GALOIS FIELD ARITHMETIC UNIT

Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber

CMPE 450: Systems Requirement Review

BACKGROUND

Galois Field (pronounced “Gal-o-AH”)

- Field that contains a finite number of elements
  - Fields are bounded over +, -, *, /
  - Every operation has an inverse
- Represented as GF(*p*), where *p* is a prime number
- GF(2) is the best known and most frequently used
- Each term of the field is generated from a “generating polynomial” which is irreducible

Galois Field Arithmetic Unit

- The arithmetic logic unit (ALU) deals with irreducible polynomials in $GF(2^n)$, for $2 \leq n \leq 16$
- The unit:
  - Determines irreducibility
  - Generates the terms
  - Allows operations to be applied between the terms:
    - Addition
    - Subtraction
    - Multiplication
    - Division
    - Logarithm

Purpose and Scope

- Serve as a computation engine for a relatively low-powered microcontroller, and would enable complex code and encryption algorithms
- Advanced Encryption Standard (AES) has one step which uses Galois Fields

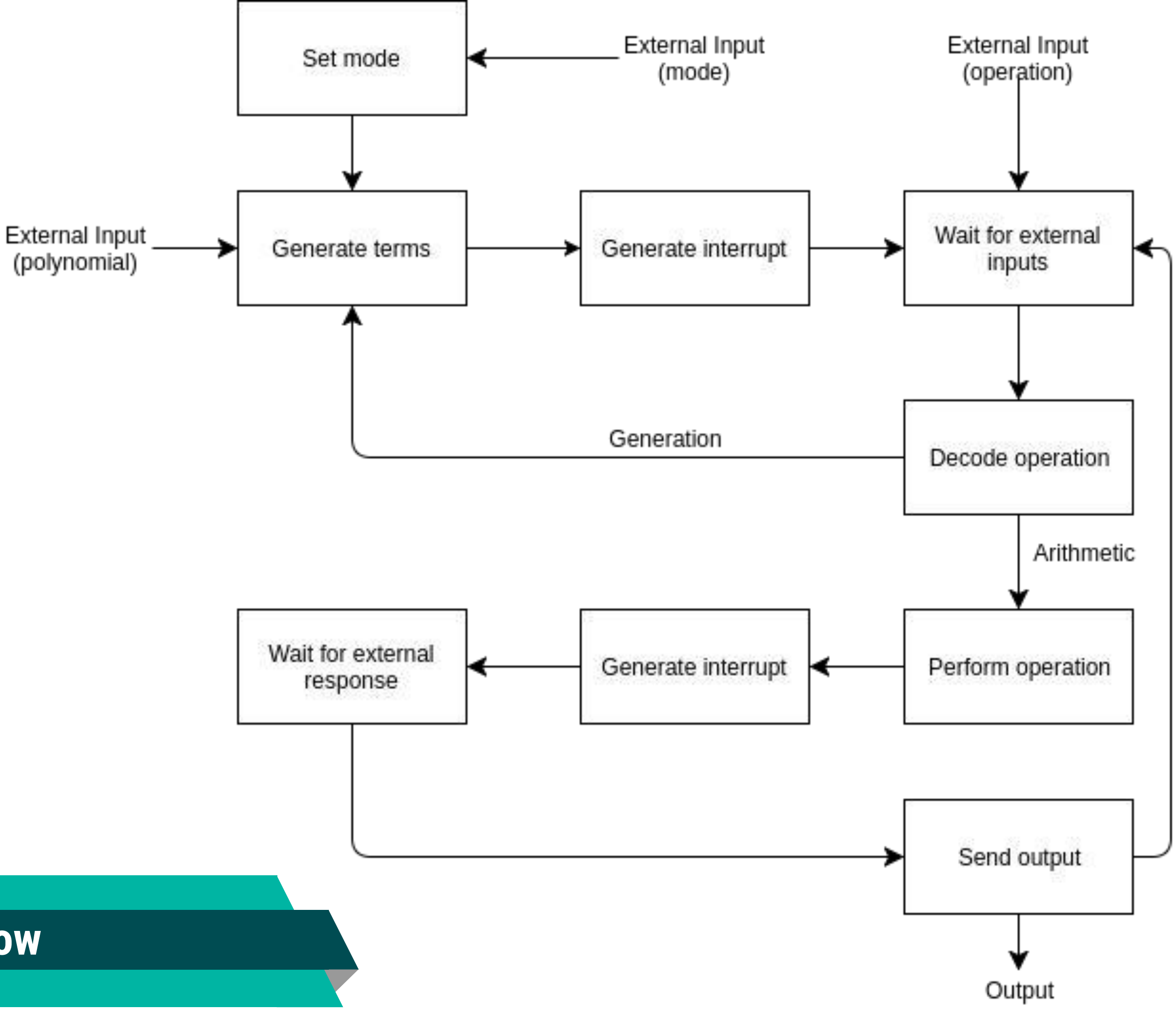
MISSION AND REQUIREMENTS

Mission Requirements

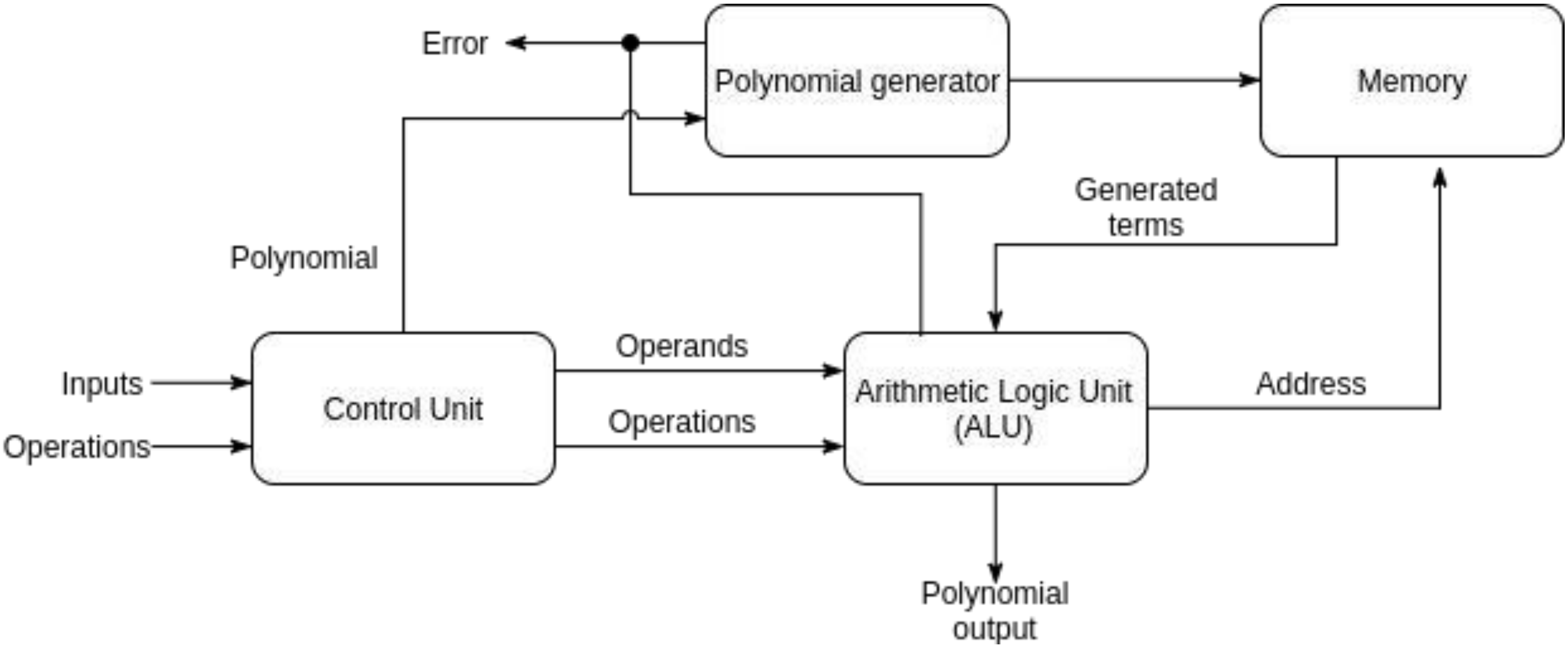
- **The ALU shall be able to:**
  - Generate Galois fields given a valid generating polynomial
  - Perform operations within the generated field
  - Store generated fields in memory
  - Convert input symbols to their polynomial values before completing operations
  - Lookup polynomial values in the table
  - Conduct all external communication on busses

Functional Flow

1. Set mode bits
2. Give generating polynomial
