# A Solder-Defined Computer Architecture for Backdoor and Malware Resistance

Candidate: Marc W. Abel

Committee: Travis Doom, Ph.D. Dissertation Director
Jack Jean, Ph.D.
Michael Raymer, Ph.D.
Krishnaprasad Thirunarayan, Ph.D. T.K. Prasad
Vincent Schmidt, Ph.D. Air Force Research Laboratory

For slides: https://wakesecure.com

Department of Computer Science and Engineering
30 November 2022

WRIGHT STATE UNIVERSITY

## Three walls to defend

- Software
- Personnel
- Hardware

## Four kinds of hardware problems

- Outdated approaches ignore security
- Excessive complexity hides problems
- Manufacturer interests prevail
- Silicon chips can't be repaired later

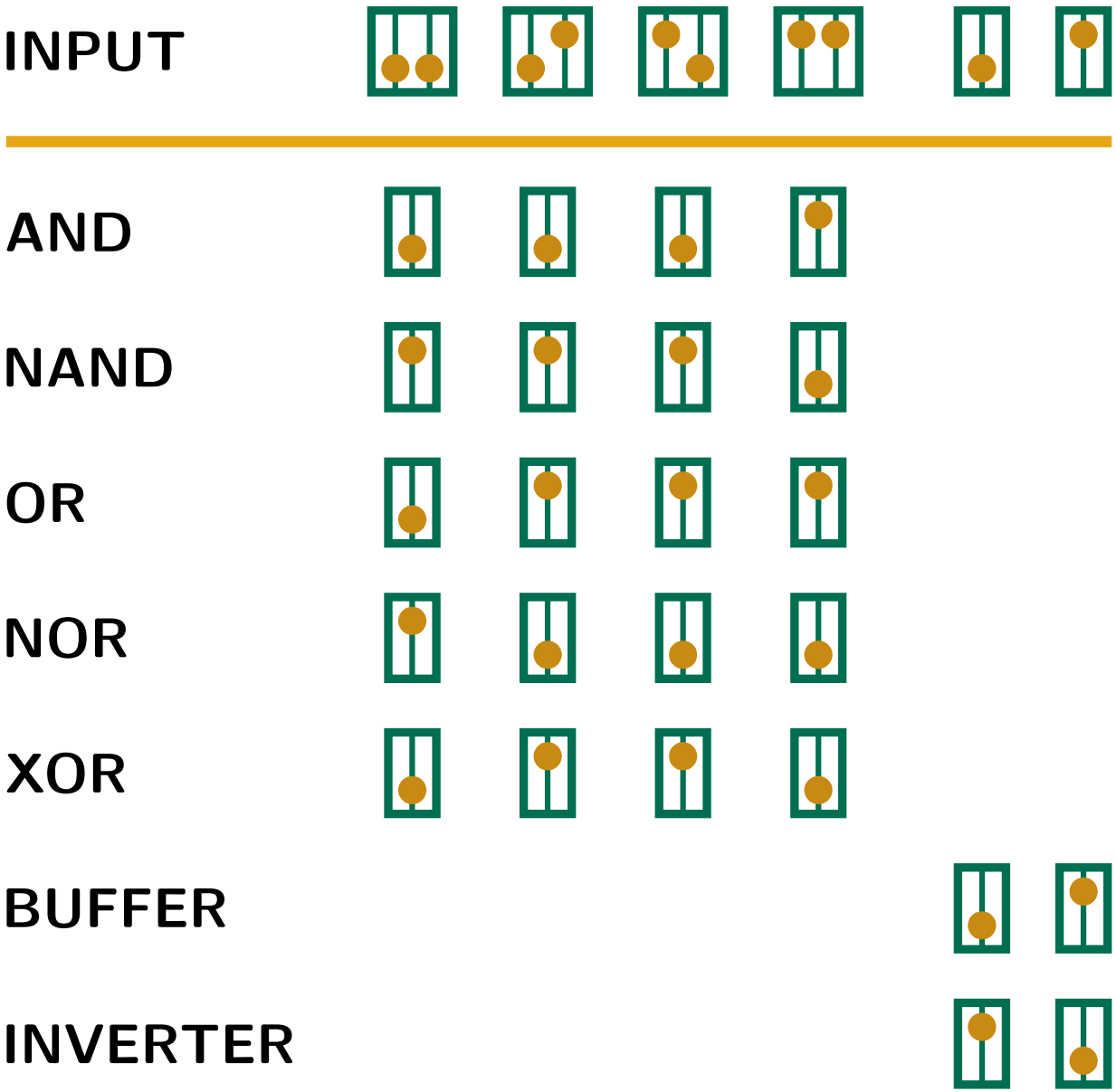
## Three freedoms sought

- Independence from vendors
- Full ownership rights
