


# Polymorphic Gates and Their Applications in Hardware Security



Gang Qu

University of Maryland, College Park

[gangqu@umd.edu](mailto:gangqu@umd.edu)

Electronic Design Process Symposium

Milpitas, California, USA

September 14, 2018

# Outline

- # Polymorphic electronics: a brief history
- # Finding polymorphic gates
  - Design approach
  - Findings
- # Polymorphic gates for security
  - Circuit watermarking and fingerprinting
  - Authentication and random number generation
- # More readings

# Polymorphic Electronics

## # Evolvable Hardware

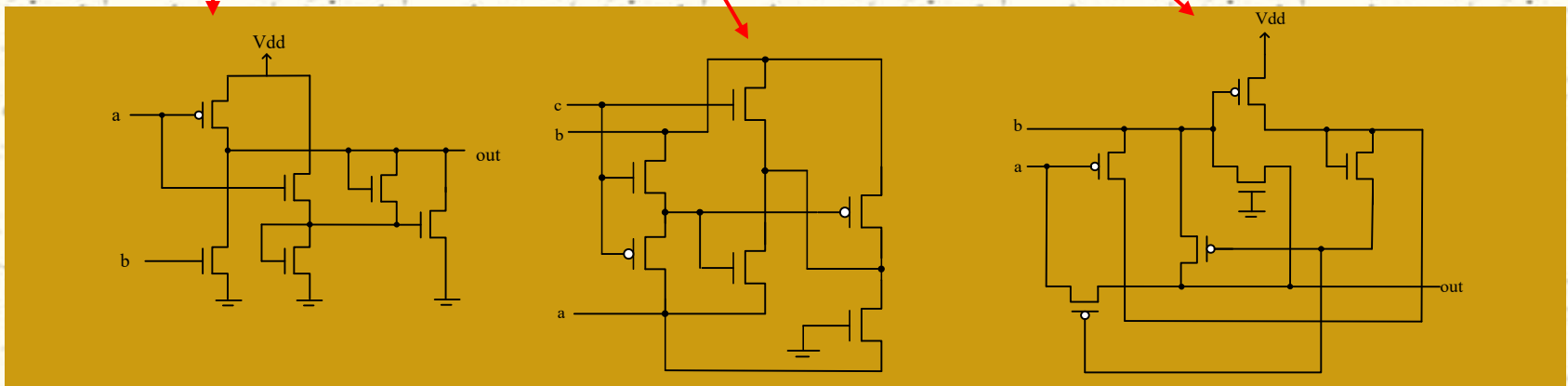
- Reconfigurable to the environment
- Applicable to extreme conditions, e.g. space or deep sea.

## # Polymorphic electronics/circuits

- First proposed by A. Stoica, 2001
- Function changes in response to the environment
- Polymorphic gate: logic gate that integrates multiple functions
  - FPTA, CMOS, emerging devices

# Polymorphic Electronics

Function	Control	Control values	Transistors
AND/OR[A.stoica,2001]	temperature	27/125C	6
AND/OR[A.stoica,2001]	ext. voltage	3.3V/0V	6
AND/OR[A.stoica,2002]	$V_{dd}$	3.3V/1.2V	8
AND/OR/XOR[A.stoica,2001]	ext. voltage	3.3V/0V/1.5V	10
NAND/NOR[A.stoica,2004]	$V_{dd}$	3.3V/1.8V	6
NAND/NOR[L. Sekanina,2008]	$V_{dd}$	5V/3.3V	8
NAND/XOR[R. Ruzicka,2008]	ext. voltage	3.3V/0V	9



