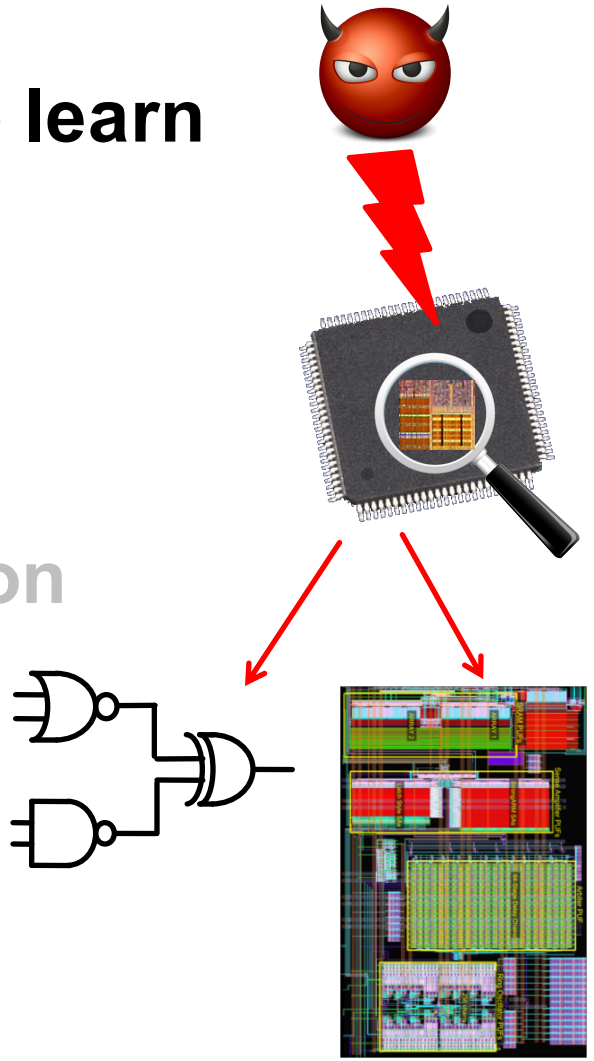
IC Reverse Engineering

“VAX – when you care to steal the very best”

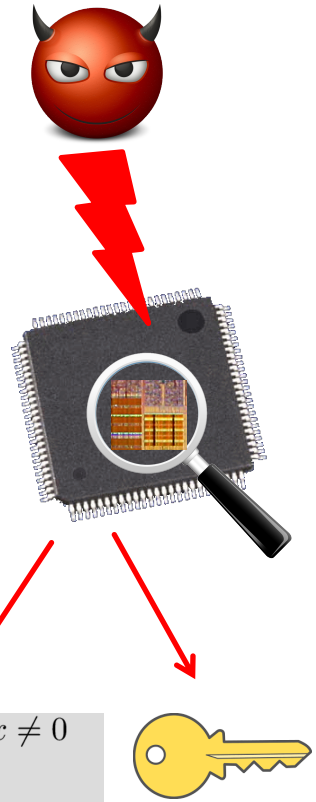
RE Attacker Model

- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks



RE Attacker Model

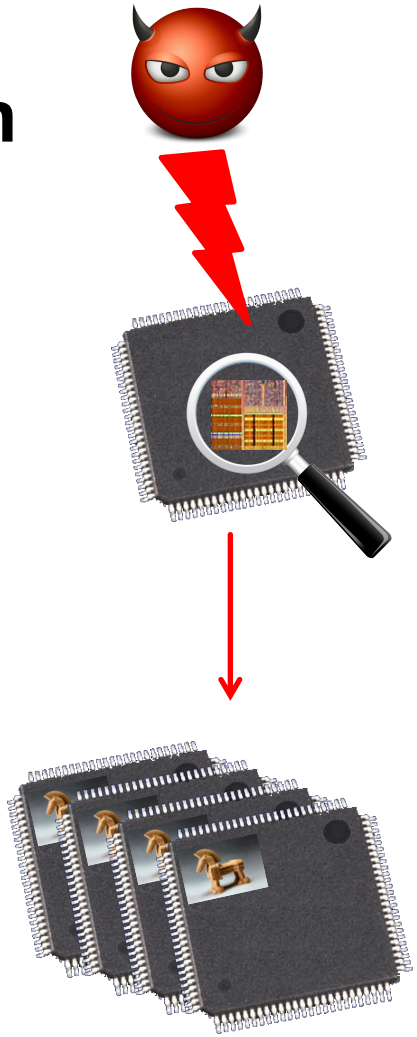
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks



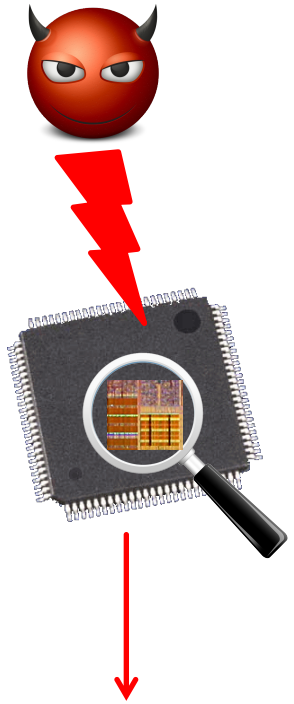
Require: $n \geq 0 \vee x \neq 0$
Ensure: $y = x^n$
  $y \leftarrow 1$
  if $n < 0$ **then**
    $X \leftarrow 1/x$
    $N \leftarrow -n$
  else
    $X \leftarrow x$
    $N \leftarrow n$
  end if

RE Attacker Model

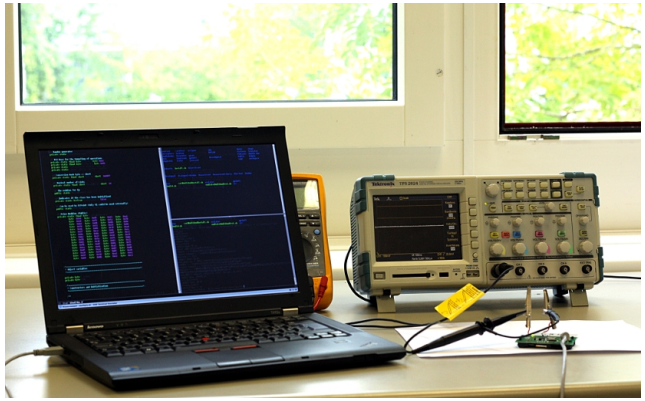
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks



RE Attacker Model

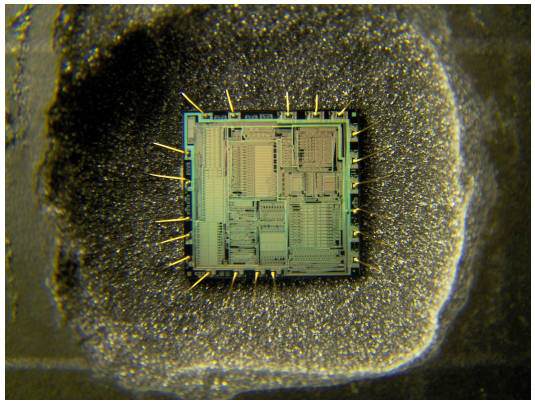


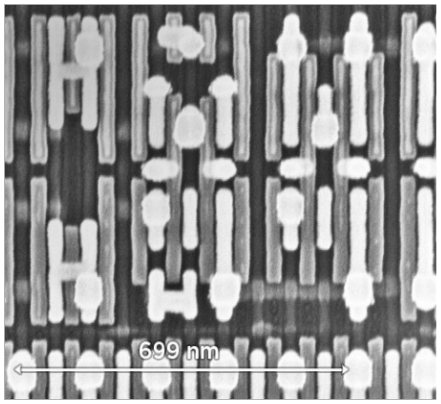
- **Goal: Reverse engineer the IC to learn**
  - Functionality
  - Internal structure
  - Manufacturing process details
- **Uses for the extracted information**
  - Steal intellectual property and secrets
  - Create clones or insert Trojans
  - Enhance other attacks

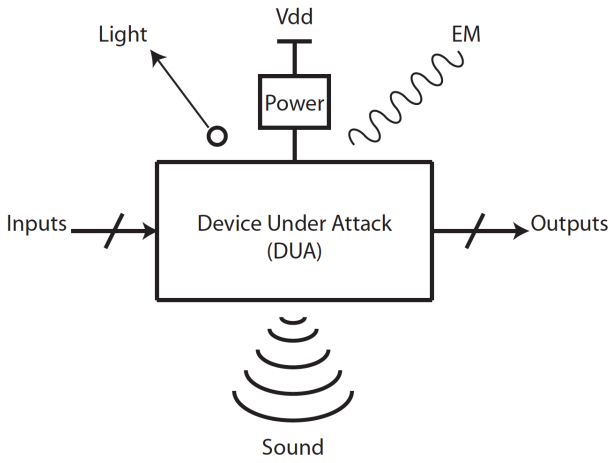


Assumptions

- **Attacker has direct prolonged physical access**
  - Multiple (but not unlimited) samples
- **State-of-art IC reverse engineering capabilities**
  - De-packaging and de-layering
  - Advanced probing and imaging
  - Side-channel examination
- **Design & manufacturing secured by other means**





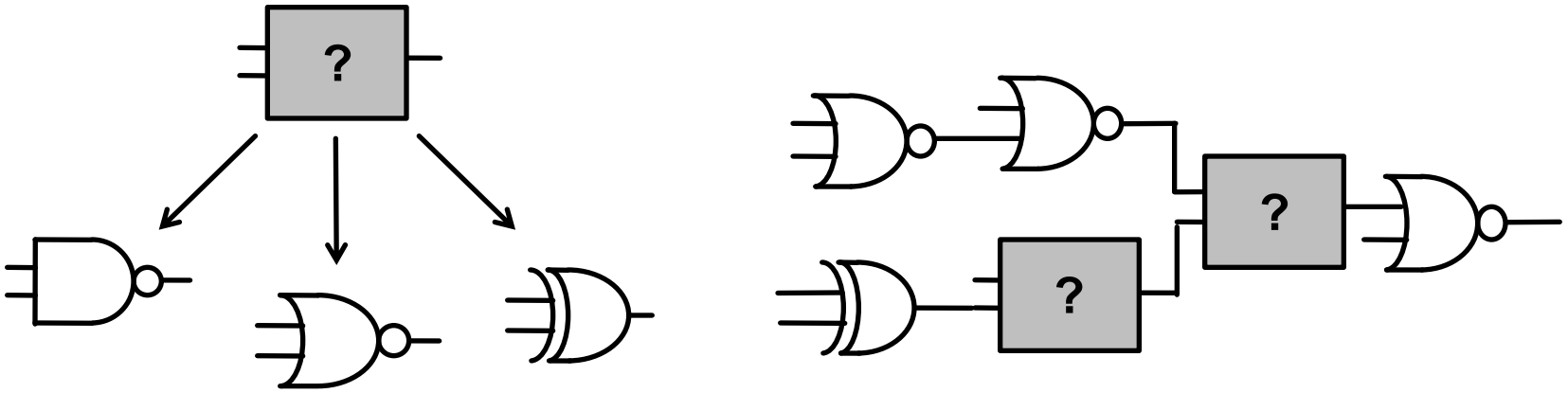


Reverse Engineering Countermeasures

- Tamper resistant design
- Keyed logic and FSMs[1] [2]
- Camouflaged gates[3] [4]

[1] Y. Alkabani et al., "Active Hardware Metering for IP Protection and Security", USENIX'07.
[2] J. Rajendran et al., "Security Analysis of Logic Obfuscation", DAC'12.
[3] J. Rajendran et al., "Security Analysis of Integrated Circuit Camouflaging", CCS'13.
[4] SypherMedia Circuit Camouflage Technology [Online]. Available: http://www.smi.tv/camo_data_sheet.pdf

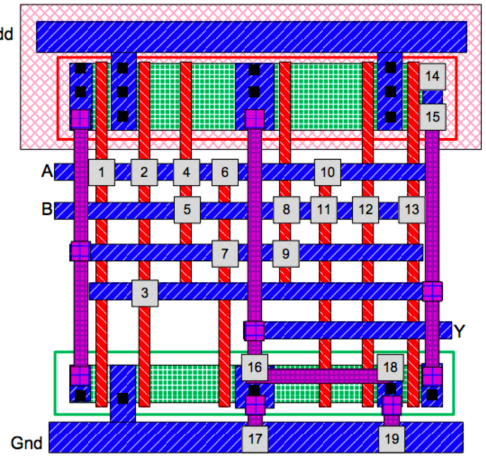
Camouflaged Gates



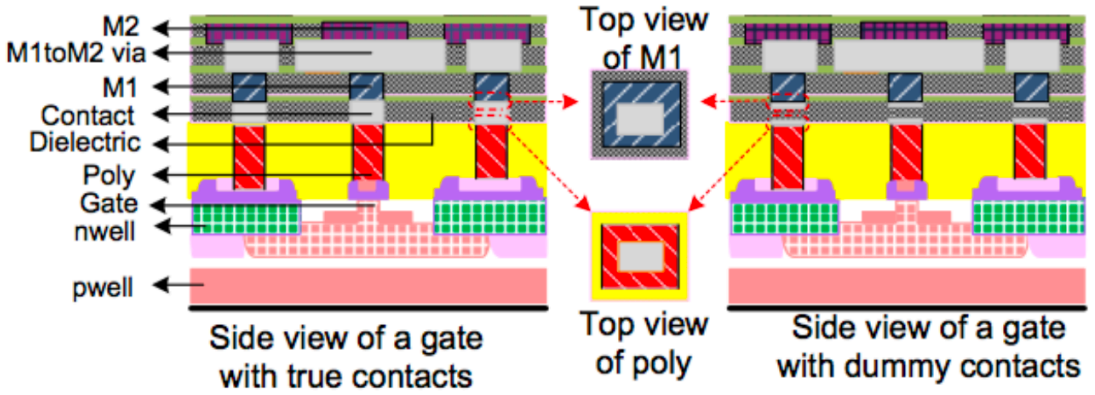
- **Hide logical function of gate from attacker**
- **Use look-alike gates**
  - Very similar layouts
  - Different Boolean function
- **Replace some gates w/ camouflaged ones**

[1] J. Rajendran et al., "Security Analysis of Integrated Circuit Camouflaging", CCS'13.
[2] SypherMedia Circuit Camouflage Technology [Online]. Available: http://www.smi.tv/camo_data_sheet.pdf

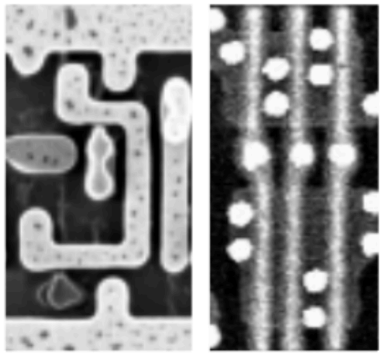
Example Camouflaged Gates



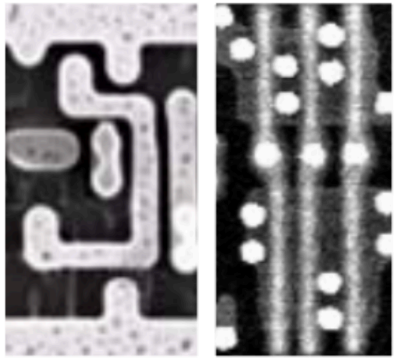
[J. Rajendran et al.]



[J. Rajendran et al.]



SypherMedia Regular AND2 gate[2]



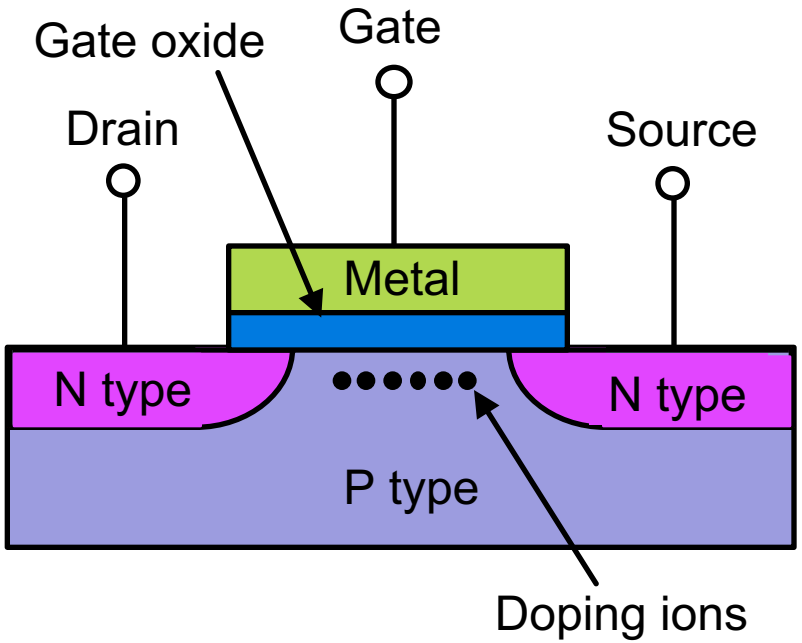
SypherMedia AND2 look-alike gate[2]

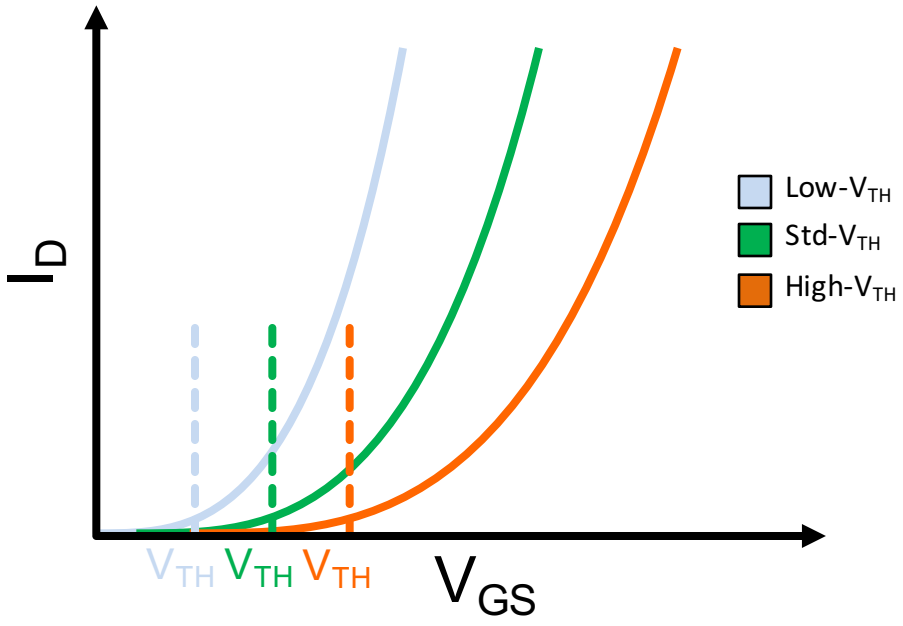
[1] J. Rajendran et al., "Security Analysis of Integrated Circuit Camouflaging", CCS'13.
[2] SypherMedia Circuit Camouflage Technology [Online]. Available: http://www.smi.tv/camo_data_sheet.pdf

Issues w/ Current Camouflaged Gates

- **Security relies on limited RE resolution**
  - Dummy contact detectable with careful de-processing
  - Look-alike gates may be discernable
- **Incompatibility w/ standard process and tools**
  - Additional mask layers and process steps
  - DRC waivers and non-standard structures
- **High area, power, and delay overheads**
  - Up to 4x, 5.5x, and 1.8x respectively
  - Limits # of gates that can be feasibly camouflaged

Threshold Voltage Defined Logic (TVD)





- Today's processes offer multiple transistor V_{TH}'s
- Devices differ only in # ions implanted in channel
- Allow designers to trade-off speed and power

Can we build a gate that uses V_{TH} to set function?

