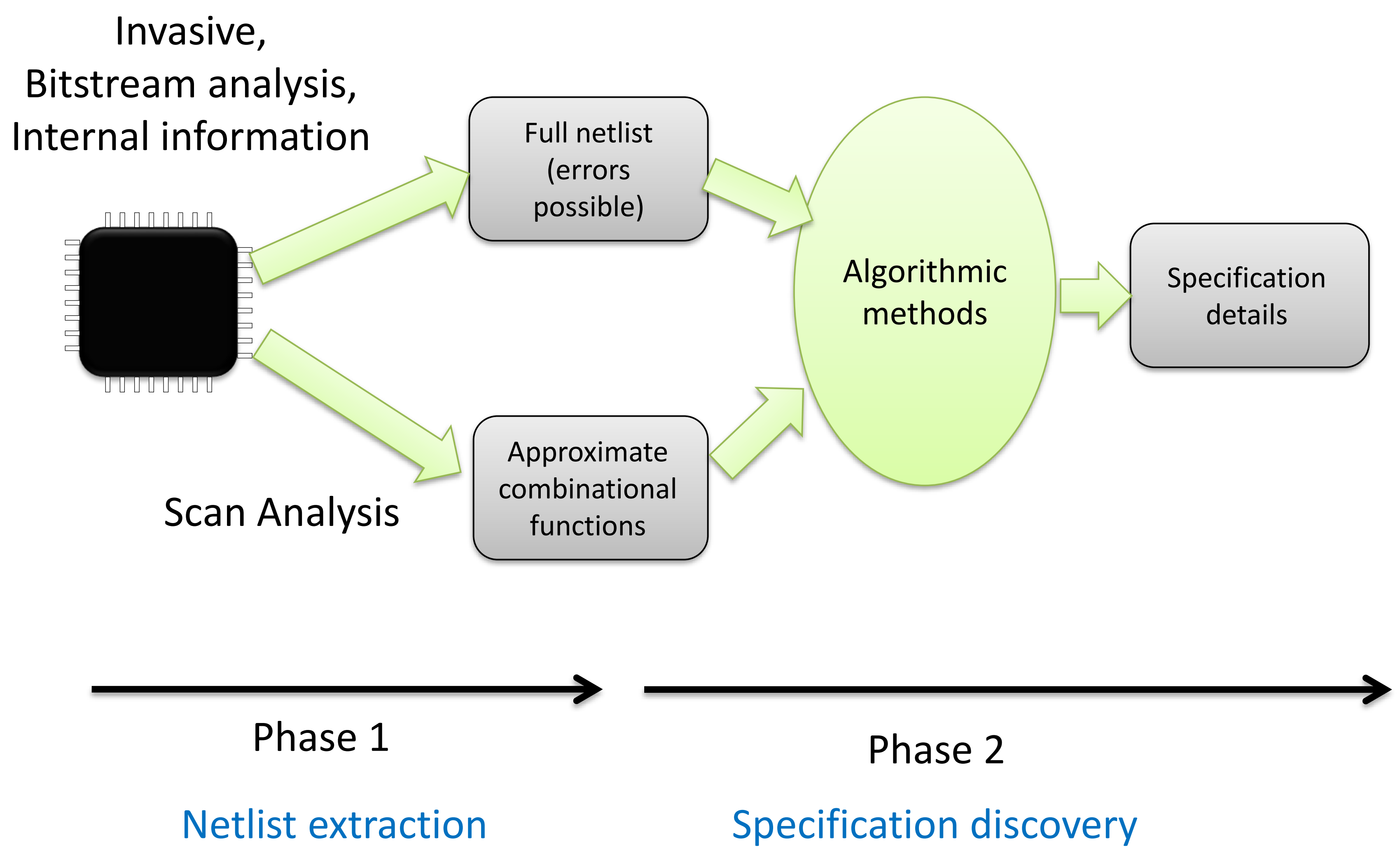
- Partial data: not all dependencies discovered
  - Estimation: vast majority is there
  - Longer runs reveal few more links



- ~95% of logic cones can be directly reverse engineered at the logic function level

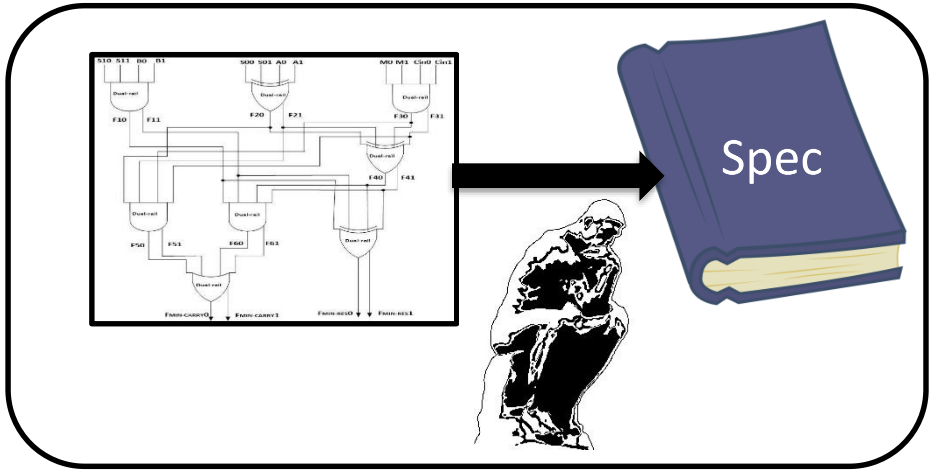
The two phases

Hiroshi Fujiwara
Cyber Security
Research Center



Specification Discovery

- What actually the spec is?
- No universal definition or format
- Can be
  – Finding familiar elements
  – Translating to a higher level language
  – Goal dependent, e.g. finding specific properties

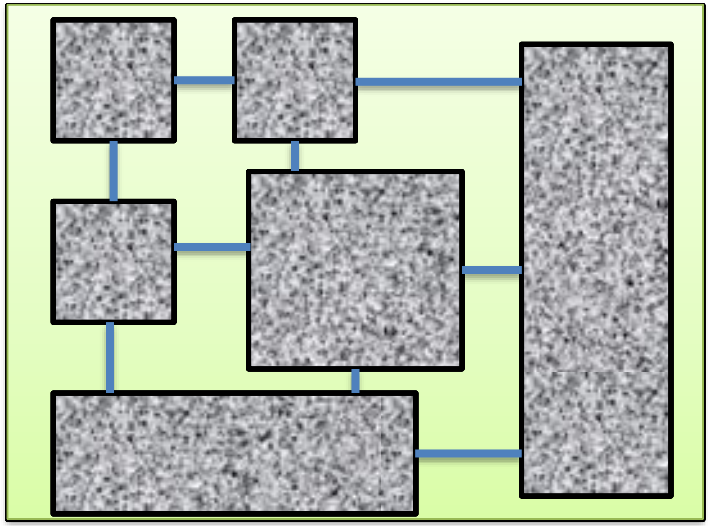


Outline

Hiroshi Fujiwara Cyber Security Research Center

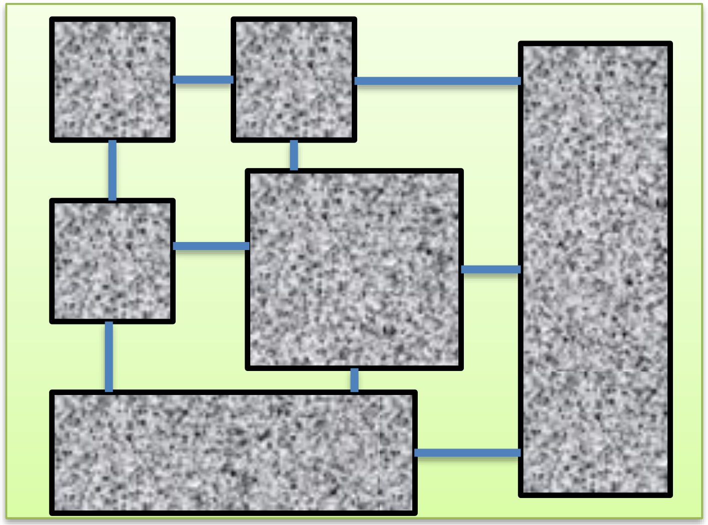
- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