3. After terms are generated, arithmetic operations can be done
4. A new generating polynomial can be given to generate a new field, but the old one will be overwritten



Functional Flow


Error
Polynomial generator
Memory
Generated terms
Polynomial
Operands
Inputs
Control Unit
Arithmetic Logic Unit (ALU)
Address
Operations
Operations
Polynomial output

Data Flow

PRELIMINARY REQUIREMENTS

Architectural Synthesis

- Scalable - many trade-off options
- Decisions on trade-offs can be made down the road
- Term generation and logarithm operation are scalable
- Simpler operations are done in constant time

Trade-off Details

- Terms generated per clock vs. number of gates used
- Speed vs. memory
- Clock speed vs. terms generated per clock

System Interface

- Inputs, controls and errors given/received on a data bus
- Data bus can be set to use either 8, 16, or 32 bits to interface with a variety of external devices
- Depending on the size of the Galois field and bus size, inputs and controls may need to be sent on separate cycles
- Mode register to store settings

Specification Development

- Currently, all physical and cost specifications are concrete
- Specifications to be determined: design size and speed
  - Depends on the details of the design of purchased FPGA
- Flexible design
  - Trade-off decisions can be made later
- Unsure about power requirements

Constraints

- Prototype budget under $400.00
- Cost of large scale production to be less than $1 per chip
- Included in prototype
  - 64 or fewer pins
  - Area less than 24 square inches
- Shooting for [50]MHz