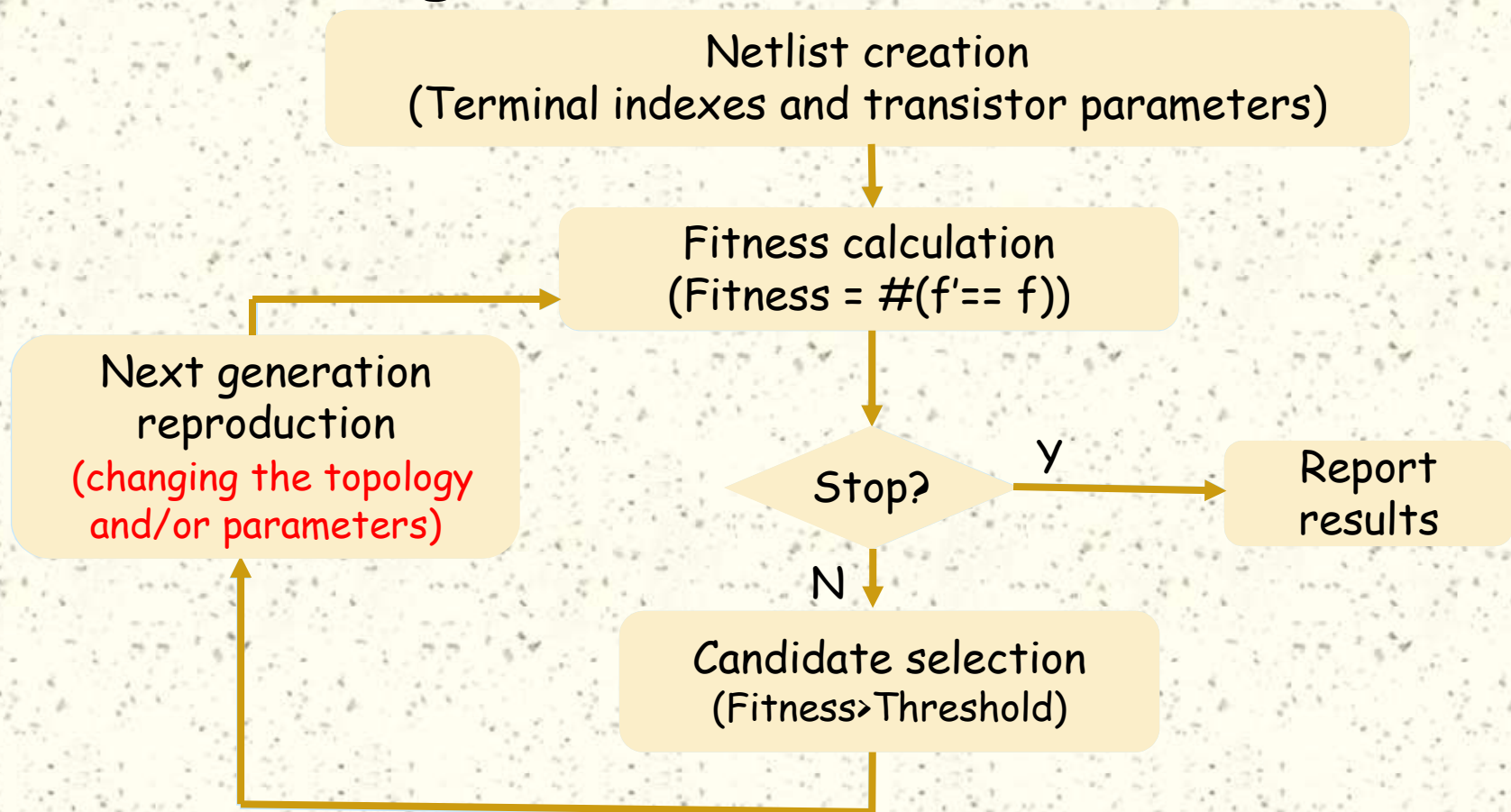
# Polymorphic Electronics

- # Flexibility
  - Adaptive systems
- # Reliability
  - Self-checking circuits
- # Low overhead
  - Multi-function circuits

Finding polymorphic gates is HARD.