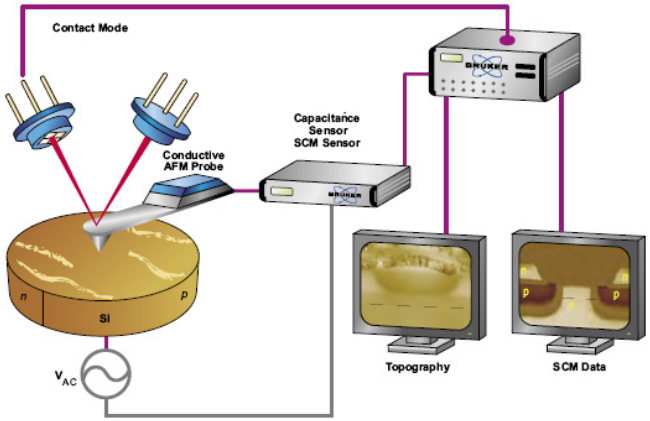
Threshold Voltage Defined Logic (TVD)

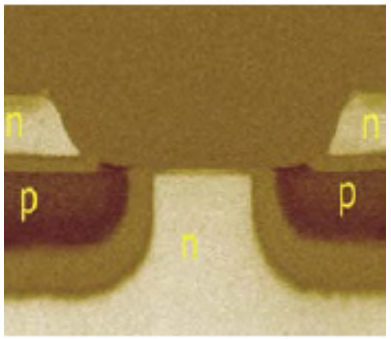
DARPA 2015 Young Faculty Award Call

Technical Area One: **Threshold-Defined Logic Engines:** YFA proposers are invited to submit ideas for CMOS chip architectures which enable a single fixed chip design and layout to present as multiple disparate logic engines, where each logic engine is defined solely by the threshold voltages asserted on each device during manufacturing. The logic engines must be distinct from one another, with each being stable and robust to conventional process / voltage / temperature (PVT) tolerances. Proposers should not offer conventional ROM/ROS memory array solutions which are personalized by threshold or enhancement/depletion mode NMOS or PMOS; but rather very specific true logic engines which assume very different personalities given the same inputs, dependent only upon the threshold voltages selected. Assume that the threshold voltages available are limited to the three typical current device offerings made available by the major fabs:

- High Vt, low leakage, lower performance bulk PFETs and NFETs
- Regular Vt, nominal leakage, nominal performance bulk PFETs and NFETs
- Low Vt, high leakage, high performance bulk PFETs and NFETs

Reverse Engineering Transistor V_{TH}

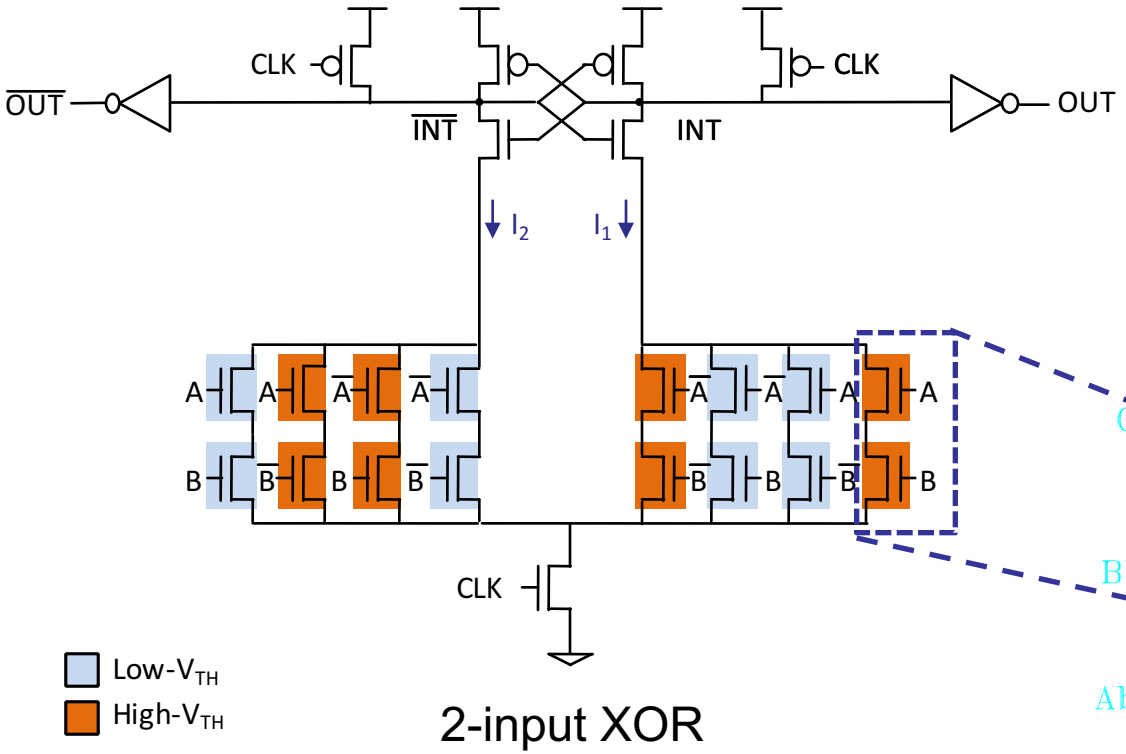


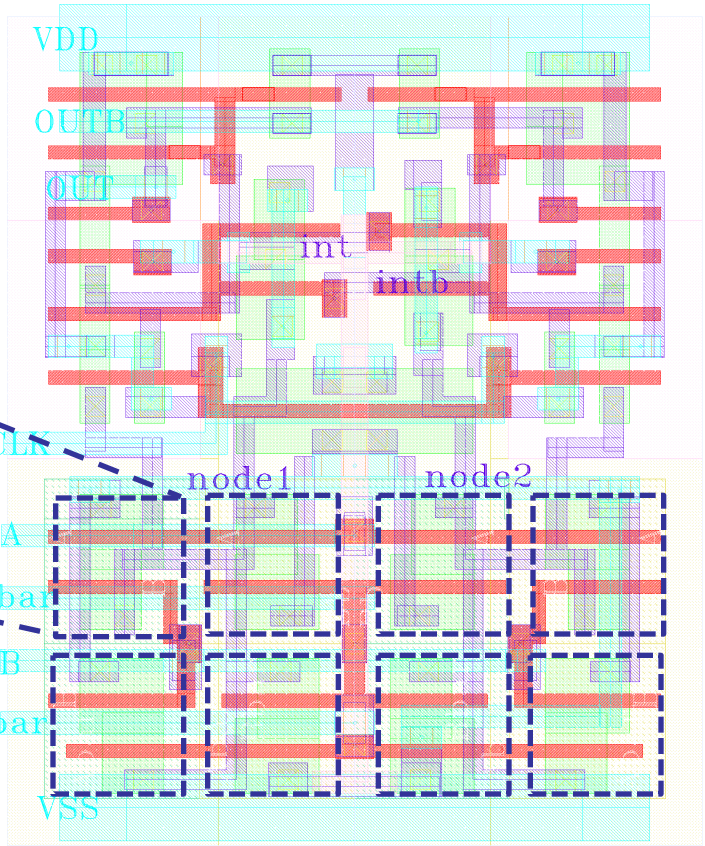


- **Can the attacker read out the V_{TH}?**
  - Yes and no …
- **Yes – Can measure individual device channel doping**
  - Spreading resistance profiling[1]
  - Secondary ion-mass spectrometry[2]
  - Scanning capacitance microscopy[3]
- **No – Infeasible for large scale RE**
  - Limited spatial resolution and accuracy
  - Large number of device V_{TH}'s to probe out
  - Unsuitable for chip-scale RE

[1] W. Vandervorst et al., "Spreading resistance roadmap towards and beyond the 70nm technology", Journal of Vac. Sci and Tech., 2002.
[2] N. Duhayon et al., "Assessing the performance of two-dimensional dopant profiling techniques", Journal of Vac. Sci and Tech., 2004.
[3] C. C. Williams, "Two-dimensional Dopant Profiling by Scanning Capacitance Microscopy", Annual Review of Materials Sci., 1999.

Sneak Peek …



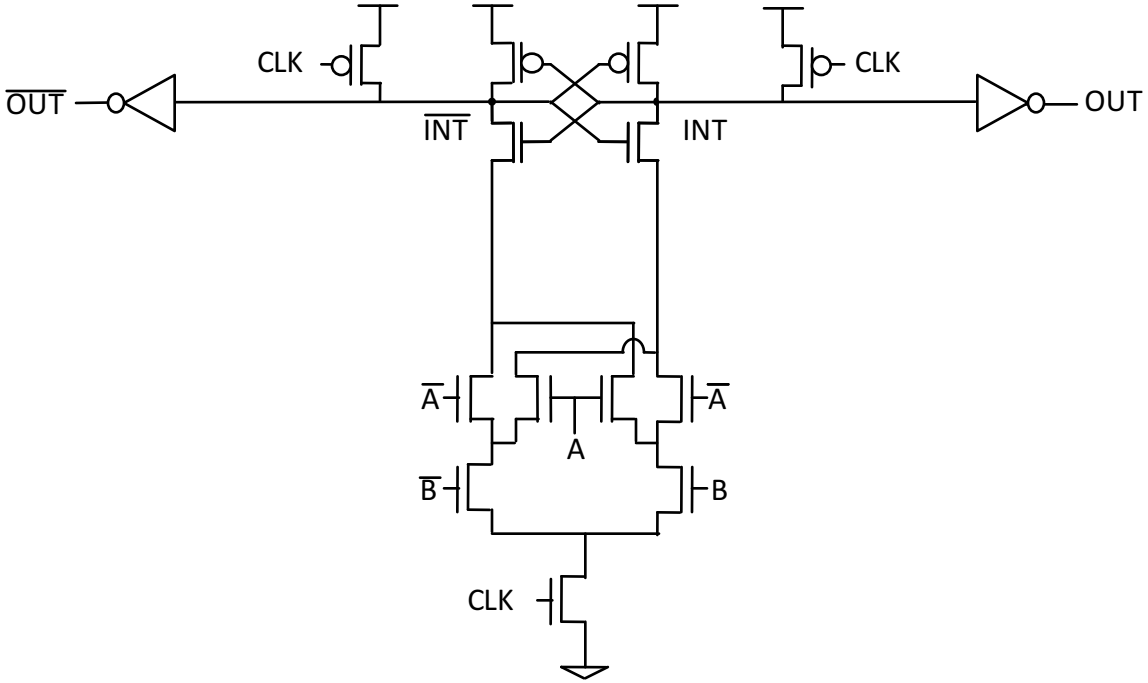


- **Differential dynamic amplifying gate**
- **Logic function set by V_{TH} implant**
- **All gates have identical layout (except V_{TH} masks)**

TVD Camouflaging Advantages

- **Security not reliant on limited RE resolution**
  - V_{TH} to set logic function, otherwise identical layout
- **Fully CMOS logic process compatible**
  - No special layers, masks, or DRC waivers needed
- **Modest area, power, and delay overheads**
  - Large-scale camouflaging of gates feasible
- **Low side-channel emissions (power/timing)**
  - Due to differential structure and homogeneity

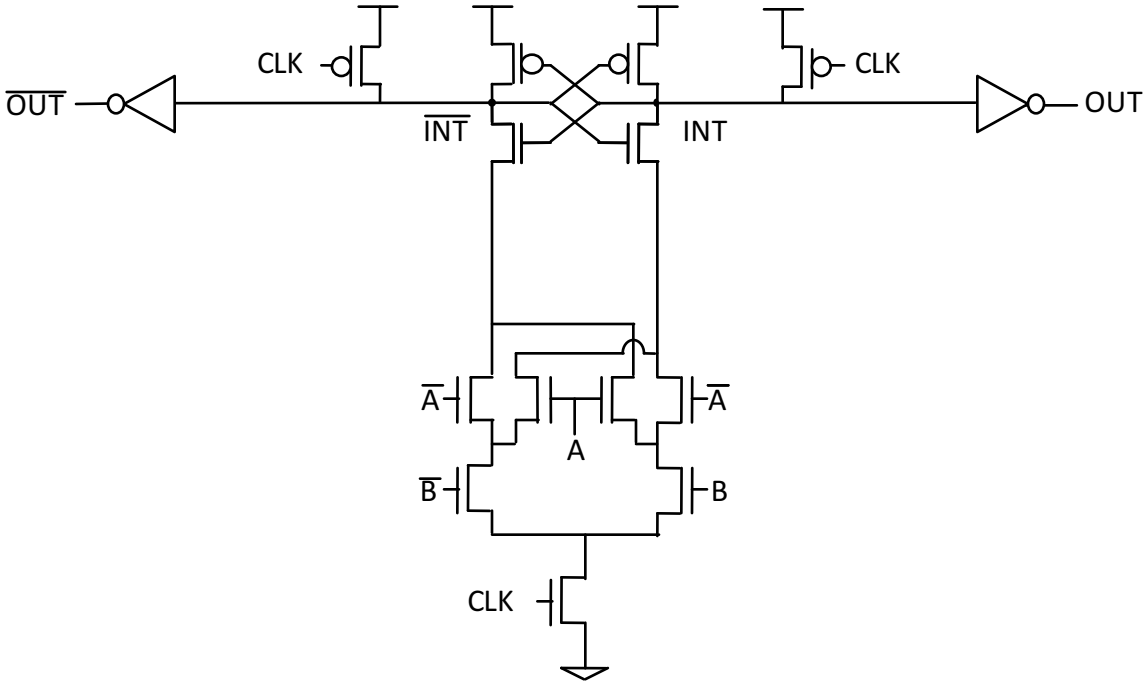
Sense-Amplifier Based Logic



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

- **Dual-rail dynamic amplifying logic family**
- **Two phases of operation**
  - Pre-charge
  - Evaluate

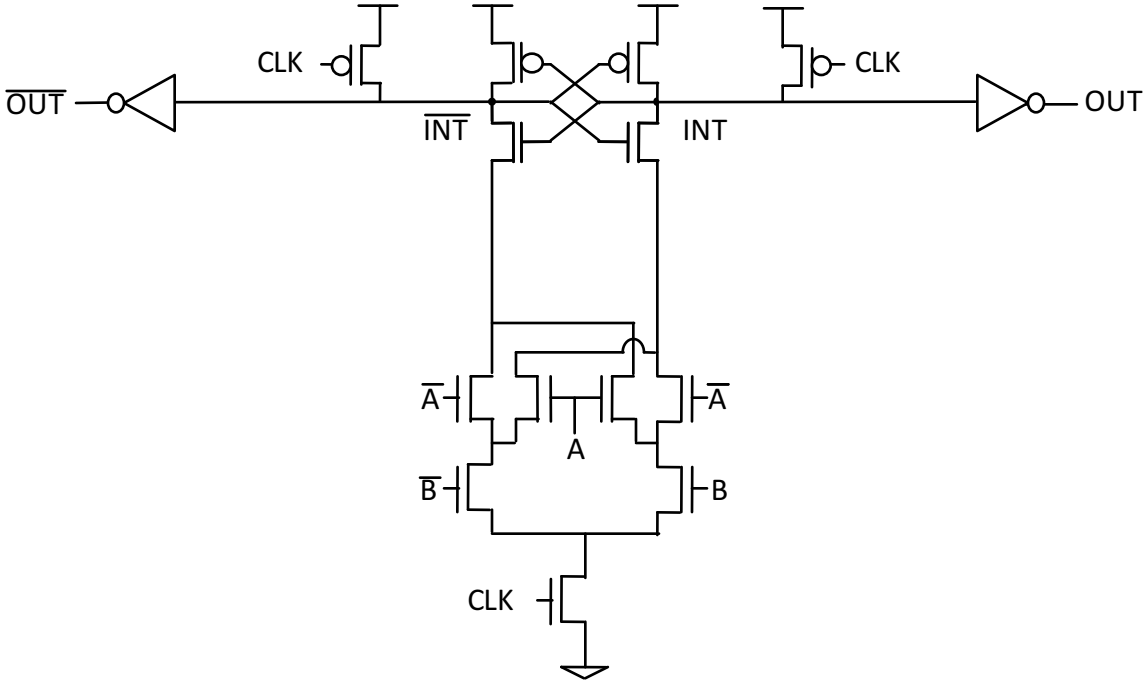
Sense-Amplifier Based Logic



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

- **Dual-rail dynamic amplifying logic family**
- **Two phases of operation**
  - Pre-charge
  - Evaluate

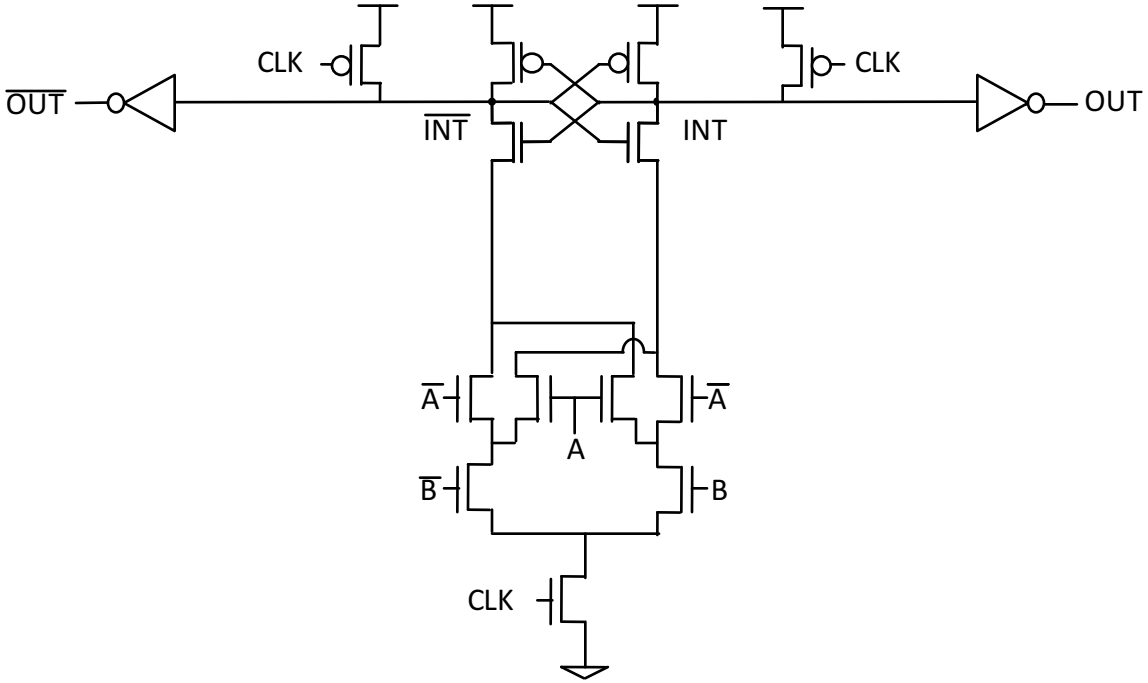
Sense-Amplifier Based Logic



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

- **Dual-rail dynamic amplifying logic family**
- **Two phases of operation**
  - Pre-charge
  - Evaluate

