

HW #4 Discussion

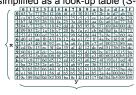
- Problem 1 did just a simple adder work?
- Problem 2 how did you implement the permutation table?
- Problem 3 did you use a counter?

November 2, 2006 CprE 583 – Reconfigurable Computing

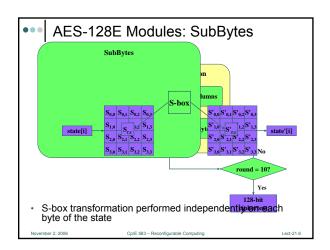
AES-128E Algorithm Round Transformation ShiftRows MixColumns Found++ No round = 10? Yes 128-bit ciphertext November 2, 2006 CprE 583 - Reconfigurable Computing

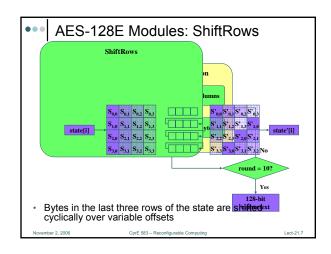
• • Overview of AES (cont.)

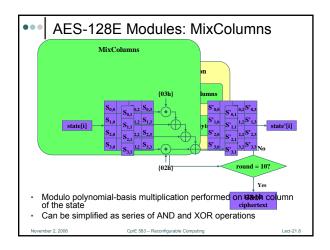
- 128-bit input is copied into a two-dimensional (4x4) byte array referred to as the state
 - · Round transformations operate on the state array
 - Final state copied back into 128-bit output
- AES makes use of a non-linear substitution function that operates on a single byte
 - Can be simplified as a look-up table (S-box)

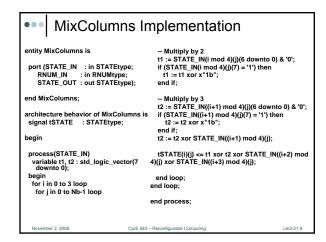


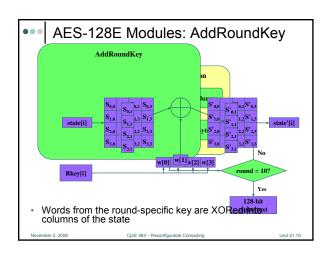
vember 2, 2006 CprE 583 – Reconfigurable Computing

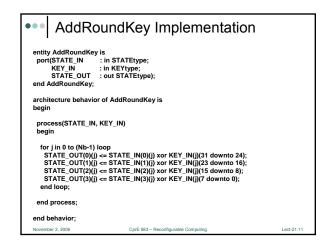


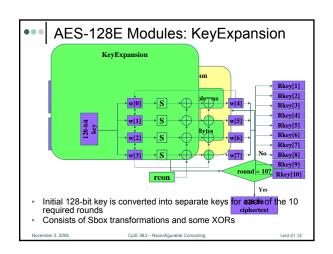












Design Decisions

- · Online/offline key generation
- · Inter-round layout decisions
 - Round unrolling
 - Round pipelining
- · Intra-round layout decisions
 - · Transformation pipelining
 - Transformation partitioning
- Technology mapping decisions
 - S-box synthesis as Block SelectRAM, distributed ROM primitives, or logic gates

November 2, 2006

ParE E93 Reconfigurable Computing

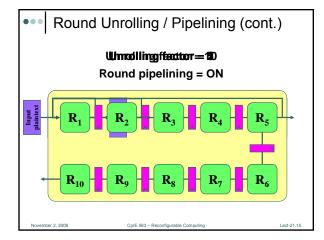
••• Round Unrolling / Pipelining

- Unrolling replaces a loop body (round) with N copies of that loop body
- AES-128E algorithm is a loop that iterates 10 times
 N ∈ [1, 10]
 - N = 1 corresponds to original looping case
 - N = 10 is a fully unrolled implementation
- Pipelining is a technique that increases the number of blocks of data that can be processed concurrently
 - Pipelining in hardware can be implemented by inserting registers
 - Unrolled rounds can be split into a certain number of pipeline stages
- These transformations will increase throughput but increase area and latency