# Finding Polymorphic Gates

## # Genetic algorithm



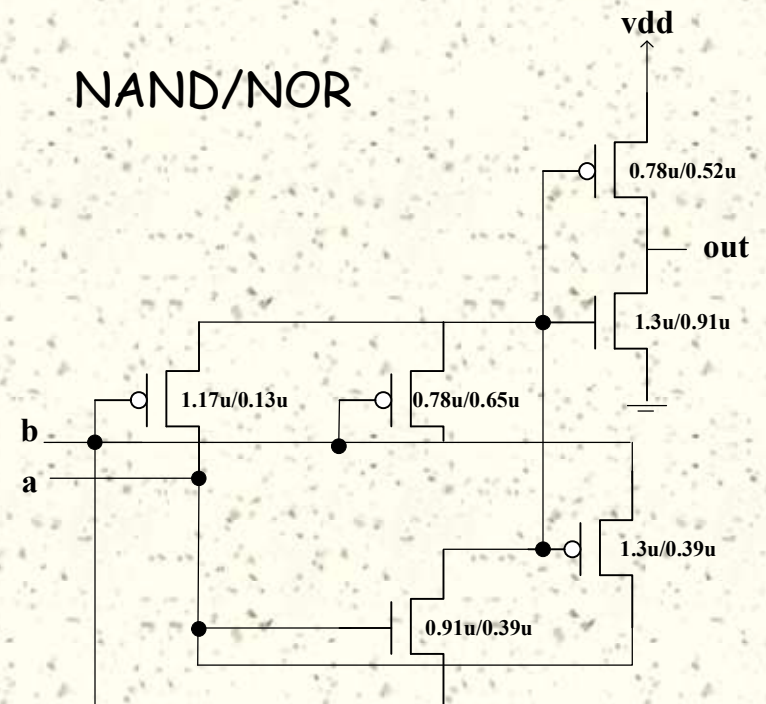
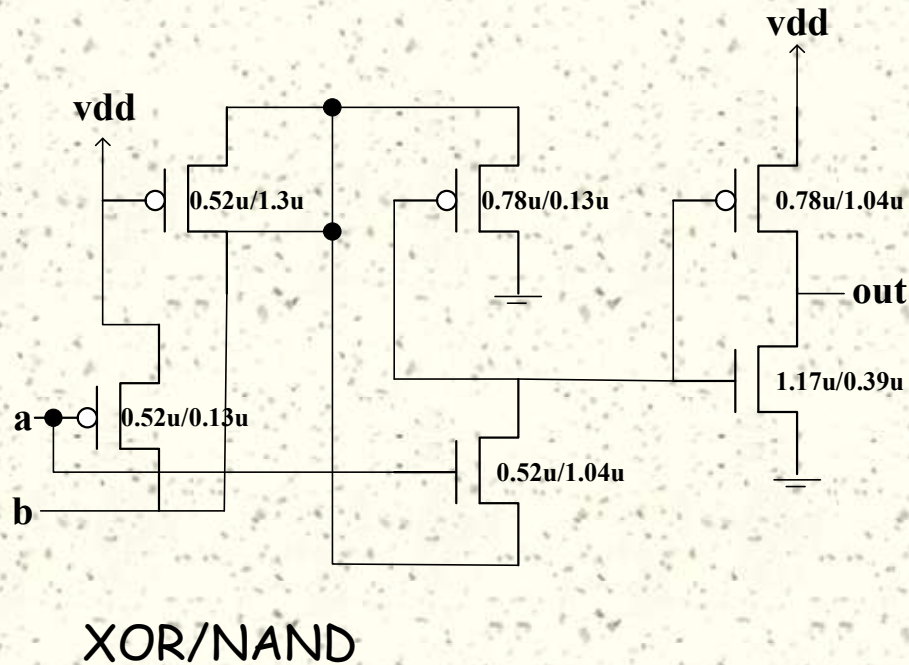
# Our Experiments

- # Software: evolutionary algorithm based approach to find polymorphic gates by a **C netlist modifier** and **Hspice** as the simulator.
- # Experiment setup
  - Target technology: 0.13um SMIC library.
  - Transistors: 4 P-type transistors and 2 N-type transistors.
  - Supply voltage  $V_{dd} = 1.2V$ .
  - Temperature: 8 discrete values from  $-25^{\circ}C$  to  $150^{\circ}C$ .