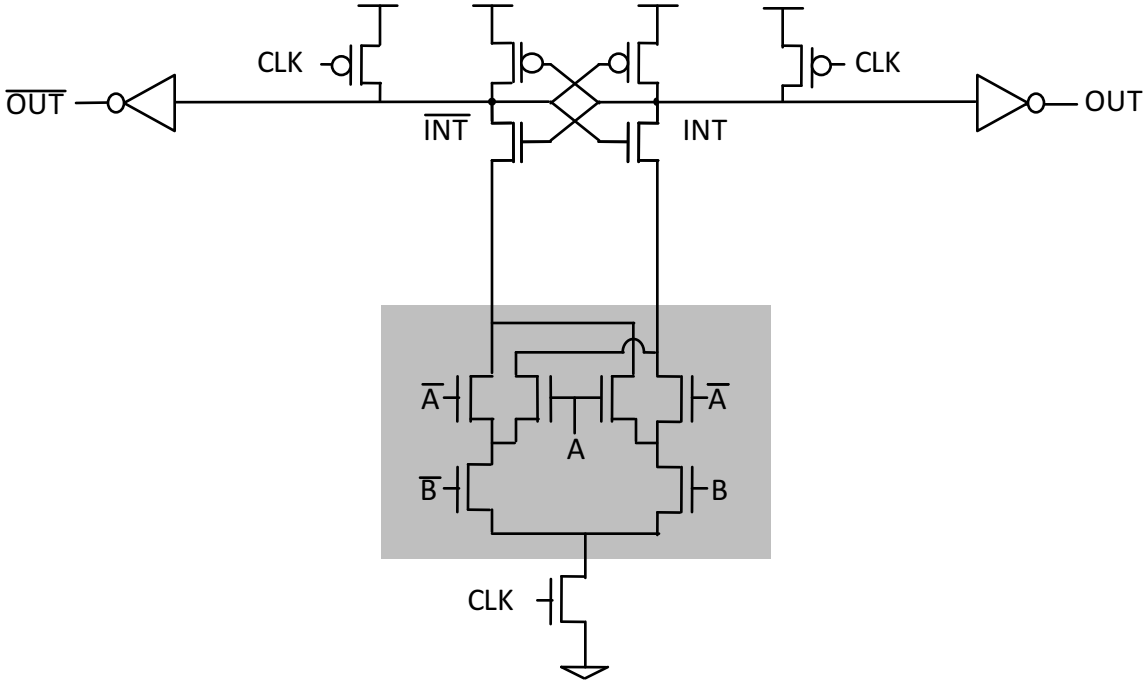
Sense-Amplifier Based Logic



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

- **Dual-rail dynamic amplifying logic family**
- **Two phases of operation**
  - Pre-charge
  - Evaluate

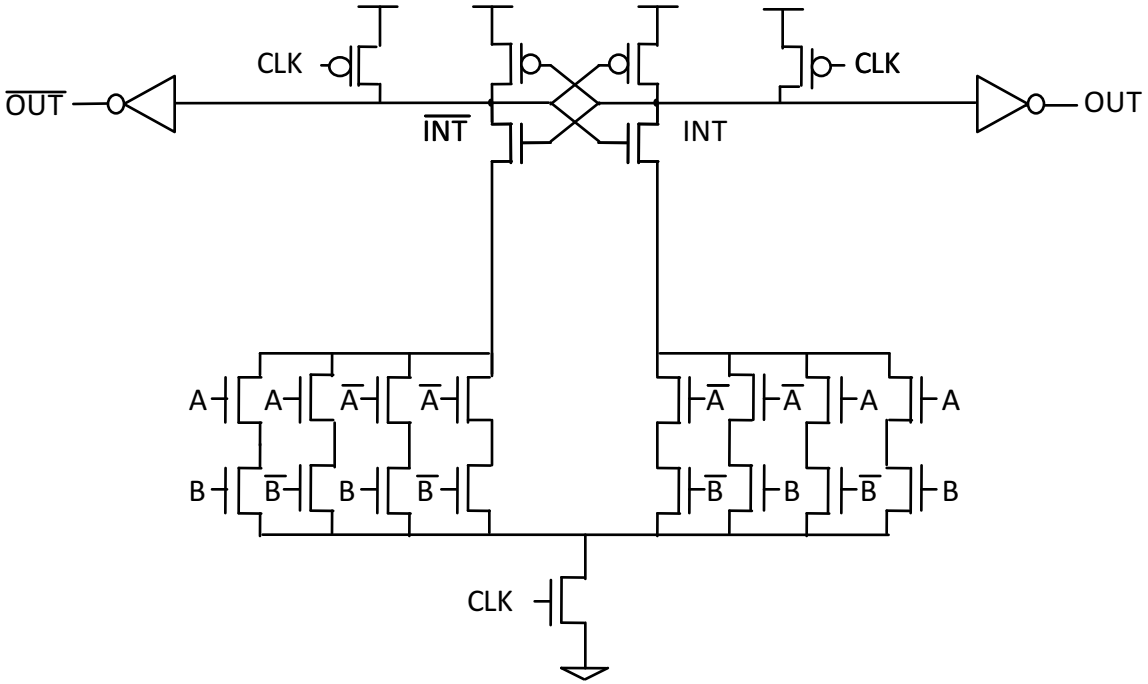
Sense-Amplifier Based Logic



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

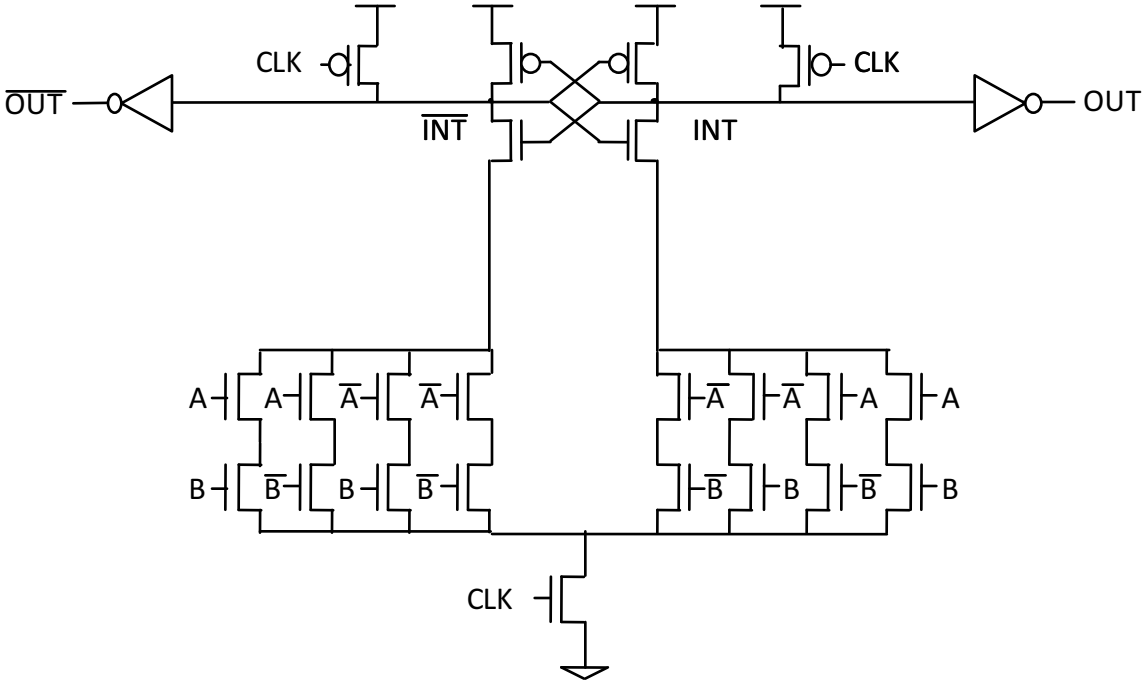
- **Dual-rail dynamic amplifying logic family**
- **Two phases of operation**
  - Pre-charge
  - Evaluate

Generic 2-input TVD Logic Gate



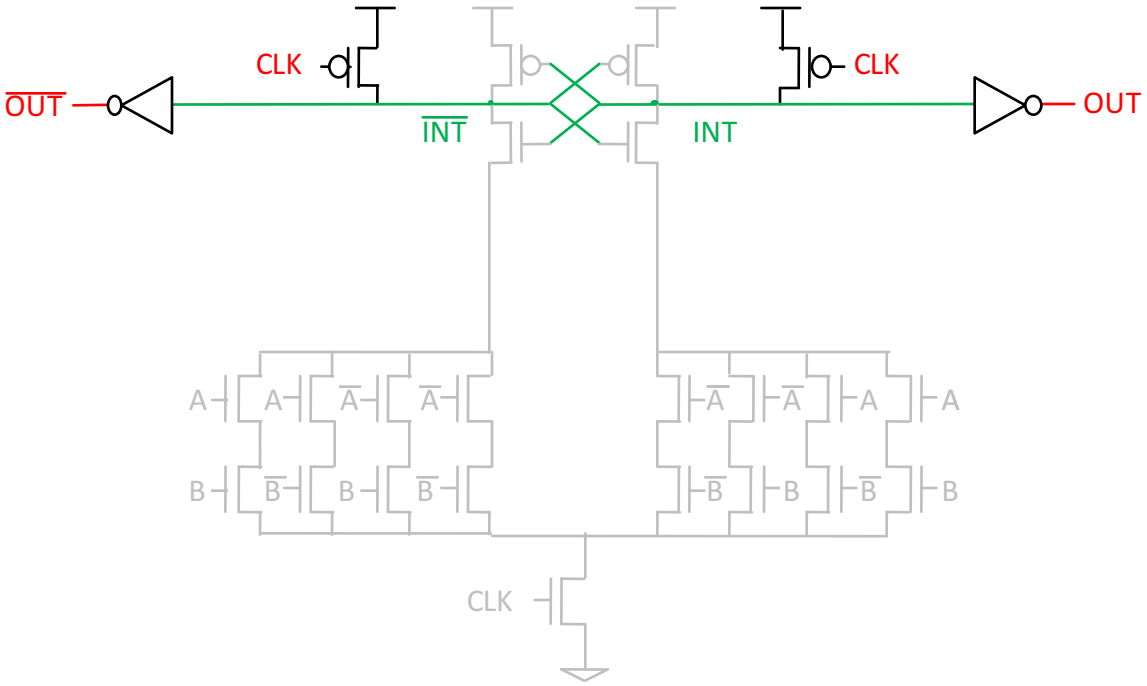
- Generic differential pull-down network
- Both left & right branches conduct (asymmetrically)
- Current difference (ΔI) amplified when gate fires
- Use different V_{TH} implants to introduce ΔI