Circuit Partitioning



- Find basic structure in the flat graph

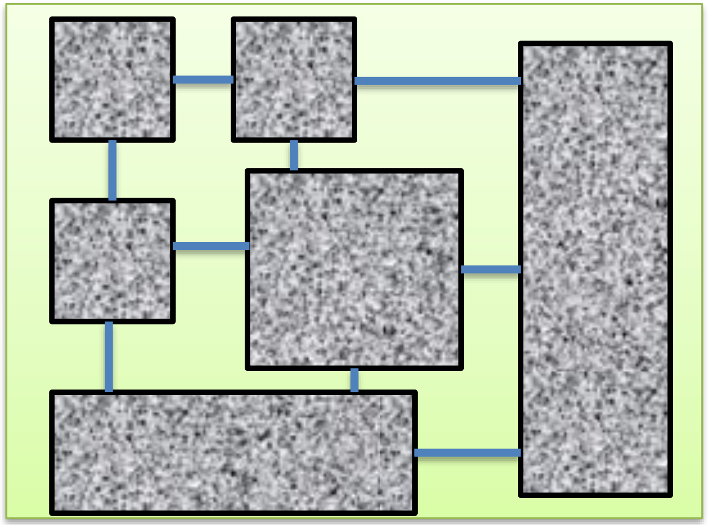
Circuit Partitioning



- Goal: match the source design partitioning

Circuit Partitioning

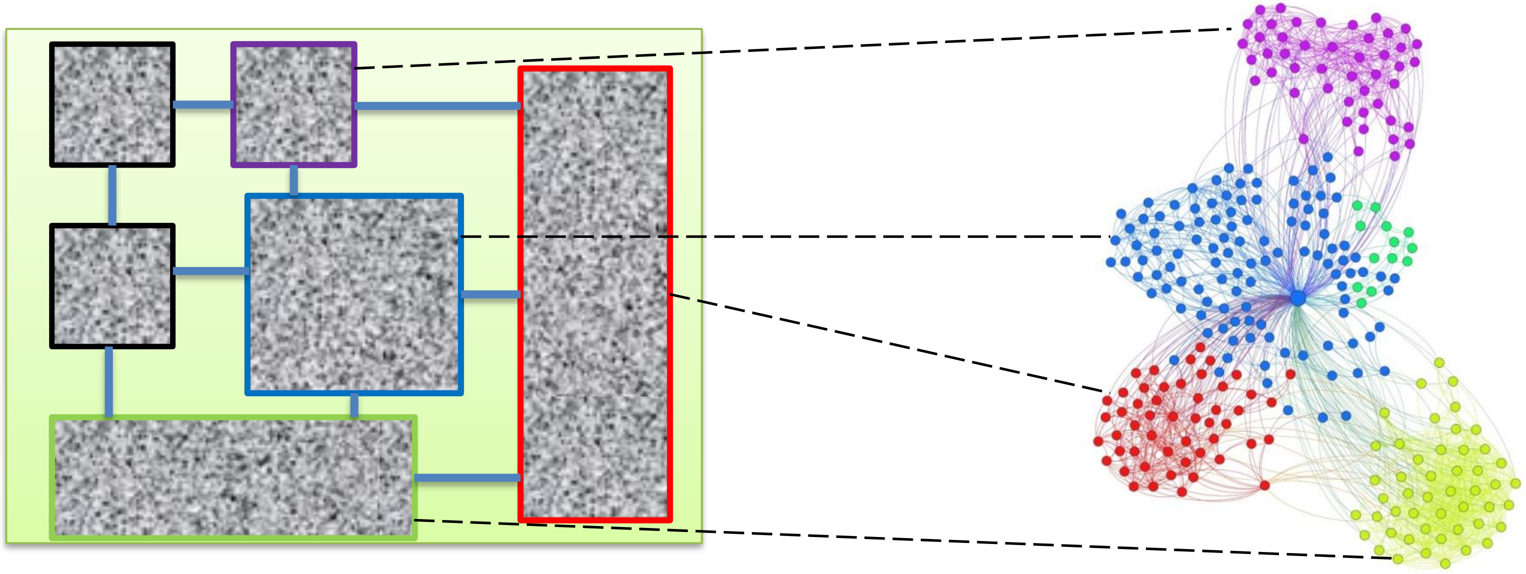
Hiroshi Fujiwara
Cyber Security
Research Center



- Goal: match the source design partitioning
- Criteria: wire density

Circuit Partitioning

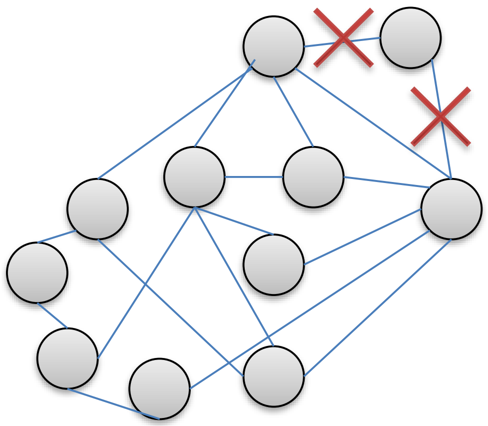
Hiroshi Fujiwara Cyber Security Research Center



- Goal: match the source design partitioning
- Criteria: wire density
- Method: graph clustering

Minimum cut

- Partition a graph by removing minimum number of edges
- Widely used in the VLSI CAD tools
- Top-down approach
- Poor choice for our problem:
  - Fixed number of partitions
  - Uneven split



More top-down methods

Hiroshi Fujiwara Cyber Security Research Center

- Min-Ncut
  - Normalized min-cut

$$NCut(A,B) = \frac{cut(A,B)}{assoc(A,V)} + \frac{cut(A,B)}{assoc(B,V))}.$$

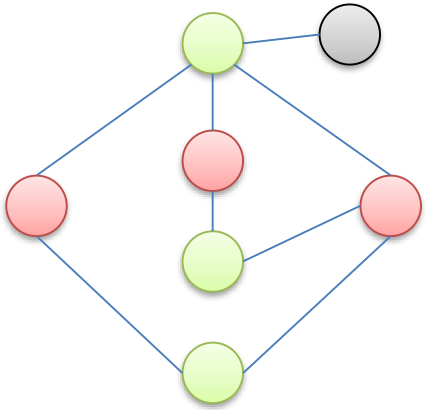
- Modularity maximization
  - Find best partition to maximize modularity

$$Modularity(G_i \in \mathrm{G}) = \frac{|E|_{G_i} - |E|_{G*_i = \{V_{G_i}, E_{random}\}}}{|E|_G}$$