# Findings (I)

# Polymorphic gates controlled by temperature

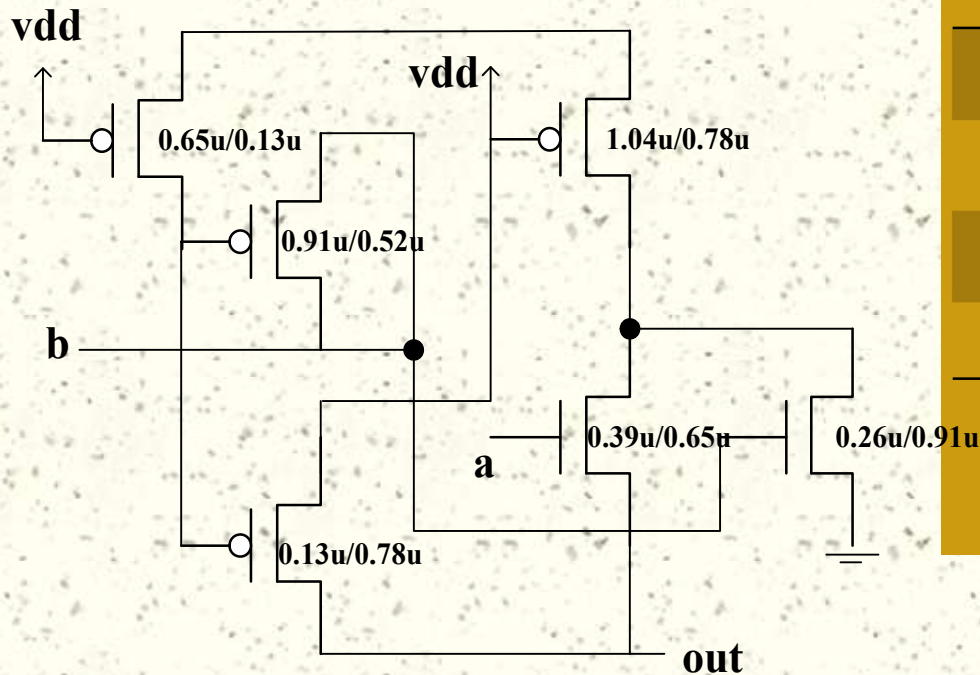




# Findings (II)

## # Partial polymorphic gates

Partial NOR gate

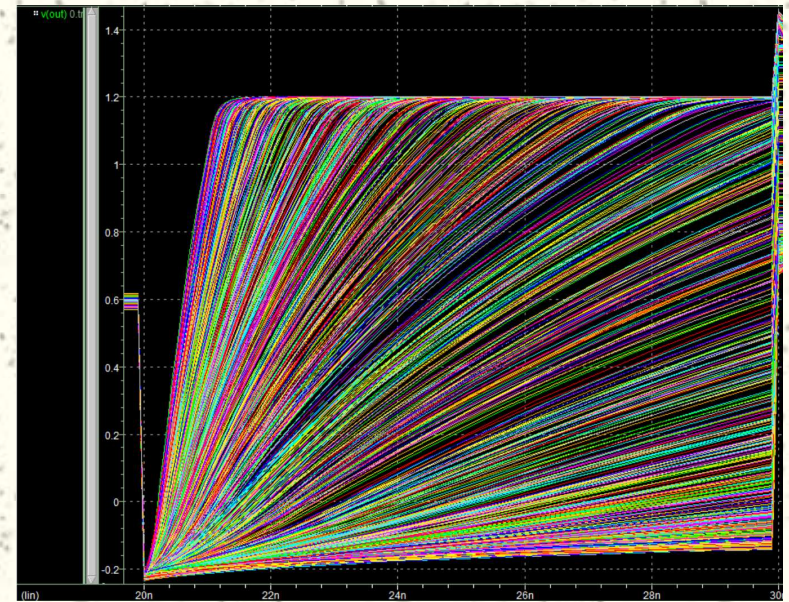
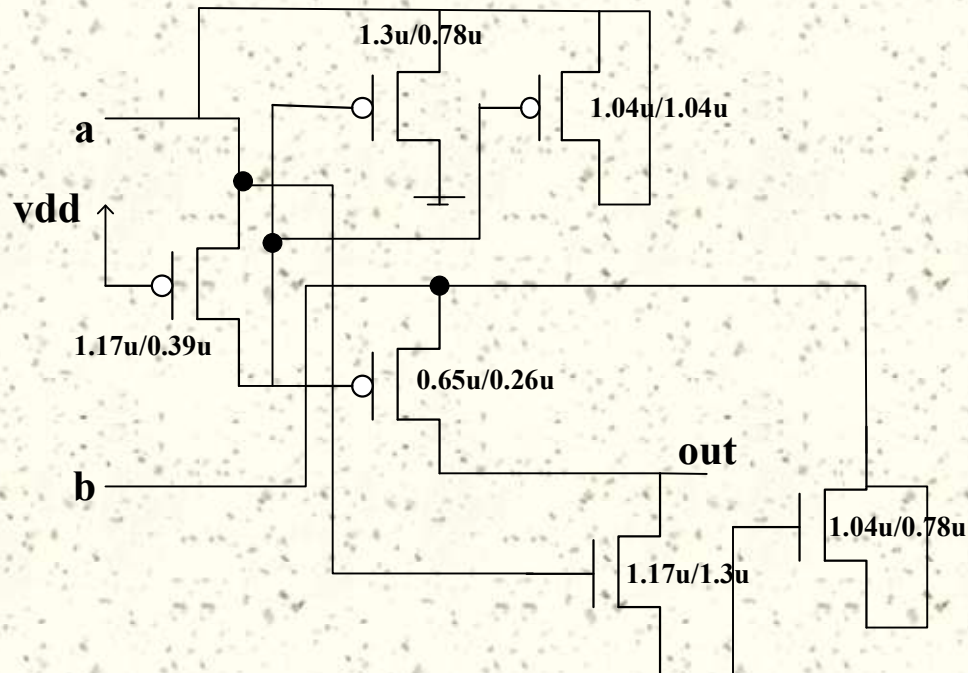


