Hiding Countermeasures in Cryptographic Hardware: Part II

Cryptographic Hardware for Embedded Systems

ECE 3170

Fall 2026

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

©Georgia Institute of Technology, 2018-2026

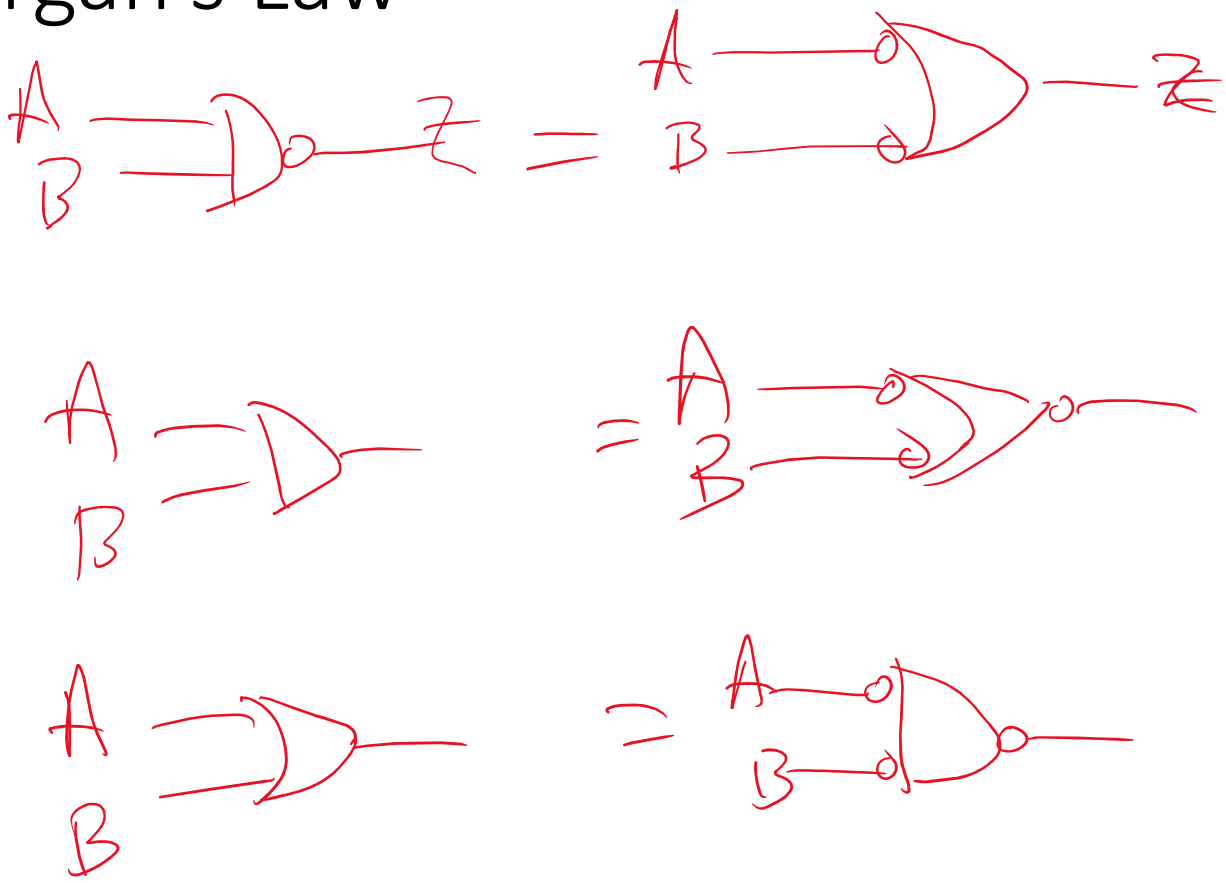
Reading

- This lecture is based on the paper by K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for DPA Resistant ASIC or FPGA Implementation,” *Proceedings of the Design, Automation and Test in Europe Conference* (DATE’04), Vol. I, February 2004.
- All figures in this lecture are from the aforementioned paper.

©Georgia Institute of Technology, 2018-2026

Refresher: DeMorgan's Law

- $\overline{AB} = \bar{A} + \bar{B}$
- $AB = \overline{\bar{A} + \bar{B}}$
- $A + B = \overline{\bar{A}\bar{B}}$

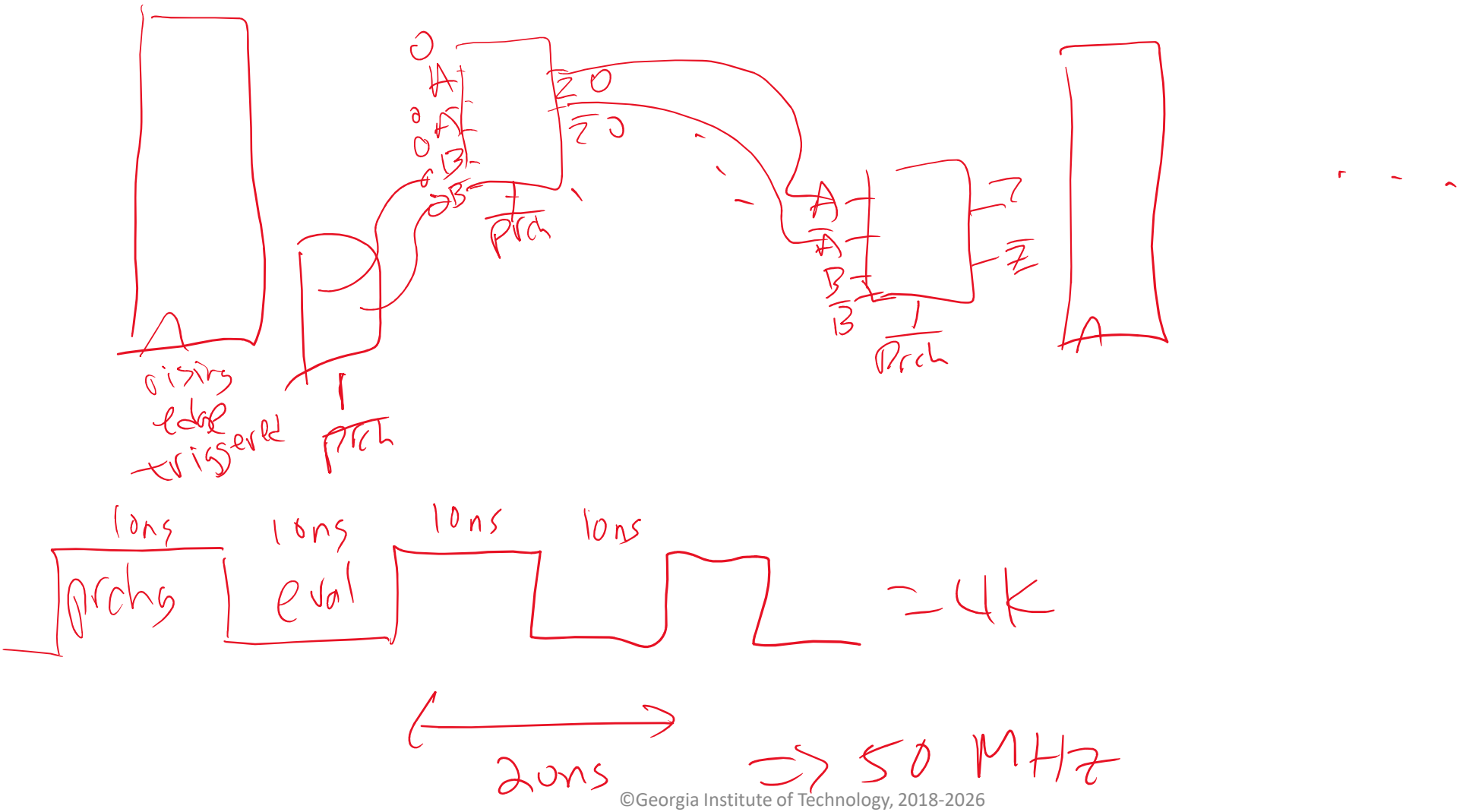


©Georgia Institute of Technology, 2018-2026

Concept of Precharging

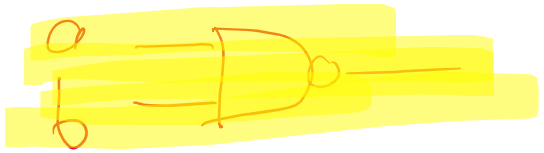
- Typical digital computation in silicon is based on clock edges
  - All computation occurs between clock edges in a pipeline
  - Logic gates follow a pull-up / pull-down design where p-type Field-Effect Transistors (pFETs) are used exclusively for the pull-up network (where they are more efficient) and n-type Field-Effect Transistors (nFETs) are used exclusively for the pull-down network
  - Flip-flops store intermediate results
- In precharging, the output is set to 1 (or 0) in a *precharge* phase (portion of a clock) followed by a pull-down (or pull-up if the precharge was to 0) in an *evaluation* phase
- In the 1970s this was very common where silicon chips only had nFETs

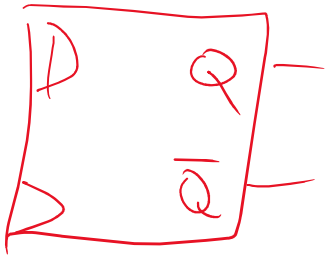
©Georgia Institute of Technology, 2018-2026



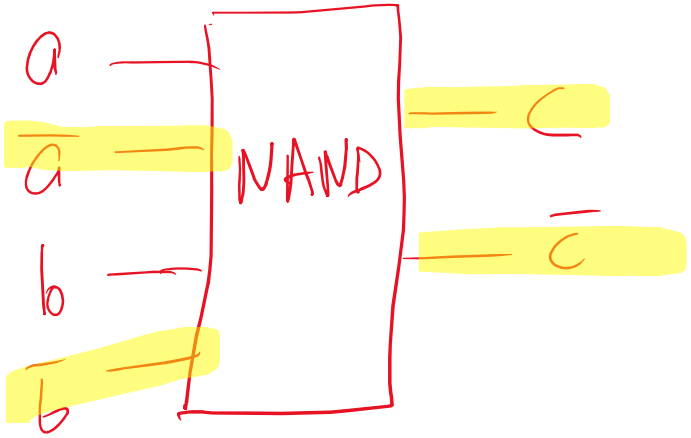
©Georgia Institute of Technology, 2018-2026

Single Rail versus Dual Rail





- SR NAND
  - inputs a, b
  - output c
- DR NAND
  - inputs a, $\bar{a}$, b, $\bar{b}$
  - Outputs c, $\bar{c}$



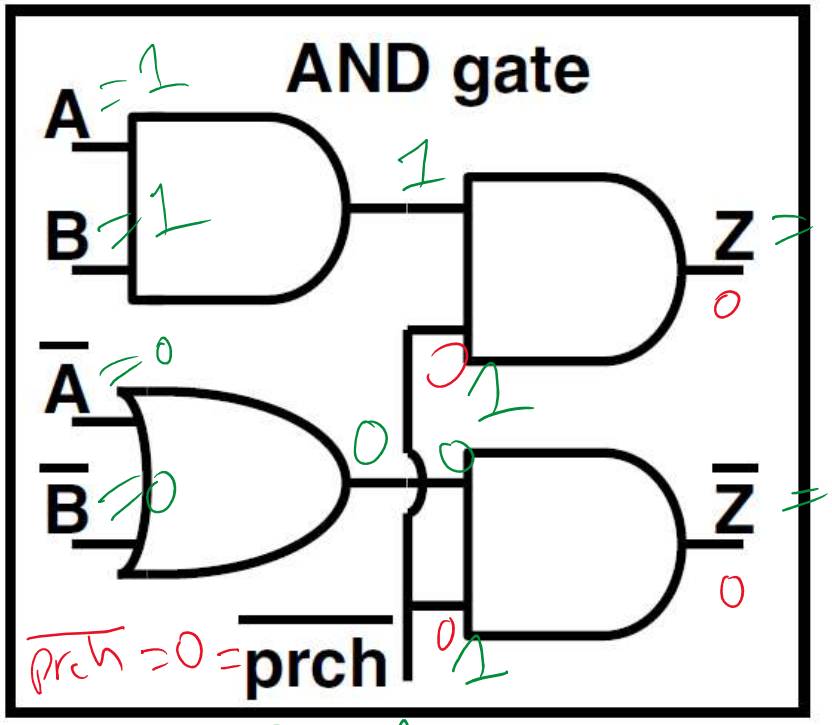
©Georgia Institute of Technology, 2018-2026

Goals of SDDL and WDDL

- Remove power side channel
- No information leakage
- All calculations have the same power regardless of Boolean input values
- Hint: SDDL will fail, but WDDL will succeed!