- Permanent security

## Two enablers of success

- Surface-mount technology
- Firmware in RAM as logic

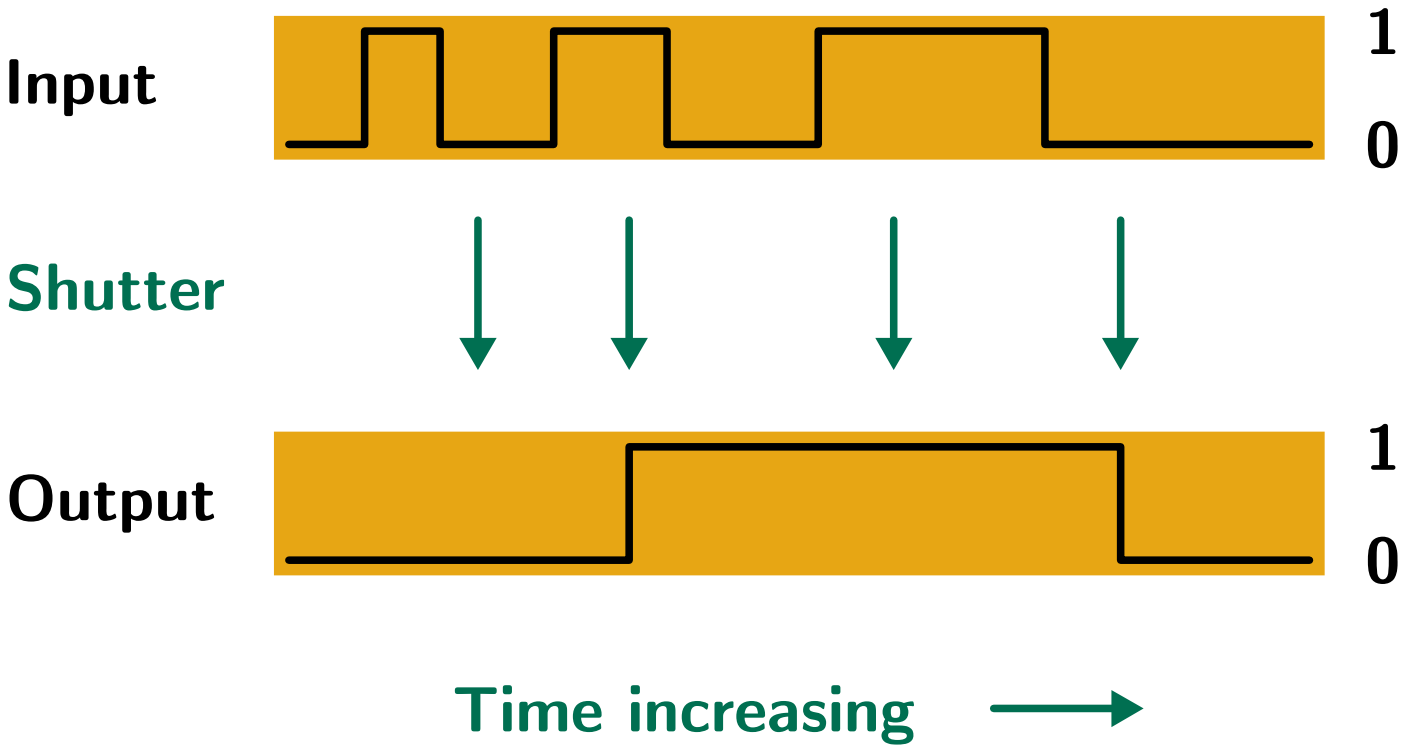
WRIGHT STATE
UNIVERSITY



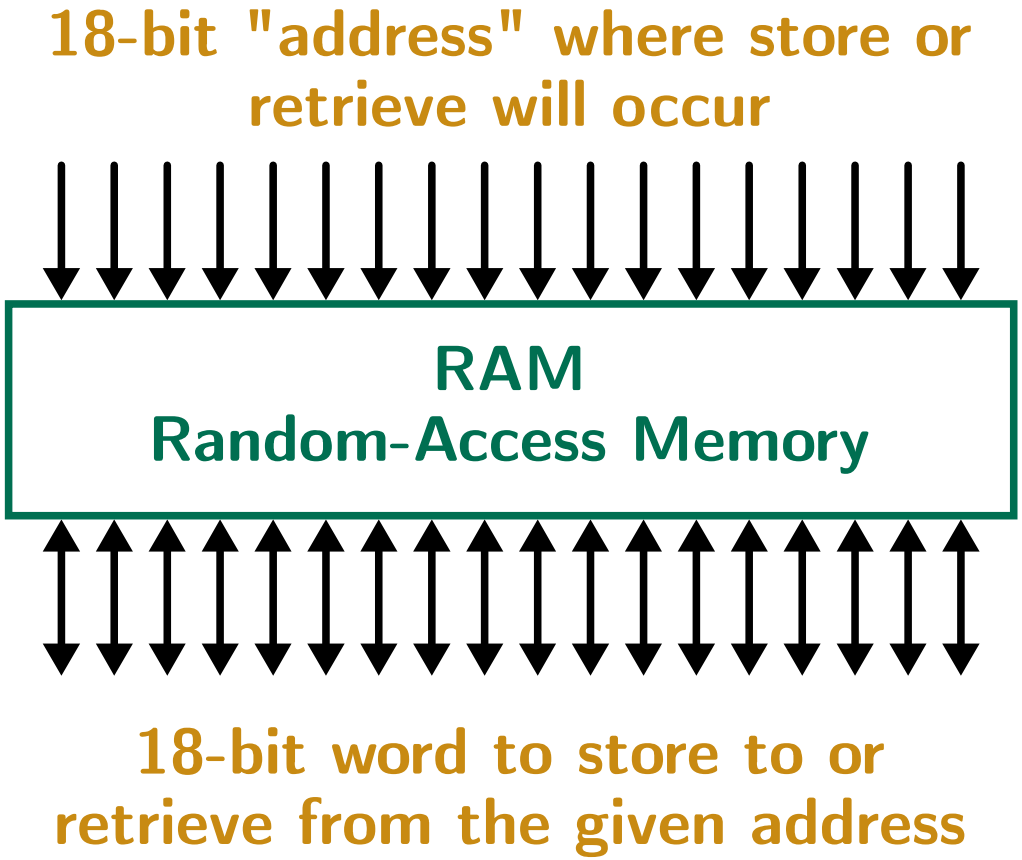

# Seven Basic Logic Gates

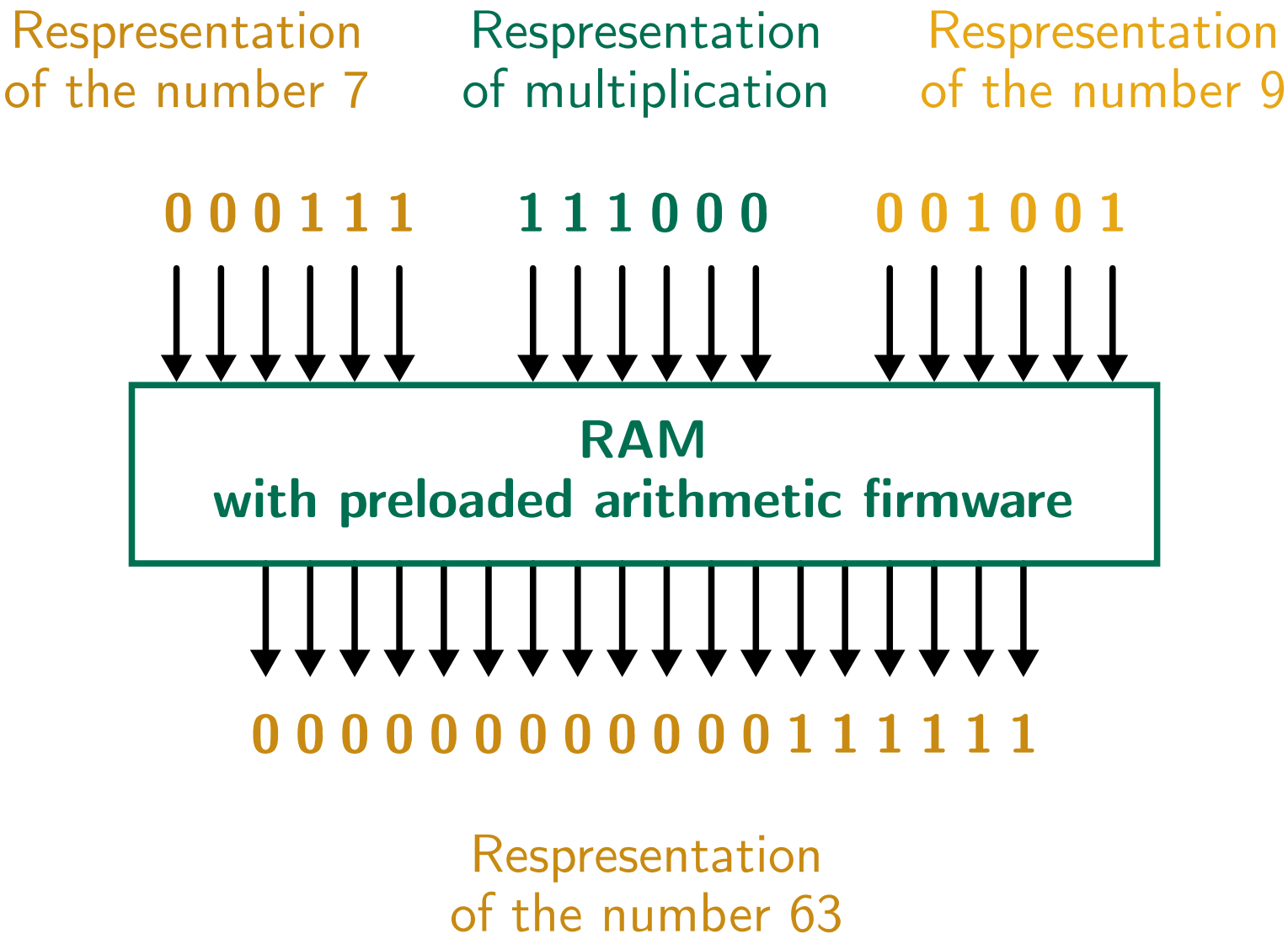
A D flip-flop only changes its output when:

1. told it's time to check, and
2. output doesn't already reflect the input.

