INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY BANGALORE

Project Elective

on

Optimization of Parametric NTT Hardware Accelerator

under the guidance

of

Dr. Madhav Rao

Submitted by

Aman Prajapati [MT2022501] [Aman.Prajapati@iiitb.ac.in]

Lokesh Maji [MT2022509] [Lokesh.Maji@iiitb.ac.in]

FPGA IMPLEMENTATION OF PARAMETRIC NTT HARDWARE ACCELERATOR

Generated by:	Xilinx Vivado 2018.1
Generated on:	Jun 30 2023
Board:	Zedboard Zynq
Module:	NTTN
Operating conditions:	PVT_1P1V_0C (balanced_tree)
Ring size:	512
Area unit:	μm^2
Power unit:	W
Timing unit:	ns
Frequency unit:	GHz

1. Resource Utilization

a) 28 – bits

No. of PEs	LUTs	Reg	BRAM	DSP
2	1952	1704	11	14
4	3706	3021	12	28
8	7562	5684	16	56

b) 30 – bits

No. of PEs	LUTs	Reg	BRAM	DSP
2	2017	1818	11	14
4	3919	3241	12	28
8	8023	6116	16	56

2. Power

a) 28 – bits

No. of PEs	Device Static	Dynamic	Total
2	0.107	0.057	0.164
4	0.108	0.102	0.210
8	0.106	0.166	0.272

b) 30 – bits

No. of PEs	Device Static	Dynamic	Total
2	0.109	0.064	0.173
4	0.110	0.111	0.221
8	0.106	0.169	0.275

3. Timing

a) 28 – bits

No. of PEs	Clock Time Period	Worst Negative Slack	Frequency
2	15	0.435	0.06866
4	15	0.470	0.06882
8	15	0.495	0.06894

b) 30 – bits

No. of PEs	Clock Time Period	Worst Negative Slack	Frequency
2	15	0.483	0.06888
4	15	0.592	0.06941
8	15	0.469	0.06881

FPGA SYNTHESIS OF MODULUS MULTIPLICATION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR

Generated by:	Xilinx Vivado 2018.1
Generated on:	Jul 11 2023
Board:	Zedboard Zynq
Module:	ModRed
Operating conditions:	PVT_1P1V_0C (balanced_tree)
Ring size:	512
No. of PEs:	8
Area unit:	μm^2
Power unit:	W
Timing unit:	ns
Frequency unit:	GHz

1. Resource Utilization

a) 32 – bits

Type	LUTs	Reg	BRAM	DSP
CA	269	440	0	8
KA	299	517	0	0
OKA	58	366	0	0
Radix-4	56	364	0	0

b) 64 – bits

Type	LUTs	Reg	BRAM	DSP
CA	1814	1567	0	79
KA	994	1920	0	0
OKA	111	1352	0	0
Radix-4	111	1352	0	0

c) 128 – bits

Type	LUTs	Reg	BRAM	DSP
CA	20799	5055	0	189
KA	2191	4070	0	0
OKA	210	2776	0	0
Radix-4	210	2784	0	0

2. Power

a) 32 – bits

Type	Device Static	Dynamic	Total
CA	0.107	0.059	0.166
KA	0.107	0.102	0.209
OKA	0.104	0.005	0.109
Radix-4	0.104	0.005	0.109

b) 64 – bits

Type	Device Static	Dynamic	Total
CA	0.110	0.135	0.245
KA	0.108	0.055	0.163
OKA	0.105	0.013	0.118
Radix-4	0.105	0.013	0.118

c) 128 – bits

Type	Device Static	Dynamic	Total
CA	0.112	0.283	0.395
KA	0.109	0.087	0.196
OKA	0.105	0.041	0.146
Radix-4	0.105	0.041	0.146

3. Timing

a) 32 – bits

Type	Clock Time Period	Worst Negative Slack	Frequency
CA	20	9.603	0.09618
KA	30	20.100	0.10101
OKA	30	21.522	0.11795
Radix-4	30	21.522	0.11795

b) 64 – bits

Type	Clock Time Period	Worst Negative Slack	Frequency
CA	20	7.860	0.08237
KA	30	20.100	0.10101
OKA	30	21.522	0.11795
Radix-4	30	21.522	0.11795

c) 128 – bits

Type	Clock Time Period	Worst Negative Slack	Frequency
CA	30	9.517	0.04882
KA	30	20.100	0.10101
OKA	30	20.910	0.11001
Radix-4	30	20.910	0.11001