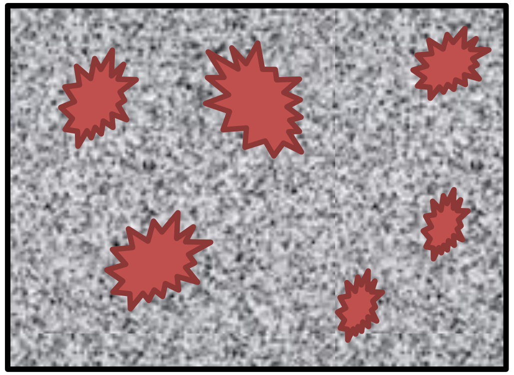
Couch, “Functional block identification in circuit design recovery”, *IEEE HOST 2016;* Blondel, "Fast unfolding of communities in large networks“, *Journal of Statistical Mechanics: Theory and Experiment. 2008*

Shared Nearest Neighbors (SNN)

- Every pair of nodes with >threshold shared neighbors are assigned to the same cluster



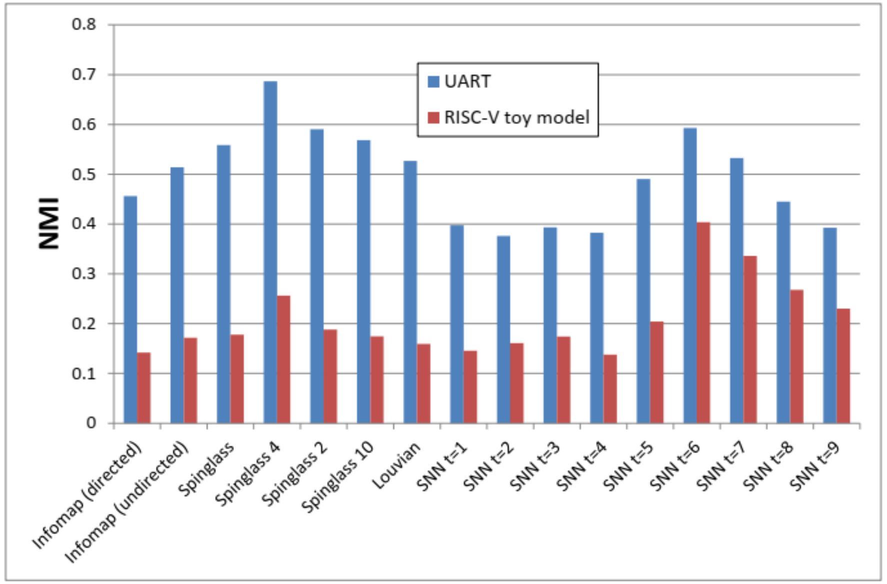
SNN (threshold=2)



Bottom-up

Clustering algorithms evaluation

- Goal: match the original design hierarchy
- Metric: Should reflect the goal
- NMI: Normalized Mutual Information
  - Information theoretical metric



Mutual Information

$$NMI = \frac{I(\Omega, \quad)}{[H(\Omega) + H(\quad)]/2}$$

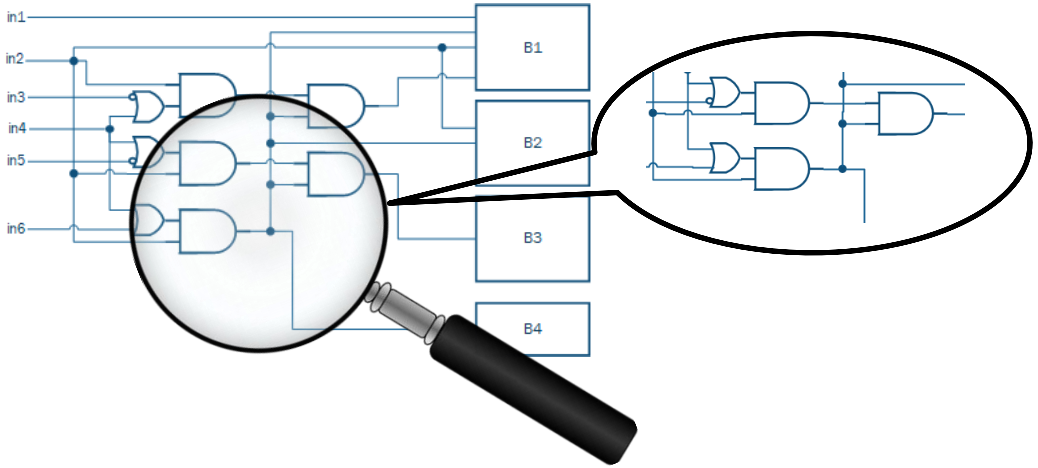
Entropy

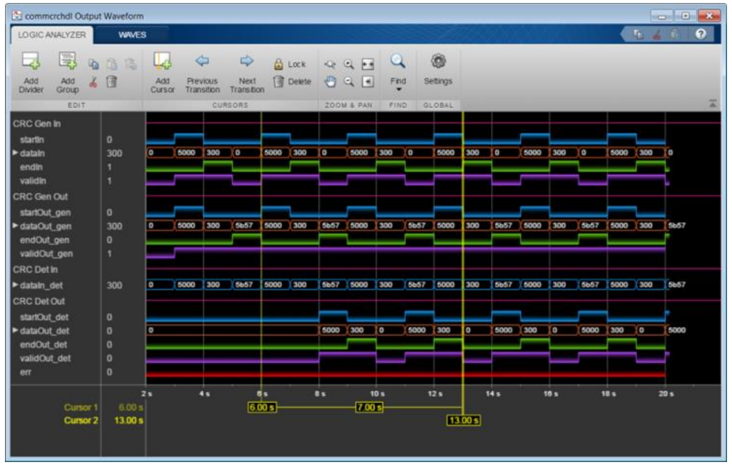
Outline

Hiroshi Fujiwara Cyber Security Research Center

- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

Matching against a library



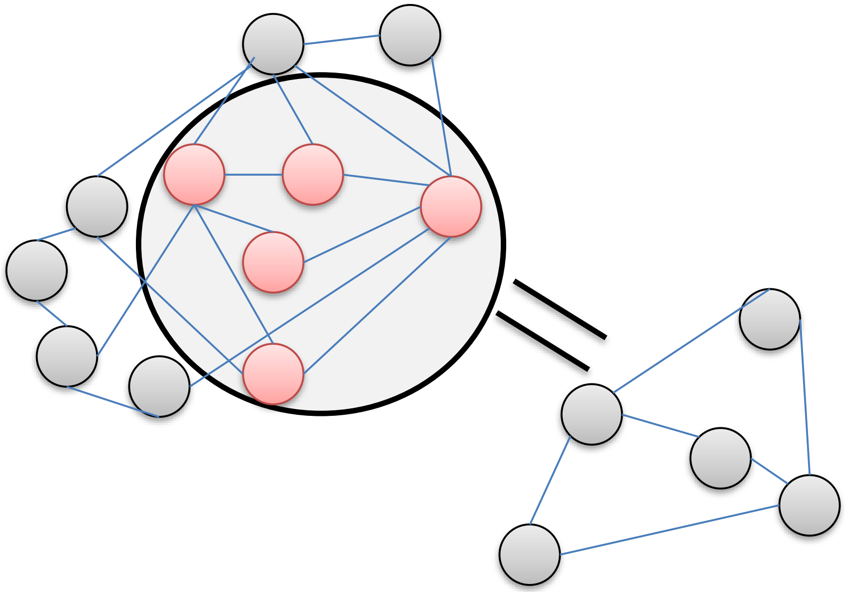


- Structural Analysis
  - Syntactic match
  - Isomorphism
  - Less flexible
- Functional Analysis
  - Semantic match
  - Functional identity
  - Static / simulations

