EE671: VLSI Design Course Project
Lagrange Interpolator for Threshold Signature Scheme

Group 37

November 29, 2025

1 Executive Summary

This report documents the design and synthesis of a 256-bit Lagrange Interpolator for (2,3) threshold signature schemes. The implementation includes finite field arithmetic over the secp256k1 prime modulus and has successfully completed RTL design, verification, and logic synthesis. Physical design is pending and will be completed subsequently.

2 Introduction

2.1 Project Overview

The project implements the Lagrange interpolation component of a (2,3) threshold signature scheme used in blockchain systems. Given two shares (x_1, y_1) and (x_2, y_2) from participants, the design reconstructs the secret $P(0)$ where $P(x)$ is a degree-1 polynomial.

2.2 Mathematical Foundation

For a polynomial $P(x) = a_0 + a_1 x$, the secret is reconstructed as:

$$secret = y_1 \cdot \frac{-x_2}{x_1 - x_2} + y_2 \cdot \frac{-x_1}{x_2 - x_1} p$$

where

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1.$$

3 Architecture and Design

3.1 Top-Level Module

```
module lagrange_interp (
    input wire clk, rst_n,
    input wire [255:0] x1, y1, x2, y2,
    input wire start,
    output reg [255:0] secret,
    output reg done, error
);
```

3.2 Submodules

- `mod_add.v` – Modular addition
- `mod_sub.v` – Modular subtraction
- `mod_mul.v` – Modular multiplication
- `mod_inv.v` – Modular inversion

3.3 Finite State Machine

The design uses a 10-state FSM:

1. IDLE
2. CALC_DENOMS
3. CALC_NUMERATORS
4. MOD_INV_1
5. CALC_L1
6. MOD_INV_2
7. CALC_L2
8. CALC_TERM1
9. CALC_TERM2
10. FINAL_ADD $\rightarrow$ DONE

4 Pre-Synthesis Verification

4.1 Testbench Design

Testbench includes three major tests:

- **Test 1:** Basic reconstruction
- **Test 2:** Error case (duplicate x-values)
- **Test 3:** Large random values

4.2 Simulation Results

```
=== Test Summary ===
Passed: 3/3
ALL TESTS PASSED!
```

5 Logic Synthesis

5.1 Synthesis Setup

- **Tool:** Cadence Genus 21.19
- **Technology:** TSMC 65nm (tcbn65gpluswc$_c cs.lib$)
- **Clock:** 100MHz (10ns period)
- **Constraints:** Input/output delay of 1.5ns

5.2 Synthesis Challenges

- Large 256-bit datapath requiring 4.5M+ instances
- Peak memory usage 13.6GB
- Tool internal errors requiring PBS disabling
- Runtime exceeding 3 hours