SYNTHESIS OF PARAMETRIC NTT HARDWARE ACCELERATOR

Generated by:	Genus (TM) Synthesis Solution 21.10-p002_1
Generated on:	Jun 27 2023
Module:	NTTN
Technology library:	fast_vdd1v0 1.0
Technology node:	45 nm
Operating conditions:	PVT_1P1V_0C (balanced_tree)
Wireload mode:	enclosed
Area mode:	timing library
Ring size:	512
Area unit:	μm^2
Power unit:	W
Timing unit:	ns
Frequency unit:	GHz

1. Cells Count

a) 28 – bits

No. of PEs		Sequential	Inverter	Buffer	Logic	Total
Before Optimisation	2	146801	14888	11390	116789	289868
	4	177996	22156	11485	142707	354344
	8	183196	19744	5201	157973	366114
After Optimisation	2	146801	15453	11553	116785	290592
	4	177996	29073	11350	142610	361029
	8	183196	19333	9241	157747	369517

b) 30 – bits

No. of PEs		Sequential	Inverter	Buffer	Logic	Total
Before Optimisation	2	157235	18707	12121	125504	313567
	4	190664	20464	11970	160539	383637
	8	196236	26740	8640	168484	400100
After Optimisation	2	157235	19086	12562	125512	314395
	4	190664	25137	12447	160424	388672
	8	196236	26890	10677	168452	402255

2. Area

a) 28 – bits

No. of PEs	2	4	8
Before Optimization	1358759.844	1664750.664	1730785.050
After Optimization	1361497.212	1665951.084	1733996.088

b) 30 – bits

No. of PEs	2	4	8
Before Optimization	1463784.966	1793634.390	1863956.772
After Optimization	1459124.532	1793057.778	1863239.598

3. Power

a) 28 – bits

No. of PEs		Leakage	Internal	Switching	Total
Before Optimisation	2	7.20072e-05	4.45046e-02	1.47621e-03	4.60529e-02
	4	8.93349e-05	5.40839e-02	2.07826e-03	5.62515e-02
	8	9.31129e-05	6.05634e-02	3.24476e-03	6.39013e-02
After Optimisation	2	7.15813e-05	4.44778e-02	1.49869e-03	4.60480e-02
	4	8.90948e-05	5.40364e-02	2.07177e-03	5.61973e-02
	8	9.29892e-05	6.05156e-02	3.26561e-03	6.38742e-02

b) 30 – bits

No. of PEs		Leakage	Internal	Switching	Total
Before Optimisation	2	7.72525e-05	4.77479e-02	1.60918e-03	4.94343e-02
	4	9.57238e-05	5.79289e-02	2.26026e-03	6.02849e-02
	8	1.00802e-04	6.67305e-02	3.85174e-03	7.06831e-02
After Optimisation	2	7.67020e-05	4.77214e-02	1.63491e-03	4.94330e-02
	4	9.54060e-05	5.78852e-02	2.25296e-03	6.02335e-02
	8	1.00587e-04	6.67283e-02	3.80395e-03	7.06328e-02

4. Timing

a) 28 – bits

No. of PEs		Clock Time Period	Critical Path Slack	Frequency
Before Optimisation	2	10	7.5876	0.41452
	4	10	7.4630	0.39417
	8	10	7.4845	0.39753
After Optimisation	2	10	7.5859	0.41423
	4	10	7.4615	0.39393
	8	10	7.4830	0.39729

b) 30 – bits

No. of PEs		Clock Time Period	Critical Path Slack	Frequency
Before Optimisation	2	10	7.4217	0.38785
	4	10	7.3093	0.37165
	8	10	7.3052	0.37108
After Optimisation	2	10	7.4200	0.38759
	4	10	7.3078	0.37144
	8	10	7.3038	0.37144

SYNTHESIS OF MODULUS MULTIPLICATION BLOCK OF PARAMETRIC NTT HARDWARE ACCELERATOR

Generated by:	Genus (TM) Synthesis Solution 21.10-p002_1
Generated on:	JuL 11 2023
Module:	ModRed
Technology library:	fast_vdd1v0 1.0
Technology node:	45 nm
Operating conditions:	PVT_1P1V_0C (balanced_tree)
Wireload mode:	enclosed
Area mode:	timing library
Ring size:	512
No. of PEs:	8
Area unit:	μm^2
Power unit:	W
Timing unit:	ns
Frequency unit:	GHz

