

Delta Force



presents...

Primality Verification Chip

VLSI Design

Dr. Cavallaro

December 7, 2000

Nick Reinhart

Ajeet Pai

Jeff Hale

Mike Clifford

Goals / Motivation

- Primes are heart of modern public-key encryption
- Security of system rests on primality
- Real-world project

Bad Approaches

- Several approaches explored
 - Simple trial division
 - Base-A pseudo-primality testing
 - Miller-Rabin test
- Avoid approaches requiring mod-exp
- Require factorization

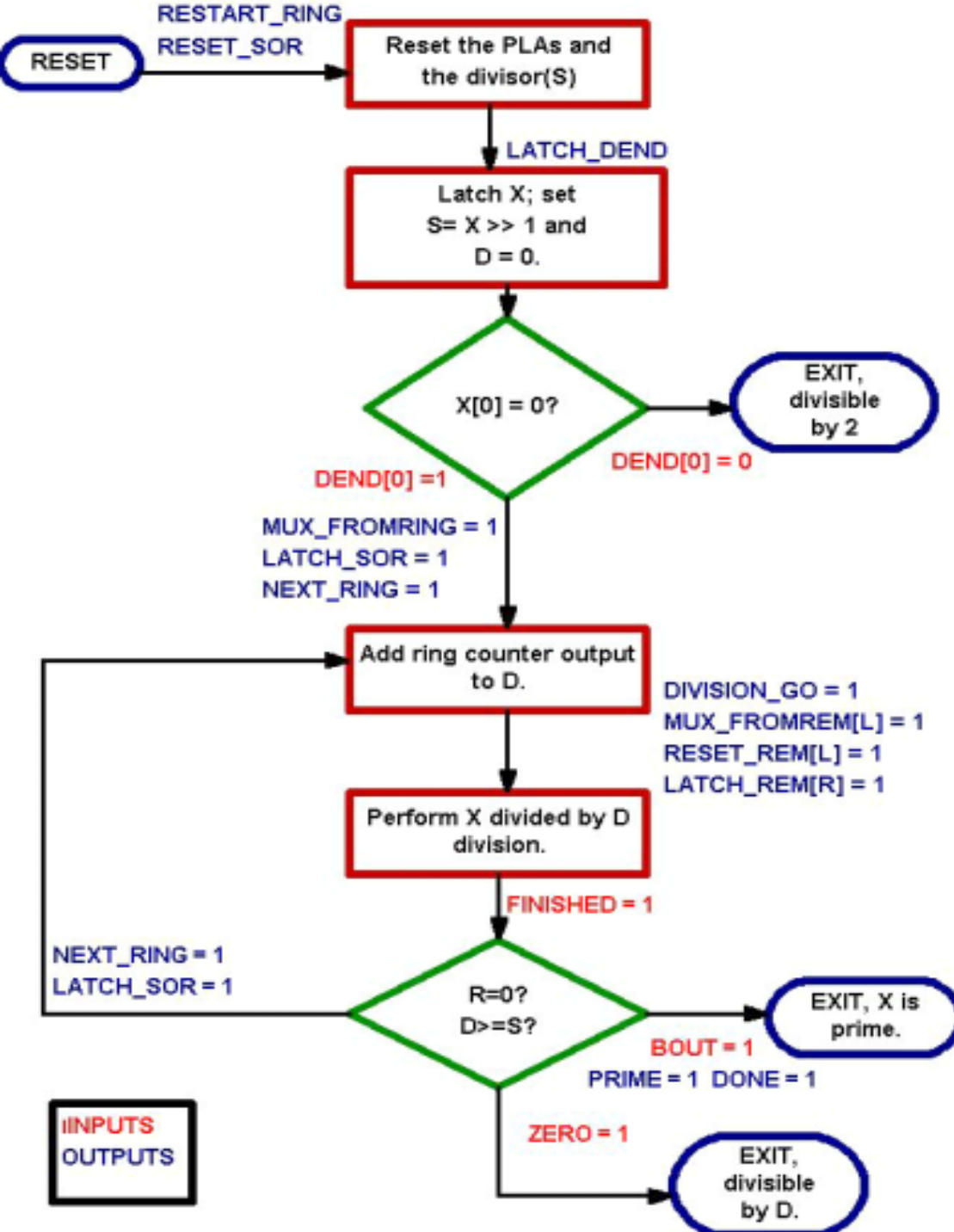
Really Bad Approaches

- Random Guessing
- Multiply-and-guess
- Division with Memory
- Assuming the best
- Hopeful indifference
- Asking Laura
- Divine Intervention
- Onefish-Twofish
- Ask a friend
- CDMA algorithm
- Beer & Fortitude
- Lookup table
- Exhaustive Search
- Fried Cheese

