INDIAN INSTITUTE OF TECHNOLOGY, GUWAHATI

Department of Computer Science and Engineering

Project Report on

Crypto Sign Synth

Submitted To

Assoc. Prof.

Dr. Chandan Karfa

Submitted By

Anuj Singh Thakur (224101008)

Nihal M. Singh (224101038)

Vaishali Chaudhari (224101055)

Shikha (224101066)

Yashvi Bipinbhai Rajvir (224101061)

For course fulfilment of CS577: C-BASED-VLSI-DESIGN

Phase 2 Report:

In this phase of the project, we focused on improving area efficiency and reducing latency in hardware implementation. We achieve this through two distinct optimization strategies:

Area Optimization

- **Function Inlining:**

  We replace function calls with the actual code of the function at the call site. This optimization reduces function call overhead and enhances execution speed.

- **Loop Unrolling:**

  We duplicate loop bodies to decrease the number of loop iterations, thus eliminating loop overhead. This results in faster execution of loop-based operations.

- **Function Allocation Instance Set to 1:**

  We ensure that only one instance of each function is created and reused throughout the code. This reduces memory overhead and enhances the efficiency of function invocation.

Latency Optimization

To reduce latency, we implement a pipeline architecture in the code. The pipeline architecture enables the concurrent execution of multiple stages of processing, reducing the overall latency. The following steps are undertaken:

- The code is broken down into smaller, independent stages.
- These stages are processed in parallel, making efficient use of system resources.
- The pipeline architecture minimizes waiting times for dependent operations, thereby reducing overall latency and enhancing performance.

Experimental Result

- **Low Area Overhead (Flip Flops, LUT, BRAM etc.)**
  - Initial Resource Utilization Summary:

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	0	253	-
FIFO	-	-	-	-	-
Instance	70	88	42281	183797	0
Memory	-	-	-	-	-
Multiplexer	-	-	-	114	-
Register	-	-	174	-	-
Total	70	88	42455	184164	0
Available	730	740	269200	134600	0
Utilization (%)	9	11	15	136	0

Experimental Result

- **Optimized Resource Utilization Summary:**

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	3	-	-	-
Expression	-	10	0	3997	-
FIFO	-	-	-	-	-
Instance	34	75	21614	99072	0
Memory	29	-	0	0	0
Multiplexer	-	-	-	3331	-
Register	-	-	2294	-	-
Total	63	88	23908	106400	0
Available	730	740	269200	134600	0
Utilization (%)	8	11	8	79	0

Resource Utili zation Comparison			
	Initial	Optimized	Percentage Reduce
LUT	184164	106400	42.22 %
FF	42455	23908	43.68%
BRAM	70	63	1.00 %
DSP	88	88	0.00 %

Experimental Result

- Initial Co-simulation Report for 'pqcrystals_dilithium2_ref'

Result

		Latency			Interval		
RTL	Status	min	avg	max	min	avg	max
VHDL	NA	NA	NA	NA	NA	NA	NA
Verilog	Pass	449330	573221	697113	697114	697114	697114

- **After Optimization:**
  - Co-simulation Report for 'pqcrystals_dilithium2_ref'

Result

		Latency			Interval		
RTL	Status	min	avg	max	min	avg	max
VHDL	NA	NA	NA	NA	NA	NA	NA
Verilog	Pass	376465	471544	566624	566625	566625	566625

Latency Comparison in Co-Simulation Report			
	Initial	Optimized	Percentage Reduce
Min	449330	376465	16.21%
Avg.	573221	471544	17.73%
Max	697113	566624	18.71 %

Conclusion:

This project represents an effort to synthesize the **Dilithium** AES digital signature scheme into hardware, with a focus on optimization for both area and latency.