1. Area

a) 32 – bits

Type	Sequential	Inverter	Buffer	Logic	Area
CA	541	297	0	2709	12188.538
KA	493	56	0	478	4479.516
OKA	497	37	512	637	5741.154
Radix-4	360	33	0	363	3020.866

b) 64 – bits

Type	Sequential	Inverter	Buffer	Logic	Area
CA	1997	1084	0	14813	67104.846
KA	1850	106	0	1572	16314.768
OKA	1800	71	1792	2255	20249.820
Radix-4	1352	71	0	1358	11057.202

c) 128 – bits

Type	Sequential	Inverter	Buffer	Logic	Area
CA	4096	2105	160	49349	227438.550
KA	3990	176	0	3156	35062.866
OKA	3800	136	4096	4838	43671.690
Radix-4	2776	136	0	2790	22659.210

2. Power

a) 32 – bits

Type	Leakage	Internal	Switching	Total
CA	7.48758e-07	7.19894e-04	2.14789e-04	9.35432e-04
KA	2.79742e-07	3.00427e-04	3.35964e-05	3.35964e-04
OKA	3.71525e-07	2.62180e-04	2.61158e-05	2.88668e-04
Radix-4	1.88668e-07	1.83142e-04	1.69779e-05	2.00309e-04

b) 64 – bits

Type	Leakage	Internal	Switching	Total
CA	4.17438e-06	3.84269e-03	1.30815e-03	5.15501e-03
KA	1.02455e-06	1.13058e-03	6.39600e-05	1.19556e-03
OKA	1.31194e-06	9.38693e-04	2.65140e-05	9.66519e-04
Radix-4	6.94682e-07	6.80970e-04	1.23263e-05	6.93991e-04

c) 128 – bits

Type	Leakage	Internal	Switching	Total
CA	1.42813e-05	1.27252e-02	5.03143e-03	1.77710e-02
KA	2.20845e-06	2.44440e-03	1.37144e-04	2.58375e-03
OKA	2.83525e-06	1.99388e-03	5.99412e-05	2.05665e-03
Radix-4	1.42567e-06	1.39362e-03	2.42144e-05	1.41926e03

3. Timing

a) 32 – bits

Type	Clock Time Period	Critical Path Slack	Frequency
CA	10	6.4747	0.28366
KA	10	7.4663	0.39468
OKA	10	7.4798	0.39679
Radix-4	10	7.6530	0.42607

b) 64 – bits

Type	Clock Time Period	Critical Path Slack	Frequency
CA	10	3.5966	0.15617
KA	10	5.5593	0.22519
OKA	10	6.0136	0.25085
Radix-4	10	6.0915	0.25585

c) 128 – bits

Type	Clock Time Period	Critical Path Slack	Frequency
CA	10	0.1421	0.10144
KA	10	1.6940	0.12039
OKA	10	2.9257	0.14136
Radix-4	10	3.2860	0.14894

Comparison between Conventional Algorithm, Karatsuba Algorithm and Booth Radix – 4 Algorithm for top module NTTN

Generated by:	Genus (TM) Synthesis Solution 21.10-p002_1
Generated on:	JuL 18 2023
Module:	NTTN
Technology library:	fast_vdd1v0 1.0
Technology node:	45 nm
Operating conditions:	PVT_1P1V_0C (balanced_tree)
Wireload mode:	enclosed
Area mode:	timing library
Ring size:	512
Word size:	32 bits
No. of PEs:	8
Area unit:	μm^2
Power unit:	W
Timing unit:	ns
Frequency unit:	GHz

1. Area

No. of PEs	2	4	8
CA	1567394.208	1943704.674	2039650.038
KA	1551156.732	1897370.514	1960125.804
Radix-4	1542444.624	1890850.626	1948264.902

2. Power

No. of PEs	2	4	8
CA	5.23860e-02	6.67615e-02	7.65302e-02
KA	5.13042e-02	6.58049e-02	7.25853e-02
Radix-4	5.07187e-02	6.26243e-02	7.12235e-02

3. Performance

No. of PEs	2	4	8
CA	0.35265	0.35265	0.34864
KA	0.34410	0.33892	0.33892
Radix-4	0.34376	0.32376	0.33916