Wille's Algorithm

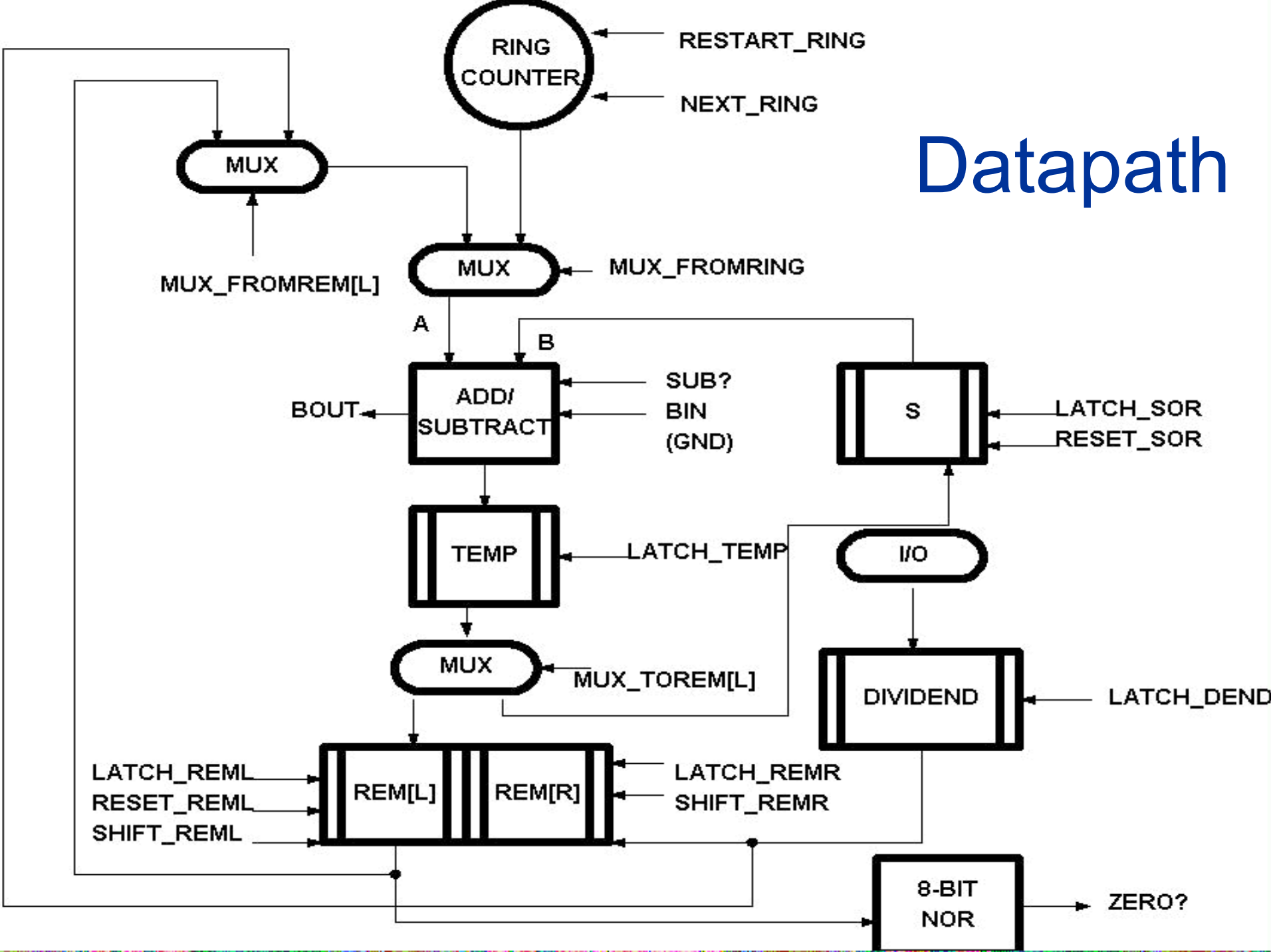
- Seek elegant way to factor primes
- Optimized trial-division method
- Use number-theory pattern to reduce field
- Eliminate all numbers divisible by 2,3,5
 - 50% eliminated on first pass
 - 33% eliminated on second pass
 - At 7, step through using {6,4,2,4,2,4,6,2}