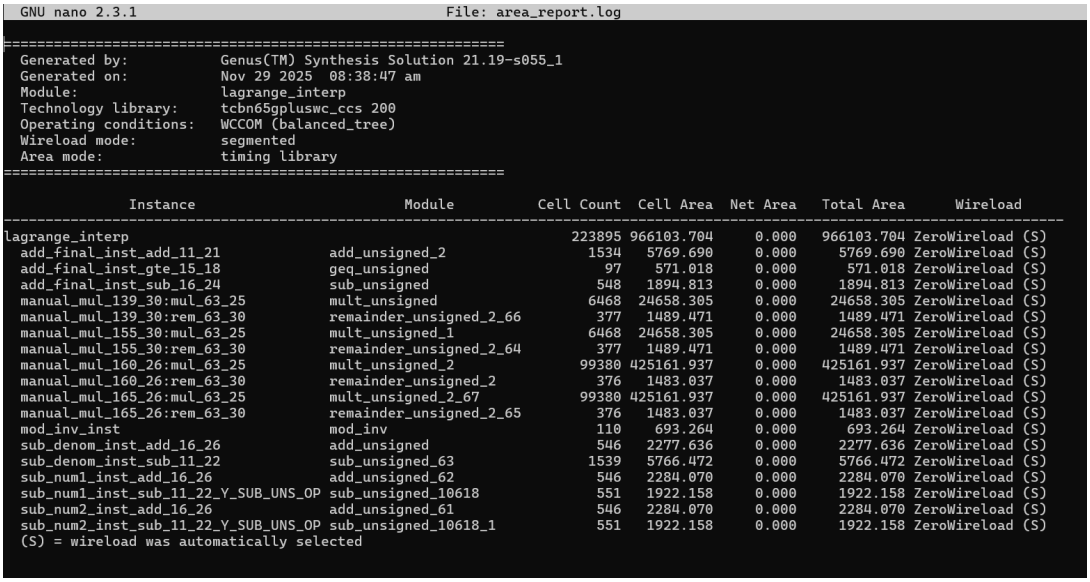
5.3 Synthesis Results

Generated output:

- `post_synthesis_netlist.v`
- `area_report.log`
- `timing_report.log`

6 Performance Analysis

6.1 Area Results



```
GNU nano 2.3.1                                File: area_report.log

=======================================================
  Generated by:           Genus(TM) Synthesis Solution 21.19-s055_1
  Generated on:           Nov 29 2025  08:38:47 am
  Module:                 lagrange_interp
  Technology library:     tcbn65gpluswc_ccs 200
  Operating conditions:   WCCOM (balanced_tree)
  Wireload mode:          segmented
  Area mode:              timing library
=======================================================

              Instance                          Module          Cell Count  Cell Area  Net Area   Total Area      Wireload
-------------------------------------------------------------------------------------------------------------------------------
lagrange_interp                                                   223895 966103.704     0.000   966103.704 ZeroWireload (S)
  add_final_inst_add_11_21             add_unsigned_2                1534   5769.690     0.000     5769.690 ZeroWireload (S)
  add_final_inst_gte_15_18             geq_unsigned                    97    571.018     0.000      571.018 ZeroWireload (S)
  add_final_inst_sub_16_24             sub_unsigned                   548   1894.813     0.000     1894.813 ZeroWireload (S)
  manual_mul_139_30:mul_63_25          mult_unsigned                 6468  24658.305     0.000    24658.305 ZeroWireload (S)
  manual_mul_139_30:rem_63_30          remainder_unsigned_2_66        377   1489.471     0.000     1489.471 ZeroWireload (S)
  manual_mul_155_30:mul_63_25          mult_unsigned_1               6468  24658.305     0.000    24658.305 ZeroWireload (S)
  manual_mul_155_30:rem_63_30          remainder_unsigned_2_64        377   1489.471     0.000     1489.471 ZeroWireload (S)
  manual_mul_160_26:mul_63_25          mult_unsigned_2              99380 425161.937     0.000   425161.937 ZeroWireload (S)
  manual_mul_160_26:rem_63_30          remainder_unsigned_2           376   1483.037     0.000     1483.037 ZeroWireload (S)
  manual_mul_165_26:mul_63_25          mult_unsigned_2_67           99380 425161.937     0.000   425161.937 ZeroWireload (S)
  manual_mul_165_26:rem_63_30          remainder_unsigned_2_65        376   1483.037     0.000     1483.037 ZeroWireload (S)
  mod_inv_inst                         mod_inv                        110    693.264     0.000      693.264 ZeroWireload (S)
  sub_denom_inst_add_16_26             add_unsigned                   546   2277.636     0.000     2277.636 ZeroWireload (S)
  sub_denom_inst_sub_11_22             sub_unsigned_63               1539   5766.472     0.000     5766.472 ZeroWireload (S)
  sub_num1_inst_add_16_26              add_unsigned_62                546   2284.070     0.000     2284.070 ZeroWireload (S)
  sub_num1_inst_sub_11_22_Y_SUB_UNS_OP sub_unsigned_10618             551   1922.158     0.000     1922.158 ZeroWireload (S)
  sub_num2_inst_add_16_26              add_unsigned_61                546   2284.070     0.000     2284.070 ZeroWireload (S)
  sub_num2_inst_sub_11_22_Y_SUB_UNS_OP sub_unsigned_10618_1           551   1922.158     0.000     1922.158 ZeroWireload (S)
  (S) = wireload was automatically selected
```