Chisholm, “Understanding integrated circuits.” IEEE Design & Test of Computers 16, 2 (1999)

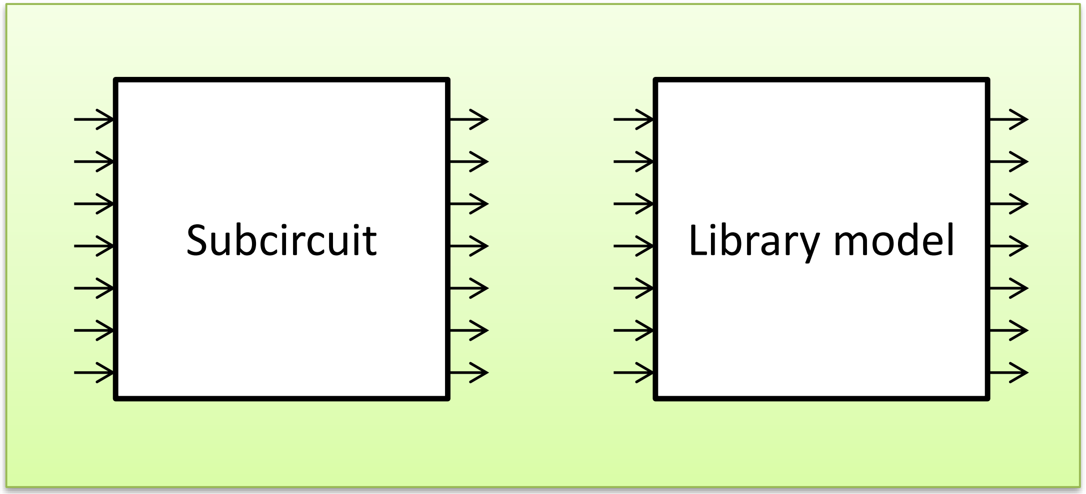
Matching library components

- Subgraph isomorphism
  - Structural match
  - NP-complete
- Heuristics
  - Dimension reduction
  - Signatures



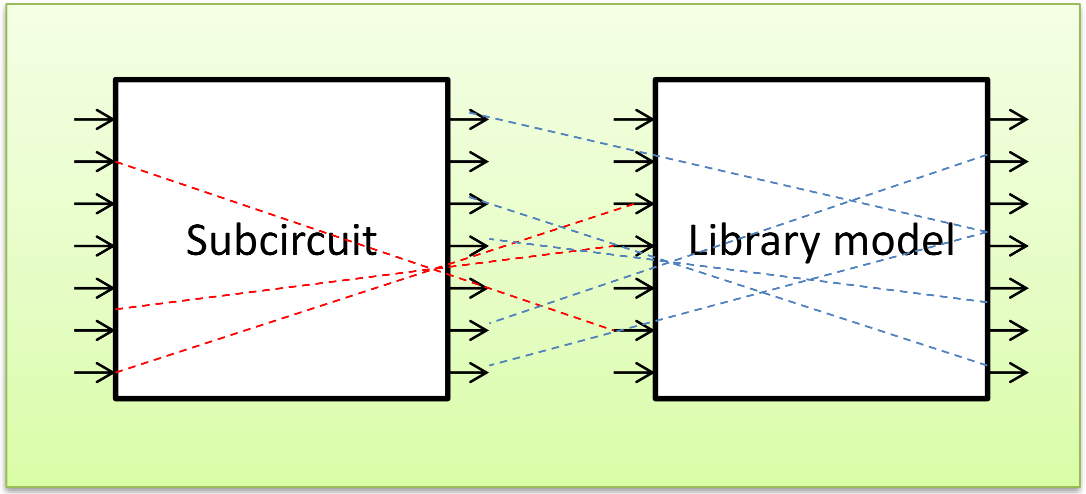
Couch, "Functional block identification in circuit design recovery", *IEEE HOST 2016*

NPNP-invariant matching



NPNP-invariant matching

- Input/output permutation

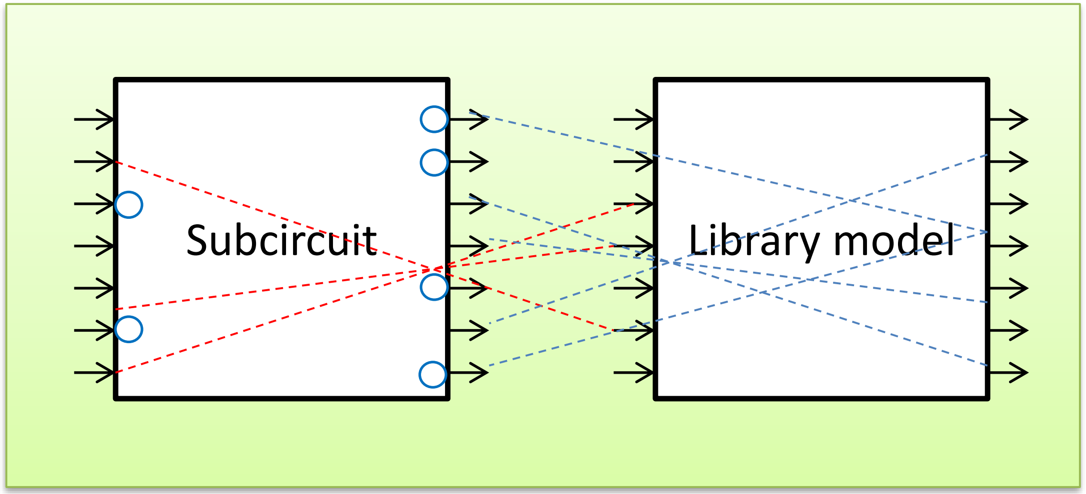


Soeken, “Simulation graphs for reverse engineering”, *FMCAD 2015*

NPNP-invariant matching

Hiroshi Fujiwara Cyber Security Research Center

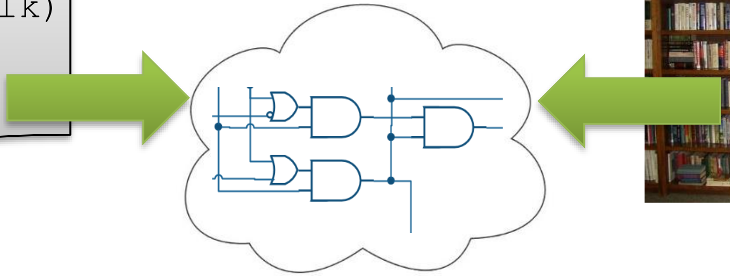
- Input/output permutation
- Input/output negation

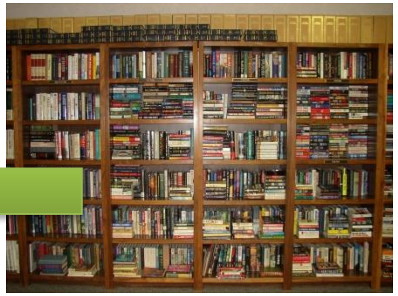


Soeken, “Simulation graphs for reverse engineering”, *FMCAD 2015*

Technology mapping

```
wire a = b & c;
always_ff @(posedge clk)
  out1 <= in1;
…
```