Algorithm Flowchart

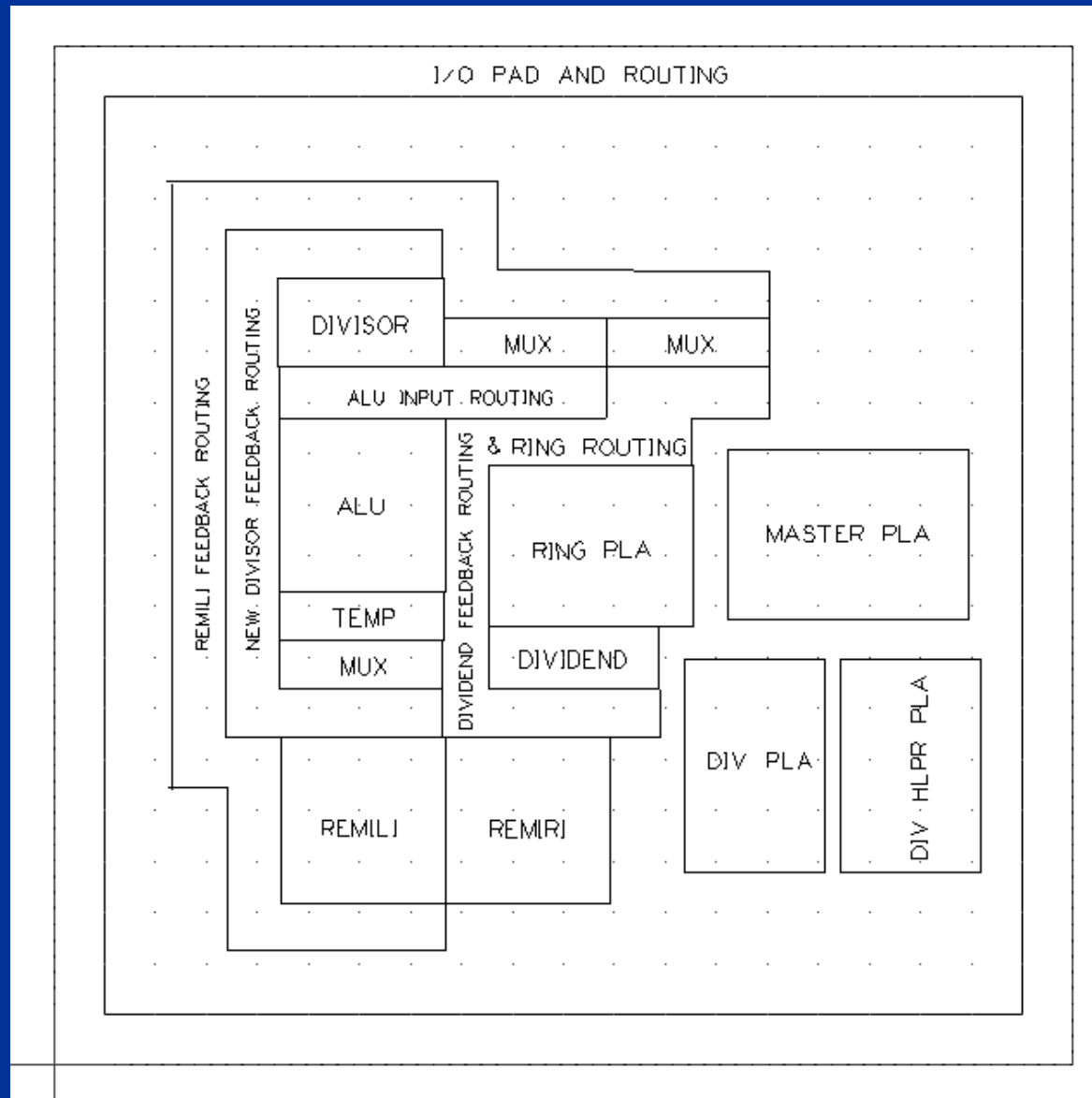


- 0) Input X, set $D = 1$
- 1) $X / 2 = 0? \Rightarrow$ exit
- 2) $X \% D = 0? \Rightarrow$ exit