Example: 2-input TVD XOR Gate



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate

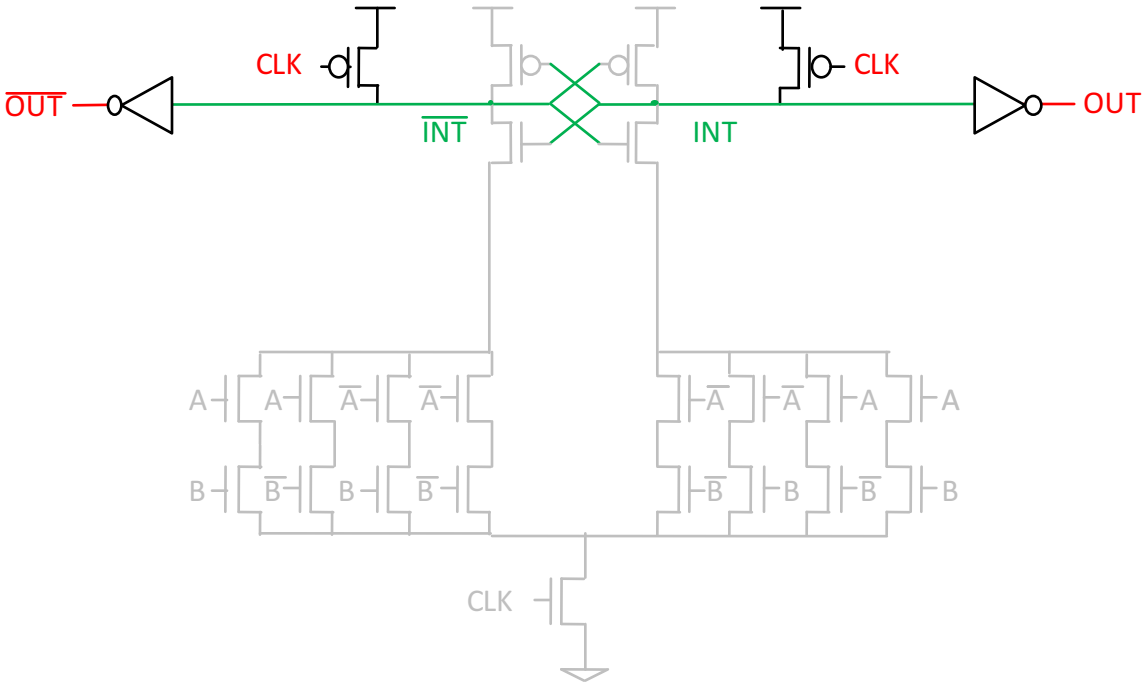


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

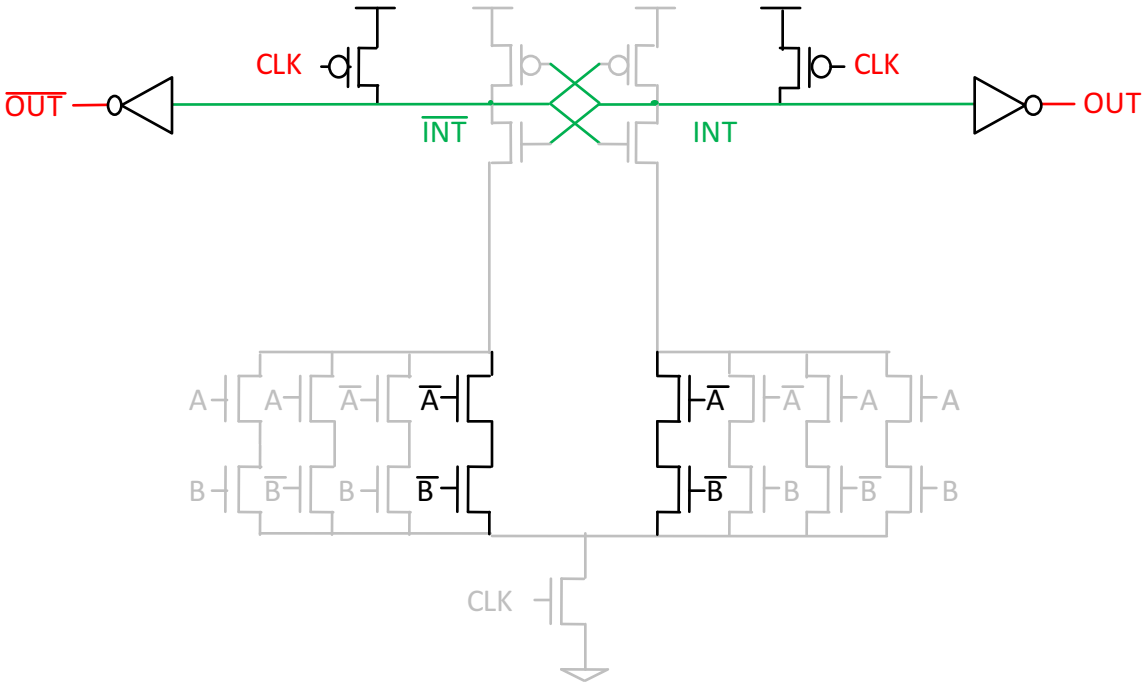


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

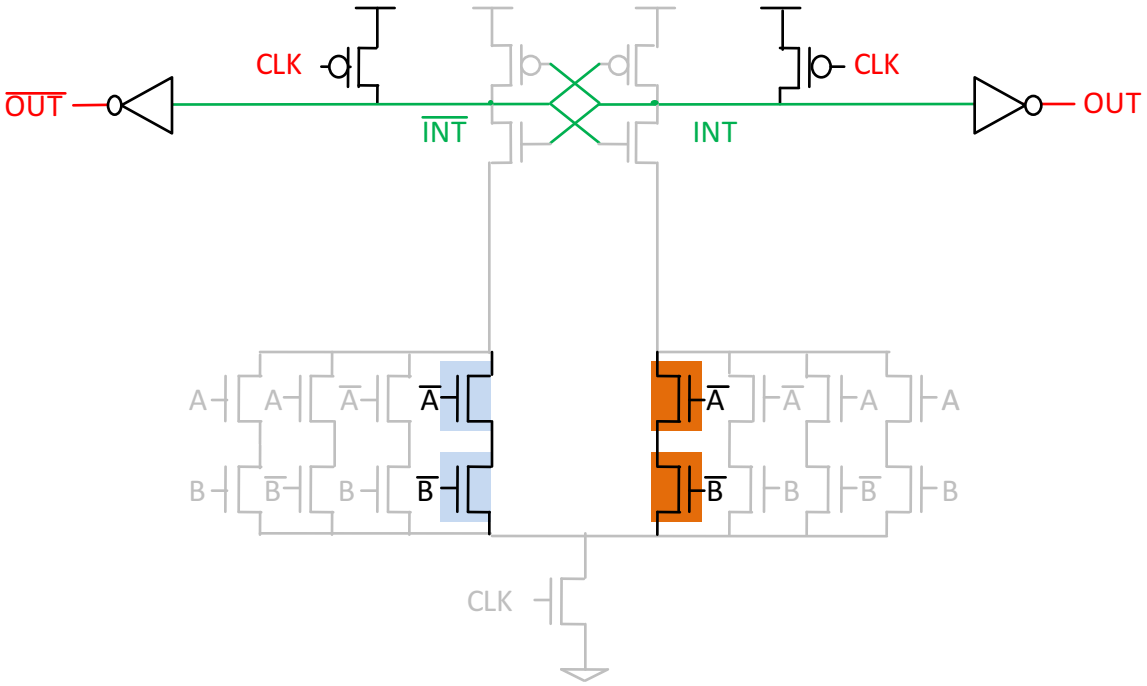


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

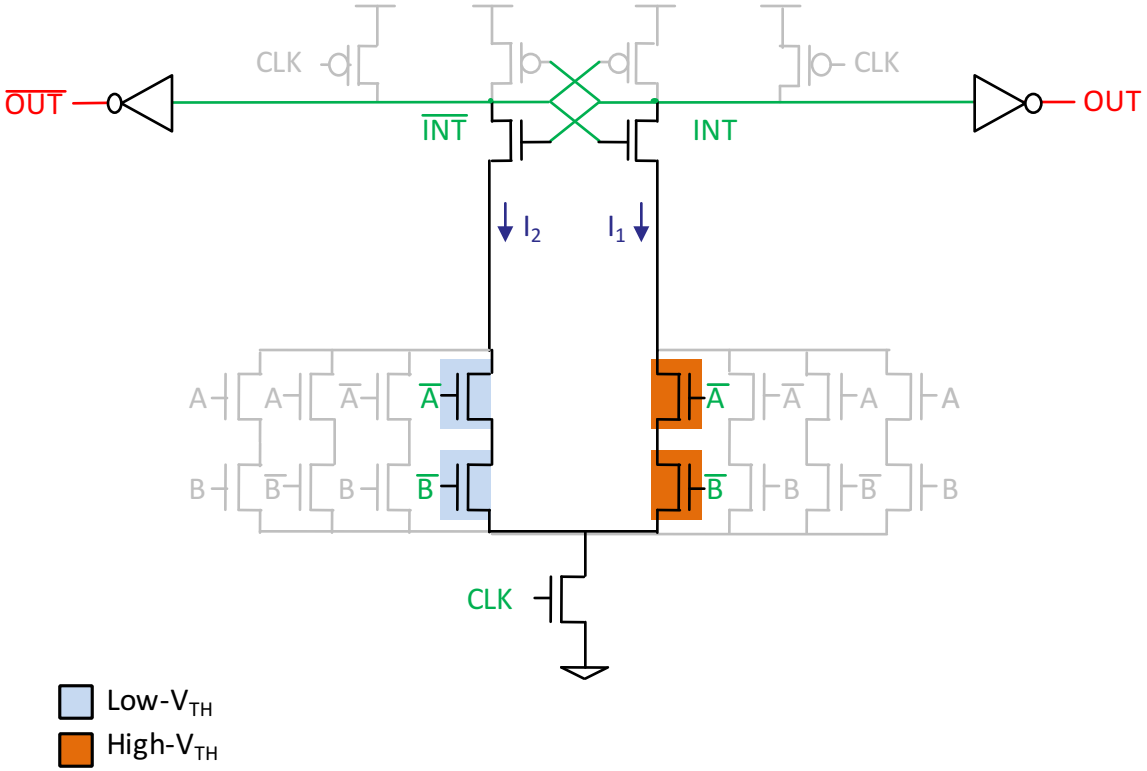


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

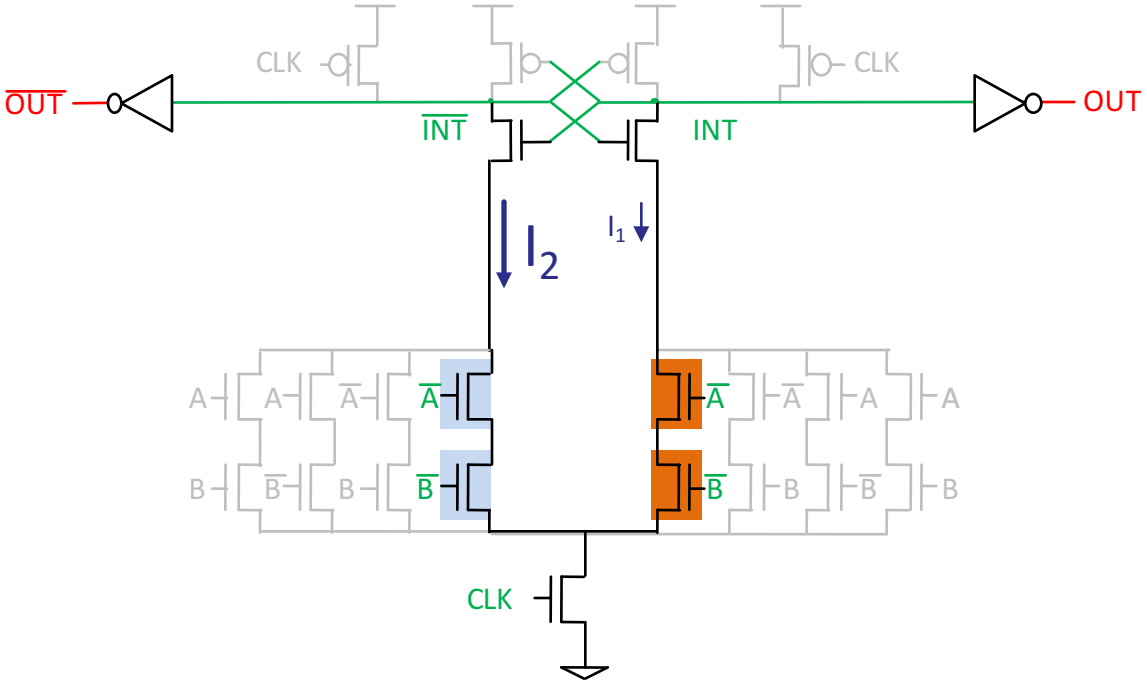


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

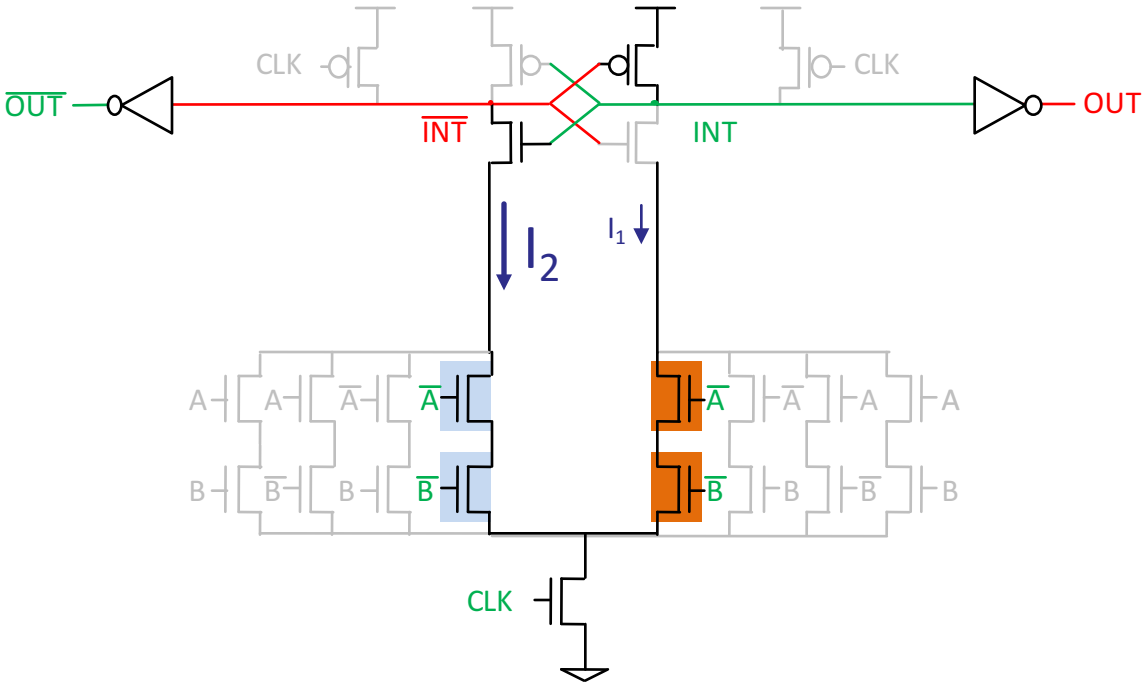


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

0

Example: 2-input TVD XOR Gate

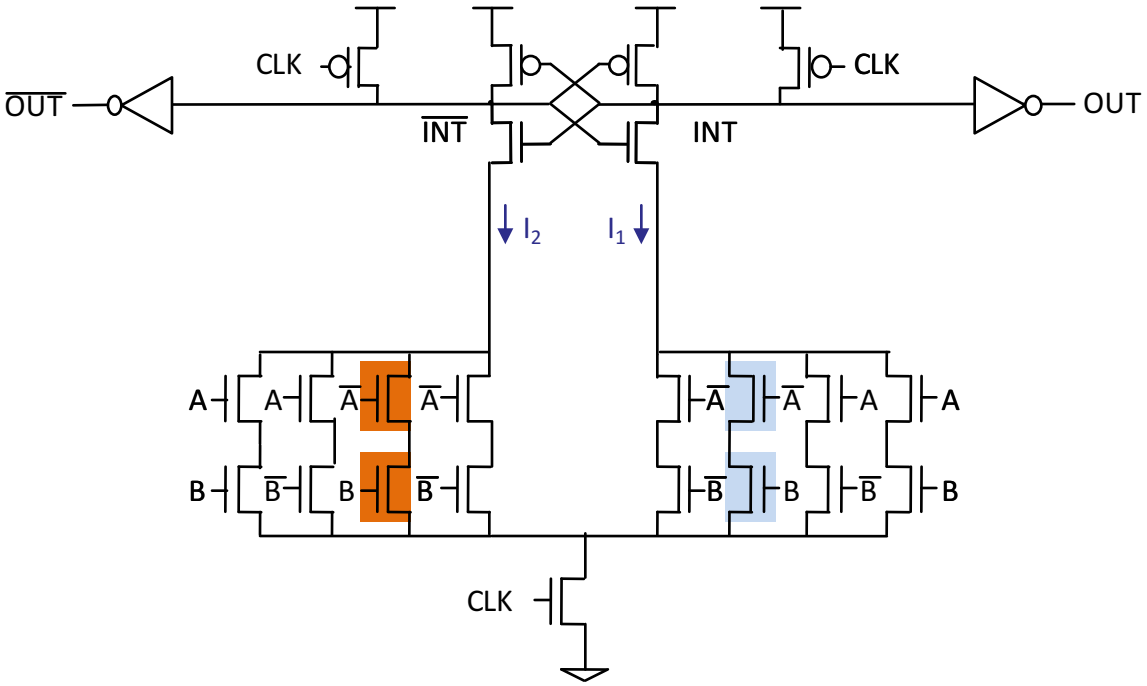


A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

1

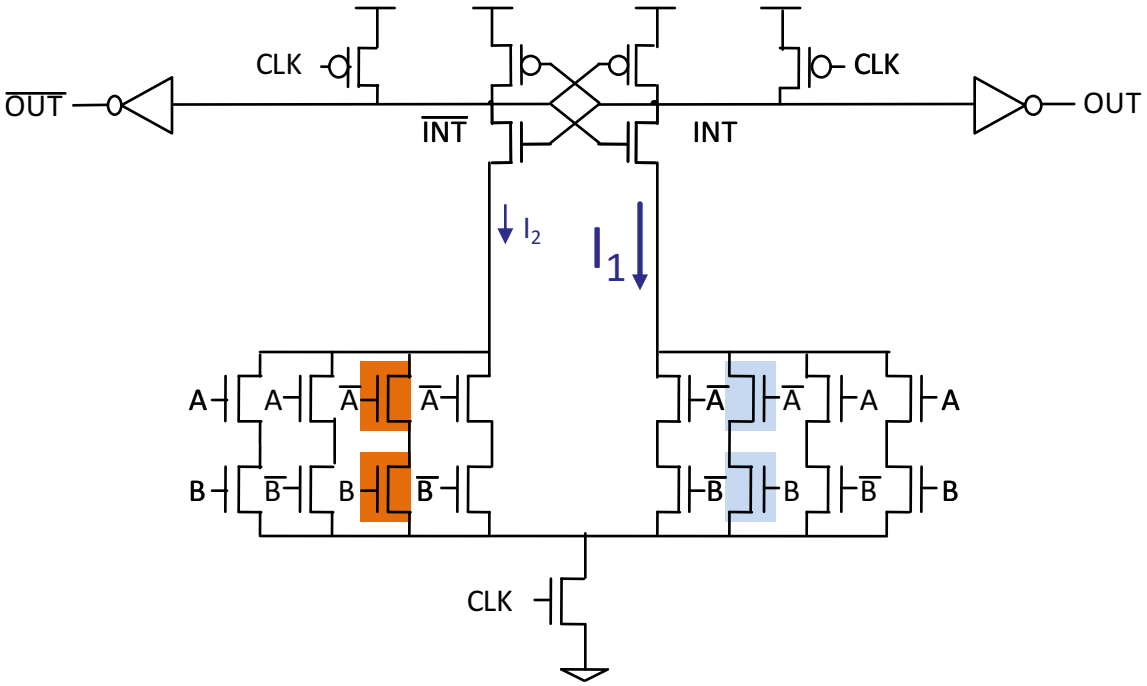
0

Example: 2-input TVD XOR Gate



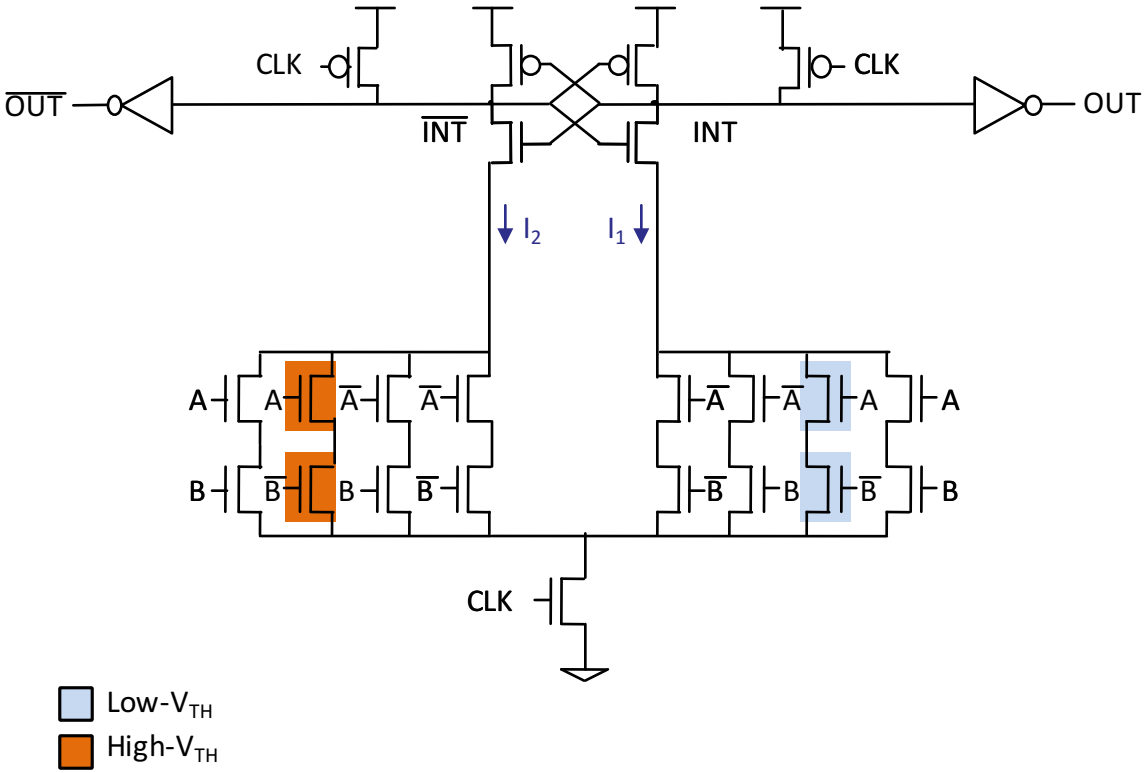
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



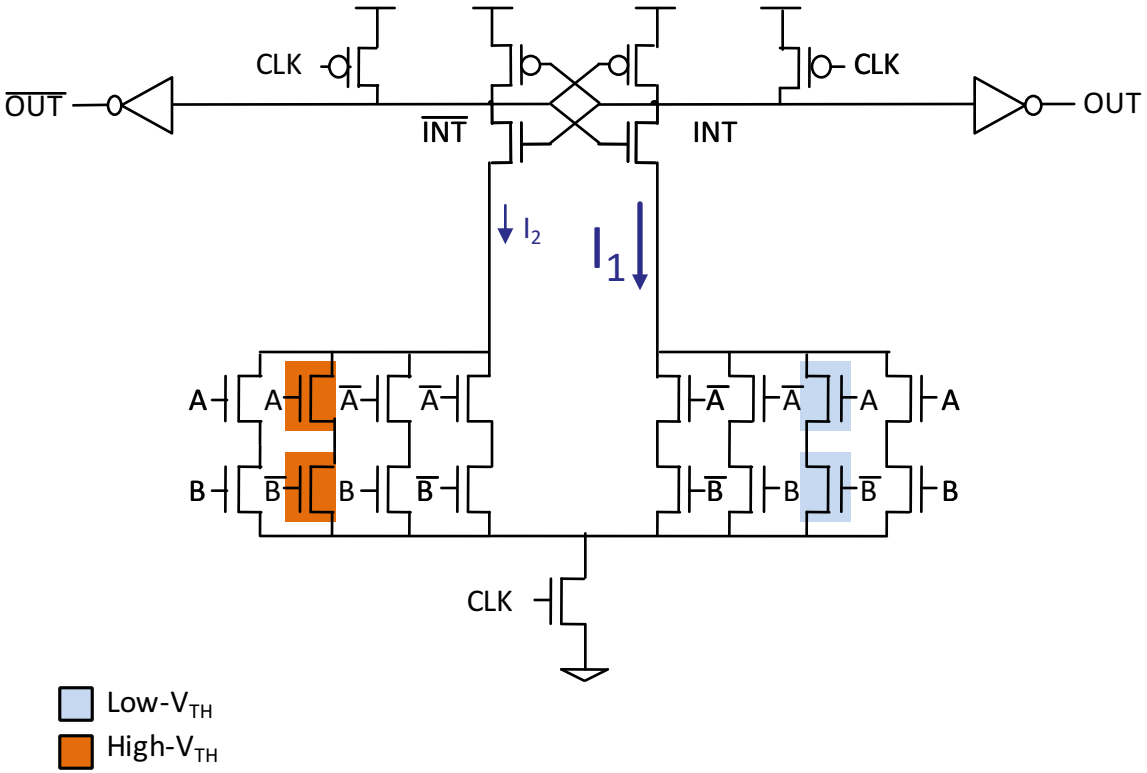
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