Cell library

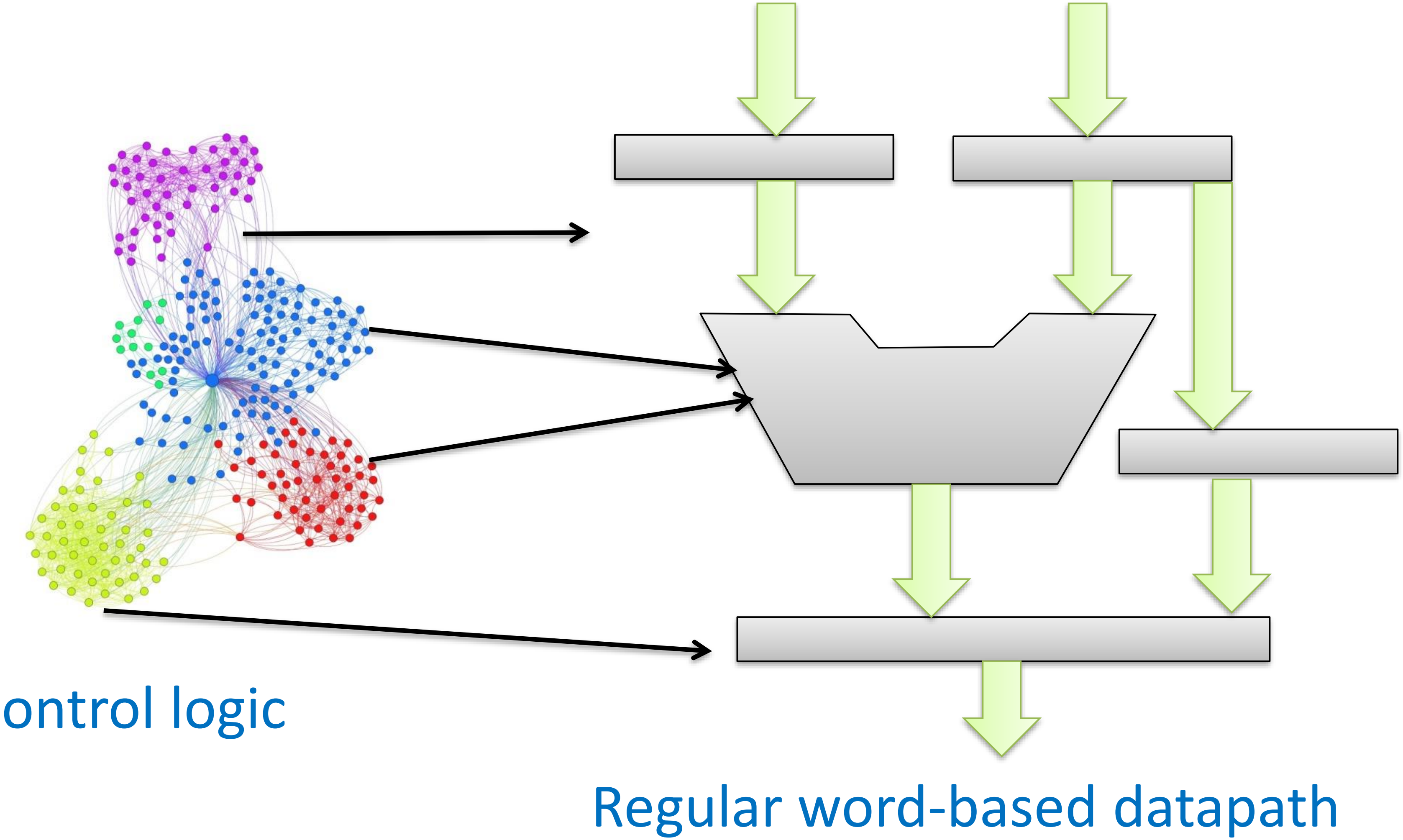
- RTL synthesis
  - Map generic logic to technology cells
  - npnp-invariant matching

Outline

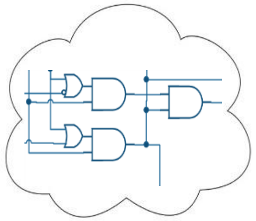
Hiroshi Fujiwara Cyber Security Research Center

- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

Looking for more structure



WordRev: construct bit slices

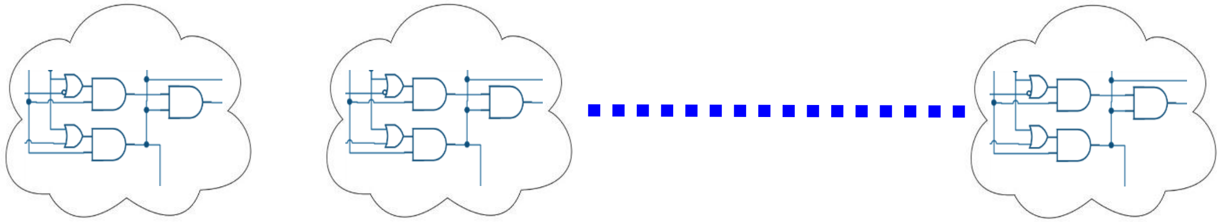


6-Feasible cut

(K-Feasible cut of N = K nodes that completely define the value of N)

Li, “WordRev: Finding word-level structures in a sea of bit-level gates,” HOST 2013

WordRev: group equivalent slices

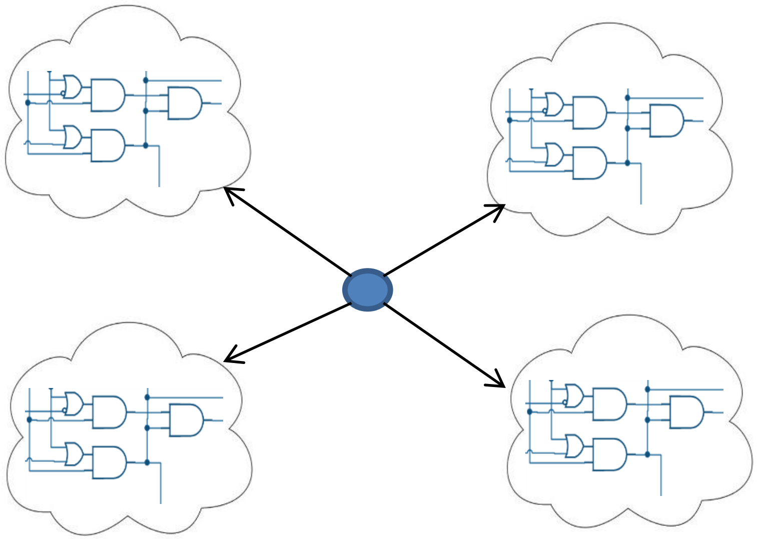


Permutation-invariant Boolean matching

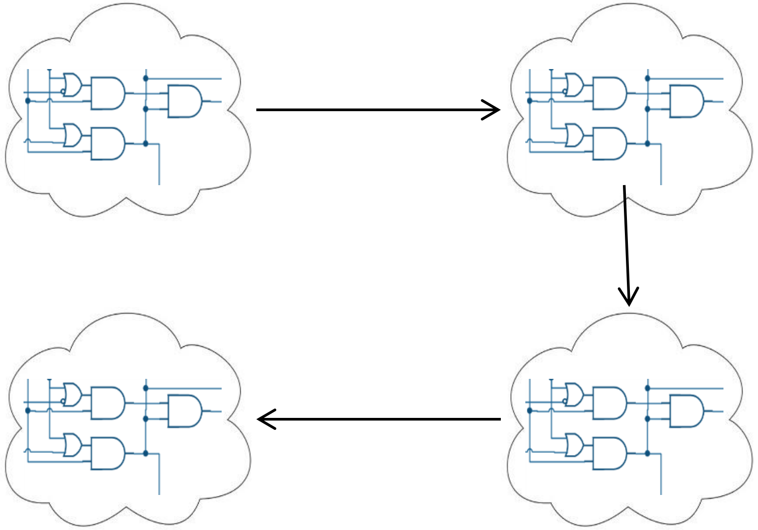
Li, “WordRev: Finding word-level structures in a sea of bit-level gates,” HOST 2013

