MEMO NUMBER: 03
DATE: October 15, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: System Requirement Specifications Draft

1 Introduction

A Galois field is a field with a finite number of elements. The nomenclature $GF(q)$ is used to indicate a Galois field with q elements. For $GF(q)$ in general, q must be a power of a prime. For each prime power, there exists exactly one finite field. The best known and most used Galois field is $GF(2)$, the binary field.

The Galois Field Arithmetic Unit handles irreducible polynomials in $GF(2^n)$, where $\{2 \leq n \leq 16\}$. The ALU generates all the terms in the field of the polynomial, and allows the user to view and apply addition, subtraction, multiplication, division or logarithm between them.

1.1 Document Overview

1.2 System Overview

1.3 Mission Scenario

Cryptography has many expensive calculations that are difficult for low power and inexpensive microcontroller units to handle. The GFAU will make Galois field calculations more accessible to these low power devices.

1.4 System Boundary Diagram

1.5 Data Flow Diagram

1.6 Functional Flow Diagram

2 Requirements

2.1 System Requirements

2.2 Hardware Requirements

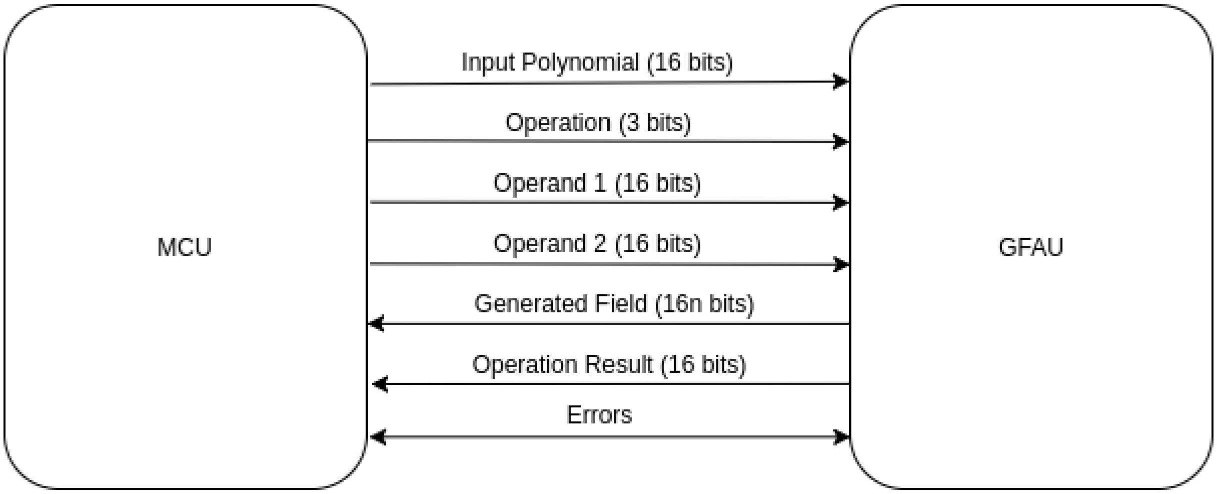
MCU
GFAU
Input Polynomial (16 bits)
Operation (3 bits)
Operand 1 (16 bits)
Operand 2 (16 bits)
Generated Field (16n bits)
Operation Result (16 bits)
Errors

Figure 1: System Boundary Diagram of the Galois Field Arithmetic Unit , where n is the Number of Terms

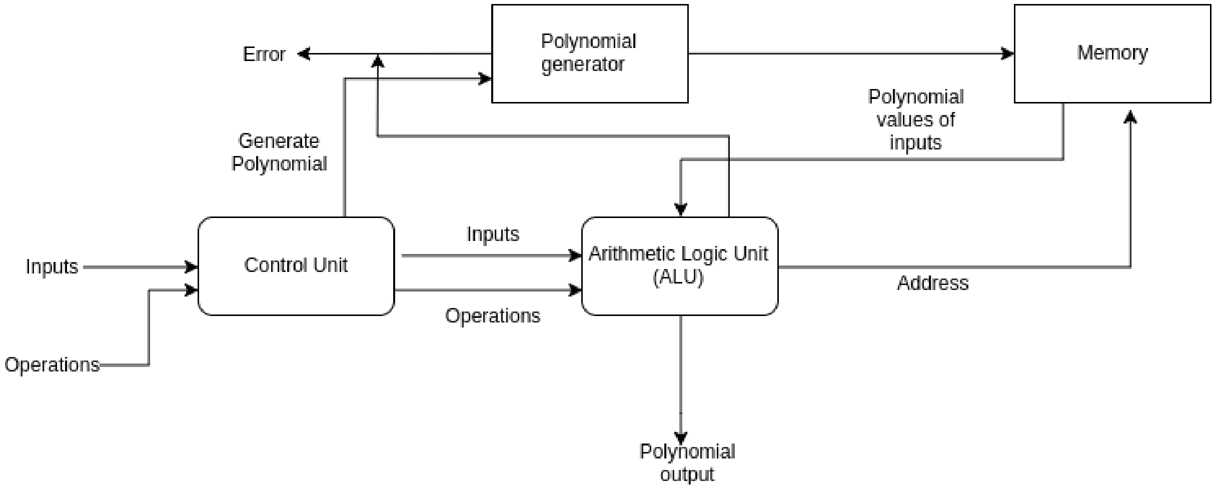

Figure 2: Data Flow Diagram of the Galois Field Arithmetic Unit