Input(a, b)	Output
0,0	1
0,1	u
1,0	0
1,1	0

Truth table  
(Temperature = 25°C)

# Findings (III)

## # Random output gates

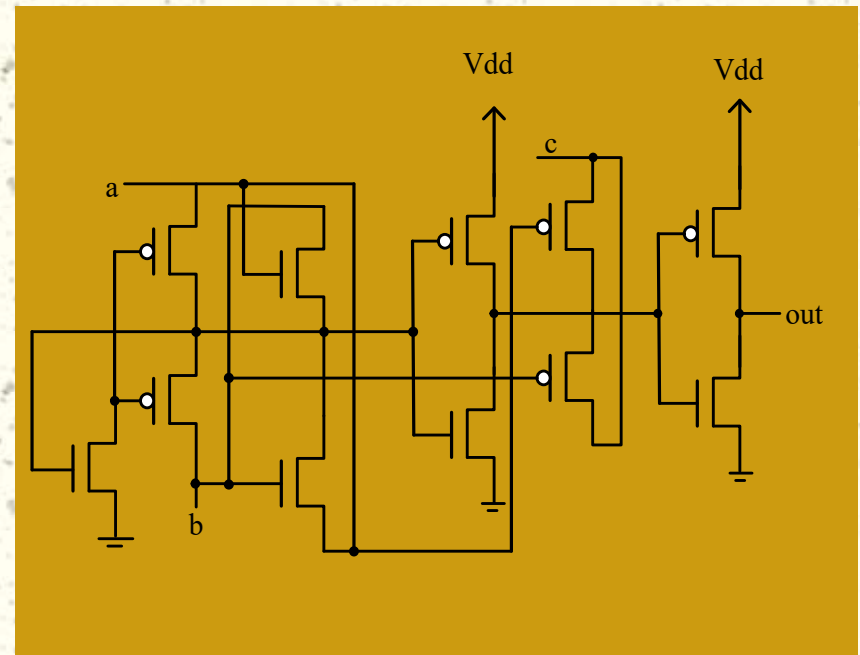


$V(out)$  with process variation and unstable supply voltage

# Findings (IV)

- # Two-input; SMIC 0.13um; Vdd = 1.2V
- # External input triggered.

Gate functionalities	#Transistor
NOR(C=1) - INV (C=0)	6
NAND(C=1) - INV (C=0)	7
AND(C=1) - BUF (C=0)	9
AND(C=1) - OR (C=0)	11
NAND(C=1) - NOR (C=0)	9