©Georgia Institute of Technology, 2018-2026

Simple Dynamic Differential Logic (SDDL)

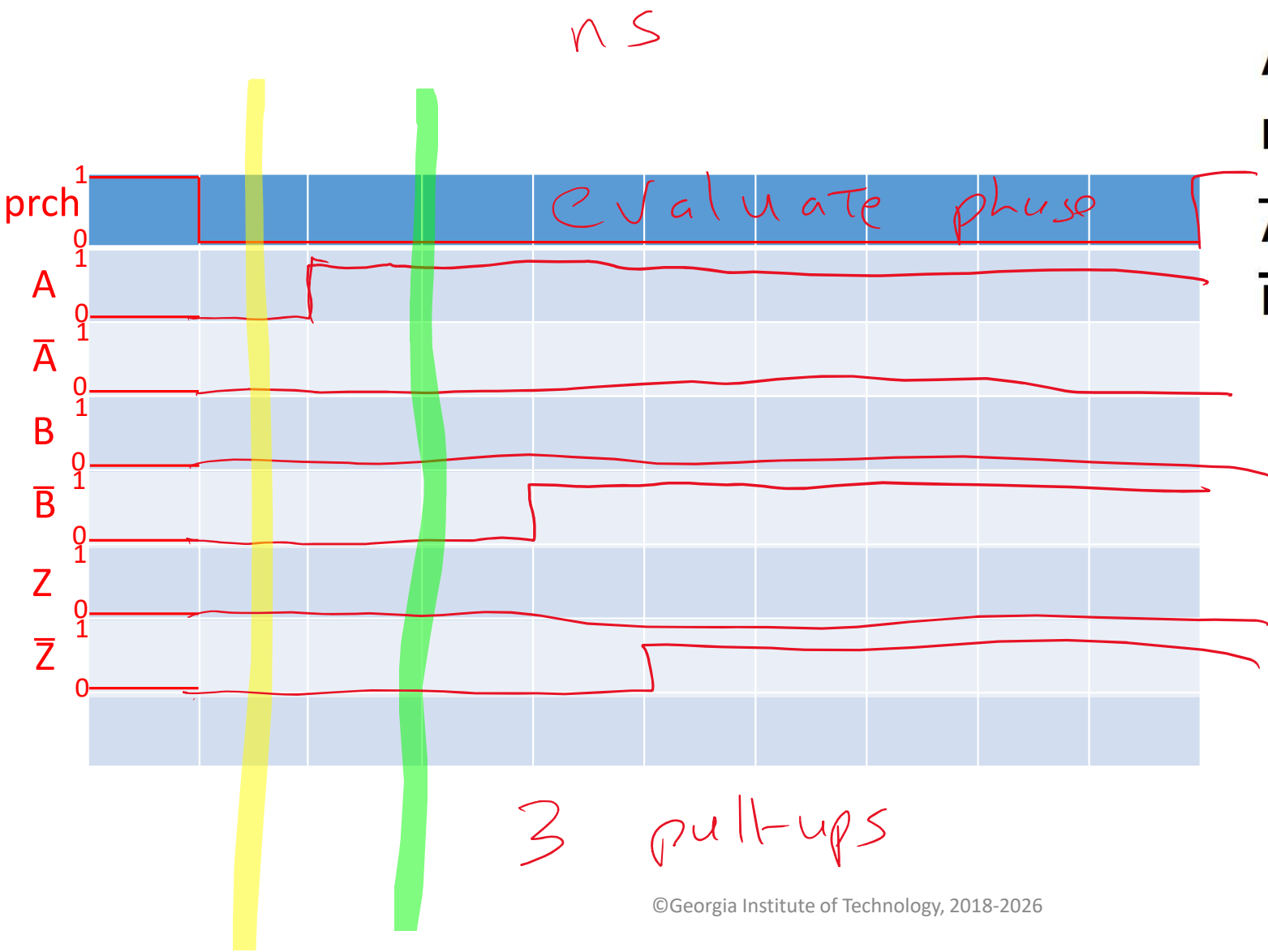


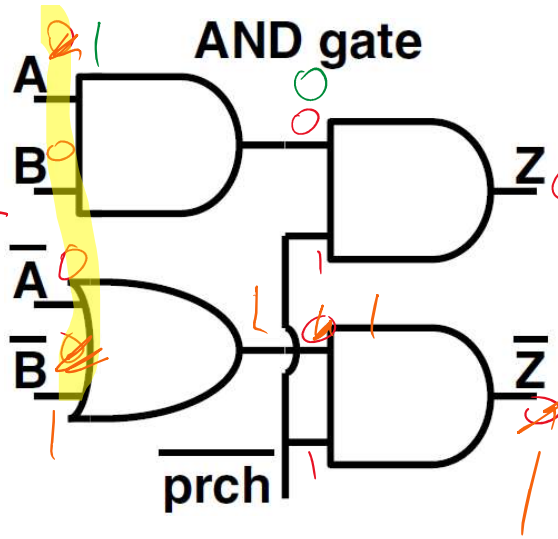
$$(A.B).\overline{prch} \leftrightarrow (\bar{A}+\bar{B}).\overline{prch}$$

A	B	$\bar{A}$	$\bar{B}$	prch	Z	$\bar{Z}$
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
X	X	X	X	1	0	0

Fig. 1. SDDL: AND-gate (left); truth table (right)

