MEMO NUMBER: GFAU-SRS
DATE: September 27, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: GFAU Specification Requirements Statement

1 INTRODUCTION

This document servers to enumerate specific requirements of the GFAU.

2 BACKGROUND

The Galois Field Arithmetic Unit (GFAU) is a hardware-based unit for performing arithmetic operations in Galois Field 2^n, where n = 2 . . . 10. Unit will accept inputs to determine n, and to establish the field generating polynomial. A GFAU would serve as a computation engine for a relatively low-powered microcontroller, and would enable complex code and encryption algorithms. Project will include implementation of a Reed Solomon encoder and decoder using the GFAU.

3 SPECIFICATION

1. At a minimum, the GFAU shall handle inputs up to polynomial degree 8 (G(8)).
2. The GFAU should handle inputs up to polynomial degree 16 (G(16)).
3. The GFAU shall be implemented using FPGA.
4. The GFAU shall provide addition, subtraction, multiplication, division, and logarithms within the context of Galois Fields.
5. The GFAU shall be able to generate lookup tables for each operation in (4) given an irreducible polynomial.
6. The GFAU should be able to determine if an input polynomial is reducible or not.
7. The total cost should be under $400.