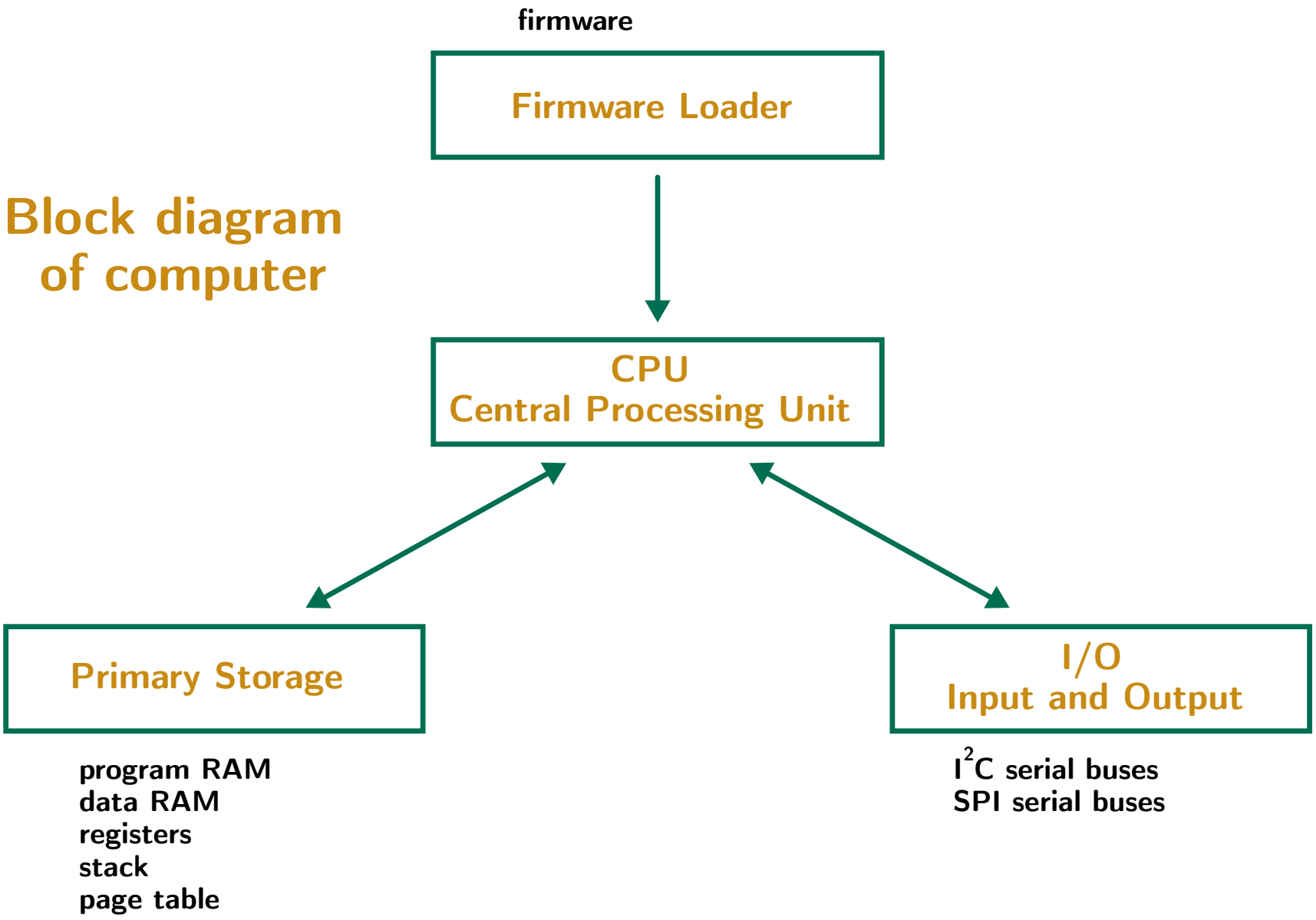


# A RAM can remember a lot of 18-bit words.

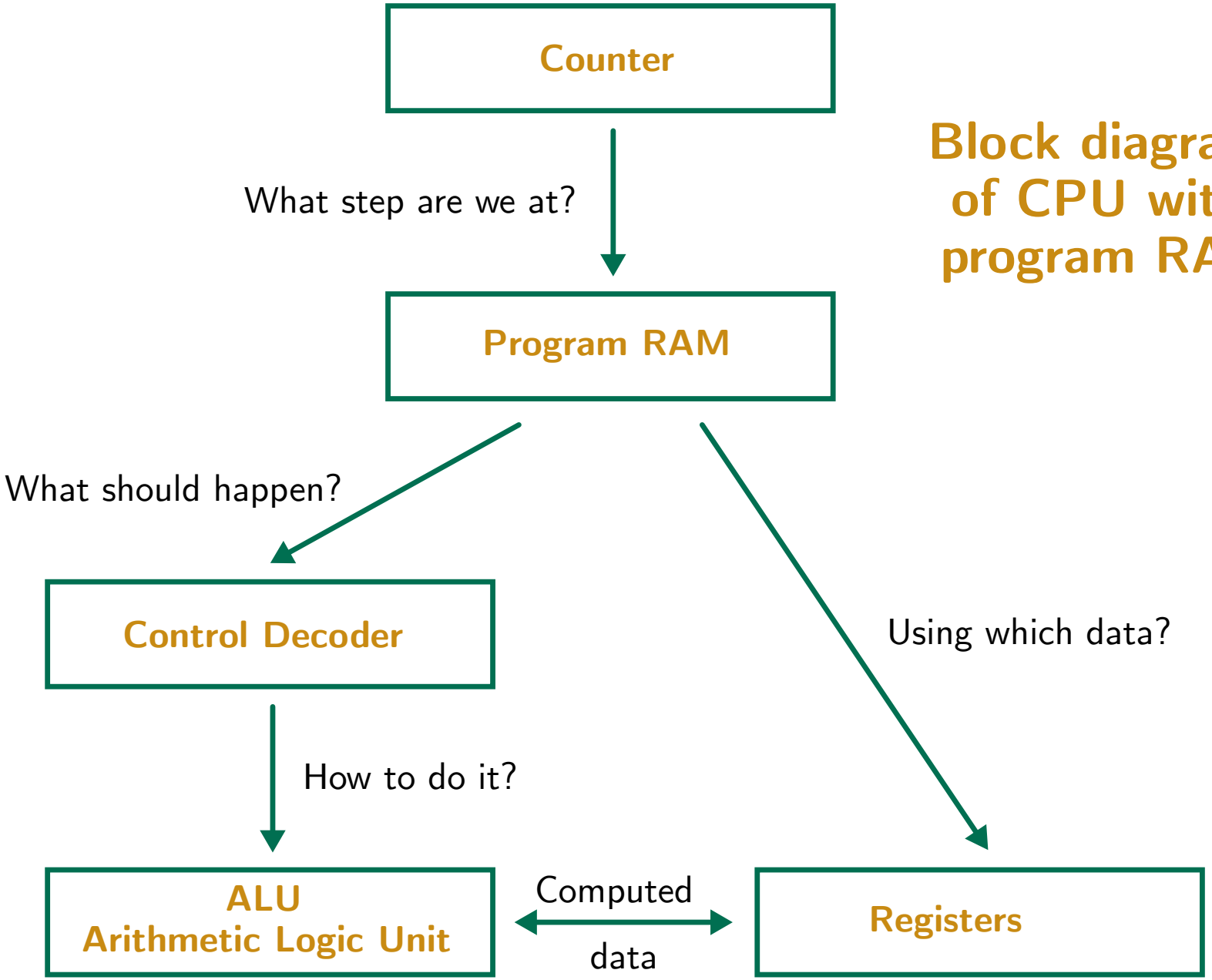


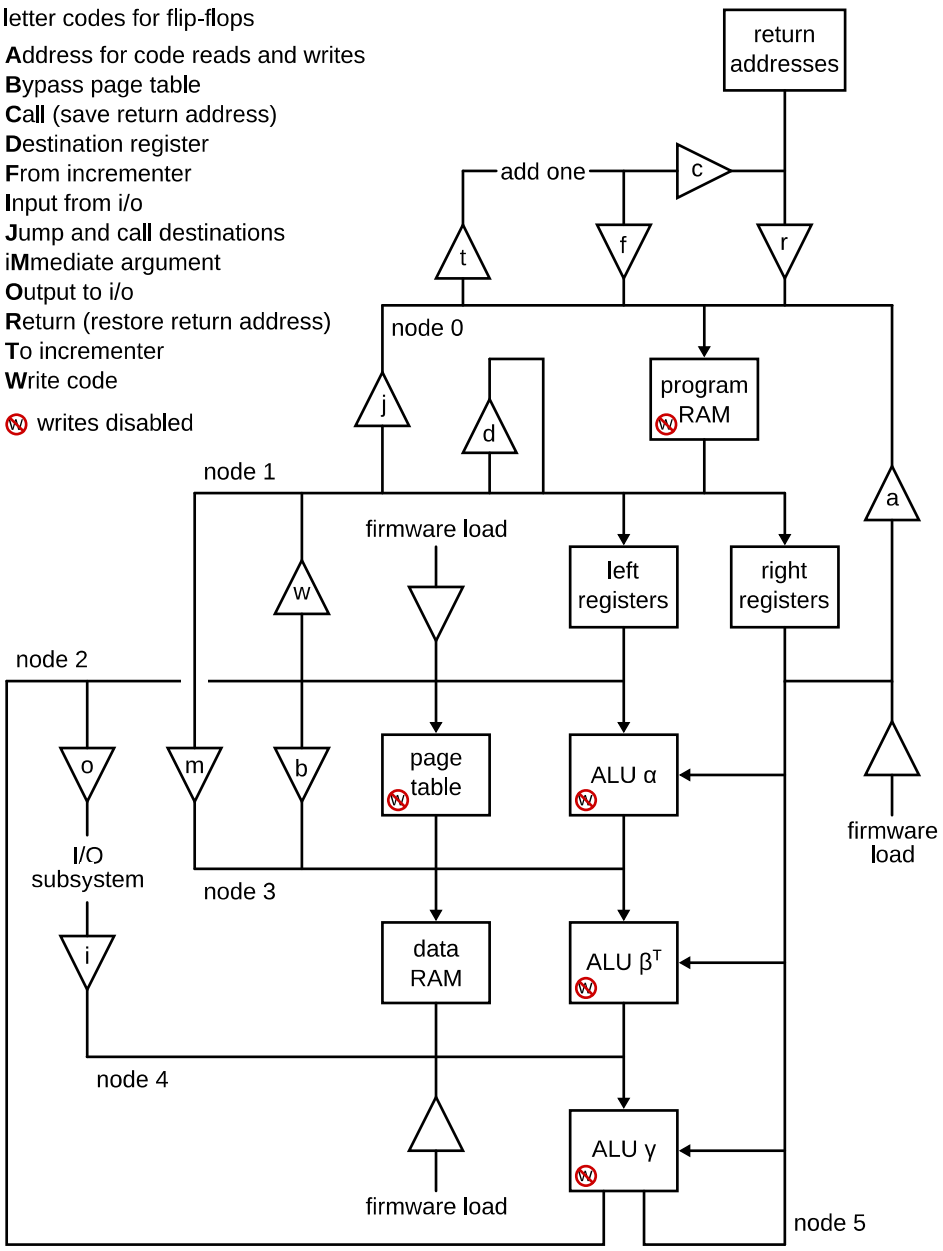

Respresentation
of the number 7
Respresentation
of multiplication
Respresentation
of the number 9
0 0 0 1 1 1
1 1 1 0 0 0
0 0 1 0 0 1
RAM
with preloaded arithmetic firmware
0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1
Respresentation
of the number 63