©Georgia Institute of Technology, 2018-2026





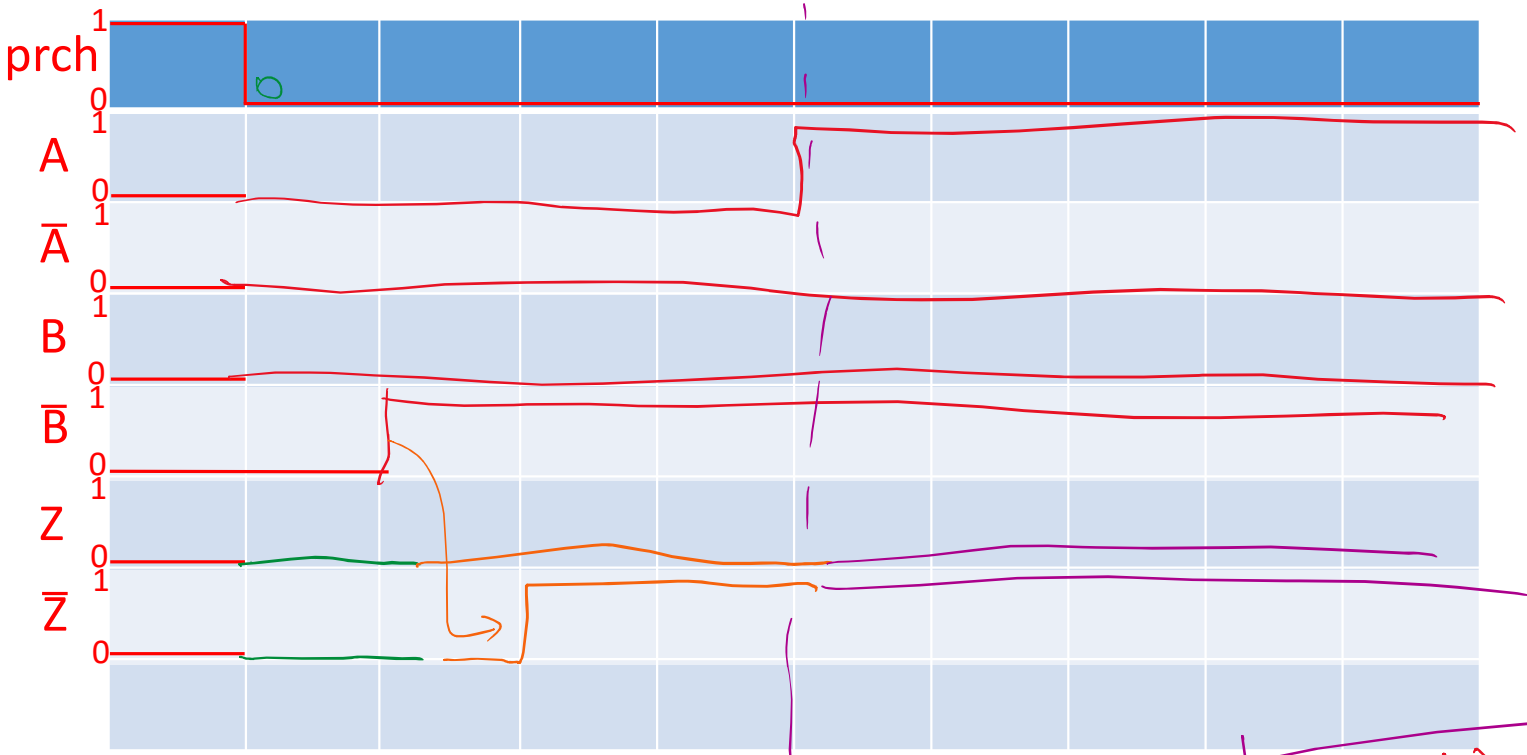
ns

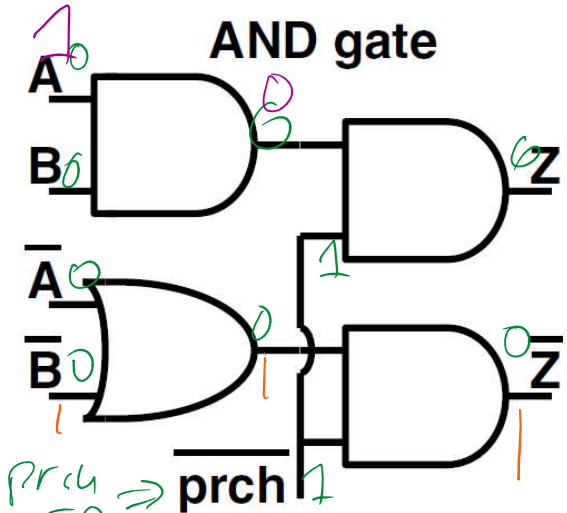
3 pull-ups

50 MHz

20 ns

©Georgia Institute of Technology, 2018-2026

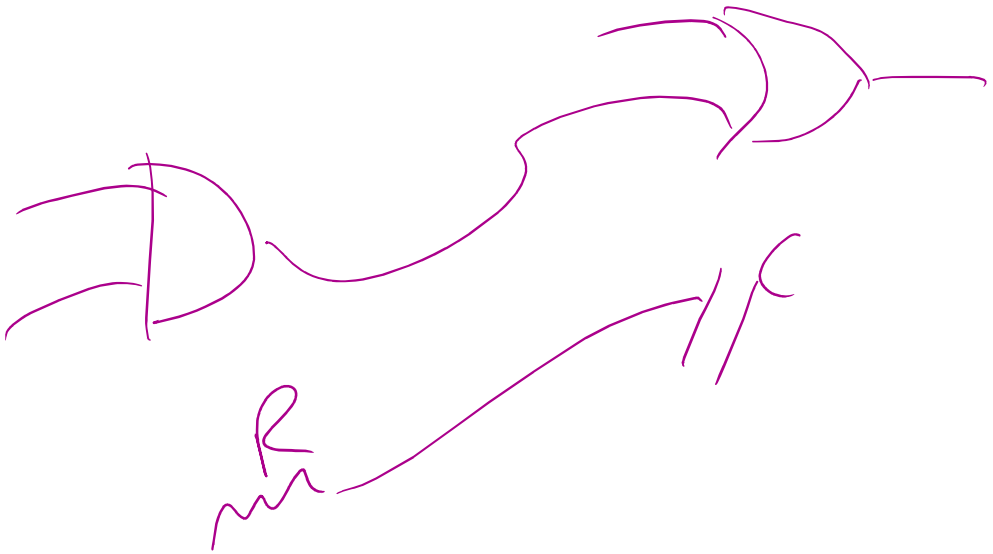




OR gate

all SPDL | AND, OR gate 3 pull-ups

©Georgia Institute of Technology, 2018-2026



RC = seconds

©Georgia Institute of Technology, 2018-2026

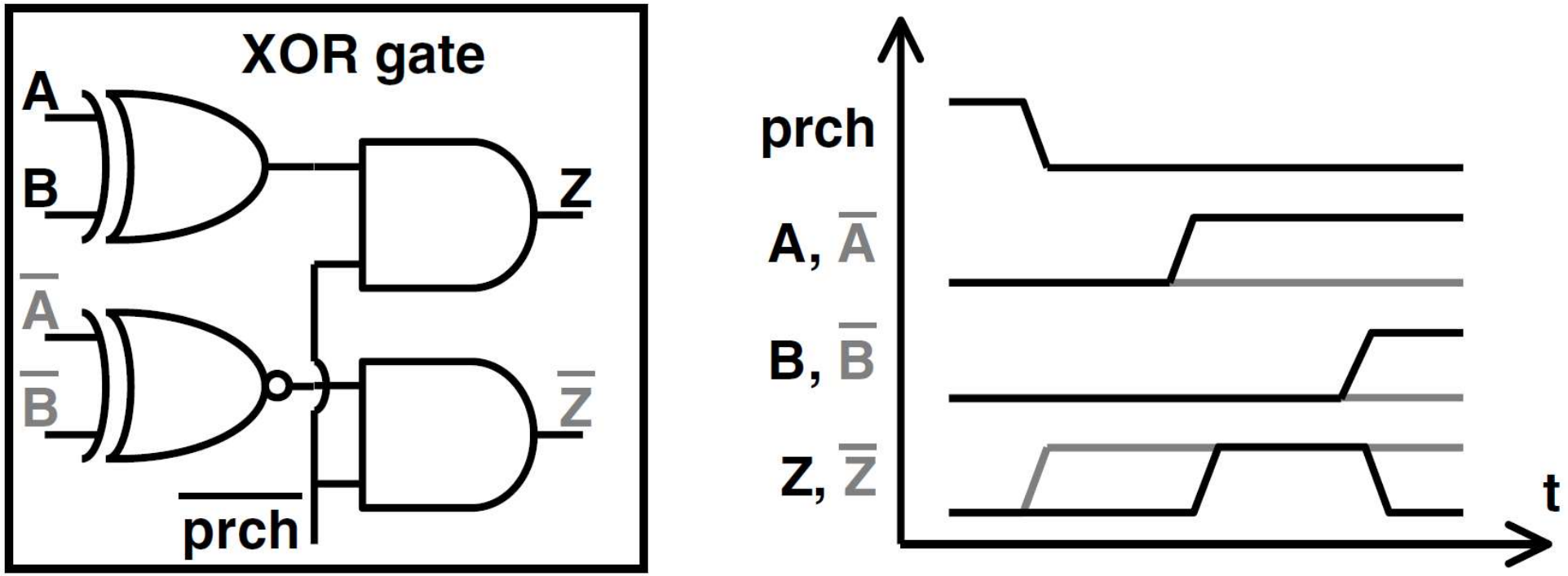
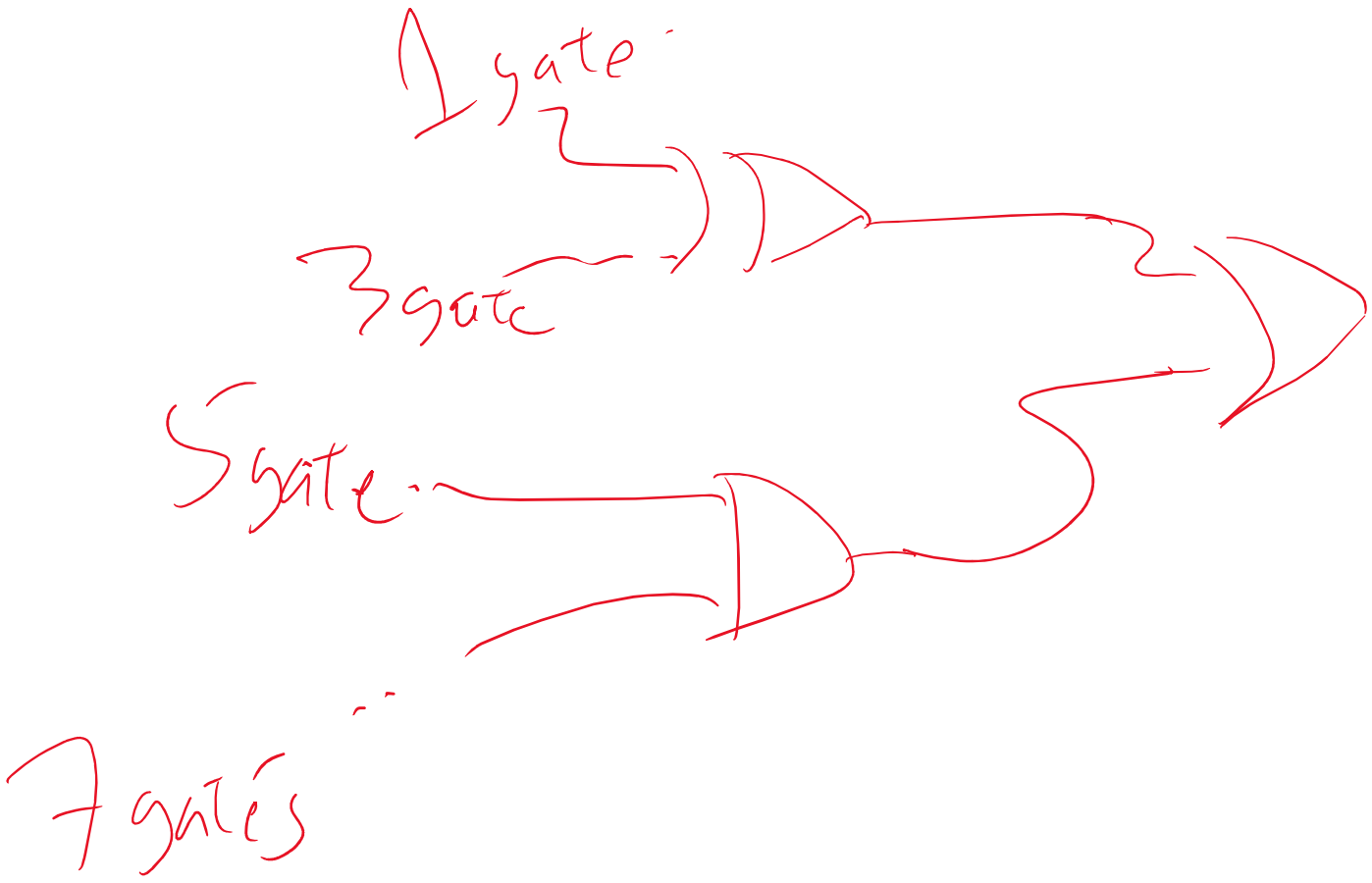
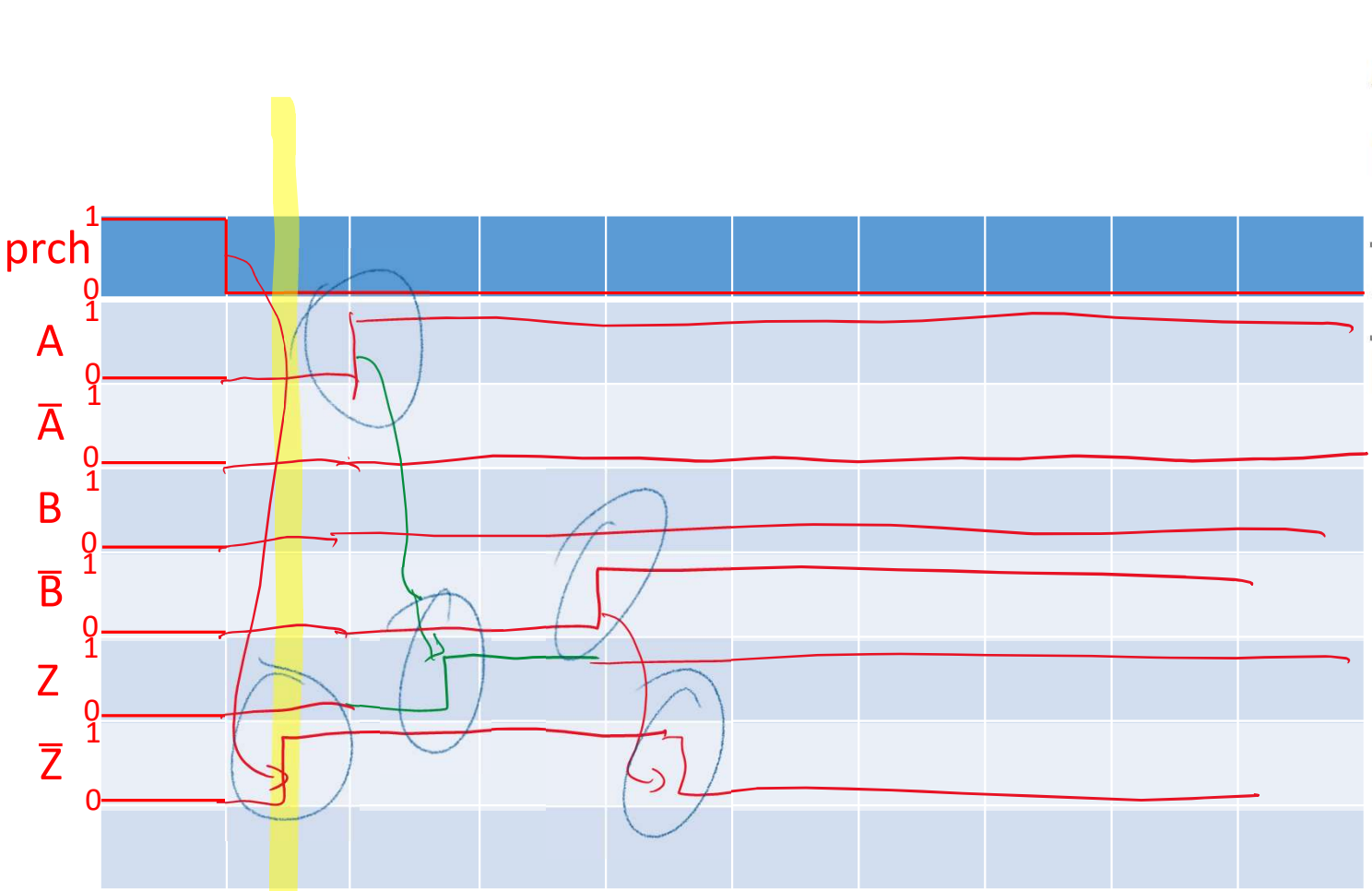