WordRev: group by connections

Hiroshi Fujiwara
Cyber Security
Research Center



Parallel connection
(e.g. MUX select)

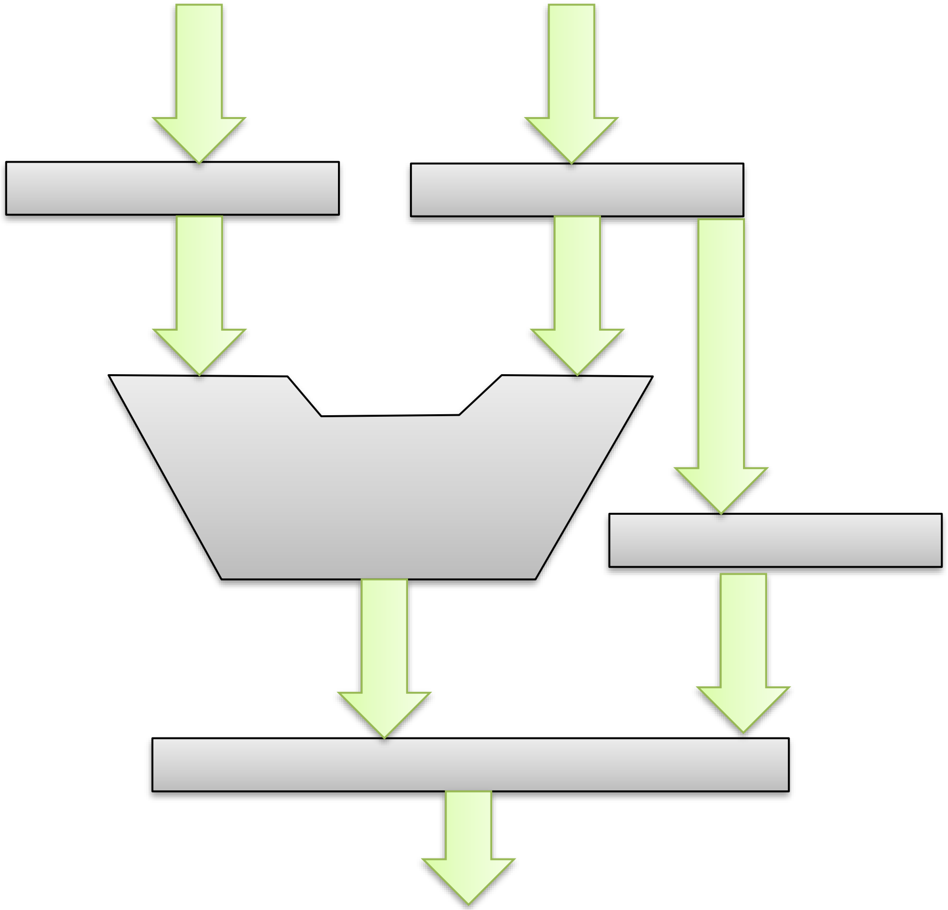


Serial connection
(e.g. carry propagation)

Li, “WordRev: Finding word-level structures in a sea of bit-level gates,” HOST 2013

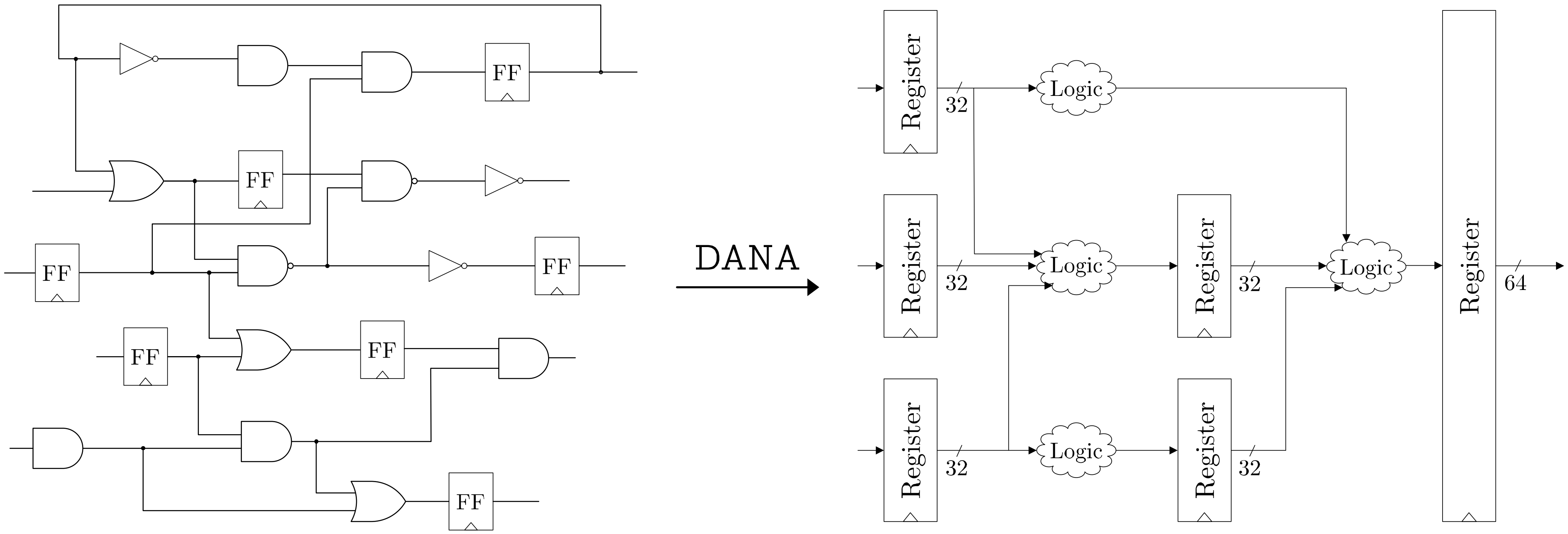
WordRev: propagate word structures

Hiroshi Fujiwara Cyber Security Research Center



Li, “WordRev: Finding word-level structures in a sea of bit-level gates,” HOST 2013