# Block diagram of computer



# Block diagram of CPU with program RAM

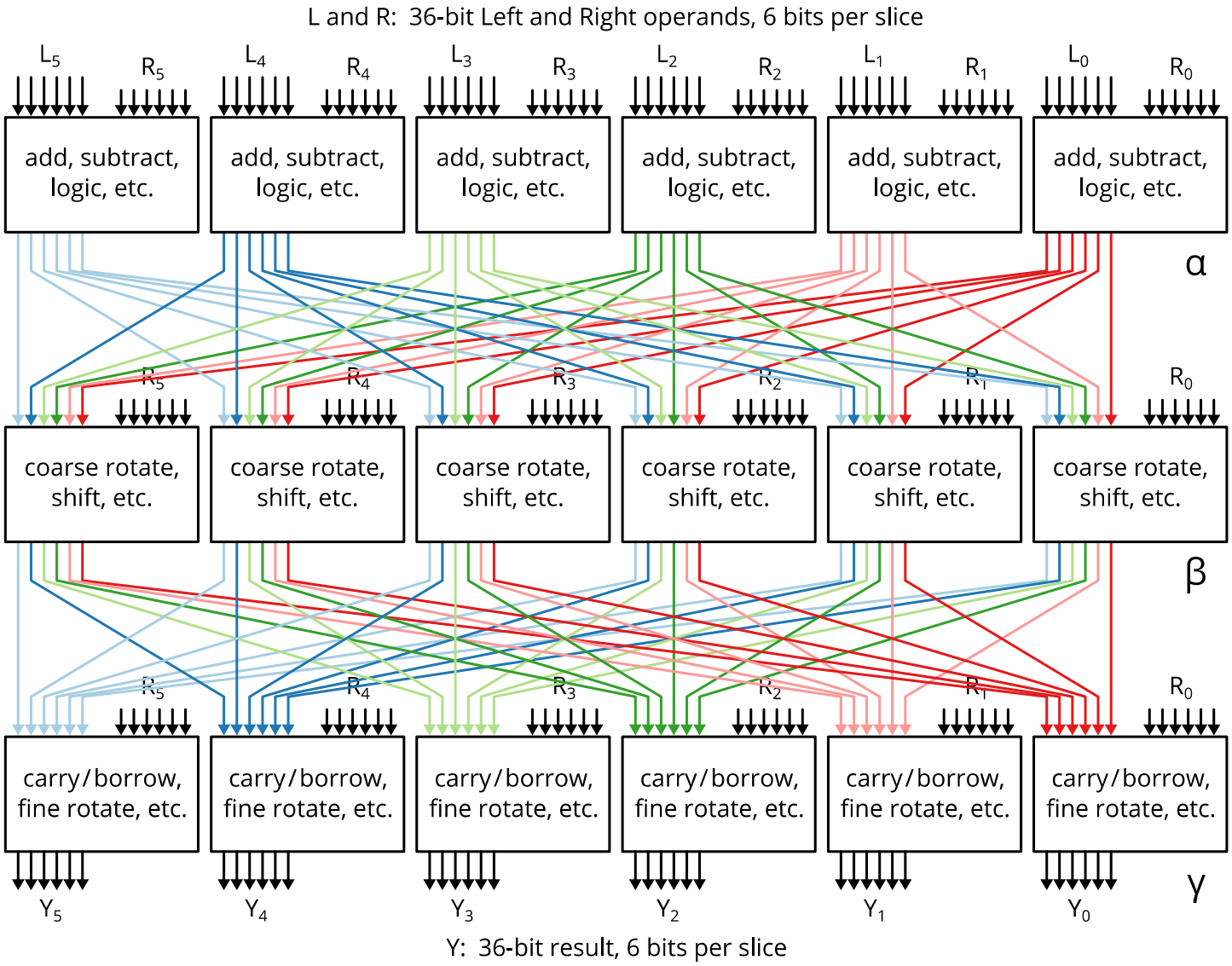


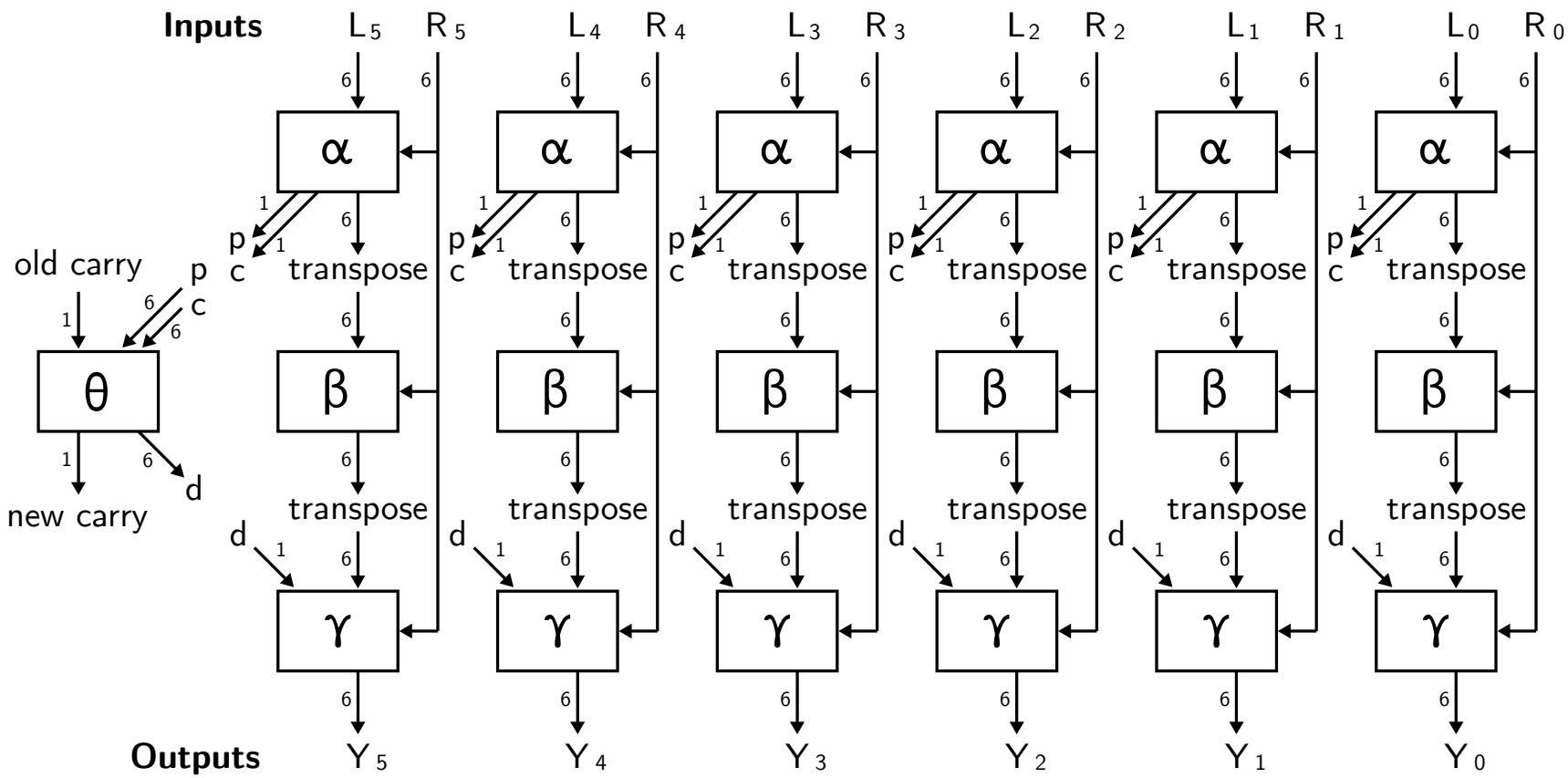



# CPU Principal Data Paths

From page 17 in text.

# Data Layers of ALU





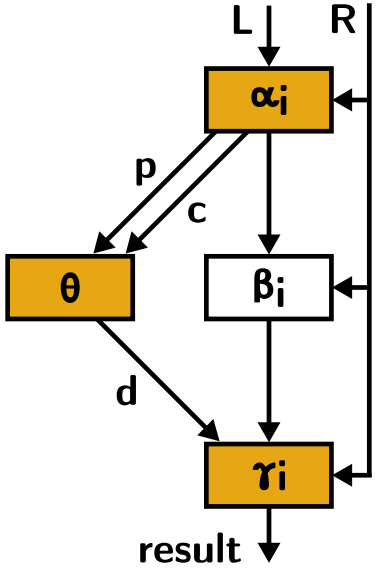

# ALU with carry propagation elements shown

Small digits that are not subscripts indicate number of wires. From page 88 in text.

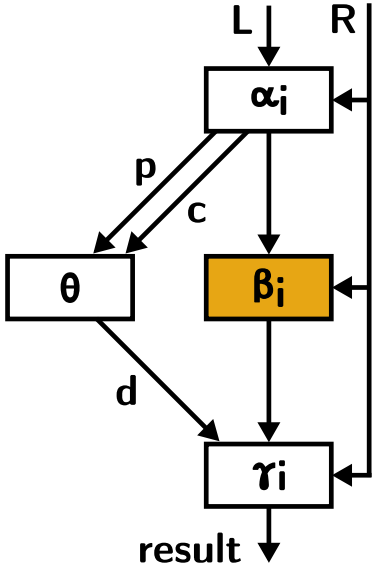
# Superposition of ALU Operations

From page 76 in text.