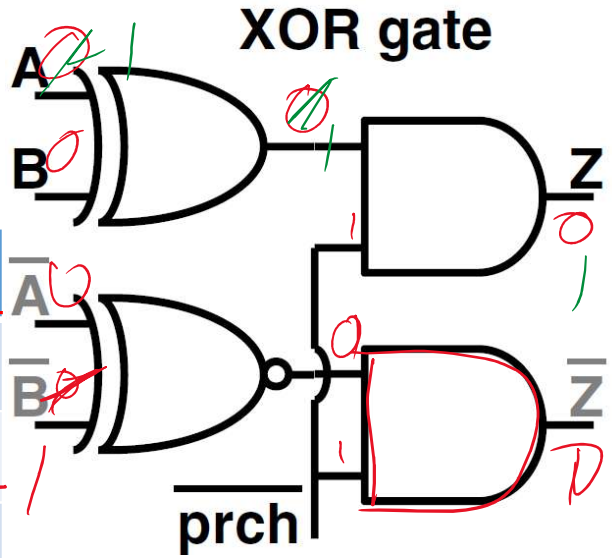
Fig. 2. SDDL: XOR-gate (left); timing diagram (right)

©Georgia Institute of Technology, 2018-2026



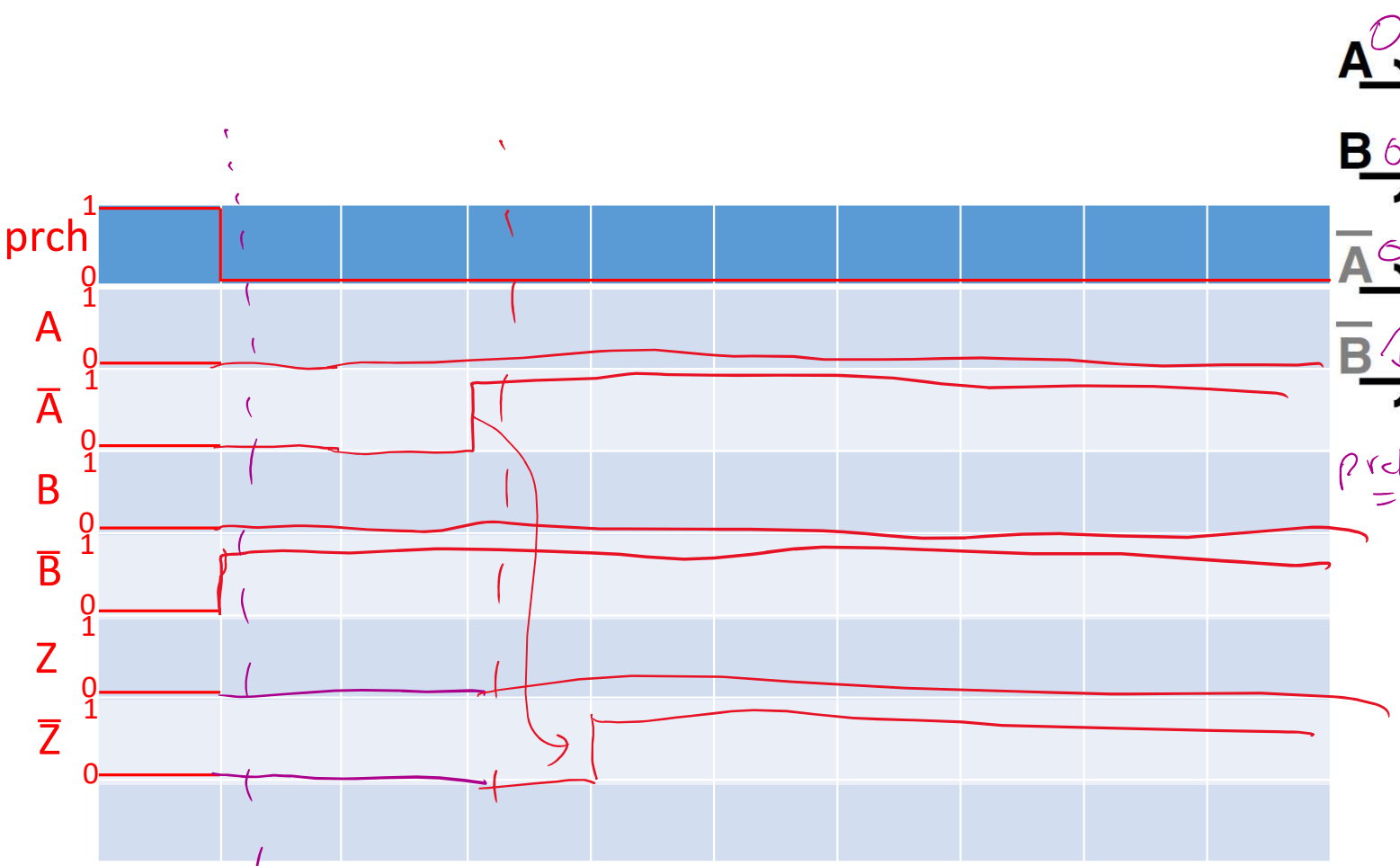
©Georgia Institute of Technology, 2018-2026

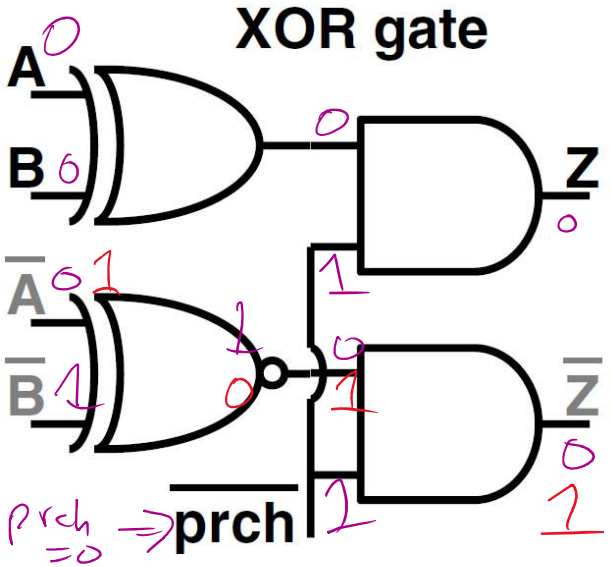




5 transitions > 3

©Georgia Institute of Technology, 2018-2026





3 pull-ups

©Georgia Institute of Technology, 2018-2026

Comments

- SDDL includes the previous two gates
  - AND SDDL gate
  - XOR SDDL gate
  - OR SDDL gate (not shown, just flip the two gates on the left hand side of AND SDDL)
- SDDL does not achieve energy consumption which is independent of the inputs or arrival order

→ ∃ relationship which could be exploited between inputs + energy consumption

©Georgia Institute of Technology, 2018-2026

Recall even a 1% relationship can potentially be exploited

If an attack can reduce Brute force search to polynomial, attacker can guess successfully

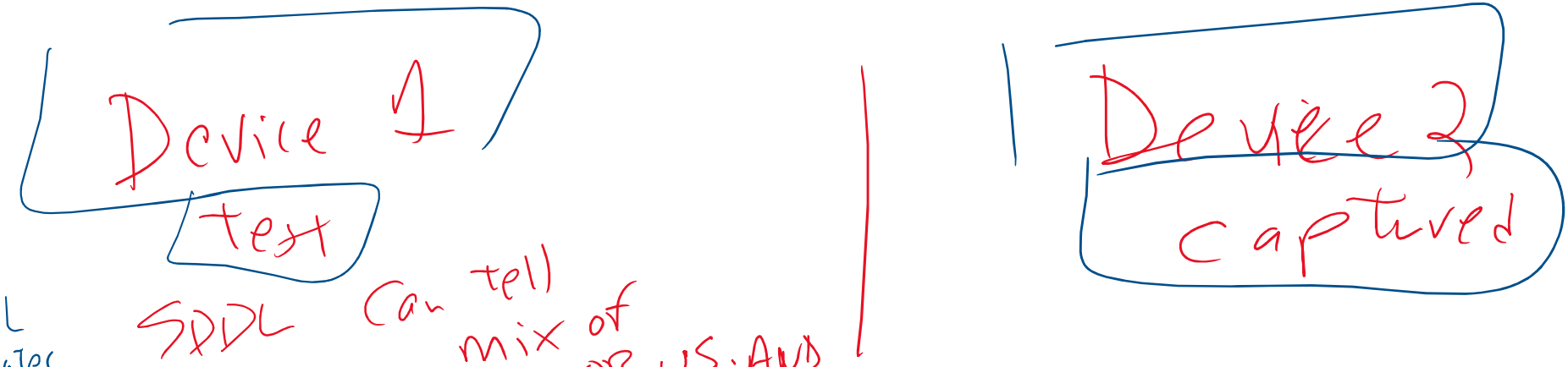
2^{128}

$16 * 2^8 = 2^{12}$

©Georgia Institute of Technology, 2018-2026

We are hiding data values

Logic gates will be fixed

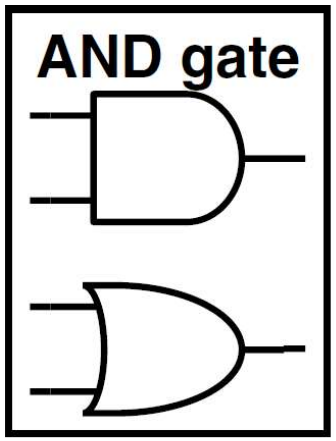


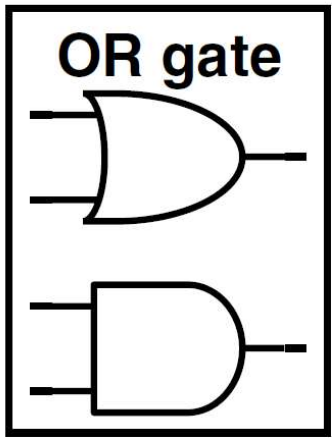
SDDL all gates save energy consumption

SDDL Can tell mix of XOR vs. AND or SR

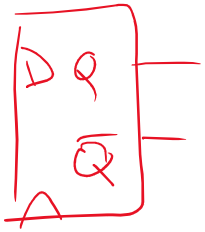
©Georgia Institute of Technology, 2018-2026