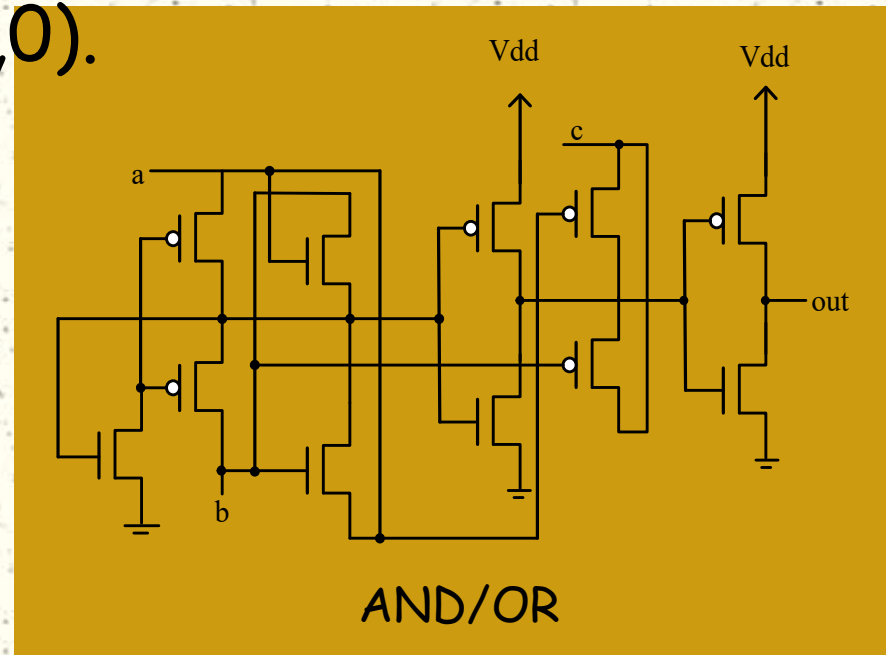


# Differentiating Input Values

# Input combinations that will make polymorphic gates produce different outputs at different modes.

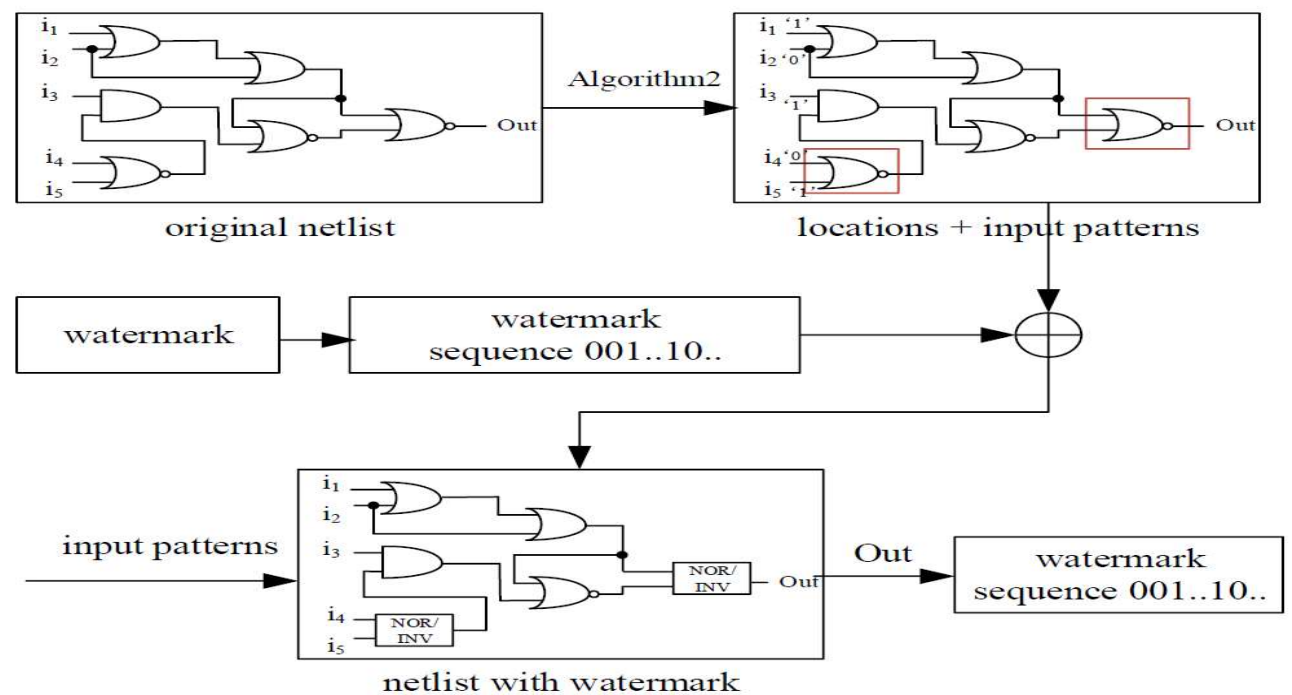
# Example: (0,1) or (1,0).

