Group Name: 8 bit adder

Members:
Arpan Khanna 200101121
Mukul Lakra 200101069
Aman Soni 200101012
Om Gunjal 200101037
Kartik Malaysia 200101053

Description:

PartA: To minimize area overhead (no. of FF, LUTs, BRAMs, etc.) of the given PQC code
Approach used includes inlining of the code to reduce the area overhead of the code.

In the file fips202.c, the following changes are made:
1. HLS INLINE in the functions keccak_absorb, keccak_squeezeblocks, shake_128_absorb, shake_128_squeezeblocks, shake256_absorb, shake256_squeezeblocks, shake_128, shake_256, sha3_256, sha3_512.
2. HLS ALLOCATION in the function keccak_squeezeblocks.

In the file indcpa.c, the following changes are made:
1. HLS INLINE in the functions gen_matrix, indcpa_enc, indcpa_dec.

In the file poly.c, the following changes are made:
1. HLS INLINE in the functions poly_tomont, poly_reduce, poly_csubq, poly_add, poly_sub.

In the file polyvec.c, the following changes are made:
1. HLS INLINE in the functions polyvec_ntt, polyvec_invntt_tomont, polyvec_pointwise_acc_montgomery, polyvec_reduce, polyvec_csubq, polyvec_add.

Old Values of Area:
BRAM_18K: 81
DSP48E: 145
FF: 27242
LUT: 122132

New Values of Area:
BRAM_18K: 61

DSP48E: 134
FF: 13256
LUT: 50846

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	-	-	-	-
Expression	-	-	0	251	-
FIFO	-	-	-	-	-
Instance	66	145	27044	120744	0
Memory	15	-	48	25	0
Multiplexer	-	-	-	1112	-
Register	-	-	150	-	-
Total	81	145	27242	122132	0
Available	2060	2800	607200	303600	0
Utilization (%)	3	5	4	40	0

Old values of area

Summary

Name	BRAM_18K	DSP48E	FF	LUT	URAM
DSP	-	76	-	-	-
Expression	-	-	0	4808	-
FIFO	-	-	-	-	-
Instance	18	58	9831	41497	0
Memory	43	-	70	41	0
Multiplexer	-	-	-	4500	-
Register	-	-	3355	-	-
Total	61	134	13256	50846	0
Available	2060	2800	607200	303600	0
Utilization (%)	2	4	2	16	0

New values of area

PartB: To minimize the latency of the the given PQC code
Approach uses include loop unrolling, pipelining of the code to reduce the latency of the code.

In the file fips202.c, the following changes are made:
1. HLS UNROLL in function load64 in line 24
2. HLS UNROLL in function store64 in line 42
3. HLS INLINE, HLS UNROLL factor=25,HLS PIPELINE in function keccak_absorb in line 60
4. HLS ALLOCATION, HLS INLINE, HLS UNROLL factor=25,HLS PIPELINE in function keccak_squeezeblocks in line 90
5. Similarly HLS inline in shake_128, shake256, sha3_256, sha3_512. Also HLS UNROLL factor=32 in sha3_256 and factor = 64 sha3_512. Also HLS pipeline in the above functions are done.

In the file indcpa.c, the following changes are made:
1. HLS UNROLL in the functions pack_pk, unpack_pk.
2. HLS INLINE in the functions gen_matrix, indcpa_enc, indcpa_dec.

In the file poly.c, the following changes are made:
1. HLS UNROLL in the functions poly_frommsg, poly_basemul_montgomery, poly_tomont, poly_reduce, poly_csubq, poly_add, poly_sub.
2. HLS INLINE in the functions poly_tomont, poly_reduce, poly_add.
3. HLS PIPELINE in the functions poly_compress, poly_decompress, poly_tobytes, poly_frombytes, poly_tomsg.

In the file polyvec.c:
1. HLS INLINE in polyvec_ntt, polyvec_invtt_tomont, polyvec_pointwise_acc_montgomery, polyvec_reduce, polyvec_csubq, polyvec_add.

In the file symmetric-shake.c:
1. HLS UNROLL in the functions kyber_shake128_absorb, kyber_shake256_prf.

Old value of latency:
Min: 214392
Avg: 214469
Max: 214547

New value of latency:
Min: 178946

Avg: 178952
Max: 178958

Cosimulation Report for 'crypto_kem_dec'

Result

		Latency			Interval		
RTL	Status	min	avg	max	min	avg	max
VHDL	NA	NA	NA	NA	NA	NA	NA
Verilog	Pass	214392	214469	214547	214548	214548	214548

Old values of Latency

Cosimulation Report for 'crypto_kem_dec'

Result

		Latency			Interval		
RTL	Status	min	avg	max	min	avg	max
VHDL	NA	NA	NA	NA	NA	NA	NA
Verilog	Pass	178946	178952	178958	178947	178947	178947

New values of Latency