Idea: remove precharge, only use AND and OR





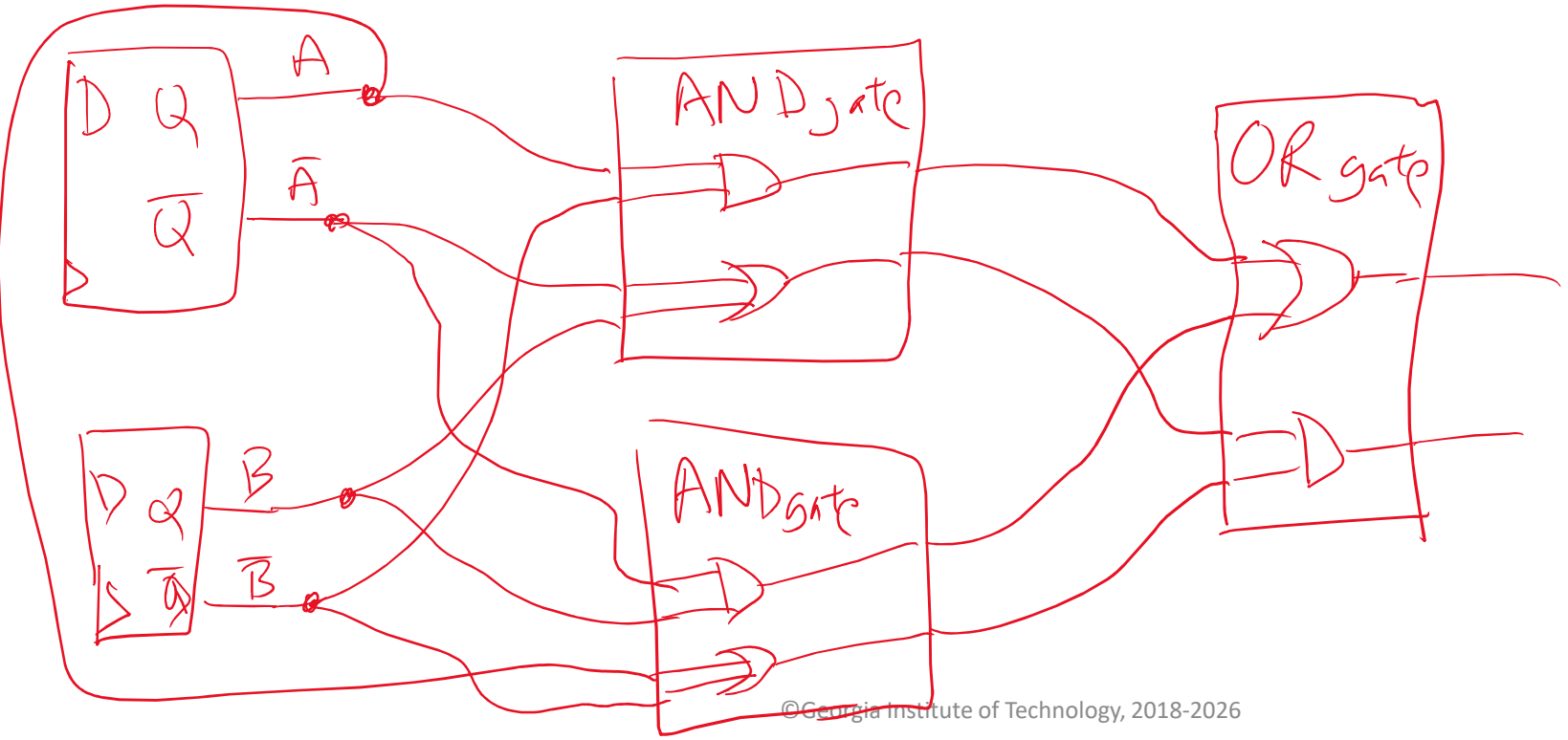
- Precharging can be removed if always begin with all inputs equal to zero
  - Any AND gate as well as any OR gate with inputs equal to zero will have outputs equal to zero
  - Assume that the flip-flop (FF) design begins with both Q and $\bar{Q}$ outputs of the FF equal to zero, then one (either Q or $\bar{Q}$) rises
- Inversion is automatic since both Z and $\bar{Z}$ are output from each gate
  - Instead of using an inverter, just swap output wires
- All Boolean logic functions can be provably calculated from AND, OR and NOT
  - In fact, AND and NOT is sufficient
  - As is OR and NOT (recall DeMorgan's Law!)



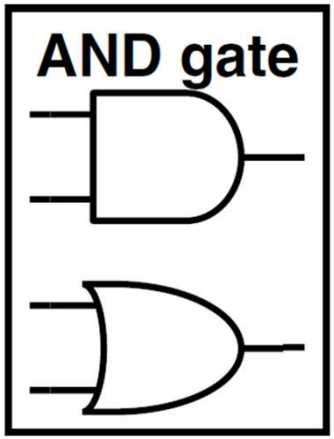
©Georgia Institute of Technology, 2018-2026

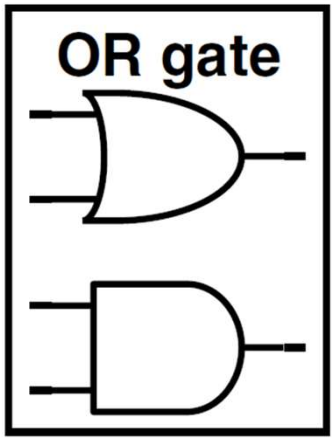
XOR w/ NDDL

$A \text{ XOR } B = (A \text{ AND } \bar{B}) \text{ OR } (\bar{A} \text{ AND } B)$



©Georgia Institute of Technology, 2018-2026





©Georgia Institute of Technology, 2018-2026

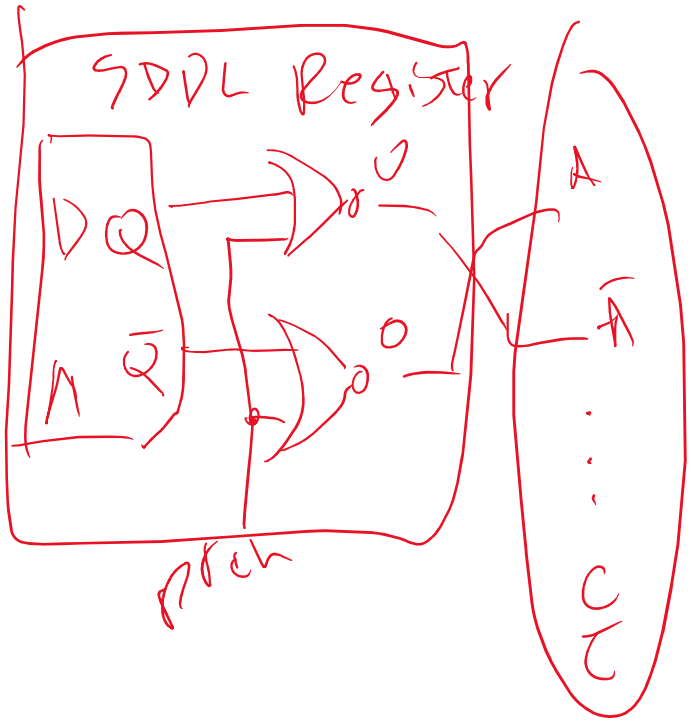
Wave Dynamic Differential Logic (WDDL)

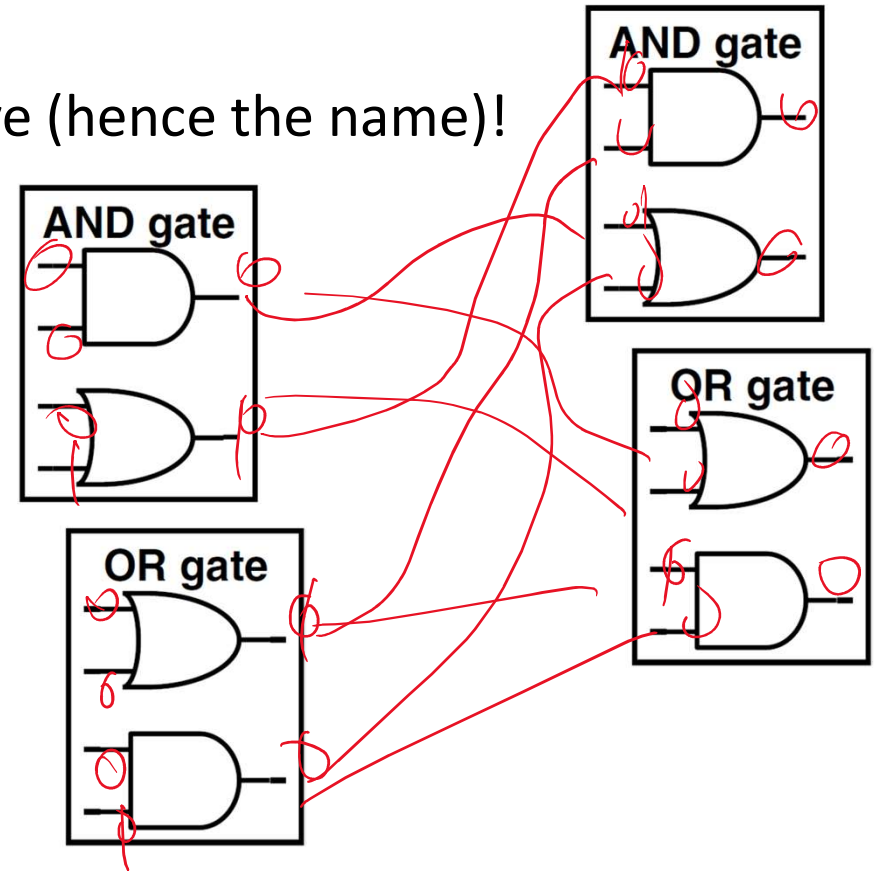
- Only two logic gate types: AND and OR (without any precharging)
- At precharge phase, all inputs and outputs are set to zero
- During the evaluate phase
  - Each combination of an input and its complement make one and only one transition
  - The result of the inputs transitioning appropriately is that each output Z and $\bar{Z}$ make one and only one transition from zero to one
- Consider *n* sets of complemented (e.g., Z and $\bar{Z}$) values
  - For each clock cycle (evaluate), there are exactly *n* logic value transitions
  - In other words, per clock, there is a 100% chance of exactly *n* energy consuming transitions occurring

©Georgia Institute of Technology, 2018-2026

Question: How to Precharge WDDL?

- Answer: create a wave (hence the name)!