A	B	AB	A+B
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1



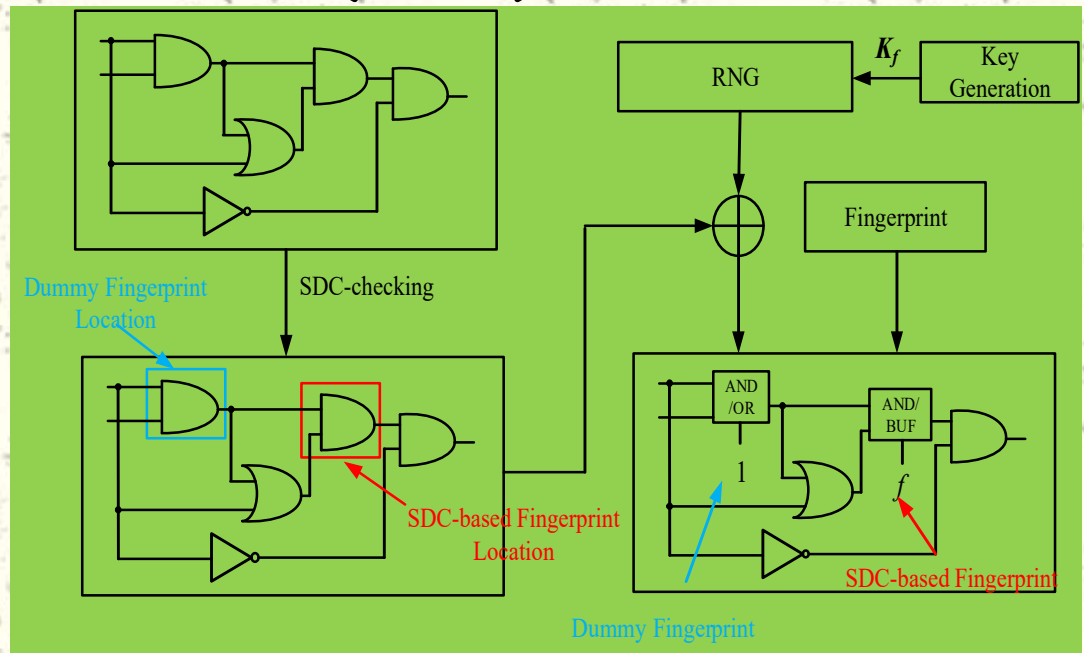
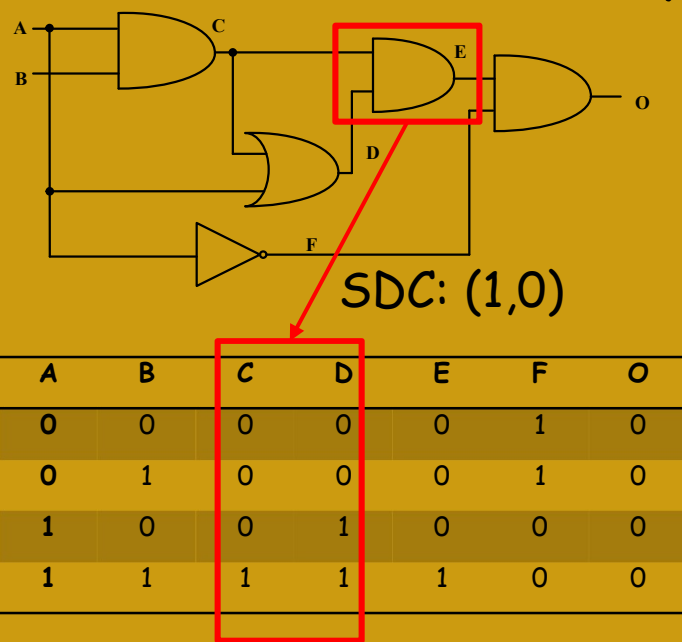
# Circuit Watermarking

- # What is circuit watermarking?
- # Why we need to watermark design?
- # Polymorphic gates based watermarking.



# Circuit Fingerprinting

- # What is circuit fingerprinting?
- # Why we need to fingerprint design?
- # Polymorphic gates based fingerprinting.
  - Satisfiability don't care (SDC) conditions.



# Evaluation Results

## # Evaluation setup

- SMIC 0.13um technology
- Integration of polymorphic gates in synthesis library
- ISCAS 85/MCNC benchmark
- Synopsys Design Compiler

Circuit	#Gates	#SDC-based fingerprint	#Dummy fingerprint
C880	290	42	114
C1355	424	69	64
C1908	396	52	106
C3540	943	116	124
C5315	1428	47	548
dalv	1228	52	398
des	3483	70	1712
ex5	609	155	64
i8	1174	208	267
i10	1914	134	509



# Evaluation Results

## # Overhead

Circuit	16-bit real + 16-bit dummy			32-bit real + 32-bit dummy		
	$\Delta$ Delay(%)	$\Delta$ Area(%)	$\Delta$ Power(%)	$\Delta$ Delay(%)	$\Delta$ Area(%)	$\Delta$ Power(%)
C880	1.08	8.11	8.16	1.08	16.31	11.90
C1355	5.72	5.9	7.23	11.74	12.275	8.02
C1908	5.1	6.31	4.13	7.05	13.17	5.09
C3540	0.55	3	2.78	1.11	5.835	4.72
C5315	0	1.645	1.93	6.8	3.355	2.05
dalu	2.38	2.56	2.26	5.71	4.77	2.49
des	4.59	0.77	0.50	4.59	1.455	0.55
ex5	0	3.54	13.05	1.65	6.485	13.26
i8	0	1.845	1.79	0	3.635	2.29
i10	0.74	1.205	0.77	0.74	2.4	0.98
Avg	2.02	3.485	4.26	4.04	6.97	5.14