November 2 2006

CprE 583 - Reconfigurable Computing

Loct-21 14

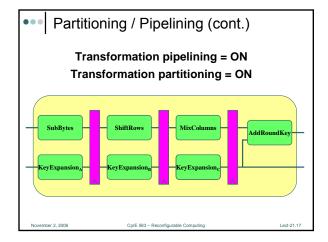


Transformation Partitioning/Pipelining

- FPGA maximum clock frequency depends on critical logic path
 - Inter-round transformations can't improve critical path
 - Individual transformations can be pipelined with registers similar to the rounds
- Transformations that are part of the maximum delay path can be partitioned and pipelined as well
- Can result in large gains in throughput with only minimal area increases

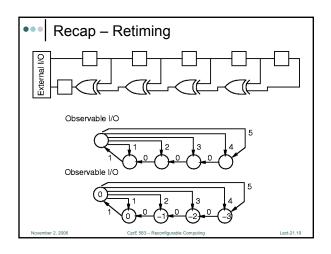
November 2, 200

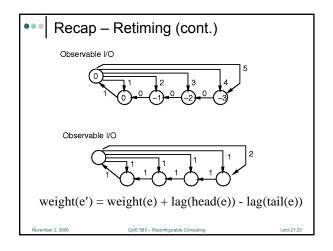
Lect-21.16

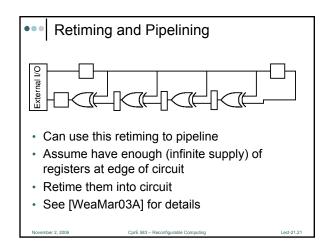


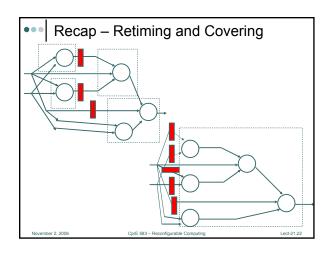
S-box Technology Mapping

- With synthesis primitives, can map the S-box lookup tables to different hardware components
- Two S-boxes can fit on a single Block SelectRAM









Outline HW #4 Discussion Recap HW/SW Codesign Motivation Specification Partitioning Automation Reconfigurable Computing Lect-21.23

Definition 1 – the concurrent and co-operative design of hardware and software components of an embedded system
 Definition 2 – A design methodology supporting the cooperative and concurrent development of hardware and software (co-specification, co-development, and co-verification) in order to achieve shared functionality and performance goals for a combined system [MicGup97A]

Hardware/Software Codesign

••• Motivation

- Not possible to put everything in hardware due to limited resources
- Some code more appropriate for sequential implementation
- Desirable to allow for parallelization, serialization
- Possible to modify existing compilers to perform the task

November 2, 2006

CorE 593 Pasantiauroble Computing

l act-21 25

••• Why put CPUs on FPGAs?

- · Shrink a board to a chip
- · What CPUs do best:
 - Irregular code
 - Code that takes advantage of a highly optimized datapath
- · What FPGAs do best:
 - · Data-oriented computations
 - · Computations with local control

November 2 2006

OprE 583 - Reconfigurable Computing

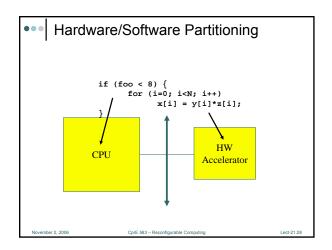
Computational Model

General-Purpose Processor

Memory
bus

FPGA

 Most recent work addressing this problem assumes relatively slow bus interface
 FPGA has direct interface to memory in this model



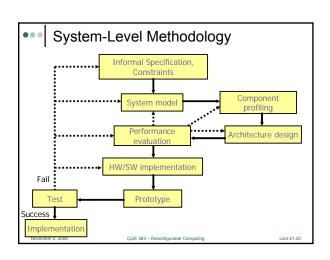
Methodology

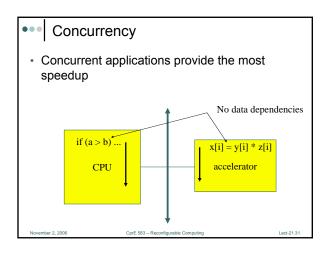
- · Separation between function, and communication
- · Unified refinable formal specification model
 - · Facilitates system specification
 - · Implementation independent
 - · Eases HW/SW trade-off evaluation and partitioning
- From a more practical perspective:
 - Measure the application
 - · Identify what to put onto the accelerator
 - Build interfaces