©Georgia Institute of Technology, 2018-2026

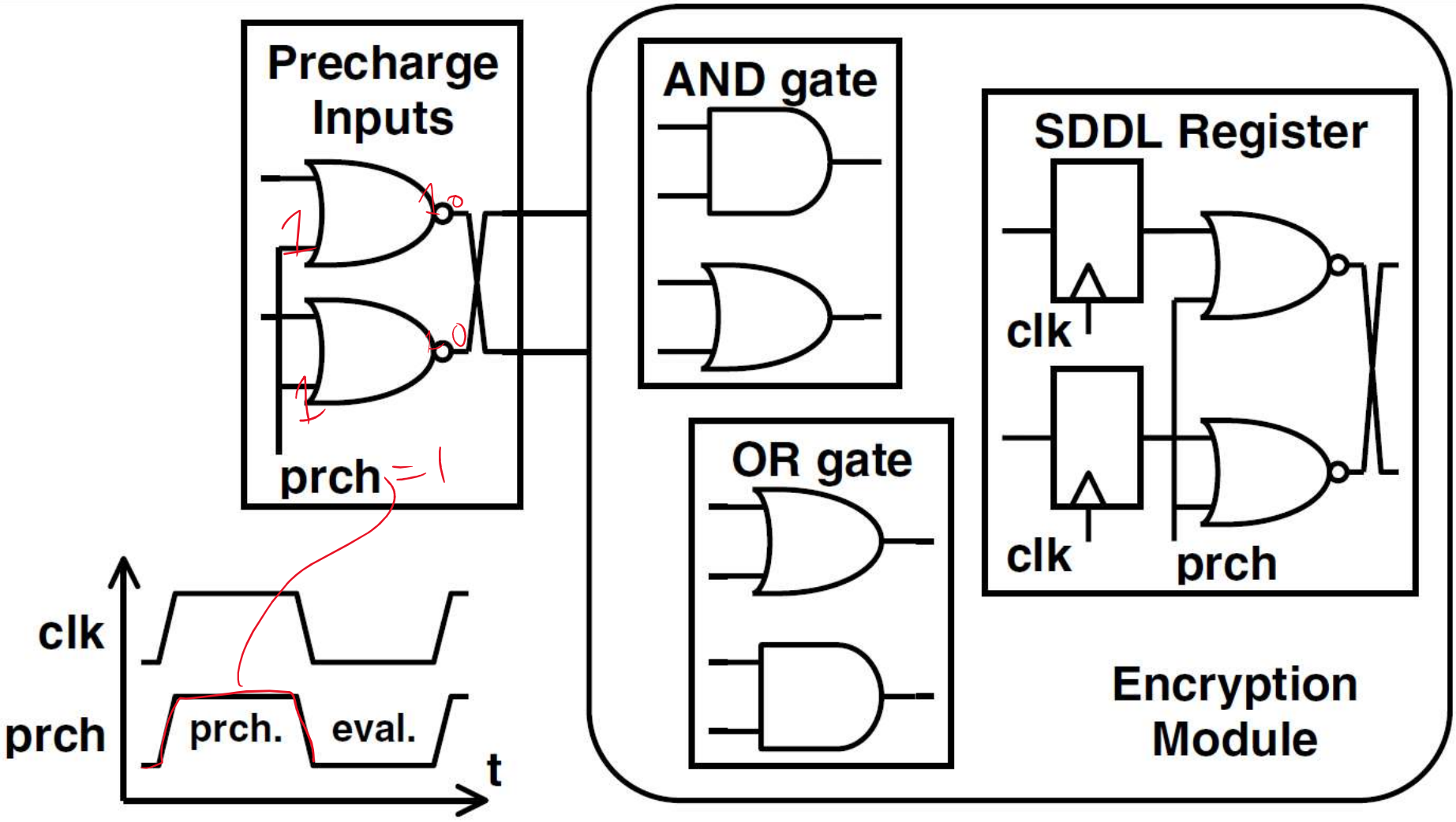
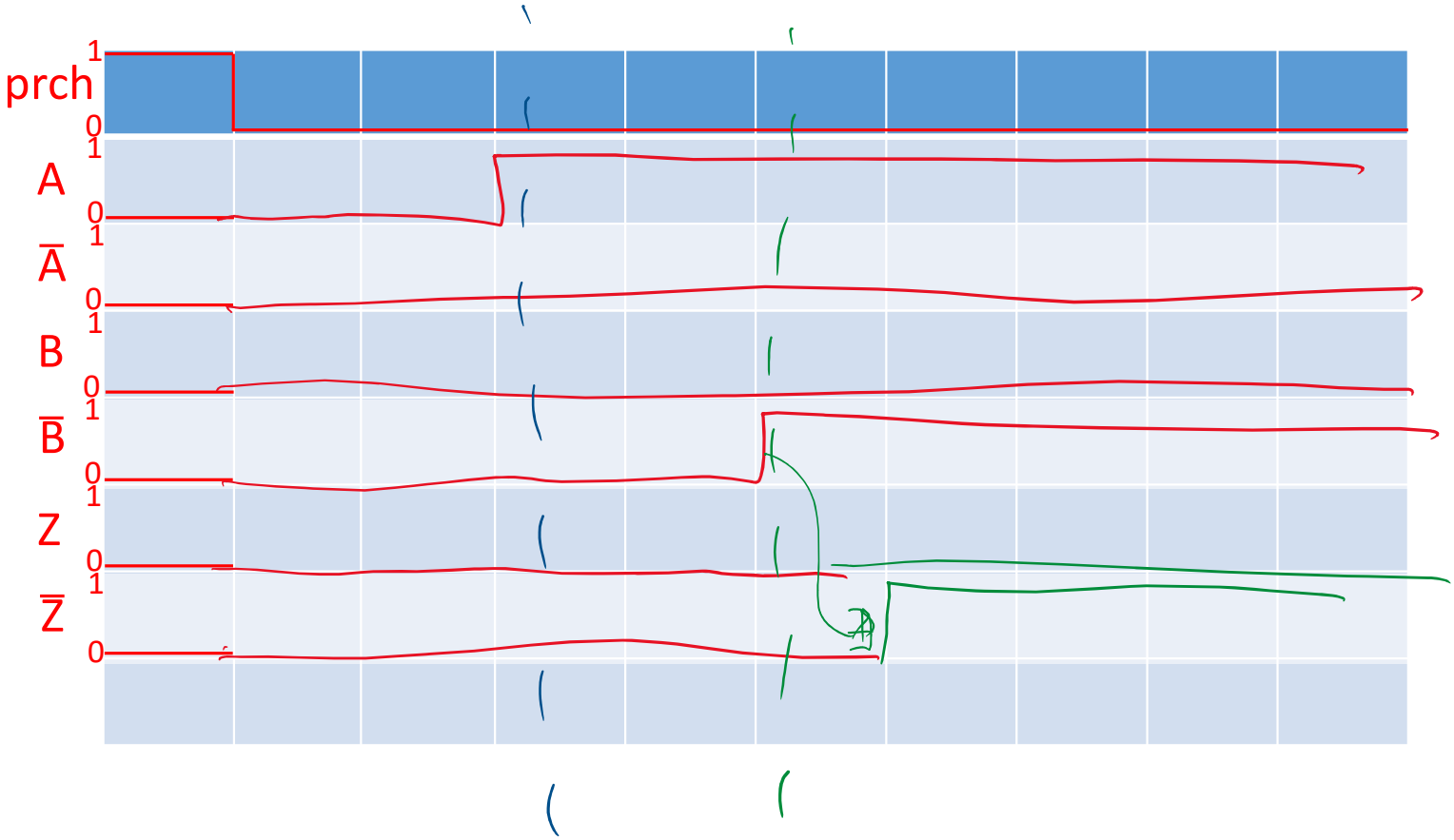
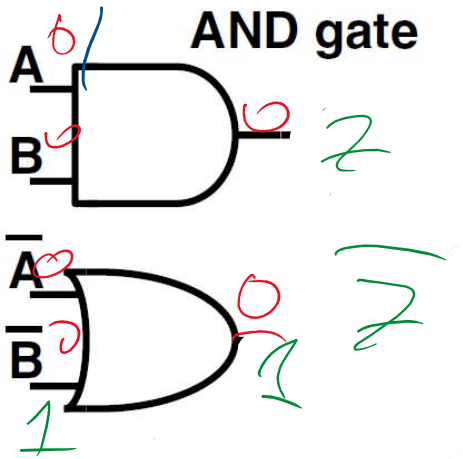


Fig. 3. Precharge wave generation with SDDL FF's





MDDL

AND

$\overline{\text{SDDL}}$

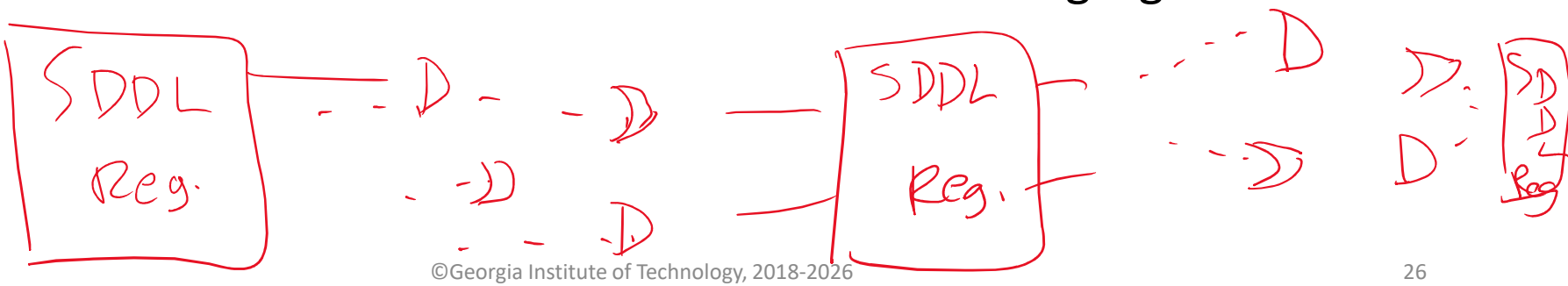
AND

minus prch

©Georgia Institute of Technology, 2018-2026

Summary So Far

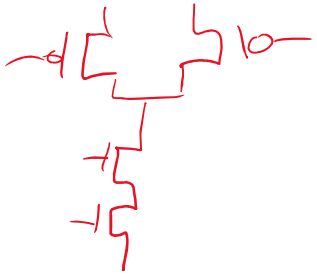
- A precharge phase sets all WDDL logic (And/Or and Or/And) gate inputs and outputs to zero
- An evaluate phase propagates all Flip-Flop (FF) outputs to the next pipeline stage's FF inputs
- We have not covered SDDL FF design for equal energy consumption regardless of input change from 1 to 0 or 0 to 1, but such FF designs exist and in fact have less overhead than the WDDL logic gates

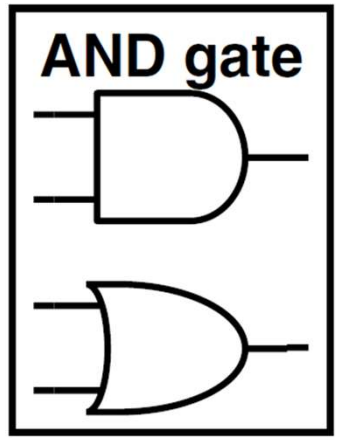


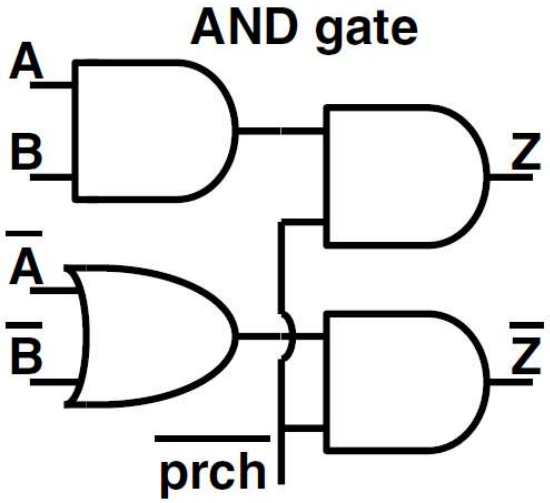
©Georgia Institute of Technology, 2018-2026

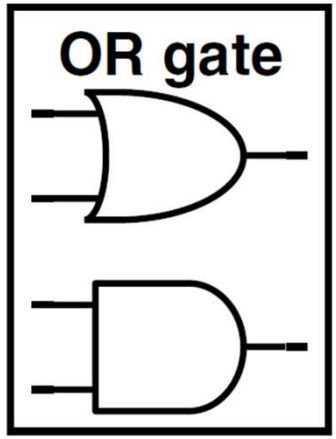
WDDL Overheads

- Area
  - A 2-input NAND or NOR can be implemented with four transistors
  - And-Or WDDL gate? (Recall that $AB = \overline{\bar{A} + \bar{B}}$)
  - And-Or SDDL gate?