# Logic Obfuscation

- # A promising countermeasure for reverse engineering (RE).
- # IC reverse engineering
  - Depackaging the IC using corrosive chemicals.
  - Imaging the top-view of each layer using an optical micro-scope or single electron microscope (SEM).
  - Extraction of gate-level netlist from the images
  - Reproduce identical copies of IC
  - Facilitate hardware Trojan insertion
  - Circuit redesign or integration



# Logic Obfuscation

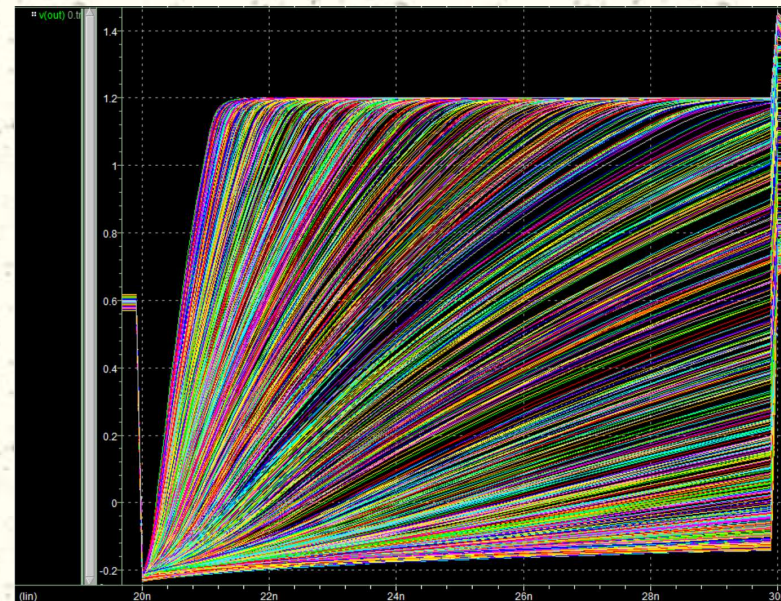
- # Obfuscation: using configurable logic cells
  - can be configured as different logic gates
  - cannot be observed under optical or electron microscopy
  - The only way to know the logic is to traverse all the possible inputs and read the corresponding output.
- # Polymorphic gates:
  - Non-standard topology is obfuscation by default.
  - Polymorphic and partial polymorphic gates.

# Randomness

- # Random number generator
- # Unique ID for circuit identification

Input(a,b)	Output
0,0	1
0,1	u
1,0	0
1,1	0

Truth table  
(Temperature = 25°C)



V(out) with process variation  
and unstable supply voltage

# Conclusion and Future Work

- # Genetic algorithm to find polymorphic gates
- # New types of polymorphic gates
- # Polymorphic gates for hardware security applications: IP protection, xRNG, etc.
- # Future work
  - Fabrication of polymorphic gates and polymorphic circuits
  - Explore more security applications

1. **"Polymorphic Gate based IC Watermarking Techniques"**, 23rd Asia and South Pacific Design Automation Conference (ASPDAC'18), pp. 90-96, January, 2018.
2. **"A novel polymorphic gate based circuit fingerprinting technique"**, 28th IEEE/ACM Great Lakes Symposium on VLSI (GLSVLSI'18), May 2018.
3. **"20 Years of Research on Intellectual Property Protection"**, IEEE International Symposium on Circuits and Systems (ISCAS'17), May 2017.
4. **"Polymorphic electronics,"** International Conference on Evolvable Systems. Springer Berlin Heidelberg, pp. 291-302, 2001.
5. **"Taking evolutionary circuit design from experimentation to implementation: Some useful techniques and a silicon demonstration,"** IEE Proceedings-Computers and Digital Techniques, vol.151, no.4, pp.295-300,2004.
6. **"Evolution of multifunctional combinational modules controlled by the power supply voltage,"** 1st NASA/ESA Conference on Adaptive Hardware and Systems, pp. 86-193, 2006.

# Thank You!

This work is sponsored in part by NSF under grant CNS1745466 and by a research agreement between the University of Maryland and the Laboratory for Physical Sciences.



**Tian Wang, Prof. Xiaoxin Cui**

Peking University

**Omid Aramoon, Timothy Dunlap**

University of Maryland

**Dr. Bill Johnson**

Laboratory for Physical Sciences