# Research Project Executive Summary

<table>
<thead>
<tr>
<th><strong>Project Name:</strong></th>
<th>Accelerating Galois Field Arithmetics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary as of Date:</strong></td>
<td>Nov 2015</td>
</tr>
<tr>
<td><strong>Project Type (Proposed, New or Continuing):</strong></td>
<td>Continuing</td>
</tr>
<tr>
<td><strong>Project Center (UCSC), Center Director:</strong></td>
<td>Ethan L. Miller</td>
</tr>
<tr>
<td><strong>Project Investigators:</strong></td>
<td>Ethan Miller, Darrell Long, Andy Hospodor, Lincoln Thurlow, Andrew Kwong</td>
</tr>
<tr>
<td><strong>Affiliates/Collaborators:</strong></td>
<td>UCSC</td>
</tr>
</tbody>
</table>

## Project Description:
Investigating performance benefits of using SIMD for Galois field arithmetic. Galois fields are used in many applications including Reed-Solomon (RS) codes and Algebraic signatures. Increasing the performance of the underlying Galois field arithmetic provides increased performance benefit for applications such as Erasure Codes.

## Proposed Budget:
$45,000 per year

## Estimated (or Actual) Start Date:
Winter 2015

## Progress to Date:
Nov 2015: AVX2 GF(8)/GF(16) works better, on average 30% faster than previously published SSSE3 implementations. Known issue with algorithm saturating L1, L2, and L3 caches causing performance degradation for larger region size multiplication. Testing different algorithms based on cache performance, implementing SSSE3 on ARM using NEON instruction set.


## Publications (past 6 months)
N/A
Milestones and Deliverables for Current Year

Months 1–6
- Understand Galois Fields + Erasure Codes
- Implement previously published methods in library

Months 7–12
- Implement previously published methods using AVX2
- Improve AVX2 implementation using improved algorithms
- Implement arithmetic for algebraic signatures
- Benchmark and analyze system performance

Completion Criteria (if known)
- Open Source Gferasure library
- Publication to top systems conference

Develop new Approach
- For Galois arithmetic in GF(8) and GF(16) using AVX2
- For extending Galois arithmetic to algebraic signatures

Related Work within CRSS:
- “Screaming Fast Galois Field Arithmetic Using Intel SIMD Extensions” FAST 2013
- “Optimizing Galois Field Arithmetic for Diverse Processor Architectures” MASCOTS 2008
- “Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage” ICDCS 2006

Related Work Elsewhere:
- “The Mathematics of RAID 6” 2007 (Linux Kernel)
- GF-Complete (Library, Jim Plank)
- Libmoepgf (Library, Stephan Matthias Günther)
- “Efficient GF Arithmetic for Linear Network Coding using Hardware SIMD Extensions” NetCod 2014

How Our Proposal Is Different:
Using AVX/AVX2 to determine if instruction set provides additional performance. Additionally implementing functions, which can be used for Rabinesque and other algebraic signatures.

Potential Benefits to CRSS Members:
Faster methods for encoding using Reed-Solomon codes. Open source library with very easy integration and modification for commercial applications.