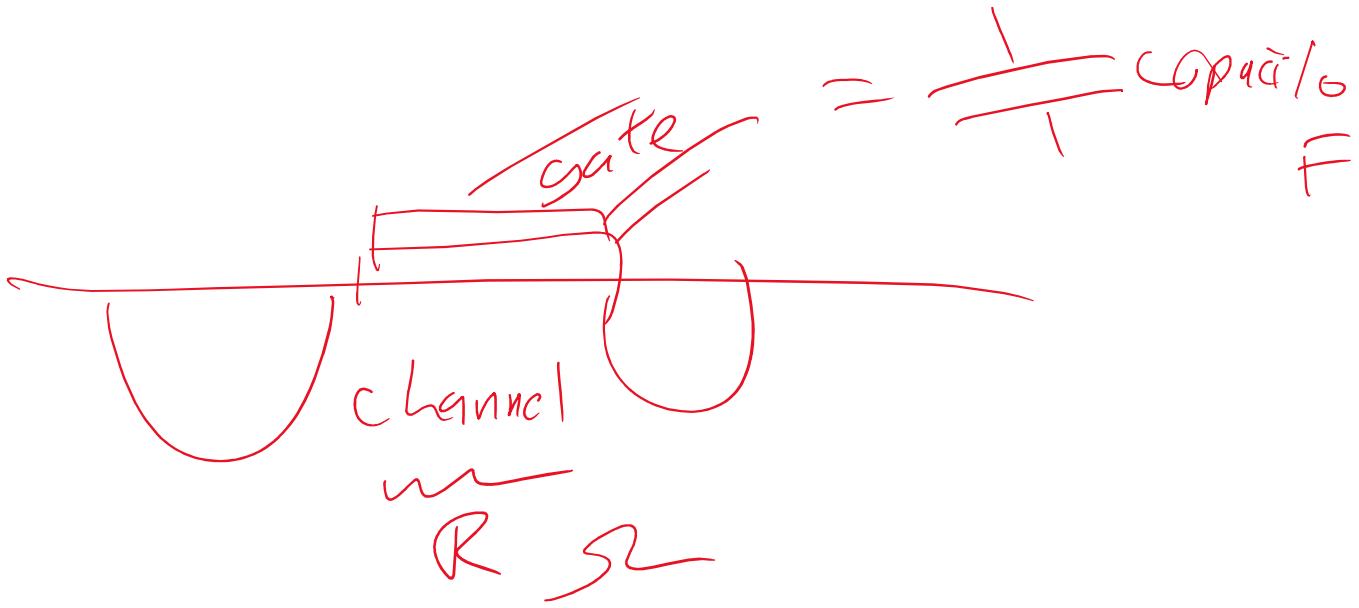








©Georgia Institute of Technology, 2018-2026



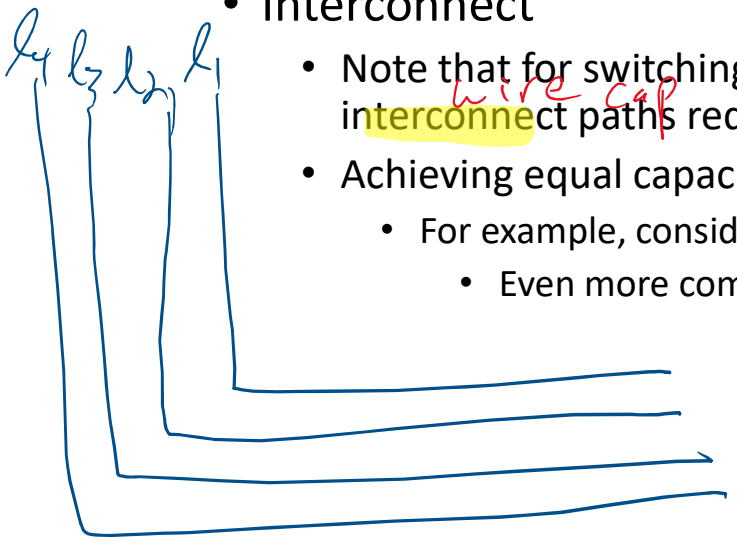
$= \frac{1}{\text{capacitance}}$ F

time = Ω F = seconds

©Georgia Institute of Technology, 2018-2026

WDDL Overheads (Cont'd)

- Capacitance
  - Gate capacitances
    - Inputs, outputs and internal
  - Interconnect
    - Note that for switching events to consume equal energy regardless of 0 versus 1, the interconnect paths require equal capacitance for both cases (0 versus 1)
    - Achieving equal capacitance values for 0 to 1 as well as 1 to 0 events can be complicated
      - For example, consider the carry-bit in a carry lookahead adder or multiplier
        - Even more complicated for larger number sizes, e.g., 64 bits versus 32



©Georgia Institute of Technology, 2018-2026

Recall: Gate Model Based on R, C, Switch

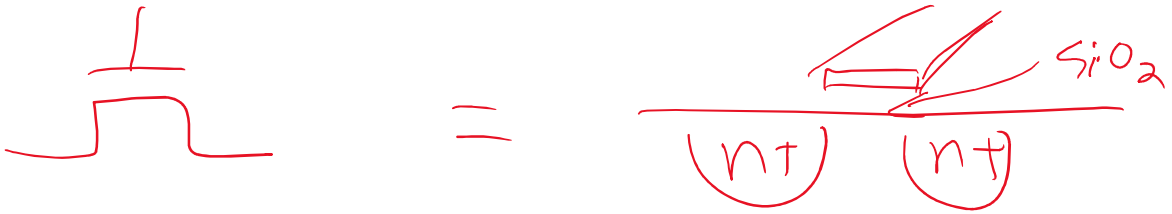


achieving equal R + C values for all 0 → 1 and 1 → 0 transitions is impractical

©Georgia Institute of Technology, 2018-2026

©Georgia Institute of Technology, 2018-2026

Power



- Recall that for a capacitor's charge, Q = CV
- Recall that current is change in charge (i.e., movement) over time:
- i = dQ/dt
- Thus, i = d(CV)/dt = C*(dV/dt)
- => dt = (C*dV)/i
- So, for a constant voltage supply (VDD) and current, doubling the capacitance doubles the amount of time it takes to transfer charge between the capacitor and the power supply (Vdd or Gnd)
- Similarly, energy consumption doubles

©Georgia Institute of Technology, 2018-2026

Fig. 9 shows the statistical properties of the instantaneous supply current. The WDDL mean current is a representative switching event. The point wise absolute variation and standard deviation are small throughout the entire event. This is not the case for the single ended design.

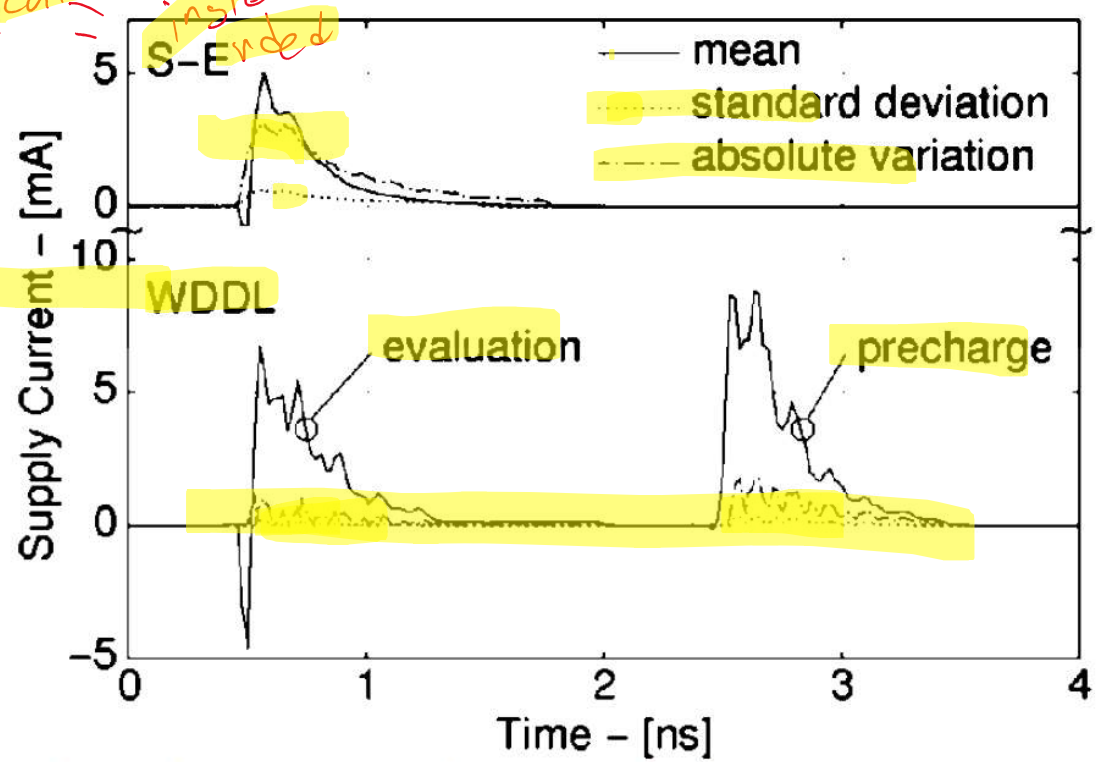


Fig. 9. Supply current characteristics

Table 2 indicates a reduction of a factor 37 in the NED and a factor 52 in the NSD, which are the normalized absolute variation and the normalized standard deviation of the energy per cycle respectively. The reduction comes with an increase of a factor 3.5 in the power consumption.

Table 2. Characterisation of energy consumption

	NED	NSD	E/cycle (pJ)
S-ended	0.4231	0.1152	2.26
WDDL	0.0112	0.0022	7.95

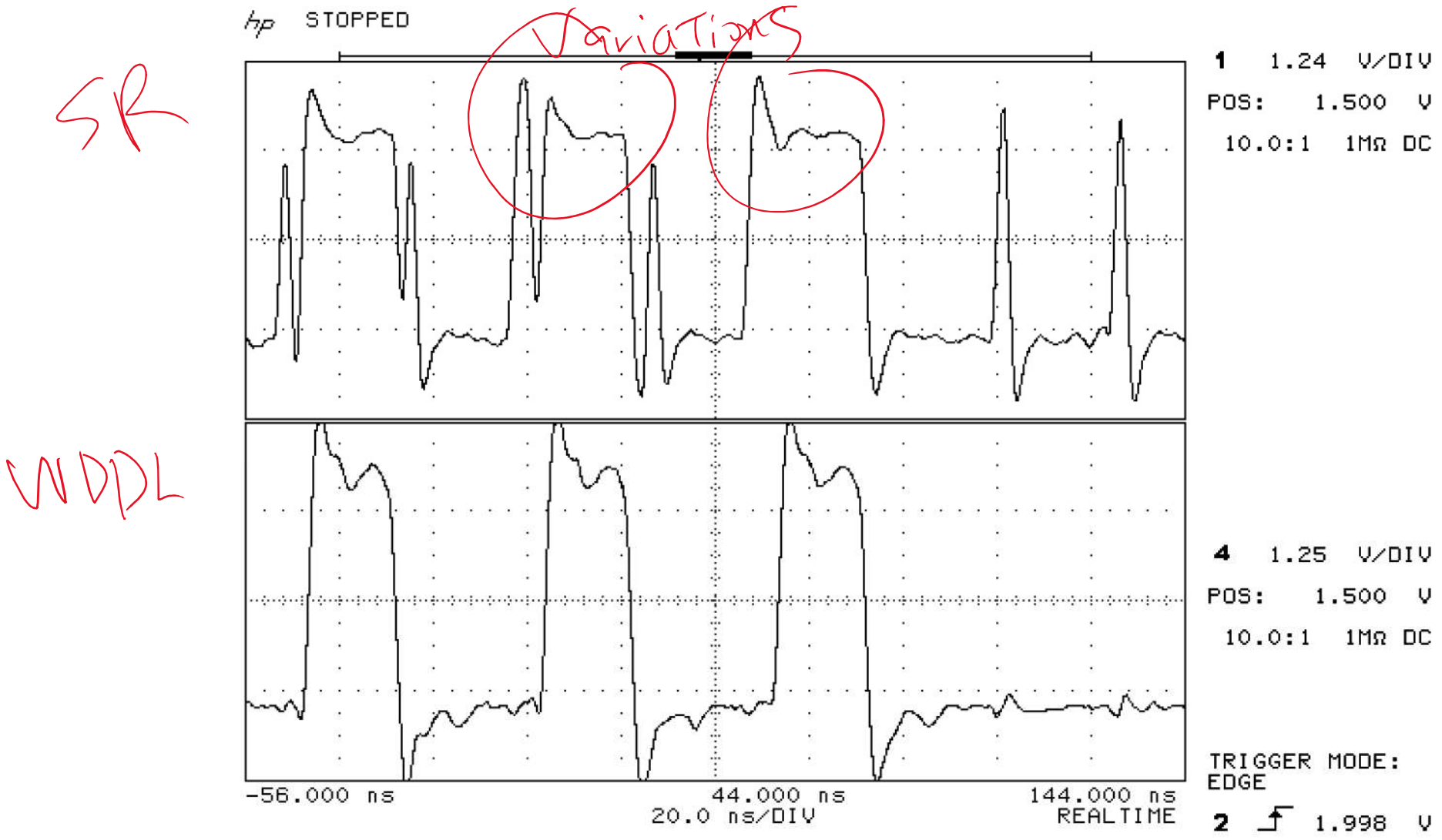


Fig. 10. Output transient: S-E (top); WDDL (bottom)

Single Rail versus Dual Rail

1st problem:

- SR NAND
  - inputs a, b
  - output c
- DR NAND
  - inputs a, $\bar{a}$, b, $\bar{b}$
  - Outputs c, $\bar{c}$

WDDL
Not supported by Std. cell libraries

- NOTE: MODERN SILICON VLSI DESIGN AND FABRICATION PROCESSING TECHNOLOGY ONLY SUPPORTS SR, NOT DR!!!