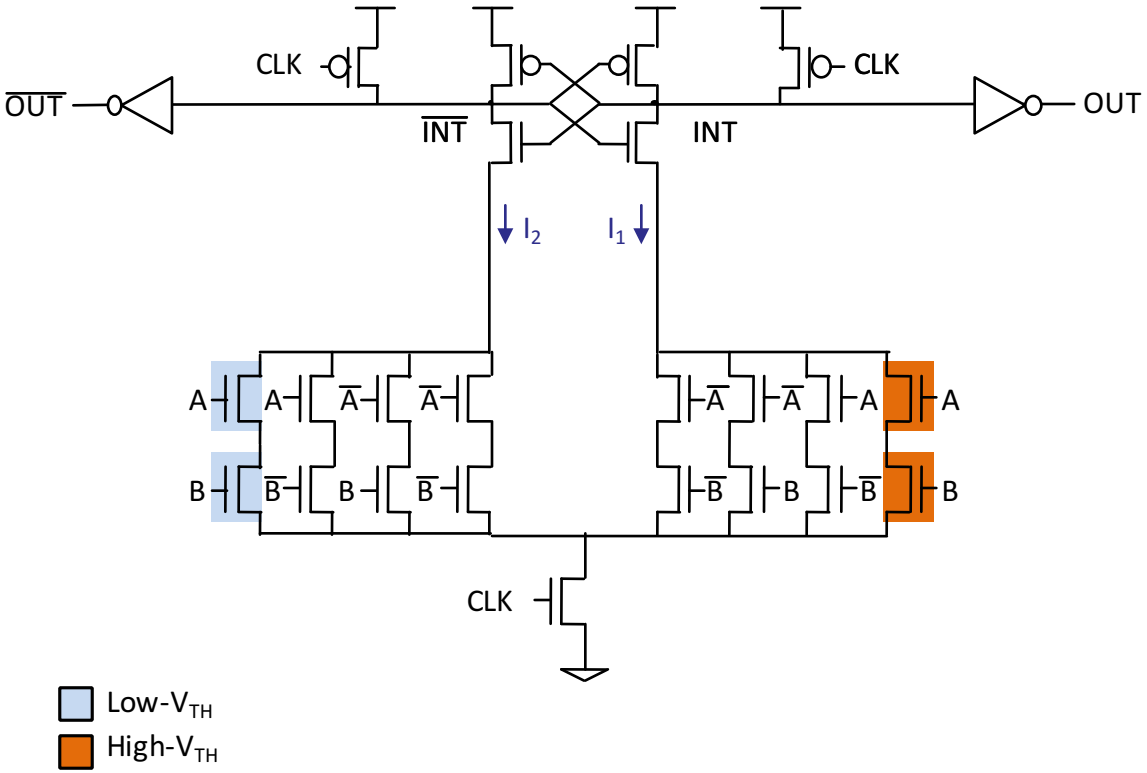
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



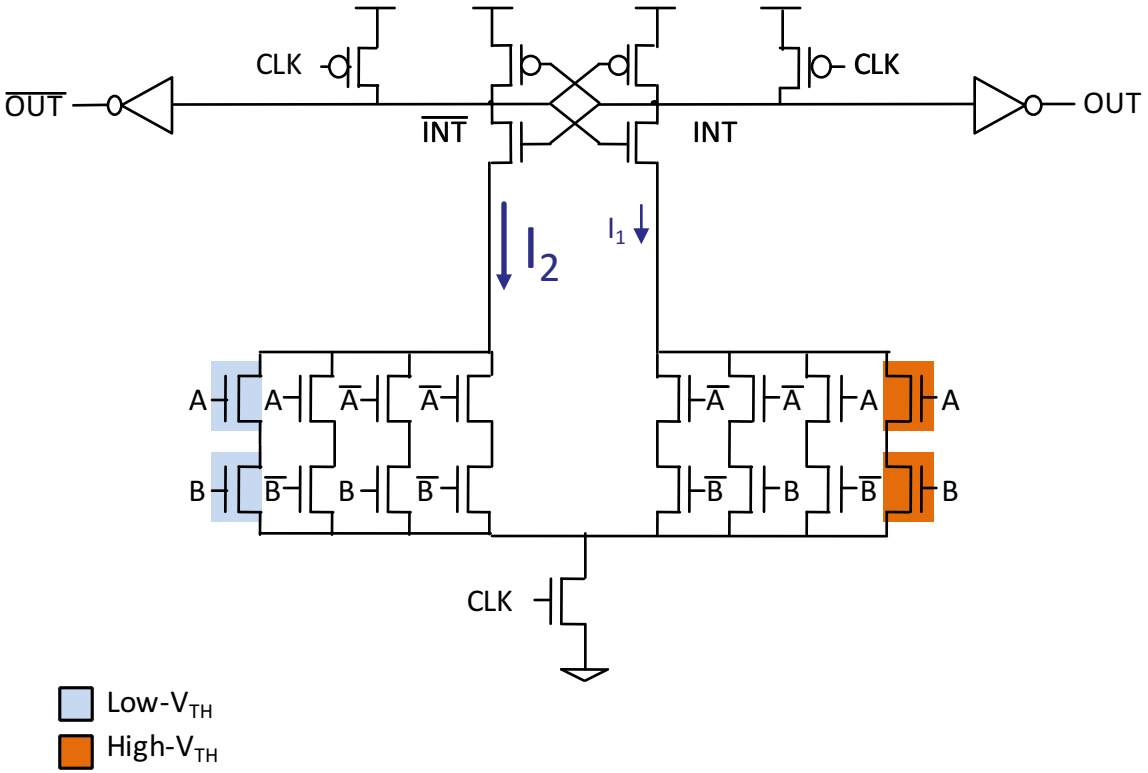
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



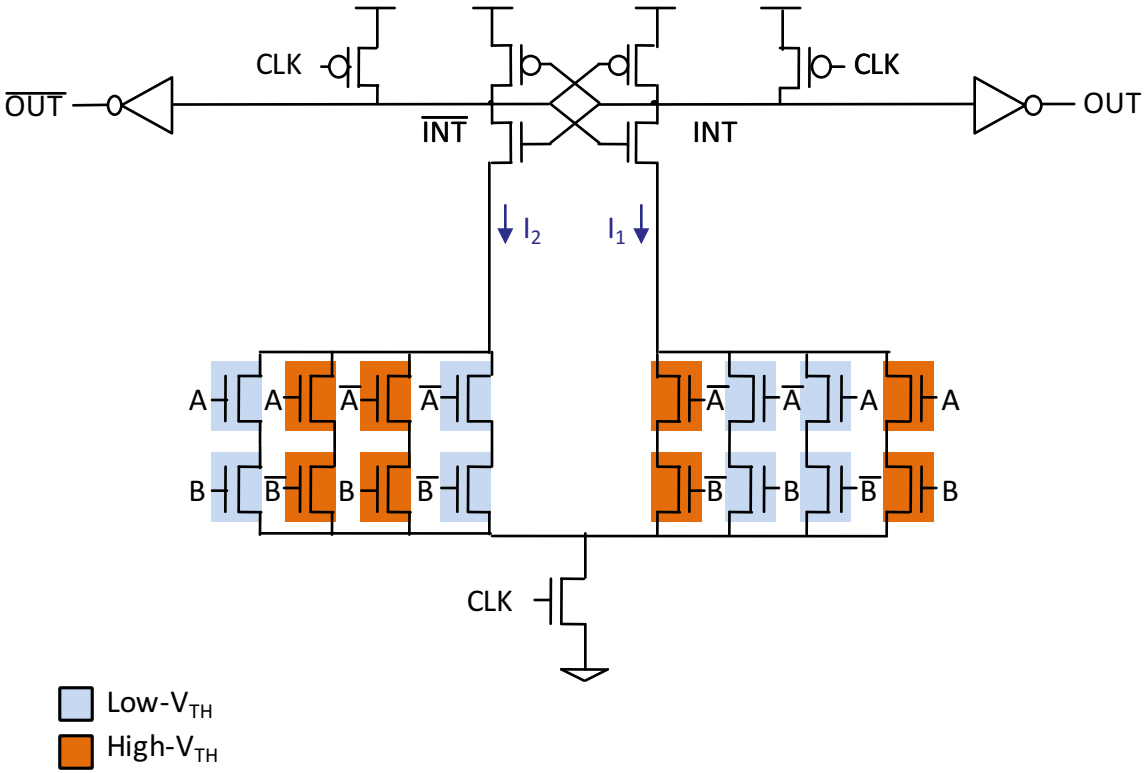
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



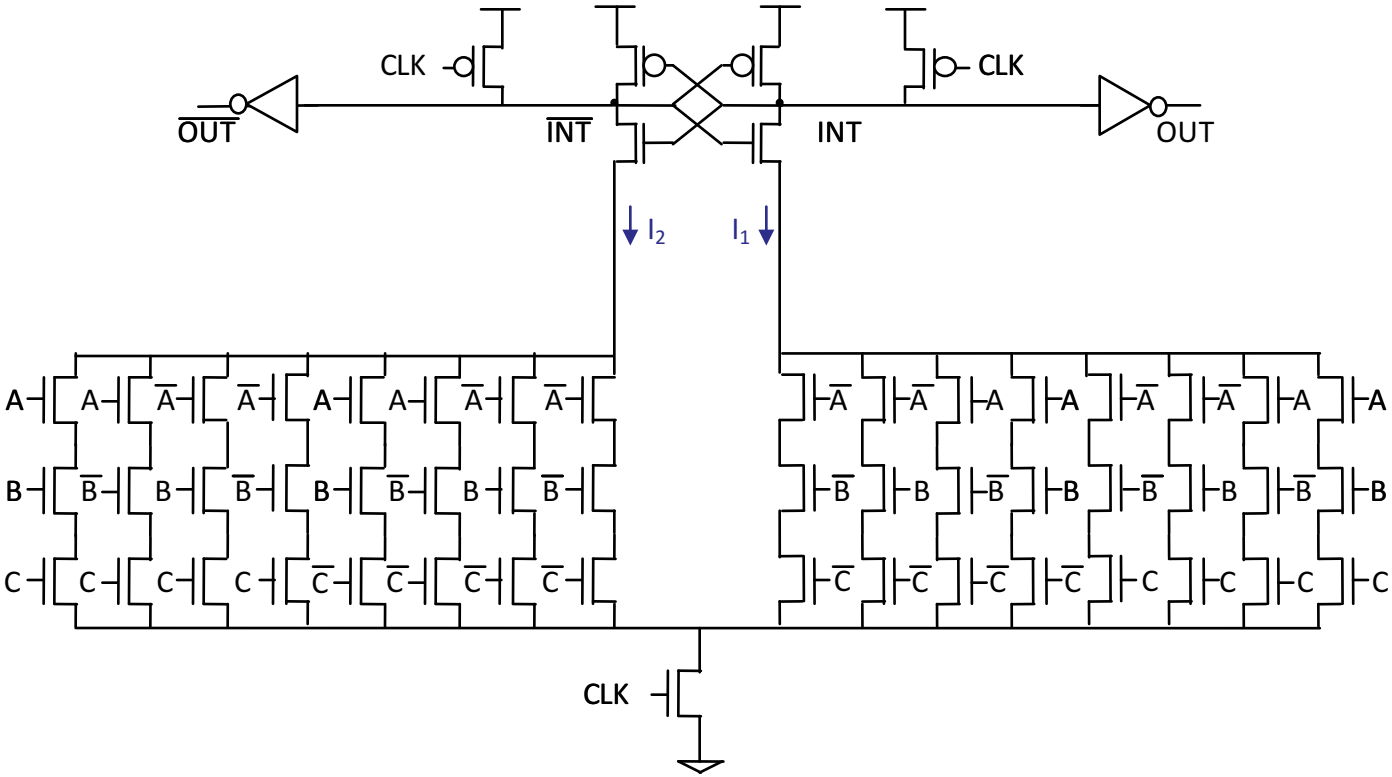
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

Example: 2-input TVD XOR Gate



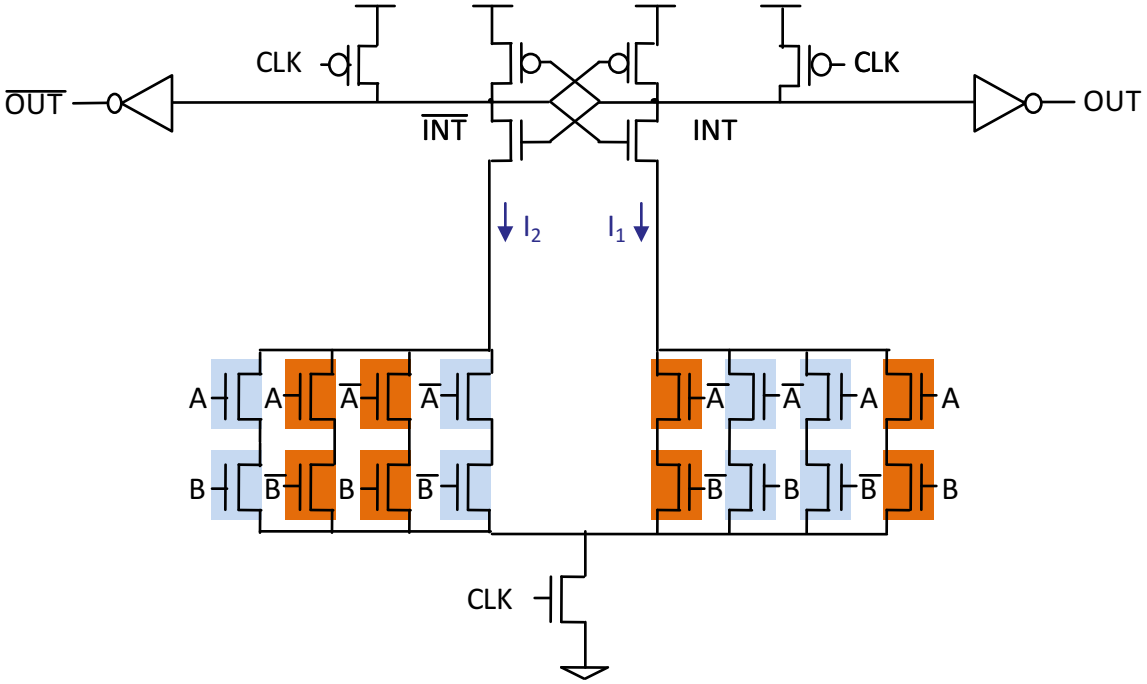
A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

3-Input TVD Logic Gate



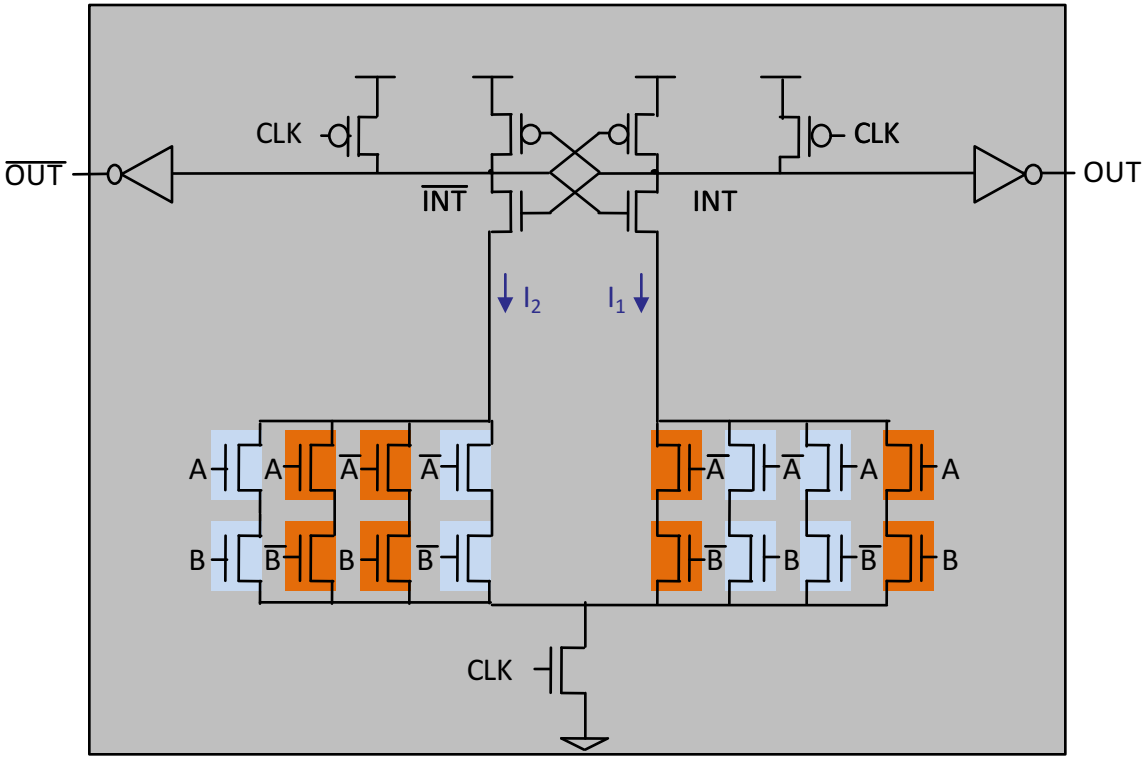
- Implements any 3-input Boolean function
- TVD concept scales to any n-input gate
- Number of parallel strings increases exponentially (2^n)