- 3) Repeat as necessary, incrementing S by $\{6, 4, 2, 4, 2, 4, 6, 2\}$
- 4) If divisor = $X/2$ output PRIME

Datapath

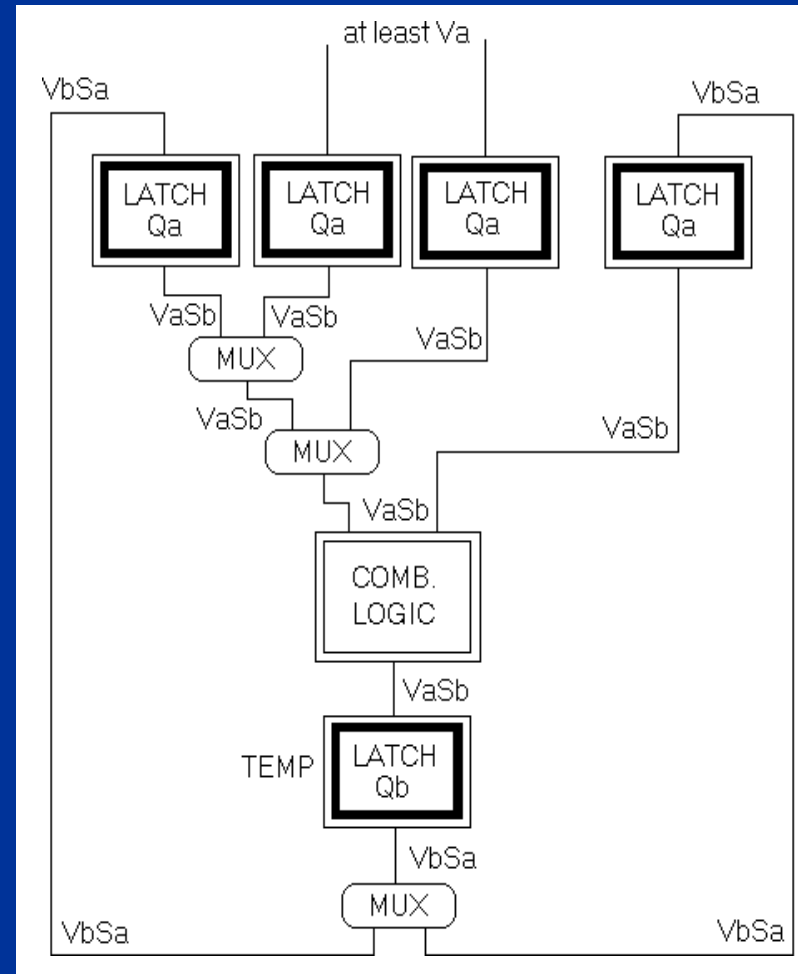
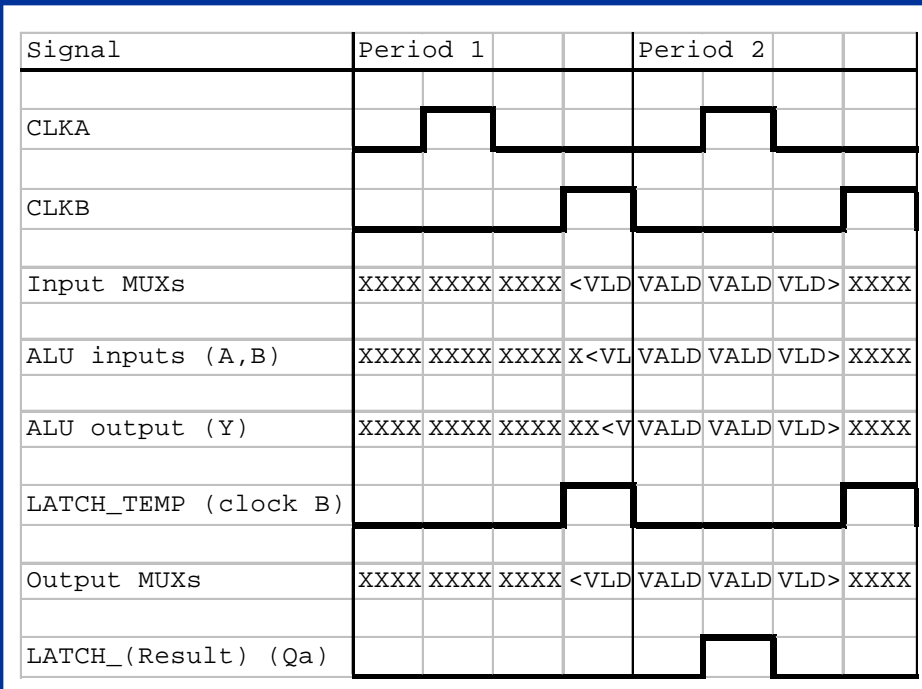