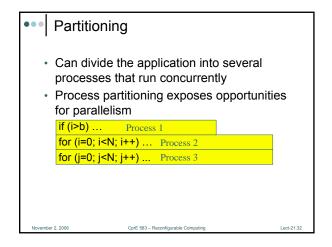
November 2, 2006

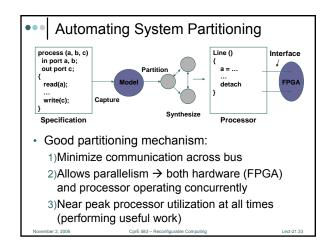
CprE 583 – Reconfigurable Computing

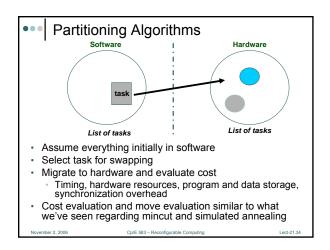
ect-21.29

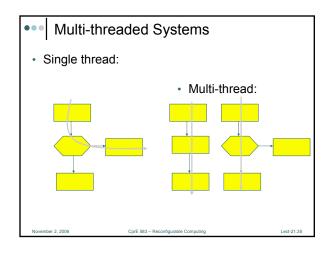


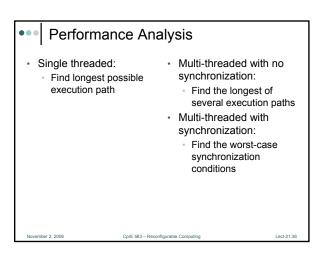


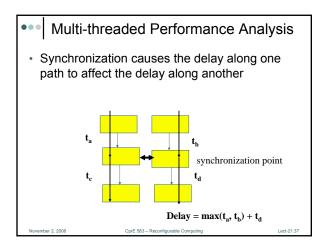


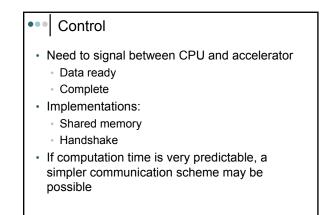


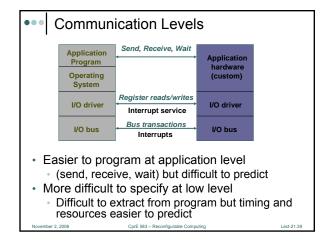


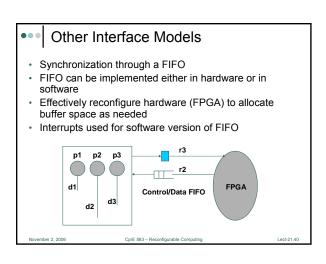


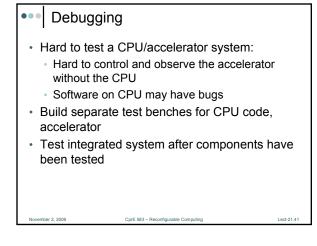


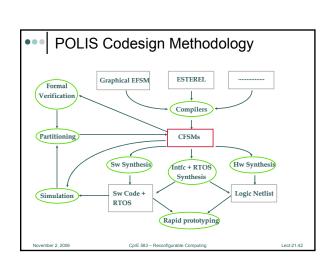












Codesign Finite State Machines

- · POLIS uses an FSM model for
 - Uncommitted
 - Synthesizable
 - Verifiable

Control-dominated HW/SW specification

- Translators from
 - · State diagrams,
 - Esterel, ECL, ReactiveJava
 - HDI s

Into a single FSM-based language

CprE 583 - Reconfigurable Computing

••• CFSM behavior

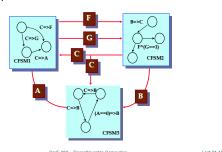
- · Four-phase cycle:
 - ☆ Idle
 - O Detect input events
 - Execute one transition
 - Emit output events
- Software response could take a long time:
 - Unbounded delay assumption
- · Need efficient hw/sw communication primitive:
 - Event-based point-to-point communication

Nevember 2, 200

CprE 583 - Reconfigurable Computing

••• Network of CFSMs

Globally Asynchronous, Locally Synchronous (GALS) model



••• Summary

- Hardware/software codesign complicated and limited by performance estimates
- Algorithms not generally as good as human partitioning
- Other interesting issues include dual processors, special memory interfaces
- Will likely evolve at faster rate as compilers evolve

November 2, 200

CprE 583 – Reconfigurable Computing

Lect-21.46