DANA - Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering

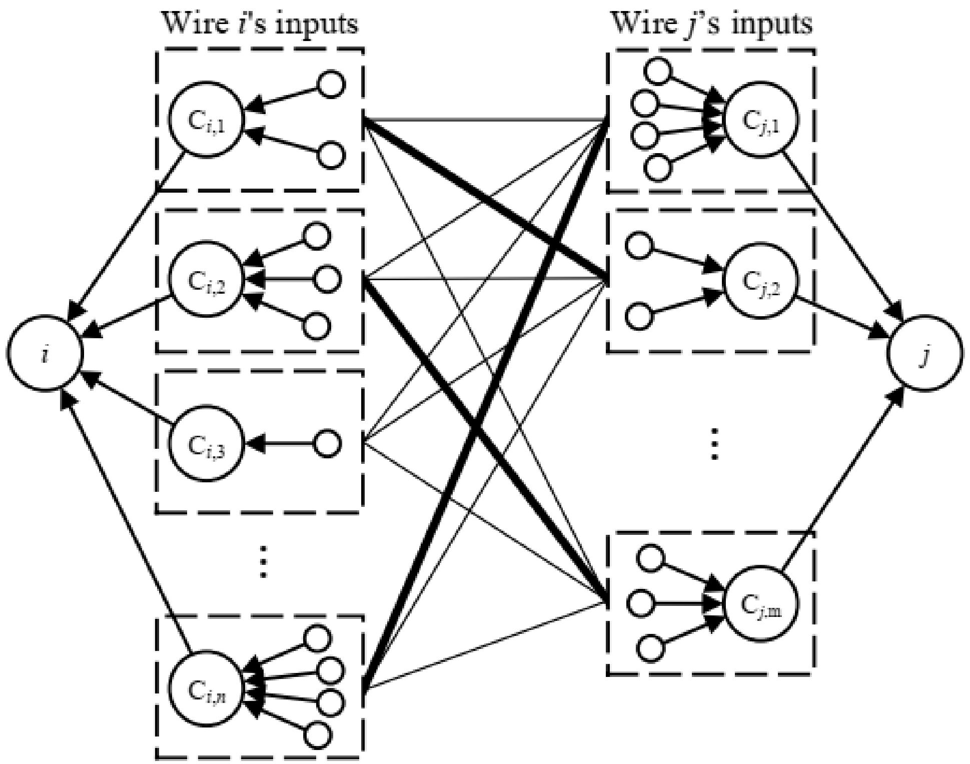


Albartus, N et all, “DANA—Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering,” Cryptology ePrint Archive: Report 2020/751

RELIC tool

Hiroshi Fujiwara Cyber Security Research Center

- Detecting registers in data words
  - Loose topological comparison of fan-in structures
- Preprocess to simple gates
- Recursive search
  - Similarity metrics
  - Based on number of inputs
  - Connecting nodes with *similarity > threshold*



Meade, "Gate-level netlist reverse engineering for hardware security: Control logic register identification.," ISCAS 2016

Extracting state machines

Hiroshi Fujiwara Cyber Security Research Center

- Mark registers with feedback path as FSM registers
  - Too many false positives

Kenneth, “Methods and apparatuses for automatic extraction of finite state machines,” US Patent 2001; Shi, “A highly efficient method for extracting FSMs from flattened gate-level netlist,” ISCAS 2010

Extracting state machines

- Mark registers with feedback path as FSM registers
  - Too many false positives
- Narrowing down
  - Select registers that control datapath
  - Group registers that have the same enable signal
  - Group registers that have shared gates in their combinational feedback path

Kenneth, "Methods and apparatuses for automatic extraction of finite state machines," US Patent 2001; Shi, "A highly efficient method for extracting FSMs from flattened gate-level netlist," ISCAS 2010

Outline

Hiroshi Fujiwara Cyber Security Research Center

- IC Reverse Engineering in a nutshell
- Scan-based netlist extraction
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Summary and Future Directions

Logic Equivalence Check

Hiroshi Fujiwara Cyber Security Research Center

- Massively used in the VLSI design process
- Uses anchors
  - Named registers
  - Hierarchical boundaries
- Usually combinational match only
  - Still a SAT problem, but there is a structure

Machine learning for RE

Hiroshi Fujiwara Cyber Security Research Center

- Some unsupervised learning used for clustering
- Can the full ML power be harnessed for RE?
- Problem: insufficient dataset

Using CNN for circuit recognition

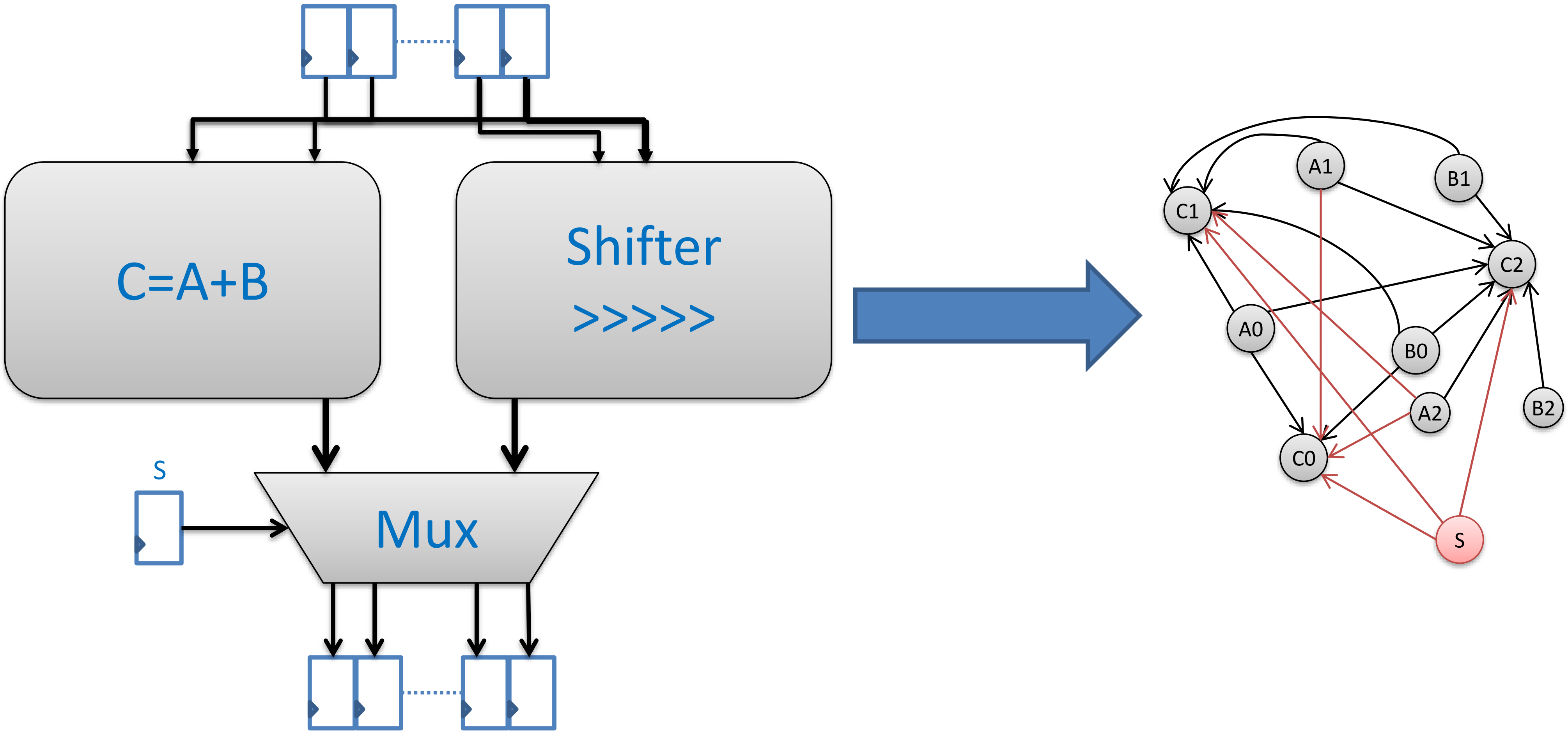
Hiroshi Fujiwara Cyber Security Research Center