Floorplan

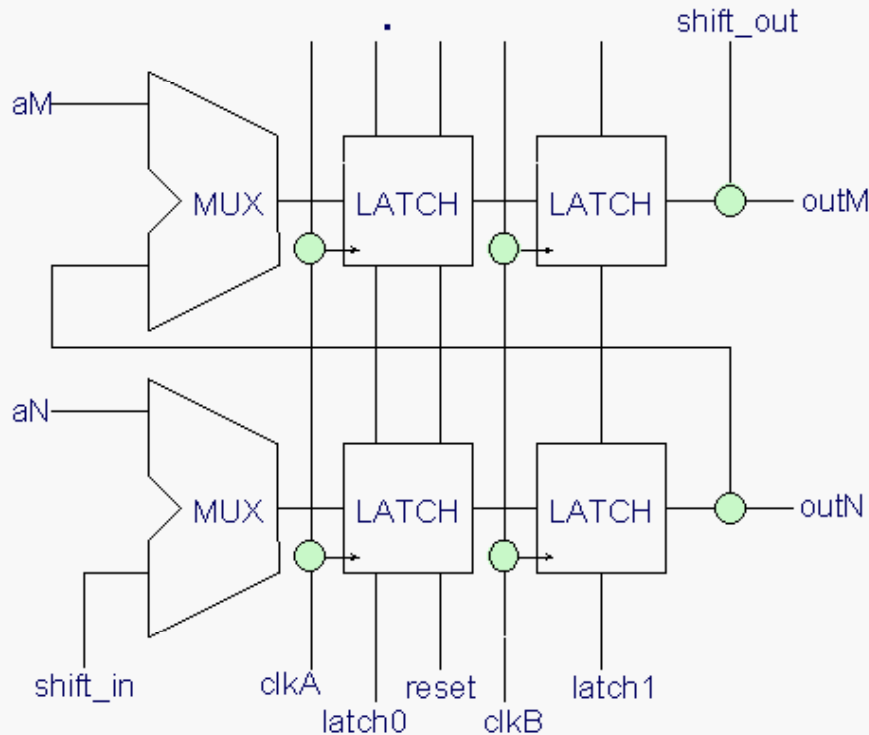


System Timing

- PLA sets input and output MUXs.
- ALU inputs and outputs stabilize.
- Result latched in appropriate LATCH on next CLK A.