Chaining TVD Logic Gates



A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

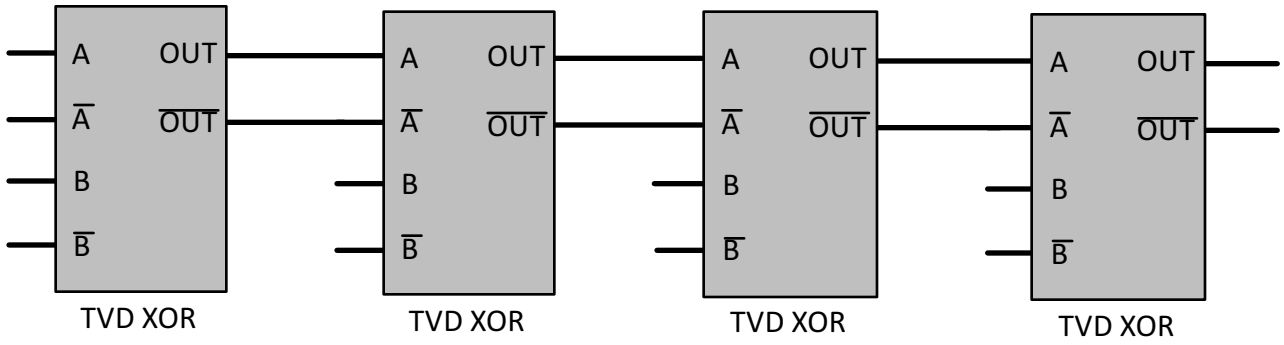
Chaining TVD Logic Gates



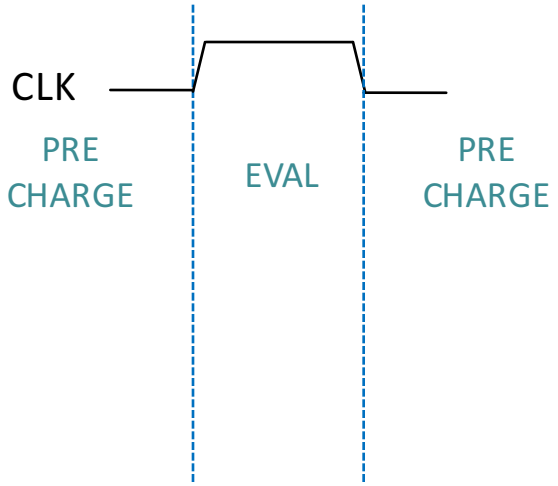
TVD XOR

A	B	XOR	XNOR
0	0	0	1
0	1	1	0
1	0	1	0
1	1	0	1

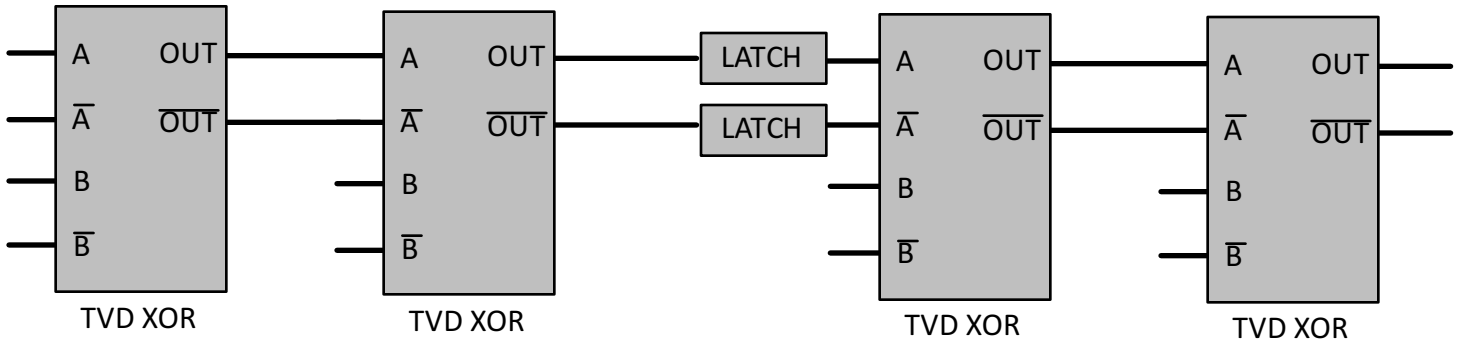
Chaining TVD Logic Gates



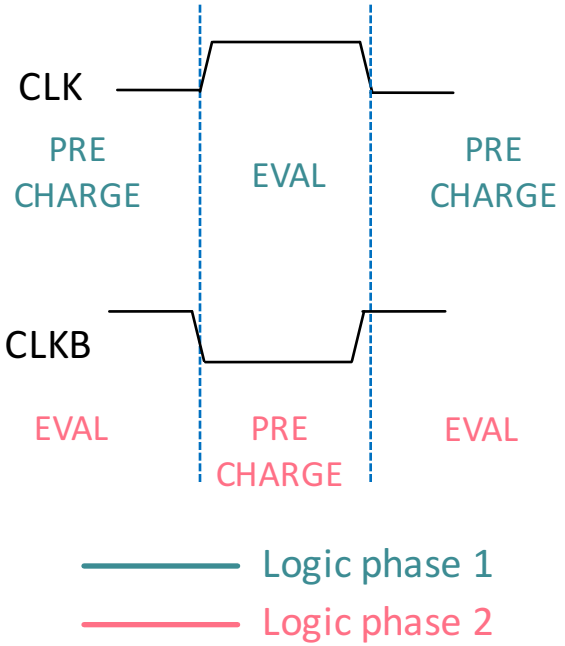
- **TVD logic chains like domino logic**
- **Coloring TVD logic**
  - Use the other phase of clock for evaluation
- **Logic divided into two phases**
  - Halves operate at the opposite clock phases
  - Latches between the phases



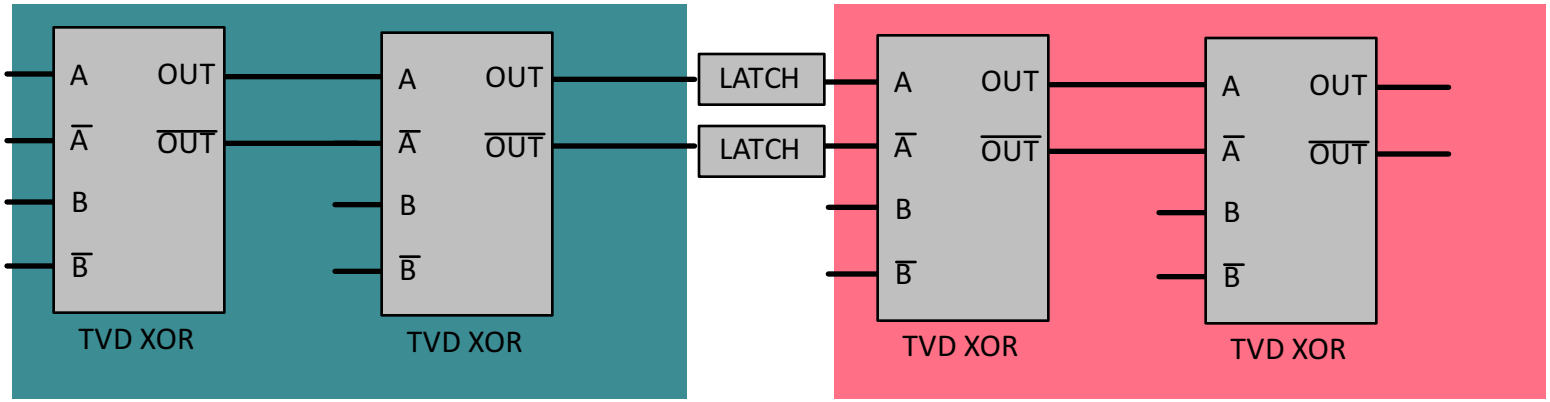
Chaining TVD Logic Gates



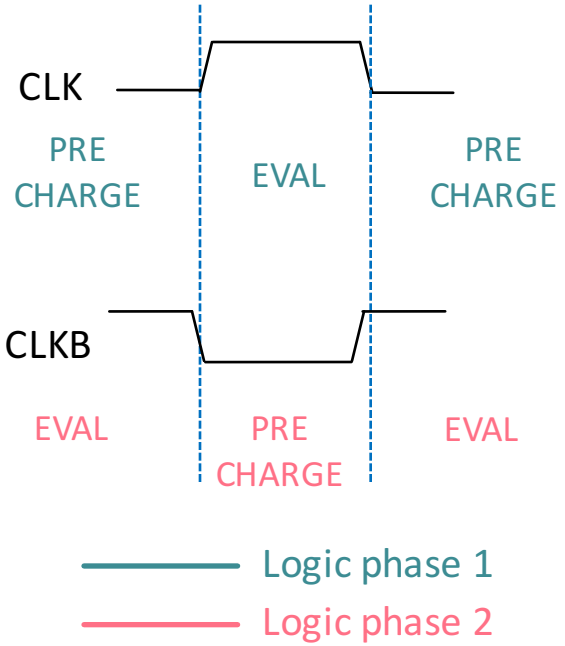
- **TVD logic chains like domino logic**
- **Coloring TVD logic**
  - Use the other phase of clock for evaluation
- **Logic divided into two phases**
  - Halves operate at the opposite clock phases
  - Latches between the phases



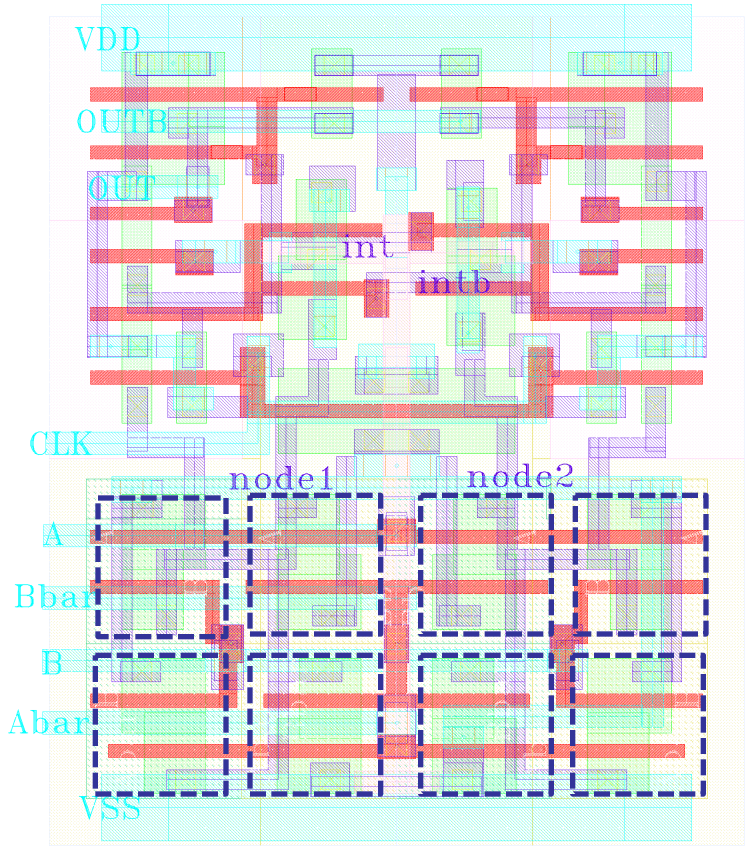
Chaining TVD Logic Gates



- **TVD logic chains like domino logic**
- **Coloring TVD logic**
  - Use the other phase of clock for evaluation
- **Logic divided into two phases**
  - Halves operate at the opposite clock phases
  - Latches between the phases



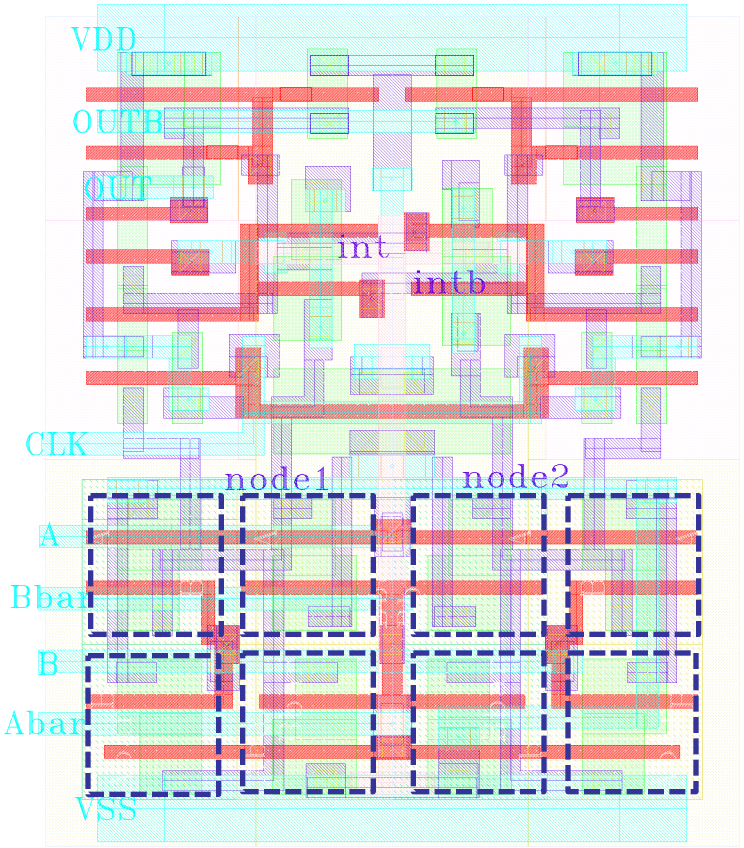
2-input TVD Logic Gate Layout



- Industrial 65nm bulk CMOS process
- 2.86 µm x 3.45 µm gate
- Symmetric layout to minimize systematic offsets

Experimental Methodology

- **Industrial 65nm bulk CMOS process**
- **Comparison between**
  - Standard CMOS library
  - TVD Logic
- **Post-layout extracted simulation**
- **XOR, AND, and OR gates**



Experimental Methodology (cont.)

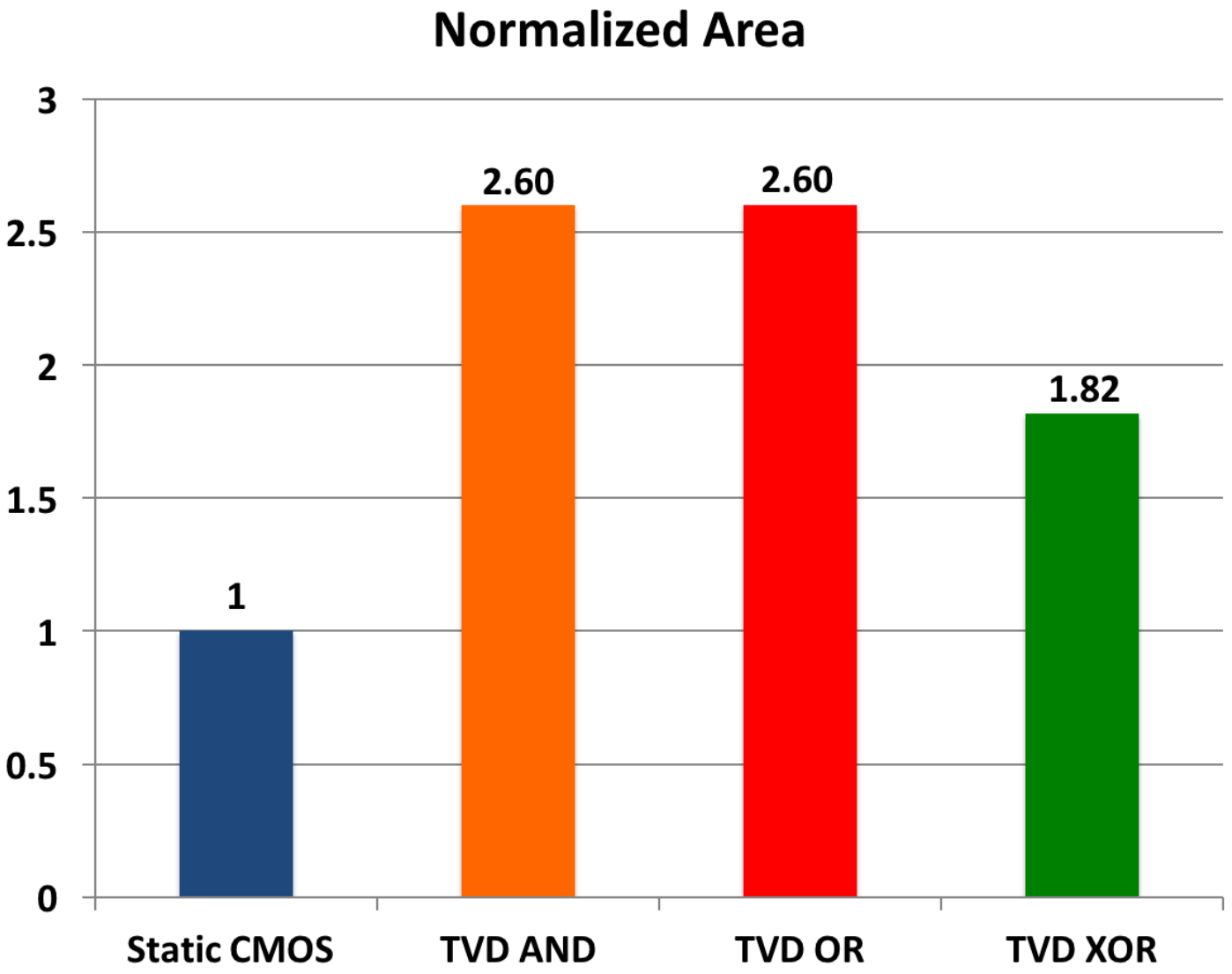
- **VLSI Metrics**
  - Layout area
  - Gate delay
  - Power
- **Security Metrics**
  - Power SCA: Normalized energy deviation (NED)

$$\mathrm{NED} = \frac{\max(\mathrm{E}) - \min(\mathrm{E})}{\max(\mathrm{E})} \qquad \mathrm{E} = \mathrm{VDD} \cdot \int_0^{\mathrm{T}} \mathrm{IDD}(\mathrm{t})\, \mathrm{dt}$$

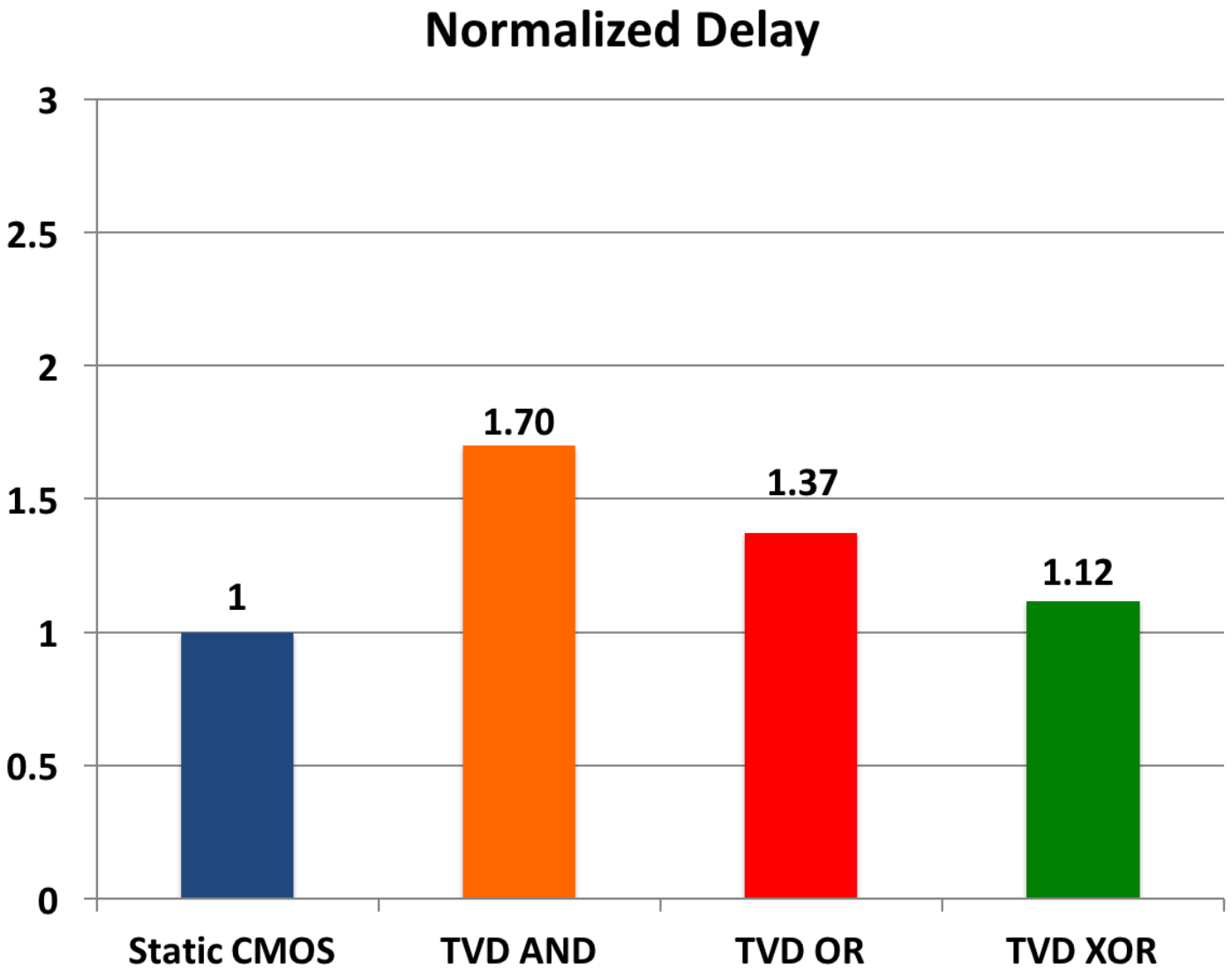
  - Timing SCA: Maximum deviation in delay (MDD)

$$\mathrm{MDD} = \frac{\max(\mathrm{delay}) - \min(\mathrm{delay})}{\max(\mathrm{delay})}$$