©Georgia Institute of Technology, 2018-2026

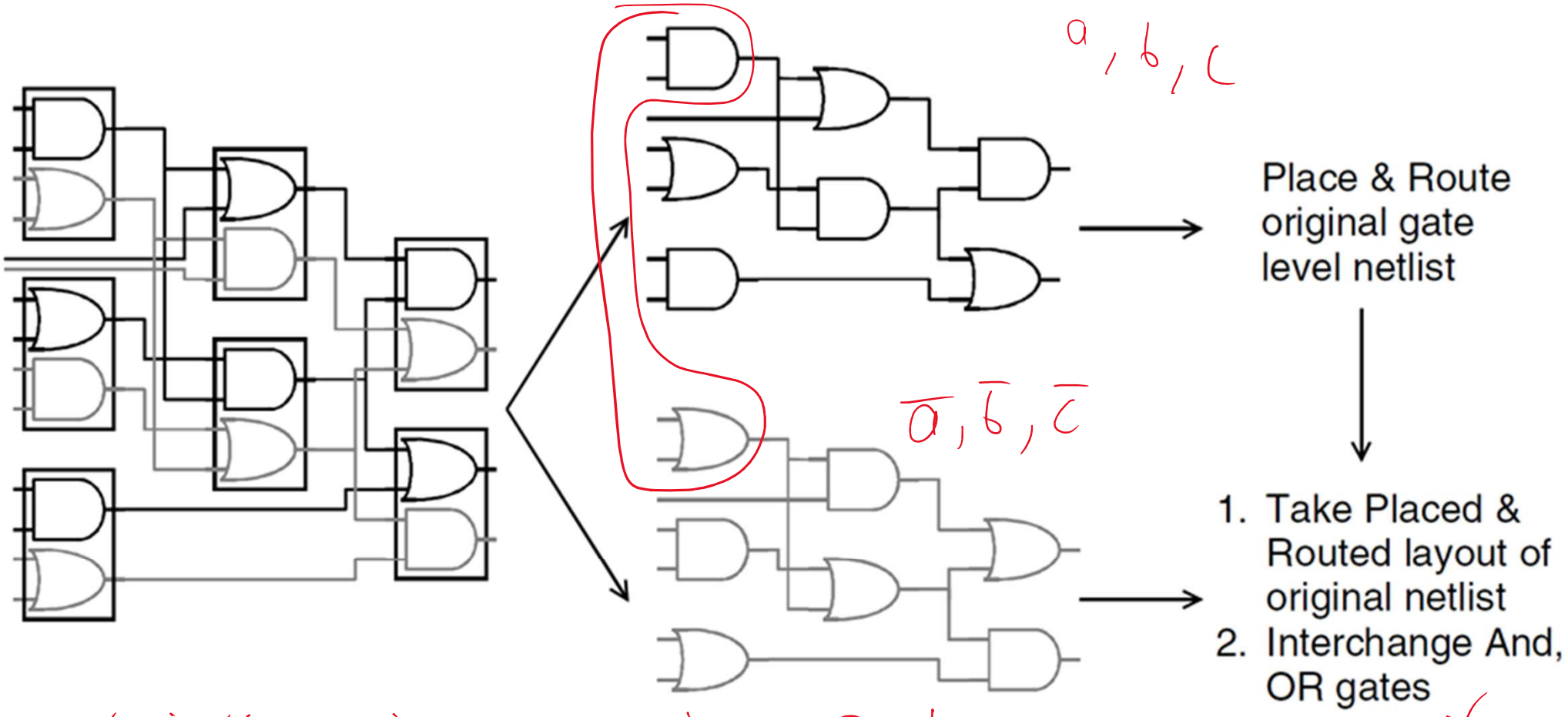


Fig. 5. Derivation of Divided WDDL

variations in energy increase due to separation of positive rail + negative rail

©Georgia Institute of Technology, 2018-2026

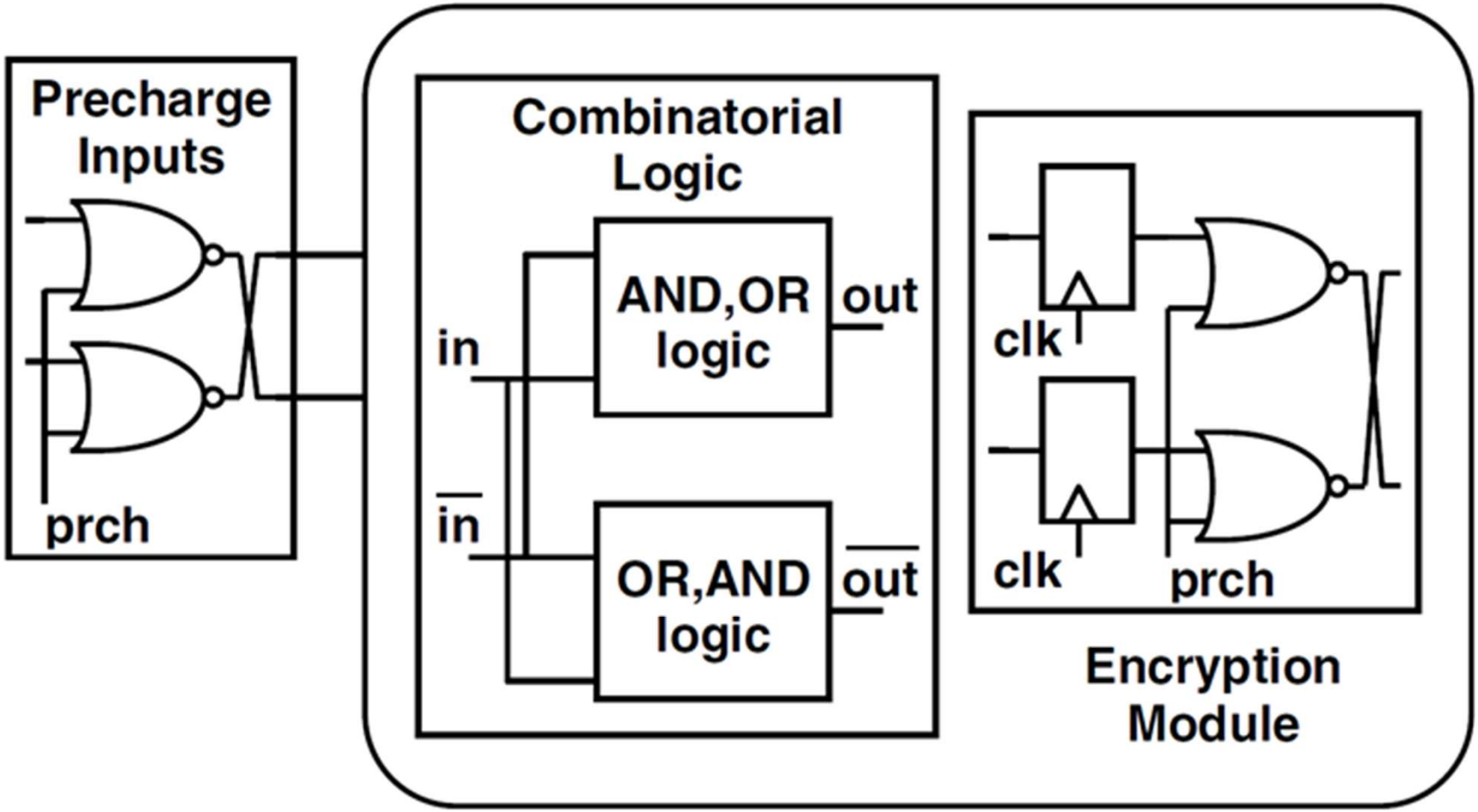
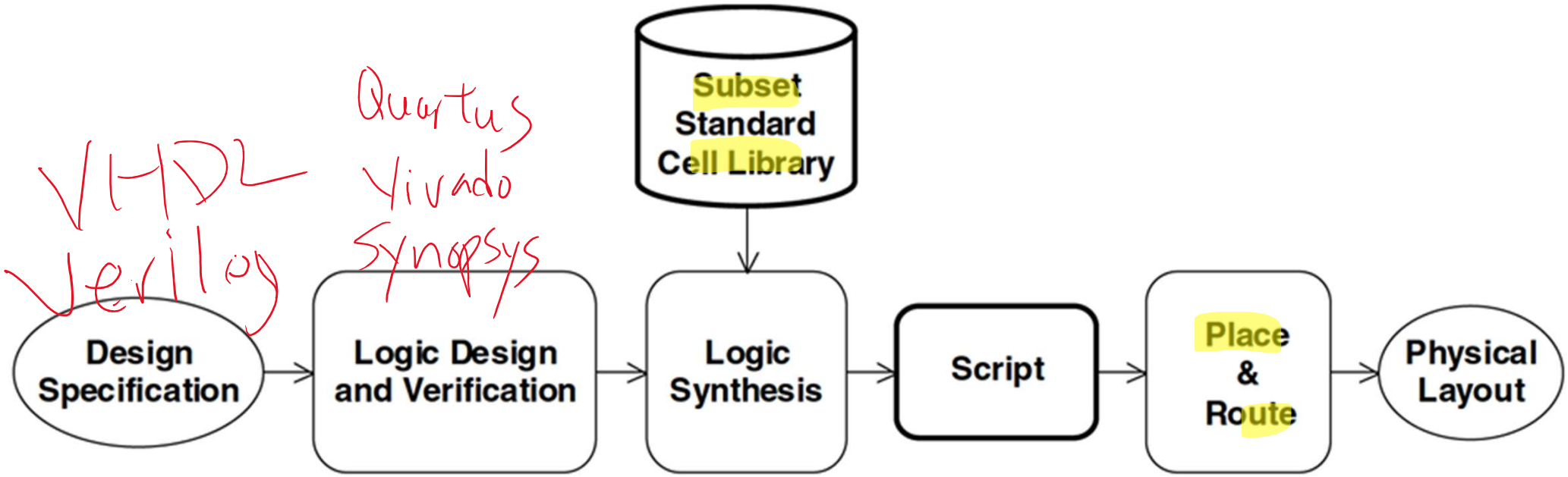


Fig. 6. Divided Wave Dynamic Differential Logic

©Georgia Institute of Technology, 2018-2026



VHDL
Verilog

Quartus
Vivado
Synopsys

Fig. 7. Secure digital design flow

These tools also increase variations in logic gates chosen

©Georgia Institute of Technology, 2018-2026

Conclusions

(1) WDDL reduces the power side channel by 40X to 50X

(2) Power ↑ 3.5 X

(3) Delay ↑ 3.5 X

(4) manufacturing variations in silicon (gates) still result in a power side channel

(5) DR not supported, synthesis tools make it even harder to impl. WDDL

©Georgia Institute of Technology, 2018-2026