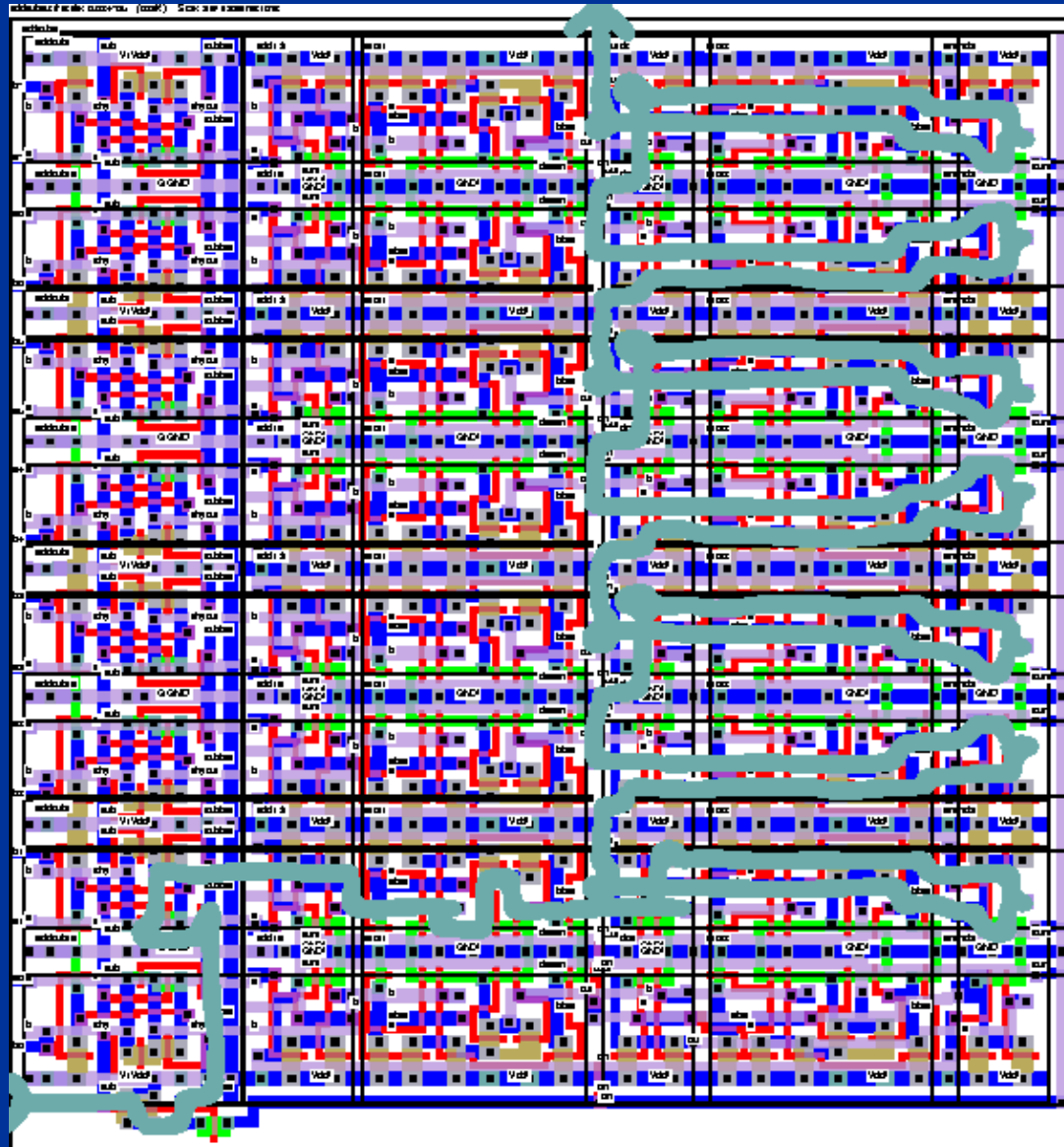
Layout Example



- Shift register functional diagram
- Because of tiling, seek minimal layout

Layout Example: Shift Register

Preliminary Performance



Preliminary Performance

- 30 ns worst-case propagation
- Assume 50 ns clock high
- Assume 25% duty cycle (2 phase clock)
- Total clock period ~ 200 ns
- Worst-case clocking: 5Mhz

Status

- Major subcell layout/testing complete
- PLA design/testing complete
- Timing analysis complete
- Final layout incomplete
- Total layout simulation incomplete
- I/O padframe placement incomplete