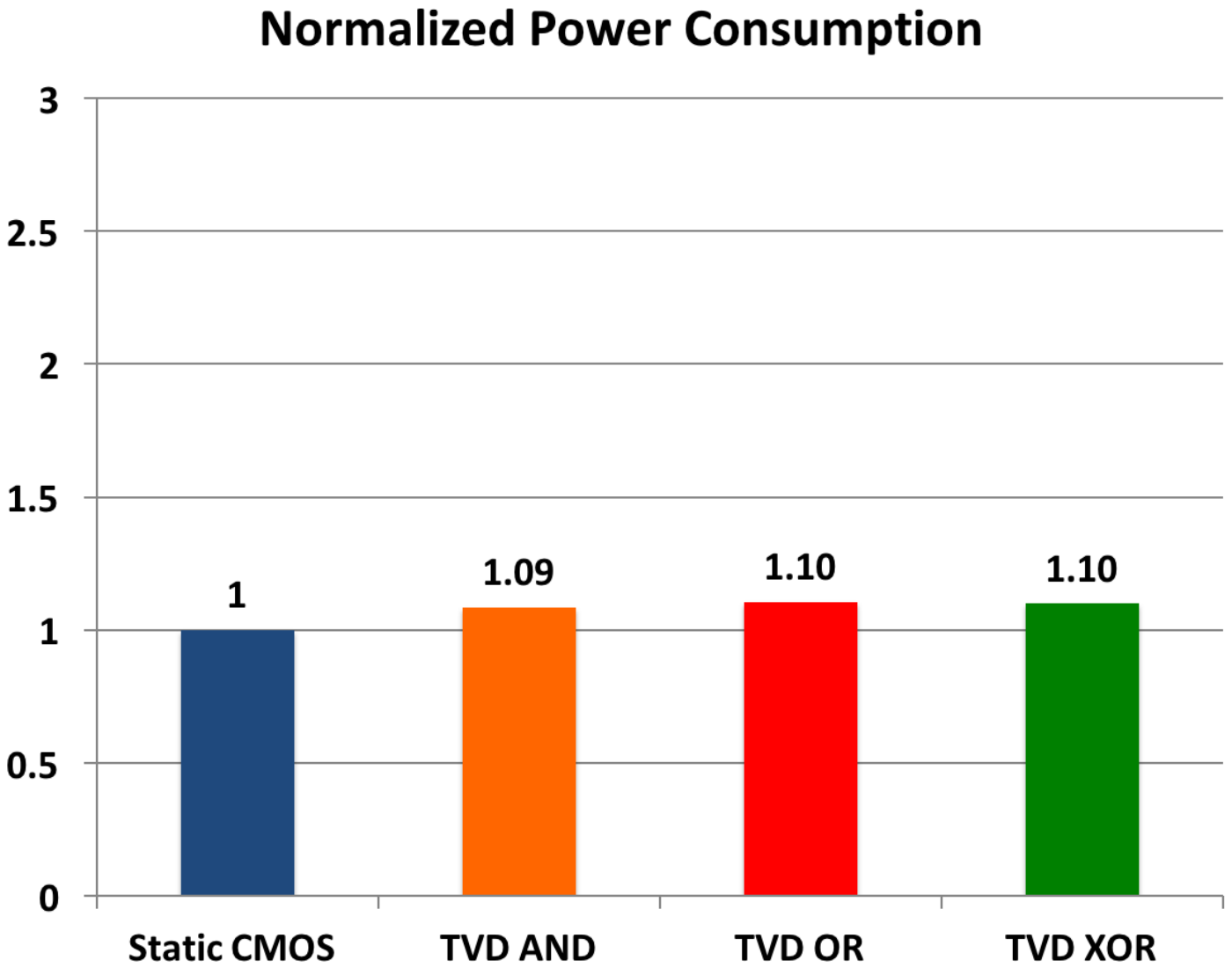
Results: Area



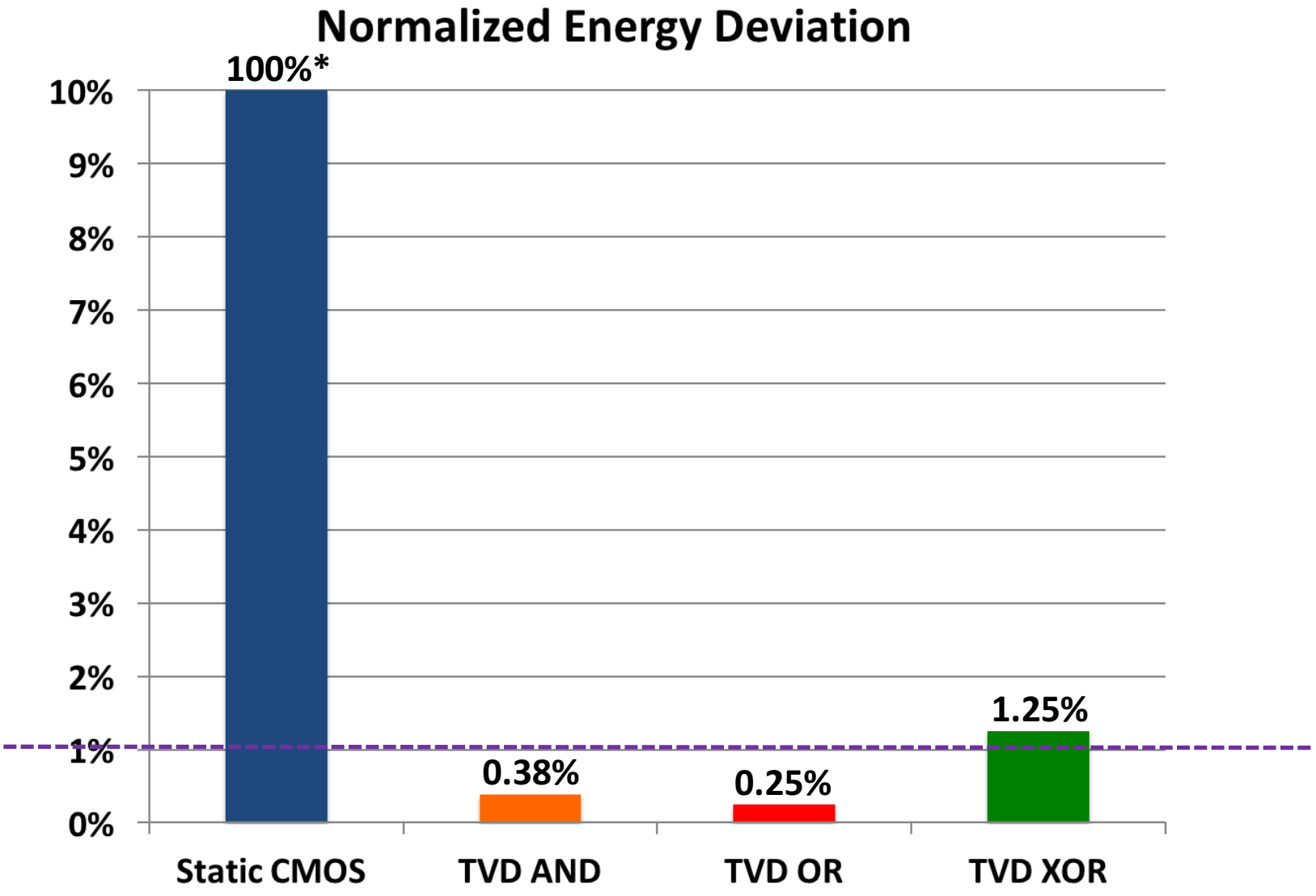
Results: Delay



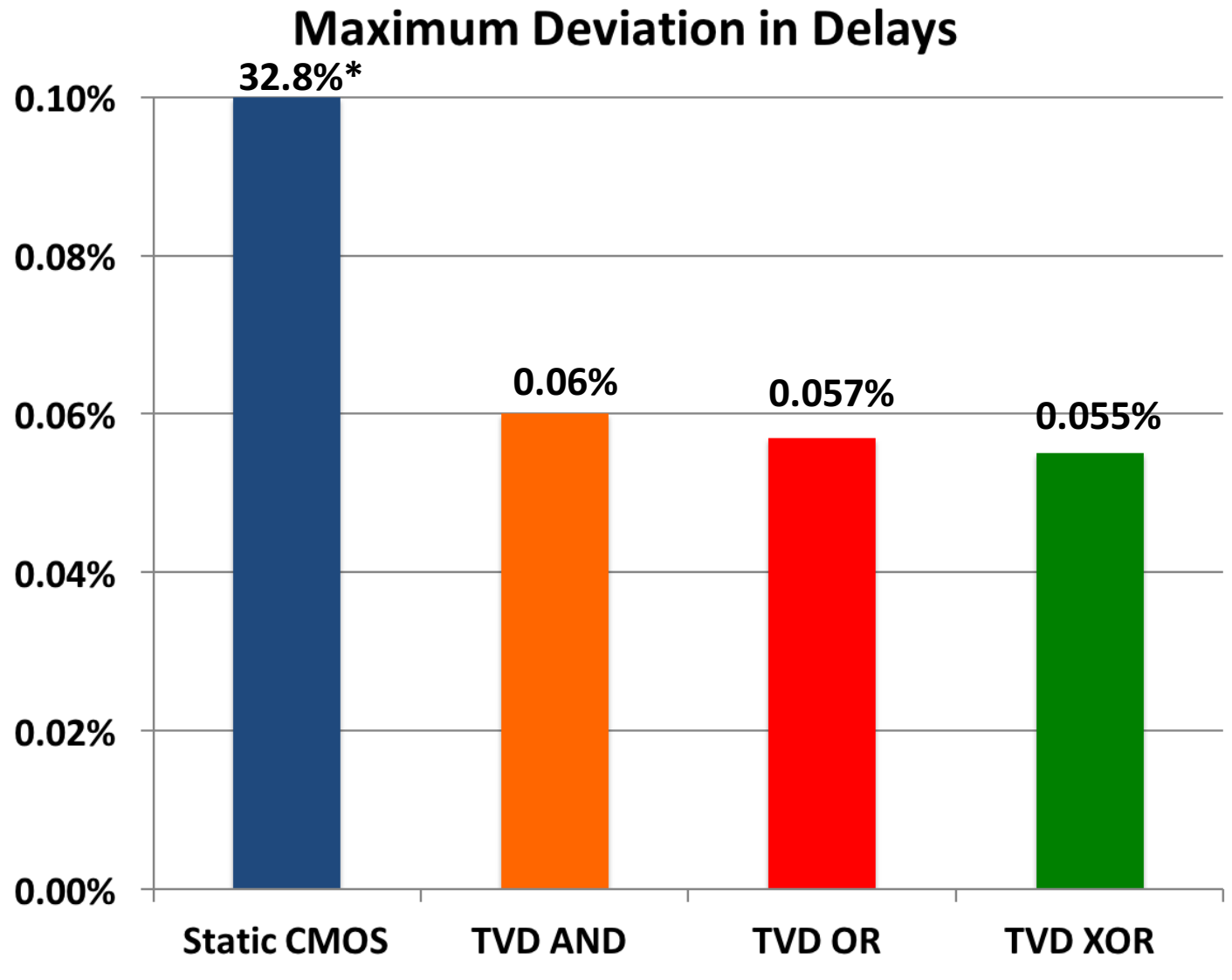
Results: Power



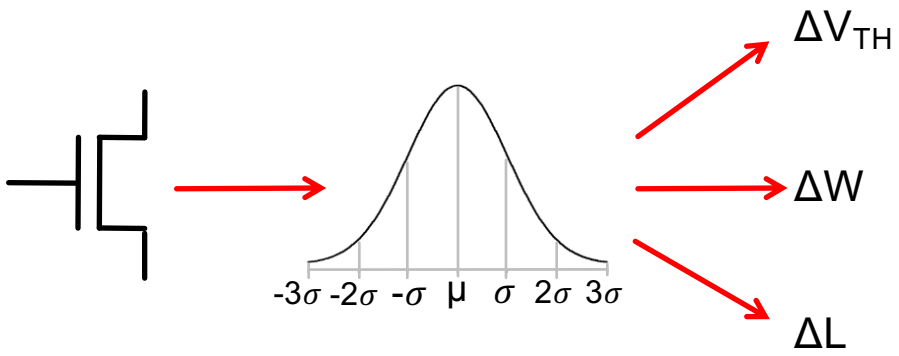
Results: Normalized Energy Deviation



Results: Maximum Deviation in Delay

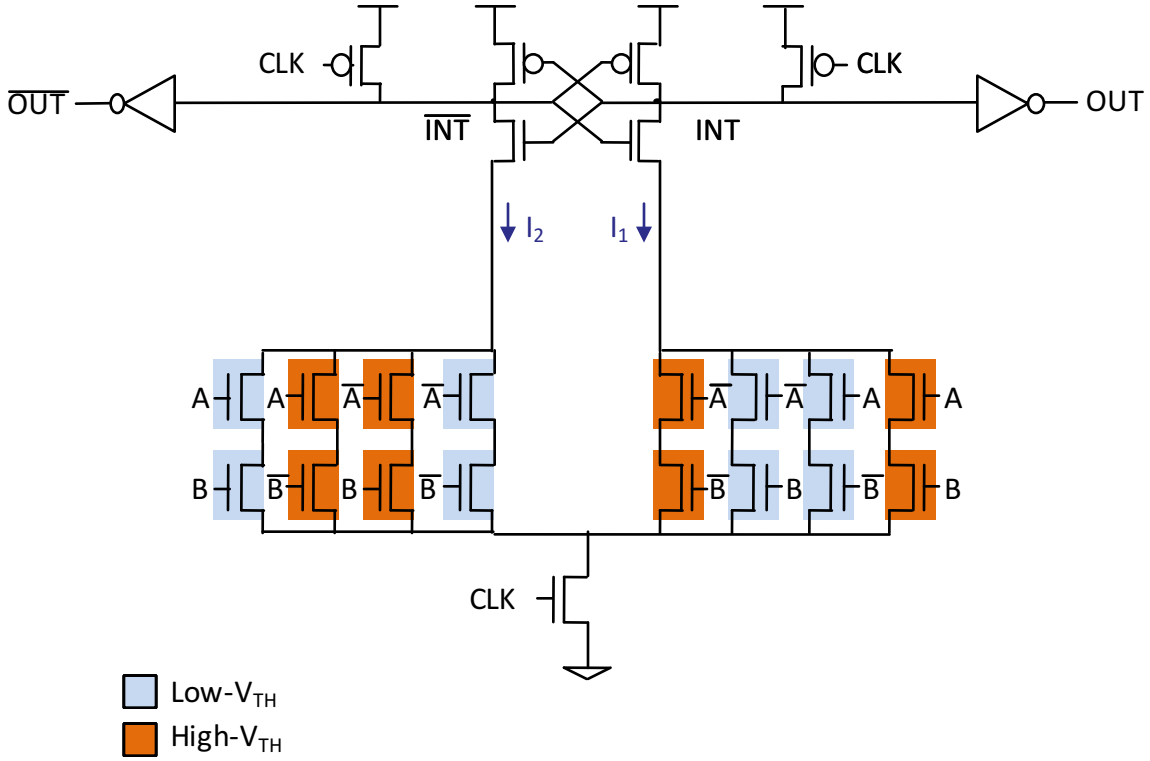


Robustness and Reliability

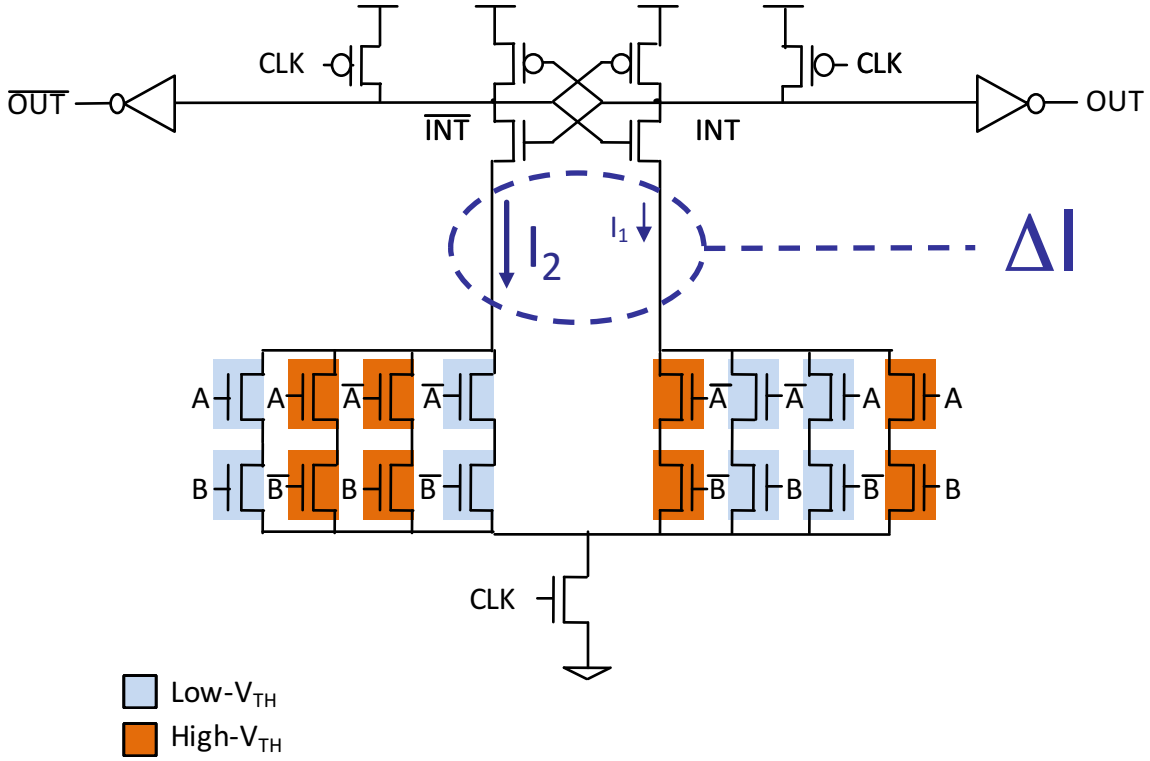


- **Monte Carlo (MC) analysis to evaluate robustness**
  - Industrial process variability models based on test data
  - Inter and intra-die variability modeled
- **MC simulations of post-layout extracted gates**
  - 5000 random samples
  - Examine distribution of ΔI