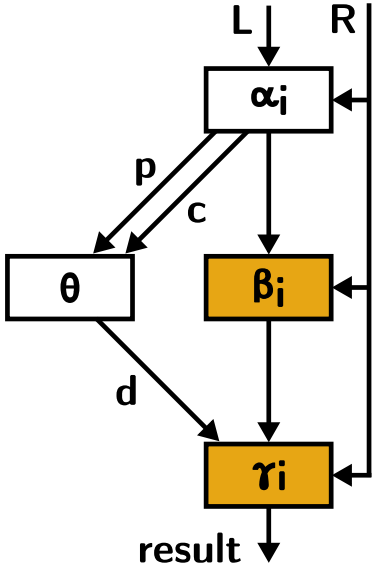
Carry-skip adder



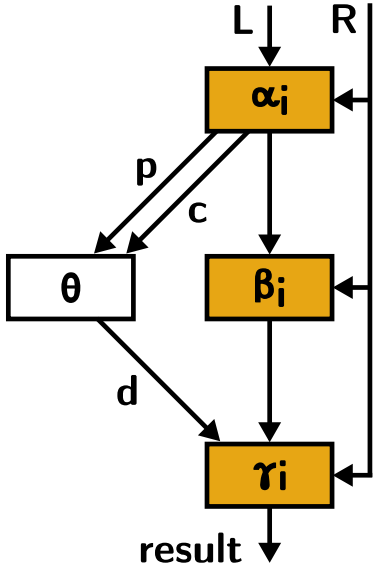

Swizzler




Logarithmic shifter




Substitute & permute

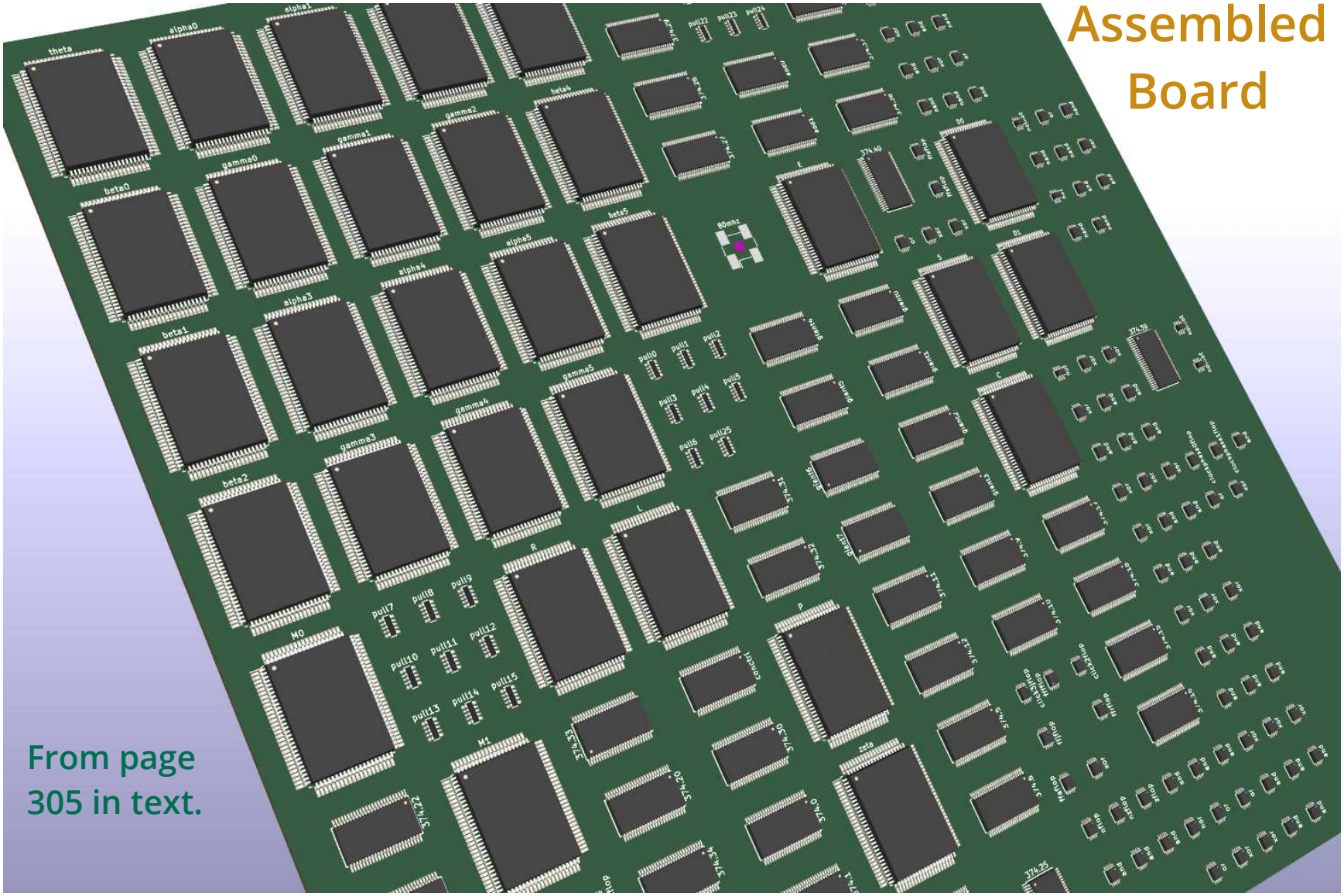



Same circuit
Same chips
Same board space

# Circuit Board Floorplan

From page 180 in text.

# Sketch of Assembled Board




From page 305 in text.

## Fast Enough For

- Hardened desktop apps
- Electronic mail
- Light- to moderate-use servers
- Controlling objects that move
- Process controls
- Peripheral & device controllers
- Telephony
- Modest Ethernet switches

## Too Slow For

- Most Web surfing
- Machine learning
- Image and video processing
- Self-driving vehicles
- Fast raster or vector graphics
- Fast symmetric cryptography
- Fast asymmetric cryptography
- Bioinformatics

# Security Improvements

- Sticky out-of-range flag for all arithmetic
- Mixed-sign variants for add, subtract, multiply, shift, abs. value
- Stack overflow unlikely, can't lead to privilege escalation
- No program access to stack except CALL and RETURN
- No branch to addresses not present in the instruction word
- No privilege escalation via the CPU
- No DRAM or DRAM-associated vulnerabilities
- No complex logic from IC manufacturers within CPU
- Every I/O device confined to its own bus and buffer
- No CPU persistent state except for one firmware IC
- No secret functionality
- No vendor lock-in
- No encrypted or closed-source firmware
- No license fees to build, use, or modify
- No purpose of use limitations
- No right to repair infringements

# Demonstration

# Before This Can Be Built

- Preemptive multitasking
- I/O subsystem to support SPI and $I^2C$ buses
- Firmware loader
- Resolution of clock skew concern

# Ways to Get Involved

- Firmware upgrade for faster multiplication
- Support for integer division
- Floating point like IEEE 754-2019, but 36- and 72-bit formats
- Floating point for compatibility (32- and 64-bit formats)
- More assembler features
- Lightweight operating system
- Lightweight scripting language
- Lightweight programming language
- Minimalist toolchain that can be audited
- I/O device drivers
- TCP/IP stack
- TLS 1.3
- New block cipher to leverage architecture
- Formal verification (similar to seL4 or INTEGRITY-178B)

WRIGHT STATE
UNIVERSITY