- Map a circuit to a library of 4-LUTs
- 222 isomorphism classes to make the LUT npn-invariant
- Existence vectors: classes of adjacent elements
- Reduced existence matrix is fed to CNN
- Total set of 250 synthetic circuits
- Efficient for a small number of classes
  - One class (detect whether multiplier is present): 97% accuracy
  - 9 classes: 75% accuracy

Dai, “Circuit recognition with deep learning,” HOST 2017

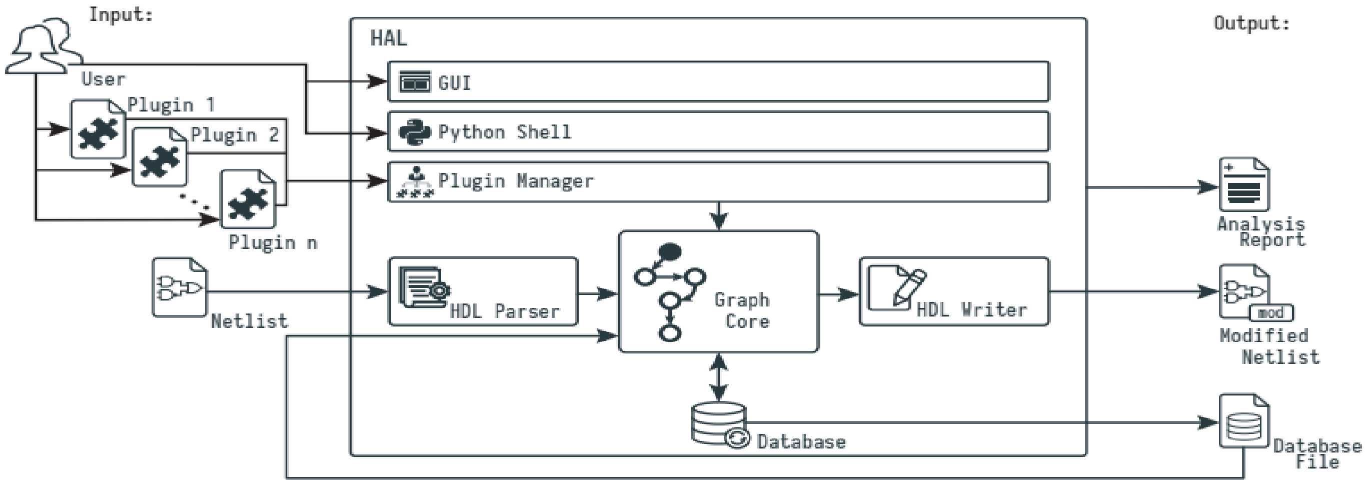
Spectral Graph Methods

Hiroshi Fujiwara
Cyber Security
Research Center



Reverse Engineering Tools

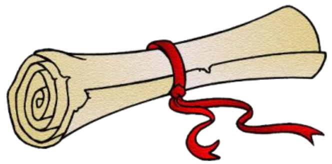
- Commercial
  - ChipWorks
  - Texplained ChipJuice (phase 1)
- Academia
  - Degate (phase 1)
  - HAL



Outline

- IC Reverse Engineering at a glimpse
- Partitioning
- The matching problem
- Structural Analysis
- Functional Analysis
- Algorithmic Reverse Engineering Tools
- Summary and Future Directions

Future research directions



- Uniform output format
  - Streamline the research
  - Evaluation baseline and common metrics
- Quantifying success
  - How to measure spec information
  - Is number of classified gates the right metric
- Graph methods
  - Take advantage of the big advancement in the social network analysis

Future research directions

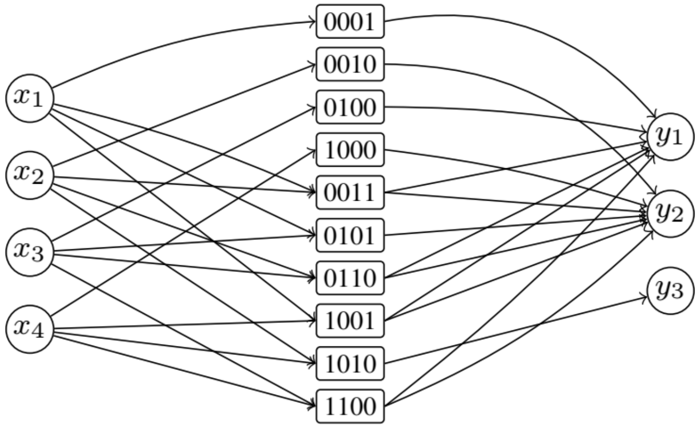
- Functional analysis
  - Use Boolean function properties
- Machine learning
  - Generate a synthetic data set
  - Generative Adversarial Networks
  - One-shot learning
- Protection
  - Logical obfuscation
  - Structural obfuscation

Questions

Hiroshi Fujiwara Cyber Security Research Center

Matching using simulation vectors

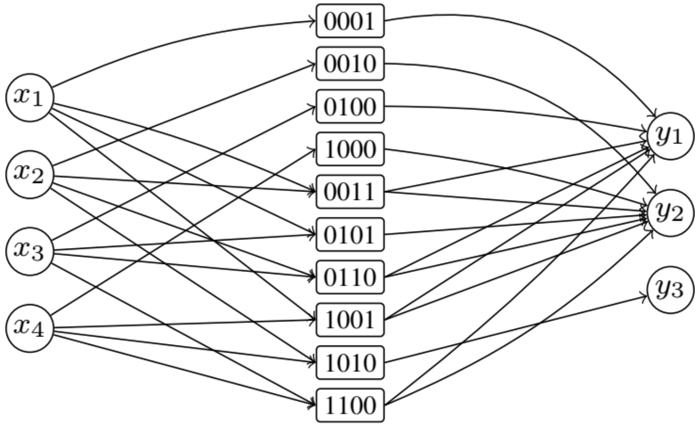
- Permutation invariance
  - One-hot and two-hot vectors
  - Simulation graphs
  - Matching subgraphs



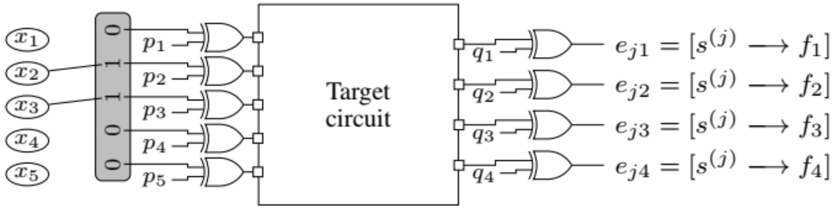
Soeken, “Simulation graphs for reverse engineering”, *FMCAD 2015*

Matching using simulation vectors

- Permutation invariance
  - One-hot and two-hot vectors
  - Simulation graphs
  - Matching subgraphs



- Negation invariance
  - Add polarity variables
  - SAT problem



Soeken, "Simulation graphs for reverse engineering", *FMCAD 2015*