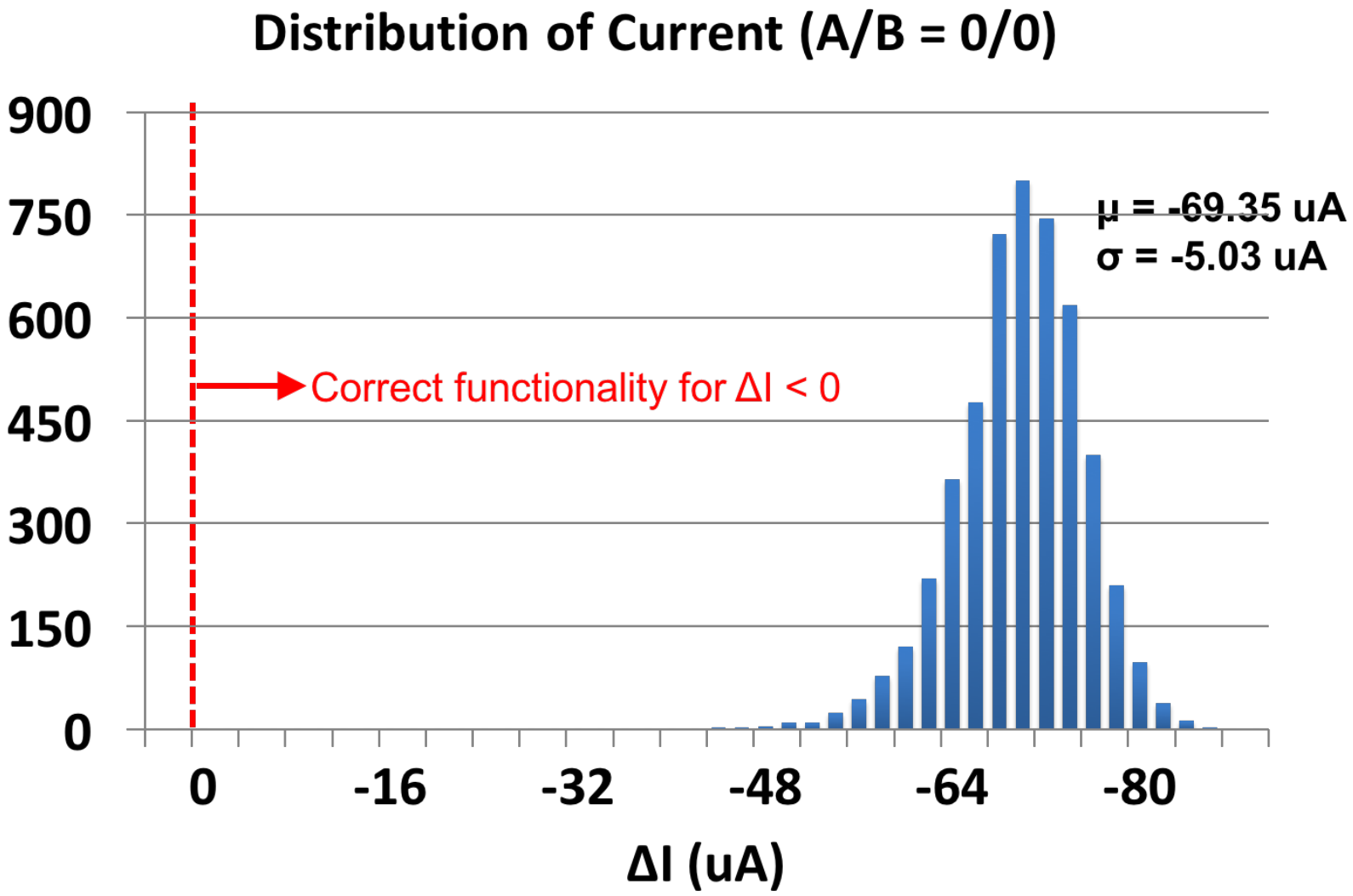
Robustness and Reliability (cont.)



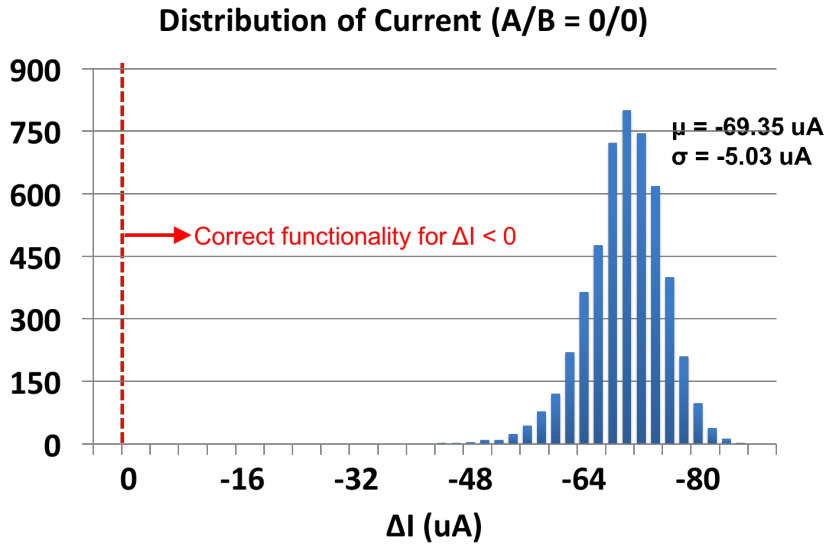
Robustness and Reliability (cont.)

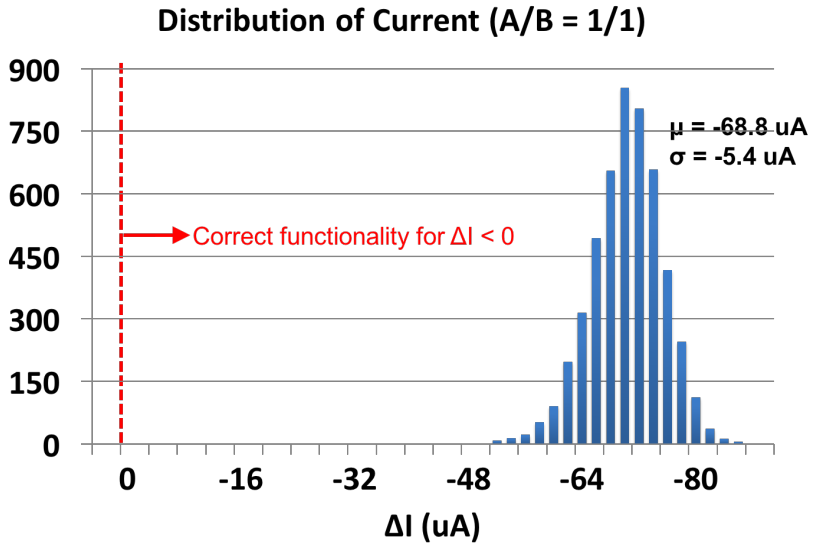


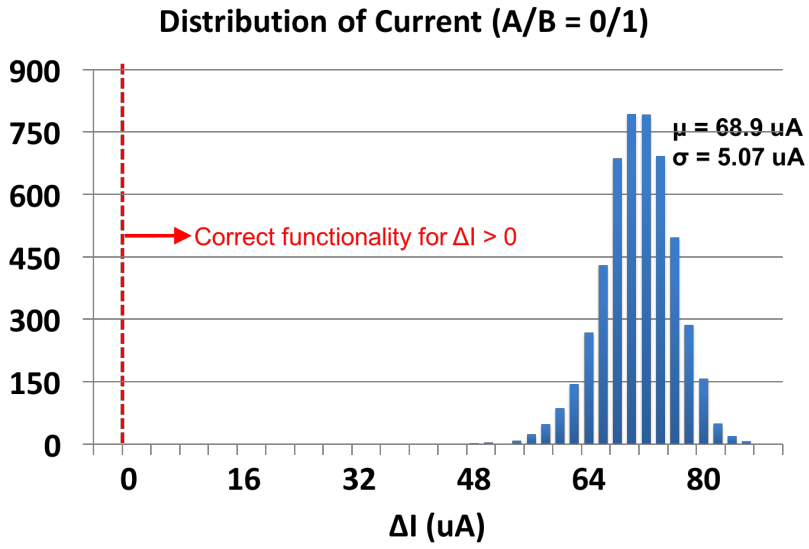
Robustness and Reliability (cont.)

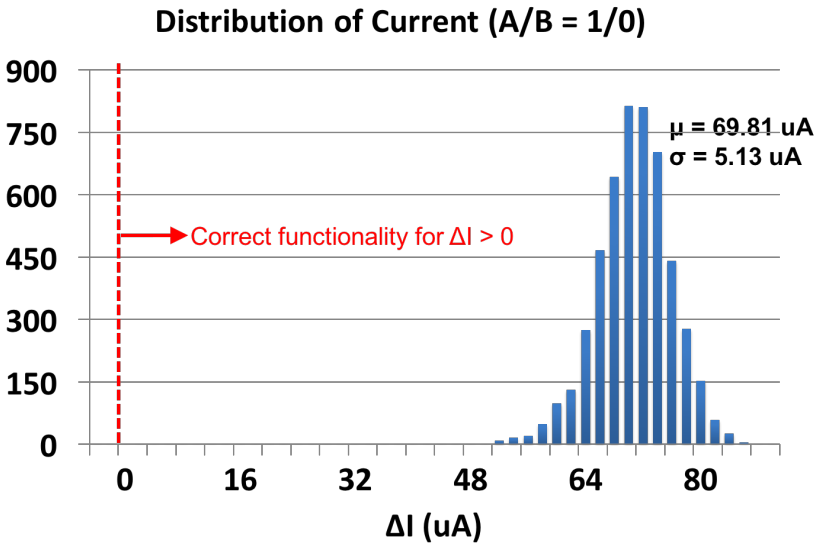


Robustness and Reliability (cont.)





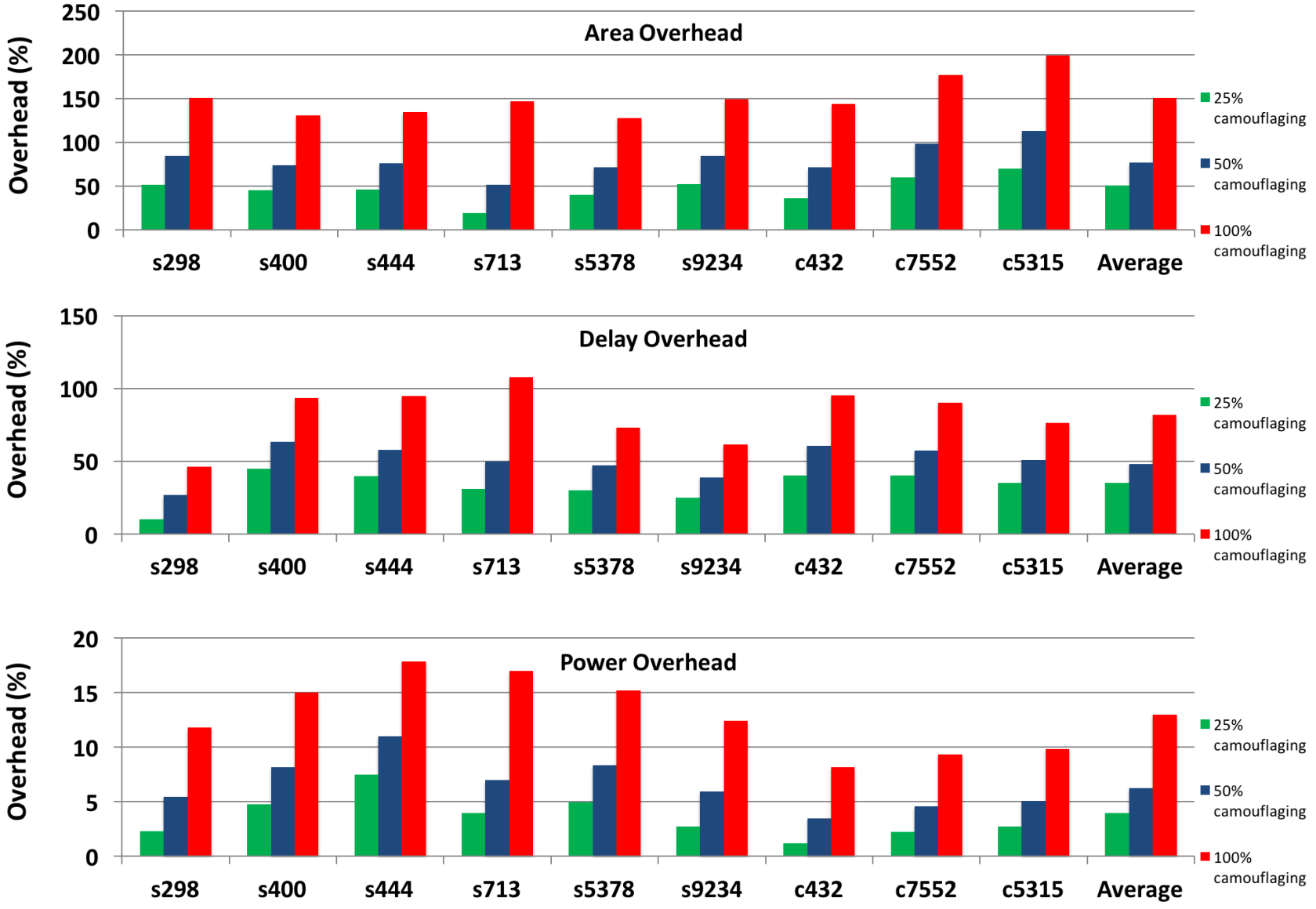




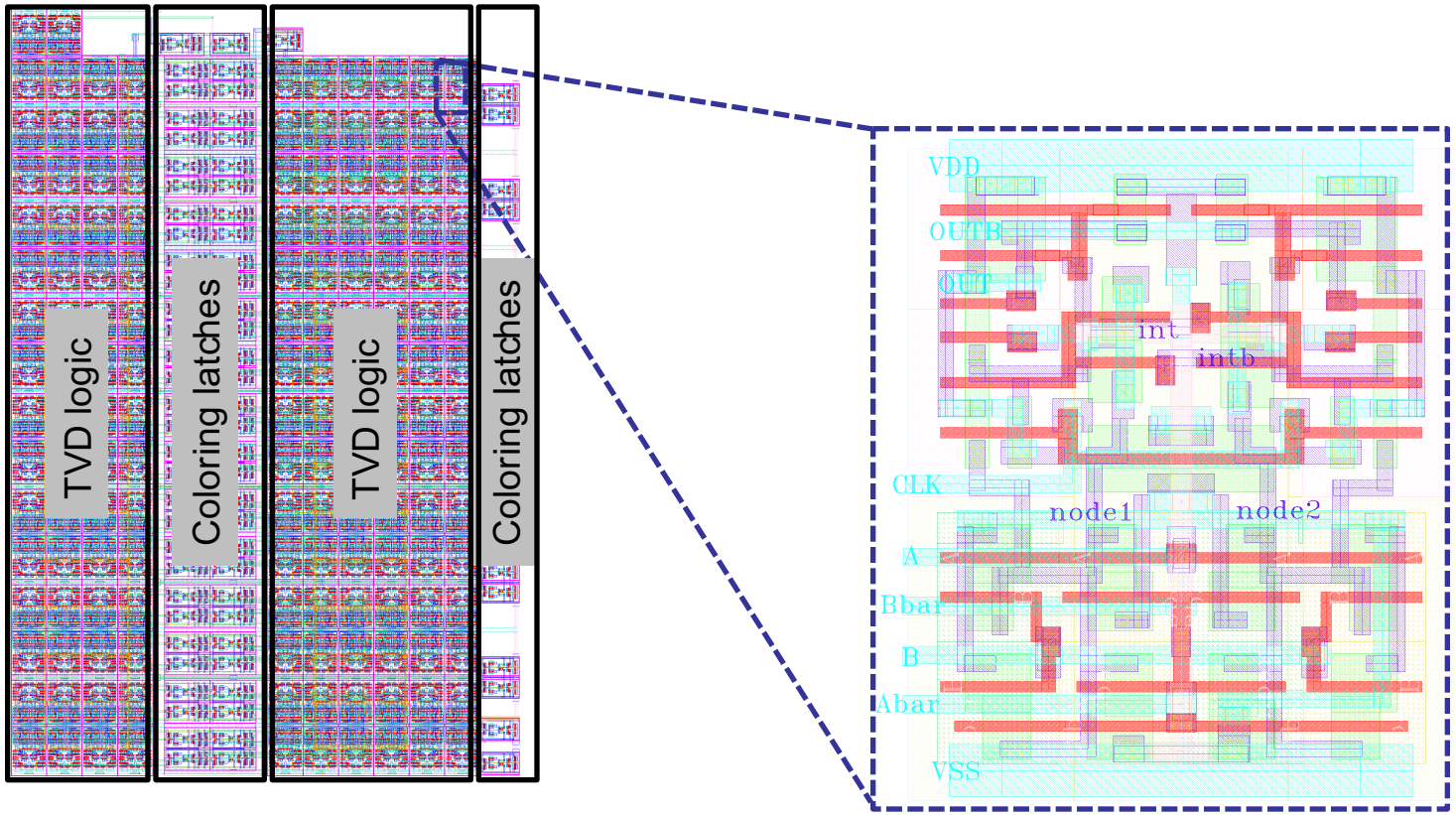
Macro-Block Overheads

- Apply TVD gates to example macro-blocks
  - Subset of 9 ISCAS benchmark designs
- Random selection of gate replacements
  - Previous work on gate selection alg. orthogonal
  - 25%, 50%, and 100% replacement
- Evaluated area, delay, and power overheads
  - *Estimates* based on simulation of standard designs

Macro-Block Overheads (cont.)



Example 16b Adder Layout



- 16b adder with 100% gate replacement
- Homogenous grids of 2-input TVD logic gates
- Bank of latches between stages to color the logic

Conclusions

- **Threshold voltage defined logic style**
  - Security not reliant on limited RE resolution
  - Fully CMOS logic process compatible
  - Modest area, power, and delay overheads
  - Low side-channel emissions (power/timing)

- **Future directions**
  - Silicon testchip validation
  - Additional macro-block evaluation
  - What if the manufacturing is not secure?

Thank You