Figure 1: Area utilization report

Key metrics:

- Total Cell Count: 222,895
- Combinational Area: 966,103.704 μm^2
- Sequential Area: 0.000 μm^2
- Total Area: 966,103.704 μm^2

6.2 Timing Results

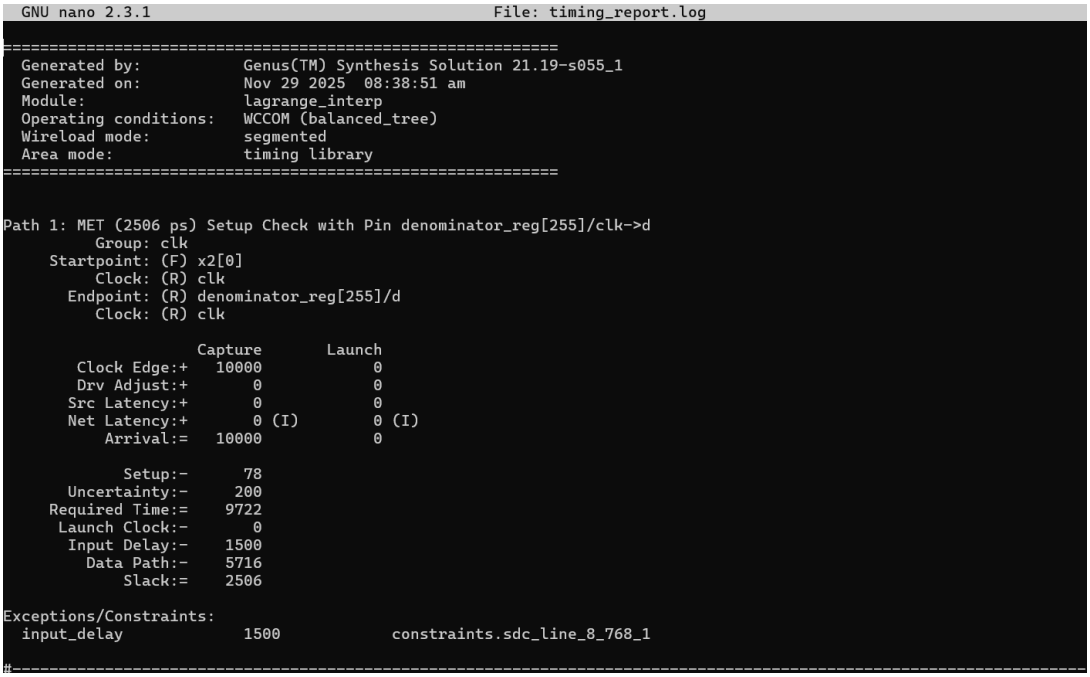


Figure 2: Timing analysis report

Key timing metrics:

- Worst Negative Slack (WNS): +2506 ps
- Total Negative Slack (TNS): 0 ns
- Clock: 100MHz
- Timing: MET

7 Conclusion and Future Work

7.1 Completed Work

- RTL design
- Finite field arithmetic modules
- Full verification
- Synthesis (TSMC 65nm)

7.2 Pending Work

- Physical design
- Gate-level simulation

- Post-layout verification
- DRC/LVS cleanup

7.3 Technical Challenges Overcome

- Complex finite-field arithmetic
- Large datapath optimization
- Tool limitations and memory constraints

8 Contributions

Name	**Contributions**
Shivam Panwar	Verilog development and logic synthesis using Cadence Genus

Table 1: Individual contributions to the project