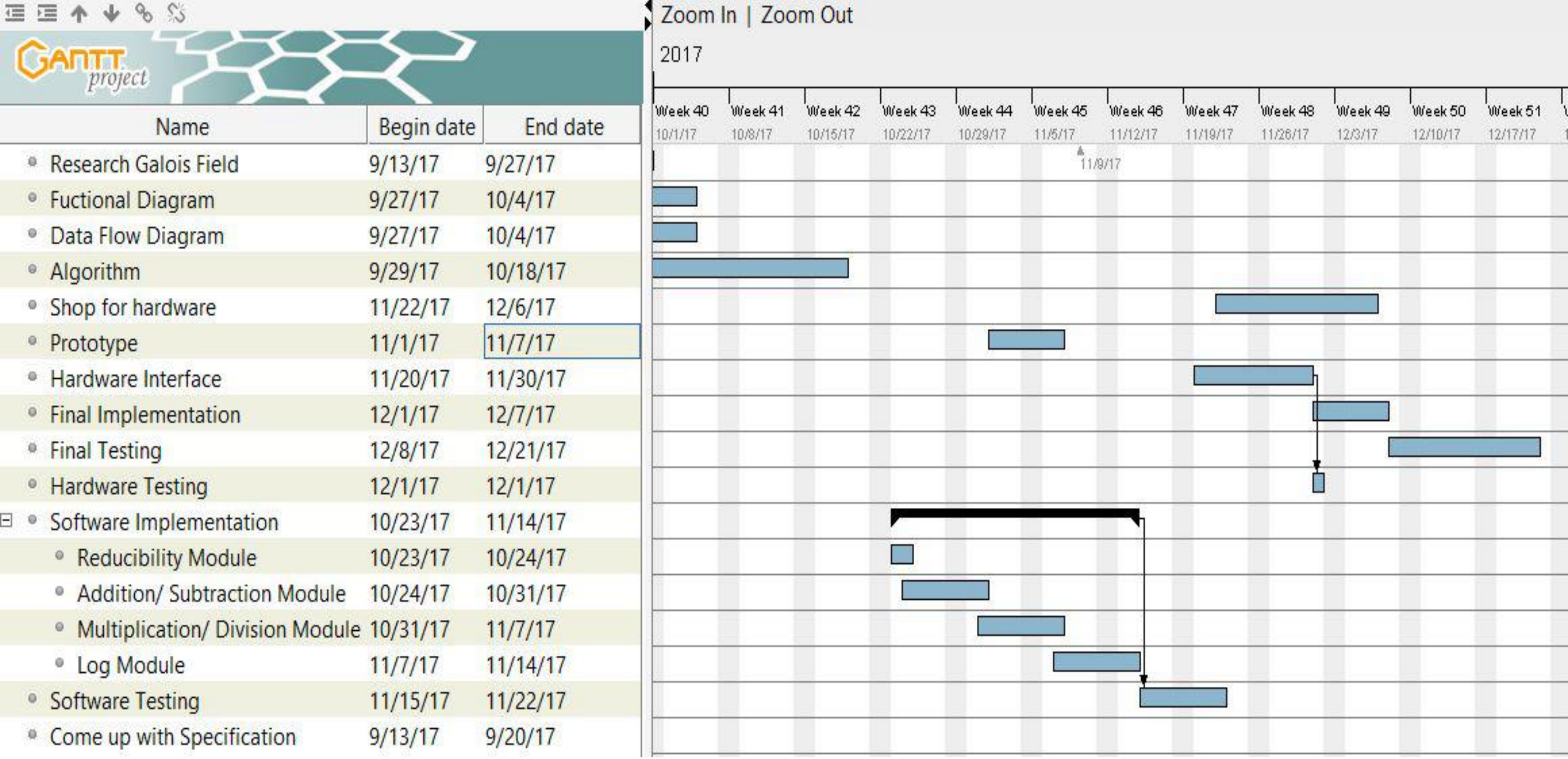
PROGRAM RISK ANALYSIS

Challenges

- Communication between microcontroller and FPGA
- Memory/register bandwidth could be a large limiting factor
- FPGA size
- Variable sized data bus

Testing/ Measurement

- Digital logic analyzer
- Oscilloscope
- VHDL simulations
  - All simulations should work by the end of the semester



Name	Begin date	End date
Research Galois Field	9/13/17	9/27/17
Fuctional Diagram	9/27/17	10/4/17
Data Flow Diagram	9/27/17	10/4/17
Algorithm	9/29/17	10/18/17
Shop for hardware	11/22/17	12/6/17
Prototype	11/1/17	11/7/17
Hardware Interface	11/20/17	11/30/17
Final Implementation	12/1/17	12/7/17
Final Testing	12/8/17	12/21/17
Hardware Testing	12/1/17	12/1/17
Software Implementation	10/23/17	11/14/17
Reducibility Module	10/23/17	10/24/17
Addition/ Subtraction Module	10/24/17	10/31/17
Multiplication/ Division Module	10/31/17	11/7/17
Log Module	11/7/17	11/14/17
Software Testing	11/15/17	11/22/17
Come up with Specification	9/13/17	9/20/17

Schedule

QUESTIONS?

GFAU